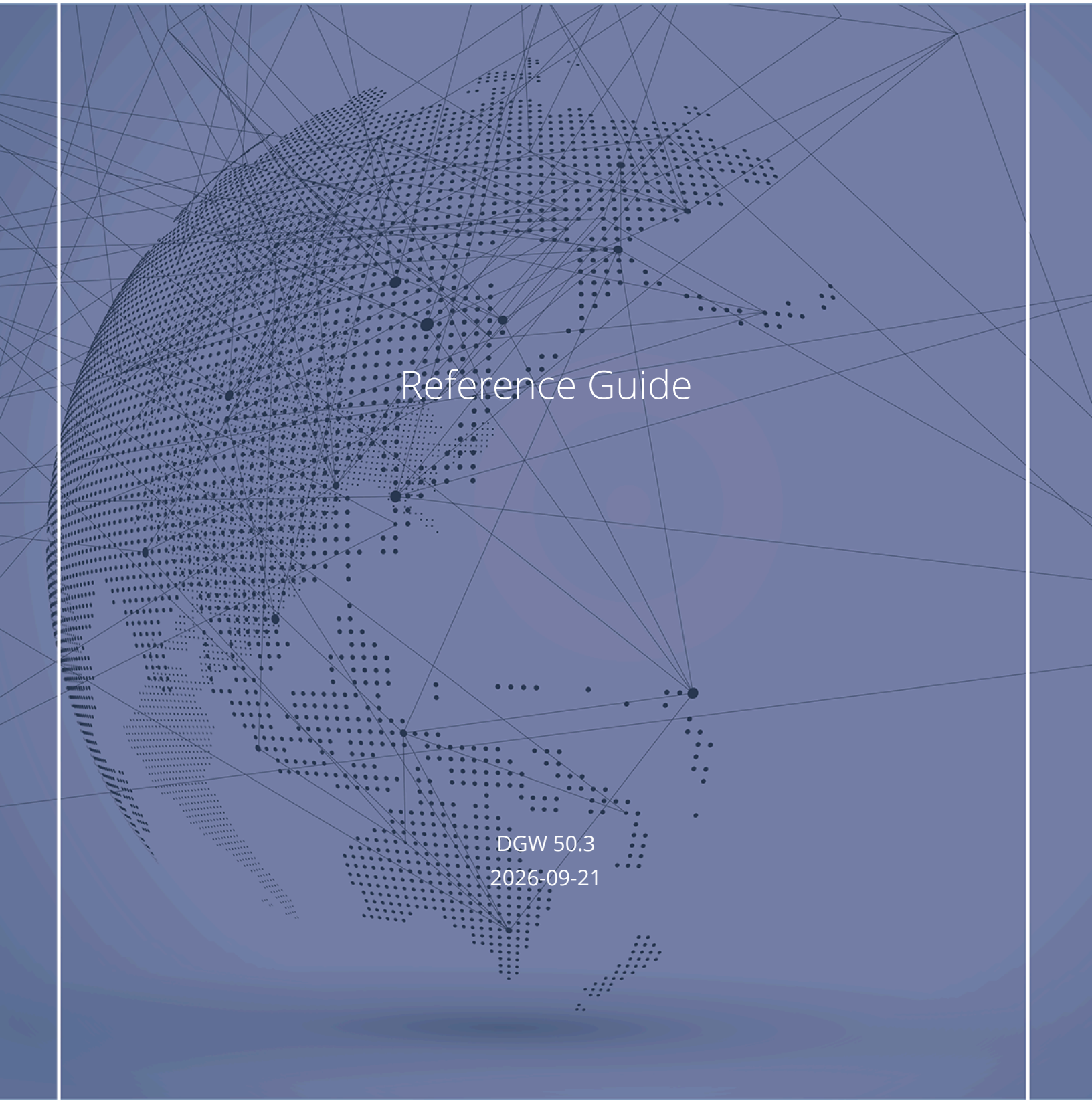
media5 corporation



Reference Guide

DGW 50.3

2026-09-21

Table of Contents

Special Scripting Commands 4

Services 5

Authentication, Authorization and Accounting (Aaa) 5
Basic Network Interfaces (Bni) 22
Call Detail Record (Cdr) 47
Certificate Manager (Cert) 56
Command Line Interface (Cli) 78
Configuration Manager (Conf) 89
Call Routing (CRout) 146
CPE WAN Management Protocol (Cwmp) 228
Device Control Manager (Dcm) 251
Dynamic Host Configuration Protocol Server (Dhcp) 269
E&M Channel Associated Signaling (Eam) 311
Element Management System (Ems) 344
Endpoint Administration (EpAdm) 355
Endpoint Services (EpServ) 369
Ethernet Manager (Eth) 440
File Manager (File) 460
Firmware Pack Updater (Fpu) 480
High Availability (Ha) 501
Host Configuration (Hoc) 513
IP routing (IpRouting) 540
Integrated Services Digital Network (Isdn) 556
Local Firewall (Lfw) 619
Link Layer Discovery Protocol (Lldp) 636

Local Quality of Service (LQos) 647
Media IP Transport (Mipt) 657
Music on Hold (Moh) 796
Network Address Translation (Nat) 807
Network Firewall (Nfw) 828
Notifications and Logging Manager (Nlm) 847
Network Traffic Control (Ntc) 873
Process Control Manager (Pcm) 880
Plain Old Telephony System Line (Pots) 887
R2 Channel Associated Signaling (R2) 924
Session Border Controller (Sbc) 978
Service Controller Manager (Scm) 1101
SIP Endpoint (SipEp) 1113
SIP Proxy (SipProxy) 1254
Simple Network Management Protocol (Snmp) 1287
Basic Telephony Interface (Tellf) 1301
Virtual Machine (Vm) 1329
Web Service (Web) 1353

Hardware Components 1365

Hardware (Hardware) 1365

Copyright Notice 1386

Special Scripting Commands

Command	Description
Pause ss	Pause the script for ss seconds. The value of ss must be between 1 and 300 seconds. This command cannot be aborted. The timer of the Pause command must be elapsed before another action can be performed. This command is only available in configuration scripts. It is not available with Cli or with Snmp. If a longer pause is necessary, multiple consecutive Pause commands can be used. Long pauses must be used with caution. Pauses extend the duration of a script execution, and there are several restrictions during a script execution. For instance, starting or stopping services is delayed until the end of the script.

Services

Authentication, Authorization and Accounting (Aaa)

The Authentication, Authorization and Accounting (AAA) service allows the management of user accounts (provide access rights, create user types, configure lock protection, etc.) and configure Radius servers.

Parameters

Users (Table: user-defined, 10 lines max.)

This table contains the users that are allowed in the system.

UserName (Index) | Table: Users

Type	Text
Range	Size(0..50)
Script/CLI	Aaa.Users[].UserName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1000.1.100.1.100

Contains the user name. Cannot be empty.

Password (Config Parameter) | Table: Users

Type	Text
Range	
Default	
Script/CLI	Aaa.Users[].Password
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1000.1.100.1.200

Contains the securely hashed user password.
Also supports entering a new password in clear text, which will be converted into a secure one-way hash representation the password.

AccessRights (Config Parameter) | Table: Users

Type	Enum
Range	Admin(100) | User(200) | Observer(300)
Default	Admin
Script/CLI	Aaa.Users[].AccessRights
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1000.1.100.1.250

Identifies the user role defining the access rights.

- Admin: User has administrator access rights and is allowed to read, modify, and execute all configuration objects of the unit.
- User: User has end-user access rights and is only allowed to read/modify configuration parameters, execute configuration scripts, and export configurations.
- Observer: User has observer access rights and is only allowed to read the configuration parameters.

LockProtectionEnable (Config Parameter) | Table: Users

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Aaa.Users[].LockProtectionEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1000.1.100.1.275

To configure the locking mechanism to protect a user account against brute force attacks.

- Enable: The user account will be temporarily locked after repetitive login failures.
- Disable: The user account will never be locked, regardless of the amount of failed login attempts.

For more configuration, refer to the following parameters (not configurable from the DGW Web interface):

- **Aaa.LoginLockedMaxRetry**
- **Aaa.LoginLockedTimeoutS**

Delete (Row Command) | Table: Users

Script/CLI:	Aaa.Users[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1000.1.100.1.300

Deletes this row.
Note: The current activities of the user are not terminated upon removal. The system must be restarted to completely remove the user.

UsersStatus (Table)

This table displays the list of all currently allowed users.

UserName (Index) | Table: UsersStatus

Type	Text
Range	
Script/CLI	Aaa.UsersStatus[].UserName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1000.1.150.1.100

Contains the user name.

Password (Status Parameter) | Table: UsersStatus

Type	Text
Range	
Script/CLI	Aaa.UsersStatus[].Password
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1000.1.150.1.200

Contains the securely hashed user password.

Locked (Status Parameter) | Table: UsersStatus

Type	Enum
Range	Unlocked(100) | Locked(200)
Script/CLI	Aaa.UsersStatus[].Locked
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1000.1.150.1.300

Indicates when a user account has been temporarily locked due to excessive login failures. All login attempts will be rejected while the user account is locked. See the **Aaa.Users.LockProtectionEnable** parameter for more details.

BatchUser (Config Parameter)

Type	Text
Range	
Default	
Script/CLI	Aaa.BatchUser
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1000.1.200

User name that is used for scheduled tasks.

ServicesAaaType (Table)

Aaa type used by services.

Service (Index) | Table: ServicesAaaType

Type	Text
Range	
Script/CLI	Aaa.ServicesAaaType[].Service
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1000.1.300.1.100

Service name for which the Aaa types are configured.

AuthenticationType (Config Parameter) | Table: ServicesAaaType

Type	Enum
Range	Local(100) | Radius(200)
Default	Local
Script/CLI	Aaa.ServicesAaaType[].AuthenticationType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1000.1.300.1.200

Authentication type a service uses for incoming authentication requests.

- Local: Incoming authentication attempts are validated against the user names and passwords stored in the **Aaa.Users** table.
- Radius: Incoming authentication attempts are validated against the first responding Radius server configured in the **Aaa.RadiusServers** table. When no servers reply or when no server is configured in the **Aaa.RadiusServers** table, an authentication attempt of type Local is performed against the user names and passwords stored in the **Aaa.Users** table.

AccountingType (Config Parameter) | Table: ServicesAaaType

Type	Enum
Range	None(100) | Radius(200)
Default	None
Script/CLI	Aaa.ServicesAaaType[].AccountingType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1000.1.300.1.300

Accounting type a service uses once a user is successfully authenticated on the unit. Accounting starts once users are successfully authenticated and stops when their session is over.

- None: Accounting is disabled.
- Radius: Accounting is done by the first responding Radius server configured in the **Aaa.RadiusServers** table.

RadiusServersTimeoutS (Config Parameter)

Type	UInt32
Range	1..5
Default	5
Script/CLI	Aaa.RadiusServersTimeoutS
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1000.1.10000.100

Maximum time, in seconds, the unit waits for a reply from a Radius server. When the timeout is reached, the request is sent to the next configured server in the **Aaa.RadiusServers** table.

RadiusUserAccessRights (Config Parameter)

Type	Enum
Range	Admin(100) | User(200) | Observer(300)
Default	Admin
Script/CLI	Aaa.RadiusUserAccessRights
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1000.1.10000.200

Identifies the user role defining the access rights for all Radius users.

- Admin: User has administrator access rights and is allowed to read, modify, and execute all configuration objects of the unit.
- User: User has end-user access rights and is only allowed to read/modify configuration parameters, execute configuration scripts, and export configurations.
- Observer: User has observer access rights and is only allowed to read the configuration parameters.

RadiusServers (Table)

Radius servers used by services.

Service (Index) | Table: RadiusServers

Type	Text
Range	
Script/CLI	Aaa.RadiusServers[].Service
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1000.1.10000.1000.1.100

Name of the service for which Radius servers are configured.

Priority (Index) | Table: RadiusServers

Type	UInt32
Range	
Script/CLI	Aaa.RadiusServers[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1000.1.10000.1000.1.200

Radius server priority determining their usage order for Aaa requests.

AuthenticationHost (Config Parameter) | Table: RadiusServers

Type	IpHostNamePort
Range	
Default	
Script/CLI	Aaa.RadiusServers[].AuthenticationHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1000.1.10000.1000.1.300

Hostname and port of a Radius server used for authentication requests.

AuthenticationSecret (Config Parameter) | Table: RadiusServers

Type	Text
Range	Size(0..512)
Default	
Script/CLI	Aaa.RadiusServers[].AuthenticationSecret
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1000.1.10000.1000.1.400

Secret key shared between the Radius server and the unit. The **Aaa.RadiusServers.AuthenticationSecret** key must be the same as the secret key stored on its associated Radius authentication server host.

AccountingHost (Config Parameter) | Table: RadiusServers

Type	IpHostNamePort
Range	
Default	
Script/CLI	Aaa.RadiusServers[].AccountingHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1000.1.10000.1000.1.500

Hostname and port of a Radius server used for accounting requests.

AccountingSecret (Config Parameter) | Table: RadiusServers

Type	Text
Range	Size(0..512)
Default	
Script/CLI	Aaa.RadiusServers[].AccountingSecret
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1000.1.10000.1000.1.600

Secret key shared between the Radius server and the unit. The **Aaa.RadiusServer.AccountingSecret** key must be the same as the secret key stored on its associated Radius accounting server host.

LoginLockedMaxRetry (Config Parameter)

Type	UInt32
Range	1..5
Default	5
Script/CLI	Aaa.LoginLockedMaxRetry
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1000.1.20000.100

Defines the maximum number of failed login attempts allowed before temporarily locking the user account.
This parameter has no effect when the **Aaa.Users.LockProtectionEnable** parameter is disabled.

LoginLockedTimeoutS (Config Parameter)

Type	UInt32
Range	5..3600
Default	300
Script/CLI	Aaa.LoginLockedTimeoutS
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1000.1.20000.200

Defines the duration of the locked period (in seconds), after which the user is allowed to log in again.
This parameter has no effect when the **Aaa.Users.LockProtectionEnable** parameter is disabled.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Aaa.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1000.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.

- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Aaa.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1000.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

InsertUser (Command)

Inserts a new user in the **Aaa.Users** table.

UserName (Argument) | Command: InsertUser

Type	Text
Range	Size(1..50)
Default	

Contains the user name. Cannot be empty.

Password (Argument) | Command: InsertUser

Type	Text
Range	Size(0..255)
Default	

Contains the securely hashed user password.
Also supports entering a new password in clear text, which will be converted into a secure one-way hash representation the password.

Important: Double quotes must be used around the value.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Aaa service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.1000.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	Authentication failed for user %1$s.	Info	The specified user attempted to authenticate unsuccessfully.
20	Successfully changed password for user %1$s.	Info	This message is issued when the password for a user is modified.
30	Successfully authenticated user %1$s.	Info	This message is issued when a user has been authenticated successfully.
40	Radius server at %1$s is unreachable.	Error	An authentication or accounting request could not be completed because the server is unreachable.
50	The Radius server at %1$s replied to a request with an invalid response.	Warning	The Radius server replied to a request by using a response with invalid information.
60	No Radius servers are configured or none of them are reachable, attempting to authenticate user %1$s locally.	Warning	No Radius servers are configured or none of them are reachable. The user is then authenticated against the local usernames and passwords.
70	Accounting session startup has failed.	Error	No Radius servers are configured or none of them are reachable and an accounting session could not be started.
80	Accounting session termination has failed.	Error	No Radius servers are configured or none of them are reachable and an accounting session could not be terminated.
90	User %1$s has been added to the system.	Info	Creation of this user has been completed with success.
100	User %1$s has been removed from the system.	Info	Deletion of this user has been initiated with success. The system must be restarted to completely remove the user.
110	The default users have been restored.	Warning	The Users table is restored to its default value when a partial reset or a factory reset is invoked. This can also occur after a firmware update from a old firmware version.
120	User %1$s has been temporarily locked due to excessive login failures.	Warning	This message is issued after repetitive login failures and causes the user account to be temporarily locked. See the **Aaa.Users** table for more details.

NumKey	Message	Severity	Description
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.

NumKey	Message	Severity	Description
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Aaa.

Message	Severity	Description
Users table is empty. Remember to create new users.	Warning	At least one user should exist in the **Aaa.Users** table. If the unit is restarted with an empty **Aaa.Users** table, the default users and passwords will be restored.
User %1$s already exists.	Error	Creation of this user is unauthorised because it already exists.
Password for user %1$s must contain at least %2$d character(s).	Error	Password configuration of this user is not authorised because the password does not have the minimal length.
Password for user %1$s must contain at least one lower case character and one upper case character.	Error	Password configuration of this user is not authorised because the password does not contain a lower and an upper case character.
Password for user %1$s must contain at least one numeral character.	Error	Password configuration of this user is not authorised because the password does not contain a numeral character.
Password for user %1$s must contain at least one special (non-alphanumeric) character.	Error	Password configuration of this user is not authorised because the password does not contain a special (non-alphanumeric) character.
Hashed password for user %1$s is corrupted.	Error	Password entered was detected as being hashed but its format is incorrect.
Password for user %1$s cannot be the default password.	Error	Password configuration for this user is not authorised because it is the same as the profile default one.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.

Message	Severity	Description
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Basic Network Interfaces (Bni)

The Basic Network Interfaces (Bni) service manages the layer 3 network interfaces. The parameters of the Bni service are used to configure the network interfaces and PPPoE connections used by the application. The Bni service also handles the "Rescue" network interface, which is used for the partial reset feature.

Parameters

DhcpClientIdentifierPresentation (Config Parameter)

Type	Enum
Range	Disabled(100) | MacAscii(200) | MacBinary(300)
Default	MacAscii
Script/CLI	Bni.DhcpClientIdentifierPresentation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.200.100

The method used to present the value of the Client Identifier (Option 61) field through a DHCPv4 request.

- Disabled: The Client Identifier option is not presented in a DHCPv4 request.
- MacAscii: The Client Identifier value is presented as the client MAC address in ASCII format. The MAC address is in lower case.
- MacBinary: The Client Identifier value is presented as the client MAC address in a binary format.

DhcpClientDuplicateIpAddressDetectionEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Bni.DhcpClientDuplicateIpAddressDetectionEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.200.200

Defines if the received DHCPv4 IP address is checked to make sure it is not already used on the network before using it.

- Enable: Verifies that the received DHCPv4 IP address is not already used on the network. If it is already used on the network, a DHCPv4 DECLINE is sent to the DHCPv4 server and the DHCPv4 process is restarted after 10 to 20 seconds.
- Disable: The received DHCPv4 IP address is used without verifying if it is already used on the network.

DhcpClientClasslessStaticRouteOption (Config Parameter)

Type	Enum
Range	None(100) | Request(200)
Default	None
Script/CLI	Bni.DhcpClientClasslessStaticRouteOption
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.200.300

Defines if the Classless Static Route Option is enabled.

- Request: The device requests the Classless Static Route Option 121.
- None: Routes received from the DHCP server are ignored.

DhcpClientUserClass (Config Parameter)

Type	Text
Range	Size(0..254)
Default	
Script/CLI	Bni.DhcpClientUserClass
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.200.400

Defines if the User Class Route Option is enabled.
List of User Class values to be sent over Option 77. When defining the list of options in the DHCP server,

- user class value items are separated by a comma;
- items must not be empty;
- hexadecimal values are supported using the '\xXX' format where XX is the hexadecimal value;
- when the parameter is empty, the user class option is not sent.

PppServiceName (Config Parameter)

Type	Text
Range	Size(0..64)
Default	
Script/CLI	Bni.PppServiceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.400.100

Name of the service requested by the PPPOE Access Concentrator (AC) when establishing the next PPPoE connection.
This string is used as the Service-Name field of the PADI packet broadcasted to the Access Concentrators.

PppRetryInterval (Config Parameter)

Type	UInt32
Range	1..900
Default	10
Script/CLI	Bni.PppRetryInterval
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.400.200

Interval, in seconds, before a connection is automatically retried when it fails due to a transient error. The only error type considered non-transient is a configuration error.

PppAuthenticationProtocol (Config Parameter)

Type	Enum
Range	Pap(100) | Chap(200)
Default	Chap
Script/CLI	Bni.PppAuthenticationProtocol
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.400.300

Authentication protocol used for authenticating the system to the PPP peer over the PPPoE connection.

- Pap: Use the Password Authentication Protocol.

- Chap: Use the Challenge Handshake Authentication Protocol.

PppIdentity (Config Parameter)

Type	Text
Range	Size(0..64)
Default	
Script/CLI	Bni.PppIdentity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.400.400

Name that identifies the system to the PPP peer during the authentication process.

PppSecret (Config Parameter)

Type	Text
Range	Size(0..64)
Default	
Script/CLI	Bni.PppSecret
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.400.500

Secret password that identifies the system to the PPP peer during the authentication process. The password is always displayed as "*****", regardless of its value.

IcmpRedirect (Config Parameter)

Type	Enum
Range	AcceptIpv4AndIpv6(100) | AcceptIpv4Only(200)
Default	AcceptIpv4AndIpv6
Script/CLI	Bni.IcmpRedirect
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.500.100

Internet Control Message Protocol (ICMP) redirect is used to inform a remote host that a better route is available for a specific destination and to send the packets by this alternate route. This parameter defines if ICMP redirect will be allowed for packets arriving by IPv4 or IPv6.

- AcceptIpv4AndIpv6: The redirection is applied to packets received by IPv4 or IPv6.

- AcceptIpv4Only: The redirection is applied to packets received by IPv4 only.

IpTtlValue (Config Parameter)

Type	UInt32
Range	64..255
Default	64
Script/CLI	Bni.IpTtlValue
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.600.100

Specifies the IP traffic default Time-To-Live (TTL) value on all network interfaces. The TTL is the maximum number of network hops allowed before the IP packet is dropped by the network.
Only supported on packets using IPv4.

NetworkInterfaces (Table: user-defined, 48 lines max.)

Allows the configuration of the network interfaces.

Idx (Index) | Table: NetworkInterfaces

Type	UInt32
Range	
Script/CLI	Bni.NetworkInterfaces[].Idx
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.1000.1.50

Unique identifier of the row in the table.

InterfaceName (Config Parameter) | Table: NetworkInterfaces

Type	Text
Range	Size(0..50)
Default	
Script/CLI	Bni.NetworkInterfaces[].InterfaceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.1000.1.100

Network interface name. Whenever a network interface is used in the DGW application, it is here that it is first created. This parameter is case sensitive. The following special values are NOT allowed:

- All
- Loop
- LoopV6
- Rescue

To be valid, the Interface name

- must start with a letter;
- cannot contain characters other than letters, numbers, and underscores.

LinkName (Config Parameter) | Table: NetworkInterfaces

Type	Text
Range	Size(0..50)
Default	
Script/CLI	Bni.NetworkInterfaces[].LinkName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.1000.1.200

Name of the link interface associated with the network interface.

ConnectionType (Config Parameter) | Table: NetworkInterfaces

Type	Enum
Range	IpDhcp(100) | IpStatic(200) | Ip6AutoConf(225) | Ip6Static(250) | PppIpcp(300) | IpSystem(400)
Default	IpStatic
Script/CLI	Bni.NetworkInterfaces[].ConnectionType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.1000.1.250

Connection type of the network interface.

- IpDhcp: An IPv4 DHCP connection. The address and the network mask are provided by a DHCP server .
- IpStatic: An IPv4 static connection. The address and the network mask are configured with the value in the **Bni.NetworkInterfaces.StaticIpAddr**) column.
- Ip6AutoConf: An IPv6 state-less auto-configuration.

- Ip6Static: An IPv6 static connection. The address and the network mask are configured with the value in the **Bni.NetworkInterfaces.StaticIpAddr**) column.
- PppIpcp: An IPv4 over PPPoE connection. The address and the network mask are provided by the PPP peer using IPCP.
- IpSystem: The IPv4 address and the network mask are retrieved from the Operating System. Applicable only if DGW is running in a non-Mediatrix environment, for example in a virtual host or cloud environment.

DHCP servers and PPP peers may provide a list of DNS to use. If that is the case, the DNS are forwarded to the Host Configuration service where they can be used.

StaticIpAddr (Config Parameter) | Table: NetworkInterfaces

Type	IpAddrMask
Range	
Default	192.168.0.10/24
Script/CLI	Bni.NetworkInterfaces[].StaticIpAddr
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.1000.1.300

IP address and network mask of the network interface when the **Bni.NetworkInterfaces.ConnectionType** parameter is set to **IpStatic** (IPv4 Static).

StaticDefaultRouter (Config Parameter) | Table: NetworkInterfaces

Type	IpAddress
Range	
Default	
Script/CLI	Bni.NetworkInterfaces[].StaticDefaultRouter
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.1000.1.350

IP address of the default router for the network interface when the **Bni.NetworkInterfaces.ConnectionType** parameter is set to **IpStatic** (IPv4 Static) or **Ip6Static** (IPv6 Static).

Activation (Config Parameter) | Table: NetworkInterfaces

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Bni.NetworkInterfaces[].Activation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.1000.1.400

Indicates if the network interface is activated or not on the system.

- Enable: The network interface is activated on the system and can be used for configuration.
- Disable: The network interface is not activated on the system.

The actual status of a network interface is displayed in the **Bni.NetworkInterfacesStatus**.

Priority (Config Parameter) | Table: NetworkInterfaces

Type	UInt32
Range	0..100
Default	50
Script/CLI	Bni.NetworkInterfaces[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.1000.1.450

Prioritise the network interface. In case of address conflicts between two or more network interfaces, the network interface with the highest priority will remain enabled and all other interfaces will be set to invalid configuration. If the priority is the same, only the first enabled network interface will be able to use the IP address. When a conflict ends, all conflictual network interfaces are automatically returned to an operational state.
The actual status of network interfaces is shown in the **Bni.NetworkInterfacesStatus**.

ConfigStatus (Status Parameter) | Table: NetworkInterfaces

Type	Enum
Range	ValidConfig(100) | EmptyInterfaceName(200)| DuplicateInterfaceName(300) | InvalidLinkName(400) | InvalidStaticIpAddr(500) | MultipleDynamicOnSameLink(600)
Script/CLI	Bni.NetworkInterfaces[].ConfigStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.1000.1.480

Configuration status of the row.
It indicates whether the configuration of the row is valid or not.

- ValidConfig: This entry is valid.
- EmptyInterfaceName: This entry is not valid because the **Bni.NetworkInterfaces.InterfaceName** parameter is empty.
- DuplicateInterfaceName: This entry is not valid because the value of the **Bni.NetworkInterfaces.InterfaceName** parameter is already used.
- InvalidLinkName: This entry is not valid because the **Bni.NetworkInterfaces.LinkName** parameter is either empty or refers to an nonexistent link.
- InvalidStaticIpAddr: This entry is not valid because the value of the **Bni.NetworkInterfaces.StaticIpAddr** parameter is either invalid or is in conflict with another network IP address.
- MultipleDynamicOnSameLink: This entry is not valid because there is a dynamic connection configured several times on the same link. May result in an unexpected behavior.

Delete (Row Command) | Table: NetworkInterfaces

Script/CLI:	Bni.NetworkInterfaces[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.1000.1.500

Deletes the network interface and removes it permanently from the system.

NetworkInterfacesStatus (Table)

This table displays the status of all currently enabled network interfaces, including interfaces with an invalid configuration or waiting for a response.

Idx (Index) | Table: NetworkInterfacesStatus

Type	UInt32
Range	
Script/CLI	Bni.NetworkInterfacesStatus[].Idx
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.2000.1.50

Unique identifier of the row in the table.

InterfaceName (Status Parameter) | Table: NetworkInterfacesStatus

Type	Text
Range	
Script/CLI	Bni.NetworkInterfacesStatus[].InterfaceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.2000.1.100

Network interface name. This parameter is case sensitive. Note that using the following special values is not allowed:

- All
- Loop
- LoopV6
- Rescue

To be valid, the Interface name

- must start with a letter;
- cannot contain characters other than letters, numbers, and underscores.

InterfaceStatus (Status Parameter) | Table: NetworkInterfacesStatus

Type	Enum
Range	InvalidConfig(200) | NetworkConflict(225) | LinkDown(250) | WaitingResponse(300) | Active(400)
Script/CLI	Bni.NetworkInterfacesStatus[].InterfaceStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.2000.1.150

Displays the operational status of the network interface.

- Invalid Config: The interface is not operational because its configuration is not valid.
- Network Conflict: The interface is configured with an IP address that is already used on the network.
- Link Down: The interface is configured with a link that has no connectivity.
- Waiting Response: The interface is not operational because a response from a peer or server is required.
- Active: The interface is operational.

LinkName (Status Parameter) | Table: NetworkInterfacesStatus

Type	Text
Range	
Script/CLI	Bni.NetworkInterfacesStatus[].LinkName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.2000.1.200

Name of the link interface associated with the network interface.

IpAddr (Status Parameter) | Table: NetworkInterfacesStatus

Type	IpAddrMask
Range	
Script/CLI	Bni.NetworkInterfacesStatus[].IpAddr
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.2000.1.300

Current IP address and network mask of the network interface.

DefaultRouter (Status Parameter) | Table: NetworkInterfacesStatus

Type	Text
Range	
Script/CLI	Bni.NetworkInterfacesStatus[].DefaultRouter
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.2000.1.400

Current default router of the network interface.

ConnectionUptime (Status Parameter) | Table: NetworkInterfacesStatus

Type	UInt32
Range	
Script/CLI	Bni.NetworkInterfacesStatus[].ConnectionUptime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.2000.1.500

The time, in seconds, during which this IP interface has been connected.

- If the IP interface is using DHCP, this is the time during which the DHCP client has been only in the Bound or Renewing states and the lower-layer interface has continuously maintained a link.
- If the IP interface is using static addressing, this is the time during which the lower-layer interface has continuously maintained a link.

VlanOverrideEnable (Status Parameter) | Table: NetworkInterfacesStatus

Type	EnableDisable
Range	
Script/CLI	Bni.NetworkInterfacesStatus[].VlanOverrideEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.2000.1.600

Indicates if the VLAN ID of the current network interface is overridden by the values received from the LLDP protocol.

- Enable: The VLAN network interface configuration is overridden by LLDP.
- Disable: The VLAN network interface configuration is not overridden by LLDP.

InterfaceStatistics (Table)

This table contains the statistics of each network interface.

LinkName (Index) | Table: InterfaceStatistics

Type	Text
Range	
Script/CLI	Bni.InterfaceStatistics[].LinkName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.10000.100.1.100

Name of the link interface associated with the network interface.

TxBytes (Status Parameter) | Table: InterfaceStatistics

Type	UInt64
Range	
Script/CLI	Bni.InterfaceStatistics[].TxBytes
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.10000.100.1.200

Total number of bytes transmitted on the network interface at the link level.

RxBytes (Status Parameter) | Table: InterfaceStatistics

Type	UInt64
Range	
Script/CLI	Bni.InterfaceStatistics[].RxBytes
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.10000.100.1.300

Total number of bytes received on the network interface at the link level.

TxPackets (Status Parameter) | Table: InterfaceStatistics

Type	UInt64
Range	
Script/CLI	Bni.InterfaceStatistics[].TxPackets
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.10000.100.1.400

Total number of IP packets transmitted on this network interface.

RxPackets (Status Parameter) | Table: InterfaceStatistics

Type	UInt64
Range	
Script/CLI	Bni.InterfaceStatistics[].RxPackets
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.10000.100.1.500

Total number of IP packets received on this network interface.

RxErrors (Status Parameter) | Table: InterfaceStatistics

Type	UInt64
Range	
Script/CLI	Bni.InterfaceStatistics[].RxErrors
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.10000.100.1.600

Total number of IP packets discarded on this network interface.

CollectTime (Status Parameter) | Table: InterfaceStatistics

Type	UInt32
Range	
Script/CLI	Bni.InterfaceStatistics[].CollectTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.10000.100.1.10000

Time, in seconds, since the network statistics were last reset.

ResetStat (Row Command) | Table: InterfaceStatistics

Script/CLI:	Bni.InterfaceStatistics[].ResetStat
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.10000.100.1.11000

Reset all statistics parameters for this network interface.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Bni.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Bni.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.200.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

AddNetwork (Command)

Adds a new network interface.

Idx (Argument) | Command: AddNetwork

Type	UInt32
Range	0..2147483647
Default	0

Index of the network interface.

Name (Argument) | Command: AddNetwork

Type	Text
Range	Size(0..50)
Default	

Name of the network interface to create. This parameter is case sensitive. Note that using the following special values is not allowed:

- All
- Loop
- LoopV6
- Rescue

To be valid, the Interface name:

- Must start with a letter
- Cannot contain characters other than letters, numbers, and underscores

DisableAllNetworks (Command)

Disables all network interfaces. Network interfaces will no longer be available to the system.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Bni service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.200.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	Static configuration changed for Network Interface %1$s.	Debug	The static configuration of a network interface was modified.
20	PPP configuration changed for Network Interface %1$s.	Debug	The PPP configuration of a network interface was modified.
30	Network Interface %1$s connected to the PPP peer bearing IP address %2$s.	Info	A network interface connected to a PPP peer.
40	Network Interface %1$s was disconnected by PPP peer.	Warning	The peer closed a PPPoE connection.
50	Network Interface %1$s was disconnected because the PPP peer is not responding.	Warning	A PPP peer did not reply to echo requests.
60	PPP negotiation failed for Network Interface %1$s.	Warning	The PPPoE connection negotiation could not be completed up to the IPCP level.
70	PPP authentication failed for Network Interface %1$s.	Error	The PPPoE connection negotiation failed due to an authentication error.
80	PPP connection for Network Interface %1$s was disconnected locally	Debug	The PPPoE connection of a Network Interface was disabled.
90	Invalid data received from PPP peer on the Network Interface %1$s.	Warning	The unit received a PPP message containing invalid information.
100	DHCP lease acquired for address %1$s on the Network Interface %2$s.	Info	A DHCP server responded with an ACK to a lease request.
110	DHCP lease refused for the Network Interface %1$s.	Error	A DHCP server responded with a NAK to a lease request.
120	DHCP lease expired for address %1$s on the Network Interface %2$s.	Error	The unit could not renew a DHCP lease before its expiration.

NumKey	Message	Severity	Description
130	DHCP lease renewed for address %1$s on the Network Interface %2$s.	Debug	The unit renewed a DHCP lease before its expiration.
140	Invalid data received from DHCP server on the Network Interface %1$s.	Warning	The unit received a DHCP message containing invalid information.
150	Domain Name Server address %1$s received for automatic configuration on interface %2$s.	Debug	This message is issued for each DNS address received via the DHCP or PPPoE protocol on the specified network interface.
160	Network Time Server address %1$s received for automatic configuration on interface %2$s.	Debug	An NTP server address was received via the DHCP protocol on the specified network interface.
170	Router address %1$s received for automatic configuration on interface %2$s.	Debug	A router address was received via the DHCP or PPPoE protocol on the specified network interface.
175	Domain name %1$s received for automatic configuration on interface %2$s.	Debug	A domain name was received via the DHCP protocol on the specified network interface.
180	Invalid Domain Name Server address received on interface %1$s.	Warning	An invalid DNS address was received via the DHCP or PPPoE protocol. Invalid DNS addresses are discarded for automatic configuration.
190	Invalid router address received on interface %1$s.	Warning	An invalid router address was received via the DHCP or PPPoE protocol. Invalid router addresses are discarded for automatic configuration.
230	Partial reset: the %1$s network interface has been set to invalid because it conflicted with the Rescue network interface.	Warning	The user performs a partial reset and a network interface is set to invalid because it is in conflict with the Rescue network interface.

NumKey	Message	Severity	Description
240	Partial reset: the Rescue network interface has been enabled and set to the IPv4 address %1$s and to the IPv6 address %2$s.	Warning	The user performs a partial reset and the Rescue network interface becomes the management network interface.
270	Error: cannot enable network interface %1$s because link %2$s does not exist.	Error	The system tries to enable a network interface but the configured link does not exist.
280	Error: cannot enable network interface %1$s because IP address %2$s is already used on network interface %3$s.	Error	The system tries to enable a network interface with an IP address that is already currently used by another network interface.
285	Error: cannot enable network interface %1$s because IP address %2$s is already used on the network.	Error	The system tries to enable a network interface with an IP address that is already currently used on the network.
290	Network interface named %1$s had an invalid name. It has been automatically updated to %2$s.	Warning	A network interface with an invalid name was encountered when a service was started. An invalid name starts with a character that is not a letter or contains a character other than a letter, number or underscore, or the words All, Loop, LoopV6, or Rescue were used as the name of the network interface.
300	Network interface named %1$s had an invalid name. It has been automatically updated to %2$s. An error occurred while generating a valid interface name, please verify SIP gateways and system management configuration settings.	Error	An error occurred during the generation of a valid interface name. Generating a valid interface name occurs when a service starts and one or more network interfaces has an invalid name. An invalid name starts with a character that is not a letter or contains a character other than a letter,a number or an underscore. All, Loop, LoopV6, and Rescue cannot be used as network interface names.
330	Dhcp autoprovisionning option %1$s received on interface %2$s.	Debug	A tftp-server (option 66) or bootline (option 67) option was received via DHCP.

NumKey	Message	Severity	Description
340	DHCP vendor-specific options (%1$d) received on interface %2$s.	Debug	Some vendor-specific options (DHCPv4 options 43 or 125) were received via DHCP.
350	Invalid DHCP vendor-specific options received on interface %1$s.	Warning	Some vendor-specific options (DHCPv4 options 43 or 125) were received on the %1$s interface, but are invalid or unsupported.
360	DHCPv4 Classless Static Route to destination %1$s/%2$d via gateway %3$s received on interface %4$s.	Info	The Classless Static Route Option for DHCPv4 (option 121) was received.
370	Invalid DHCPv4 Classless Static Route to destination %1$s/%2$d via gateway %3$s received on interface %4$s.	Warning	The Classless Static Route Option for DHCPv4 (option 121) was received but is not valid.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.

NumKey	Message	Severity	Description
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.

NumKey	Message	Severity	Description
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Bni.

Message	Severity	Description
Invalid configuration on network interface %1$s: only %2$d network interfaces(s) can have a PPP connection type.	Error	The maximum number of connections was reached while trying to set a connection type to PPPoE .
Deleting the Rescue network interface is not allowed.	Error	The user is trying to delete the Rescue network interface.
Renaming the Rescue network interface is not allowed.	Error	The user is trying to rename the Rescue network interface.
Creating a network interface with the name %1$s is forbidden because this is a reserved name.	Error	The user is trying to create a network interface with a reserved name, i.e. All, Loop, LoopV6, or Rescue.
Warning: network interface %1$s has been assigned link %2$s, which does not exist.	Warning	The user assigns to a network interface a link that does not exist.
Warning: network interface %1$s has been configured with static IP address %2$s, which conflicts with network interface %3$s's current IP address.	Warning	The user assigns a static IP address that is already currently used by another network interface.
%1$s is an invalid network interface name. A valid name starts with a letter and does not contain characters other than letters, numbers or underscores.	Error	The user tried to add a network interface with an invalid name. A valid name starts with a letter and does not contain characters other than letters, numbers, or underscores. All, Loop, LoopV6, and Rescue cannot be used as network interface names.
Warning: Dynamic connection configured on the same link multiple times. May result in unexpected behavior.	Warning	The user changed the configuration and more than one dynamic connection was configured on the same link.
Warning: Multiple IPv6 auto-conf network interfaces on the same link. Only one will be active.	Warning	The user changed the configuration and more than one Ip6AutoConf connection was configured on the same link.
Contains empty item.	Error	The value of the **Bni.DhcpClientUserClass** parameter was left empty by the user. This parameter does not accept empty items.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.

Message	Severity	Description
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.

Message	Severity	Description
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Call Detail Record (Cdr)

The Call Detail Record (CDR) is a DGW user service allowing the administrator to generate custom call notifications with information such as endpoints, point of origin, duration, etc.

Parameters

SyslogRemoteHost (Config Parameter)

Type	IpHostNamePort
Range	
Default	
Script/CLI	Cdr.SyslogRemoteHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4200.1.400.100

Host name and port number of the device that archives CDR log entries. Specifying no port (or port 0) sends notifications to port 514.

SyslogFormat (Config Parameter)

Type	Text
Range	Size(0..1024)
Default	
Script/CLI	Cdr.SyslogFormat
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4200.1.400.200

Specifies the format of the syslog Call Detail Record.
Formal Syntax Description of the Protocol is as follows:

- Precision=DIGIT

- Width=DIGIT
- MacroId=(ALPHA / "_")
- Macro=%[Width]|[.Precision]|[Width.Precision]MacroId

The Width field is the minimum width of the converted argument.

- If the converted argument has fewer characters than the specified field width, then it is padded with spaces.
- If the converted argument has more characters than the specified field width, the field width is extended to whatever is required.

The Precision field specifies the maximum number of characters to be printed from a string.

A config error message is issued when applying a Syslog Format containing an unknown macro.

Any invalid macros will remain unchanged in the syslog.

Examples: sipid=SipUser001

- CDR Log : %sipid --> CDR Log : SipUser001
- CDR Log : %15sipid --> CDR Log : SipUser001
- CDR Log : %15.5sipid --> CDR Log : SipUs
- CDR Log : %.5sipid --> CDR Log : SipUs

Call Detail Record control characters:

- %% : %
- \n : Split message

Call detail record macros:

- %id : CDR ID. The CDR ID is unique. The ID is incremented by one each time it is represented in a CDR record.
- %sipid : SIP call ID. Blank if no SIP interface was used during the call.
- %ocgnum : Original calling number. Calling number as received by the unit.
- %cgnum : Calling number. Calling number after manipulation by the call router.
- %ocdnum : Original called number. Called number as received by the unit.
- %cdnum : Called number. Called number after manipulation by the call router.
- %oiname : Origin interface name. Interface on which the call was received. Ex. isdn-Slot2/Pri1.
- %diname : Destination interface name. Interface on which the call was relayed. Ex. SIP-Default.
- %chan : Channel number. Blank if no PRI/BRI interface was used during the call. If 2 PRI/BRI interfaces were involved, display the originating interface.
- %sipla : SIP local IP address.
- %sipra : SIP remote IP address or FQDN (next hop).
- %siprp : SIP remote port (next hop).

- %mra : Media remote IP address. Source IP address of the incoming media stream. If the stream was modified during the call, display the last stream.
- %mrsp : Media remote source port. Source port of the incoming media stream. If the stream was modified during the call, display the last stream.
- %mrp : Media remote port. Destination port of the outgoing media stream. If the stream was modified during the call, display the last stream.
- %tz : Local time zone
- %cd : Call duration (in seconds) (connect/disconnect).
- %sd : Call duration (in seconds) (setup/connect).
- %pdd : Post dial delay (in seconds) (setup/progress).
- %css : Call setup second (local time)
- %csm : Call setup minute (local time)
- %csh : Call setup hour (local time)
- %csd : Call setup day (local time)
- %csmm : Call setup month (local time)
- %csy : Call setup year (local time)
- %ccs : Call connect second (local time)
- %ccm : Call connect minute (local time)
- %cch : Call connect hour (local time)
- %ccd : Call connect day (local time)
- %ccmm : Call connect month (local time)
- %ccy : Call connect year (local time)
- %cds : Call disconnect second (local time)
- %cdm : Call disconnect minute (local time)
- %cdh : Call disconnect hour (local time)
- %cdd : Call disconnect day (local time)
- %cdmm : Call disconnect month (local time)
- %cdy : Call disconnect year (local time)
- %miptxc : IP Media last transmitted codec
- %miptxp : IP Media last transmitted p-time
- %dr : Call disconnect reason, expressed as a Q.850 cause. The Q.850 codes are used to represent the disconnect cause no matter what type of interface initiated the disconnect (SIP, FXS, ISDN, ...). A value of 0 means that no cause code is available.
- %rxp : Received media packets. Excluding T.38.
- %txp : Transmitted media packets. Excluding T.38.
- %rxpl : Received media packets lost. Excluding T.38.
- %rxmd : Received packets mean playout delay (ms, 2 decimals). Excluding T.38.

- %rxaj : Received packets average jitter (ms, 2 decimals). Excluding T.38.
- %sipdr : SIP status code of the received SIP response that caused the disconnect or rejection. A value of 0 means that no status code is available.

SyslogFacility (Config Parameter)

Type	Enum
Range	Local0(100) | Local1(200) | Local2(300) | Local3(400) | Local4(500) | Local5(600) | Local6(700) | Local7(800)
Default	Local0
Script/CLI	Cdr.SyslogFacility
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4200.1.400.300

Syslog facility used by the unit to route the Call Detail Record messages. The application can use local0 through local7.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Cdr.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4200.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Cdr.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4200.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Cdr service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.4200.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	The CDR message string size (%1$d) exceeds the maximum size of the transport protocol.	Warning	This message is issued when the CDR message string exceeds the maximum allowed by the transport protocol. The CDR message string is truncated.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.

NumKey	Message	Severity	Description
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Cdr.

Message	Severity	Description
The CDR %%%1$s macro is unknown.	Error	This message is issued when an unknown CDR macro is found.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.

Message	Severity	Description
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Certificate Manager (Cert)

The Certificate Manager (Cert) system service manages the security certificates used for the authentication of the unit and its peers before establishing a secure connection.

Parameters

HostCertificatesInfo (Table: user-defined, 10 lines max.)

This table contains information about each certificate used to certify the host system. (maximum of 10 Host certificates)

FileName (Index) | Table: HostCertificatesInfo

Type	Text
Range	
Script/CLI	Cert.HostCertificatesInfo[].FileName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.100.1.100

Certificate file name.

IssuedTo (Status Parameter) | Table: HostCertificatesInfo

Type	Text
Range	
Script/CLI	Cert.HostCertificatesInfo[].IssuedTo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.100.1.200

Certificate subject name. This is the common name that must match the host being authenticated.

IssuedBy (Status Parameter) | Table: HostCertificatesInfo

Type	Text
Range	
Script/CLI	Cert.HostCertificatesInfo[].IssuedBy
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.100.1.300

Certificate issuer name. This is the certificate authority that signed this certificate.

ValidFrom (Status Parameter) | Table: HostCertificatesInfo

Type	Text
Range	
Script/CLI	Cert.HostCertificatesInfo[].ValidFrom
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.100.1.400

Date from which the certificate is valid.

ValidTo (Status Parameter) | Table: HostCertificatesInfo

Type	Text
Range	
Script/CLI	Cert.HostCertificatesInfo[].ValidTo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.100.1.500

Date until which the certificate is valid.

Usage (Status Parameter) | Table: HostCertificatesInfo

Type	Text
Range	
Script/CLI	Cert.HostCertificatesInfo[].Usage
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.100.1.550

Identifies if the certificate can be used to authenticate a host acting as a TLS client or TLS server. Possible values are:

- TlsClient: The certificate identifies a TLS client. A host authenticated by this kind of certificate can act as a client in a SIP over TLS connection when mutual authentication is required by the server.
- TlsServer: The certificate identifies a TLS server. A host authenticated by this kind of certificate can serve files or Web pages using the HTTPS protocol or can act as a server in a SIP over TLS connection.

Delete (Row Command) | Table: HostCertificatesInfo

Script/CLI:	Cert.HostCertificatesInfo[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.100.1.600

Removes the certificate from the unit.

OthersCertificatesInfo (Table: user-defined, 20 lines max.)

This table contains information about the trusted root and intermediate certificate authorities to validate remote systems. (maximum of 20 certificates)
The Cert service does not support certificate files that concatenate all the certificates of the chain. In that case, only the first certificate of the file is taken into account.

FileName (Index) | Table: OthersCertificatesInfo

Type	Text
Range	
Script/CLI	Cert.OthersCertificatesInfo[].FileName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.200.1.100

Certificate file name.

IssuedTo (Status Parameter) | Table: OthersCertificatesInfo

Type	Text
Range	
Script/CLI	Cert.OthersCertificatesInfo[].IssuedTo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.200.1.200

Certificate subject name. This is the common name that must match the host being authenticated.

IssuedBy (Status Parameter) | Table: OthersCertificatesInfo

Type	Text
Range	
Script/CLI	Cert.OthersCertificatesInfo[].IssuedBy
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.200.1.300

Certificate issuer name. This is the certificate authority that signed this certificate.

ValidFrom (Status Parameter) | Table: OthersCertificatesInfo

Type	Text
Range	
Script/CLI	Cert.OthersCertificatesInfo[].ValidFrom
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.200.1.400

Date from which the certificate is valide.

ValidTo (Status Parameter) | Table: OthersCertificatesInfo

Type	Text
Range	
Script/CLI	Cert.OthersCertificatesInfo[].ValidTo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.200.1.500

Date until which the certificate is valid.

Usage (Status Parameter) | Table: OthersCertificatesInfo

Type	Text
Range	
Script/CLI	Cert.OthersCertificatesInfo[].Usage
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.200.1.550

Identifies if the certificate can be used to authenticate a host acting as a TLS client or TLS server. Possible values are:

- TlsClient: The certificate identifies a TLS client. A host authenticated by this kind of certificate can act as a client in a SIP over TLS connection when mutual authentication is required by the server.
- TlsServer: The certificate identifies a TLS server. A host authenticated by this kind of certificate can serve files or web pages using the HTTPS protocol or can act as a server in a SIP over TLS connection.

CertificateAuthority (Status Parameter) | Table: OthersCertificatesInfo

Type	Enum
Range	Yes(100) | No(200)
Script/CLI	Cert.OthersCertificatesInfo[].CertificateAuthority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.200.1.600

Indicates if the certificate is a CA certificate. Possible values are:

- Yes: The certificate is a CA certificate.
- No: The certificate is not a CA certificate.

Delete (Row Command) | Table: OthersCertificatesInfo

Script/CLI:	Cert.OthersCertificatesInfo[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.200.1.700

Removes the certificate from the unit.

HostCertificateAssociation (Table)

This table indicates which DGW service can use the host certificate to establish secure TLS connections.

FileName (Index) | Table: HostCertificateAssociation

Type	Text
Range	
Script/CLI	Cert.HostCertificateAssociation[].FileName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.300.1.100

Certificate file name.

Sip (Config Parameter) | Table: HostCertificateAssociation

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Cert.HostCertificateAssociation[].Sip
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.300.1.200

Specifies if the certificate can be used to secure SIP connections.

Web (Config Parameter) | Table: HostCertificateAssociation

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Cert.HostCertificateAssociation[].Web
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.300.1.300

Specifies if the certificate can be used to secure Web connections.

Eap (Config Parameter) | Table: HostCertificateAssociation

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Cert.HostCertificateAssociation[].Eap
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.300.1.400

Specifies if the certificate can be used to secure Wired Ethernet Authentication with EAP (802.1x) connections.

Conf (Config Parameter) | Table: HostCertificateAssociation

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Cert.HostCertificateAssociation[].Conf
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.300.1.500

Specifies if the certificate can be used to secure HTTPS connections for configuration scripts transfers.

Fpu (Config Parameter) | Table: HostCertificateAssociation

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Cert.HostCertificateAssociation[].Fpu
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.300.1.600

Specifies if the certificate can be used to secure connections used for firmware transfers.

File (Config Parameter) | Table: HostCertificateAssociation

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Cert.HostCertificateAssociation[].File
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.300.1.700

Specifies if the certificate can be used to secure file transfers.

Cert (Config Parameter) | Table: HostCertificateAssociation

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Cert.HostCertificateAssociation[].Cert
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.300.1.800

Specifies if the certificate can be used to secure connections used for certificate transfers.

Sbc (Config Parameter) | Table: HostCertificateAssociation

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Cert.HostCertificateAssociation[].Sbc
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.300.1.900

Specifies if the certificate can be used to secure SBC connections.

Cwmp (Config Parameter) | Table: HostCertificateAssociation

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Cert.HostCertificateAssociation[].Cwmp
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.300.1.1000

Specifies if the certificate can be used to secure CWMP connections.

Nlm (Config Parameter) | Table: HostCertificateAssociation

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Cert.HostCertificateAssociation[].Nlm
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.300.1.1100

Specifies if the certificate can be used to secure connections used for Packet Capture file transfers.

CertificateAuthorities (Table)

This table contains information specific to the certificate authority (CA) files present on the unit. The Cert service does not support certificate files that concatenate all the certificates of the chain. In that case, only the first certificate of the file is taken into account.

FileName (Index) | Table: CertificateAuthorities

Type	Text
Range	
Script/CLI	Cert.CertificateAuthorities[].FileName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.400.1.100

Certificate authority (CA) file name.

OverrideIssuedCertificateOcspUrl (Config Parameter) | Table: CertificateAuthorities

Type	Text
Range	Size(0..512)
Default	
Script/CLI	Cert.CertificateAuthorities[].OverrideIssuedCertificateOcspUrl
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.100.400.1.200

Defines a specific OCSP URL to use for certificate revocation status of certificates issued by this certificate authority (CA).
The URL should have one of these formats:

- http://hostname[:port]
- http://hostname/path/filename.xxx

Note: The default empty value means that the OCSP URL present in the certificate to verify will be used for checking its revocation status.

TransferHttpsCipherSuite (Config Parameter)

Type	Enum
Range	CS1(100) | CS2(200) | CS3(300)
Default	CS1
Script/CLI	Cert.TransferHttpsCipherSuite
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.500.100

Defines the allowed cipher suites for the network security settings when using the HTTPS transfer protocol. When the unit initiates an HTTPS connection to a server, it will negotiate the cipher suite according to its configuration.

- CS1:
  - TLS_DHE_DSS_WITH_AES_128_CBC_SHA
  - TLS_DHE_DSS_WITH_AES_256_CBC_SHA
  - Also includes ciphers from CS2 and CS3 below

- CS2:
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - Also includes ciphers from CS3 below
- CS3:
  - The following are TLS 1.2 ciphers:
  - TLS_RSA_WITH_AES_128_CBC_SHA256
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_CBC_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
  - The following are TLS 1.3 ciphers:
  - TLS_AES_256_GCM_SHA384
  - TLS_AES_128_GCM_SHA256
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_CCM_8_SHA256
  - TLS_AES_128_CCM_SHA256

TransferHttpsTlsVersion (Config Parameter)

Type	Enum
Range	TLSv1(200) | TLSv1_1(300) | TLSv1_2(400) | TLSv1_3(500)
Default	TLSv1
Script/CLI	Cert.TransferHttpsTlsVersion
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.500.200

Defines the allowed TLS version for the network security settings when using the HTTPS transfer protocol. When the unit initiates an HTTPS connection to a server, it will negotiate the TLS version according to its configuration.

- TLSv1: Allow TLS versions 1 and up.
- TLSv1_1: Allow TLS versions 1.1 and up.
- TLSv1_2: Allow TLS versions 1.2 and up.
- TLSv1_3: Allow TLS version 1.3 only.

The unit will always send its highest supported TLS version in the ClientHello message. The server will select the highest supported TLS version it supports from the ClientHello message. The unit will then validate that the selected version is allowed. If the version is not allowed the unit will close the connection.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Cert.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.

- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Cert.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2300.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

DownloadCertificate (Command)

Launches the download of the certificate.
Note: The Cert service does not support certificate files that concatenate all the certificates of the chain. In that case, only the first certificate of the file is taken into account.

FileUrl (Argument) | Command: DownloadCertificate

Type	Text
Range	
Default	

URL of the Certificate file that is loaded when using the `Download` command. Supported transfer protocols are:

- HTTP
- HTTPS
- TFTP
- FTP

Examples of valid URLS:

- http://www.myserver.com/Cert_MxDefault001.der
- tftp://myserver.com:69/myfolder/Cert_MxDefault001.der

When the port is not included in the URL, the default port for the chosen protocol is used.
This field may contain macros that will be substituted by the actual value at the moment of fetching the configuration script.

Supported macros are:

- %mac% - the MAC address of the unit.
- %product% - the product name of the unit.
- %serial% - the serial number of the unit.

UserName (Argument) | Command: DownloadCertificate

Type	Text
Range	Size(0..63)
Default	

When authentication is required by the remote file server, this parameter is used as the username.

Password (Argument) | Command: DownloadCertificate

Type	Text
Range	Size(0..63)
Default	

When authentication is required by the remote file server, the value of this parameter is used as the password.

Type (Argument) | Command: DownloadCertificate

Type	Enum
Range	Host(100) | Other(200)
Default	Host

Type of certificate to transfer.

- Host: Certificate and its encryption key used to certify the unit (e.g., a Web server with HTTPS requires a host certificate).

- Other: Trusted CA certificates used to certify peers (e.g., a remote SIP server over TLS).

InstallCertificate (Command)

Install the certificate received in the **FileContent** argument.
Note: Is it recommended to use this command within a configuration script file. Although it is possible to use this command through the CLI, the command total length must be kept under 8 KB, and may take considerable time to complete on low-density platforms like the Mediatrix 4102S.

Note: The Cert service does not support certificate files that concatenate all the certificates of the chain. In that case, only the first certificate of the file is taken into account.

Name (Argument) | Command: InstallCertificate

Type	Text
Range	
Default	

The name to be given to the certificate file, which will be used as the 'File Name'.

Type (Argument) | Command: InstallCertificate

Type	Enum
Range	Host(100) | Other(200)
Default	Host

Type of certificate to install.

- Host: Certificate and its encryption key used to certify the unit (e.g., a Web server with HTTPS requires a host certificate).
- Other: Trusted CA certificates used to certify peers (e.g., a remote SIP server over TLS).

FileContent (Argument) | Command: InstallCertificate

Type	Text
Range	
Default	

The full content of the certificate file, encoded in Base64.

Note: The whole certificate file must be encoded in Base64, including the portions that are already in Base64.

Note: Double quotes must be used around the Base64 value.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

MakeCertificateFactory (Command)

Converts a specific host certificate from the **HostCertificatesInfo** table into a factory certificate. The certificate will be automatically inserted into the **HostCertificatesInfo** table when performing a factory reset.
WARNING: This action cannot be reverted. There is no mechanism to delete a factory certificate. Removing the certificate from the **HostCertificatesInfo** table does not prevent the automatic insertion after a factory reset.

FileName (Argument) | Command: MakeCertificateFactory

Type	Text
Range	
Default	

The file name of the certificate in the **HostCertificatesInfo** table.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Cert service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.2300.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
30	Unable to transfer the requested file because the connection failed.	Error	This message is issued when the Cert service fails to transfer the requested file because the connection could not be established. If using HTTPS file transfers, this error may be due to mismatched security certificates.
40	Unable to transfer the requested file, reason: file not found.	Error	This message is issued when the Cert service fails to transfer the requested file because the host reports it does not exist.
50	Unable to transfer the requested file, reason: access denied.	Error	This message is issued when the Cert service fails to transfer the requested file because the server authentication failed.
60	Unable to transfer the requested file, reason: timed out.	Error	This message is issued when the Cert service fails to transfer the requested file because a timeout occurred.
70	Unable to transfer the requested file, reason: internal error.	Error	This message is issued when the Cert service fails to transfer the requested file and an unexpected situation happened.
80	Unable to transfer the requested file, reason: could not resolve host name.	Error	This message is issued when the Cert service fails to transfer the requested file because the host name cannot be resolved.
90	Unable to transfer the requested file, reason: host or port unreachable.	Error	This message is issued when the Cert service fails to transfer the requested file because the host or port cannot be reached.
100	Certificate successfully downloaded.	Info	This message is issued when the certificate is successfully downloaded and successfully stored.
110	Transferred certificate is invalid.	Error	This message is issued when the Cert service fails to validate the transferred certificate because the certificate is invalid.
120	Unable to store the transferred certificate, reason: file already exists.	Error	This message is issued when the Cert service fails to validate the transferred certificate because the same file name already exists on the host.
130	The transferred certificate file was tagged as host certificate but no private key could be restored from file.	Error	This message is issued when the Cert service fails to validate the transferred certificate because the file was transferred as a host certificate and the file does not contain a valid private key.

NumKey	Message	Severity	Description
140	Unable to store the transferred certificate, reason: certificate file name is too long (maximum 50 characters).	Error	This message is issued when the Cert service fails to store the transferred certificate because the file name is too long (maximum 50 characters).
150	Multiple host certificates are associated with the service %s.	Warning	This message is issued when there are more than one host certificate associated with the service in the **Cert.HostCertificateAssociation** table.
170	Unable to store the transferred certificate, reason: the maximum number is reached for this type of certificate.	Error	This message is issued when the Cert service fails to upload a new certificate because the maximum number of certificates is reached for this type of certificate. (10 Host certificates and 20 Others certificates)
190	Certificate successfully installed.	Info	This message is issued when the certificate is successfully stored.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.

NumKey	Message	Severity	Description
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.

NumKey	Message	Severity	Description
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Cert.

Message	Severity	Description
URL %1$s is invalid, download cancelled.	Error	URL format is invalid and the download has been cancelled.
Download cancelled, a download is currently in progress.	Error	The download has been cancelled since a download is currently being performed. A download must be stopped or completed before another download can be triggered.
Specified association does not match certificate usage.	Warning	This message is issued when a host certificate association is configured by the administrator but will not be used because of its **Cert.OthersCertificatesInfo.Usage** field.
Invalid Base64 file content.	Error	This message is issued when the `Cert.InstallCertificate` command failed because the Base64 file content could not be decoded.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.

Message	Severity	Description
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Command Line Interface (Cli)

The Command Line Interface (CLI) service provides an access to interactively configure all the Mediatrix unit parameters using the SSH or Telnet protocols.

Parameters

InactivityTimeOut (Config Parameter)

Type	UInt32
Range	1..90
Default	15
Script/CLI	Cli.InactivityTimeOut
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2700.1.100

Inactivity expiration delay after which the CLI session closes. This value is expressed in minutes.

WelcomeMessage (Config Parameter)

Type	Text
Range	Size(0..1024)
Default	
Script/CLI	Cli.WelcomeMessage
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2700.1.200

Message displayed when connecting to the CLI.
The following escape characters are supported:

- \\n for new line
- \\t for tab
- \\\\ for \\ character
- Other characters are left unchanged

For Telnet connections, the welcome message appears before the username and password prompts. For SSH connections, the welcome message appears after the username prompt, but before the password prompt.

EnableTelnet (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Cli.EnableTelnet
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2700.1.1000.100

Enable/Disable access to the unit by Telnet.

TelnetPort (Config Parameter)

Type	IpPort
Range	
Default	23
Script/CLI	Cli.TelnetPort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2700.1.1000.200

Port on which the Telnet service should listen for incoming Telnet requests.

EnableSsh (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Cli.EnableSsh
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2700.1.1100.100

Enable/Disable access to the unit by SSH.

SshPort (Config Parameter)

Type	IpPort
Range	
Default	22
Script/CLI	Cli.SshPort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2700.1.1100.200

Port on which the SSH service should listen for incoming SSH requests.

SshSecurityLevel (Config Parameter)

Type	Enum
Range	Permissive(100) | Standard(200) | MostSecure(300)
Default	Standard
Script/CLI	Cli.SshSecurityLevel
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2700.1.1100.300

Selects the encryption group for the required security level.

Permissive: Identical to the Standard group.

Standard: Good compromise between security and interoperability.

- cipher: aes256-ctr, aes128-ctr
- mac: hmac-sha1,hmac-sha2-256
- key exchange: diffie-hellman-group14-sha1, diffie-hellman-group14-sha256, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, curve25519-sha256@libssh.org

Most Secure: Only the most secure encryption algorithms are included. May not work with some SSH clients.

- cipher: aes256-ctr
- mac: hmac-sha2-256
- key exchange: ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, curve25519-sha256@libssh.org

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Cli.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2700.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Cli.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2700.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Cli service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.2700.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.

NumKey	Message	Severity	Description
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Cli.

Message	Severity	Description
Syntax Error in Command Line.	Error	This message is issued when CLI fails to parse the Command Line.
Evaluation failed, reason is: %1$s	Error	This message is issued when CLI fails to evaluate a parameter or run a command.
Assignment failed, reason is: %1$s	Error	This message is issued when CLI fails to assign a value to a parameter.
Warning in evaluation, reason is: %1$s	Error	This message is issued when CLI evaluates a parameter or runs a command and that a warning condition is detected.
Warning in assignment, reason is: %1$s	Error	This message is issued when CLI assigns a value to a parameter and a warning condition is detected.
No such %1$s service, or it is not started.	Error	This message is issued when CLI fails to change the context to an unknown or not started service.
Cannot alias, reason is: %1$s	Error	This message is issued when CLI fails to add an alias to an entity.
Cannot remove alias: No such alias name.	Error	This message is issued when CLI fails to remove an alias.
Alias name is already used.	Error	This message is issued when CLI fails to add an alias.
No such entity name.	Error	This message is issued when CLI fails to add an alias when the entity name is failed.
%1$s is a reserved word.	Error	This message is issued when CLI fails to add an alias when the alias name is a reserved word used by a module, a MIB parameter in current context or a Macro.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.

Message	Severity	Description
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Configuration Manager (Conf)

The Configuration Manager (Conf) service allows executing configuration scripts as well as performing backup/restore of the unit's configuration.

Parameters

ScriptGenericFileName (Config Parameter)

Type	Text
Range	Size(0..254)
Default	
Script/CLI	Conf.ScriptGenericFileName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.100

Name of the generic configuration script to run. Using a generic configuration script but no specific configuration script or vice-versa is allowed. Using both generic and specific configuration scripts is also allowed.
This field may contain some macros that are substituted by the actual value at the moment of fetching the configuration script.

The supported macros are:

- %mac% - the MAC address of the unit.
- %version% - the MFP version of the unit.
- %product% - the product name of the unit.
- %productseries% - the product series name of the unit.
- %profile% - the MFP profile of the unit.
- %serial% - the serial number of the unit.

ScriptSpecificFileName (Config Parameter)

Type	Text
Range	Size(0..254)
Default	
Script/CLI	Conf.ScriptSpecificFileName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.200

Name of the specific configuration script to run. Using a specific configuration script but no generic configuration script or vice-versa is allowed. Using both generic and specific configuration scripts is also allowed. When using a specific configuration script and a generic configuration script, commands from the specific configuration script override commands from the generic configuration script.
This field may contain some macros that are substituted by the actual value at the moment of fetching the configuration script.

The supported macros are:

- %mac% - the MAC address of the unit.
- %version% - the MFP version of the unit.
- %product% - the product name of the unit.
- %productseries% - the product series name of the unit.
- %profile% - the MFP profile of the unit.
- %serial% - the serial number of the unit.

ScriptsLocation (Config Parameter)

Type	Text
Range	Size(0..255)
Default	
Script/CLI	Conf.ScriptsLocation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.300

Path to the location of the configuration files. The path is relative to the root of the configuration scripts server referenced by the parameter **ScriptsTransfer/ScriptsTransferSrvHostname**. Use '/' to separate subdirectories.

This field may contain some macros that are substituted by the actual value at the moment of fetching the configuration script.

The supported macros are:

- %mac% - the MAC address of the unit.
- %version% - the MFP version of the unit.
- %product% - the product name of the unit.
- %productseries% - the product series name of the unit.
- %profile% - the MFP profile of the unit.
- %serial% - the serial number of the unit.

ScriptsTransferProtocol (Config Parameter)

Type	Enum
Range	Http(100) | Https(200) | Tftp(300) | Ftp(400) | File(500)
Default	Https
Script/CLI	Conf.ScriptsTransferProtocol
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.400.100

Protocol used to transfer the configuration script files.

- HTTP
- HTTPS
- TFTP
- FTP
- File: Stored locally. These files are listed under the Management/File page of the DGW Web interface.

ScriptsTransferUsername (Config Parameter)

Type	Text
Range	Size(0..63)
Default	
Script/CLI	Conf.ScriptsTransferUsername
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.400.200

User name used to transfer the configuration script, if the protocol selected by the parameter **ScriptsTransferProtocol** requires it.

ScriptsTransferPassword (Config Parameter)

Type	Text
Range	Size(0..255)
Default	
Script/CLI	Conf.ScriptsTransferPassword
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.400.300

Password used to transfer the configuration script, if the protocol selected by the parameter **ScriptsTransferProtocol** requires it.

Password encryption is supported via the **Dcm.PasswordEncryption** table.

When **Dcm.PasswordEncryption** is enabled clear text passwords will be automatically encrypted.

Unencrypted password maximal length is 63.

Encrypted password maximal length is 113.

ScriptsTransferSrvHostname (Config Parameter)

Type	IpHostNamePort
Range	
Default	0.0.0.0:0
Script/CLI	Conf.ScriptsTransferSrvHostname
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.400.400

Configuration scripts server hostname and port. Use the special port value zero to indicate the protocol default.

ScriptsTransferCertificateValidation (Config Parameter)

Type	Enum
Range	NoValidation(100) | HostName(200)
Default	HostName
Script/CLI	Conf.ScriptsTransferCertificateValidation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.400.500

When downloading a script from an HTTPS server, this parameter defines the level of security to use when validating the server's certificate.

- NoValidation: Allow a connection to the server without validating its certificate. The only condition is to receive a certificate from the server. This option provides partial security and should be selected with care.
- HostName: Allow a connection to the server by validating its certificate is trusted and valid. The validations performed on the certificate include the expiration date and that the Subject Alternate Name (SAN) or Common Name (CN) matches the FQDN or IP address of the server.

ScriptsTransferCertificateTrustLevel (Config Parameter)

Type	Enum
Range	LocallyTrusted(100) | OcspOptional(200) | OcspMandatory(300)
Default	LocallyTrusted
Script/CLI	Conf.ScriptsTransferCertificateTrustLevel
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.400.600

Define how a peer certificate is considered trusted for a HTTPS connection.

- LocallyTrusted: A certificate is considered trusted when the certificate authority (CA) that signed the peer certificate is present in the **Cert.OthersCertificatesInfo** table. The certificate revocation status is not verified.
- OcspOptional: A certificate is considered trusted when it is locally trusted and is not revoked by its certificate authority (CA). The certificate revocation status is queried using the Online Certificate Status Protocol (OCSP). If the OCSP server is not available or the verification status is unknown, the certificate is considered trusted.
- OcspMandatory: A certificate is considered trusted when it is locally trusted and is not revoked by its certificate authority (CA). The certificate revocation status is queried using the Online Certificate Status Protocol (OCSP). If the OCSP server is not available or the verification status is unknown, the certificate is considered not trusted.

ScriptsTransferCipherSuite (Config Parameter)

Type	Enum
Range	CS1(100) | CS2(200) | CS3(300)
Default	CS1
Script/CLI	Conf.ScriptsTransferCipherSuite
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.400.700

Defines the allowed cipher suites for the network security settings when using the HTTPS transfer protocol. When the device initiates an HTTPS connection to a server it will negotiate the cipher suite according to its configuration.

- CS1:
  - TLS_DHE_DSS_WITH_AES_128_CBC_SHA
  - TLS_DHE_DSS_WITH_AES_256_CBC_SHA
  - Also includes ciphers from CS2 and CS3 below
- CS2:
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - Also includes ciphers from CS3 below

- CS3:
  - The following are TLS 1.2 ciphers:
  - TLS_RSA_WITH_AES_128_CBC_SHA256
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_CBC_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
  - The following are TLS 1.3 ciphers:
  - TLS_AES_256_GCM_SHA384
  - TLS_AES_128_GCM_SHA256
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_CCM_8_SHA256
  - TLS_AES_128_CCM_SHA256

ScriptsTransferTlsVersion (Config Parameter)

Type	Enum
Range	TLSv1(200) | TLSv1_1(300) | TLSv1_2(400) | TLSv1_3(500)
Default	TLSv1
Script/CLI	Conf.ScriptsTransferTlsVersion
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.400.800

Defines the allowed TLS version for the network security settings when using the HTTPS transfer protocol. When the device initiates an HTTPS connection to a server it will negotiate the TLS version according to its configuration.

- TLSv1: Allow TLS versions 1 and up.
- TLSv1_1: Allow TLS versions 1.1 and up.
- TLSv1_2: Allow TLS versions 1.2 and up.
- TLSv1_3: Allow TLS version 1.3 only.

The device will always send its highest supported TLS version in the ClientHello message. The server will select the highest supported TLS version it supports from the ClientHello message. The device will then validate that the selected version is allowed. If the version is not allowed the device will close the connection.

ScriptsTransferOnRestartEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Conf.ScriptsTransferOnRestartEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.500.100

Enables the automatic configuration scripts transfer when the unit is restarted.

- Enable: Configuration scripts are automatically transferred when the unit is restarted.
- Disable: Configuration scripts are not automatically transferred when the unit is restarted.

The **ScriptsTransferOnRestartEnable** and the **ScriptsDhcpDownloadEnable** parameters depend on the **ScriptsTransferOnRestartDhcpScriptMaxDelay** parameter. For more details refer to the **ScriptsTransferOnRestartDhcpScriptMaxDelay** parameter.

ScriptsTransferRetriesNumber (Config Parameter)

Type	Int32
Range	-1..100
Default	-1
Script/CLI	Conf.ScriptsTransferRetriesNumber
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.500.150

Maximum attempts to retry a scripts transfer until its success when it fails upon an automatic transfer on restart or automatic periodic transfer. The retries are only attempted if the server is unreachable. Unreachable port or file not found errors don't trigger the retry mechanism. The time interval between retries is 30 seconds.

- -1 means a retry to infinity.

- 0 means no retry.

ScriptsTransferPeriodicEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Conf.ScriptsTransferPeriodicEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.500.200

Enables the automatic periodic configuration scripts transfer. This requires that the device time is correctly set, which can be done with the HOC service.

- Enable: Configuration scripts are automatically transferred periodically.
- Disable: Configuration scripts transfer is not periodic.

ScriptsTransferPeriodicTimeUnit (Config Parameter)

Type	Enum
Range	Minutes(100) | Hours(200) | Days(300)
Default	Hours
Script/CLI	Conf.ScriptsTransferPeriodicTimeUnit
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.500.300

Time unit for the parameter **ScriptsTransferInterval**.

- Minutes: Automatic configuration scripts transfer is performed every x minutes.
- Hours: Automatic configuration scripts transfer is performed every x hours.
- Days: Automatic configuration scripts transfer is performed every x days at the time specified by the **ScriptsTransferTimeRange** parameter.

ScriptsTransferInterval (Config Parameter)

Type	UInt32
Range	1..60
Default	1
Script/CLI	Conf.ScriptsTransferInterval
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.500.400

Time interval between automatic configuration scripts transfer. The time unit is selected by the **ScriptsTransferPeriodicTimeUnit** parameter.

ScriptsTransferTimeOfDay (Config Parameter)

Type	Int32
Range	-1..23
Default	-1
Script/CLI	Conf.ScriptsTransferTimeOfDay
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.500.500

This parameter is obsolete and has been replaced by the **ScriptsTransferTimeRange** parameter.

ScriptsDhcpDownloadEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Conf.ScriptsDhcpDownloadEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.500.600

When enabled, the tftp-server (66) and bootfile (67) DHCP options or sub-options 66 and 67 of the vendor-specific option (43) are used to download a configuration script. If this configuration script is identical to the last executed script, it will not be run twice. The script retry mechanism is not enabled for the DHCP triggered scripts.

If options 66 and 67 are received, both scripts are executed independently and the **ScriptsAllowRepeatedExecution** parameter will have no effect since the service keeps only the last executed script. The script defined by the tftp-server (option 66) option is executed first.

The **ScriptsTransferOnRestartEnable** and the **ScriptsDhcpDownloadEnable** parameters depend on the **ScriptsTransferOnRestartDhcpScriptMaxDelay** parameter. For more details refer to the **ScriptsTransferOnRestartDhcpScriptMaxDelay** parameter.

ScriptsDhcpOptionsFormat (Config Parameter)

Type	Enum
Range	FullyQualified(100) | Url(200) | ServerHost(300) | AutoDetect(400)
Default	AutoDetect
Script/CLI	Conf.ScriptsDhcpOptionsFormat
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.500.650

Defines the file server address format of DHCP options 66 and 67.

- FullyQualified: Allow up to 2 DHCP options (66 and/or 67) to specify a string in the format Script=[protocol]://[username]:[password]@[server]/[path]/[file].
- Url: Allow one DHCP option to specify a file or folder URL in the format [protocol]://[username]:[password]@[server]/[path]/[file]. It is possible to use macros in the URL (see below). If the URL ends with a '/', it is further completed with the path and filename specified in **ScriptLocation** and **ScriptGenericFileName** parameters.
- ServerHost: Allow one DHCP option to specify the IP address or FQDN of a file server. Uses the path and filename specified in the **ScriptLocation** and **ScriptGenericFileName** parameters, use the transfer protocol, username and password specified in **ScriptTransferProtocol**, **ScriptTransferUsername** and **ScriptTransferPassword** parameters.
- AutoDetect: Automatically detects the format of the DHCP Option, according to these criteria:
  - A value beginning with "Script=" is considered as "FullyQualified";
  - A value beginning with "[protocol]://" is considered as a URL;
  - A value that looks like an IPv4/IPv6 address or domain name is considered as a "ServerHost".

The following macros can be inserted in the URL and will be replaced by their actual values:

- %mac% - the MAC address of the unit.
- %version% - the MFP version of the unit.
- %product% - the product name of the unit.
- %productseries% - the product series name of the unit.
- %profile% - the MFP profile of the unit.
- %serial% - the serial number of the unit.

ScriptsTransferOnRestartDhcpScriptMaxDelay (Config Parameter)

Type	UInt32
Range	0..360
Default	0
Script/CLI	Conf.ScriptsTransferOnRestartDhcpScriptMaxDelay
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.500.660

This parameter allows the prioritization of the DHCP script versus the automatic script at startup when both **ScriptsDhcpDownloadEnable** and **ScriptsTransferOnRestartEnable** parameters are set to 'Enable'.

When the unit is restarted and the delay is set to 0, the script associated with the **ScriptsTransferOnRestartEnable** parameter is immediately transferred.

When the unit is restarted and the delay is set to a value other than 0, the script associated with the **ScriptsTransferOnRestartEnable** parameter is transferred when this delay is expired. While the script is delayed:

- If DHCP options provide script information to transfer, then the transfer of the script associated with the **ScriptsTransferOnRestartEnable** parameter is aborted.
- If there is no DHCP option providing script information to transfer, once the delay is expired, the script associated with the **ScriptsTransferOnRestartEnable** parameter is transferred.

This value is expressed in seconds (s).

ScriptsTransferTimeRange (Config Parameter)

Type	Text
Range	Size(0..24)
Default	
Script/CLI	Conf.ScriptsTransferTimeRange
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.500.700

Time range when the automatic configuration scripts transfer occurs. The time unit selected by the **ScriptsTransferPeriodicTimeUnit** parameter must be Days.

If a time range is specified, the unit will fetch the configuration files at a random time within the interval specified.

The format should be one of the following:

- hh[:mm[:ss]]

- hh[:mm[:ss]] - hh[:mm[:ss]]

Where:

- hh: Hours.
- mm: Minutes.
- ss: Seconds.

ScriptsSecretKey (Config Parameter)

Type	Text
Range	Size(0..512)
Default	
Script/CLI	Conf.ScriptsSecretKey
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.600

Key used to decrypt both the generic and specific configuration scripts. No need to specify the encryption method, it is automatically detected from the file.
The format of the key depends on the method that has been used to encrypt the configuration script:

- Blowfish: The key is encoded in hexadecimal notation, meaning only characters in the range 0-9 and A-F can be used. The maximum key length is 64 hex characters, which gives a binary key of 256 bits. It is the maximum key size accepted by the MxCryptFile external tool. For example, a 32-bit key could look like: A36CB299.
- Aes256Gcm: A password of variable-length ASCII characters. For optimal security, it is recommended to use a password of at least 42 characters. The maximum length is 256 characters.

Note: When a key is defined, unencrypted configuration scripts are not allowed to be executed.

Password encryption is supported via the **Dcm.PasswordEncryption** table.

When **Dcm.PasswordEncryption** is enabled clear text passwords will be automatically encrypted.

Unencrypted password maximal length is 256.

Encrypted password maximal length is 389.

ScriptsAllowRepeatedExecution (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Conf.ScriptsAllowRepeatedExecution
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.650

Allows the execution of a script even if it is identical to the last executed script. It has no effect when the two DHCP options tftp-server (66) and bootfile (67) are present since only the last executed script is kept.

ScriptExportContent (Config Parameter)

Type	Enum
Range	AllConfig(100) | ModifiedConfig(200) | AllConfigAndFiles(300)
Default	ModifiedConfig
Script/CLI	Conf.ScriptExportContent
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.1000.100

Content to export in generated configuration script.

- AllConfig: Export everything.
- ModifiedConfig: Export only the configuration that has been modified (differs from the default values).
- AllConfigAndFiles: Export everything, including certificates and SBC ruleset files under sbc/rulesets.

Note: A file larger than 48 KB will not be exported.

ScriptExportServiceName (Config Parameter)

Type	Text
Range	Size(0..64)
Default	All
Script/CLI	Conf.ScriptExportServiceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.1000.150

Name of the service from which to export configuration. The special value 'All' can be used to export the configuration of all services.

ScriptExportUrl (Config Parameter)

Type	Text
Range	Size(0..512)
Default	
Script/CLI	Conf.ScriptExportUrl
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.1000.200

URL where to send the exported configuration script. The URL should follow this format: protocol://[user[:password]@]hostname[:port]/[path/]filename

The brackets [] denote an optional parameter.

The filename may contain alphanumerical and '-._%$' characters as well as macros that are substituted at the moment of sending the configuration script.

The supported macros are:

- %mac% - the MAC address of the unit.
- %version% - the MFP version of the unit.
- %serial% - the serial number of the unit.

The transfer protocols supported are:

- HTTP: The server must support the PUT method.
- HTTPS: The server must support the PUT method.
- TFTP
- FTP
- File: Stored locally. These files are listed under the Management/File page of the DGW Web interface.

Examples of valid URLs:

- http://webserver.com/script.cfg
- https://username:password@webserver.com/script.cfg
- tftp://tftpserver.com:69/folder/script.cfg
- ftp://guest@ftpserver.com/script.cfg
- ftp://username:password@ftpserver.com/script.cfg
- file://script.cfg

ScriptExportSecretKey (Config Parameter)

Type	Text
Range	Size(0..512)
Default	
Script/CLI	Conf.ScriptExportSecretKey
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.1000.300

Key used to encrypt the exported configuration script. If no key is specified, then the configuration script will not be encrypted.
The format of the key depends on the encryption method specified in the **Conf.ScriptExportPrivacyAlgo** parameter:

- Blowfish: The key is encoded in hexadecimal notation, meaning only characters in the range 0-9 and A-F can be used. The maximum key length is 64 hex characters, which gives a binary key of 256 bits. It is the maximum key size accepted by the MxCryptFile external tool. For example, a 32-bit key could look like: A36CB299.
- Aes256Gcm: A password of variable-length ASCII characters. For optimal security, it is recommended to use a password of at least 42 characters. The maximum length is 256 characters.

Password encryption is supported via the **Dcm.PasswordEncryption** table.

When **Dcm.PasswordEncryption** is enabled clear text passwords will be automatically encrypted.

Unencrypted password maximal length is 256.

Encrypted password maximal length is 389.

ScriptExportPrivacyAlgo (Config Parameter)

Type	Enum
Range	Blowfish(200) | Aes256Gcm(300)
Default	Aes256Gcm
Script/CLI	Conf.ScriptExportPrivacyAlgo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.1000.400

Defines the encryption method for scripts export.

- Blowfish: scripts are encrypted with legacy Blowfish ECB mode.
- Aes256Gcm: scripts are encrypted with AES-256 GCM mode. This is the recommended algorithm.

ScriptsStatsCurrentTransferState (Status Parameter)

Type	Enum
Range	Idle(100) | Transfering(200) | Running(300)
Script/CLI	Conf.ScriptsStatsCurrentTransferState
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.10000.700

The current state of the configuration script transfer and execution.

- Idle: No configuration script is currently running.
- Transfering: A configuration script is currently being transferred.
- Running: The transferred configuration script is currently running.

ScriptsStatsLastTransferResult (Status Parameter)

Type	Enum
Range	None(100) | Success(200) | ExecutionFailed(300) | TransferFailed(400)
Script/CLI	Conf.ScriptsStatsLastTransferResult
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.10000.800

Result of the last configuration scripts transfer and run command.

- None: No configuration scripts transfer performed since the last reset to default settings.

- Success: The last configuration scripts transfer succeeded and the transferred scripts were ran successfully.
- ExecutionFailed: The last configuration scripts transfer succeeded but at least one of the transferred scripts failed to run.
- TransferFailed: At least one of the last configuration scripts transfer failed.

ScriptsStatsLastTransferDateTime (Status Parameter)

Type	Text
Range	Size(0..255)
Script/CLI	Conf.ScriptsStatsLastTransferDateTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.10000.900

Date and time of the last successful configuration script transfer and execution command since the last reset to default settings.

ScriptsStatsCurrentExportState (Status Parameter)

Type	Enum
Range	Idle(100) | Transfering(200) | Exporting(300)
Script/CLI	Conf.ScriptsStatsCurrentExportState
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.10000.1000

The current state of the configuration script exportation.

- Idle: No configuration script is currently exporting.
- Exporting: A configuration script exportation is currently in progress.
- Transfering: The exported configuration script is currently being transferred.

ScriptsStatsLastExportResult (Status Parameter)

Type	Enum
Range	None(100) | Success(200) | ExportationFailed(300) | TransferFailed(400)
Script/CLI	Conf.ScriptsStatsLastExportResult
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.10000.1100

Result of the last configuration script exportation command.

- None: No configuration script exportation performed since the last reset to default settings.
- Success: The last configuration script exportation succeeded and has been transferred successfully.
- ExportationFailed: The last configuration script exportation failed.
- TransferFailed: The last configuration script exportation succeeded but the script failed to transfer.

ScriptsStatsLastExportDateTime (Status Parameter)

Type	Text
Range	Size(0..255)
Script/CLI	Conf.ScriptsStatsLastExportDateTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.100.10000.1200

Date and time of the last successful configuration script exportation and transfer command since the last reset to default settings.

ImageFileName (Config Parameter)

Type	Text
Range	Size(0..254)
Default	
Script/CLI	Conf.ImageFileName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.200.100

Name of the file used to backup (save) and restore (load) the unit's configuration. It is composed of alphanumerical and '-._%$' characters as well as macros. The macros used in this field are replaced by the unit's MAC address or MFP version right before backing up or restoring the unit's configuration.
The supported macros are:

- %mac% - the MAC address of the unit.
- %version% - the MFP version of the unit.
- %product% - the product name of the unit.
- %productseries% - the product series name of the unit.
- %profile% - the MFP profile of the unit.
- %serial% - the serial number of the unit.

ImageLocation (Config Parameter)

Type	Text
Range	Size(0..255)
Default	
Script/CLI	Conf.ImageLocation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.200.200

Path to the location of the configuration image file. The path is relative to the root of the transfer server. Use '/' to separate subdirectories.
This field may contain some macros that are substituted by the actual value at the moment of fetching the configuration script.

The supported macros are:

- %mac% - the MAC address of the unit.
- %version% - the MFP version of the unit.
- %product% - the product name of the unit.
- %productseries% - the product series name of the unit.
- %profile% - the MFP profile of the unit.
- %serial% - the serial number of the unit.

ImageBackupContent (Config Parameter)

Type	Enum
Range	Config(100) | ConfigAndCertificates(200)
Default	ConfigAndCertificates
Script/CLI	Conf.ImageBackupContent
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.200.250

Defines what to include in the backup image file.

- Config: Only the unit's configuration and ruleset files are included in the backup image.
- ConfigAndCertificates: The unit's configuration, ruleset files and certificates are included in the backup image. It is strongly recommended to activate encryption (see the **ImagePrivacyAlgo** and **ImageSecretKey** parameters) when including certificates in the backup image because host certificates include the private key.

- Note: Only ruleset files from the folder '/sbc/rulesets' in the File service are included in the backup image.

ImageTransferProtocol (Config Parameter)

Type	Enum
Range	Http(100) | Https(200) | Tftp(300) | Ftp(400) | File(500)
Default	Https
Script/CLI	Conf.ImageTransferProtocol
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.200.300.100

Protocol used to upload a configuration image during backup, or to retrieve a configuration image during restore.

- HTTP
- HTTPS
- TFTP
- FTP
- File: Stored locally. These files are listed under the Management/File page of the DGW Web interface.

Note: To backup over HTTP and HTTPS, the server must support the PUT method.

ImageTransferUsername (Config Parameter)

Type	Text
Range	Size(0..63)
Default	
Script/CLI	Conf.ImageTransferUsername
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.200.300.200

User name used to transfer the configuration image, if the protocol selected by the parameter **ImageTransferProtocol** requires it.

ImageTransferPassword (Config Parameter)

Type	Text
Range	Size(0..255)
Default	
Script/CLI	Conf.ImageTransferPassword
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.200.300.300

Password used to transfer the configuration image, if the protocol selected by the parameter **ImageTransferProtocol** requires it.

Password encryption is supported via the **Dcm.PasswordEncryption** table.

When **Dcm.PasswordEncryption** is enabled clear text passwords will be automatically encrypted.

Unencrypted password maximal length is 63.

Encrypted password maximal length is 113.

ImageTransferSrvHostname (Config Parameter)

Type	IpHostNamePort
Range	
Default	0.0.0.0:0
Script/CLI	Conf.ImageTransferSrvHostname
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.200.300.400

Configuration backup/restore server hostname and port. Use the special value zero to indicate the protocol default.

ImageTransferCipherSuite (Config Parameter)

Type	Enum
Range	CS1(100) | CS2(200) | CS3(300)
Default	CS1
Script/CLI	Conf.ImageTransferCipherSuite
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.200.300.500

Defines the allowed cipher suites for the network security settings when using the HTTPS transfer protocol. When the device initiates an HTTPS connection to a server it will negotiate the cipher suite according to its configuration.

- CS1:
  - TLS_DHE_DSS_WITH_AES_128_CBC_SHA
  - TLS_DHE_DSS_WITH_AES_256_CBC_SHA
  - Also includes ciphers from CS2 and CS3 below
- CS2:
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - Also includes ciphers from CS3 below

- CS3:
  - The following are TLS 1.2 ciphers:
  - TLS_RSA_WITH_AES_128_CBC_SHA256
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_CBC_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
  - The following are TLS 1.3 ciphers:
  - TLS_AES_256_GCM_SHA384
  - TLS_AES_128_GCM_SHA256
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_CCM_8_SHA256
  - TLS_AES_128_CCM_SHA256

ImageTransferTlsVersion (Config Parameter)

Type	Enum
Range	TLSv1(200) | TLSv1_1(300) | TLSv1_2(400) | TLSv1_3(500)
Default	TLSv1
Script/CLI	Conf.ImageTransferTlsVersion
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.200.300.600

Defines the allowed TLS version for the network security settings when using the HTTPS transfer protocol. When the device initiates an HTTPS connection to a server it will negotiate the TLS version according to its configuration.

- TLSv1: Allow TLS versions 1 and up.
- TLSv1_1: Allow TLS versions 1.1 and up.
- TLSv1_2: Allow TLS versions 1.2 and up.
- TLSv1_3: Allow TLS version 1.3 only.

The device will always send its highest supported TLS version in the ClientHello message. The server will select the highest supported TLS version it supports from the ClientHello message. The device will then validate that the selected version is allowed. If the version is not allowed the device will close the connection.

ImagePrivacyAlgo (Config Parameter)

Type	Enum
Range	None(100) | Blowfish(200) | Aes256Gcm(300)
Default	None
Script/CLI	Conf.ImagePrivacyAlgo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.200.400.100

Defines the encryption method for backup operations. Restore operations ignore this parameter, since the encryption method is automatically detected.

- None: Backup images are not encrypted.
- Blowfish: Backup images are encrypted with legacy Blowfish CBC mode. This algorithm cannot be decrypted by the MxCryptFile stand-alone tool.
- Aes256Gcm: Backup images are encrypted with AES-256 GCM mode. This is the recommended algorithm.

ImageSecretKey (Config Parameter)

Type	Text
Range	Size(0..512)
Default	
Script/CLI	Conf.ImageSecretKey
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.200.400.200

Key used both to encrypt a backup image, and to decrypt an image to restore.
For backup operations to be encrypted, make sure the **ImagePrivacyAlgo** parameter is not set to "None".

The format of the key depends on the encryption method (see the **Conf.ImagePrivacyAlgo** parameter):

- Blowfish: The key is encoded in hexadecimal notation, meaning only characters in the range 0-9 and A-F can be used. The maximum key length is 64 hex characters, which gives a binary key of 256 bits. It is the maximum key size accepted by the MxCryptFile external tool. For example, a 32-bit key could look like: A36CB299.
- Aes256Gcm: A password of variable-length ASCII characters. For optimal security, it is recommended to use a password of at least 42 characters. The maximum length is 256 characters.

Password encryption is supported via the **Dcm.PasswordEncryption** table.

When **Dcm.PasswordEncryption** is enabled clear text passwords will be automatically encrypted.

Unencrypted password maximal length is 256.

Encrypted password maximal length is 389.

ImageBackupStatus (Status Parameter)

Type	Enum
Range	None(100) | Success(200) | Failed(300)
Script/CLI	Conf.ImageBackupStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.200.600

Result of the last configuration backup command.

- None: No configuration backup operation has been performed since the last reset to default settings.
- Success: Last configuration backup operation succeeded.
- Failed: Last configuration backup operation failed.

ImageRestoreStatus (Status Parameter)

Type	Enum
Range	None(100) | Success(200) | ApplyFailed(300) | LoadFailed(400)
Script/CLI	Conf.ImageRestoreStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.200.800

Result of the last configuration restore command.

- None: No configuration restore has been performed since the last reset to default settings.

- Success: The last configuration restore succeeded.
- ApplyFailed: The configuration load succeeded but restoring failed during the last configuration restore command execution.
- LoadFailed: The configuration load failed during the last configuration restore command.

Macros (Table)

This table contains information about macro functions.

Name (Index) | Table: Macros

Type	Text
Range	
Script/CLI	Conf.Macros[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.300.100.1.100

Displays the macro name.

Description (Status Parameter) | Table: Macros

Type	Text
Range	
Script/CLI	Conf.Macros[].Description
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.300.100.1.200

Shows the macro description.

Alias (Table)

This table contains information about alias.

Name (Index) | Table: Alias

Type	Text
Range	
Script/CLI	Conf.Alias[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.300.200.1.100

Displays the alias name.

Entity (Status Parameter) | Table: Alias

Type	Text
Range	
Script/CLI	Conf.Alias[].Entity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.300.200.1.200

Shows the alias value.

Type (Status Parameter) | Table: Alias

Type	Enum
Range	Module(100) | Object(200) | Columnar(300)
Script/CLI	Conf.Alias[].Type
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.300.200.1.300

Shows the alias type.

Context (Status Parameter) | Table: Alias

Type	Text
Range	
Script/CLI	Conf.Alias[].Context
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.300.200.1.400

Shows the alias context.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Conf.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Conf.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.800.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

BackupImage (Command)

Launches the configuration backup operation using the specified arguments. The content of the backup image depends on the value of the **ImageBackupContent** parameter. All rulesets (.crs and .rrs) under /sbc/rulesets/ in the file service are backed up as external files.

FileName (Argument) | Command: BackupImage

Type	Text
Range	Size(0..255)
Default	

Name of the file used to backup (save) and restore (load) the unit's configuration.
This argument may contain alphanumerical and '-._%$' characters as well as some macros that are substituted by the actual value at the moment of fetching the configuration script.

The supported macros are:

- %mac% - the MAC address of the unit.
- %version% - the MFP version of the unit.
- %product% - the product name of the unit.
- %productseries% - the product series name of the unit.
- %profile% - the MFP profile of the unit.
- %serial% - the serial number of the unit.

Location (Argument) | Command: BackupImage

Type	Text
Range	Size(0..255)
Default	

Path to the location of the configuration image file. The path is relative to the root of the transfer server. Use '/' to separate subdirectories.
This argument may contain some macros that are substituted by the actual value at the moment of fetching the configuration script.

The supported macros are:

- %mac% - the MAC address of the unit.
- %version% - the MFP version of the unit.
- %product% - the product name of the unit.
- %productseries% - the product series name of the unit.
- %profile% - the MFP profile of the unit.
- %serial% - the serial number of the unit.

TransferProtocol (Argument) | Command: BackupImage

Type	Enum
Range	Http(100) | Https(200) | Tftp(300) | Ftp(400) | File(500)
Default	Https

Protocol used to back up a configuration image.

- HTTP: The server must support the PUT method.
- HTTPS: The server must support the PUT method.
- TFTP
- FTP
- File: Stored locally. These files are listed under the Management/File page of the DGW Web interface.

TransferUsername (Argument) | Command: BackupImage

Type	Text
Range	Size(0..63)
Default	

User name used to transfer the configuration image, if the protocol selected by the parameter **ImageTransferProtocol** requires it.

TransferPassword (Argument) | Command: BackupImage

Type	Text
Range	Size(0..63)
Default	

Password used to transfer the configuration image, if the protocol selected by the parameter **ImageTransferProtocol** requires it.

TransferSrvHostname (Argument) | Command: BackupImage

Type	IpHostNamePort
Range	
Default	0.0.0.0:0

Configuration backup/restore server hostname. Use the special port value zero to indicate the protocol default.

SecretKey (Argument) | Command: BackupImage

Type	Text
Range	Size(0..256)
Default	

Key used to encrypt the backup image. If no key is specified, then the backup image will not be encrypted.
The format of the key depends on the encryption method specified in the **ImagePrivacyAlgo** argument:

- Blowfish: The key is encoded in hexadecimal notation, meaning only characters in the range 0-9 and A-F can be used. The maximum key length is 64 hex characters, which gives a binary key of 256 bits. It is the maximum key size accepted by the MxCryptFile external tool. For example, a 32-bit key could look like: A36CB299.
- Aes256Gcm: A password of variable-length ASCII characters. For optimal security, it is recommended to use a password of at least 42 characters. The maximum length is 256 characters.

ImagePrivacyAlgo (Argument) | Command: BackupImage

Type	Enum
Range	Blowfish(200) | Aes256Gcm(300)
Default	Aes256Gcm

Defines the encryption method for backup image.

- Blowfish: Backup images are encrypted with legacy Blowfish CBC mode. This algorithm cannot be decrypted by the MxCryptFile stand-alone tool.
- Aes256Gcm: Backup images are encrypted with AES-256 GCM mode. This is the recommended algorithm.

ConfiguredBackupImage (Command)

Launches the configuration backup operation using the configuration parameters of the Conf service.

ConfiguredRestoreImage (Command)

Launches the configuration restore operation using the configured parameters. If the configuration image transfer or loading is successful, the configuration is automatically restored.

ConfiguredScriptExport (Command)

Generates a configuration script using the current configuration.

ConfiguredScriptsTransferAndRun (Command)

Launches the configuration scripts transfer using the configured parameters. If successful, the configuration scripts will run. The corresponding parameter values are used for missing arguments.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

RebootIfNeeded (Command)

Initiates a unit reboot only if a hardware configuration has been modified. If applicable, the configuration scripts transfer and run is performed again after the reboot.

RestoreImage (Command)

Launches the configuration restore operation in background. The **ImageBackupStatus** parameter indicates the progress of the backup.

Note: All rulesets files (.crs and .rrs) under the folder '/sbc/rulesets/' in the file service are removed before the image is restored.

FileName (Argument) | Command: RestoreImage

Type	Text
Range	Size(0..255)
Default	

Name of the file used to backup (save) and restore (load) the unit's configuration.
This argument may contain some macros that are substituted by the actual value at the moment of fetching the configuration script.

The supported macros are:

- %mac% - the MAC address of the unit.
- %version% - the MFP version of the unit.
- %product% - the product name of the unit.
- %productseries% - the product series name of the unit.
- %profile% - the MFP profile of the unit.
- %serial% - the serial number of the unit.

Location (Argument) | Command: RestoreImage

Type	Text
Range	Size(0..255)
Default	

Path to the location of the configuration image file. The path is relative to the root of the transfer server. Use '/' to separate subdirectories.
This argument may contain some macros that are substituted by the actual value at the moment of fetching the configuration script.

The supported macros are:

- %mac% - the MAC address of the unit.

- %version% - the MFP version of the unit.
- %product% - the product name of the unit.
- %productseries% - the product series name of the unit.
- %profile% - the MFP profile of the unit.
- %serial% - the serial number of the unit.

TransferProtocol (Argument) | Command: RestoreImage

Type	Enum
Range	Http(100) | Https(200) | Tftp(300) | Ftp(400) | File(500)
Default	Https

Protocol used to transfer the configuration image to restore.

- HTTP
- HTTPS
- TFTP
- FTP
- File: Stored locally. These files are listed under the Management/File page of the DGW Web interface.

TransferUsername (Argument) | Command: RestoreImage

Type	Text
Range	Size(0..63)
Default	

User name used to transfer the configuration image, if the protocol selected by the parameter **ImageTransferProtocol** requires it.

TransferPassword (Argument) | Command: RestoreImage

Type	Text
Range	Size(0..63)
Default	

Password used to transfer the configuration image, if the protocol selected by the parameter **ImageTransferProtocol** requires it.

TransferSrvHostname (Argument) | Command: RestoreImage

Type	IpHostNamePort
Range	
Default	0.0.0.0:0

Configuration backup/restore server hostname. Use the special port value zero to indicate the protocol default.

SecretKey (Argument) | Command: RestoreImage

Type	Text
Range	Size(0..256)
Default	

Key used to decrypt a backup image file. No need to specify the encryption method, it is automatically detected from the file.
The format of the key depends on the method that has been used to encrypt the backup image:

- Blowfish: The key is encoded in hexadecimal notation, meaning only characters in the range 0-9 and A-F can be used. The maximum key length is 64 hex characters, which gives a binary key of 256 bits. It is the maximum key size accepted by the MxCryptFile external tool. For example, a 32-bit key could look like: A36CB299.
- Aes256Gcm: A password of variable-length ASCII characters. For optimal security, it is recommended to use a password of at least 42 characters. The maximum length is 256 characters.

ScriptExport (Command)

Generates a configuration script using the configuration given in the command's arguments.

Content (Argument) | Command: ScriptExport

Type	Enum
Range	AllConfig(100) | ModifiedConfig(200) | AllConfigAndFiles(300)
Default	ModifiedConfig

Content to export in generated configuration script.

- AllConfig: Export everything.
- ModifiedConfig: Export only the configuration that has been modified (differs from the default values).
- AllConfigAndFiles: Export everything, including certificates and SBC ruleset files under sbc/rulesets.

Note: A file larger than 48 KB will not be exported.

ServiceName (Argument) | Command: ScriptExport

Type	Text
Range	Size(0..64)
Default	All

Name of the service from which to export configuration. The special value 'All' can be used to export the configuration of all services.

Url (Argument) | Command: ScriptExport

Type	Text
Range	Size(0..512)
Default	

URL where to send the exported configuration script. The URL should follow this format: protocol://[user[:password]@]hostname[:port]/[path/]filename

The brackets [] denote an optional parameter.
The filename may only be composed of alphanumerical and '-._%$' characters.

The transfer protocols supported are:

- HTTP: The server must support the PUT method.
- HTTPS: The server must support the PUT method.

- TFTP
- FTP
- File: Stored locally. These files are listed under the Management/File page of the DGW Web interface.

Examples of valid URLs:

- http://webserver.com/script.cfg
- https://username:password@webserver.com/script.cfg
- tftp://tftpserver.com:69/folder/script.cfg
- ftp://guest@ftpserver.com/script.cfg
- ftp://username:password@ftpserver.com/script.cfg
- file://script.cfg

SecretKey (Argument) | Command: ScriptExport

Type	Text
Range	Size(0..256)
Default	

Key used to encrypt the exported configuration script. If no key is specified, then the configuration script will not be encrypted.
The format of the key depends on the encryption method specified in the **PrivacyAlgo** argument:

- Blowfish: The key is encoded in hexadecimal notation, meaning only characters in the range 0-9 and A-F can be used. The maximum key length is 64 hex characters, which gives a binary key of 256 bits. It is the maximum key size accepted by the MxCryptFile external tool. For example, a 32-bit key could look like: A36CB299.
- Aes256Gcm: A password of variable-length ASCII characters. For optimal security, it is recommended to use a password of at least 42 characters. The maximum length is 256 characters.

PrivacyAlgo (Argument) | Command: ScriptExport

Type	Enum
Range	Blowfish(200) | Aes256Gcm(300)
Default	Aes256Gcm

Defines the encryption method for scripts export.

- Blowfish: scripts are encrypted with legacy Blowfish ECB mode.

- Aes256Gcm: scripts are encrypted with AES-256 GCM mode. This is the recommended algorithm.

ScriptsTransferAndRun (Command)

Launches the configuration scripts transfer in background. If successful, the configuration scripts will run. The corresponding parameter values are used for missing arguments.

GenericFileName (Argument) | Command: ScriptsTransferAndRun

Type	Text
Range	Size(0..254)
Default	

Name of the generic configuration script. Using a generic configuration script but no specific configuration script or vice-versa is allowed. Using both generic and specific configuration scripts is also allowed.
This argument may contain some macros that are substituted by the actual value at the moment of fetching the configuration script.

The supported macros are:

- %mac% - the MAC address of the unit.
- %version% - the MFP version of the unit.
- %product% - the product name of the unit.
- %productseries% - the product series name of the unit.
- %profile% - the MFP profile of the unit.
- %serial% - the serial number of the unit.

SpecificFileName (Argument) | Command: ScriptsTransferAndRun

Type	Text
Range	Size(0..254)
Default	

Name of the specific configuration script. Using a specific configuration script but no generic configuration script or vice-versa is allowed. Using both generic and specific configuration scripts is also allowed. When using a specific configuration script and a generic configuration script, commands from the specific configuration script override commands from the generic configuration script.

This argument may contain some macros that are substituted by the actual value at the moment of fetching the configuration script.

The supported macros are:

- %mac% - the MAC address of the unit.
- %version% - the MFP version of the unit.
- %product% - the product name of the unit.
- %productseries% - the product series name of the unit.
- %profile% - the MFP profile of the unit.
- %serial% - the serial number of the unit.

Location (Argument) | Command: ScriptsTransferAndRun

Type	Text
Range	Size(0..255)
Default	

Path to the location of the configuration files. The path is relative to the root of the configuration scripts server referenced by the parameter **ScriptsTransfer/ScriptsTransferSrvHostname**. Use '/' to separate subdirectories.

This argument may contain some macros that are substituted by the actual value at the moment of fetching the configuration script.

The supported macros are:

- %mac% - the MAC address of the unit.
- %version% - the MFP version of the unit.
- %product% - the product name of the unit.
- %productseries% - the product series name of the unit.
- %profile% - the MFP profile of the unit.
- %serial% - the serial number of the unit.

TransferProtocol (Argument) | Command: ScriptsTransferAndRun

Type	Enum
Range	Http(100) | Https(200) | Tftp(300) | Ftp(400) | File(500)
Default	Https

Protocol used to transfer the configuration script files.

- HTTP
- HTTPS
- TFTP
- FTP
- File: Stored locally. These files are listed under the Management/File page of the DGW Web interface.

TransferUsername (Argument) | Command: ScriptsTransferAndRun

Type	Text
Range	Size(0..63)
Default	

User name used to transfer the configuration script, if the protocol selected by the parameter **ScriptsTransferProtocol** requires it.

TransferPassword (Argument) | Command: ScriptsTransferAndRun

Type	Text
Range	Size(0..63)
Default	

Password used to transfer the configuration script, if the protocol selected by the parameter **ScriptsTransferProtocol** requires it.

TransferSrvHostname (Argument) | Command: ScriptsTransferAndRun

Type	IpHostNamePort
Range	
Default	0.0.0.0:0

Configuration scripts server hostname. Use the special port value zero to indicate the protocol default.

AllowRepeatedExecution (Argument) | Command: ScriptsTransferAndRun

Type	Enum
Range	Auto(100) | Enable(200) | Disable(300)
Default	Auto

Allows the execution of a script even if it is identical to the last executed script.

- Auto: Use the configured value of ScriptsAllowRepeatedExecution.
- Enable: Allow repeated execution of the same script.
- Disable: Do not allow repeated execution of the same script.

CertificateValidation (Argument) | Command: ScriptsTransferAndRun

Type	Enum
Range	Auto(1) | NoValidation(100) | HostName(200)
Default	Auto

When downloading a script from an HTTPS server, this parameter defines the level of security to use when validating the server's certificate.

- Auto: Use the configured value of **ScriptsTransferCertificateValidation**.
- NoValidation: Allow a connection to the server without validating its certificate. The only condition is to receive a certificate from the server. This option provides partial security and should be selected with care.
- HostName: Allow a connection to the server by validating its certificate is trusted and valid. The validations performed on the certificate include the expiration date and that the Subject Alternate Name (SAN) or Common Name (CN) matches the FQDN or IP address of the server.

CertificateTrustLevel (Argument) | Command: ScriptsTransferAndRun

Type	Enum
Range	Auto(1) | LocallyTrusted(100) | OcspOptional(200) | OcspMandatory(300)
Default	Auto

Define how a peer certificate is considered trusted for a HTTPS connection.

- Auto: Use the configured value of **ScriptsTransferCertificateTrustLevel**.

- LocallyTrusted: A certificate is considered trusted when the certificate authority (CA) that signed the peer certificate is present in the **Cert.OthersCertificatesInfo** table. The certificate revocation status is not verified.
- OcspOptional: A certificate is considered trusted when it is locally trusted and is not revoked by its certificate authority (CA). The certificate revocation status is queried using the Online Certificate Status Protocol (OCSP). If the OCSP server is not available or the verification status is unknown, the certificate is considered trusted.
- OcspMandatory: A certificate is considered trusted when it is locally trusted and is not revoked by its certificate authority (CA). The certificate revocation status is queried using the Online Certificate Status Protocol (OCSP). If the OCSP server is not available or the verification status is unknown, the certificate is considered not trusted.

SecretKey (Argument) | Command: ScriptsTransferAndRun

Type	Text
Range	Size(0..256)
Default	

Key used to decrypt both the generic and specific configuration scripts. No need to specify the encryption method, it is automatically detected from the file.
The format of the key depends on the method that has been used to encrypt the configuration script:

- Blowfish: The key is encoded in hexadecimal notation, meaning only characters in the range 0-9 and A-F can be used. The maximum key length is 64 hex characters, which gives a binary key of 256 bits. It is the maximum key size accepted by the MxCryptFile external tool. For example, a 32-bit key could look like: A36CB299.
- Aes256Gcm: A password of variable-length ASCII characters. For optimal security, it is recommended to use a password of at least 42 characters. The maximum length is 256 characters.

Note: When a key is defined, unencrypted configuration scripts are not allowed to be executed.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Conf service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.800.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
1100	Transfer and Run Configuration Scripts Command Received.	Debug	This message is issued when the service receives the `ConfigScriptsTransferAndRun` command.
1200	Transfer and Run Configuration Scripts On Restart Triggered.	Info	This message is issued when the automatic configuration scripts transfer and run on restart is triggered by a system restart.
1210	Transfer and execution of the configuration scripts when unit is restarted, was aborted. Reason: Selected DHCP options require to transfer the script by DHCP. Aborted Transfer and Run Configuration Scripts On Restart, reason: DHCP options provided script information to transfer.	Info	This message is issued when the automatic configuration scripts transfer and run on restart is aborted by the system after receiving the script information to transfer via DHCP options.
1220	Delayed for %1$d (s) the transfer and the execution of the configuration scripts when the unit is restarted. Reason: allow DHCP options to provide script transfer information.	Info	This message is issued when the automatic configuration scripts transfer and run on restart is delayed by **ScriptsTransferOnRestartDhcpScriptMaxDelay** value to allow DHCP options to provide script information.
1250	Transfer and Resume Configuration Scripts On Restart Triggered.	Warning	This message is issued when configuration scripts resume their execution after a system restart.
1300	Periodic Transfer and Run Configuration Scripts Triggered.	Info	This message is issued when the automatic periodic configuration scripts transfer and execution is triggered.
1350	Execution started for specific configuration script (%1$s).	Info	This message is issued when a specific configuration script execution is about to be executed.
1400	Transfer and Run Configuration Script command succeeded for Specific configuration script.	Info	This message is issued when the service successfully completes a `TranferAndRunConfigurationScripts` command for the specific configuration script.

NumKey	Message	Severity	Description
1450	Execution started for generic configuration script (%1$s).	Info	This message is issued when a generic configuration script execution is about to be executed.
1500	Transfer and Run Configuration Script command succeeded for Generic configuration script.	Info	This message is issued when the service successfully completes a `ConfigScriptsTransferAndRun` command for the generic configuration script.
1600	Execution of specific script not requested.	Info	The current configuration specifies no specific script to execute.
1700	Execution of generic script not requested.	Info	The current configuration specifies no generic script to execute.
1800	Transfer and Run Specific Configuration Script Command failed. See previous messages for the cause.	Error	This message is issued when the service fails a `TransferAndRunConfigurationScripts` command for the specific configuration script.
1900	Transfer and Run Generic Configuration Script Command failed. See previous messages for the cause.	Error	This message is issued when the service fails a `TransferAndRunConfigurationScripts` command for the generic configuration script.
2000	Transfer and Run Specific Configuration Script Command completed with a warning. See previous messages for details.	Info	This message is issued when the result code of a `TransferAndRunConfigurationScripts` command is a warning.
2050	Transfer and Run Specific Configuration Script Command completed with errors. See previous messages for details.	Info	This message is issued when the result code of a `TransferAndRunConfigurationScripts` command is an error.
2100	Transfer and Run Generic Configuration Script Command completed with a warning. See previous messages for details.	Info	This message is issued when the result code of a `TransferAndRunConfigurationScripts` command is a warning.

NumKey	Message	Severity	Description
2150	Transfer and Run Generic Configuration Script Command completed with errors. See previous messages for details.	Info	This message is issued when the result code of a `TransferAndRunConfigurationScripts` command is an error.
2200	Syntax error in configuration script %1$s, line %2$d.	Error	This message is issued when the service fails to parse the transferred configuration script.
2300	In script %1$s, line %2$d: evaluation of expression %4$s in service %3$s failed, reason is: '%5$s'.	Error	This message is issued when the service fails to evaluate a parameter or run a command.
2400	In script %1$s, line %2$d: assignment of value %5$s to expression %4$s in service %3$s failed, reason is: '%6$s'.	Error	This message is issued when the service fails to assign a value to a parameter.
2500	In script %1$s, line %2$d: evaluation of expression %4$s in service %3$s issued the following warning: '%5$s'.	Warning	This message is issued when the service evaluates a parameter or runs a command and that a warning condition is detected.
2600	In script %1$s, line %2$d: assignment of value %5$s to expression %4$s in service %3$s issued the following warning: '%6$s'.	Warning	This message is issued when the service assigns a value to a parameter and that a warning condition is detected.
2700	Failed to schedule Periodic Transfer and Run Configuration Scripts.	Error	This message is issued when the automatic periodic configuration scripts transfer and run failed a scheduled attempt.
3400	Script %1$s has been stopped prematurely at line %2$d.	Warning	Happens when a unit is rebooted while a configuration script is running.
3425	Reboot initiated to apply hardware settings.	Warning	The `RebootIfNeeded` command triggered a reboot.

NumKey	Message	Severity	Description
3450	Scripts execution will start again automatically after the reboot process.	Info	The scripts execution has been suspended because of a unit reboot command, but will complete after the reboot process.
3475	Scripts execution will not start again automatically after the reboot process.	Error	A repetitive reboot protection has been applied. The scripts will not complete their execution after the reboot.
3500	Unknown %1$s service, or it is not started.	Error	This message is issued when the service fails to change the context to an unknown or not started service.
3700	Cannot add %1$s alias to entity %2$s, reason is: '%3$s'.	Error	This message is issued when the service fails to add an alias to an entity.
3800	Cannot remove %1$s alias : No such alias name.	Error	This message is issued when the service fails to remove an alias.
3900	Alias name is already used.	Error	This message is issued when the service fails to add an alias.
4000	No such entity name.	Error	This message is issued when the service fails to add an alias when the entity name is failed.
4100	%1$s is a reserved word.	Error	This message is issued when the service fails to add an alias when the alias name is a reserved word used by a module, a MIB parameter in current context or a Macro.
4200	The script %1$s does not contain valid commands, it contains only comments or empty lines.	Warning	This message is issued when a script contains only comments or empty lines.
4300	Retrying to transfer and execute automatic configuration scripts.	Info	This message is issued when the unit is retrying to transfer and run configuration scripts after a failed periodic transfer or a failed transfer on restart. The delay between each retries is 30 seconds.
4400	Reboot if needed command received.	Info	This message is issued when the `RebootIfNeeded` command is received, whether from a configuration script or from the user.
4550	The file %1$s is identical to the last transferred script. Skipping execution.	Info	This message is issued when a script execution is skipped because this newly transferred script is identical to the last executed script.

NumKey	Message	Severity	Description
4600	Export Script Configuration command succeeded.	Info	This message is issued when the service successfully completes a `ConfiguredScriptExport` command.
4700	Export Script Configuration command received.	Debug	This message is issued when the service receives the `ConfiguredScriptExport` command.
4900	Export Configuration Script Command failed.	Error	This message is issued when the service fails to complete a `ConfiguredScriptExport` command. A previous error message in the log explains why.
4950	Configuration script execution is paused for %1$d seconds.	Debug	This message is issued when a `Pause` command is executed.
4960	File %1$s is too large to be exported.	Warning	This message is issued when trying to export a file over 48 KB.
5100	Backup Configuration command succeeded.	Info	This message is issued when the service successfully completes a `BackupConfiguration` command.
5200	Backup Configuration command received.	Debug	This message is issued when the service receives the `BackupConfigImage` command.
5400	Backup Configuration Command failed.	Error	This message is issued when the service fails to complete a `BackupConfiguration` command. A previous error message in the log explains why.
5500	Unable to gather backup data.	Error	The service failed to collect all data to backup.
10100	Restore Configuration command succeeded. The unit will now reboot to apply the restored configuration.	Info	This message is issued when the service successfully completes a `RestoreConfiguration` command.
10200	Restore Configuration command received.	Debug	This message is issued when the service receives the `RestoreConfigImage` command.
10300	No restore data found for service %1$s, a factory default reset will be performed on it.	Warning	This message is issued when the service does not find the configuration data for a service that was reported to be present in the unit.

NumKey	Message	Severity	Description
10320	No restore data found for hardware %1$s, a factory default reset will be performed on it.	Warning	This message is issued when the service does not find the configuration data for a hardware that was reported to be present in the unit.
10340	Restore data with unsupported version for service %1$s, a factory default reset will be performed on it.	Warning	This message is issued when the service detects an unsupported version in the configuration data for a service present in the unit.
10360	Restore data with unsupported version for hardware %1$s, a factory default reset will be performed on it.	Warning	This message is issued when the service detects an unsupported version in the configuration data for a hardware present in the unit.
10500	Restore Configuration Command failed.	Error	This message is issued when the service fails to complete a `RestoreConfiguration` command. A previous error message in the log explains why.
10600	Invalid Restore data.	Error	Syntax of the restore file is invalid.
10700	Configuration backup file not applied since it was taken from a different platform.	Error	This message is issued when the service is requested to restore a configuration backup file taken on another platform, which is not allowed.
10800	Configuration file not restored since it was backed up from a more recent version.	Error	This message is issued when the version of the configuration backup file is more recent than the DGW version currently used in the unit, which is not allowed.
15100	Unable to transfer the file %1$s, reason: host or port unreachable.	Error	This message is issued when the service fails to transfer the requested file because the host or port cannot be reached.
15200	Unable to transfer the %1$s file because the connection failed.	Error	This message is issued when the service fails to transfer the requested file because the connection could not be established. If using HTTPS file transfers, this error may be due to mismatched security certificates.
15250	Unable to transfer the file %1$s, reason: rejected.	Error	This message is issued when the service fails to transfer the requested file because the host reports an HTTP error 402.
15300	Unable to transfer the file %1$s, reason: file not found.	Error	This message is issued when the service fails to transfer the requested file because the host reports it does not exist.

NumKey	Message	Severity	Description
15350	Unable to transfer the file %1$s, reason: file already exists.	Error	This message is issued when the service fails to transfer the requested file because the host reports it already exists.
15400	Unable to transfer the file %1$s, reason: access denied.	Error	This message is issued when the service fails to transfer the requested file because authentication failed.
15500	Unable to transfer the file %1$s, reason: timed out.	Error	This message is issued when the service fails to transfer the requested file, a timeout occurred.
15600	Unable to transfer the file %1$s, reason: internal error.	Error	This message is issued when the service fails to transfer the requested file, an unexpected situation happened.
15700	Unable to transfer the file %1$s, reason: transfer parameters are invalid.	Error	This message is issued when the service fails to transfer the requested file because of invalid configuration parameters.
15800	Unable to transfer the file %1$s, reason: couldn't resolve host name.	Error	This message is issued when the service fails to transfer the requested file because the host name cannot be resolved.
15900	Unable to transfer the file %1$s, reason: trying to access forbidden path.	Error	This message is issued when the service fails to transfer the requested file because the path is illegal (points to a forbidden location in the system's file system).
15950	Unable to transfer the file %1$s, reason: not enough space to store file.	Error	This message is issued when the service fails to transfer the requested file because it does not have enough space in the file system to store it.
16000	The transferred file size is too big. The maximal allowed size is %1$d bytes.	Error	This message is issued when the service transfers a file too big to be used.
16100	Unable to transfer the file %1$s, reason: untrusted certificate.	Error	This message is issued when the service fails to transfer the requested file because the remote certificate is not trusted by any of the certificates in the unit.
16200	Unable to transfer the file %1$s, reason: hostname does not match the certificate.	Error	This message is issued when the service fails to transfer the requested file, the hostname used to connect to the server does not match the hostname configured in the certificate.

NumKey	Message	Severity	Description
16300	OCSP verification of the certificate of %1$s with responder URL %2$s completed with status %3$s.	Info	This message is issued every time an OCSP request is completed (successfully or not).
16400	Certificate revocation status cannot be verified for HTTPS connection with remote host %1$s because the OCSP responder %2$s is unreachable.	Warning	This message is issued when certificate revocation status cannot be verified because the received peer certificate does not include the Authority Information Access extension providing the URI for the OCSP responder or the OCSP responder cannot be reached.
16500	Certificate revocation status cannot be verified for HTTPS connection with remote host %1$s because the response from OCSP responder %2$s could not be accepted.	Warning	This message is issued when the response obtained from the OCSP responder cannot be accepted. Possible causes include: failure to match the response with the request, response delay too large, response cannot be parsed and response fails verification.
16600	Certificate revocation status cannot be verified on the certificate of %1$s because the responder URL %2$s is not valid.	Warning	This message is issued when the responder URL does not follow the supported syntax.
16700	Unable to transfer the file %1$s, reason: max number of file reached.	Error	This message is issued when the service fails to transfer the requested file because it reach the maximum number of file limit.
16800	Unable to transfer the file %1$s, reason: write permission denied.	Error	This message is issued when the service fails to transfer the requested file because the user does not have write permission on the destination folder.
20100	Unable to encrypt the file.	Error	This message is issued when the service fails to encrypt a backup image.
20200	Unable to decrypt file.	Error	This message is issued when the service fails to decrypt either a script or a restore image.
20300	Missing privacy key for cryptographic operation.	Error	Encryption or decryption was requested, but no privacy secret key was specified.

NumKey	Message	Severity	Description
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.

NumKey	Message	Severity	Description
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Conf.

Message	Severity	Description
Evaluation of expression %2$s in service %1$s failed, reason is: '%3$s'.	Error	This message is issued when the service fails to evaluate a parameter or run a command.
Assignment of value %3$s to expression %2$s in service %1$s failed, reason is: '%4$s'.	Error	This message is issued when the service fails to assign a value to a parameter.
Evaluation of expression %2$s in service %1$s issued the following warning: '%3$s'.	Warning	This message is issued when the service evaluates a parameter or runs a command and that a warning condition is detected.
Assignment of value %3$s to expression %2$s in service %1$s issued the following warning: '%4$s'.	Warning	This message is issued when the service assigns a value to a parameter and a warning condition is detected.
Script successfully queued for execution.	Info	This message is issued when an asynchronous execution of script(s) are successfully submitted.
Cannot perform operation, service is busy.	Error	Happens when a synchronous operation is requested from the service while another operation is in progress.
Unknown %1$s service, or it is not started.	Error	This message is issued when the service fails to change the context to an unknown or not started service.
Unable to transfer the requested file, because filename is missing.	Error	This message is issued when the service fails to transfer the requested file because the filename is missing (empty filename).
Export Script Configuration request successfully queued for execution.	Info	This message is issued when an asynchronous script exportation is successfully submitted.
Backup request successfully queued for execution.	Info	This message is issued when an asynchronous backup request is successfully submitted.
Restore request successfully queued for execution.	Info	This message is issued when an asynchronous restore request is successfully submitted.
File transfer protocol can't be used, File Service is not available.	Error	This message is issued when the File Service is not available in application.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.

Message	Severity	Description
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.

Message	Severity	Description
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Call Routing (CRout)

The Call Routing (CRout) service transforms properties and routes calls between telephony interfaces and SIP endpoints.

Parameters

ConfigModifiedStatus (Status Parameter)

Type	Enum
Range	Yes(100) | No(200)
Script/CLI	CRout.ConfigModifiedStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.100

Indicates if the call routing configuration has been modified without being applied.

1. Yes: The configuration has been modified but has not been applied.
2. No: The call routing service uses the most recent call routing configuration.

Use the `ApplyConfig` command to apply the configuration.

InterfaceStatus (Table)

This table shows the SIP and ISDN interfaces currently available.

Index (Index) | Table: InterfaceStatus

Type	UInt32
Range	
Script/CLI	CRout.InterfaceStatus[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.200.1.100

Unique identifier of the row in the table.

Name (Status Parameter) | Table: InterfaceStatus

Type	Text
Range	
Script/CLI	CRout.InterfaceStatus[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.200.1.200

Name of the interface.
The name may have the following format:

- sip-'name': SIP interface with the name 'name'
- isdn-'name': ISDN interface with the name 'name'
- r2-'name': R2 interface with the name 'name'
- e&m-'name': E&M interface with the name 'name'
- fxs-'name': FXS interface with the name 'name'
- fxo-'name': FXO interface with the name 'name'

RouteStatus (Table)

This table shows the actual route used by the call routing service.

Index (Index) | Table: RouteStatus

Type	UInt32
Range	
Script/CLI	CRout.RouteStatus[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.300.1.100

Unique identifier of the row in the table.

Type (Status Parameter) | Table: RouteStatus

Type	Enum
Range	User(100) | Auto(200)
Script/CLI	CRout.RouteStatus[].Type
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.300.1.150

Displays the type of route based on their origin:

- user: The route is manually defined and entered by a user.
- auto: The route is automatically generated following the activation of the auto-routing feature (see the **autoRoutingEnable** parameter).

SourceCriteria (Status Parameter) | Table: RouteStatus

Type	Text
Range	
Script/CLI	CRout.RouteStatus[].SourceCriteria
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.300.1.200

The source compared against the criteria property to determine if the route can be used.
The source of the call can be:

- route-'name': the route 'name'
- sip-'name': the SIP interface 'name'
- isdn-'name': the ISDN interface 'name'
- r2-'name': the R2 interface 'name'

- e&m-'name': the E&M interface 'name'
- fxs-'name': the FXS interface 'name'
- fxo-'name': the FXO interface 'name'

PropertiesCriteria (Status Parameter) | Table: RouteStatus

Type	Enum
Range	None(100) | CalledE164(200) | CallingE164(300) | CalledName(400) | CallingName(500) | CalledTon(600) | CallingTon(700) | CalledNpi(800) | CallingNpi(900) | CalledHost(1000) | CallingHost(1100) | CallingPi(1200) | CallingSi(1300) | CallingItc(1400) | CalledUri(1500) | CallingUri(1600) | DateTime(1700) | CalledPhoneContext(1800) | CallingPhoneContext(1900) | CalledSipUsername(2000) | CallingSipUsername(2100) | CalledBearerChannel(2200) | CallingBearerChannel(2300) | CallingSipPrivacy(2400)
Script/CLI	CRout.RouteStatus[].PropertiesCriteria
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.300.1.300

The call property part of the criteria used to determine if the route can be applied or not. The other part of the criteria is the expression defined in the **RouteStatus.ExpressionCriteria** parameter.

The Call Property on which the route matching criteria is based on:

- CalledE164: the called party E.164 properties
- CallingE164: the calling party E.164 properties
- CalledName: the called party name properties
- CallingName: the calling party name properties
- CalledTon: the called party type of number properties
- CallingTon: the calling party type of number properties
- CalledNpi: the called party numbering plan indicator properties
- CallingNpi: the calling party numbering plan indicator properties
- CalledHost: the calling host properties
- CallingHost: the called host properties
- CallingPi: the calling party presentation indicator.
- CallingSi: the calling party screening indicator
- CallingItc: the calling party information transfer capability
- CalledUri: the called party SIP URI
- CallingUri: the calling party SIP URI
- DateTime: the date and/or time the call arrived at the call router

- CalledPhoneContext: the called party phone context
- CallingPhoneContext: the calling party phone context
- CalledSipUsername: the called SIP username
- CallingSipUsername: the calling SIP username
- CalledBearerChannel: the called bearer channel properties
- CallingBearerChannel: the calling bearer channel properties
- CallingSipPrivacy: the calling SIP privacy properties

See **RouteStatus.ExpressionCriteria**.

ExpressionCriteria (Status Parameter) | Table: RouteStatus

Type	Text
Range	
Script/CLI	CRout.RouteStatus[].ExpressionCriteria
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.300.1.400

The expression part of the criteria used to determine if the route can be applied or not. The other part of the criteria is the call property defined in the **RouteStatus.PropertiesCriteria** parameter.

The expression syntax is related to the selected criteria properties or can be a special tag:

- CalledE164: Regular expression
- CallingE164: Regular expression
- CalledName: Regular expression
- CallingName: Regular expression
- CalledTon: 'unknown', 'international', 'national', 'network', 'subscriber', or 'abbreviated'
- CallingTon: 'unknown', 'international', 'national', 'network', 'subscriber', or 'abbreviated'
- CalledNpi: 'unknown', 'isdn', 'data', 'telex', 'national', or 'private'
- CallingNpi: 'unknown', 'isdn', 'data', 'telex', 'national', or 'private'
- CalledHost: Regular expression. The format is 'Fqdn[:port]'. If the '[:port]' is not present, the table uses the well-known port of the signaling protocol.
- CallingHost: Regular expression. The format is 'Fqdn[:port]'. If the '[:port]' is not present, the table uses the well-known port of the signaling protocol.
- CallingPi: 'allowed', 'restricted', or 'interworking'
- CallingSi: 'not-screened', 'passed', 'failed', or 'network'
- CallingItc: 'speech', 'unrestricted', 'restricted', '3.1Khz', 'udi-ta', or 'video'
- CalledUri: Regular expression
- CallingUri: Regular expression

- DateTime: Day of week and time period and/or date and time period
- CalledPhoneContext: Regular expression
- CallingPhoneContext: Regular expression
- CalledSipUsername: Regular expression
- CallingSipUsername: Regular expression
- CalledBearerChannel: Regular expression
- CallingBearerChannel: Regular expression
- CallingSipPrivacy: 'disabled', 'none', or 'id'

Special tags:

- <undefined>: Matches if the property is not defined for the call.
- <default>: Always matches. Generally used to set a default route if the previous criteria did not match.

Accepted DateTime formats:

Date/Time Period format:

- 'DD.MM.YYYY/HH:MM:SS-DD.MM.YYYY/HH:MM:SS'
- 'DD.MM.YYYY/HH:MM:SS-HH:MM:SS'
- 'DD.MM.YYYY-DD.MM.YYYY'
- 'DD.MM.YYYY'
- 'HH:MM:SS-HH:MM:SS'

Week Day/Time period format:

- 'DDD'
- 'DDD,DDD...'
- 'DDD/HH:MM:SS-HH:MM:SS'
- 'DDD,DDD.../HH:MM:SS-HH:MM:SS'

where DDD must be one of: SUN, MON, TUE, WED, THU, FRI, or SAT.

Several of the previous formats can be concatenated to form one expression. They must be separated by |. Example: 25.12.2006 | SUN

Note: Whitespace at the end of a regular expression is ignored.

See **RouteStatus.PropertiesCriteria**.

Destination (Status Parameter) | Table: RouteStatus

Type	Text
Range	
Script/CLI	CRout.RouteStatus[].Destination
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.300.1.500

Destination to apply to the call if it matches the criteria.
The destination can be set to:

- route-'name': the route 'name'
- hunt-'name': the hunt 'name'
- sip-'name': the SIP interface 'name'
- isdn-'name': the ISDN interface 'name'
- r2-'name': the R2 interface 'name'
- e&m-'name': the E&M interface 'name'
- fxs-'name': the FXS interface 'name'
- fxo-'name': the FXO interface 'name'
- SipRedirect-'name': When the Route source is a SIP interface, incoming SIP Invites are replied with a 302 'Moved Temporarily' SIP response.

Mappings (Status Parameter) | Table: RouteStatus

Type	Text
Range	
Script/CLI	CRout.RouteStatus[].Mappings
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.300.1.600

Name of the transformations to apply to the call if the criteria matches. The transformations are executed before sending the call to the new destination.
More than one transformation can be specified. In this case, the transformations are separated with ',' and are executed in sequential order.

SignalingProperties (Status Parameter) | Table: RouteStatus

Type	Text
Range	
Script/CLI	CRout.RouteStatus[].SignalingProperties
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.300.1.700

Name of the signaling properties to apply to the call.

MappingTypeStatus (Table)

This table shows which Call Properties are involved in the transformations currently in use by the call routing service. The Transformation Rules (**MappingExpressionStatus**) table shows the detailed rules related to each transformation.

Index (Index) | Table: MappingTypeStatus

Type	UInt32
Range	
Script/CLI	CRout.MappingTypeStatus[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.400.1.100

Unique identifier of the row in the table.

Name (Status Parameter) | Table: MappingTypeStatus

Type	Text
Range	
Script/CLI	CRout.MappingTypeStatus[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.400.1.200

Name of the call property transformations defined by this row.
The name of the call property transformation is unique in the table.

See **RouteStatus.Mapping**

Criteria (Status Parameter) | Table: MappingTypeStatus

Type	Enum
Range	None(100) | E164(200) | CalledE164(300) | CallingE164(400) | Name(500) | CalledName(600) | CallingName(700) | Ton(800) | CalledTon(900) | CallingTon(1000) | Npi(1100) | CalledNpi(1200) | CallingNpi(1300) | Host(1400) | CalledHost(1500) | CallingHost(1600) | CallingPi(1700) | CallingSi(1800) | CallingItc(1900) | Uri(2000) | CalledUri(2100) | CallingUri(2200) | DateTime(2300) | PhoneContext(2400) | CalledPhoneContext(2500) | CallingPhoneContext(2600) | SipUsername(2700) | CalledSipUsername(2800) | CallingSipUsername(2900) | LastDivertingReason(3000) | LastDivertingE164(3100) | LastDivertingPartyNumberType(3110) | LastDivertingPublicTypeOfNumber(3120) | LastDivertingPrivateTypeOfNumber(3130) | LastDivertingNumberPresentation(3140) | OriginalDivertingReason(3200) | OriginalDivertingE164(3300) | OriginalDivertingPartyNumberType(3400) | OriginalDivertingPublicTypeOfNumber(3500) | OriginalDivertingPrivateTypeOfNumber(3600) | OriginalDivertingNumberPresentation(3700) | CalledBearerChannel(3800) | CallingBearerChannel(3900) | CallingSipPrivacy(4000)
Script/CLI	CRout.MappingTypeStatus[].Criteria
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.400.1.300

The call property part of the criteria used to determine if the transformation can be applied or not. The other part of the criteria is the expression defined in the **MappingExpressionStatus.Criteria** parameter.

The call properties can be:

- E164: called or calling E.164 properties
- CalledE164: called E.164 properties
- CallingE164: calling E.164 properties
- Name: called or calling name properties.
- CalledName: called name properties
- CallingName: calling name properties
- Ton: called or calling type of number properties
- CalledTon: called type of number properties
- CallingTon: calling type of number properties
- Npi: called or calling numbering plan indicator properties
- CalledNpi: called numbering plan indicator properties

- CallingNpi: calling numbering plan indicator properties
- Host: calling or called host properties
- CalledHost: calling host properties
- CallingHost: called host properties
- CallingPi: calling presentation indicator
- CallingSi: calling screening indicator
- CallingItc: calling information transfer capability
- Uri: calling or called SIP URI properties
- CalledUri: called SIP URI properties
- CallingUri: calling SIP URI properties
- DateTime: route calls based on the date and/or time the call arrived at the call router
- PhoneContext: called or calling phone context properties
- CalledPhoneContext: called phone context properties
- CallingPhoneContext: calling phone context properties
- SipUsername: called or calling SIP username properties
- CalledSipUsername: called SIP username properties
- CallingSipUsername: calling SIP username properties
- LastDivertingReason: last diverting reason properties
- LastDivertingE164: last diverting E.164 properties
- LastDivertingPartyNumberType: party number type of the last diverting number properties
- LastDivertingPublicTypeOfNumber: public type of number of the last diverting number properties
- LastDivertingPrivateTypeOfNumber: private type of number of the last diverting number properties
- LastDivertingNumberPresentation: presentation of the last diverting number properties
- OriginalDivertingReason: original diverting reason properties
- OriginalDivertingE164: original diverting E.164 properties
- OriginalDivertingPartyNumberType: party number type of the original diverting number properties
- OriginalDivertingPublicTypeOfNumber: public type of number of the original diverting number properties
- OriginalDivertingPrivateTypeOfNumber: private type of number of the original diverting number properties
- OriginalDivertingNumberPresentation: presentation of the original diverting number properties
- CalledBearerChannel: called bearer channel properties
- CallingBearerChannel: calling bearer channel properties

- CallingSipPrivacy: calling SIP privacy properties

See **MappingExpressionStatus.Criteria**.

Transformation (Status Parameter) | Table: MappingTypeStatus

Type	Enum
Range	None(100) | E164(200) | CalledE164(300) | CallingE164(400) | Name(500) | CalledName(600) | CallingName(700) | Ton(800) | CalledTon(900) | CallingTon(1000) | Npi(1100) | CalledNpi(1200) | CallingNpi(1300) | Host(1400) | CalledHost(1500) | CallingHost(1600) | CallingPi(1700) | CallingSi(1800) | CallingItc(1900) | Uri(2000) | CalledUri(2100) | CallingUri(2200) | PhoneContext(2300) | CalledPhoneContext(2400) | CallingPhoneContext(2500) | SipUsername(2600) | CalledSipUsername(2700) | CallingSipUsername(2800) | LastDivertingReason(2900) | LastDivertingE164(3000) | LastDivertingPartyNumberType(3010) | LastDivertingPublicTypeOfNumber(3020) | LastDivertingPrivateTypeOfNumber(3030) | LastDivertingNumberPresentation(3040) | OriginalDivertingReason(3100) | OriginalDivertingE164(3200) | OriginalDivertingPartyNumberType(3300) | OriginalDivertingPublicTypeOfNumber(3400) | OriginalDivertingPrivateTypeOfNumber(3500) | OriginalDivertingNumberPresentation(3600) | CalledBearerChannel(3700) | CallingBearerChannel(3800) | Debug(60000)
Script/CLI	CRout.MappingTypeStatus[].Transformation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.400.1.400

Call properties to transform. The transformation is defined in the **MappingExpressionStatus.Transformation** parameter.

The call properties can be:

- E164: called or calling E.164 properties
- CalledE164: called E.164 properties
- CallingE164: calling E.164 properties
- Name: called or calling name properties
- CalledName: called name properties
- CallingName: calling name properties
- Ton: called or calling type of number properties
- CalledTon: called type of number properties
- CallingTon: calling type of number properties
- Npi: called or calling numbering plan indicator properties
- CalledNpi: called numbering plan indicator properties

- CallingNpi: calling numbering plan indicator properties
- Host: calling or called host properties
- CalledHost: calling host properties
- CallingHost: called host properties
- CallingPi: calling presentation indicator
- CallingSi: calling screening indicator
- CallingItc: calling information transfer capability
- Uri: calling or called SIP URI properties
- CalledUri: called SIP URI properties
- CallingUri: calling SIP URI properties
- PhoneContext: calling or called phone context properties
- CalledPhoneContext: called phone context properties
- CallingPhoneContext: calling phone context properties
- SipUsername: calling or called SIP username properties
- CalledSipUsername: called phone SIP username properties
- CallingSipUsername: calling phone SIP username properties
- LastDivertingReason: last diverting reason properties
- LastDivertingE164: last diverting E.164 properties
- LastDivertingPartyNumberType: party number type of the last diverting number properties
- LastDivertingPublicTypeOfNumber: public type of number of the last diverting number properties
- LastDivertingPrivateTypeOfNumber: private type of number of the last diverting number properties
- LastDivertingNumberPresentation: presentation of the last diverting number properties
- OriginalDivertingReason: original diverting reason properties
- OriginalDivertingE164: original diverting E.164 properties
- OriginalDivertingPartyNumberType: party number type of the original diverting number properties
- OriginalDivertingPublicTypeOfNumber: public type of number of the original diverting number properties
- OriginalDivertingPrivateTypeOfNumber: private type of number of the original diverting number properties
- OriginalDivertingNumberPresentation: presentation of the original diverting number properties
- CalledBearerChannel: called bearer channel properties
- CallingBearerChannel: calling bearer channel properties
- Debug: reserved for debug configuration

See **MappingExpressionStatus.Transformation**.

MappingExpressionStatus (Table)

This table shows the definition of the actual transformations used by the call routing services.

Index (Index) | Table: MappingExpressionStatus

Type	UInt32
Range	
Script/CLI	CRout.MappingExpressionStatus[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.500.1.100

Unique identifier of the row in the table.

Name (Status Parameter) | Table: MappingExpressionStatus

Type	Text
Range	
Script/CLI	CRout.MappingExpressionStatus[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.500.1.200

Name of the transformation defined by this row.
More than one row can have the same name. In this case, the first row matching the call will be used. The rows are used in ascending order.

See **RouteStatus.Mapping**.

Criteria (Status Parameter) | Table: MappingExpressionStatus

Type	Text
Range	
Script/CLI	CRout.MappingExpressionStatus[].Criteria
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.500.1.300

The expression part of the criteria used to determine if the transformation can be applied or not. The other part of the criteria is the call property defined in the **MappingTypeStatus.Criteria** parameter.

The expression syntax is related to the selected Criteria call property or can be a special tag:

- E164: regular expression
- CalledE164: regular expression
- CallingE164: regular expression
- Name: regular expression
- CalledName: regular expression
- CallingName: regular expression
- Ton: 'unknown', 'international', 'national', 'network', 'subscriber', or 'abbreviated'
- CalledTon: 'unknown', 'international', 'national', 'network', 'subscriber', or 'abbreviated'
- CallingTon: 'unknown', 'international', 'national', 'network', 'subscriber', or 'abbreviated'
- Npi: 'unknown', 'isdn', 'data', 'telex', 'national', or 'private'
- CalledNpi: 'unknown', 'isdn', 'data', 'telex', 'national', or 'private'
- CallingNpi: 'unknown', 'isdn', 'data', 'telex', 'national', or 'private'
- Host: Regular expression. The call property format is 'Fqdn[:port]'. If the '[:port]' is not present, the table uses the well-known port of the signaling protocol.
- CalledHost: Regular expression. The call property format is 'Fqdn[:port]'. If the '[:port]' is not present, the table uses the well-known port of the signaling protocol.
- CallingHost: Regular expression. The call property format is 'Fqdn[:port]'. If the '[:port]' is not present, the table uses the well-known port of the signaling protocol.
- CallingPi: 'allowed', 'restricted', or 'interworking'
- CallingSi: 'not-screened', 'passed', 'failed', or 'network'
- CallingItc: 'speech', 'unrestricted', 'restricted', '3.1Khz', 'udi-ta', or 'video'
- Uri: regular expression
- CalledUri: regular expression
- CallingUri: regular expression
- DateTime: day of week and time period and/or date and time period
- PhoneContext: regular expression
- CalledPhoneContext: regular expression
- CallingPhoneContext: regular expression
- SipUsername: regular expression
- CalledSipUsername: regular expression
- CallingSipUsername: regular expression
- LastDivertingReason: 'cfu', 'cfb', 'cfnr', or 'unknown'
- LastDivertingE164: Regular expression
- LastDivertingPartyNumberType: 'unknown', 'public', or 'private'
- LastDivertingPublicTypeOfNumber: 'unknown', 'international', 'national', 'network-specific', 'local', or 'abbreviated'

- LastDivertingPrivateTypeOfNumber: 'unknown', 'leg2-reg', 'leg1-reg', 'pisn-specific', 'subscriber', or 'abbreviated'
- LastDivertingNumberPresentation: 'allowed', 'restricted', 'interworking', or 'restricted-address'
- OriginalDivertingReason: 'cfu', 'cfb', 'cfnr', or 'unknown'
- OriginalDivertingE164: Regular expression
- OriginalDivertingPartyNumberType: 'unknown', 'public', or 'private'
- OriginalDivertingPublicTypeOfNumber: 'unknown', 'international', 'national', 'network-specific', 'local', or 'abbreviated'
- OriginalDivertingPrivateTypeOfNumber: 'unknown', 'leg2-reg', 'leg1-reg', 'pisn-specific', 'subscriber', or 'abbreviated'
- OriginalDivertingNumberPresentation: 'allowed', 'restricted', 'interworking', or 'restricted-address'
- CalledBearerChannel: regular expression
- CallingBearerChannel: regular expression
- CallingSipPrivacy: 'disabled', 'none', or 'id'

Special tags:

- <undefined>: Matches if the property is not defined for the call.
- <default>: Always matches. Generally used to set a default transformation if the previous criteria did not match.

Accepted **DateTime** formats:

Date/Time Period format:

- 'DD.MM.YYYY/HH:MM:SS-DD.MM.YYYY/HH:MM:SS'
- 'DD.MM.YYYY/HH:MM:SS-HH:MM:SS'
- 'DD.MM.YYYY-DD.MM.YYYY'
- 'DD.MM.YYYY'
- 'HH:MM:SS-HH:MM:SS'

Week Day/Time Period format:

- 'DDD'
- 'DDD,DDD...'
- 'DDD/HH:MM:SS-HH:MM:SS'
- 'DDD,DDD.../HH:MM:SS-HH:MM:SS'

where DDD must be one of: SUN, MON, TUE, WED, THU, FRI, or SAT

Several of the previous formats can be concatenated to form one expression. They must be separated by |. Example: 25.12.2006 | SUN

Note: Whitespace at the end of a regular expression is ignored.

See **MappingTypeStatus.Criteria**.

Transformation (Status Parameter) | Table: MappingExpressionStatus

Type	Text
Range	
Script/CLI	CRout.MappingExpressionStatus[].Transformation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.500.1.400

Transformation to apply to the call properties. It is applied on the call properties defined in the **MappingTypeStatus.Transformation** parameter.
The transformation syntax is related to the selected properties to transform:

- Ton: 'unknown', 'international', 'national', 'network', 'subscriber', or 'abbreviated'
- CalledTon: 'unknown', 'international', 'national', 'network', 'subscriber', or 'abbreviated'
- CallingTon: 'unknown', 'international', 'national', 'network', 'subscriber', or 'abbreviated'
- Npi: 'unknown', 'isdn', 'data', 'telex', 'national', or 'private'
- CalledNpi: 'unknown', 'isdn', 'data', 'telex', 'national', or 'private'
- CallingNpi: 'unknown', 'isdn', 'data', 'telex', 'national', or 'private'
- CallingPi: 'allowed', 'restricted', or 'interworking'
- CallingSi: 'not-screened', 'passed', 'failed', or 'network'
- CallingItc: 'speech', 'unrestricted', 'restricted', '3.1Khz', 'udi-ta', or 'video'
- LastDivertingReason: 'cfu', 'cfb', 'cfnr', or 'unknown'
- LastDivertingPartyNumberType: 'unknown', 'public', or 'private'
- LastDivertingPublicTypeOfNumber: 'unknown', 'international', 'national', 'network-specific', 'local', or 'abbreviated'
- LastDivertingPrivateTypeOfNumber: 'unknown', 'leg2-reg', 'leg1-reg', 'pisn-specific', 'subscriber', or 'abbreviated'
- LastDivertingNumberPresentation: 'allowed', 'restricted', 'interworking', or 'restricted-address'
- OriginalDivertingReason: 'cfu', 'cfb', 'cfnr', or 'unknown'
- OriginalDivertingPartyNumberType: 'unknown', 'public', or 'private'
- OriginalDivertingPublicTypeOfNumber: 'unknown', 'international', 'national', 'network-specific', 'local', or 'abbreviated'
- OriginalDivertingPrivateTypeOfNumber: 'unknown', 'leg2-reg', 'leg1-reg', 'pisn-specific', 'subscriber', or 'abbreviated'
- OriginalDivertingNumberPresentation: 'allowed', 'restricted', 'interworking', or 'restricted-address'
- All others: string where '\0' to '\9' is replaced by the corresponding group in the regular expression set in the criteria rule (see **MappingStatus.ExpressionCriteria**). The value can be

set to the '<local_ip_port>' macro to replace the properties by the local IP address and port of the listening socket of the SIP gateway used to send the INVITE.

See **MappingTypeStatus.Transformation**

SubMappings (Status Parameter) | Table: MappingExpressionStatus

Type	Text
Range	
Script/CLI	CRout.MappingExpressionStatus[].SubMappings
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.500.1.500

Name of the next transformation to be executed.
More than one transformation can be specified. In this case, the transformations are separated with ',' and are executed in an sequential order.

HuntStatus (Table)

This table shows the actual hunt used by the call routing services.

Index (Index) | Table: HuntStatus

Type	UInt32
Range	
Script/CLI	CRout.HuntStatus[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.600.1.100

Unique identifier of the row in the table.

Name (Status Parameter) | Table: HuntStatus

Type	Text
Range	
Script/CLI	CRout.HuntStatus[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.600.1.200

Name of the hunt defined by this row. It must be unique in the table.

Destinations (Status Parameter) | Table: HuntStatus

Type	Text
Range	
Script/CLI	CRout.HuntStatus[].Destinations
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.600.1.300

List of hunt destinations separated by commas.
The call destination can be:

- route-'name': the route 'name'
- hunt-'name': the hunt 'name'
- sip-'name': the SIP interface 'name'
- isdn-'name': the ISDN interface 'name'
- r2-'name': the R2 interface 'name'
- e&m-'name': the E&M interface 'name'
- fxs-'name': the FXS interface 'name'
- fxo-'name': the FXO interface 'name'
- SipRedirect-'name': When the Route source is a SIP interface, incoming SIP Invites are replied with a 302 'Moved Temporarily' SIP response.

Note: Only FXS interfaces are supported if 'Simultaneous' is selected for the **Selection Algorithm** parameter.

Example: 'isdn-Slot2/Bri1, route-something'

SelectionAlgorithm (Status Parameter) | Table: HuntStatus

Type	Enum
Range	Sequential(100) | Cyclic(200) | Simultaneous(300)
Script/CLI	CRout.HuntStatus[].SelectionAlgorithm
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.600.1.400

Algorithm used to select the destination order.
The destination order can be:

- Sequential: The hunt tries the destination in the same order as listed. The first destination hunted is the first listed.

- Cyclic: The hunt starts from the destination that follows the destination used for the last hunt. Subsequent calls try another first destination in a round-robin method.
- Simultaneous: The hunt tries every available destination at the same time. The first destination to pick up has the call. Other destinations stop ringing. This method can only have FXS endpoints as destinations.

Example of cyclic selection: If the destination is set to 'x,y,z', the destination the hunt tries is in the following order:

1. x,y,z
2. y,z,x
3. z,x,y
4. x,y,z

Timeout (Status Parameter) | Table: HuntStatus

Type	UInt32
Range	
Script/CLI	CRout.HuntStatus[].Timeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.600.1.500

Maximal time allowed to the destination to handle the call.
A value of '0' disables the timeout.

This value is expressed in seconds (s).

Note: Not applicable if 'Simultaneous' was selected for the **Selection Algorithm** parameter.

Causes (Status Parameter) | Table: HuntStatus

Type	Text
Range	
Script/CLI	CRout.HuntStatus[].Causes
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.600.1.600

Lists call rejection causes to continue the hunt. The causes are separated by commas. The available hunt causes are:
Normal event:

- 1: Unassigned (unallocated) number
- 2: No route to specified transit network
- 3: No route to destination

- 6: Channel unacceptable.
- 7: Call awarded and being delivered in an established channel
- 17: User busy
- 18: No user responding
- 19: User alerting, no answer
- 21: Call rejected
- 22: Number changed
- 26: Non-selected user clearing
- 27: Destination out of order
- 28: Invalid number format (incomplete number)
- 29: Facility rejected
- 30: Response to STATUS ENQUIRY
- 31: Normal, unspecified

Unavailable resource:

- 34: No circuit/channel available
- 38: Network out of order
- 41: Temporary failure
- 42: Switching equipment congestion
- 43: Access information discarded
- 44: Requested circuit/channel not available
- 47: Resource unavailable, unspecified

Service or option not available:

- 57: Bearer capability not authorised
- 58: Bearer capability not presently available
- 63: Service or option not available, unspecified

Service or option not implemented:

- 65: Bearer capability not implemented
- 66: Channel type not implemented
- 69: Requested facility not implemented
- 70: Only restricted digital information bearer capability is available
- 79: Service or option not implemented, unspecified

Invalid message:

- 81: Invalid call reference value
- 82: Identified channel does not exist

- 83: A suspended call exists, but this call identity does not exist
- 84: Call identity in use
- 85: No call suspended
- 86: Call having the requested call identity has been cleared
- 88: Incompatible destination
- 91: Invalid transit network selection
- 95: Invalid message, unspecified

Protocol error:

- 96: Mandatory information element missing
- 97: Message type non-existent or not implemented
- 98: Message not compatible with call state or message type non-existent or not implemented
- 99: Information element non-existent or not implemented
- 100: Invalid information element contents
- 101: Message not compatible with call state
- 102: Recovery on time expiry
- 111: Protocol error, unspecified

Interworking:

- 127: Interworking, unspecified.

Note: Not applicable if 'Simultaneous' was selected for the **Selection Algorithm** parameter.

SignalingPropertiesStatus (Table)

This table shows the actual signaling properties used by the call routing services.

Index (Index) | Table: SignalingPropertiesStatus

Type	UInt32
Range	
Script/CLI	CRout.SignalingPropertiesStatus[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.700.1.100

Unique identifier of the row in the table.

Name (Status Parameter) | Table: SignalingPropertiesStatus

Type	Text
Range	
Script/CLI	CRout.SignalingPropertiesStatus[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.700.1.200

Name of the Signaling properties defined by this row. It must be unique in the table.

EarlyConnect (Status Parameter) | Table: SignalingPropertiesStatus

Type	EnableDisable
Range	
Script/CLI	CRout.SignalingPropertiesStatus[].EarlyConnect
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.700.1.300

Enable/Disable the early connect feature.
When early connect is enabled, the SIP call is connected by sending a 200 OK message instead of a 183 Session Progress message with early media.

EarlyDisconnect (Status Parameter) | Table: SignalingPropertiesStatus

Type	EnableDisable
Range	
Script/CLI	CRout.SignalingPropertiesStatus[].EarlyDisconnect
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.700.1.400

Enable/Disable the early disconnect feature.
When early disconnect is enabled, the SIP BYE message is sent upon ISDN 'Disconnect' signal reception.

When early disconnect is disabled, the SIP BYE message is sent upon ISDN 'Call release' signal reception.

If early disconnect is enabled but no ISDN 'Disconnect' message is received, the SIP BYE message will be sent upon receiving an ISDN 'Call release' as if the early disconnect was disabled.

DestinationHost (Status Parameter) | Table: SignalingPropertiesStatus

Type	Text
Range	
Script/CLI	CRout.SignalingPropertiesStatus[].DestinationHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.700.1.500

SIP message destination.
The value can be set to the '<local_ip_port>' macro to replace the properties by the local IP address and port of the listening socket of the SIP gateway used to send the INVITE.

Allow180Sdp (Status Parameter) | Table: SignalingPropertiesStatus

Type	EnableDisable
Range	
Script/CLI	CRout.SignalingPropertiesStatus[].Allow180Sdp
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.700.1.600

Enable/Disable the 180 with SDP allowed.
When disabled, a SIP 183 with SDP is sent instead of a 180 with SDP.

This does not affect the 180 without SDP.

Allow183NoSdp (Status Parameter) | Table: SignalingPropertiesStatus

Type	EnableDisable
Range	
Script/CLI	CRout.SignalingPropertiesStatus[].Allow183NoSdp
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.700.1.700

Enable/Disable the 183 without SDP allowed.
When disabled, a 183 without SDP is not sent.

This does not affect the 183 with SDP.

Privacy (Status Parameter) | Table: SignalingPropertiesStatus

Type	Enum
Range	Disable(100) | None(200) | AssertedId(250) | PreferredId(300) | Rpid(400)
Script/CLI	CRout.SignalingPropertiesStatus[].Privacy
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.700.1.800

Indicates the privacy level of the call.

- Disable: No privacy is used.
- None: Use P-Asserted Identity and privacy "none".
- AssertedId: Use P-Asserted Identity and privacy "id" when restricted.
- PreferredId: Use P-Preferred Identity and privacy "id" when restricted.
- Rpid: Use Remote-Party-ID header.

CallPropertiesTranslation (Status Parameter) | Table: SignalingPropertiesStatus

Type	Text
Range	
Script/CLI	CRout.SignalingPropertiesStatus[].CallPropertiesTranslation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.700.1.900

Name of the call property translation to apply to the call.
The translation modifies the call properties before the call is sent to its destination.

More than one translation can be specified. In that case, the translations are separated with ',' and are executed in sequential order.

SipHeadersTranslation (Status Parameter) | Table: SignalingPropertiesStatus

Type	Text
Range	
Script/CLI	CRout.SignalingPropertiesStatus[].SipHeadersTranslation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.700.1.1000

Name of the SIP header translation to apply to the call.
The translation modifies the SIP headers before the call is sent to its destination.

More than one translation can be specified. In this case, the translations are separated with ',' and are executed in sequential order.

SipHeadersTranslationStatus (Table)

This table shows the configured SIP header translations to be used by the call routing service. The configuration is not used until the `ApplyConfig` command is executed.

Index (Index) | Table: SipHeadersTranslationStatus

Type	UInt32
Range	
Script/CLI	CRout.SipHeadersTranslationStatus[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.800.1.100

Unique identifier of the row in the table.

Name (Status Parameter) | Table: SipHeadersTranslationStatus

Type	Text
Range	Size(0..64)
Script/CLI	CRout.SipHeadersTranslationStatus[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.800.1.200

Name of the SIP header translation defined in this row.

SipHeader (Status Parameter) | Table: SipHeadersTranslationStatus

Type	Enum
Range	FromHeaderHostPart(100) | FromHeaderUserPart(200) | IdentityHeaderHostPart(300) | IdentityHeaderUserPart(400) | IdentityHeaderPhoneNumber(500) | IdentityHeaderFriendlyName(550) | RequestLineHostPart(600) | RequestLineUserPart(700) | ToHeaderHostPart(800) | ToHeaderUserPart(900)
Script/CLI	CRout.SipHeadersTranslationStatus[].SipHeader
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.800.1.300

Sets which SIP header is modified by this translation.
The SIP headers can be:

- FromHeaderHostPart: host part of the From header URI
- FromHeaderUserPart: user part of the From header URI
- IdentityHeaderHostPart: host part of the Identity header URI
- IdentityHeaderUserPart: user part of the Identity header URI
- IdentityHeaderPhoneNumber: phone number in the Identity header tel URI
- IdentityHeaderFriendlyName: friendly name in the Identity header URI
- RequestLineHostPart: host part of the Request line URI
- RequestLineUserPart: user part of the Request line URI
- ToHeaderHostPart: host part of the To header URI
- ToHeaderUserPart: user part of the To header URI

BuiltFrom (Status Parameter) | Table: SipHeadersTranslationStatus

Type	Enum
Range	CalledE164(100) | DestinationHost(200) | Domain(300) | FixValue(400) | HostName(500) | LocalIp(600) | CallingBearerChannel(700) | SipEndpointUsername(800) | CallingName(900) | CallingE164(1000)
Script/CLI	CRout.SipHeadersTranslationStatus[].BuiltFrom
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.800.1.400

Sets what information is used to build the selected SIP header.
The information can be retrieved from:

- CalledE164: Use the called party E.164 property.
- DestinationHost: Use the destination host configured in the signaling properties of which this translation is part of.
- Domain: Use the domain name configured in the unit.
- FixValue: Use a fixed value (see **SipHeadersTranslation.FixValue**).
- HostName: Use the host name configured on the unit.
- LocalIp: Use the local IP address.
- CallingBearerChannel: Use the calling bearer channel.
- SipEndpointUsername: Use the SIP username associated with the endpoint.
- CallingName: Use the calling party name property.
- CallingE164: Use the calling party E.164 property.

FixValue (Status Parameter) | Table: SipHeadersTranslationStatus

Type	Text
Range	Size(0..255)
Script/CLI	CRout.SipHeadersTranslationStatus[].FixValue
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.800.1.500

Fixed value to be inserted in the SIP header when the **SipHeadersTranslation.BuiltFrom** parameter is set to 'FixValue'.

CallPropertiesTranslationStatus (Table)

This table shows the configured call property translations to be used by the call routing service. The configuration is not used until the `ApplyConfig` command is executed.

Index (Index) | Table: CallPropertiesTranslationStatus

Type	UInt32
Range	
Script/CLI	CRout.CallPropertiesTranslationStatus[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.900.1.100

Unique identifier of the row in the table.

Name (Status Parameter) | Table: CallPropertiesTranslationStatus

Type	Text
Range	Size(0..64)
Script/CLI	CRout.CallPropertiesTranslationStatus[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.900.1.200

Name of the call property translation defined by this row.

CallProperty (Status Parameter) | Table: CallPropertiesTranslationStatus

Type	Enum
Range	CalledE164(100) | CallingE164(200) | CalledName(300) | CallingName(400) | CalledUri(500) | CallingUri(600) | CalledBearerChannel(700)
Script/CLI	CRout.CallPropertiesTranslationStatus[].CallProperty
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.900.1.300

Sets which call property is modified by this translation.
The call properties can be:

- CalledE164: called party E.164 property
- CallingE164: calling party E.164 property
- CalledName: called party name property
- CallingName: calling party name property
- CalledUri: called URI name property
- CallingUri: calling URI name property
- CalledBearerChannel: called bearer channel property

BuiltFrom (Status Parameter) | Table: CallPropertiesTranslationStatus

Type	Enum
Range	Domain(100) | FixValue(200) | FromHeaderUri(300) | FromHeaderFriendlyName(400) | FromHeaderUserPart(500) | IdentityHeaderUri(600) | IdentityHeaderUserPart(700) | IdentityHeaderPhoneNumber(800) | IdentityHeaderFriendlyName(850) | LocalIp(900) | RequestLineUri(1000) | RequestLineUserPart(1100) | ToHeaderUri(1200) | ToHeaderFriendlyName(1300) | ToHeaderUserPart(1400)
Script/CLI	CRout.CallPropertiesTranslationStatus[].BuiltFrom
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.900.1.400

Sets what information is used to build the selected call property.
The information can be retrieved from:

- Domain: Use the domain name configured in the unit.
- FixValue: Use a fixed value (see **CallPropertiesTranslation.FixValue**).
- FromHeaderUri: Use the From header URI.

- FromHeaderFriendlyName: Use the friendly name part of the From header.
- FromHeaderUserPart: Use the user part of the From header URI.
- IdentityHeaderUri: Use the Identity header URI.
- IdentityHeaderUserPart: Use the user part of the Identity header URI.
- IdentityHeaderPhoneNumber: Use the phone number in the Identity header tel URL.
- IdentityHeaderFriendlyName: Use the friendly name in the Identity header URI.
- LocalIp: Use the local IP address.
- RequestLineUri: Use the Request line URI.
- RequestLineUserPart: Use the user part of the Request line URI.
- ToHeaderUri: Use the To header URI.
- ToHeaderFriendlyName: Use the friendly name part of the To header.
- ToHeaderUserPart: Use the user part of the To header URI.

FixValue (Status Parameter) | Table: CallPropertiesTranslationStatus

Type	Text
Range	Size(0..255)
Script/CLI	CRout.CallPropertiesTranslationStatus[].FixValue
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.900.1.500

Fixed value to be inserted in the call property when the CallPropertiesTranslation.BuiltFrom parameter is set to 'FixValue'.

SipRedirectStatus (Table)

This table shows the actual Redirect entry used by the call routing service.

Index (Index) | Table: SipRedirectStatus

Type	UInt32
Range	
Script/CLI	CRout.SipRedirectStatus[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.1000.1.100

Unique identifier of the row in the table.

Name (Status Parameter) | Table: SipRedirectStatus

Type	Text
Range	Size(0..64)
Script/CLI	CRout.SipRedirectStatus[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.1000.1.200

Name of the SIP Redirect defined by this row.
The name must be unique in the table.

DestinationHost (Status Parameter) | Table: SipRedirectStatus

Type	Text
Range	
Script/CLI	CRout.SipRedirectStatus[].DestinationHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.100.1000.1.300

Host address inserted in the Moved Temporarily response.

AutoRoutingEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	CRout.AutoRoutingEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.200

Enable/Disable the automatic insertion of default routes for selected endpoints.
When enabled, routes are automatically added to the Route Table in order to connect the endpoints marked as eligible for auto-routing and the designated SIP gateway (see the **Autoroutable** and the **AutoroutingGateway** parameters). These automatic routes are displayed in the **Routes** Table of the Status page but do not show up in the configuration.

Route (Table: user-defined, 150 lines max.)

This table shows the configured route to be used by the call routing service. The configuration is not used until the `ApplyConfig` command is executed.

Note: Too many entries may introduce delay in the call establishment, especially on low-processing platforms.

Index (Index) | Table: Route

Type	UInt32
Range	
Script/CLI	CRout.Route[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.300.1.100

Unique identifier of the row in the table.

SourceCriteria (Config Parameter) | Table: Route

Type	Text
Range	Size(0..2048)
Default	
Script/CLI	CRout.Route[].SourceCriteria
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.300.1.200

One or many sources the service compares and matches the call to, in order to apply the route. The source the call comes from can be:

- route-'name': the route 'name'
- sip-'name': the SIP interface 'name'
- isdn-'name': the ISDN interface 'name'
- r2-'name': the R2 interface 'name'
- e&m-'name': Tthe E&M interface 'name'
- fxs-'name': the FXS interface 'name'
- fxo-'name': the FXO interface 'name'

Multiple sources must be separated by commas.

PropertiesCriteria (Config Parameter) | Table: Route

Type	Enum
Range	None(100) | CalledE164(200) | CallingE164(300) | CalledName(400) | CallingName(500) | CalledTon(600) | CallingTon(700) | CalledNpi(800) | CallingNpi(900) | CalledHost(1000) | CallingHost(1100) | CallingPi(1200) | CallingSi(1300) | CallingItc(1400) | CalledUri(1500) | CallingUri(1600) | DateTime(1700) | CalledPhoneContext(1800) | CallingPhoneContext(1900) | CalledSipUsername(2000) | CallingSipUsername(2100) | CalledBearerChannel(2200) | CallingBearerChannel(2300) | CallingSipPrivacy(2400)
Default	None
Script/CLI	CRout.Route[].PropertiesCriteria
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.300.1.300

The call property part of the criteria used to determine if the route can be applied or not. The other part of the criteria is the expression defined in the **RouteStatus.ExpressionCriteria** parameter.

Calls can be routed based on the following Call Properties:

- CalledE164: the called party E.164 properties
- CallingE164: the calling party E.164 properties
- CalledName: the called party name properties
- CallingName: the calling party name properties
- CalledTon: the called party type of number properties
- CallingTon: the calling party type of number properties
- CalledNpi: the called party numbering plan indicator properties
- CallingNpi: the calling party numbering plan indicator properties
- CalledHost: the calling host properties
- CallingHost: the called host properties
- CallingPi: the calling party presentation indicator
- CallingSi: the calling party screening indicator
- CallingItc: the calling party information transfer capability
- CalledUri: the called party SIP URI
- CallingUri: the calling party SIP URI
- DateTime: the date and/or time the call arrived at the call router
- CalledPhoneContext: the called party phone context properties
- CallingPhoneContext: the calling party phone context properties
- CalledSipUsername: the called party SIP username properties

- CallingSipUsername: the calling party SIP username properties
- CalledBeareChannel: the called bearer channel properties
- CallingBeareChannel: the calling bearer channel properties
- CallingSipPrivacy: the calling SIP privacy properties

See **RouteStatus.ExpressionCriteria**.

ExpressionCriteria (Config Parameter) | Table: Route

Type	Text
Range	Size(0..256)
Default	
Script/CLI	CRout.Route[].ExpressionCriteria
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.300.1.400

The call property part of the criteria rule used to determine if the route can be applied or not. The other part of the criteria is the expression defined in the **RouteStatus.PropertiesCriteria** parameter.

The criteria rule syntax is related to the selected criteria properties or can be a special tag:

- CalledE164: regular expression
- CallingE164: regular expression
- CalledName: regular expression
- CallingName: regular expression
- CalledTon: 'unknown', 'international', 'national', 'network', 'subscriber', or 'abbreviated'
- CallingTon: 'unknown', 'international', 'national', 'network', 'subscriber', or 'abbreviated'
- CalledNpi: 'unknown', 'isdn', 'data', 'telex', 'national', or 'private'
- CallingNpi: 'unknown', 'isdn', 'data', 'telex', 'national', or 'private'
- CalledHost: Regular expression. The call properties format is 'Fqdn[:port]'. If the '[:port]' is not present, the table uses the well-known port of the signaling protocol.
- CallingHost: Regular expression. The call properties format is 'Fqdn[:port]'. If the '[:port]' is not present, the table uses the well-known port of the signaling protocol.
- CallingPi: 'allowed', 'restricted', or 'interworking'
- CallingSi: 'not-screened', 'passed', 'failed', or 'network'
- CallingItc: 'speech', 'unrestricted', 'restricted', '3.1Khz', 'udi-ta', or 'video'
- CalledUri: regular expression
- CallingUri: regular expression
- DateTime: day of week and time period and/or date and time period

- CalledPhoneContext: regular expression
- CallingPhoneContext: regular expression
- CalledSipUsername: regular expression
- CallingSipUsername: regular expression
- CalledBearerChannel: regular expression
- CallingBearerChannel: regular expression
- CallingSipPrivacy: 'disabled', 'none', or 'id'

Special tags:

- <undefined>: Matches if the property is not defined for the call.
- <default>: Always matches. Generally used to set a default route if the previous criteria did not match.

Accepted **DateTime** formats:

Date/Time Period format:

- 'DD.MM.YYYY/HH:MM:SS-DD.MM.YYYY/HH:MM:SS'
- 'DD.MM.YYYY/HH:MM:SS-HH:MM:SS'
- 'DD.MM.YYYY-DD.MM.YYYY'
- 'DD.MM.YYYY'
- 'HH:MM:SS-HH:MM:SS'

Week Day/Time Period format:

- 'DDD'
- 'DDD,DDD...'
- 'DDD/HH:MM:SS-HH:MM:SS'
- 'DDD,DDD.../HH:MM:SS-HH:MM:SS'

where DDD must be one of: SUN, MON, TUE, WED, THU, FRI,or SAT

Several of the previous formats can be concatenated to form one expression. They must be separated by |. Example: 25.12.2006 | SUN

Note: Whitespace at the end of a regular expression is ignored.

See **RouteStatus.PropertiesCriteria**.

Destination (Config Parameter) | Table: Route

Type	Text
Range	Size(0..64)
Default	
Script/CLI	CRout.Route[].Destination
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.300.1.500

Destination to apply to the call if it matches the criteria.
The call destination can be set to:

- route-'name': the route 'name'
- hunt-'name': the hunt 'name'
- sip-'name': the SIP interface 'name'
- isdn-'name': the ISDN interface 'name'
- r2-'name': the R2 interface 'name'
- e&m-'name': the E&M interface 'name'
- fxs-'name': the FXS interface 'name'
- fxo-'name': the FXO interface 'name'
- SipRedirect-'name': When the Route source is a SIP interface, incoming SIP Invites are replied with a 302 'Moved Temporarily' SIP response.

Mappings (Config Parameter) | Table: Route

Type	Text
Range	Size(0..2048)
Default	
Script/CLI	CRout.Route[].Mappings
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.300.1.600

Name of the transformations to apply to the call if the criteria match. The transformations are executed before sending the call to the new destination.
More than one transformation can be specified. In that case, the transformations are separated with ',' and are executed in sequential order.

SignalingProperties (Config Parameter) | Table: Route

Type	Text
Range	Size(0..512)
Default	
Script/CLI	CRout.Route[].SignalingProperties
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.300.1.650

Name of the signaling properties to apply to the call.

ConfigStatus (Status Parameter) | Table: Route

Type	Text
Range	
Script/CLI	CRout.Route[].ConfigStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.300.1.700

Configuration status of the row.
It indicates if the configuration of the row is valid.

Up (Row Command) | Table: Route

Script/CLI:	CRout.Route[].Up
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.300.1.800

Moves the current row upwards.

Down (Row Command) | Table: Route

Script/CLI:	CRout.Route[].Down
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.300.1.900

Moves the current row downwards.

Insert (Row Command) | Table: Route

Script/CLI:	CRout.Route[].Insert
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.300.1.1000

Inserts a new row before this row.

Delete (Row Command) | Table: Route

Script/CLI:	CRout.Route[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.300.1.1100

Deletes this row.

MappingType (Table: user-defined, 150 lines max.)

This table defines which Call Properties are used in the transformations configured in the call routing service. The Transformation Rules (**CRout.MappingExpression**) table contains the detailed rules related to each transformation. The configuration is not used until the `ApplyConfig` command is executed.

Note: Too many entries may introduce delay in the call establishment, especially on low-processing platforms.

Index (Index) | Table: MappingType

Type	UInt32
Range	
Script/CLI	CRout.MappingType[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.500.1.100

Unique identifier of the row in the table.

Name (Config Parameter) | Table: MappingType

Type	Text
Range	Size(0..64)
Default	
Script/CLI	CRout.MappingType[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.500.1.200

Name of the property transformations defined by this row.
The name must be unique in the table.

See **Route.Mapping** parameter.

Criteria (Config Parameter) | Table: MappingType

Type	Enum
Range	None(100) | E164(200) | CalledE164(300) | CallingE164(400) | Name(500) | CalledName(600) | CallingName(700) | Ton(800) | CalledTon(900) | CallingTon(1000) | Npi(1100) | CalledNpi(1200) | CallingNpi(1300) | Host(1400) | CalledHost(1500) | CallingHost(1600) | CallingPi(1700) | CallingSi(1800) | CallingItc(1900) | Uri(2000) | CalledUri(2100) | CallingUri(2200) | DateTime(2300) | PhoneContext(2400) | CalledPhoneContext(2500) | CallingPhoneContext(2600) | SipUsername(2700) | CalledSipUsername(2800) | CallingSipUsername(2900) | LastDivertingReason(3000) | LastDivertingE164(3100) | LastDivertingPartyNumberType(3110) | LastDivertingPublicTypeOfNumber(3120) | LastDivertingPrivateTypeOfNumber(3130) | LastDivertingNumberPresentation(3140) | OriginalDivertingReason(3200) | OriginalDivertingE164(3300) | OriginalDivertingPartyNumberType(3400) | OriginalDivertingPublicTypeOfNumber(3500) | OriginalDivertingPrivateTypeOfNumber(3600) | OriginalDivertingNumberPresentation(3700) | CalledBearerChannel(3800) | CallingBearerChannel(3900) | CallingSipPrivacy(4000)
Default	None
Script/CLI	CRout.MappingType[].Criteria
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.500.1.300

The call property part of the criteria used to determine if the transformation rule can be applied or not. The other part of the criteria is the expression defined in the **MappingExpression.Criteria**.

The expression syntax is related to the criteria property:

- E164: called or calling E.164 properties
- CalledE164: called E.164 properties
- CallingE164: calling E.164 properties
- Name: called or calling name properties
- CalledName: called name properties
- CallingName: calling name properties
- Ton: called or calling type of number properties
- CalledTon: called type of number properties
- CallingTon: calling type of number properties
- Npi: called or calling numbering plan indicator properties
- CalledNpi: called numbering plan indicator properties
- CallingNpi: calling numbering plan indicator properties
- Host: calling or called host properties
- CalledHost: calling host properties
- CallingHost: called host properties
- CallingPi: calling presentation indicator
- CallingSi: calling screening indicator
- CallingItc: calling information transfer capability
- Uri: calling or called SIP URI properties
- CalledUri: called SIP URI properties
- CallingUri: calling SIP URI properties
- DateTime: routes calls based on the date and/or time the call arrived at the call router
- PhoneContext: called or calling phone context properties
- CalledPhoneContext: called phone context properties
- CallingPhoneContext: calling phone context properties
- SipUsername: called or calling SIP username properties
- CalledSipUsername: called SIP username properties
- CallingSipUsername: calling SIP username properties
- LastDivertingReason: last diverting reason properties
- LastDivertingE164: last diverting E.164 properties
- LastDivertingPartyNumberType: party number type of the last diverting number properties
- LastDivertingPublicTypeOfNumber: public type of number of the last diverting number properties
- LastDivertingPrivateTypeOfNumber: private type of number of the last diverting number properties
- LastDivertingNumberPresentation: presentation of the last diverting number properties

- OriginalDivertingReason: original diverting reason properties
- OriginalDivertingE164: original diverting E.164 properties
- OriginalDivertingPartyNumberType: party number type of the original diverting number properties
- OriginalDivertingPublicTypeOfNumber: public type of number of the original diverting number properties
- OriginalDivertingPrivateTypeOfNumber: private type of number of the original diverting number properties
- OriginalDivertingNumberPresentation: presentation of the original diverting number properties
- CalledBearerChannel: called bearer channel properties
- CallingBearerChannel: calling bearer channel properties
- CallingSipPrivacy: calling SIP privacy properties

See **MappingStatus.ExpressionCriteria**.

Transformation (Config Parameter) | Table: MappingType

Type	Enum
Range	None(100) | E164(200) | CalledE164(300) | CallingE164(400) | Name(500) | CalledName(600) | CallingName(700) | Ton(800) | CalledTon(900) | CallingTon(1000) | Npi(1100) | CalledNpi(1200) | CallingNpi(1300) | Host(1400) | CalledHost(1500) | CallingHost(1600) | CallingPi(1700) | CallingSi(1800) | CallingItc(1900) | Uri(2000) | CalledUri(2100) | CallingUri(2200) | PhoneContext(2300) | CalledPhoneContext(2400) | CallingPhoneContext(2500) | SipUsername(2600) | CalledSipUsername(2700) | CallingSipUsername(2800) | LastDivertingReason(2900) | LastDivertingE164(3000) | LastDivertingPartyNumberType(3010) | LastDivertingPublicTypeOfNumber(3020) | LastDivertingPrivateTypeOfNumber(3030) | LastDivertingNumberPresentation(3040) | OriginalDivertingReason(3100) | OriginalDivertingE164(3200) | OriginalDivertingPartyNumberType(3300) | OriginalDivertingPublicTypeOfNumber(3400) | OriginalDivertingPrivateTypeOfNumber(3500) | OriginalDivertingNumberPresentation(3600) | CalledBearerChannel(3700) | CallingBearerChannel(3800) | Debug(60000)
Default	None
Script/CLI	CRout.MappingType[].Transformation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.500.1.400

Call properties to transform. The transformation is defined in the **MappingExpression.Transformation** parameter.

The call properties can be:

- E164: called or calling E.164 properties.
- CalledE164: called E.164 properties.
- CallingE164: calling E.164 properties.
- Name: called or calling name properties.
- CalledName: called name properties.
- CallingName: calling name properties.
- Ton: called or calling type of number properties.
- CalledTon: called type of number properties.
- CallingTon: calling type of number properties.
- Npi: called or calling numbering plan indicator properties.
- CalledNpi: called numbering plan indicator properties.
- CallingNpi: calling numbering plan indicator properties.
- Host: calling or called host properties.
- CalledHost: calling host properties.
- CallingHost: called host properties.
- CallingPi: calling presentation indicator.
- CallingSi: calling screening indicator.
- CallingItc: calling information transfer capability.
- Uri: calling or called SIP URI properties.
- CalledUri: called SIP URI properties.
- CallingUri: calling SIP URI properties.
- PhoneContext: calling or called phone context properties.
- CalledPhoneContext: called phone context properties.
- CallingPhoneContext: calling phone context properties.
- SipUsername: calling or called SIP username properties.
- CalledSipUsername: called SIP username properties.
- CallingSipUsername: calling SIP username properties.
- LastDivertingReason: last diverting reason properties.
- LastDivertingE164: last diverting E.164 properties.
- LastDivertingPartyNumberType: party number type of the last diverting number properties.
- LastDivertingPublicTypeOfNumber: public type of number of the last diverting number properties.
- LastDivertingPrivateTypeOfNumber: private type of number of the last diverting number properties.
- LastDivertingNumberPresentation: presentation of the last diverting number properties.
- OriginalDivertingReason: original diverting reason properties.

- OriginalDivertingE164: original diverting E.164 properties.
- OriginalDivertingPartyNumberType: party number type of the original diverting number properties.
- OriginalDivertingPublicTypeOfNumber: public type of number of the original diverting number properties.
- OriginalDivertingPrivateTypeOfNumber: private type of number of the original diverting number properties.
- OriginalDivertingNumberPresentation: presentation of the original diverting number properties.
- CalledBearerChannel: called bearer channel properties.
- CallingBearerChannel: calling bearer channel properties.
- Debug: reserved for debug configuration.

See **MappingStatus.Transformation** parameter.

ConfigStatus (Status Parameter) | Table: MappingType

Type	Text
Range	
Script/CLI	CRout.MappingType[].ConfigStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.500.1.500

Configuration status of the row.
Indicates if the configuration of the row is valid.

Up (Row Command) | Table: MappingType

Script/CLI:	CRout.MappingType[].Up
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.500.1.600

Moves the current row upwards.

Down (Row Command) | Table: MappingType

Script/CLI:	CRout.MappingType[].Down
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.500.1.700

Moves the current row downwards.

Insert (Row Command) | Table: MappingType

Script/CLI:	CRout.MappingType[].Insert
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.500.1.800

Inserts a new row before this row.

Delete (Row Command) | Table: MappingType

Script/CLI:	CRout.MappingType[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.500.1.900

Deletes this row.

MappingExpression (Table: user-defined, 150 lines max.)

This table shows the transformation rules used by the call routing service. The Transformations (**MappingType**) table contains the transformation related to this rule. The configuration is not used until the `ApplyConfig` command is executed.

Note: Too many entries may introduce delay in the call establishment, especially on low-processing platforms.

Index (Index) | Table: MappingExpression

Type	UInt32
Range	
Script/CLI	CRout.MappingExpression[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.700.1.100

Unique identifier of the row in the table.

Name (Config Parameter) | Table: MappingExpression

Type	Text
Range	Size(0..64)
Default	
Script/CLI	CRout.MappingExpression[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.700.1.200

Name of the transformation rule defined by this row. It must match the name of a row in the Transformations (**MappingType**) table.

More than one row can have the same name. In that case, the first row matching the call will be used. The row are used in ascending order.

See **MappingType.Name**.

Criteria (Config Parameter) | Table: MappingExpression

Type	Text
Range	Size(0..256)
Default	
Script/CLI	CRout.MappingExpression[].Criteria
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.700.1.300

The call property part of the criteria used to determine if the transformation rule can be applied or not. The other part of the criteria is the expression defined in the **MappingType.Criteria** parameter.

The expression syntax is related to the selected criteria properties or can be a special tag:

- E164: regular expression
- CalledE164: regular expression
- CallingE164: regular expression
- Name: regular expression
- CalledName: regular expression
- CallingName: regular expression
- Ton: 'unknown', 'international', 'national', 'network', 'subscriber', or 'abbreviated'
- CalledTon: 'unknown', 'international', 'national', 'network', 'subscriber', or 'abbreviated'
- CallingTon: 'unknown', 'international', 'national', 'network', 'subscriber', or 'abbreviated'
- Npi: 'unknown', 'isdn', 'data', 'telex', 'national', or 'private'

- CalledNpi: 'unknown', 'isdn', 'data', 'telex', 'national', or 'private'.
- CallingNpi: 'unknown', 'isdn', 'data', 'telex', 'national', or 'private'.
- Host: Regular expression. The call property format is 'Fqdn[:port]'. If the '[:port]' is not present, the table uses the well-known port of the signaling protocol.
- CalledHost: Regular expression. The call property format is 'Fqdn[:port]'. If the '[:port]' is not present, the table uses the well-known port of the signaling protocol.
- CallingHost: Regular expression. The call property format is 'Fqdn[:port]'. If the '[:port]' is not present, the table uses the well-known port of the signaling protocol.
- CallingPi: 'allowed', 'restricted', or 'interworking'
- CallingSi: 'not-screened', 'passed', 'failed', or 'network'
- CallingItc: 'speech', 'unrestricted', 'restricted', '3.1Khz', 'udi-ta', or 'video'
- DateTime: day of week and time period and/or date and time period
- PhoneContext: regular expression
- CalledPhoneContext: regular expression
- CallingPhoneContext: regular expression
- SipUsername: regular expression
- CalledSipUsername: regular expression
- CallingSipUsername: regular expression
- LastDivertingReason: 'cfu', 'cfb', 'cfnr', or 'unknown'
- LastDivertingE164: regular expression
- LastDivertingPartyNumberType: 'unknown', 'public', or 'private'
- LastDivertingPublicTypeOfNumber: 'unknown', 'international', 'national', 'network-specific', 'local', or 'abbreviated'.
- LastDivertingPrivateTypeOfNumber: 'unknown', 'leg2-reg', 'leg1-reg', 'pisn-specific', 'subscriber', or 'abbreviated'.
- LastDivertingNumberPresentation: 'allowed', 'restricted', 'interworking', or 'restricted-address'
- OriginalDivertingReason: 'cfu', 'cfb', 'cfnr', or 'unknown'
- OriginalDivertingE164: regular expression
- OriginalDivertingPartyNumberType: 'unknown', 'public', or 'private'
- OriginalDivertingPublicTypeOfNumber: 'unknown', 'international', 'national', 'network-specific', 'local', or 'abbreviated'
- OriginalDivertingPrivateTypeOfNumber: 'unknown', 'leg2-reg', 'leg1-reg', 'pisn-specific', 'subscriber', or 'abbreviated'
- OriginalDivertingNumberPresentation: 'allowed', 'restricted', 'interworking', or 'restricted-address'
- CalledBearerChannel: regular expression
- CallingBearerChannel: regular expression
- CallingSipPrivacy: 'disabled', 'none', or 'id'

Special tags:

- <undefined>: Matches if the property is not defined for the call.
- <default>: Always matches. Generally used to set a default transformation if the previous transformation does not match.

Accepted **DateTime** formats:

Date/Time Period format:

- 'DD.MM.YYYY/HH:MM:SS-DD.MM.YYYY/HH:MM:SS'
- 'DD.MM.YYYY/HH:MM:SS-HH:MM:SS'
- 'DD.MM.YYYY-DD.MM.YYYY'
- 'DD.MM.YYYY'
- 'HH:MM:SS-HH:MM:SS'

Week Day/Time Period format:

- 'DDD'
- 'DDD,DDD...'
- 'DDD/HH:MM:SS-HH:MM:SS'
- 'DDD,DDD.../HH:MM:SS-HH:MM:SS'

where DDD must be one of: SUN, MON, TUE, WED, THU, FRI, or SAT.

Several of the previous formats can be concatenated to form one expression. They must be separated by |. Example: 25.12.2006 | SUN

Note: Whitespace at the end of a regular expression is ignored.

See **MappingStatus.PropertiesCriteria**.

Transformation (Config Parameter) | Table: MappingExpression

Type	Text
Range	Size(0..64)
Default	
Script/CLI	CRout.MappingExpression[].Transformation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.700.1.400

Transformation rule to apply to the call properties. The rule is applied on the call properties defined in the **MappingType.Transformation** parameter.

The transformation rule syntax is related to the selected properties to transform:

- Ton: 'unknown', 'international', 'national', 'network', 'subscriber', or 'abbreviated'
- CalledTon: 'unknown', 'international', 'national', 'network', 'subscriber', or 'abbreviated'

- CallingTon: 'unknown', 'international', 'national', 'network', 'subscriber', or 'abbreviated'
- Npi: 'unknown', 'isdn', 'data', 'telex', 'national', or 'private'
- CalledNpi: 'unknown', 'isdn', 'data', 'telex', 'national', or 'private'
- CallingNpi: 'unknown', 'isdn', 'data', 'telex', 'national', or 'private'
- CallingPi: 'allowed', 'restricted', or 'interworking'
- CallingSi: 'not-screened', 'passed', 'failed', or 'network'
- CallingItc: 'speech', 'unrestricted', 'restricted', '3.1Khz', 'udi-ta', or 'video'
- LastDivertingReason: 'cfu', 'cfb', 'cfnr', or 'unknown'
- LastDivertingPartyNumberType: 'unknown', 'public', or 'private'
- LastDivertingPublicTypeOfNumber: 'unknown', 'international', 'national', 'network-specific', 'local', or 'abbreviated'
- LastDivertingPrivateTypeOfNumber: 'unknown', 'leg2-reg', 'leg1-reg', 'pisn-specific', 'subscriber', or 'abbreviated'
- LastDivertingNumberPresentation: 'allowed', 'restricted', 'interworking', or 'restricted-address'
- OriginalDivertingReason: 'cfu', 'cfb', 'cfnr', or 'unknown'
- OriginalDivertingPartyNumberType: 'unknown', 'public', or 'private'
- OriginalDivertingPublicTypeOfNumber: 'unknown', 'international', 'national', 'network-specific', 'local' or 'abbreviated'
- OriginalDivertingPrivateTypeOfNumber: 'unknown', 'leg2-reg', 'leg1-reg', 'pisn-specific', 'subscriber', or 'abbreviated'
- OriginalDivertingNumberPresentation: 'allowed', 'restricted', 'interworking', or 'restricted-address'
- All others: string where '\0' to '\9' is replaced by the corresponding group in the regular expresion set in the criteria rule (see **MappingStatus.ExpressionCriteria**). The value can be set to the '<local_ip_port>' macro to replace the properties by the local IP address and port of the listening socket of the SIP gateway used to send the INVITE.

See **MappingStatus.PropertiesToTransform**.

SubMappings (Config Parameter) | Table: MappingExpression

Type	Text
Range	Size(0..512)
Default	
Script/CLI	CRout.MappingExpression[].SubMappings
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.700.1.500

Name of a next transformation to execute.

More than one transformation can be specified. In that case, the transformations are separated with ',' and are executed in sequential order.

ConfigStatus (Status Parameter) | Table: MappingExpression

Type	Text
Range	
Script/CLI	CRout.MappingExpression[].ConfigStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.700.1.600

Configuration status of the row.
It indicates if the configuration of the row is valid.

Up (Row Command) | Table: MappingExpression

Script/CLI:	CRout.MappingExpression[].Up
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.700.1.700

Moves the current row upwards.

Down (Row Command) | Table: MappingExpression

Script/CLI:	CRout.MappingExpression[].Down
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.700.1.800

Moves the current row downwards.

Insert (Row Command) | Table: MappingExpression

Script/CLI:	CRout.MappingExpression[].Insert
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.700.1.900

Inserts a new row before this row.

Delete (Row Command) | Table: MappingExpression

Script/CLI:	CRout.MappingExpression[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.700.1.1000

Deletes this row.

Hunt (Table: user-defined, 40 lines max.)

This table shows the configured hunt to be used by the call routing service. The configuration is not used until the `ApplyConfig` command is executed.

Index (Index) | Table: Hunt

Type	UInt32
Range	
Script/CLI	CRout.Hunt[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.900.1.100

Unique identifier of the row in the table.

Name (Config Parameter) | Table: Hunt

Type	Text
Range	Size(0..64)
Default	
Script/CLI	CRout.Hunt[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.900.1.200

Name of the hunt defined by this row. It must be unique in the table.

Destinations (Config Parameter) | Table: Hunt

Type	Text
Range	
Default	
Script/CLI	CRout.Hunt[].Destinations
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.900.1.300

List of hunt destinations separated by commas.
The call destination can be:

- route-'name': the route 'name'
- hunt-'name': the hunt 'name'
- sip-'name':the SIP interface 'name'
- isdn-'name': the ISDN interface 'name'
- r2-'name': the R2 interface 'name'
- e&m-'name': the E&M interface 'name'
- fxs-'name': the FXS interface 'name'
- fxo-'name': the FXO interface 'name'
- SipRedirect-'name': When the Route source is a SIP interface, incoming SIP Invites are replied with a 302 'Moved Temporarily' SIP response.

Note: Only FXS interfaces are supported if 'Simultaneous' is selected for the **Selection Algorithm** parameter.

Example: 'isdn-Slot2/Bri1, route-something'

SelectionAlgorithm (Config Parameter) | Table: Hunt

Type	Enum
Range	Sequential(100) | Cyclic(200) | Simultaneous(300)
Default	Sequential
Script/CLI	CRout.Hunt[].SelectionAlgorithm
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.900.1.400

Algorithm used to select the destination order.
The destination order can be:

- Sequential: The hunt tries the destination in the same order as listed. The first destination hunted is the first listed.
- Cyclic: The hunt starts from the destination that follows the destination used for the last hunt. Subsequent calls try another first destination in a round-robin method.
- Simultaneous: The hunt tries every available destination at the same time. The first destination to pick up has the call. Other destinations stop ringing. This method can only have FXS endpoints as destinations.

Example of cyclic selection: If the destination is set to 'x,y,z', the destination the hunt group tries is in the following order:

1. x,y,z
2. y,z,x
3. z,x,y
4. x,y,z

Timeout (Config Parameter) | Table: Hunt

Type	UInt32
Range	0..100
Default	0
Script/CLI	CRout.Hunt[].Timeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.900.1.500

Maximal time allowed to the destination to handle the call.
A value of '0' disables the timeout.

This value is expressed in seconds (s).

Note: Not applicable if 'Simultaneous' is used for the **Selection Algorithm** parameter.

Causes (Config Parameter) | Table: Hunt

Type	Text
Range	Size(0..255)
Default	31, 34, 38, 41, 42, 43, 44, 47
Script/CLI	CRout.Hunt[].Causes
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.900.1.600

Lists the call rejection causes to continue the hunt. The causes are separated by commas. The available hunt causes are:
Normal event:

- 1: unassigned (unallocated) number
- 2: no route to specified transit network
- 3: no route to destination
- 6: channel unacceptable
- 7: call awarded and being delivered in an established channel
- 16: normal call clearing
- 17: user busy
- 18: no user responding
- 19: user alerting, no answer
- 21: call rejected
- 22: number changed
- 26: non-selected user clearing
- 27: destination out of order
- 28: invalid number format (incomplete number)
- 29: facility rejected
- 30: response to STATUS ENQUIRY
- 31: normal, unspecified

Resource unavailable:

- 34: no circuit/channel available
- 38: network out of order
- 41: temporary failure
- 42: switching equipment congestion
- 43: access information discarded
- 44: requested circuit/channel not available
- 47: resource unavailable, unspecified

Service or option not available:

- 57: bearer capability not authorised
- 58: bearer capability not presently available
- 63: service or option not available, unspecified

Service or option not implemented:

- 65: bearer capability not implemented
- 66: channel type not implemented
- 69: requested facility not implemented
- 70: only restricted digital information bearer capability is available

- 79: service or option not implemented, unspecified

Invalid message:

- 81: invalid call reference value
- 82: identified channel does not exist
- 83: a suspended call exists, but this call identity does not
- 84: call identity in use
- 85: no call suspended
- 86: call having the requested call identity has been cleared
- 88: incompatible destination
- 91: invalid transit network selection
- 95: invalid message, unspecified

Protocol error:

- 96: mandatory information element is missing
- 97: message type non-existent or not implemented
- 98: message not compatible with call state or message type non-existent or not implemented
- 99: information element non-existent or not implemented
- 100: invalid information element contents
- 101: message not compatible with call state
- 102: recovery on time expiry
- 111: Protocol error, unspecified

Interworking:

- 127: Interworking, unspecified

Note: Not applicable if 'Simultaneous' is used for the **Selection Algorithm** parameter.

ConfigStatus (Status Parameter) | Table: Hunt

Type	Text
Range	
Script/CLI	CRout.Hunt[].ConfigStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.900.1.700

Configuration status of the row.
It indicates if the configuration of the row is valid.

Up (Row Command) | Table: Hunt

Script/CLI:	CRout.Hunt[].Up
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.900.1.800

Moves the current row upwards.

Down (Row Command) | Table: Hunt

Script/CLI:	CRout.Hunt[].Down
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.900.1.900

Moves the current row downwards.

Insert (Row Command) | Table: Hunt

Script/CLI:	CRout.Hunt[].Insert
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.900.1.1000

Inserts a new row before this row.

Delete (Row Command) | Table: Hunt

Script/CLI:	CRout.Hunt[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.900.1.1100

Deletes this row.

SignalingProperties (Table: user-defined, 40 lines max.)

This table shows the configured signaling properties to be used by the call routing service. The configuration is not used until the `ApplyConfig` command is executed.

Index (Index) | Table: SignalingProperties

Type	UInt32
Range	
Script/CLI	CRout.SignalingProperties[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1200.1.100

Unique identifier of the row in the table.

Name (Config Parameter) | Table: SignalingProperties

Type	Text
Range	Size(0..64)
Default	
Script/CLI	CRout.SignalingProperties[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1200.1.200

Name of the signaling properties defined by this row. It must be unique in the table.

EarlyConnect (Config Parameter) | Table: SignalingProperties

Type	EnableDisable
Range	
Default	Disable
Script/CLI	CRout.SignalingProperties[].EarlyConnect
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1200.1.300

Enable/Disable the early connect feature.
When early connect is enabled, the SIP call is connected by sending a 200 OK message instead of a 183 Session Progress message with early media.

EarlyDisconnect (Config Parameter) | Table: SignalingProperties

Type	EnableDisable
Range	
Default	Disable
Script/CLI	CRout.SignalingProperties[].EarlyDisconnect
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1200.1.400

Enable/Disable the early disconnect feature.
When early disconnect is enabled, the SIP BYE message is sent upon ISDN 'Disconnect' signal reception.

When early disconnect is disabled, the SIP BYE message is sent upon ISDN 'Call release' signal reception.

If early disconnect is enabled but no ISDN 'Disconnect' message is received, the SIP BYE message will be sent upon receiving an ISDN 'Call release' as if the early disconnect was disabled.

DestinationHost (Config Parameter) | Table: SignalingProperties

Type	Text
Range	Size(0..255)
Default	
Script/CLI	CRout.SignalingProperties[].DestinationHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1200.1.500

SIP message destination.
The value can be set to the '<local_ip_port>' macro to replace the properties by the local IP address and port of the listening socket of the SIP gateway used to send the INVITE.

Allow180Sdp (Config Parameter) | Table: SignalingProperties

Type	EnableDisable
Range	
Default	Enable
Script/CLI	CRout.SignalingProperties[].Allow180Sdp
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1200.1.550

Enable/Disable the 180 with SDP allowed.
When disabled, a SIP 183 with SDP is sent instead of a 180 with SDP.

This does not affect the 180 without SDP.

Allow183NoSdp (Config Parameter) | Table: SignalingProperties

Type	EnableDisable
Range	
Default	Enable
Script/CLI	CRout.SignalingProperties[].Allow183NoSdp
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1200.1.560

Enable/Disable the 183 without SDP allowed.
When disabled, a 183 without SDP is not sent.

This does not affect the 183 with SDP.

Privacy (Config Parameter) | Table: SignalingProperties

Type	Enum
Range	Disable(100) | None(200) | AssertedId(250) | PreferredId(300) | Rpid(400)
Default	Disable
Script/CLI	CRout.SignalingProperties[].Privacy
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1200.1.570

Sets the privacy level of the call.

- Disable: No privacy is used.
- None: Use P-Asserted Identity and privacy "none".
- AssertedId: Use P-Asserted Identity and privacy "id" when restricted.
- PreferredId: Use P-Preferred Identity and privacy "id" when restricted.
- Rpid: Use Remote-Party-ID header.

CallPropertiesTranslation (Config Parameter) | Table: SignalingProperties

Type	Text
Range	Size(0..512)
Default	
Script/CLI	CRout.SignalingProperties[].CallPropertiesTranslation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1200.1.580

Name of the call property translation to apply to the call.
The translation modifies the call properties before the call is sent to its destination.

More than one translation can be specified. In this case, the translations are separated with ',' and are executed in sequential order.

SipHeadersTranslation (Config Parameter) | Table: SignalingProperties

Type	Text
Range	Size(0..512)
Default	
Script/CLI	CRout.SignalingProperties[].SipHeadersTranslation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1200.1.590

Name of the SIP header translations to apply to the call.
The translation modifies the SIP headers before the call is sent to its destination.

More than one translation can be specified. In that case, the translations are separated with ',' and are executed in sequential order.

ConfigStatus (Status Parameter) | Table: SignalingProperties

Type	Text
Range	
Script/CLI	CRout.SignalingProperties[].ConfigStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1200.1.600

Configuration status of the row.
It indicates if the configuration of the row is valid.

Up (Row Command) | Table: SignalingProperties

Script/CLI:	CRout.SignalingProperties[].Up
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1200.1.700

Moves the current row upwards.

Down (Row Command) | Table: SignalingProperties

Script/CLI:	CRout.SignalingProperties[].Down
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1200.1.800

Moves the current row downwards.

Insert (Row Command) | Table: SignalingProperties

Script/CLI:	CRout.SignalingProperties[].Insert
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1200.1.900

Inserts a new row before this row.

Delete (Row Command) | Table: SignalingProperties

Script/CLI:	CRout.SignalingProperties[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1200.1.1000

Deletes this row.

SipHeadersTranslation (Table: user-defined, 150 lines max.)

This table shows the configured SIP header translations to be used by the call routing service. The configuration is not used until the `ApplyConfig` command is executed.

Index (Index) | Table: SipHeadersTranslation

Type	UInt32
Range	
Script/CLI	CRout.SipHeadersTranslation[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1400.1.100

Unique identifier of the row in the table.

Name (Config Parameter) | Table: SipHeadersTranslation

Type	Text
Range	Size(0..64)
Default	
Script/CLI	CRout.SipHeadersTranslation[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1400.1.200

Name of the SIP header translation defined by this row.

SipHeader (Config Parameter) | Table: SipHeadersTranslation

Type	Enum
Range	FromHeaderHostPart(100) | FromHeaderUserPart(200) | IdentityHeaderHostPart(300) | IdentityHeaderUserPart(400) | IdentityHeaderPhoneNumber(500) | IdentityHeaderFriendlyName(550) | RequestLineHostPart(600) | RequestLineUserPart(700) | ToHeaderHostPart(800) | ToHeaderUserPart(900)
Default	FromHeaderHostPart
Script/CLI	CRout.SipHeadersTranslation[].SipHeader
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1400.1.300

Sets which SIP header is modified by this translation.
The SIP headers can be:

- FromHeaderHostPart: host part of the From header URI
- FromHeaderUserPart: user part of the From header URI
- IdentityHeaderHostPart: host part of the Identity header URI

- IdentityHeaderUserPart: user part of the Identity header URI
- IdentityHeaderPhoneNumber: phone number in the Identity header tel URL
- IdentityHeaderFriendlyName: friendly name in the Identity header URI
- RequestLineHostPart: host part of the Request line URI
- RequestLineUserPart: user part of the Request line URI
- ToHeaderHostPart: host part of the To header URI
- ToHeaderUserPart: user part of the To header URI

BuiltFrom (Config Parameter) | Table: SipHeadersTranslation

Type	Enum
Range	CalledE164(100) | DestinationHost(200) | Domain(300) | FixValue(400) | HostName(500) | LocalIp(600) | CallingBearerChannel(700) | SipEndpointUsername(800) | CallingName(900) | CallingE164(1000)
Default	FixValue
Script/CLI	CRout.SipHeadersTranslation[].BuiltFrom
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1400.1.400

Sets what information is used to build the selected SIP header.
The information can be retrieved from:

- CalledE164: the called party E.164 property
- DestinationHost:the destination host configured in the signaling properties of which this translation is part
- Domain: the domain name configured in the unit
- FixValue: a fixed value (see **SipHeadersTranslation.FixValue**)
- HostName: the host name configured on the unit
- LocalIp: the local IP address
- CallingBearerChannel: the calling bearer channel
- SipEndpointUsername: the SIP username associated with the endpoint
- CallingName: the calling party name property
- CallingE164: the calling party E.164 property

FixValue (Config Parameter) | Table: SipHeadersTranslation

Type	Text
Range	Size(0..255)
Default	
Script/CLI	CRout.SipHeadersTranslation[].FixValue
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1400.1.500

Fixed value to be inserted in the SIP header when the **SipHeadersTranslation.BuiltFrom** parameter is set to 'FixValue'.

ConfigStatus (Status Parameter) | Table: SipHeadersTranslation

Type	Text
Range	
Script/CLI	CRout.SipHeadersTranslation[].ConfigStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1400.1.600

Configuration status of the row.
It indicates if the configuration of the row is valid.

Up (Row Command) | Table: SipHeadersTranslation

Script/CLI:	CRout.SipHeadersTranslation[].Up
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1400.1.700

Moves the current row upwards.

Down (Row Command) | Table: SipHeadersTranslation

Script/CLI:	CRout.SipHeadersTranslation[].Down
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1400.1.800

Moves the current row downwards.

Insert (Row Command) | Table: SipHeadersTranslation

Script/CLI:	CRout.SipHeadersTranslation[].Insert
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1400.1.900

Inserts a new row before this row.

Delete (Row Command) | Table: SipHeadersTranslation

Script/CLI:	CRout.SipHeadersTranslation[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1400.1.1000

Deletes this row.

CallPropertiesTranslation (Table: user-defined, 150 lines max.)

This table shows the configured call properties translations to be used by the call routing service. The configuration is not used until the `ApplyConfig` command is executed.

Index (Index) | Table: CallPropertiesTranslation

Type	UInt32
Range	
Script/CLI	CRout.CallPropertiesTranslation[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1600.1.100

Unique identifier of the row in the table.

Name (Config Parameter) | Table: CallPropertiesTranslation

Type	Text
Range	Size(0..64)
Default	
Script/CLI	CRout.CallPropertiesTranslation[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1600.1.200

Name of the call property translation defined by this row.

CallProperty (Config Parameter) | Table: CallPropertiesTranslation

Type	Enum
Range	CalledE164(100) | CallingE164(200) | CalledName(300) | CallingName(400) | CalledUri(500) | CallingUri(600) | CalledBearerChannel(700)
Default	CalledE164
Script/CLI	CRout.CallPropertiesTranslation[].CallProperty
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1600.1.300

Sets which call property is modified by this translation.
The call properties can be:

- CalledE164: called party E.164 property
- CallingE164: calling party E.164 property
- CalledName: called party name property
- CallingName: calling party name property
- CalledUri: called URI name property
- CallingUri: calling URI name property
- CalledBearerChannel: called bearer channel property

BuiltFrom (Config Parameter) | Table: CallPropertiesTranslation

Type	Enum
Range	Domain(100) | FixValue(200) | FromHeaderUri(300) | FromHeaderFriendlyName(400) | FromHeaderUserPart(500) | IdentityHeaderUri(600) | IdentityHeaderUserPart(700) | IdentityHeaderPhoneNumber(800) | IdentityHeaderFriendlyName(850) | LocalIp(900) | RequestLineUri(1000) | RequestLineUserPart(1100) | ToHeaderUri(1200) | ToHeaderFriendlyName(1300) | ToHeaderUserPart(1400)
Default	FixValue
Script/CLI	CRout.CallPropertiesTranslation[].BuiltFrom
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1600.1.400

Sets what information is used to build the selected call property.
The information can be retrieved from:

- Domain: the domain name configured in the unit.
- FixValue: a fixed value (see **CallPropertiesTranslation.FixValue**)
- FromHeaderUri: the From header URI
- FromHeaderFriendlyName: the friendly name part of the From header
- FromHeaderUserPart: the user part of the From header URI
- IdentityHeaderUri: the Identity header URI
- IdentityHeaderUserPart: the user part of the Identity header URI
- IdentityHeaderPhoneNumber: the phone number in the Identity header tel URL
- IdentityHeaderFriendlyName: the friendly name in the Identity header URI
- LocalIp: the local IP address
- RequestLineUri: the Request line URI
- RequestLineUserPart: the user part of the Request line URI
- ToHeaderUri: the To header URI
- ToHeaderFriendlyName: Uthe friendly name part of the To header
- ToHeaderUserPart: the user part of the To header URI

FixValue (Config Parameter) | Table: CallPropertiesTranslation

Type	Text
Range	Size(0..255)
Default	
Script/CLI	CRout.CallPropertiesTranslation[].FixValue
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1600.1.500

Fixed value to be inserted in the call property when the **CallPropertiesTranslation.BuiltFrom** parameter is set to 'FixValue'.

ConfigStatus (Status Parameter) | Table: CallPropertiesTranslation

Type	Text
Range	
Script/CLI	CRout.CallPropertiesTranslation[].ConfigStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1600.1.600

Configuration status of the row.
It indicates if the configuration of the row is valid.

Up (Row Command) | Table: CallPropertiesTranslation

Script/CLI:	CRout.CallPropertiesTranslation[].Up
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1600.1.700

Moves the current row upwards.

Down (Row Command) | Table: CallPropertiesTranslation

Script/CLI:	CRout.CallPropertiesTranslation[].Down
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1600.1.800

Moves the current row downwards.

Insert (Row Command) | Table: CallPropertiesTranslation

Script/CLI:	CRout.CallPropertiesTranslation[].Insert
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1600.1.900

Inserts a new row before this row.

Delete (Row Command) | Table: CallPropertiesTranslation

Script/CLI:	CRout.CallPropertiesTranslation[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1600.1.1000

Deletes this row.

AutoRouting (Table)

This table holds the parameters required for the configuration of the auto-routing feature.

EpId (Index) | Table: AutoRouting

Type	Text
Range	
Script/CLI	CRout.AutoRouting[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1900.1.100

Character string that identifies an endpoint in other tables.

Autoroutable (Config Parameter) | Table: AutoRouting

Type	Enum
Range	Enable(100) | Disable(200) | HardwareDependent(300)
Default	HardwareDependent
Script/CLI	CRout.AutoRouting[].Autoroutable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1900.1.200

Determines whether or not automatic routes are generated for the endpoint when auto-routing is enabled (see the **AutoRoutingEnable** parameter).

- Enable: Automatic routes allowing incoming and outgoing calls to and from the endpoint are added to the **Route** Table when auto-routing is enabled.
- Disable: Automatic route generation is turned off for this endpoint.
- HardwareDependent: Automatic routes are generated if the endpoint belongs to an FXS interface.

AutoRoutingGateway (Config Parameter) | Table: AutoRouting

Type	Text
Range	Size(0..255)
Default	
Script/CLI	CRout.AutoRouting[].AutoRoutingGateway
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1900.1.300

The name of the SIP gateways to use as the destination of outgoing calls and the source of incoming calls when generating auto-routing rules.

More than one SIP gateway can be defined. The SIP gateways names are separated by comas. Example: 'gw1,gw2,gw3'.

When one SIP gateway is defined:

- A route is automatically created from the SIP gateway to the telephony interface.
- A route is automatically created from the telephony interface to the SIP gateway if the **AutoRouting.AutoRoutingDestination** parameter is empty. Otherwise, the destination of the route is the destination defined in the **AutoRouting.AutoRoutingDestination** parameter.

When more than one SIP gateway is defined:

- Routes are automatically created from each defined SIP gateway to the telephony interface.
- A route is automatically created from the telephony interface to the hunt defined in the **AutoRouting.AutoRoutingDestination** parameter.

AutoRoutingDestination (Config Parameter) | Table: AutoRouting

Type	Text
Range	Size(0..255)
Default	
Script/CLI	CRout.AutoRouting[].AutoRoutingDestination
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1900.1.350

The destination to use for the routes from the telephony interface.
The destination can be set to:

- route-'name': the route 'name'
- hunt-'name': the hunt 'name'
- sip-'name': the SIP interface 'name'
- isdn-'name': the ISDN interface 'name'
- r2-'name': the R2 interface 'name'
- e&m-'name': the E&M interface 'name'
- fxs-'name': the FXS interface 'name'
- fxo-'name': the FXO interface 'name'

See the **AutoRouting.AutoRoutingGateway** parameter.

E164 (Status Parameter) | Table: AutoRouting

Type	Text
Range	SIZE(0..255)
Script/CLI	CRout.AutoRouting[].E164
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1900.1.400

The telephone number associated with this endpoint, if any. This reflects the **Username** configured in the **UserAgent** table of the SIP Endpoint (SipEp) service as long as the name follows the E.164 syntax.

SipUsername (Status Parameter) | Table: AutoRouting

Type	Text
Range	SIZE(0..255)
Script/CLI	CRout.AutoRouting[].SipUsername
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1900.1.450

The SIP username associated with this endpoint, if any. This simply reflects the **Username** configured in the **UserAgent** table of the SIP Endpoint (SipEp) service without the **Username** parameter.

For example: If the **SipEp.UserAgent.Username** parameter is set to "123456_test", the SIP username field will display "123456_test".

Name (Status Parameter) | Table: AutoRouting

Type	Text
Range	SIZE(0..255)
Script/CLI	CRout.AutoRouting[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.1900.1.500

The FriendlyName associated with this endpoint, if any. This reflects the **FriendlyName** configured in the **UserAgent** table of the SIP Endpoint (SipEp) service.

AutoRoutingCriteriaType (Config Parameter)

Type	Enum
Range	E164(100) | SipUsername(200)
Default	E164
Script/CLI	CRout.AutoRoutingCriteriaType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.2000

Determines the type of criteria to use to create an automatic rule from SIP to the telephony endpoints.

- E164: The E164 associated with the endpoint is used as the criteria. (See **AutoRouting.E164**).
- SipUsername: The SIP username associated with the endpoint is used as the criteria. (See **AutoRouting.SipUsername**).

AutoRoutingIncomingMappings (Config Parameter)

Type	Text
Range	Size(0..512)
Default	
Script/CLI	CRout.AutoRoutingIncomingMappings
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.2100

Name of the transformations associated with the route from the SIP gateway to the endpoint. More than one transformation can be specified. In that case, the transformations are separated with ',' and are executed in an sequential order.

See also **Route.Mappings**.

AutoRoutingOutgoingMappings (Config Parameter)

Type	Text
Range	Size(0..512)
Default	
Script/CLI	CRout.AutoRoutingOutgoingMappings
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.2200

Name of the transformations associated with the route from the endpoint to the SIP gateway. More than one transformation can be specified. In this case, the transformations are separated with ',' and are executed in sequential order.

See also **Route.Mappings**

AutoRoutingIncomingSignalingProperties (Config Parameter)

Type	Text
Range	Size(0..512)
Default	
Script/CLI	CRout.AutoRoutingIncomingSignalingProperties
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.2300

Name of the signaling properties associated with the route from the SIP gateway to the endpoint.
See also **Route.SignalingProperties**

AutoRoutingOutgoingSignalingProperties (Config Parameter)

Type	Text
Range	Size(0..512)
Default	
Script/CLI	CRout.AutoRoutingOutgoingSignalingProperties
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.2400

Name of the signaling properties associated with the route from the endpoint to the SIP gateway.
See also **Route.SignalingProperties**

SipRedirect (Table: user-defined, 150 lines max.)

This table allows the configuration of SIP redirections that can be used as Route or Hunt destinations. When the Route source is a SIP interface, incoming SIP Invites are replied with a 302 'Moved Temporarily' SIP response.

Index (Index) | Table: SipRedirect

Type	UInt32
Range	
Script/CLI	CRout.SipRedirect[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.2500.1.100

Unique identifier of the row in the table.

Name (Config Parameter) | Table: SipRedirect

Type	Text
Range	Size(0..64)
Default	
Script/CLI	CRout.SipRedirect[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.2500.1.200

Name of the SIP Redirect defined by this row. It must be unique in the table.

DestinationHost (Config Parameter) | Table: SipRedirect

Type	Text
Range	Size(0..255)
Default	
Script/CLI	CRout.SipRedirect[].DestinationHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.2500.1.300

Host address to be inserted in the 'Moved Temporarily' response.

ConfigStatus (Status Parameter) | Table: SipRedirect

Type	Text
Range	
Script/CLI	CRout.SipRedirect[].ConfigStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.2500.1.400

Configuration status of the row.
Indicates if the configuration of the row is valid.

Up (Row Command) | Table: SipRedirect

Script/CLI:	CRout.SipRedirect[].Up
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.2500.1.500

Moves the current row upwards.

Down (Row Command) | Table: SipRedirect

Script/CLI:	CRout.SipRedirect[].Down
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.2500.1.600

Moves the current row downwards.

Insert (Row Command) | Table: SipRedirect

Script/CLI:	CRout.SipRedirect[].Insert
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.2500.1.700

Inserts a new row before this row.

Delete (Row Command) | Table: SipRedirect

Script/CLI:	CRout.SipRedirect[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.2500.1.800

Deletes this row.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	CRout.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	CRout.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1750.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

ApplyConfig (Command)

Applies the call routing configuration. The configuration is not applied if an error is detected.

ClearCallSimulationSettings (Command)

Clear all the Call Properties previously applied by the `SetCallSimulationProperty` command.

InsertCallPropertiesTranslation (Command)

Inserts a new row at the end of the Call Properties Translation Overrides table.

InsertHunt (Command)

Inserts a new row at the end of the Hunt table.

InsertMappingExpression (Command)

Inserts a new row at the end of the **MappingExpression** table.

InsertMappingType (Command)

Inserts a new row at the end of the Transformations (**MappingType**) table.

InsertRoute (Command)

Inserts a new row at the end of the **Routes** table.

InsertSignalingProperties (Command)

Inserts a new row at the end of the Signaling Properties table.

InsertSipHeadersTranslation (Command)

Inserts a new row at the end of the SIP Header Translation Overrides table.

InsertSipRedirect (Command)

Inserts a new row at the end of the Sip Redirects (**SipRedirect**) table.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

RollbackConfig (Command)

Rolls back the current configuration to the running configuration as showed in the status.
The current configuration will be lost.

SetCallSimulationProperty (Command)

Set a Call Property for the Call Simulation.
The supported Call Properties that can be used for a Call Simulation are:

- CalledE164 / CallingE164: the called / calling party E.164 property
- CalledName / CallingName: the called / calling party name property
- CalledHost / CallingHost: the called / calling host property
- CalledUri / CallingUri: the called / calling party SIP URI
- CalledNpi / CallingNpi: the called / calling party Numbering Plan Indicator property
- CalledTon / CallingTon: the called / calling party Type Of Number property
- CalledItc / CallingItc: the called / calling party Information Transfer Capability property
- CalledPi / CallingPi: the called / calling party Presentation Indicator property
- CalledSi / CallingSi: the called / calling party Screening Indicator property
- CalledCcc / CallingCcc: the called / calling Clear Channel Codec property
- CalledEf / CallingEf: the called / calling Emergency Flag property
- CalledDr / CallingDr: the called / calling Distinctive Ringing property

- CalledUsr / CallingUsr: the called / calling SIP Username property
- CalledBchan / CallingBchan: the called / calling Bearer Channel property
- CalledDivc / CallingDivc: the called / calling Diverting Counter property
- CalledLdivr / CallingLdivr: the called / calling Last Diverting Reason property
- CalledLdive / CallingLdive: the called / calling Last Diverting E.164 property
- CalledLdivpnt / CallingLdivpnt: the called / calling Last Diverting PNT property
- CalledLdivpriton / CallingLdivpriton: the called / calling Last Diverting Private TON property
- CalledLdivpubton / CallingLdivpubton: the called / calling Last Diverting Public TON property
- CalledLdivpre / CallingLdivpre: the called / calling Last Diversting Presentation property
- CalledOdivr / CallingOdivr: the called / calling Original Diverting Reason property
- CalledOdive / CallingOdive: the called / calling Original Diverting E.164 property
- CalledOdivpnt / CallingOdivpnt: the called / calling Original Diverting Party Number Type property
- CalledOdivpriton / CallingOdivpriton: the called / calling Original Diverting Private TON property
- CalledOdivpubton / CallingOdivpubton: the called / calling Original Diverting Public TON property
- CalledOdivpre / CallingOdivpre: the called / calling Original Diverting Presentation property

Property (Argument) | Command: SetCallSimulationProperty

Type	Text
Range	Size(0..30)
Default	

The name of the Call Property to set.

PropertyValue (Argument) | Command: SetCallSimulationProperty

Type	Text
Range	Size(0..200)
Default	

The value to set in the Call Property defined in the **Property** argument.

StartCallSimulation (Command)

Start the Call Simulation with the Call Properties previously applied by the `SetCallSimulationProperty` command.
Once the call simulation is no longer needed, the unit must be restarted.

SourceInterface (Argument) | Command: StartCallSimulation

Type	Text
Range	Size(0..30)
Default	

The telephony source interface where the call comes from. Refer to the **EpAdm.Endpoint** table for the available telephony interfaces.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the CRout service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.1750.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	The call %s failed because it has reached the maximum redirection limit in call routing.	Warning	The call failed because it has reached the maximum number of allowed redirections to a route or a hunt. Verify that there are no loops in the route and hunt configuration.
20	The call %s encountered the maximum call properties manipulation limit.	Warning	The call reached the maximum allowed call property manipulation limit. Verify that there are no loops in the property manipulation configuration.
30	The unsupported destinations of hunt %s were not applied.	Warning	This hunt is configured with at least one unsupported destination. Hunts with simultaneous algorithms only support FXS destinations.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.

NumKey	Message	Severity	Description
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.

NumKey	Message	Severity	Description
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to CRout.

Message	Severity	Description
The configuration was applied with some warnings.	Warning	This message is sent when a warning is raised while applying the CRout rules.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.

Message	Severity	Description
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

CPE WAN Management Protocol (Cwmp)

The CPE WAN Management Protocol (Cwmp) service allows the administrator to manage the unit using the TR-069 protocol.

Parameters

RootElement (Config Parameter)

Type	Enum
Range	Device(100) | InternetGatewayDevice(200)
Default	Device
Script/CLI	Cwmp.RootElement
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.100

Determines the data model used for the configuration.

- Device: Uses the Device data model as defined in TR-106.
- InternetGatewayDevice: Uses the Internet Gateway Device data model as defined in TR-098.

NetworkInterface (Config Parameter)

Type	Text
Range	SIZE(0..50)
Default	
Script/CLI	Cwmp.NetworkInterface
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.190

Specifies to which network interface the Cwmp service is bound. The name specified here must match an existing InterfaceName of the **NetworkInterfaces** table of the Bni service. The DHCP options for the automatic configuration are retrieved from this network interface.

The possible values are:

- Empty: Use the network interface configured in the **Hoc.ManagementInterface** parameter.
- 'All': Use any network interface.
- A valid IPv4 network interface name.

Note that this parameter is case-sensitive.

Note that Advance IP Routing could be required to forward the packet over the correct network.

ListeningPort (Config Parameter)

Type	ExtIpPort
Range	
Default	0
Script/CLI	Cwmp.ListeningPort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.200

Port on which the unit listens for incoming TR-069 connections.
Note: If set to 0, the unit uses the default TR-069 port 7547.

AcsUrlConfigSource (Config Parameter)

Type	Enum
Range	Dhcp(100) | Static(200) | DhcpWithFailover(300)
Default	Dhcp
Script/CLI	Cwmp.AcsUrlConfigSource
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.1000.100

Determines the method to obtain the URL of the ACS.

- Dhcp: Uses the DHCP protocol to find the URL as defined in TR-106 section 3.1.
- Static: Uses the URL defined in the **AcsStaticUrl** parameter.
- DhcpWithFailover: Uses the DHCP protocol to find the URL or the URL defined in the **AcsStaticUrl** parameter if the DHCP method fails.

AcsStaticUrl (Config Parameter)

Type	Text
Range	SIZE(0..256)
Default	
Script/CLI	Cwmp.AcsStaticUrl
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.1000.200

URL used by the unit to connect to the ACS using the CPE WAN Management Protocol if the **AcsUrlConfigSource** parameter is set to 'Static'.

This parameter must be a valid HTTP or HTTPS URL.

Example:

- 'http://somewhere.com'.
- 'https://somewhere.secure.com'.

Username (Config Parameter)

Type	Text
Range	SIZE(0..256)
Default	
Script/CLI	Cwmp.Username
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.1000.300

Username used to authenticate the unit when making a connection to the ACS using the CPE WAN Management Protocol.

Password (Config Parameter)

Type	Text
Range	Size(0..512)
Default	
Script/CLI	Cwmp.Password
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.1000.600

Password used to authenticate the unit when making a connection to the ACS the CPE WAN Management Protocol.
Password encryption is supported via the **Dcm.PasswordEncryption** table.

When **Dcm.PasswordEncryption** is enabled clear text passwords will be automatically encrypted.

Unencrypted password maximal length is 256.

Encrypted password maximal length is 389.

Note: This parameter's value cannot be set to an encrypted value when setting the parameter through Cwmp.

AcsStatus (Status Parameter)

Type	Enum
Range	Starting(100) | Connected(200) | NoUrl(300) | ErrorCannotResolve(400) | ErrorNotResponding(500) | ErrorAuthFailure(600) | ErrorOther(700)
Script/CLI	Cwmp.AcsStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.1000.700

Indicates the status of the connection with the ACS.

- Starting: Cwmp service is starting and no connection attempt have been made so far.
- Connected: The Cwmp service is connected to the ACS.
- NoUrl: The Cwmp service cannot connect with the ACS because no ACS URL is configured.
- ErrorCannotResolve: The Cwmp service cannot connect with the ACS because the FQDN cannot be resolved.
- ErrorNotResponding: The Cwmp service cannot connect with the ACS because the ACS is not responding.
- ErrorAuthFailure: The Cwmp service failed authenticating to the ACS.
- ErrorOther: The Cwmp service cannot connect to the ACS for unspecified reason. See device and ACS logs.

AcsUrl (Status Parameter)

Type	Text
Range	
Script/CLI	Cwmp.AcsUrl
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.1000.750

Current ACS URL used by the unit.

ConnectionRequestUsername (Config Parameter)

Type	Text
Range	SIZE(0..256)
Default	admin
Script/CLI	Cwmp.ConnectionRequestUsername
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.1000.800

Username used to authenticate an ACS making a Connection Request to the CPE.

ConnectionRequestPassword (Config Parameter)

Type	Text
Range	Size(0..512)
Default	administrator
Script/CLI	Cwmp.ConnectionRequestPassword
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.1000.900

Password used to authenticate an ACS making a Connection Request to the CPE.
Password encryption is supported via the **Dcm.PasswordEncryption** table.

When **Dcm.PasswordEncryption** is enabled clear text passwords will be automatically encrypted.

Unencrypted password maximal length is 256.

Encrypted password maximal length is 389.

Note: This parameter's value cannot be set to an encrypted value when setting the parameter through Cwmp.

PeriodicInformEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Cwmp.PeriodicInformEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.2000.100

Defines whether or not the unit needs to periodically send CPE information to the ACS using the Inform method call.

- Disable: The unit does not send periodic inform.
- Enable: The unit sends periodic inform.

PeriodicInformInterval (Config Parameter)

Type	UInt32
Range	1..31536000
Default	3600
Script/CLI	Cwmp.PeriodicInformInterval
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.2000.200

The duration, in seconds, of the interval for which the unit will attempt to connect with the ACS and call the Inform method if the **PeriodicInformEnable** parameter is set to 'Enable'.

PeriodicInformTime (Config Parameter)

Type	Text
Range	SIZE(20..20)
Default	0001-01-01T00:00:00Z
Script/CLI	Cwmp.PeriodicInformTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.2000.300

An absolute time reference in UTC to determine when the unit initiates the periodic Inform method calls. Each Inform call MUST occur at this reference time plus or minus an integer multiple of the **PeriodicInformInterval** parameter.

The **PeriodicInformTime** parameter is used only to set the "phase" of the periodic Informs. The actual value of **PeriodicInformTime** can be arbitrarily far into the past or future.

For example, if the **PeriodicInformInterval** parameter is 86400 (a day) and if the **PeriodicInformTime** parameter is set to UTC midnight on some day (in the past, present, or future), then periodic Informs will occur every day at UTC midnight. These MUST begin on the very next midnight, even if the **PeriodicInformTime** parameter refers to a day in the future.

The Unknown Time value indicates that no particular time reference is specified. That is, the unit locally chooses the time reference and needs only to follow the specified **PeriodicInformInterval**.

If absolute time is not available to the unit, its periodic Inform behavior is the same as if the **PeriodicInformTime** parameter was set to the Unknown Time value.

The format of the value is 'CCYY-MM-DDThh:mm:ssZ' where:

- CCYY: Year number.
- MM: Month number in the year.
- DD: Day number in the month.

- hh: Hour number in the day.
- mm: Minute number in the hour.
- ss: Second number in the minute.

Example: 1969-07-21T02:28:00Z.

The Unknown Time value is defined at '0001-01-01T00:00:00Z'.

Tr069AnnexFEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Cwmp.Tr069AnnexFEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.2100.100

Enables/disables the support of parameters under the TR-069 **Device.GatewayInfo** tree.

Tr104Enable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Cwmp.Tr104Enable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.2900.100

Enables/disables the support of parameters under the TR-069 **Device.Services.VoiceService** tree.

Tr106LanNetworkInterface (Config Parameter)

Type	Text
Range	SIZE(0..50)
Default	
Script/CLI	Cwmp.Tr106LanNetworkInterface
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.3000.100

Network interface referred by the TR-106 LAN profile.

- If empty, use the network interface configured in the **Hoc.ManagementInterface** parameter.
- If the **Hoc.ManagementInterface** parameter is set to 'All', use the network interface used for contacting the ACS.

Tr111StunEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Cwmp.Tr111StunEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.4000.100

Enables/disables the use of STUN binding requests to discover the unit's external IP address and port and to set the **ManagementServer.UDPConnectionRequestAddress** parameter accordingly. The ACS can then send UDP connection requests to the unit at that IP address and port.

- Enable: Enables the use of STUN by the unit.
- Disable: Disables the use of STUN by the unit.

Tr111NatDetected (Status Parameter)

Type	Enum
Range	No(100) | Yes(200)
Script/CLI	Cwmp.Tr111NatDetected
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.4000.200

When the **Tr111StunEnable** parameter is enabled, this parameter indicates whether or not the unit has detected the address and/or port mapping in use.

- Yes: the **Tr111StunEnable** parameter is enabled and the unit has detected the address and/or port mapping.
- No: the **Tr111StunEnable** parameter is disabled or the unit has not detected the address and/or port mapping.

Tr111StunServerHost (Config Parameter)

Type	IpHostNamePort
Range	
Default	
Script/CLI	Cwmp.Tr111StunServerHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.4000.300

Host name or IP address of the STUN server for the unit to send Binding Requests if the **Tr111StunEnable** parameter is enabled.

If the **Tr111StunServerHost** parameter is empty and the **Tr111StunEnable** parameter is enabled, the unit uses the address of the ACS extracted from the host portion of the ACS URL.

If the port is not specified or set to 0, the default STUN port (3478) is used.

Tr111StunKeepAlivePeriod (Config Parameter)

Type	Text
Range	SIZE(0..256)
Default	60-60
Script/CLI	Cwmp.Tr111StunKeepAlivePeriod
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.4000.400

If the **Tr111StunEnable** parameter is enabled, this is the period, in seconds, at which STUN Binding Requests must be sent by the unit for the purpose of maintaining the STUN connection. The timeouts must be entered in the 'minimum-maximum' format.

The value must be less than or equal to 3600 seconds.

Note: The current implementation does not allow a range. The minimum and maximum values must be the same.

Tr111StunUsername (Config Parameter)

Type	Text
Range	SIZE(0..256)
Default	
Script/CLI	Cwmp.Tr111StunUsername
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.4000.500

If non-empty, the value of the STUN username attribute to be used in Binding Requests when the **Tr111StunEnable** parameter is enabled.

Tr111StunStatus (Status Parameter)

Type	Enum
Range	Disabled(0) | Starting(100) | Connected(200) | ErrorCannotResolve(400) | ErrorNotResponding(500) | ErrorOther(700)
Script/CLI	Cwmp.Tr111StunStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.4000.600

Indicates the status of the connection with the STUN server.

- Disabled: TR-111 is disabled.
- Starting: Cwmp service is starting and no connection attempt have been made so far.
- Connected: The Cwmp service is connected to the STUN server.
- ErrorCannotResolve: The Cwmp service cannot connect with the STUN server because the FQDN cannot be resolved.
- ErrorNotResponding: The Cwmp service cannot connect with the STUN server because the server is not responding.
- ErrorOther: The Cwmp service cannot connect to the STUN server for unspecified reason or because no ACS URL is configured. See device and ACS logs.

NlmLocalLogLogEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Cwmp.NlmLocalLogLogEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.4500.100

Add the object .X_0090F8_Nlm.LocalLog.Log{i}. to the data model.

This object contains the notifications stored locally on the device.

Making this object accessible requires significant CPU resources when notifications are frequently sent to the local log.

TransportHttpsCipherSuite (Config Parameter)

Type	Enum
Range	CS1(100) | CS2(200) | CS3(300)
Default	CS1
Script/CLI	Cwmp.TransportHttpsCipherSuite
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.5000.100

Defines the allowed cipher suites for the network security settings when using the HTTPS protocol to connect to the ACS. When the device initiates an HTTPS connection to the ACS, it will negotiate the cipher suite according to its configuration.

- CS1:
  - TLS_DHE_DSS_WITH_AES_128_CBC_SHA
  - TLS_DHE_DSS_WITH_AES_256_CBC_SHA
  - Also includes ciphers from CS2 and CS3 below
- CS2:
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - Also includes ciphers from CS3 below

- CS3:
  - The following are TLS 1.2 ciphers:
  - TLS_RSA_WITH_AES_128_CBC_SHA256
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_CBC_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
  - The following are TLS 1.3 ciphers:
  - TLS_AES_256_GCM_SHA384
  - TLS_AES_128_GCM_SHA256
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_CCM_8_SHA256
  - TLS_AES_128_CCM_SHA256

TransportHttpsTlsVersion (Config Parameter)

Type	Enum
Range	TLSv1(200) | TLSv1_1(300) | TLSv1_2 (400) | TLSv1_3 (500)
Default	TLSv1
Script/CLI	Cwmp.TransportHttpsTlsVersion
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.5000.150

Defines the allowed TLS versions for the network security settings when using the HTTPS protocol to connect to the ACS. When the device initiates an HTTPS connection to the ACS, it will negotiate the TLS version according to its configuration.

- TLSv1: Allow TLS versions 1 and up.
- TLSv1_1: Allow TLS versions 1.1 and up.
- TLSv1_2: Allow TLS versions 1.2 and up.
- TLSv1_3: Allow TLS version 1.3 only.

The device will always send its highest supported TLS version in the ClientHello message. The server will select the highest supported TLS version it supports from the ClientHello message. The device will then validate that the selected version is allowed. If the version is not allowed the device will close the connection.

TransportCertificateValidation (Config Parameter)

Type	Enum
Range	NoValidation(100) | HostName(200)
Default	HostName
Script/CLI	Cwmp.TransportCertificateValidation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.5000.200

When connecting to the ACS using HTTPS, this parameter defines the level of security to use when validating the server's certificate.

- NoValidation: Allow a connection to the server without validating its certificate. The only condition is to receive a certificate from the server. This option provides partial security and should be selected with care.
- HostName: Allow a connection to the server by validating its certificate is trusted and valid. The validations performed on the certificate include the expiration date and that the Subject Alternate Name (SAN) or Common Name (CN) matches the FQDN or IP address of the server.

InteropAllowUnauthenticatedUDPConnectionRequests (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Cwmp.InteropAllowUnauthenticatedUDPConnectionRequests
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.50000.100

Determines the CPE behavior when receiving a UDP connection request message.

- Enable: Allow any UDP connection request without authentication. This behavior goes against the UDP Connection Request described by TR-069 Amendment-2 specification.

- Disable: Force the authentication of a UDP connection request.

InteropParameterTypeValidation (Config Parameter)

Type	Enum
Range	Tolerant(100) | Strict(200)
Default	Tolerant
Script/CLI	Cwmp.InteropParameterTypeValidation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.50000.200

Defines the parameter type validation when the ACS assigns a value to a parameter.

- Tolerant: The client target type is evaluated and conversion is done (if possible): i.e., string to boolean, string to int, string to unsigned int, string to datetime, etc.
- Strict: The ACS and the client must have matching xsd:type otherwise the client rejects the parameter value.

InteropMacAddressFormat (Config Parameter)

Type	Enum
Range	LowerCase(100) | UpperCaseWithColon(200)
Default	LowerCase
Script/CLI	Cwmp.InteropMacAddressFormat
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.50000.300

LAN.MACAddress Display Format

- LowerCase: MAC address is in lower case format. Ex.: 0090f80d5b4a
- UpperCaseWithColon: MAC address is in upper case format, each octet separated by colons. Ex.: 00:90:F8:0D:5B:4A

InteropCwmpIdHeader (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Cwmp.InteropCwmpIdHeader
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.50000.400

Determines whether the CPE sends a <Cwmp:ID> header when contacting the ACS.

- Enable: The CWMP Inform requests sent to the ACS will contain a SOAP header with a <Cwmp:ID> element. The content of the <Cwmp:ID> will be the "null" characters.
- Disable: The CWMP Inform requests sent to the ACS will not contain a SOAP header.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Cwmp.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Cwmp.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3900.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Cwmp service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.3900.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	The ACS has requested a firmware upgrade for image at location '%1$s'.	Info	The ACS has requested a download and installation of a firmware upgrade image with the TR-069 method Download.
20	The requested firmware upgrade for image with at location '%1$s' has failed.	Error	The requested download for firmware upgrade image has failed. See previous notifications from the Fpu service for more information.
30	The ACS has requested a download for vendor configuration file with URL '%1$s'.	Info	The ACS has requested a download and execution of a vendor configuration file with the TR-069 method Download.
40	The requested download for vendor configuration file with URL '%1$s' has failed.	Error	The requested download for vendor configuration file has failed. See previous notifications from the Conf service for more information.
50	The ACS has requested a reboot.	Info	The ACS has requested a reboot with the TR-069 method Reboot.
55	The ACS server '%1$s' is connected.	Info	The ACS server was successfully contacted. The notification is sent whenever a connection is established with the ACS.
60	The ACS server '%1$s' is not responding.	Error	The service cannot establish a connection to the ACS because it is not responding.
70	CWMP port already in use.	Error	The service cannot establish a connection to the ACS because the port is already in use or internal error.
85	The ACS URL is invalid.	Error	The ACS URL format is invalid.
90	ACS URL provisioning fall back to automatic configuration.	Warning	The ACS cannot be contacted with the URL provided with static configuration. The unit retries to contact the ACS with automatic configuration.
92	ACS URL provisioning fall back to static configuration.	Warning	The ACS cannot be contacted with the URL provided with DHCP configuration. The unit retries to contact the ACS with static configuration.
94	ACS URL provisioning fails with both DHCP and static configuration.	Warning	The ACS cannot be contacted with the URL provided by both DHCP and static configuration. The unit waits for 5 minutes before retrying to contact the ACS with first the URL provided with DHCP and if it fails with the URL from the static configuration.
96	The ACS lost connection with the unit.	Warning	The unit lost connection with the ACS. The unit restarts the ACS discovery from DHCP.

NumKey	Message	Severity	Description
100	The configured LAN network interface does not currently exist.	Warning	The network interface configured to retrieve information on the LAN network (e.g. Address, mask, statistics, etc.) does not currently exist or is disabled. The information of the LAN profile might be incomplete or inaccurate.
110	The configured LAN network interface is not IPv4.	Error	The network interface configured to retrieve information on the LAN network (e.g. Address, mask, statistics, etc.) is not an IPv4 network. The information of the LAN profile might be incomplete or inaccurate.
120	The ACS server cannot be contacted because its URL is empty.	Warning	The ACS server cannot be contacted because its URL is empty.
130	The ACS URL '%1$s' cannot be resolved.	Error	The service cannot establish a connection to the ACS because the URL/FQDN cannot be resolved.
140	The ACS server '%1$s' authentication failed.	Error	The service cannot establish a connection to the ACS because the configured username/password were rejected by the server.
150	The ACS server '%1$s' cannot be contacted for unspecified reason.	Error	The service received an unexpected response from the ACS or internal error.
160	The STUN URL '%1$s' cannot be resolved.	Error	The service cannot establish a connection to the STUN server because the URL/FQDN cannot be resolved.
170	The STUN server '%1$s' is not responding.	Error	The service cannot establish a connection to the STUN server because it is not responding.
180	The STUN server '%1$s' cannot be contacted for unspecified reason.	Error	The service received an unexpected response from the STUN server or internal error.
190	The ACS has requested a factory reset.	Info	The ACS has requested default settings with the TR-069 method FactoryReset.
200	The ACS has requested a download for vendor ruleset file with URL '%1$s'.	Info	The ACS has requested a download of a vendor ruleset file with the TR-069 Download method.
210	The requested download for vendor ruleset file with URL '%1$s' has failed.	Error	The requested download for vendor ruleset file has failed.

NumKey	Message	Severity	Description
220	The ACS has requested an upload of the vendor log file '%1$s - %2$s' to the URL '%3$s'.	Info	The ACS has requested an upload of a vendor log file with the TR-069 Upload method.
230	The requested upload of the vendor log file '%1$s - %2$s' to the URL '%3$s' has failed.	Error	The requested upload of the vendor log file has failed.
240	The '%1$s' NetworkInterface parameter is invalid.	Error	This message is issued when the value of the **NetworkInterface** parameter is not a valid IPv4 network interface. The value must match an IPv4 **Bni.NetworkInterfaces** name. When the service starts, if the **NetworkInterface** parameter is invalid, the default value is used.
250	The ACS server ('%1$s') cannot be contacted because of an error in certificate validation.	Error	The Cwmp service cannot establish a connection to the ACS server because the time is not synchronised or the certificate is missing.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.

NumKey	Message	Severity	Description
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.

NumKey	Message	Severity	Description
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Cwmp.

Message	Severity	Description
The '%1$s' network name is not a valid IPv4 network interface.	Warning	This message is issued if the **NetworkInterface** parameter is not set to a valid value.
Assignment of value %3$s to expression %2$s in service %1$s failed, reason is: '%4$s'.	Error	CwmpEx: This message is issued when the value assignment to a parameter failed.
Assignment of value %3$s to expression %2$s in service %1$s issued the following warning: '%4$s'.	Warning	CwmpEx: This message is issued when the value assignment to a parameter detects a warning condition.
Evaluation of expression %2$s in service %1$s failed, reason is: '%3$s'.	Error	CwmpEx: This message is issued when the parameters evaluation or run command fails.
Evaluation of expression %2$s in service %1$s issued the following warning: '%3$s'.	Warning	CwmpEx: This message is issued when the parameter evaluation or running a command detects a warning condition.
Retrieving a table is not supported.	Error	CwmpEx: Retrieving a whole table, row or column is not supported.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.

Message	Severity	Description
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Device Control Manager (Dcm)

The Device Control Manager (DCM) service manages the hardware properties as well as the licence activation keys.

Parameters

UnitInfoProductName (Status Parameter)

Type	Text
Range	
Script/CLI	Dcm.UnitInfoProductName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.100.100

Name of the unit.

UnitInfoSerialNumber (Status Parameter)

Type	Text
Range	
Script/CLI	Dcm.UnitInfoSerialNumber
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.100.200

Serial number of the unit.

UnitInfoMacAddress (Status Parameter)

Type	Text
Range	
Script/CLI	Dcm.UnitInfoMacAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.100.300

MAC address of the unit.

UnitInfoHardwareRevision (Status Parameter)

Type	Text
Range	
Script/CLI	Dcm.UnitInfoHardwareRevision
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.100.400

The hardware revision of the unit.

TotalNumberOfDsp (Status Parameter)

Type	UInt32
Range	
Script/CLI	Dcm.TotalNumberOfDsp
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.100.500

The total number of DSPs present on the unit.

UnitFingerprintUuid (Status Parameter)

Type	Text
Range	
Script/CLI	Dcm.UnitFingerprintUuid
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.150.100

Fingerprint UUID. This parameter is only available on the Mediatrix Sentinel CS.

HardwareExtInfo (Table)

This table displays all hardware extensions currently installed in the unit.

Index (Index) | Table: HardwareExtInfo

Type	UInt32
Range	
Script/CLI	Dcm.HardwareExtInfo[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.300.100.1.100

The index of the Installed Hardware Extension table.
Installed hardware components are listed in an arbitrary order.

ProductName (Status Parameter) | Table: HardwareExtInfo

Type	Text
Range	
Script/CLI	Dcm.HardwareExtInfo[].ProductName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.300.100.1.200

Name of the hardware extension.

SerialNumber (Status Parameter) | Table: HardwareExtInfo

Type	Text
Range	
Script/CLI	Dcm.HardwareExtInfo[].SerialNumber
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.300.100.1.300

Serial number of the hardware extension.

Location (Status Parameter) | Table: HardwareExtInfo

Type	Text
Range	
Script/CLI	Dcm.HardwareExtInfo[].Location
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.300.100.1.400

Indicates where the hardware extension is installed in the unit.

HardwareFanInfo (Table)

This table lists the monitored fans of the unit.

FanId (Index) | Table: HardwareFanInfo

Type	UInt32
Range	
Script/CLI	Dcm.HardwareFanInfo[].FanId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.300.200.1.100

The unique ID associated to the FanName.

FanName (Status Parameter) | Table: HardwareFanInfo

Type	Text
Range	
Script/CLI	Dcm.HardwareFanInfo[].FanName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.300.200.1.200

The fan identification name. Usually refers to its location in the unit.

FanFault (Status Parameter) | Table: HardwareFanInfo

Type	Int32
Range	-1..1
Script/CLI	Dcm.HardwareFanInfo[].FanFault
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.300.200.1.300

Indicates a fan fault state:

- 0: No fault
- 1: Fault

Unit casing fans come in pairs, one fan on the left side and another one on the right side. When a fault is detected on a fan, the one on the other side will automatically run faster to compensate. This design allows the unit to continue running smoothly even if there are some faults.

HardwareTemperatureInfo (Table)

This table lists the monitored temperatures of the unit.

TemperatureId (Index) | Table: HardwareTemperatureInfo

Type	UInt32
Range	
Script/CLI	Dcm.HardwareTemperatureInfo[].TemperatureId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.300.300.1.100

The unique ID associated to the TemperatureName.

TemperatureName (Status Parameter) | Table: HardwareTemperatureInfo

Type	Text
Range	
Script/CLI	Dcm.HardwareTemperatureInfo[].TemperatureName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.300.300.1.200

The temperature sensor name. Usually refers to its location in the unit.

TemperatureCelsius (Status Parameter) | Table: HardwareTemperatureInfo

Type	Int32
Range	
Script/CLI	Dcm.HardwareTemperatureInfo[].TemperatureCelsius
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.300.300.1.300

The measured temperature, in Celsius.

TemperatureFault (Status Parameter) | Table: HardwareTemperatureInfo

Type	Int32
Range	-1..1
Script/CLI	Dcm.HardwareTemperatureInfo[].TemperatureFault
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.300.300.1.400

Indicates whether or not the temperature has exceeded the configured threshold:

- 0: No fault
- 1: Fault

The fault clears when the temperature is back under the configured threshold.

TemperatureFaultThreshold (Config Parameter) | Table: HardwareTemperatureInfo

Type	UInt32
Range	0..127
Default	0
Script/CLI	Dcm.HardwareTemperatureInfo[].TemperatureFaultThreshold
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.300.300.1.500

Configures the temperature threshold, in Celsius. Set "0" to disable temperature faults.
A fault is reported when the temperature exceeds this threshold.

ActiveFeature (Table)

This table displays the features that are currently enabled by a licence activation key.

ID (Index) | Table: ActiveFeature

Type	UInt32
Range	
Script/CLI	Dcm.ActiveFeature[].ID
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.500.100.1.100

A unique ID of a feature.

Description (Status Parameter) | Table: ActiveFeature

Type	Text
Range	
Script/CLI	Dcm.ActiveFeature[].Description
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.500.100.1.200

The description of the active feature.

Delete (Row Command) | Table: ActiveFeature

Script/CLI:	Dcm.ActiveFeature[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.500.100.1.500

Deletes the licence entry and permanently removes it from the system.

PasswordEncryption (Table)

This table configures how the passwords should be encrypted.

Parameter (Index) | Table: PasswordEncryption

Type	Text
Range	
Script/CLI	Dcm.PasswordEncryption[].Parameter
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.600.100.1.100

The path of the password parameter to encrypt.
The special parameter 'ALL' overrides the configuration for all other parameters if the **Encryption** parameter is not set to 'None'.

Encryption (Config Parameter) | Table: PasswordEncryption

Type	Enum
Range	None(100) | Enc1(200)
Default	None
Script/CLI	Dcm.PasswordEncryption[].Encryption
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.600.100.1.200

Specify if the parameter needs to be encrypted.

- None: The password will not be encrypted.
- Enc1: The password will be encrypted with a private password unique to the device.

Activating the encryption will trigger an encryption of unencrypted passwords. Deactivating the encryption will not decrypt encrypted passwords.

The password encryption will be executed at the next service start if the service of the parameter is not already started.

PersistentMemoryTotal (Status Parameter)

Type	UInt32
Range	
Script/CLI	Dcm.PersistentMemoryTotal
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.10000.100.100

The total amount (in kilobytes) of persistent memory in the system.

PersistentMemoryInUse (Status Parameter)

Type	UInt32
Range	
Script/CLI	Dcm.PersistentMemoryInUse
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.10000.100.200

The amount (in kilobytes) of persistent memory currently in use by the system.

PersistentWearPercentage (Status Parameter)

Type	Int32
Range	-1..1000
Script/CLI	Dcm.PersistentWearPercentage
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.10000.100.250

Internal SSD wear percentage.
A new SSD drive has a wear percentage of 0. A value of 100 means it has reached his minimum expected lifetime.

A value of -1 means the SSD internal drive does not provide a wear indicator.

PersistentSmartData (Status Parameter)

Type	Text
Range	
Script/CLI	Dcm.PersistentSmartData
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.10000.100.280

Internal SSD SMART Data.
SMART data format: Identification element followed by Attribute elements.

- Identification element: DriveModel=<SSD name>;
- Attribute element: <AttributeID>=<AttributeRawData>;

Both <AttributeID> and <AttributeRawData> are hexadecimal values.

Ex: "DriveModel=SP128GIMDA555SE0;A8=00000BB8;A9=00000062;AF=00000000;"

NOTE: A maximum of 30 attributes are available.

VolatileMemoryTotal (Status Parameter)

Type	UInt64
Range	
Script/CLI	Dcm.VolatileMemoryTotal
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.10000.100.300

The total amount (in kilobytes) of volatile memory in the system.

VolatileMemoryInUse (Status Parameter)

Type	UInt64
Range	
Script/CLI	Dcm.VolatileMemoryInUse
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.10000.100.400

The amount (in kilobytes) of volatile memory currently in use by the system.

InteropEthernetControllerRevA0 (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Dcm.InteropEthernetControllerRevA0
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.50000.100

When enabled, the network speed is limited to 100 Mbps on specific platforms, to improve stability and increase the unit lifetime.

Only applies to early Mediatrix G7, S7 and Sentinel 100 models.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Dcm.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.

- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Dcm.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2000.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

ActivateLicense (Command)

Activates a feature using a licence key.

LicenseKey (Argument) | Command: ActivateLicense

Type	Text
Range	SIZE(1..2000)
Default	

Licence key to activate a feature.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Dcm service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.2000.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	The activation of a licence for the unit with MAC address %1$s has failed.	Error	The licence has not been activated. This issue may occur in the following situations: • This firmware version is too old to activate this licence. In this case the licence may be partially activated. • The licence key was build for a different device. • The licence key is invalid or corrupted.
20	The activation of the %1$s licence for the unit with MAC address %2$s has succeeded.	Info	The licence has been activated with a valid licence key.
25	The removal of the %1$s licence for the unit with MAC address %2$s has succeeded.	Info	The licence has been removed with a valid deactivation licence key.
30	The Power Supply Unit # %1$d is in fault state.	Critical	A PSU fault has been detected. **Note:** This notification is platform-specific.

NumKey	Message	Severity	Description
40	The Power Supply Unit #%1$d recovered from the previous fault state.	Info	A PSU has been restored to a working state. **Note:** This notification is platform-specific.
70	Warning, disk wear level is at %1$d percent.	Critical	The wear level is becoming critical. **Note:** This notification is platform-specific.
80	Fan fault detected: %1$s.	Error	A fan fault has been detected for the specified fan. **Note:** This notification is platform-specific.
90	Temperature fault detected: %1$s.	Error	The temperature has exceeded the configured threshold for the specified location. **Note:** This notification is platform-specific.
95	Temperature OK: %1$s.	Info	The temperature has lowered under the configured threshold. **Note:** This notification is platform-specific.
100	Critical fan fault(s) detected.	Critical	Whether all the fans are in fault state or a fan controller communication problem is detected.
110	The %1$s parameter is being encrypted.	Info	This message is sent when a password is being encrypted.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.

NumKey	Message	Severity	Description
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.

NumKey	Message	Severity	Description
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Dcm.

Message	Severity	Description
The licence key to activate the feature is invalid.	Error	This message is issued when the user tries to activate a feature using an invalid licence key.
The licence has been activated.	Info	This message is issued when the user has activated a feature using a licence key.
The licence key contains unknown feature codes.	Warning	This message is issued when at least one feature could not be activated, possibly because of incompatible firmware version.
The licence key has incompatible version.	Error	This message is issued when the user tries to activate a feature using a licence that is not supported by the current version of the firmware.
The licence does not match the device.	Error	This message is issued when the user tries to activate a feature using a licence that does not belong to this device.
The licence key is expired.	Error	This message is issued when the user tries to activate a feature using an expired licence.
The licence signature is not valid.	Error	This message is issued when the user tries to activate a feature using a licence whose signature cannot be validated.
Invalid or no licensing certificate found.	Error	Whether the licensing certificate has not been found in the device, or it is invalid for this platform.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.

Message	Severity	Description
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Dynamic Host Configuration Protocol Server (Dhcp)

The Dynamic Host Configuration Protocol (DHCP) service manages a DHCP server on each network interface.

Parameters

Subnets (Table: user-defined, 48 lines max.)

This table configures the subnets of the DHCP server. The **NetworkInterfaceName** parameter must match a network interface that is Up and the **EnableSubnet** parameter must be set to 'Enable' to properly activate the DHCP server on that interface.

The `Dhcp.AddSubnet` command may be used to add a new subnet to the **SubnetsTable** and to all subnet-specific configuration tables.

NetworkInterfaceName (Index) | Table: Subnets

Type	Text
Range	
Script/CLI	Dhcp.Subnets[].NetworkInterfaceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.100.1.100

Network interface on which the DHCP server is active. That interface must be up for the DHCP server to become active.

EnableSubnet (Config Parameter) | Table: Subnets

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Dhcp.Subnets[].EnableSubnet
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.100.1.200

Enables the subnet configuration. Activates the DHCP server on the subnet when enabled.

StartAddress (Config Parameter) | Table: Subnets

Type	IpAddr
Range	
Default	
Script/CLI	Dhcp.Subnets[].StartAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.100.1.300

Start address of the subnet range. It MUST be within the network interface's subnet.

EndAddress (Config Parameter) | Table: Subnets

Type	IpAddr
Range	
Default	
Script/CLI	Dhcp.Subnets[].EndAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.100.1.400

End address of the subnet range. It MUST be within the network interface's subnet and higher than or equal to the **StartAddress** value.

AutomaticConfigurationInterface (Config Parameter) | Table: Subnets

Type	Text
Range	Size(0..50)
Default	
Script/CLI	Dhcp.Subnets[].AutomaticConfigurationInterface
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.100.1.450

The network interface that provides the automatic configuration (E.g.: DNS servers, NTP server, etc.) to this subnet.

ConfigStatus (Status Parameter) | Table: Subnets

Type	Enum
Range	Disabled(100) | InvalidConfig(200) | Ok(300)
Script/CLI	Dhcp.Subnets[].ConfigStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.100.1.500

Subnet configuration status.

- Disabled: The **EnableSubnet** parameter is disabled or the **NetworkInterfaceName** parameter does not match a network interface that is Up.
- InvalidConfig: The start or end address range is out of the network interface's subnet, or both parameters are incompatible.
- Ok: The **EnableSubnet** parameter is enabled and the subnet configuration is valid.

Delete (Row Command) | Table: Subnets

Script/CLI:	Dhcp.Subnets[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.100.1.600

Deletes a row from the table.

DefaultDomainNameConfigSource (Config Parameter)

Type	Enum
Range	HostConfiguration(200) | Static(400)
Default	HostConfiguration
Script/CLI	Dhcp.DefaultDomainNameConfigSource
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.200.100

Default configuration source of all subnets.

- HostConfiguration: The domain name is the one used by the unit.
- Static: The domain name is specified in the **DefaultStaticDomainName** parameter.

DefaultStaticDomainName (Config Parameter)

Type	IpHostName
Range	
Default	
Script/CLI	Dhcp.DefaultStaticDomainName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.200.200

Default static domain name for all subnets.

SpecificDomainNames (Table: user-defined, 48 lines max.)

This table specifies subnet-specific domain names configurations. All subnets use the default configuration unless the **SpecificDomainNames.EnableConfig** parameter is set to 'Enable'.

The `Dhcp.AddSubnet` command may be used to add a new subnet to the **SubnetsTable** and to all subnet-specific configuration tables.

SubnetName (Index) | Table: SpecificDomainNames

Type	Text
Range	
Script/CLI	Dhcp.SpecificDomainNames[].SubnetName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.200.300.1.100

Name of the subnet.

EnableConfig (Config Parameter) | Table: SpecificDomainNames

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Dhcp.SpecificDomainNames[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.200.300.1.200

Defines the domain name configuration to use for this specific subnet.

- Disable: The subnet uses the default configuration as defined in the **DefaultDomainNameConfigSource** and **DefaultStaticDomainName** parameters.
- Enable: The subnet uses the specific configuration as defined in the **SpecificDomainNames.ConfigSource** and **SpecificDomainNames.StaticName** parameters.

The configuration is only valid when the **SpecificDomainNames.EnableOption** parameter is set to 'Enable'.

EnableOption (Config Parameter) | Table: SpecificDomainNames

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Dhcp.SpecificDomainNames[].EnableOption
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.200.300.1.300

Enables the domain name (option 15).

ConfigSource (Config Parameter) | Table: SpecificDomainNames

Type	Enum
Range	HostConfiguration(200) | Static(400)
Default	Static
Script/CLI	Dhcp.SpecificDomainNames[].ConfigSource
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.200.300.1.400

Subnet's domain name specific configuration source.

- HostConfiguration: The domain name is obtained from the host configuration.
- Static: The domain name is specified in the **StaticName** parameter.

This configuration overrides the default configuration set in the **DefaultDomainNameConfigSource** parameter when the **SpecificDomainNames.EnableConfig** parameter is set to 'Enable'.

StaticName (Config Parameter) | Table: SpecificDomainNames

Type	IpHostName
Range	
Default	
Script/CLI	Dhcp.SpecificDomainNames[].StaticName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.200.300.1.500

Static Domain Name Configuration. The **SpecificDomainNames.ConfigSource** parameter must be set to 'Static' for this value to be applied.

This configuration overrides the default configuration set in the **DefaultStaticDomainName** parameter when the **SpecificDomainNames.EnableConfig** parameter is set to 'Enable'.

DomainNamesInfo (Table)

This table contains the active subnets' domain names.

SubnetName (Index) | Table: DomainNamesInfo

Type	Text
Range	
Script/CLI	Dhcp.DomainNamesInfo[].SubnetName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.200.400.1.100

Name of the subnet.

DomainName (Status Parameter) | Table: DomainNamesInfo

Type	Text
Range	
Script/CLI	Dhcp.DomainNamesInfo[].DomainName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.200.400.1.200

Indicates the subnet's current domain name.

DefaultLeaseTime (Config Parameter)

Type	UInt32
Range	
Default	86400
Script/CLI	Dhcp.DefaultLeaseTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.300.100

Specifies the lease time (in seconds) default setting for all subnets.

SpecificLeaseTimes (Table: user-defined, 48 lines max.)

This table specifies subnet-specific lease times configurations. All subnets use the default configuration unless the **SpecificLeaseTimes.EnableConfig** parameter is set to 'Enable'.

The `Dhcp.AddSubnet` command may be used to add a new subnet to the **SubnetsTable** and to all subnet-specific configuration tables.

SubnetName (Index) | Table: SpecificLeaseTimes

Type	Text
Range	
Script/CLI	Dhcp.SpecificLeaseTimes[].SubnetName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.300.200.1.100

Name of the subnet.

EnableConfig (Config Parameter) | Table: SpecificLeaseTimes

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Dhcp.SpecificLeaseTimes[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.300.200.1.200

Defines the lease time configuration to use for this specific subnet.

- Disable: The subnet uses the default configuration as defined in the **DefaultLeaseTime** parameter.
- Enable: The subnet uses the specific configuration as defined in the **SpecificLeaseTimes.LeaseTime** parameter.

LeaseTime (Config Parameter) | Table: SpecificLeaseTimes

Type	UInt32
Range	
Default	86400
Script/CLI	Dhcp.SpecificLeaseTimes[].LeaseTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.300.200.1.300

Specifies the subnet's specific lease time in seconds.
This configuration overrides the default configuration set in the **DefaultLeaseTime** parameter when the **SpecificLeaseTimes.EnableConfig** parameter is set to 'Enable'.

LeaseTimesInfo (Table)

This table contains the active subnets' lease times.

SubnetName (Index) | Table: LeaseTimesInfo

Type	Text
Range	
Script/CLI	Dhcp.LeaseTimesInfo[].SubnetName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.300.300.1.100

Name of the subnet.

Default (Status Parameter) | Table: LeaseTimesInfo

Type	UInt32
Range	
Script/CLI	Dhcp.LeaseTimesInfo[].Default
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.300.300.1.200

Indicates the subnet's current default lease time in seconds.

SpecificDefaultRouters (Table: user-defined, 48 lines max.)

This table specifies subnet-specific default routers configurations.
The `Dhcp.AddSubnet` command may be used to add a new subnet to the **SubnetsTable** and to all subnet-specific configuration tables.

SubnetName (Index) | Table: SpecificDefaultRouters

Type	Text
Range	
Script/CLI	Dhcp.SpecificDefaultRouters[].SubnetName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.400.100.1.100

Name of the subnet.

EnableOption (Config Parameter) | Table: SpecificDefaultRouters

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Dhcp.SpecificDefaultRouters[].EnableOption
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.400.100.1.200

Enables the default router (option 3).

ConfigSource (Config Parameter) | Table: SpecificDefaultRouters

Type	Enum
Range	HostInterface(100) | Static(400)
Default	HostInterface
Script/CLI	Dhcp.SpecificDefaultRouters[].ConfigSource
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.400.100.1.300

The subnet's specific router configuration source.

- HostInterface: The default router is the host address within the client's subnet.
- Static: The default router is specified in the **SpecificDefaultRouters.StaticRouter** parameter.

StaticRouter (Config Parameter) | Table: SpecificDefaultRouters

Type	IpAddr
Range	
Default	
Script/CLI	Dhcp.SpecificDefaultRouters[].StaticRouter
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.400.100.1.400

Specifies the subnet's default router. The **SpecificDefaultRouters.ConfigSource** parameter must be set to 'Static' for this value to be applied.

DefaultRoutersInfo (Table)

This table contains the active subnets' default routers.

SubnetName (Index) | Table: DefaultRoutersInfo

Type	Text
Range	
Script/CLI	Dhcp.DefaultRoutersInfo[].SubnetName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.400.200.1.100

Name of the subnet.

DefaultRouter (Status Parameter) | Table: DefaultRoutersInfo

Type	IpAddr
Range	
Script/CLI	Dhcp.DefaultRoutersInfo[].DefaultRouter
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.400.200.1.200

Indicates the subnet's current default router.

DefaultDnsServersConfigSource (Config Parameter)

Type	Enum
Range	HostConfiguration(200) | Automatic(300) | Static(400)
Default	HostConfiguration
Script/CLI	Dhcp.DefaultDnsServersConfigSource
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.500.100

Default configuration source for the DNS servers of all subnets.

- HostConfiguration: The DNS servers are obtained from the host configuration.
- Automatic: The DNS servers are automatically obtained from the network configured in the **Subnets.AutomaticConfigurationInterface** parameter of this subnet.
- Static: The DNS servers are specified in the **DefaultStaticDnsServers** table.

DefaultStaticDnsServers (Table)

This table contains the list of default static DNS servers for all subnets. The DNS servers are sorted by priority. These DNS servers are used as the current DNS servers when the Default **DnsServersConfigSource** parameter is set to 'Static'.

Priority (Index) | Table: DefaultStaticDnsServers

Type	UInt32
Range	1..4
Script/CLI	Dhcp.DefaultStaticDnsServers[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.500.200.1.100

Priority number of this static DNS server. The lower the number is, the higher the priority is.

IpAddress (Config Parameter) | Table: DefaultStaticDnsServers

Type	IpAddr
Range	
Default	
Script/CLI	Dhcp.DefaultStaticDnsServers[].IpAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.500.200.1.200

Static DNS server's IP address.

SpecificDnsServers (Table: user-defined, 48 lines max.)

This table specifies subnet-specific DNS servers configurations. All subnets use the default configuration unless the **SpecificDnsServers.EnableConfig** parameter is set to 'Enable'.

The `Dhcp.AddSubnet` command may be used to add a new subnet to the **SubnetsTable** and to all subnet-specific configuration tables.

SubnetName (Index) | Table: SpecificDnsServers

Type	Text
Range	
Script/CLI	Dhcp.SpecificDnsServers[].SubnetName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.500.300.1.100

Name of the subnet.

EnableConfig (Config Parameter) | Table: SpecificDnsServers

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Dhcp.SpecificDnsServers[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.500.300.1.200

Defines the DNS servers configuration to use for this specific subnet.

- Disable: The subnet uses the default configuration as defined in the Default**DnsServersConfigSource** and **DefaultStaticDnsServers.IpAddress** parameters.
- Enable: The subnet uses the specific configuration as defined in the following parameters: **SpecificDnsServers.ConfigSource**, **SpecificDnsServers.StaticDns1**, **SpecificDnsServers.StaticDns2**, **SpecificDnsServers.StaticDns3**, and **SpecificDnsServers.StaticDns4**.

The configuration is only valid when the **SpecificDnsServers.EnableOption** parameter is set to 'Enable'.

EnableOption (Config Parameter) | Table: SpecificDnsServers

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Dhcp.SpecificDnsServers[].EnableOption
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.500.300.1.300

Enables the DNS servers (option 6).

ConfigSource (Config Parameter) | Table: SpecificDnsServers

Type	Enum
Range	HostConfiguration(200) | Automatic(300) | Static(400)
Default	Static
Script/CLI	Dhcp.SpecificDnsServers[].ConfigSource
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.500.300.1.400

DNS servers specific configuration source for the subnet.

- HostConfiguration: The DNS servers are obtained from the host configuration.
- Automatic: The DNS servers are automatically obtained from the network configured in the **Subnets.AutomaticConfigurationInterface** parameter of this subnet.
- Static: The DNS servers are specified in the **StaticDns** parameters of this table.

This configuration overrides the default configuration set in the Default**DnsServersConfigSource** parameter when the **SpecificDnsServers.EnableConfig** parameter is set to 'Enable'.

StaticDns1 (Config Parameter) | Table: SpecificDnsServers

Type	IpAddr
Range	
Default	
Script/CLI	Dhcp.SpecificDnsServers[].StaticDns1
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.500.300.1.500

IP address of the first DNS server of the subnet. The **SpecificDnsServers.ConfigSource** parameter must be set to 'Static' for this value to be applied.

This configuration overrides the default configuration set in the **DefaultStaticDnsServers.IpAddress** parameter when the **SpecificDnsServers.EnableConfig** parameter is set to 'Enable'.

StaticDns2 (Config Parameter) | Table: SpecificDnsServers

Type	IpAddr
Range	
Default	
Script/CLI	Dhcp.SpecificDnsServers[].StaticDns2
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.500.300.1.600

IP address of the second DNS server of the subnet. The **SpecificDnsServers.ConfigSource** parameter must be set to 'Static' for this value to be applied.

This configuration overrides the default configuration set in the **DefaultStaticDnsServers.IpAddress** parameter when the **SpecificDnsServers.EnableConfig** parameter is set to 'Enable'.

StaticDns3 (Config Parameter) | Table: SpecificDnsServers

Type	IpAddr
Range	
Default	
Script/CLI	Dhcp.SpecificDnsServers[].StaticDns3
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.500.300.1.700

IP address of the third DNS server of the subnet. The **SpecificDnsServers.ConfigSource** parameter must be set to 'Static' for this value to be applied.

This configuration overrides the default configuration set in the **DefaultStaticDnsServers.IpAddress** parameter when the **SpecificDnsServers.EnableConfig** parameter is set to 'Enable'.

StaticDns4 (Config Parameter) | Table: SpecificDnsServers

Type	IpAddr
Range	
Default	
Script/CLI	Dhcp.SpecificDnsServers[].StaticDns4
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.500.300.1.800

IP address of the fourth DNS server of the subnet. The **SpecificDnsServers.ConfigSource** parameter must be set to 'Static' for this value to be applied.

This configuration overrides the default configuration set in the **DefaultStaticDnsServers.IpAddress** parameter when the **SpecificDnsServers.EnableConfig** parameter is set to 'Enable'.

DnsServersInfo (Table)

This table contains the active subnets' DNS servers.

SubnetName (Index) | Table: DnsServersInfo

Type	Text
Range	
Script/CLI	Dhcp.DnsServersInfo[].SubnetName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.500.400.1.100

Name of the subnet.

Dns1 (Status Parameter) | Table: DnsServersInfo

Type	IpAddr
Range	
Script/CLI	Dhcp.DnsServersInfo[].Dns1
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.500.400.1.200

Indicates the subnets' first DNS server.

Dns2 (Status Parameter) | Table: DnsServersInfo

Type	IpAddr
Range	
Script/CLI	Dhcp.DnsServersInfo[].Dns2
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.500.400.1.300

Indicates the subnets' second DNS server.

Dns3 (Status Parameter) | Table: DnsServersInfo

Type	IpAddr
Range	
Script/CLI	Dhcp.DnsServersInfo[].Dns3
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.500.400.1.400

Indicates the subnets' third DNS server.

Dns4 (Status Parameter) | Table: DnsServersInfo

Type	IpAddr
Range	
Script/CLI	Dhcp.DnsServersInfo[].Dns4
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.500.400.1.500

Indicates the subnets' fourth DNS server.

DefaultNtpServersConfigSource (Config Parameter)

Type	Enum
Range	HostConfiguration(200) | Automatic(300) | Static(400)
Default	HostConfiguration
Script/CLI	Dhcp.DefaultNtpServersConfigSource
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.600.100

Default configuration source for the NTP servers of all subnets.

- HostConfiguration: The NTP servers are obtained from the host configuration.
- Automatic: The NTP servers are automatically obtained from the network configured in the **Subnets.AutomaticConfigurationInterface** parameter of this subnet.
- Static: The NTP servers are specified in the **DefaultStaticNtpServers** table.

DefaultStaticNtpServers (Table)

This table contains the list of default static NTP servers for all subnets. The NTP servers are sorted by priority. These NTP servers are used as the current NTP servers when the **DefaultNtpServersConfigSource** parameter is set to 'Static'.

Priority (Index) | Table: DefaultStaticNtpServers

Type	UInt32
Range	1..4
Script/CLI	Dhcp.DefaultStaticNtpServers[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.600.200.1.100

Priority number of this static NTP server. The lower the number is, the higher the priority is.

IpAddress (Config Parameter) | Table: DefaultStaticNtpServers

Type	IpAddr
Range	
Default	
Script/CLI	Dhcp.DefaultStaticNtpServers[].IpAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.600.200.1.200

NTP server's static IP address.

SpecificNtpServers (Table: user-defined, 48 lines max.)

This table specifies subnet-specific NTP servers configurations. All subnets use the default configuration unless the **SpecificNtpServers.EnableConfig** parameter is set to 'Enable'.

The `Dhcp.AddSubnet` command may be used to add a new subnet to the **SubnetsTable** and to all subnet-specific configuration tables.

SubnetName (Index) | Table: SpecificNtpServers

Type	Text
Range	
Script/CLI	Dhcp.SpecificNtpServers[].SubnetName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.600.300.1.100

Name of the subnet.

EnableConfig (Config Parameter) | Table: SpecificNtpServers

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Dhcp.SpecificNtpServers[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.600.300.1.200

Defines the NTP servers configuration to use for this specific subnet.

- Disable: The subnet uses the default configuration as defined in the **DefaultNtpServersConfigSource** and **DefaultStaticNtpServers.IpAddress** parameters.
- Enable: The subnet uses the specific configuration as defined in the following parameters: **SpecificNtpServers.ConfigSource**, **SpecificNtpServers.StaticNtp1**, **SpecificNtpServers.StaticNtp2**, **SpecificNtpServers.StaticNtp3**, and **SpecificNtpServers.StaticNtp4**.

The configuration is only valid when the **SpecificNtpServers.EnableOption** parameter is set to 'Enable'.

EnableOption (Config Parameter) | Table: SpecificNtpServers

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Dhcp.SpecificNtpServers[].EnableOption
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.600.300.1.300

Enables the NTP servers (option 42).

ConfigSource (Config Parameter) | Table: SpecificNtpServers

Type	Enum
Range	HostConfiguration(200) | Automatic(300) | Static(400)
Default	HostConfiguration
Script/CLI	Dhcp.SpecificNtpServers[].ConfigSource
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.600.300.1.400

NTP servers specific configuration source for the subnet.

- HostConfiguration: The NTP servers are obtained from the host configuration.
- Automatic: The NTP servers are automatically obtained from the network configured in the **Subnets.AutomaticConfigurationInterface** parameter of this subnet.
- Static: The NTP servers are specified in the **StaticNtp** parameters of this table.

This configuration overrides the default configuration set in the **DefaultNtpServersConfigSource** parameter when the **SpecificNtpServers.EnableConfig** parameter is set to 'Enable'.

StaticNtp1 (Config Parameter) | Table: SpecificNtpServers

Type	IpAddr
Range	
Default	
Script/CLI	Dhcp.SpecificNtpServers[].StaticNtp1
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.600.300.1.500

IP address of the first NTP server of the subnet. The **SpecificNtpServers.ConfigSource** parameter must be set to 'Static' for this value to be applied.

This configuration overrides the default configuration set in the **DefaultStaticNtpServers.IpAddress** parameter when the **SpecificNtpServers.EnableConfig** parameter is set to 'Enable'.

StaticNtp2 (Config Parameter) | Table: SpecificNtpServers

Type	IpAddr
Range	
Default	
Script/CLI	Dhcp.SpecificNtpServers[].StaticNtp2
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.600.300.1.600

IP address of the second NTP server of the subnet. The **SpecificNtpServers.ConfigSource** parameter must be set to 'Static' for this value to be applied.

This configuration overrides the default configuration set in the **DefaultStaticNtpServers.IpAddress** parameter when the **SpecificNtpServers.EnableConfig** parameter is set to 'Enable'.

StaticNtp3 (Config Parameter) | Table: SpecificNtpServers

Type	IpAddr
Range	
Default	
Script/CLI	Dhcp.SpecificNtpServers[].StaticNtp3
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.600.300.1.700

IP address of the third NTP server of the subnet. The **SpecificNtpServers.ConfigSource** parameter must be set to 'Static' for this value to be applied.

This configuration overrides the default configuration set in the **DefaultStaticNtpServers.IpAddress** parameter when the **SpecificNtpServers.EnableConfig** parameter is set to 'Enable'.

StaticNtp4 (Config Parameter) | Table: SpecificNtpServers

Type	IpAddr
Range	
Default	
Script/CLI	Dhcp.SpecificNtpServers[].StaticNtp4
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.600.300.1.800

IP address of the fourth NTP server of the subnet. The **SpecificNtpServers.ConfigSource** parameter must be set to 'Static' for this value to be applied.

This configuration overrides the default configuration set in the **DefaultStaticNtpServers.IpAddress** parameter when the **SpecificNtpServers.EnableConfig** parameter is set to 'Enable'.

NtpServersInfo (Table)

This table contains the active subnets's NTP servers.

SubnetName (Index) | Table: NtpServersInfo

Type	Text
Range	
Script/CLI	Dhcp.NtpServersInfo[].SubnetName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.600.400.1.100

Name of the subnet.

Ntp1 (Status Parameter) | Table: NtpServersInfo

Type	IpAddr
Range	
Script/CLI	Dhcp.NtpServersInfo[].Ntp1
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.600.400.1.200

Indicates the subnets' first NTP server.

Ntp2 (Status Parameter) | Table: NtpServersInfo

Type	IpAddr
Range	
Script/CLI	Dhcp.NtpServersInfo[].Ntp2
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.600.400.1.300

Indicates the subnets' second NTP server.

Ntp3 (Status Parameter) | Table: NtpServersInfo

Type	IpAddr
Range	
Script/CLI	Dhcp.NtpServersInfo[].Ntp3
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.600.400.1.400

Indicates the subnets' third NTP server.

Ntp4 (Status Parameter) | Table: NtpServersInfo

Type	IpAddr
Range	
Script/CLI	Dhcp.NtpServersInfo[].Ntp4
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.600.400.1.500

Indicates the subnets' fourth NTP server.

DefaultStaticNbnsServers (Table)

This table contains the list of default static NBNS servers for all subnets. The NBNS servers are sorted by priority.

Priority (Index) | Table: DefaultStaticNbnsServers

Type	UInt32
Range	1..4
Script/CLI	Dhcp.DefaultStaticNbnsServers[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.700.100.1.100

Priority number of this static NBNS server. The lower the number is, the higher the priority is.

IpAddress (Config Parameter) | Table: DefaultStaticNbnsServers

Type	IpAddr
Range	
Default	
Script/CLI	Dhcp.DefaultStaticNbnsServers[].IpAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.700.100.1.200

NBNS server's static IP address.

SpecificNbnsServers (Table: user-defined, 48 lines max.)

This table specifies subnet-specific NBNS servers configurations. All subnets use the default configuration unless the **SpecificNbnsServers.EnableConfig** parameter is set to 'Enable'.

The `Dhcp.AddSubnet` command may be used to add a new subnet to the **SubnetsTable** and to all subnet-specific configuration tables.

SubnetName (Index) | Table: SpecificNbnsServers

Type	Text
Range	
Script/CLI	Dhcp.SpecificNbnsServers[].SubnetName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.700.200.1.100

Name of the subnet.

EnableConfig (Config Parameter) | Table: SpecificNbnsServers

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Dhcp.SpecificNbnsServers[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.700.200.1.200

Defines the NBNS servers configuration to use for this specific subnet.

- Disable: The subnet uses the default configuration as defined in the **DefaultStaticNbnsServers.IpAddress** parameter.
- Enable: The subnet uses the specific configuration as defined in the following parameters: **SpecificNbnsServers.StaticNbns1**, **SpecificNbnsServers.StaticNbns2**, **SpecificNbnsServers.StaticNbns3**, and **SpecificNbnsServers.StaticNbns4**.

The configuration is only valid when the **SpecificNbnsServers.EnableOption** parameter is set to 'Enable'.

EnableOption (Config Parameter) | Table: SpecificNbnsServers

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Dhcp.SpecificNbnsServers[].EnableOption
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.700.200.1.300

Enables the NBNS servers (option 44).

StaticNbns1 (Config Parameter) | Table: SpecificNbnsServers

Type	IpAddr
Range	
Default	
Script/CLI	Dhcp.SpecificNbnsServers[].StaticNbns1
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.700.200.1.400

IP address of the first NBNS server of the subnet. The **SpecificNbnsServers.ConfigSource** parameter must be set to 'Static' for this value to be applied.

This configuration overrides the default configuration set in the **DefaultStaticNbnsServers.IpAddress** parameter when the **SpecificNbnsServers.EnableConfig** parameter is set to 'Enable'.

StaticNbns2 (Config Parameter) | Table: SpecificNbnsServers

Type	IpAddr
Range	
Default	
Script/CLI	Dhcp.SpecificNbnsServers[].StaticNbns2
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.700.200.1.500

IP address of the second NBNS server of the subnet. The **SpecificNbnsServers.ConfigSource** parameter must be set to 'Static' for this value to be applied.

This configuration overrides the default configuration set in the **DefaultStaticNbnsServers.IpAddress** parameter when the **SpecificNbnsServers.EnableConfig** parameter is set to 'Enable'.

StaticNbns3 (Config Parameter) | Table: SpecificNbnsServers

Type	IpAddr
Range	
Default	
Script/CLI	Dhcp.SpecificNbnsServers[].StaticNbns3
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.700.200.1.600

IP address of the third NBNS server of the subnet. The **SpecificNbnsServers.ConfigSource** parameter must be set to 'Static' for this value to be applied.

This configuration overrides the default configuration set in the **DefaultStaticNbnsServers.IpAddress** parameter when the **SpecificNbnsServers.EnableConfig** parameter is set to 'Enable'.

StaticNbns4 (Config Parameter) | Table: SpecificNbnsServers

Type	IpAddr
Range	
Default	
Script/CLI	Dhcp.SpecificNbnsServers[].StaticNbns4
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.700.200.1.700

IP address of the fourth NBNS server of the subnet. The **SpecificNbnsServers.ConfigSource** parameter must be set to 'Static' for this value to be applied.

This configuration overrides the default configuration set in the **DefaultStaticNbnsServers.IpAddress** parameter when the **SpecificNbnsServers.EnableConfig** parameter is set to 'Enable'.

NbnsServersInfo (Table)

This table contains the active subnets' NBNS servers.

SubnetName (Index) | Table: NbnsServersInfo

Type	Text
Range	
Script/CLI	Dhcp.NbnsServersInfo[].SubnetName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.700.300.1.100

Name of the subnet.

Nbns1 (Status Parameter) | Table: NbnsServersInfo

Type	IpAddr
Range	
Script/CLI	Dhcp.NbnsServersInfo[].Nbns1
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.700.300.1.200

Indicates the subnets' first NBNS server.

Nbns2 (Status Parameter) | Table: NbnsServersInfo

Type	IpAddr
Range	
Script/CLI	Dhcp.NbnsServersInfo[].Nbns2
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.700.300.1.300

Indicates the subnets' second NBNS server.

Nbns3 (Status Parameter) | Table: NbnsServersInfo

Type	IpAddr
Range	
Script/CLI	Dhcp.NbnsServersInfo[].Nbns3
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.700.300.1.400

Indicates the subnets' third NBNS server.

Nbns4 (Status Parameter) | Table: NbnsServersInfo

Type	IpAddr
Range	
Script/CLI	Dhcp.NbnsServersInfo[].Nbns4
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.700.300.1.500

Indicates the subnets' fourth NBNS server.

StaticLeases (Table: user-defined, 1000 lines max.)

This table specifies IP addresses that are reserved for specific hosts.

MacAddress (Index) | Table: StaticLeases

Type	Text
Range	
Script/CLI	Dhcp.StaticLeases[].MacAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.800.1.100

MAC address of the host.

IpAddress (Config Parameter) | Table: StaticLeases

Type	IpAddr
Range	
Default	
Script/CLI	Dhcp.StaticLeases[].IpAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.800.1.200

The reserved IP address of the host.

Delete (Row Command) | Table: StaticLeases

Script/CLI:	Dhcp.StaticLeases[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.800.1.300

Deletes a static lease from the table.

AssignedLeasesInfo (Table)

This table lists the IP addresses that are currently assigned.

IpAddress (Index) | Table: AssignedLeasesInfo

Type	IpAddr
Range	
Script/CLI	Dhcp.AssignedLeasesInfo[].IpAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.900.1.100

IP Address of the host.

MacAddress (Status Parameter) | Table: AssignedLeasesInfo

Type	Text
Range	
Script/CLI	Dhcp.AssignedLeasesInfo[].MacAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.900.1.200

MAC address of the host.

SubnetName (Status Parameter) | Table: AssignedLeasesInfo

Type	Text
Range	
Script/CLI	Dhcp.AssignedLeasesInfo[].SubnetName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.900.1.300

Indicates on which subnet the host is located.

LeaseTimeLeft (Status Parameter) | Table: AssignedLeasesInfo

Type	UInt32
Range	
Script/CLI	Dhcp.AssignedLeasesInfo[].LeaseTimeLeft
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.900.1.400

Indicates the lease time left in seconds.

DefaultStaticOption66 (Config Parameter)

Type	Text
Range	Size(0..120)
Default	
Script/CLI	Dhcp.DefaultStaticOption66
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.1000.100

Specifies the static value of Option 66 for all subnets.
When the parameter is empty, the option is not sent.

NOTE: Some characters are not allowed: Comma, Double quotes, Space or Pound.

DefaultStaticOption67 (Config Parameter)

Type	Text
Range	Size(0..120)
Default	
Script/CLI	Dhcp.DefaultStaticOption67
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.1000.200

Specifies the static value of Option 67 for all subnets.
When the parameter is empty, the option is not sent.

NOTE: Some characters are not allowed: Comma, Double quotes, Space or Pound.

SpecificOption66 (Table: user-defined, 48 lines max.)

This table contains the Option 66 for each subnet.

SubnetName (Index) | Table: SpecificOption66

Type	Text
Range	
Script/CLI	Dhcp.SpecificOption66[].SubnetName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.1000.1000.1.100

Name of the subnet.

EnableConfig (Config Parameter) | Table: SpecificOption66

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Dhcp.SpecificOption66[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.1000.1000.1.200

Defines the Option 66 configuration to use for this specific subnet.

- Disable: The subnet uses the default configuration as defined in the **DefaultStaticOption66** parameter.
- Enable: The subnet uses the specific configuration as defined in the **SpecificOption66.Value** parameter.

The configuration is only valid when the **SpecificOption66.EnableOption** parameter is set to 'Enable'.

EnableOption (Config Parameter) | Table: SpecificOption66

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Dhcp.SpecificOption66[].EnableOption
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.1000.1000.1.300

Enables the option 66 on this subnet.

Value (Config Parameter) | Table: SpecificOption66

Type	Text
Range	Size(0..120)
Default	
Script/CLI	Dhcp.SpecificOption66[].Value
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.1000.1000.1.400

Subnet's Option 66 specific value.
This configuration overrides the default configuration set in the **DefaultStaticOption66** parameter when the **SpecificOption66.EnableConfig** parameter is set to 'Enable'.

When the parameter is empty, the option is not sent.

NOTE: Some characters are not allowed: Comma, Double quotes, Space or Pound.

SpecificOption67 (Table: user-defined, 48 lines max.)

This table contains the Option 67 for each subnet. When empty, option 67 is not sent.

SubnetName (Index) | Table: SpecificOption67

Type	Text
Range	
Script/CLI	Dhcp.SpecificOption67[].SubnetName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.1000.1100.1.100

Name of the subnet.

EnableConfig (Config Parameter) | Table: SpecificOption67

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Dhcp.SpecificOption67[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.1000.1100.1.200

Defines the Option 67 configuration to use for this specific subnet.

- Disable: The subnet uses the default configuration as defined in the **DefaultStaticOption67** parameter.
- Enable: The subnet uses the specific configuration as defined in the **SpecificOption67.Value** parameter.

The configuration is only valid when the **SpecificOption67.EnableOption** parameter is set to 'Enable'.

EnableOption (Config Parameter) | Table: SpecificOption67

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Dhcp.SpecificOption67[].EnableOption
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.1000.1100.1.300

Enables the option 67 on this subnet.

Value (Config Parameter) | Table: SpecificOption67

Type	Text
Range	Size(0..120)
Default	
Script/CLI	Dhcp.SpecificOption67[].Value
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.1000.1100.1.400

Subnet's Option 67 specific value.
This configuration overrides the default configuration set in the **DefaultStaticOption67** parameter when the **SpecificOption67.EnableConfig** parameter is set to 'Enable'.

When the parameter is empty, the option is not sent.

NOTE: Some characters are not allowed: Comma, Double quotes, Space or Pound.

SubnetsStats (Table)

This table contains the statistics for each subnet.

SubnetName (Index) | Table: SubnetsStats

Type	Text
Range	
Script/CLI	Dhcp.SubnetsStats[].SubnetName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.10000.100.1.100

Name of the subnet.

NumberOfLeases (Status Parameter) | Table: SubnetsStats

Type	UInt32
Range	
Script/CLI	Dhcp.SubnetsStats[].NumberOfLeases
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.10000.100.1.200

Number of currently assigned leases.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Dhcp.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Dhcp.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1900.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

AddStaticLease (Command)

Adds a row to the **StaticLeases** table.

MacAddress (Argument) | Command: AddStaticLease

Type	Text
Range	Size(12)
Default	

MAC address of the host.

IpAddress (Argument) | Command: AddStaticLease

Type	IpAddr
Range	
Default	

The reserved IP address of the host

AddSubnet (Command)

Adds a row to the **SubnetsTable**.

Network (Argument) | Command: AddSubnet

Type	Text
Range	Size(1..50)
Default	

Network interfaces on which the DHCP server will be active. The interface must be up for the DHCP server to become active.

StartAddress (Argument) | Command: AddSubnet

Type	IpAddr
Range	
Default	

Start address of the subnet range. It MUST be within the network interface's subnet.

EndAddress (Argument) | Command: AddSubnet

Type	IpAddr
Range	
Default	

End address of the subnet range. It MUST be within the network interface's subnet and higher than or equal to the **StartAddress** parameter.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Dhcp service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.1900.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	The DHCP server has started on the %1$s network interface.	Info	This message is issued when the DHCP server starts on a network interface.
20	The DHCP server has stopped on the %1$s network interface.	Info	This message is issued when the DHCP server stops on a network interface.
30	A DHCP server configuration change has occurred on the %1$s network interface.	Info	This message is issued when the configuration is modified.
40	The %1$s address has been leased on the %2$s network interface.	Info	This message is issued when a lease is assigned to a host.
45	The %1$s address has been renewed on the %2$s network interface.	Info	This message is issued when a lease is renewed to a host.
50	The %1$s address assigned on the %2$s network interface has expired.	Info	This message is issued when a lease has expired.
80	The %1$s start IP address range is not compatible with the %2$s network interface's CIDR range. The default range start address will be applied.	Warning	This message is issued when the subnet range start address is not compatible with its assigned network interface's CIDR range.
90	The %1$s end IP address range is not compatible with the %2$s network interface CIDR range. The default range end address will be applied.	Warning	This message is issued when the subnet range end address is not compatible with its assigned network interface's CIDR range.
100	The start and end IP addresses ranges are not compatible. The %1$s network interface CIDR range will be applied.	Warning	This message is issued when the subnet range end address entry is not greater than the subnet range start address.

NumKey	Message	Severity	Description
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.

NumKey	Message	Severity	Description
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Dhcp.

Message	Severity	Description
A DHCP subnet is already defined on network interface %1$s.	Error	This message is issued when a new subnet is added to the subnets table, but the interface on which it will be running already has a DHCP server running.
The DHCP server static lease is already defined for MAC address %1$s.	Error	This message is issued when a new static lease is added to the static leases table, but an entry already has the same index in that table.
The syntax of the entered subnet range start address is wrong: %1$s	Error	This message is issued when executing the `AddSubnet` command and the syntax of the entered subnet range start address is wrong.
The syntax of the entered subnet range end address is wrong: %1$s	Error	This message is issued when executing the `AddSubnet` command and the syntax of the entered subnet range end address is wrong.
The syntax of the entered static lease MAC address is wrong: %1$s	Error	This message is issued when executing the `AddStaticLease` command and the syntax of the entered static lease MAC address is wrong.
The syntax of the entered static lease IP address is wrong: %1$s	Error	This message is issued when executing the `AddStaticLease` command and the syntax of the entered static lease IP address is wrong.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.

Message	Severity	Description
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

E&M Channel Associated Signaling (Eam)

The E&M Channel Associated Signaling (EAM) service manages the E&M CAS telephony interfaces.

Parameters

Eam (Table)

Configuration parameters related to the E&M channel associated signaling on this managed device.

Name (Index) | Table: Eam

Type	Text
Range	
Script/CLI	Eam.Eam[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.100.1.100

Name that identifies the interface.

ChannelRange (Config Parameter) | Table: Eam

Type	Text
Range	Size(1..10)
Default	1-24
Script/CLI	Eam.Eam[].ChannelRange
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.100.1.200

Defines the range of active bearer channels.

ChannelAllocationStrategy (Config Parameter) | Table: Eam

Type	Enum
Range	Ascending(100) | Descending(200) | RoundRobinAscending(300) | RoundRobinDescending(400)
Default	Ascending
Script/CLI	Eam.Eam[].ChannelAllocationStrategy
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.100.1.300

Defines the strategy for selecting bearer channels. Available strategies are:

- Ascending: select the lowest-numbered non-busy bearer channel
- Descending: select the highest-numbered non-busy bearer channel
- RoundRobinAscending: use a cyclic round-robin search; starting from the bearer channel that follows the bearer channel used for the last call, select the lowest-numbered non-busy bearer channel
- RoundRobinDescending: use a cyclic round-robin search; starting from the bearer channel that precedes the bearer channel used for the last call, select the highest-numbered non-busy bearer channel

MaxActiveCalls (Config Parameter) | Table: Eam

Type	UInt32
Range	0..30
Default	0
Script/CLI	Eam.Eam[].MaxActiveCalls
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.100.1.400

Defines the maximum number of active calls on the interface.
Note: The special value 0 indicates no maximum number of active calls.

EncodingScheme (Config Parameter) | Table: Eam

Type	Enum
Range	G711alaw(100) | G711ulaw(200)
Default	G711alaw
Script/CLI	Eam.Eam[].EncodingScheme
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.100.1.500

Defines the voice encoding scheme in the bearer capabilities.

SignalingType (Config Parameter) | Table: Eam

Type	Enum
Range	WinkStart(100) | ImmediateStart(200) | Fgb(300) | Fgd(400)
Default	WinkStart
Script/CLI	Eam.Eam[].SignalingType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.100.1.600

Identifies the E&M signaling type.

- E&M Wink start: Set configuration parameters for basic Wink Start signaling. After setting **SignalingType**, individual configuration parameters can be overriden for detail adjustment.
- E&M Immediate Start: Set configuration parameters for basic Immediate Start signaling. After setting **SignalingType**, individual configuration parameters can be overriden for detail adjustment.
- E&M Feature Group B: Set configuration parameters for the Feature Group B signaling defined by National Exchange Carrier Association. After setting **SignalingType**, individual configuration parameters can be overriden for detail adjustment.
- E&M Feature Group D: Set configuration parameters for the Feature Group D signaling defined by National Exchange Carrier Association. After setting **SignalingType**, individual configuration parameters can be overriden for detail adjustment.

DigitAttenuation (Config Parameter) | Table: Eam

Type	UInt32
Range	0..20
Default	0
Script/CLI	Eam.Eam[].DigitAttenuation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.100.1.700

Additional attenuation in dB for MFR1/DTMF digits generation. By default, MFR1/DTMF digits generation power is determined by variant selection. This parameter provides a mean to reduce this power.

EamSignalingVariants (Table)

This table allows to override or retrieve the default signaling settings for E&M signaling parameters. This table is effective only if the **OverrideDefault** parameter is Enabled. If the **OverrideDefault** parameter is Disabled, any change in this table has no effects.

InterfaceName (Index) | Table: EamSignalingVariants

Type	Text
Range	
Script/CLI	Eam.EamSignalingVariants[].InterfaceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.200.1.100

Identifies the interface.

OverrideDefault (Config Parameter) | Table: EamSignalingVariants

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Eam.EamSignalingVariants[].OverrideDefault
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.200.1.200

Overrides the default settings of E&M Signaling parameters for the **SignalingType** and **InterfaceName**.

- Disable: The interface uses the default configuration associated with the selected Signaling Type. The configuration set in the current row has no effect on the default configuration of the selected Signaling Type. Refer to the technical documentation to get the default configurations of the various Signaling Types.
- Enable: The interface uses the specific signaling configuration as defined in the current row. To retrieve the default configuration associated with the current Signaling Type, the command implemented by the **ResetSpecific** parameter MUST be issued.

BitsBCD (Config Parameter) | Table: EamSignalingVariants

Type	Int32
Range	0..8
Default	8
Script/CLI	Eam.EamSignalingVariants[].BitsBCD
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.200.1.300

Settings of the B, C and D bits when the device transmits line signals. B, C and D bits of received line signals are ignored by the device.
BCD bits definition

- 0..7: BCD bits are set to the specified value.
- 8: BCD bits follow the A bit.

Note: On E1-CAS, the ABCD bits pair cannot be set to '0000'. If the BCD bits pair is set to '000' or to follow the A bit, then the BCD bits pair is set to '001' instead.

DnisLength (Config Parameter) | Table: EamSignalingVariants

Type	UInt32
Range	0..20
Default	0
Script/CLI	Eam.EamSignalingVariants[].DnisLength
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.200.1.400

Defines the expected length of the DNIS. DNIS (Dialed Number Identification Service) is the called party or the destination number.

- 0: Variable DNIS length used.
- 1..20: Number indicates the specific DNIS length expected.

AniLength (Config Parameter) | Table: EamSignalingVariants

Type	UInt32
Range	0..20
Default	0
Script/CLI	Eam.EamSignalingVariants[].AniLength
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.200.1.500

Defines the expected length of the ANI. ANI (Automatic Number Identification) is the number of the calling party.

- 0 : Variable ANI length.
- 1..20 : Specific ANI length.

IncomingRegisterSignaling (Config Parameter) | Table: EamSignalingVariants

Type	Enum
Range	MfR1(100) | Dtmf(200)
Default	Dtmf
Script/CLI	Eam.EamSignalingVariants[].IncomingRegisterSignaling
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.200.1.600

Defines the incoming register signaling method.

- MfR1: Multi Frequency - R1.
- Dtmf: Dual Tone Multi Frequency.

OutgoingRegisterSignaling (Config Parameter) | Table: EamSignalingVariants

Type	Enum
Range	MfR1(100) | Dtmf(200)
Default	Dtmf
Script/CLI	Eam.EamSignalingVariants[].OutgoingRegisterSignaling
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.200.1.700

Defines the outgoing register signaling method.

- MfR1: Multi Frequency - R1.
- Dtmf: Dual Tone Multi Frequency.

IncomingDialMap (Config Parameter) | Table: EamSignalingVariants

Type	Text
Range	SIZE(0..255)
Default	%dnis%t
Script/CLI	Eam.EamSignalingVariants[].IncomingDialMap
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.200.1.800

Defines the dial map expression to match against on the incoming side. The dial map expression uses a special format using macros that enables the user to construct a custom dial map using the ANI, DNIS and other special tones as separator.
Dial map macros:

- %dnis : DNIS (Dialed Number Identification Service).
- %ani : ANI (Automatic Number Identification).
- %kp : KP (start-of-pulsing) tone (MF R1 only).
- %st : ST (end-of-pulsing) tone (MF R1 only).
- %t : Interdigit timeout.
- A,B,C,D,*,# : Control tones (DTMF only).
- A,B,C,D,E : Control tones (MF R1 only).

Examples:

- %dnis*%ani : (dnis)*(ani)
- %kp%dnis%st%kp%ani%st : KP(dnis)STKP(ani)ST
- A%dnisBA%aniB : A(dnis)BA(ani)B

OutgoingDialMap (Config Parameter) | Table: EamSignalingVariants

Type	Text
Range	SIZE(0..255)
Default	%dnis%t
Script/CLI	Eam.EamSignalingVariants[].OutgoingDialMap
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.200.1.900

Defines the dial map format for the outgoing dial string. The dial string generation uses a special format using macros that enables the user to construct a custom dial string using the ANI, DNIS and other specials tones used as separator. The dial string uses regular expression to replace the macros with the proper call parameter value.
Dial map macros:

- %dnis : DNIS (Dialed Number Identification Service).
- %ani : ANI (Automatic Number Identification).
- %kp : KP (start-of-pulsing) tone (MF R1 only).
- %st : ST (end-of-pulsing) tone (MF R1 only).
- %t : Interdigit timeout.
- A,B,C,D,*,# : Control tones (DTMF only).
- A,B,C,D,E : Control tones (MF R1 only).

Examples : ANI=1234 DNIS=6789 KP=A ST=D

- %dnis*%ani : 6789*1234
- %kp%dnis%st%kp%ani%st : A6789DA1234D
- A%dnisBA%aniB : A6789BA1234B

WaitWink (Config Parameter) | Table: EamSignalingVariants

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Eam.EamSignalingVariants[].WaitWink
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.200.1.1000

Defines whether or not the outgoing register should wait for a wink before proceeding with digit transmission.

WaitWinkAck (Config Parameter) | Table: EamSignalingVariants

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Eam.EamSignalingVariants[].WaitWinkAck
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.200.1.1100

Defines whether or not the outgoing register should wait for a wink acknowledge after all digit reception.

SendWink (Config Parameter) | Table: EamSignalingVariants

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Eam.EamSignalingVariants[].SendWink
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.200.1.1200

Defines whether or not the incoming register should send a wink to notify the remote side that digit information can be sent.

SendWinkAck (Config Parameter) | Table: EamSignalingVariants

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Eam.EamSignalingVariants[].SendWinkAck
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.200.1.1300

Defines whether or not the incoming register should send a wink to acknowledge the receipt of all digits.

ResetSpecific (Row Command) | Table: EamSignalingVariants

Script/CLI:	Eam.EamSignalingVariants[].ResetSpecific
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.200.1.2000

Resets specific settings of E&M Signaling parameters with the default signaling settings. This command is used to retrieve the default configuration of the selected Signaling Type set in the **SignalingType** parameter.

EamTimerVariants (Table)

This table allows to override or retrieve the default signaling setting for E&M Timers.

InterfaceName (Index) | Table: EamTimerVariants

Type	Text
Range	
Script/CLI	Eam.EamTimerVariants[].InterfaceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.300.1.100

Identifies the interface.

OverrideDefault (Config Parameter) | Table: EamTimerVariants

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Eam.EamTimerVariants[].OverrideDefault
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.300.1.200

Overrides the default settings of E&M Signaling parameters for the **SignalingType** and **InterfaceName**.

- Disable: The interface uses the default configuration associated with the selected Signaling Type. The configuration set in the current row has no effect on the default configuration of the selected Signaling Type. Refer to the technical documentation to get the default configurations of the various Signaling Types.
- Enable: The interface uses the specific signaling configuration as defined in the current row. To retrieve the default configuration associated with the current Signaling Type, the command implemented by the **ResetSpecific** parameter MUST be issued.

BwdWaitPreWinkTimeout (Config Parameter) | Table: EamTimerVariants

Type	Int32
Range	0..2000
Default	50
Script/CLI	Eam.EamTimerVariants[].BwdWaitPreWinkTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.300.1.300

Amount of time an incoming register waits before sending the wink that acknowledges the seizure. This value is expressed in milliseconds (ms).

BwdSendWinkTimeout (Config Parameter) | Table: EamTimerVariants

Type	Int32
Range	0..5000
Default	200
Script/CLI	Eam.EamTimerVariants[].BwdSendWinkTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.300.1.400

Duration of the wink signal applied by the incoming register to signal seizure acknowledgment. This value is expressed in milliseconds (ms).

BwdWait1stDigitTimeout (Config Parameter) | Table: EamTimerVariants

Type	Int32
Range	0..20000
Default	10000
Script/CLI	Eam.EamTimerVariants[].BwdWait1stDigitTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.300.1.500

Maximum time an incoming register waits for the first incoming digit after the line seizure. This value is expressed in milliseconds (ms).

BwdClearBackwardTimeout (Config Parameter) | Table: EamTimerVariants

Type	Int32
Range	0..30000
Default	2000
Script/CLI	Eam.EamTimerVariants[].BwdClearBackwardTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.300.1.600

The maximum time an incoming register waits after sending a clear backward line signal before transiting to the idle state.
This value is expressed in milliseconds (ms).

BwdDigitCompleteTimeout (Config Parameter) | Table: EamTimerVariants

Type	Int32
Range	0..15000
Default	4000
Script/CLI	Eam.EamTimerVariants[].BwdDigitCompleteTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.300.1.700

The maximum time the incoming register waits for the next digit before considering the digit sequence as completed.
This value is expressed in milliseconds (ms).

FwdWaitWinkTimeout (Config Parameter) | Table: EamTimerVariants

Type	Int32
Range	0..10000
Default	5000
Script/CLI	Eam.EamTimerVariants[].FwdWaitWinkTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.300.1.800

Maximum time an outgoing register waits for seizure acknowledgement after seizing the line.
This value is expressed in milliseconds (ms).

FwdWaitMaxWinkOnTimeout (Config Parameter) | Table: EamTimerVariants

Type	Int32
Range	0..10000
Default	5000
Script/CLI	Eam.EamTimerVariants[].FwdWaitMaxWinkOnTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.300.1.900

The maximum time an outgoing register waits for the seizure acknowledgment wink to complete.
This value is expressed in milliseconds (ms).

FwdWaitPreDialTimeout (Config Parameter) | Table: EamTimerVariants

Type	Int32
Range	0..5000
Default	140
Script/CLI	Eam.EamTimerVariants[].FwdWaitPreDialTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.300.1.1000

The amount of time an outgoing register waits after the wink to start dialing.
This value is expressed in milliseconds (ms).

FwdWaitAnswerTimeout (Config Parameter) | Table: EamTimerVariants

Type	Int32
Range	0..300000
Default	180000
Script/CLI	Eam.EamTimerVariants[].FwdWaitAnswerTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.300.1.1100

The maximum time an outgoing register waits for the call to be answered.
This value is expressed in milliseconds (ms).

FwdClearForwardTimeout (Config Parameter) | Table: EamTimerVariants

Type	Int32
Range	0..30000
Default	2000
Script/CLI	Eam.EamTimerVariants[].FwdClearForwardTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.300.1.1200

The maximum time an outgoing register waits after sending a clear forward line signal before transiting to the idle state.
This value is expressed in milliseconds (ms).

ReleaseGuardTimeout (Config Parameter) | Table: EamTimerVariants

Type	Int32
Range	0..10000
Default	200
Script/CLI	Eam.EamTimerVariants[].ReleaseGuardTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.300.1.1300

Maximum time a register waits after sending an idle line signal to prevent a new seizure of the line. This value is expressed in milliseconds (ms).

ResetSpecific (Row Command) | Table: EamTimerVariants

Script/CLI:	Eam.EamTimerVariants[].ResetSpecific
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.300.1.1900

Resets specific settings of E&M Timers parameters with the default signaling type settings. This command is used to retrieve the default configuration of the selected Signaling Type set in the **SignalingType** parameter.

EamDigitTimerVariants (Table)

This table allows to override or retrieve the default signaling type setting for E&M Digit Timers.

InterfaceName (Index) | Table: EamDigitTimerVariants

Type	Text
Range	
Script/CLI	Eam.EamDigitTimerVariants[].InterfaceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.400.1.100

Identifies the interface.

OverrideDefault (Config Parameter) | Table: EamDigitTimerVariants

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Eam.EamDigitTimerVariants[].OverrideDefault
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.400.1.200

Overrides the default settings of E&M Signaling parameters for the **SignalingType** and **InterfaceName**.

- Disable: The interface uses the default configuration associated with the selected Signaling Type. The configuration set in the current row has no effect on the default configuration of the selected Signaling Type. Refer to the technical documentation to get the default configurations of the various Signaling Types.
- Enable: The interface uses the specific signaling configuration as defined in the current row. To retrieve the default configuration associated with the current Signaling Type, the command implemented by the **ResetSpecific** parameter MUST be issued.

KPOnTimeout (Config Parameter) | Table: EamDigitTimerVariants

Type	Int32
Range	0..10000
Default	100
Script/CLI	Eam.EamDigitTimerVariants[].KPOnTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.400.1.300

The time during which the MF R1 KP tone is on.
This value is expressed in milliseconds (ms).

KPOffTimeout (Config Parameter) | Table: EamDigitTimerVariants

Type	Int32
Range	0..10000
Default	68
Script/CLI	Eam.EamDigitTimerVariants[].KPOffTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.400.1.400

The duration of the pause after the MF R1 KP tone.
This value is expressed in milliseconds (ms).

ResetSpecific (Row Command) | Table: EamDigitTimerVariants

Script/CLI:	Eam.EamDigitTimerVariants[].ResetSpecific
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.400.1.900

Resets specific settings of E&M Digit Timers parameters with the default signaling type settings. This command is used to retrieve the default configuration of the selected Signaling Type set in the **SignalingType** parameter.

EamLinkTimerVariants (Table)

This table allows to override or retrieve the default signaling type setting for E&M Link Timers.

InterfaceName (Index) | Table: EamLinkTimerVariants

Type	Text
Range	
Script/CLI	Eam.EamLinkTimerVariants[].InterfaceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.500.1.100

Identifies the interface.

OverrideDefault (Config Parameter) | Table: EamLinkTimerVariants

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Eam.EamLinkTimerVariants[].OverrideDefault
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.500.1.200

Overrides the default settings of E&M Signaling parameters for the **SignalingType** and **InterfaceName**.

- Disable: The interface uses the default configuration associated with the selected Signaling Type. The configuration set in the current row has no effect on the default configuration of the selected Signaling Type. Refer to the technical documentation to get the default configurations of the various Signaling Types.
- Enable: The interface uses the specific signaling configuration as defined in the current row. To retrieve the default configuration associated with the current Signaling Type, the command implemented by the **ResetSpecific** parameter MUST be issued.

LinkActivationTimeout (Config Parameter) | Table: EamLinkTimerVariants

Type	Int32
Range	0..10000
Default	1000
Script/CLI	Eam.EamLinkTimerVariants[].LinkActivationTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.500.1.300

The maximum time the unit waits for an activation indication coming from the physical link. The activation indication is used to indicate that the physical layer connection has been activated. This value is expressed in milliseconds (ms).

LinkActivationRetryTimeout (Config Parameter) | Table: EamLinkTimerVariants

Type	Int32
Range	0..10000
Default	3000
Script/CLI	Eam.EamLinkTimerVariants[].LinkActivationRetryTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.500.1.400

The maximum time the unit waits before attempting to reestablish the physical link. The attempt is made when the physical layer connection has been deactivated.
This value is expressed in milliseconds (ms).

ResetSpecific (Row Command) | Table: EamLinkTimerVariants

Script/CLI:	Eam.EamLinkTimerVariants[].ResetSpecific
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.500.1.900

Resets specific settings of E&M Link Timers parameters with the default signaling settings. This command is used to retrieve the default signaling configuration set in the **SignalingType** parameter.

EamToneVariants (Table)

This table allows to override or retrieve the default signaling setting for E&M Tone variants.

InterfaceName (Index) | Table: EamToneVariants

Type	Text
Range	
Script/CLI	Eam.EamToneVariants[].InterfaceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.600.1.100

Identifies the interface.

OverrideDefault (Config Parameter) | Table: EamToneVariants

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Eam.EamToneVariants[].OverrideDefault
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.600.1.200

Overrides the default settings of E&M Signaling parameters for the **SignalingType** and **InterfaceName**.

- Disable: The interface uses the default configuration associated with the selected Signaling Type. The configuration set in the current row has no effect on the default configuration of the selected Signaling Type. Refer to the technical documentation to get the default configurations of the various Signaling Types.
- Enable: The interface uses the specific signaling configuration as defined in the current row. To retrieve the default configuration associated with the current Signaling Type, the command implemented by the **ResetSpecific** parameter MUST be issued.

KpTone (Config Parameter) | Table: EamToneVariants

Type	Enum
Range	None(100) | MF0(200) | MF1(300) | MF2(400) | MF3(500) | MF4(600) | MF5(700) | MF6(800) | MF7(900) | MF8(1000) | MF9(1100) | MF10(1200) | MF11(1300) | MF12(1400) | MF13(1500) | MF14(1600)
Default	MF10
Script/CLI	Eam.EamToneVariants[].KpTone
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.600.1.300

Specifies the KP (start-of-pulsing) signal.

- None : No tone used.
- MF0..MF14 : MF R1 Tone

StTone (Config Parameter) | Table: EamToneVariants

Type	Enum
Range	None(100) | MF0(200) | MF1(300) | MF2(400) | MF3(500) | MF4(600) | MF5(700) | MF6(800) | MF7(900) | MF8(1000) | MF9(1100) | MF10(1200) | MF11(1300) | MF12(1400) | MF13(1500) | MF14(1600)
Default	MF13
Script/CLI	Eam.EamToneVariants[].StTone
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.600.1.400

Specifies the ST (end-of-pulsing) signal.

- None : No tone used.
- MF0..MF14 : MF R1 Tone

ResetSpecific (Row Command) | Table: EamToneVariants

Script/CLI:	Eam.EamToneVariants[].ResetSpecific
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.100.600.1.900

Resets specific settings of E&M Tones parameters with the default signaling settings. This command is used to retrieve the default signaling configuration set in the **SignalingType** parameter.

BearerChannelInfo (Table)

Port-specific operational, statistics, and active call data for B channels.

Index (Index) | Table: BearerChannelInfo

Type	Text
Range	
Script/CLI	Eam.BearerChannelInfo[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.200.100.1.100

Identifies the Bearer Channel..

State (Status Parameter) | Table: BearerChannelInfo

Type	Enum
Range	Idle(100) | InUse(200) | Maintenance(300) | Error(400) | Disabled(500)
Script/CLI	Eam.BearerChannelInfo[].State
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.200.100.1.200

The current call control state for this channel:

- Idle: The channel is available
- InUse: The channel is currently used
- Maintenance: Maintenance state, temporarily unavailable
- Error: Error on this channel
- Disabled: The channel is disabled

PhysicalLinkInfo (Table)

The physical link information table contains status information for all interfaces on this managed device.

InterfaceName (Index) | Table: PhysicalLinkInfo

Type	Text
Range	
Script/CLI	Eam.PhysicalLinkInfo[].InterfaceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.300.100.1.100

Identifies the interface.

State (Status Parameter) | Table: PhysicalLinkInfo

Type	Enum
Range	Up(100) | Down(200)
Script/CLI	Eam.PhysicalLinkInfo[].State
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.300.100.1.200

The layer 1 state for this interface:

- Up: Layer 1 connectivity.
- Down: No layer 1 connectivity. The interface might be in this state because no cable is plugged in or a pinout problem is detected.

PhysicalLink (Table)

The physical link table containing configuration and operational parameters for all interfaces on this managed device.

InterfaceName (Index) | Table: PhysicalLink

Type	Text
Range	
Script/CLI	Eam.PhysicalLink[].InterfaceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.300.200.1.100

Identifies the interface.

LineCoding (Config Parameter) | Table: PhysicalLink

Type	Enum
Range	B8zs(100) | Hdb3(200) | Ami(300)
Default	B8zs
Script/CLI	Eam.PhysicalLink[].LineCoding
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.300.200.1.200

Defines the transmission encoding of bits:

- B8ZS: Bipolar with 8-Zeros Substitution (T1 lines)
- HDB3: High-Density Bipolar with 3-zeros (E1 lines)
- AMI: Alternate Mark Inversion (E1 and T1 lines)

For further information, see ITU-T Recommendation G.703.

LineFraming (Config Parameter) | Table: PhysicalLink

Type	Enum
Range	Sf(100) | Esf(200) | Crc4(300) | NoCrc4(400)
Default	Esf
Script/CLI	Eam.PhysicalLink[].LineFraming
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.300.200.1.300

Defines the frame format:

- SF: Super frame. Sometimes known as D4 (T1 lines)
- ESF: Extended super frame (T1 lines)
- CRC4: Cyclic redundancy check 4 (E1 lines)
- NO-CRC4: No Cyclic redundancy check 4 (E1 lines)

For further information, see ITU-T Recommendation G.704.

ClockMode (Config Parameter) | Table: PhysicalLink

Type	Enum
Range	Master(100) | Slave(200)
Default	Slave
Script/CLI	Eam.PhysicalLink[].ClockMode
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.300.200.1.400

A port can either generate the clocking for the line or accept the clock from the line. The options master or slave determine the clocking method:

- Master: Generates clock
- Slave: Accepts clock

MonitorLinkStateEnable (Config Parameter) | Table: PhysicalLink

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Eam.PhysicalLink[].MonitorLinkStateEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.300.200.1.500

Monitors the physical link state of an E&M interface.
Enable: An E&M endpoint's operational state is affected by its interface physical link state. When the link state of an E&M interface is down, the operational state of its matching endpoint becomes "disable".

Disable: An E&M endpoint's operational state is not affected by its interface physical link state.

PortPinout (Config Parameter) | Table: PhysicalLink

Type	Enum
Range	Auto(100) | Master(200) | Slave(300)
Default	Auto
Script/CLI	Eam.PhysicalLink[].PortPinout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.300.200.1.600

Defines the port pinout:

- Auto: The pinout is set according to the clock mode.
- Master: Force the pinout to Master regardless of the clock mode.
- Slave: Force the pinout to Slave regardless of the clock mode.

See the **PhysicalLink.ClockMode** parameter for a description of the clock mode.

AutoConfigureStatus (Status Parameter)

Type	Enum
Range	Idle(100) | Sensing(200)
Script/CLI	Eam.AutoConfigureStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.400.100

Indicates the current status of the E&M automatic configuration mechanism.

- Idle: The automatic configuration mechanism is ready to be started.
- Sensing: The automatic configuration mechanism is currently started and is testing different E&M configurations to obtain a link up.

LastAutoConfigureResult (Status Parameter)

Type	Enum
Range	None(100) | Success(200) | Fail(300) | Aborted(400)
Script/CLI	Eam.LastAutoConfigureResult
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.400.200

Result of the last E&M automatic configuration.

- None: No result is available.
- Success: The last automatic configuration succeeded.
- Fail: The last automatic configuration failed.
- Aborted: The last automatic configuration has been cancelled by the user.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Eam.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Eam.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1880.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

AutoConfigure (Command)

Auto-detect and auto-configure the E&M interfaces.

Interface (Argument) | Command: AutoConfigure

Type	Text
Range	Size(0..48)
Default	

The specific E&M Interface on which the AutoConfigure command will be executed. See the **Eam.PhysicalLinkInfo** table for the exact interface name to use. Take note that the argument value is case-sensitive.
This argument is optional. If no value is provided, the command will be executed on all E&M interfaces.

CancelAutoConfigure (Command)

Stops and cancels the automatic detection and configuration mechanism.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Eam service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.1880.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
5	%1$s: Physical link state changed to up.	Info	The physical link state has changed to up.
10	%1$s: Physical link state changed to down.	Info	The physical link state has changed to down.
15	%1$s, channel %2$d: State changed to free.	Info	The channel state has changed to free.
20	%1$s, channel %2$d: State changed to used.	Info	The channel state has changed to used.
25	%1$s: Graceful lock initiated.	Info	A graceful lock has been initiated.
30	%1$s: Abrupt lock initiated.	Info	An abrupt lock has been initiated.
35	%1$s: Locked successfully.	Info	Locked successfully.
40	%1$s, Unlocked successfully.	Info	Unlocked successfully.
45	%1$s: Cannot allocate channel, line is locked.	Warning	The unit cannot allocate a channel because the line is locked.
48	%1$s: The unit cannot allocate a DSP channel to process the call: all DSP resources are currently in use.	Warning	The unit rejected the call: the endpoint could not allocate a DSP channel to process the call.
50	%1$s: Cannot allocate channel, maximum number of calls (%2$d) reached.	Warning	The unit cannot allocate a channel because the maximum number of calls has been reached.
55	%1$s: E&M frame slip detected.	Warning	This message is issued when the physical link detects a frame slip. This happens when there is a problem with clock synchronization.
60	%1$s: Received unhandled E&M message %2$s.	Warning	Received an unhandled E&M message.
65	%1$s, interface %2$d, channel %3$d: Requested number %4$s does not match any dial map.	Info	The requested number does not match any dial map.

NumKey	Message	Severity	Description
70	Cannot find a E&M interface for outgoing call.	Info	Cannot find a E&M interface for outgoing call.
100	The E&M auto-configuration process has started.	Info	An auto-configuration process has started on E&M interfaces.
110	The E&M auto-configuration process has been cancelled.	Info	The E&M auto-configuration process has been cancelled by the user.
120	The E&M auto-configuration process has completed successfully.	Info	The E&M auto-configuration process has completed successfully. NOTE: This does not mean that the auto-configuration process has succeeded on all interfaces.
130	The E&M auto-configuration process has failed.	Error	The E&M auto-configuration process has terminated because of an error.
140	%1$s: Auto-configuration has succeeded.	Info	The auto-configuration process has succeeded on the specified E&M interface.
150	%1$s: Auto-configuration has failed.	Error	The auto-configuration process has failed on the specified E&M interface.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.

NumKey	Message	Severity	Description
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.

NumKey	Message	Severity	Description
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Eam.

Message	Severity	Description
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.

Message	Severity	Description
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Element Management System (Ems)

The Element Management System (Ems) service makes the unit compatible with the Virtuo EMS infrastructure.

Parameters

EmsProvisioningEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Ems.EmsProvisioningEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4700.1.100.100

Specifies if the Ems service allows the unit to be provisioned and managed by the Virtuo EMS infrastructure.

- Disable: Unit can not be provisioned by the Virtuo EMS infrastructure.
- Enable: Unit can be provisioned by the Virtuo EMS infrastructure.

PeriodicProvisioningTimer (Config Parameter)

Type	Text
Range	Size(0..250)
Default	daily
Script/CLI	Ems.PeriodicProvisioningTimer
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4700.1.100.200

Defines the periodic interval for the provisioning.

- hourly: provision every hour, at the time defined in the **HourlyTimeRange** parameter.
- daily: provision once a day, at the time defined in the **DailyTimeRange** parameter.
- weekly: provision once a week, at the date and time defined in the **WeeklyTimeRange** parameter.

In the scenario where the provisioning failed with a "ConnectionFailure" (see the **LastProvisioningResult** parameter), the unit will frequently retry until the connection is successful. The frequency of the retry attempts will decrease over time, down to once a week if the connection still cannot be established.

Has no effect if the **EmsProvisioningEnable** parameter is disabled.

Note: Unless a specific time is defined in the hourly/daily/weekly parameters, the random value within a time range is determined at service start-up. As long as the service is not restarted, the same value will be used. For instance, if a daily timer has a range between 10:00 and 10:30 with a randomised value of 10:19, then the timer will trigger at 10:19 every day as long as the Ems service or the unit is not restarted.

HourlyTimeRange (Config Parameter)

Type	Text
Range	Size(0..30)
Default	55 - 05
Script/CLI	Ems.HourlyTimeRange
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4700.1.150.100

Expression defining the specific time or a time range into which an hourly timer will be triggered. If a range is specified, the timer will trigger randomly within that range.
The syntax is: mm[:ss][- mm[:ss]]

- mm specifies the minute within the hour. Possible values are 0 to 59.

- ss specifies the second within the minute. Possible values are 0 to 59.
- The square braces indicate the optional parts of the expression.
- The spaces around the hyphen are optional.
- The second part, i.e. [- mm[:ss]] is optional. If omited, the expression specifies a specific time instead of a range.

Examples:

- 10 - 15: The timer will trigger at a random time between the 10th and the 15th minute at each hour, e.g. between 12:10 and 12:15.
- 55 - 05: The timer will trigger at a random time between the 55th and the 5th minute at each hour, e.g. between 3:55 and 4:05.
- 12: The timer will trigger at the 12th minute every hour (i.e. at 2:12, 3:12, 4:12, ...).

DailyTimeRange (Config Parameter)

Type	Text
Range	Size(0..30)
Default	01:00 - 03:00
Script/CLI	Ems.DailyTimeRange
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4700.1.150.200

Expression defining the specific time or a time range into which a daily timer will be triggered. If a range is specified, the timer will trigger randomly within that range.
The syntax is: hh[:mm[:ss]][- hh[:mm[:ss]]]

- hh specifies the hour within the day in local time. Possible values are 0 to 23.
- mm specifies the minute within the hour. Possible values are 0 to 59.
- ss specifies the second within the minute. Possible values are 0 to 59.
- The square braces indicate the optional parts of the expression.
- The spaces around the hyphen are optional.
- The second part, i.e. [- hh[:mm[:ss]]] is optional. If omited, the expression specifies a specific time instead of a range.

Examples:

- 10 - 15: The timer will trigger at a random time between 10:00 and 15:00 every day.
- 11:10 - 11:15: The timer will trigger at a random time between 11:10 and 11:15 every day.
- 23:30 - 00:30: The timer will trigger at a random time between 23:30 and 00:30 every day.
- 14:10: The timer will trigger at 14:10 every day.

WeeklyTimeRange (Config Parameter)

Type	Text
Range	Size(0..50)
Default	Monday 01:00 - Monday 03:00
Script/CLI	Ems.WeeklyTimeRange
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4700.1.150.300

Expression defining the specific time or a time range into which a weekly timer will be triggered. If a range is specified, the timer will trigger randomly within that range.
The syntax is: dd hh[:mm[:ss]][- dd hh[:mm[:ss]]]

- dd specifies the day. Possible values are the full names in English: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday.
- hh specifies the hour within the day in local time. Possible values are 0 to 23.
- mm specifies the minute within the hour. Possible values are 0 to 59.
- ss specifies the second within the minute. Possible values are 0 to 59.
- The square braces indicate the optional parts of the expression.
- The spaces around the hyphen are optional.
- The second part, i.e. [- hh[:mm[:ss]]] is optional. If omited, the expression specifies a specific time instead of a range.

Examples:

- Sunday 10:00 - Sunday 11:00: The timer will trigger at a random time between Sunday 10:00 and Sunday 11:00.
- Monday 9 - Friday 17: The timer will trigger at a random time between Monday 9:00 and Friday 17:00.
- Friday 17 - Monday 9: The timer will trigger at a random time between Friday 17:00 and Monday 9:00.
- Wednesday 4: The timer will trigger at 4:00 every Wednesday.

LastConnectionDateTime (Status Parameter)

Type	Text
Range	Size(0..255)
Script/CLI	Ems.LastConnectionDateTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4700.1.200.100

The date and time of the last successful connection to the provisioning service.

LastProvisioningResult (Status Parameter)

Type	Enum
Range	None(100) | Success(200) | PartiallyProvisioned(300) | ConnectionFailed(400) | ProvisioningError(500) | UnmanagedUnit(600) | AuthenticationError(700)
Script/CLI	Ems.LastProvisioningResult
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4700.1.200.200

The result of the lastest provisioning against the Virtuo EMS infrastructure.

- None: No provisioning has been requested or provisioning is not yet completed.
- Success: Unit has been provisioned successfully.
- PartiallyProvisioned: Unit has been partially provisioned. See logs for details.
- ConnectionFailed: Unit could not successfully connect to Virtuo. See logs for details.
- ProvisioningError: The connection to Virtuo was successful, but unit could not be provisioned. See logs for details.
- UnmanagedUnit: The connection to Virtuo was successful, but Virtuo is not configured to manage this unit.
- AuthenticationError: The connection to Virtuo has been aborted due to an authentication problem.

AuthenticationVirtuoId (Config Parameter)

Type	Text
Range	Size(0..50)
Default	
Script/CLI	Ems.AuthenticationVirtuoId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4700.1.300.100

The Virtuo ID of the account in the Virtuo Cloud EMS server.
Usually a 5-digit number.

AuthenticationToken (Config Parameter)

Type	Text
Range	Size(0..512)
Default	
Script/CLI	Ems.AuthenticationToken
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4700.1.300.200

Authentication token for the specified Virtuo ID.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Ems.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4700.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Ems.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4700.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Ems service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.4700.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	EMS provisioning has started.	Info	The EMS provisioning process has been initiated.
20	Connection to the provisioning server failed. Reason: %1$s.	Error	The connection to the provisioning server could not be established. Unit could not be provisioned.
22	Authentication error with the provisioning server.	Error	The connection to the provisioning server has aborted due to an authentication problem.
25	Connection to the provisioning server succeeded, but the unit is not managed.	Info	The connection to the provisioning server has been established, but the provisioning server is not configured to manage this unit.
30	The %1$s Configuration provisioning has been applied successfully.	Info	The specified provisioning configuration (generic or specific) has been applied successfully.
40	The %1$s Configuration provisioning has been applied partially.	Warning	The specified provisioning configuration (generic or specific) has been applied partially.
50	The %1$s Configuration provisioning could not be applied. Reason: %2$s.	Warning	The specified provisioning configuration (generic or specific) could not be applied.
60	Retrying connection to the provisioning server.	Debug	A connection attempt will be made to the provisioning server.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.

NumKey	Message	Severity	Description
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.

NumKey	Message	Severity	Description
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Ems.

Message	Severity	Description
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.

Message	Severity	Description
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Endpoint Administration (EpAdm)

The Endpoint Administration (EpAdm) service allows for high-level management of telephony endpoints.

Parameters

UnitAdminState (Status Parameter)

Type	Enum
Range	Unlocked(100) | ShuttingDown(200) | Locked(300)
Script/CLI	EpAdm.UnitAdminState
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1500.1.100.100

Indicates the current maintenance state of a unit. This attribute reflects the result of an operator-initiated maintenance request.

- Unlocked: no operator-initiated maintenance request is affecting the operation of the unit.
- ShuttingDown: the unit is in a transition state between the unlocked and locked states. The unit will transition to a locked state only once all current activities are completed. No new request is accepted once all activities are terminated.
- Locked: an operator-initiated request has been issued for this unit. This unit is unavailable for normal operation.

UnitOpState (Status Parameter)

Type	EnableDisable
Range	
Script/CLI	EpAdm.UnitOpState
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1500.1.100.200

The operational state of the unit reflects the unit's internal state. There are certain conditions that affect the internal state of a unit.

- Enabled: the unit is operationally functional.
- Disabled: the unit is not operationally functional due to an internal condition that would not allow it to participate in normal operation. Such condition could be that all endpoints have failed to properly register.

UnitUsageState (Status Parameter)

Type	Enum
Range	Idle(100) | Active(200) | Busy(300) | IdleUnusable(400)
Script/CLI	EpAdm.UnitUsageState
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1500.1.100.300

The usage state of the unit indicates its running state.

- Idle: the unit is not currently active, but is available for use.
- Active: the unit is currently being used, is available for processing, and still has additional capacity.
- Busy: the unit is usable but is not available for any new additional processing requests, since all of its endpoints are currently being used.
- IdleUnusable: the unit is not currently active and not available for use.

Endpoint (Table)

This table displays the state of all endpoints of the unit.

EpId (Index) | Table: Endpoint

Type	Text
Range	
Script/CLI	EpAdm.Endpoint[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1500.1.200.1.100

String that identifies an endpoint in other tables.

InitialAdminStateConfig (Config Parameter) | Table: Endpoint

Type	Enum
Range	Unlocked(100)| Locked(200)
Default	Unlocked
Script/CLI	EpAdm.Endpoint[].InitialAdminStateConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1500.1.200.1.200

The initial administrative state of an endpoint.
Indicates the administrative state an endpoint will have when the service starts. Refer to **AdminState** for a description of the states.

AdminState (Status Parameter) | Table: Endpoint

Type	Enum
Range	Unlocked(100) | ShuttingDown(200) | Locked(300)
Script/CLI	EpAdm.Endpoint[].AdminState
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1500.1.200.1.300

The administrative state of an endpoint.
Indicates the current maintenance state of an endpoint. This attribute reflects the result of an operator-initiated maintenance request.

- Unlocked: no operator-initiated maintenance request is affecting the operation of the endpoint.
- ShuttingDown: the component is in a transition state between the unlocked and locked state. An active endpoint will only transition to a locked state once activity, if present, has completed. No new request are accepted once the activity is completed.

- Locked: an operator-initiated request has been issued for this endpoint. This endpoint is unavailable for normal operation.

OpState (Status Parameter) | Table: Endpoint

Type	EnableDisable
Range	
Script/CLI	EpAdm.Endpoint[].OpState
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1500.1.200.1.400

The operational state of an endpoint.
This state reflects the endpoint's capacity to participate in normal operations.

- Enabled: the endpoint is operationally functional.
- Disabled: the endpoint is not operationally functional due to an internal condition that would not allow it to participate in normal operations.

UsageState (Status Parameter) | Table: Endpoint

Type	Enum
Range	Idle(100) | Active(200) | Busy(300) | IdleUnusable(400)
Script/CLI	EpAdm.Endpoint[].UsageState
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1500.1.200.1.500

The usage state indicates the running state of an endpoint.

- Idle: the endpoint is not currently active, but is available for use.
- Active: the endpoint is currently being used, is available for processing, and still has additional capacity.
- Busy: the endpoint is usable but is not available for any new additional processing requests, since all of its resources are currently being used.
- IdleUnusable: the endpoint is not currently active and not available for use.

Unlock (Row Command) | Table: Endpoint

Script/CLI:	EpAdm.Endpoint[].Unlock
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1500.1.200.1.600

Allows the use of an endpoint.
This command sets the administrative state of the endpoint to "Unlocked".

Lock (Row Command) | Table: Endpoint

Script/CLI:	EpAdm.Endpoint[].Lock
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1500.1.200.1.700

Gracefully disallows the use of an endpoint.
When the usage state of the endpoint is "Idle" or "IdleUnusable", this command sets the administrative state to "Locked".

When the usage state of the endpoint is "Busy" or "Active", this command sets the administrative state to "ShuttingDown" until the usage state of the endpoint transits to "Idle". The administrative state is then set to "Locked".

ForceLock (Row Command) | Table: Endpoint

Script/CLI:	EpAdm.Endpoint[].ForceLock
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1500.1.200.1.800

Forcefully disallows the use of an endpoint.
This command sets the administrative state of the endpoint to "Locked". All activities in progress are terminated immediately.

UnitDisabledWhenNoGatewayReadyEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpAdm.UnitDisabledWhenNoGatewayReadyEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1500.1.300.100

Indicates if the unit operational state is automatically set to disable when all signaling gateways are not ready.

- Enabled: When all signaling gateways are not ready (**GatewayStatus.State**), the unit operational state (see the **UnitOpState** parameter) is set to disabled.
- Disabled: Signaling gateways (see the **GatewayStatus.State** parameter) have no impact on unit operational state (see the **UnitOpState** parameter).

BehaviorWhileInUnitShuttingDownState (Config Parameter)

Type	Enum
Range	BlockNewCalls(100) | AllowNewCalls(200)
Default	BlockNewCalls
Script/CLI	EpAdm.BehaviorWhileInUnitShuttingDownState
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1500.1.300.200

The behavior of the call permissions when the **UnitAdminState** parameter is 'ShuttingDown' is the following:

- BlockNewCalls: No new requests are accepted once all activity are terminated. Endpoints cannot make and receive calls.
- AllowNewCalls: New requests are accepted until all activities are simultaneously terminated. Endpoints can make and receive calls.

DisableSipGatewaysWhenTrunkLinesDown (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpAdm.DisableSipGatewaysWhenTrunkLinesDown
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1500.1.350.100

Indicates if all SIP gateways should be stopped in the event that all E1T1 lines are down.

- Enabled: When all E1T1 lines are down, all SIP gateways will be stopped. All SIP gateways will be started when at least one E1T1 line is up. The up/down state refers to the physical link state of a E1T1 line.
- Disabled: The physical link state of the E1T1 lines does not have any impact on the SIP gateways. Therefore, all SIP gateways remain operational, whether there is a E1T1 line up or not.

The delay before switching the state of the SIP gateways can be configured by the **DisableSipGatewaysWhenTrunkLinesDownDelay** parameter.

The **DisableSipGatewaysWhenTrunkLinesDown** parameter only applies to E1T1 lines.

See SipEp.GatewayTable for the list of SIP gateways.

DisableSipGatewaysWhenTrunkLinesDownDelay (Config Parameter)

Type	UInt32
Range	0..60
Default	0
Script/CLI	EpAdm.DisableSipGatewaysWhenTrunkLinesDownDelay
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1500.1.350.200

Delay, in seconds, before reporting a status change of a telephony line.
This parameter only applies if the **DisableSipGatewaysWhenTrunkLinesDown** parameter is enabled.

If the state of a telephony line changes back to its previous state within the configured delay, there would be no modification to the SIP gateways state.

A value of 0 means the status change is reported immediately.

EndpointAutomaticShutdownEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpAdm.EndpointAutomaticShutdownEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1500.1.400.100

Indicates if an endpoint is physically shutdown when it is not operational and in the 'idle-unusable' usage state.

- Disable: When an endpoint's usage state (**Endpoint.UsageState**) becomes "Idle-unusable" whatever the value of its operational state, (**Endpoint.OperationalState**) the endpoint remains physically up but the calls are denied.
- Enabled: When the usage state (**Endpoint.UsageState**) becomes "Idle-unusable" and the operational state (**Endpoint.OperationalState**) becomes "Disable", the endpoint is physically shutdown.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	EpAdm.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1500.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	EpAdm.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1500.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnitForceLock (Command)

Forcefully disallows the use of a unit.
This command sets the administrative state of the unit to "Locked". All activities in progress are terminated immediately.

UnitLock (Command)

Gracefully disallows the use of a unit.
When the usage state of the unit is "Idle" or "IdleUnusable", this command sets the administrative state to "Locked".

When the usage state of the unit is "Busy" or "Active", this command sets the administrative state to "ShuttingDown" until the usage state of the unit transits to "Idle". The administrative state is then set to "Locked".

UnitUnlock (Command)

Allows the use of a unit.
This command sets the administrative state of the unit to "Unlocked".

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the EpAdm service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.1500.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	The unit received a lock command.	Info	The unit has received a lock command and will enter the shutting down state until all endpoints are not in use. When all endpoints are not in use, the unit will enter the lock state.
20	The unit received a force lock command.	Info	The unit has received a force lock command and will enter the lock state. All activities on the endpoints will be terminated.
30	The unit received an unlock command.	Info	The unit has received an unlock command and will enter the unlock state. Activity is now allowed on unlocked endpoints.
40	The endpoint %1$s received a lock command.	Info	The endpoint has received a lock command and will enter the shutting down state until it is not in use. When the endpoint is not in use, it will enter the lock state.
50	The endpoint %1$s received a force lock command.	Info	The endpoint has received a force lock command and will enter the lock state. All activities on the endpoint will be terminated.
60	The endpoint %1$s received an unlock command.	Info	The endpoint has received an unlock command and will enter the unlock state. Activity is now allowed on the endpoint.
70	The unit unlock command is not allowed while the service is in draining mode.	Error	The unit unlock command is not allowed while the service is in draining mode.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.

NumKey	Message	Severity	Description
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.

NumKey	Message	Severity	Description
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to EpAdm.

Message	Severity	Description
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.

Message	Severity	Description
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Endpoint Services (EpServ)

The Endpoint Services (EpServ) service manages the telephony services of each endpoint.

Parameters

DefaultCallHookFlashProcessing (Config Parameter)

Type	Enum
Range	ProcessLocally(100) | TransmitUsingSignalingProtocol(200)
Default	ProcessLocally
Script/CLI	EpServ.DefaultCallHookFlashProcessing
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.100.200

Selects how to process hook-flash detection.
When a call is in progress, the user can normally put the call on hold, transfer the call, or even initiate a conference call. **DefaultCallHookFlashProcessing** defines whether these subscriber services are handled by the unit or delegated to a remote party.

- ProcessLocally: Hook-flash is processed locally. The actual behavior of the 'flash' button depends on which subscriber services are enabled for this endpoint.
- TransmitUsingSignalingProtocol: Hook-flash is processed by a remote party. The hook-flash event is carried by a signaling protocol message. The actual behavior of the 'flash' button

depends on the remote party. This option also enables the unit to receive call waiting events with caller ID via the signaling protocol.

If a specific configuration is set in the **EpSpecificCall.HookFlashProcessing** parameter and the **EpSpecificCall.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultCallAllowDirectIp (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.DefaultCallAllowDirectIp
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.100.300

Enables/Disables the direct IP address call service.
This service allows a user to make a call without the help of a server.

When this service is enabled, the user can dial an IP address and enter an optional phone number. Note that the optional phone number will be checked by using the same DTMF maps as for a normal call.

This method bypasses any server configuration found in the unit.

To make an IP address call:

1. Dial '**'.
2. Dial the numerical DTMFs of the IP address. For the dot '.', use the star '*' sign.
3. Terminate the IP call without specifying a phone number by using the star '*' or continue with a phone number by using the pound '#' sign.
4. Optionally, dial the phone number.

Example IP calls to a unit at IP address '1.2.3.4':

- If the phone number is not required, the user dials the following DTMFs: **1*2*3*4*.
- To reach the phone number '3330001', the user dials the following DTMFs: **1*2*3*4#3330001.

EpSpecificCall (Table)

A table of the telephony features configuration for the call, indexed by the endpoint ID.

EpId (Index) | Table: EpSpecificCall

Type	Text
Range	
Script/CLI	EpServ.EpSpecificCall[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.100.400.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificCall

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.EpSpecificCall[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.100.400.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultCallHookFlashProcessing** parameter.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificCall.HookFlashProcessing** parameter.

HookFlashProcessing (Config Parameter) | Table: EpSpecificCall

Type	Enum
Range	ProcessLocally(100) | TransmitUsingSignalingProtocol(200)
Default	ProcessLocally
Script/CLI	EpServ.EpSpecificCall[].HookFlashProcessing
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.100.400.1.400

Selects how to process hook-flash detection.
When a call is in progress, the user can normally put the call on hold, transfer the call, or even initiate a conference call. **DefaultCallHookFlashProcessing** defines whether these subscriber services are handled by the unit or delegated to a remote party.

- ProcessLocally: Hook-flash is processed locally. The actual behavior of the 'flash' button depends on which subscriber services are enabled for this endpoint.
- TransmitUsingSignalingProtocol: Hook-flash is processed by a remote party. The hook-flash event is carried by a signaling protocol message. The actual behavior of the 'flash' button depends on the remote party. This option also enables the unit to receive call waiting events with caller ID via the signaling protocol.

This configuration overrides the default configuration set in the **DefaultCallHookFlashProcessing** parameter if the **EpSpecificCall.EnableConfig** parameter is set to 'Enable'.

CallDtmfMapAllowed (Table)

A table of the DTMF maps that are considered valid if dialed, indexed by the DTMF map entry number.

Index (Index) | Table: CallDtmfMapAllowed

Type	UInt32
Range	1..10
Script/CLI	EpServ.CallDtmfMapAllowed[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.100.500.100.1.100

Accepted DTMF map index for this row.

Enable (Config Parameter) | Table: CallDtmfMapAllowed

Type	EnableDisable
Range	
Default	Enable
Script/CLI	EpServ.CallDtmfMapAllowed[].Enable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.100.500.100.1.200

If enabled, this DTMF map is recognised and accepted only if it is also valid.
If disabled, this DTMF map is not recognised.

ApplyTo (Config Parameter) | Table: CallDtmfMapAllowed

Type	Enum
Range	Unit(100) | Endpoint(200)
Default	Unit
Script/CLI	EpServ.CallDtmfMapAllowed[].ApplyTo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.100.500.100.1.300

Sets the entity to which apply the DTMF map.

- Unit: The DTMF map applies to all endpoints.
- Endpoint: The DTMF map applies to a specific endpoint. The endpoint is specified in the **EpId** parameter.

EpId (Config Parameter) | Table: CallDtmfMapAllowed

Type	Text
Range	
Default	
Script/CLI	EpServ.CallDtmfMapAllowed[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.100.500.100.1.400

String that identifies an endpoint in other tables.
More than one endpoint can be specified. In that case, the endpoints are separated with ','.

DtmfMap (Config Parameter) | Table: CallDtmfMapAllowed

Type	DigitMap
Range	
Default	x.T
Script/CLI	EpServ.CallDtmfMapAllowed[].DtmfMap
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.100.500.100.1.500

The DTMF map string used to validate the dialed DTMFs.
The DTMF map syntax is taken from the MGCP specification (RFC 3435 section 2.1.5). Refer to the DTMF Maps configuration in the Software Configuration Guide for examples.

Local emulation of a service code:

By using the special 'S' character to emulate a star code activation, the caller will hear a stutter dial tone after a service code has been dialed (e.g. *72). To use the special S character, it must be preceded by a valid DTMF map string. If characters are specified after the S, they must be a valid DTMF map string. If a DTMF transformation is associated with this DTMF map, the transformation is done on the signaled DTMF after the 'S' character. All dialed DTMFs will be present in the outgoing call, including the ones dialed before the stutter dial tone.

DtmfTransformation (Config Parameter) | Table: CallDtmfMapAllowed

Type	Text
Range	Size(0..32)
Default	x
Script/CLI	EpServ.CallDtmfMapAllowed[].DtmfTransformation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.100.500.100.1.600

Configures the transformation to apply to the signaled DTMF before using it as call destination. In the following description, 'x' represents the signaled number.

Add before 'x' the DTMF to prefix or/and after 'x' the suffix to add. Characters '0123456789*#ABCD' are allowed.

Use a sequence of DTMFs beween '{}' to remove a prefix/suffix to the dialed number if present. Use before 'x' to remove a prefix and after 'x' to remove a suffix. Characters '0123456789*#ABCD' are allowed.

Use a number between '()' to remove a number of DTMFs. Use before 'x' to remove DTMFs at the beginning of the number and after 'x' to remove DTMFs at the end. Characters '0123456789' are allowed.

The transformations are applied in order from left to right.

Example with '18195551111#' as signaled number.

- Add the prefix '0' to the dialed number: '0x' ==> '018195551111#'.
- Remove the suffix '#' from the dialed number: 'x{#}' ==> '18195551111'.
- Remove the first 4 DTMFs from the dialed number: '(4)x' ==> '5551111#'
- Remove the international code and termination and replace the area code by another one: '(1){819}514x{#}' ==> '5145551111'.
- Replace the signaled DTMFs by '3332222' : '3332222' ==> '3332222'.

TargetHost (Config Parameter) | Table: CallDtmfMapAllowed

Type	IpHostNamePort
Range	
Default	
Script/CLI	EpServ.CallDtmfMapAllowed[].TargetHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.100.500.100.1.700

Target to use when the DTMF map matches. The default target is used when the value is empty.

Emergency (Config Parameter) | Table: CallDtmfMapAllowed

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.CallDtmfMapAllowed[].Emergency
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.100.500.100.1.800

Enables/Disables the emergency process of the call.

- Disable: The call is processed as normal.
- Enable: The call is processed as emergency.

CallDtmfMapRefuse (Table)

A table of the DTMF maps that are considered invalid if dialed, indexed by the DTMF map entry number.

Index (Index) | Table: CallDtmfMapRefuse

Type	UInt32
Range	1..10
Script/CLI	EpServ.CallDtmfMapRefuse[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.100.500.200.1.100

Refused DTMF map index for this row.

Enable (Config Parameter) | Table: CallDtmfMapRefuse

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.CallDtmfMapRefuse[].Enable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.100.500.200.1.200

If enabled, this DTMF map is recognised and refused only if it is also valid.
If disabled, this DTMF map is not recognised.

ApplyTo (Config Parameter) | Table: CallDtmfMapRefuse

Type	Enum
Range	Unit(100) | Endpoint(200)
Default	Unit
Script/CLI	EpServ.CallDtmfMapRefuse[].ApplyTo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.100.500.200.1.300

Sets the entity to which apply the DTMF map.

- Unit: The DTMF map applies to all endpoints.
- Endpoint: The DTMF map applies to a specific endpoint. The endpoint is specified in the **EpId** parameter.

EpId (Config Parameter) | Table: CallDtmfMapRefuse

Type	Text
Range	
Default	
Script/CLI	EpServ.CallDtmfMapRefuse[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.100.500.200.1.400

String that identifies an endpoint in other tables.
More than one endpoint can be specified. In that case, the endpoints are separated with ','.

DtmfMap (Config Parameter) | Table: CallDtmfMapRefuse

Type	DigitMap
Range	
Default	
Script/CLI	EpServ.CallDtmfMapRefuse[].DtmfMap
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.100.500.200.1.500

The actual DTMF map string that is considered invalid when dialed.
The permitted DTMF map syntax is taken from the core MGCP specification, RFC 2705: ftp://ftp.isi.edu/in-notes/rfc2705.txt, section 3.4.

DefaultAutoCallEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.DefaultAutoCallEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.200.100

Enables/Disables the automatic call service. This service provides a 'redphone'-like experience. If enabled, the target address is automatically called when the user picks up the phone.

When this service is enabled, the second line service is disabled but the call waiting feature is still functional. The user can still accept incoming calls.

If a specific configuration is set in the **EpSpecificAutoCall.Enable** parameter and the **EpSpecificAutoCall.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultAutoCallTargetAddress (Config Parameter)

Type	Text
Range	Size(0..127)
Default	
Script/CLI	EpServ.DefaultAutoCallTargetAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.200.200

Address or telephone number that the user wants to automatically call.
If a specific configuration is set in the **EpSpecificAutoCall.TargetAddress** parameter and the **EpSpecificAutoCall.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

EpSpecificAutoCall (Table)

A table of the telephony features configuration for the automatic call, indexed by the endpoint ID.

EpId (Index) | Table: EpSpecificAutoCall

Type	Text
Range	
Script/CLI	EpServ.EpSpecificAutoCall[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.200.300.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificAutoCall

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.EpSpecificAutoCall[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.200.300.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultAutoCallEnable** and **DefaultAutoCallTargetAddress** parameters.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificAutoCall.Enable** and **EpSpecificAutoCall.TargetAddress** parameters.

Enable (Config Parameter) | Table: EpSpecificAutoCall

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.EpSpecificAutoCall[].Enable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.200.300.1.300

Enables/Disables the automatic call service. This service provides a 'redphone'-like experience. If enabled, the target address is automatically called when the user picks up the phone.

When this service is enabled, the second line service is disabled but the call waiting feature is still functional. The user can still accept incoming calls.

This configuration overrides the default configuration set in the **DefaultAutoCallEnable** parameter if the **EpSpecificAutoCall.EnableConfig** parameter is set to 'Enable'.

TargetAddress (Config Parameter) | Table: EpSpecificAutoCall

Type	Text
Range	Size(0..127)
Default	
Script/CLI	EpServ.EpSpecificAutoCall[].TargetAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.200.300.1.400

Address or telephone number that the user wants to automatically call.
This configuration overrides the default configuration set in the **DefaultAutoCallTargetAddress** parameter if the **EpSpecificAutoCall.EnableConfig** parameter is set to 'Enable'.

DefaultHoldEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	EpServ.DefaultHoldEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.300.100

Enables/Disables the holding service.
This service allows to temporarily put an active call on hold, usually by using the 'flash' button of the telephone. The user can resume the call in the same way.

This service has no dependencies on other services being enabled.

If a specific configuration is set in the **EpSpecificHold.Enable** parameter and the **EpSpecificHold.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

EpSpecificHold (Table)

EpId (Index) | Table: EpSpecificHold

Type	Text
Range	
Script/CLI	EpServ.EpSpecificHold[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.300.200.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificHold

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.EpSpecificHold[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.300.200.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultHoldEnable** parameter.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificHold.Enable** parameter.

Enable (Config Parameter) | Table: EpSpecificHold

Type	EnableDisable
Range	
Default	Enable
Script/CLI	EpServ.EpSpecificHold[].Enable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.300.200.1.300

Enables/Disables the holding service.
This service allows to temporarily put an active call on hold, usually by using the 'flash' button of the telephone. The user can resume the call in the same way.

This service has no dependencies on other services being enabled.

This configuration overrides the default configuration set in the **DefaultHoldEnable** parameter if the **EpSpecificHold.EnableConfig** parameter is set to 'Enable'.

HoldStatus (Table)

A table of the hold services status for the endpoint, indexed by the endpoint ID.

EpId (Index) | Table: HoldStatus

Type	Text
Range	
Script/CLI	EpServ.HoldStatus[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.300.300.1.100

String that identifies an endpoint in other tables.

State (Status Parameter) | Table: HoldStatus

Type	ActiveInactive
Range	
Script/CLI	EpServ.HoldStatus[].State
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.300.300.1.200

Status of the holding service.
See the **DefaultHoldEnabling** parameter.

DefaultCallWaitingEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	EpServ.DefaultCallWaitingEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.400.100

Enables/Disables the call waiting service.
With this service enabled, when an endpoint with an active call receives a new call, it sends a special tone indicating that a call is waiting on the second line. The user may then answer that call by using the 'flash' button of the telephone. The user can switch between the two active calls by using the 'flash' button.

To enable this service, the call hold service must be enabled as well.

The user may cancel this service by dialing the DTMF sequence stored in the **DefaultCallWaitingCancelDtmfMap** parameter.

See the **DefaultHoldEnable** and **DefaultCallWaitingCancelDtmfMap** parameters.

If a specific configuration is set in the **EpSpecificCallWaiting.Enable** parameter and the **EpSpecificCallWaiting.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultCallWaitingCancelDtmfMap (Config Parameter)

Type	DigitMap
Range	
Default	
Script/CLI	EpServ.DefaultCallWaitingCancelDtmfMap
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.400.200

DTMF map the user can dial to disable the call waiting service. This service is cancelled on a per-call basis.
This DTMF map must follow the syntax for DTMF maps as declared in the DTMF maps configuration.

Note that dialing this DTMF map does not have any effect unless the call waiting service's status is 'enabled'.

See the **DefaultCallWaitingEnable** parameter.

DefaultCallWaitingActivationDtmfMap (Config Parameter)

Type	DigitMap
Range	
Default	
Script/CLI	EpServ.DefaultCallWaitingActivationDtmfMap
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.400.210

DTMF map the user can dial to activate the call waiting service.
This DTMF map must follow the syntax for DTMF maps as declared in the DTMF maps configuration.

Note that dialing this DTMF map does not have any effect unless the call waiting service's status is 'enabled'.

See the **DefaultCallWaitingEnable** parameter.

DefaultCallWaitingDeactivationDtmfMap (Config Parameter)

Type	DigitMap
Range	
Default	
Script/CLI	EpServ.DefaultCallWaitingDeactivationDtmfMap
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.400.220

DTMF map the user can dial to deactivate the call waiting service.
This DTMF map must follow the syntax for DTMF maps as declared in the DTMF maps configuration.

Note that dialing this DTMF map does not have any effect unless the call waiting service's status is 'enabled'.

See the **DefaultCallWaitingEnable** parameter.

EpSpecificCallWaiting (Table)

EpId (Index) | Table: EpSpecificCallWaiting

Type	Text
Range	
Script/CLI	EpServ.EpSpecificCallWaiting[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.400.300.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificCallWaiting

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.EpSpecificCallWaiting[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.400.300.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultCallWaitingEnable** parameter.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificCallWaiting.Enable** parameter.

Enable (Config Parameter) | Table: EpSpecificCallWaiting

Type	EnableDisable
Range	
Default	Enable
Script/CLI	EpServ.EpSpecificCallWaiting[].Enable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.400.300.1.300

Enables/Disables the call waiting service.
With this service enabled, when an endpoint with an active call receives new calls, it sends a special tone indicating that a call is waiting on the second line. The user may then answer that call by using

the 'flash' button of the telephone. The user can switch between the two active calls by using the 'flash' button.

To enable this service, the call hold service must be enabled as well.

The user cancels this service when dialing a DTMF sequence matching the DTMF map stored in **DefaultCallWaitingCancelDtmfMap** parameter.

See the **DefaultHoldEnable** and **DefaultCallWaitingCancelDtmfMap** parameters.

This configuration overrides the default configuration set in the **DefaultCallWaitingEnable** parameter if the **EpSpecificCallWaiting.EnableConfig** parameter is set to 'Enable'.

CallWaitingStatus (Table)

A table of the call waiting service status for the endpoint, indexed by the endpoint ID.

EpId (Index) | Table: CallWaitingStatus

Type	Text
Range	
Script/CLI	EpServ.CallWaitingStatus[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.400.400.1.100

String that identifies an endpoint in other tables.

State (Status Parameter) | Table: CallWaitingStatus

Type	ActiveInactive
Range	
Script/CLI	EpServ.CallWaitingStatus[].State
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.400.400.1.200

Status of the call waiting service.
See the **DefaultCallWaitingEnable** parameter.

CallWaitingUserConfig (Table)

A table of the call waiting service user config for the endpoint, indexed by the endpoint ID.

EpId (Index) | Table: CallWaitingUserConfig

Type	Text
Range	
Script/CLI	EpServ.CallWaitingUserConfig[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.400.500.1.100

String that identifies the endpoint.

State (Config Parameter) | Table: CallWaitingUserConfig

Type	ActiveInactive
Range	
Default	Active
Script/CLI	EpServ.CallWaitingUserConfig[].State
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.400.500.1.200

User config of the call waiting service.

- Active: Indicates that the call waiting service is active (usable) for that line.
- Inactive: Indicates that the call waiting service for that line has been deactivated by the user.

DefaultSecondCallEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	EpServ.DefaultSecondCallEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.500.100

Enables/Disables the second call service.
This service allows a user with an active call to put the call on hold and initiate a new call on the second line.

This service is most useful in conjunction with the transfer and conference services.

To enable this service, the call hold service must be enabled as well. See the **DefaultHoldEnable** parameter.

If a specific configuration is set in the **EpSpecificSecondCall.Enable** parameter and the **EpSpecificSecondCall.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultSecondCallDisconnectAction (Config Parameter)

Type	Enum
Range	Wait(100) | AutoSwitch(200)
Default	Wait
Script/CLI	EpServ.DefaultSecondCallDisconnectAction
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.500.150

The action to execute when the second call disconnects:

- Wait: This is the normal behavior. The end-of-call tone will be played until the user either flash hook to go back to the first call or on-hook to disconnect the first call.
- AutoSwitch: This will play a specific tone then automatically switch back to the first call. Unless the user either flash hook or on-hook while the tone plays. Then those action have the same effect as when wait is choosen

If a specific configuration is set in the **EpSpecificSecondCall.DisconnectAction** parameter and the **EpSpecificSecondCall.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

EpSpecificSecondCall (Table)

EpId (Index) | Table: EpSpecificSecondCall

Type	Text
Range	
Script/CLI	EpServ.EpSpecificSecondCall[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.500.200.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificSecondCall

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.EpSpecificSecondCall[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.500.200.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultSecondCallEnable** parameter.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificSecondCall.Enable** parameter.

Enable (Config Parameter) | Table: EpSpecificSecondCall

Type	EnableDisable
Range	
Default	Enable
Script/CLI	EpServ.EpSpecificSecondCall[].Enable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.500.200.1.300

Enables/Disables the second call service.
This service allows a user with an active call to put the call on hold and initiate a new call on the second line.

This service is most useful in conjunction with the transfer and conference services.

To enable this service, the call hold service must be enabled as well. See the **DefaultHoldEnable** parameter.

This configuration overrides the default configuration set in the **DefaultSecondCallEnable** parameter if the **EpSpecificSecondCall.EnableConfig** parameter is set to 'Enable'.

DisconnectAction (Config Parameter) | Table: EpSpecificSecondCall

Type	Enum
Range	Wait(100) | AutoSwitch(200)
Default	Wait
Script/CLI	EpServ.EpSpecificSecondCall[].DisconnectAction
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.500.200.1.400

The action to execute when the second call disconnects:

- Wait: This is the normal behavior. The end-of-call tone will be played until the user either flash hook to go back to the first call or on-hook to disconnect the first call.
- AutoSwitch: This will play a specific tone then automatically switch back to the first call. Unless the user either flash hook or on-hook while the tone plays. Then those action have the same effect as when wait is choosen

This configuration overrides the default configuration set in the **DefaultSecondCallDisconnectAction** parameter if the **EpSpecificSecondCall.EnableConfig** parameter is set to 'Enable'.

SecondCallStatus (Table)

A table of the second call services status for the endpoint, indexed by the endpoint ID.

EpId (Index) | Table: SecondCallStatus

Type	Text
Range	
Script/CLI	EpServ.SecondCallStatus[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.500.300.1.100

String that identifies an endpoint in other tables.

State (Status Parameter) | Table: SecondCallStatus

Type	ActiveInactive
Range	
Script/CLI	EpServ.SecondCallStatus[].State
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.500.300.1.200

Status of the second call service.
See the **DefaultSecondCallEnable** parameter.

DefaultTransferBlindEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	EpServ.DefaultTransferBlindEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.600.100

Enables/Disables the blind call transfer service, also known as Transfer without Consultation or Unattended Transfer.
The method used to perform the blind transfer is defined in **DefaultTransferBlindType**

When the **DefaultTransferBlindType** is set to TargetSecondCall, this service allows a user to transfer a call on hold to a still ringing (unanswered) call.

Starting with an active call, a user can put the call on hold, initiate a call to a third party, then transfer the participant that is currently on hold to the third party. This must be done before the third party has answered. In case the third party answers, the transfer becomes an Attended Transfer.

The user requests the transfer by hanging up the handset.

Once the transfer is executed, the remaining calls (call on hold and ringing call with third party) are then connected together. The call on hold is automatically unheld and hears the ringback tone provided by the third party's ringing. In some configurations, the transfer execution is delayed until the third party answers.

To enable this service, the call hold AND second call services must be enabled as well. See the **DefaultHoldEnable** and **DefaultSecondCallEnable** parameters.

When the **DefaultTransferBlindType** is set to TargetDial, this service allows a user to transfer a call on hold directly to a dialed destination.

Starting with an active call, a user can put the call on hold, then dial the destination of the transfer. A confirmation tone is played after the dialed number match a digit map and the call on hold is been transfered. The user can then hang-up or flash to initiate a new call.

To enable this service, the call hold must be enabled as well AND the second call services must not be enabled. See the **DefaultHoldEnable** and **DefaultSecondCallEnable** parameters.

Also see the **DefaultTransferAttendedEnable** parameter for a variation of the transfer method.

If a specific configuration is set in the **EpSpecificTransfer.BlindEnable** parameter and the **EpSpecificTransfer.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

See also **SipEp.InteropWaitConfirmedDialogForBlindTransfer**.

DefaultTransferBlindType (Config Parameter)

Type	Enum
Range	TargetSecondCall(100) | TargetDial(200)
Default	TargetSecondCall
Script/CLI	EpServ.DefaultTransferBlindType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.600.150

Specifies how to initiate a blind transfer.

- TargetSecondCall: The blind transfer will be initiated from the call on hold to the unanswered call after the dialing of the target.
- TargetDial: The blind transfer will be initiated from the call on hold to the dialed target without making a call to the target.

This parameter only has an effect when the blind transfer service is enabled. See the **DefaultTransferBlindEnable** parameter.

DefaultTransferAttendedEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	EpServ.DefaultTransferAttendedEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.600.200

Enables/Disables the attended call transfer service, also known as Transfer with Consultation. This service allows a user to transfer a call on hold to an active call.

Starting with an active call, a user can put the call on hold, initiate a call to a third party, wait for the third party to answer, then transfer the participant that is currently on hold to the third party.

The transfer is triggered by the user hanging up the handset. The remaining calls (call on hold and active call with third party) are then connected together.

To enable this service, the call hold AND second call services must be enabled as well. See the **DefaultHoldEnable** and **DefaultSecondCallEnable** parameters.

If a specific configuration is set in the **EpSpecificTransfer.AttendedEnable** parameter and the **EpSpecificTransfer.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

EpSpecificTransfer (Table)

EpId (Index) | Table: EpSpecificTransfer

Type	Text
Range	
Script/CLI	EpServ.EpSpecificTransfer[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.600.300.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificTransfer

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.EpSpecificTransfer[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.600.300.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultTransferBlindEnable** and **DefaultTransferAttendedEnable** parameters.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificTransfer.BlindEnable** and **EpSpecificTransfer.AttendedEnable** parameter.

BlindEnable (Config Parameter) | Table: EpSpecificTransfer

Type	EnableDisable
Range	
Default	Enable
Script/CLI	EpServ.EpSpecificTransfer[].BlindEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.600.300.1.500

Enables/Disables the blind call transfer service, also known as called Transfer without Consultation or Unattended Transfer.
The method used to perform the blind transfer is defined in **DefaultTransferBlindType**

When the **DefaultTransferBlindType** is set to TargetSecondCall, this service allows a user to transfer a call on hold to a still ringing (unanswered) call.

Starting with an active call, a user can put the call on hold, initiate a call to a third party, then transfer the participant that is currently on hold to the third party. This must be done before the third party has answered. In case the third party answers, the transfer becomes an Attended Transfer.

The user requests the transfer by hanging up the handset.

Once the transfer is executed, the remaining calls (call on hold and ringing call with third party) are then connected together. The call on hold is automatically unheld and hears the ringback tone provided by the third party's ringing. In some configurations, the transfer execution is delayed until the third party answers.

To enable this service, the call hold AND second call services must be enabled as well. See the **DefaultHoldEnable** and **DefaultSecondCallEnable** parameters.

When the **DefaultTransferBlindType** is set to TargetDial, this service allows a user to transfer a call on hold directly to a dialed destination.

Starting with an active call, a user can put the call on hold, then dial the destination of the transfer. A confirmation tone is played after the dialed number match a digit map and the call on hold is been transfered. The user can then hang-up or flash to initiate a new call.

To enable this service, the call hold must be enabled as well AND the second call services must not be enabled. See the **DefaultHoldEnable** and **DefaultSecondCallEnable** parameters.

Also see the **DefaultTransferAttendedEnable** parameter for a variation of the transfer method.

This configuration overrides the default configuration set in the **DefaultTransferBlindEnable** parameter if the **EpSpecificTransfer.EnableConfig** parameter is set to 'Enable'.

See also **SipEp.InteropWaitConfirmedDialogForBlindTransfer**.

AttendedEnable (Config Parameter) | Table: EpSpecificTransfer

Type	EnableDisable
Range	
Default	Enable
Script/CLI	EpServ.EpSpecificTransfer[].AttendedEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.600.300.1.600

Enables/Disables the attended call transfer service, also known as Transfer with Consultation. This service allows a user to transfer a call on hold to an active call.

Starting with an active call, a user can put the call on hold, initiate a call to a third party, wait for the third party to answer, then transfer the participant that is currently on hold to the third party.

The transfer is triggered by the user hanging up the handset. The remaining calls (call on hold and active call with third party) are then connected together.

For this service to be enabled, the call hold AND second call services must be enabled as well. See the **DefaultHoldEnable** and **DefaultSecondCallEnable** parameters.

This configuration overrides the default configuration set in the **DefaultTransferAttendedEnable** parameter if the **EpSpecificTransfer.EnableConfig** parameter is set to 'Enable'.

TransferStatus (Table)

A table of the transfer services status for the endpoint, indexed by the endpoint ID.

EpId (Index) | Table: TransferStatus

Type	Text
Range	
Script/CLI	EpServ.TransferStatus[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.600.400.1.100

String that identifies an endpoint in other tables.

BlindState (Status Parameter) | Table: TransferStatus

Type	ActiveInactive
Range	
Script/CLI	EpServ.TransferStatus[].BlindState
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.600.400.1.200

Status of the blind transfer service.
See the **DefaultTransferBlindEnable** parameter.

AttendedState (Status Parameter) | Table: TransferStatus

Type	ActiveInactive
Range	
Script/CLI	EpServ.TransferStatus[].AttendedState
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.600.400.1.300

Status of the attended transfer service.
See the **DefaultTransferAttendedEnable** parameter.

DefaultConferenceEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	EpServ.DefaultConferenceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.700.100

Enables/Disables the call conference service.
This service allows a user to link two or more calls together to form a single conversation, called a conference.

Starting with an active call, a user can put the call on hold, initiate a call to a third party, wait for the third party to answer, then use the 'flash' button of the telephone to start the conference with the call that is already on hold.

- Currently, only 3-way conferences are supported.

- Currently, a participant of the conference can put the conference on hold and attempt other calls. This participant may then rejoin the conference at a later time by unholding it. The endpoint that has initiated the conference is NOT able to put the conference on hold.

To enable this service, the call hold AND second call services must be enabled as well. See the **DefaultHoldEnable** parameter and **DefaultSecondCallEnable**.

If a specific configuration is set in the **EpSpecificConference.Enable** parameter and the **EpSpecificConference.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultConferenceType (Config Parameter)

Type	Enum
Range	Local(100) | ConferenceServer(200)
Default	Local
Script/CLI	EpServ.DefaultConferenceType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.700.150

Specifies how to manage the conference. This configuration only applies to a conference initiated by one of the unit's endpoint.

- Local: The media of the conference is locally mixed by the unit. This conference type does not require any special support of the call peer or server. Using this type of conference can reduce the number of simultaneous calls supported.
- ConferenceServer: The unit uses an external server to mix the media of the conference. This conference type requires the configuration of an external server (See the **SipEp.DefaultStaticConferenceServerUri** parameter). Using this type of conference does not affect the number of simultaneous calls supported.

This parameter only has an effect when the conference service is enabled. See the **DefaultConferenceEnable** parameter.

In Local mode, the number of participants is limited to the unit's model capacity. In ConferenceServer mode, the number of participants is limited by the server's capacity.

If a specific configuration is set in the **EpSpecificConference.Enable** parameter and the **EpSpecificConference.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

EpSpecificConference (Table)

EpId (Index) | Table: EpSpecificConference

Type	Text
Range	
Script/CLI	EpServ.EpSpecificConference[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.700.200.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificConference

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.EpSpecificConference[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.700.200.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultConferenceEnable** and **DefaultConferenceType** parameters.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificConference.Enable** and **EpSpecificConference.Type** parameters.

Enable (Config Parameter) | Table: EpSpecificConference

Type	EnableDisable
Range	
Default	Enable
Script/CLI	EpServ.EpSpecificConference[].Enable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.700.200.1.300

Enables/Disables the call conference service.
This service allows a user to link two or more calls together to form a single conversation, called a conference.

Starting with an active call, a user can put the call on hold, initiate a call to a third party, wait for the third party to answer, then use the 'flash' button of the telephone to start the conference with the call that is already on hold.

- Currently, only 3-way conferences are supported.
- Currently, a participant of the conference can put the conference on hold and attempt other calls. This participant may then rejoin the conference at a later time by unholding it. The endpoint that has initiated the conference is NOT able to put the conference on hold.

To enable this service, the call hold AND second call services must be enabled as well. See the **DefaultHoldEnable** parameter and **DefaultSecondCallEnable**.

This configuration overrides the default configuration set in the **DefaultConferenceEnable** parameter if the **EpSpecificConference.EnableConfig** parameter is set to 'Enable'.

Type (Config Parameter) | Table: EpSpecificConference

Type	Enum
Range	Local(100) | ConferenceServer(200)
Default	Local
Script/CLI	EpServ.EpSpecificConference[].Type
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.700.200.1.400

Specifies how to manage the conference. This configuration only applies to a conference initiated by one of the unit's endpoint.

- Local: The media of the conference is locally mixed by the unit. This conference type does not require any special support of the call peer or server. Using this type of conference can reduce the number of simultaneous calls supported.
- ConferenceServer: The unit use an external server to mix the media of the conference. This conference type requires the configuration of an external server (See the **SipEp.DefaultStaticConferenceServerUri** parameter). Using this type of conference does not affect the number of simultaneous calls supported.

This parameter only has an effect when the conference service is enabled. See the **DefaultConferenceEnable** parameter.

This configuration overrides the default configuration set in the **DefaultConferenceType** parameter if the **EpSpecificConference.EnableConfig** parameter is set to 'Enable'.

ConferenceStatus (Table)

A table of the conference services status for the endpoint, indexed by the endpoint ID.

EpId (Index) | Table: ConferenceStatus

Type	Text
Range	
Script/CLI	EpServ.ConferenceStatus[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.700.300.1.100

String that identifies an endpoint in other tables.

State (Status Parameter) | Table: ConferenceStatus

Type	ActiveInactive
Range	
Script/CLI	EpServ.ConferenceStatus[].State
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.700.300.1.200

Status of the conference service.
See the **DefaultConferenceEnable** parameter.

DefaultForwardUnconditionalEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.DefaultForwardUnconditionalEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.100.100

Enables/Disables the unconditional call forward service.
This service allows a user to forward ALL incoming calls to a specified target. A short ring is emitted to alert the user that the call has been forwarded, but the user cannot pick up the call from that location.

If enabled, the user can dial the DTMF maps for enabling and disabling this service.

See the **ForwardingAddress**, **DefaultForwardUnconditionalDtmfMapActivation** and **DefaultForwardUnconditionalDtmfMapDeactivation** parameters.

If a specific configuration is set in the **EpSpecificForwardUnconditional.Enable** parameter and the **EpSpecificForwardUnconditional.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultForwardUnconditionalDtmfMapActivation (Config Parameter)

Type	DigitMap
Range	
Default	
Script/CLI	EpServ.DefaultForwardUnconditionalDtmfMapActivation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.100.200

DTMF map the user can dial to enable the application of the service.
This DTMF map must follow the syntax for DTMF maps as declared in the DTMF maps configuration.

Note that dialing this DTMF map does not have any effect unless the service's status is 'enabled'.

See the **DefaultForwardUnconditionalEnable** parameter.

DefaultForwardUnconditionalDtmfMapDeactivation (Config Parameter)

Type	DigitMap
Range	
Default	
Script/CLI	EpServ.DefaultForwardUnconditionalDtmfMapDeactivation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.100.300

DTMF map the user can dial to disable the application of the service.
This DTMF map must follow the syntax for DTMF maps as declared in the DTMF maps configuration.

Note that dialing this DTMF map does not have any effect unless the service's status is 'enabled'.

See the **DefaultForwardUnconditionalEnable** parameter.

EpSpecificForwardUnconditional (Table)

EpId (Index) | Table: EpSpecificForwardUnconditional

Type	Text
Range	
Script/CLI	EpServ.EpSpecificForwardUnconditional[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.100.400.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificForwardUnconditional

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.EpSpecificForwardUnconditional[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.100.400.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultForwardUnconditionalEnable** parameter.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificForwardUnconditional.Enable** parameter.

Enable (Config Parameter) | Table: EpSpecificForwardUnconditional

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.EpSpecificForwardUnconditional[].Enable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.100.400.1.300

Enables/Disables the unconditional call forward service.
This service allows a user to forward ALL incoming calls to a specified target. A short ring is emitted to alert the user that the call has been forwarded, but the user cannot pick up the call from that location.

If enabled, the user can dial the DTMF maps for enabling and disabling this service.

See the **ForwardingAddress** parameter.

This configuration overrides the default configuration set in the **DefaultForwardUnconditionalEnable** parameter if the **EpSpecificForwardUnconditional.EnableConfig** parameter is set to 'Enable'.

ForwardUnconditionalConfig (Table)

A table of the unconditional call forward activation for the endpoint, indexed by the endpoint ID.

EpId (Index) | Table: ForwardUnconditionalConfig

Type	Text
Range	
Script/CLI	EpServ.ForwardUnconditionalConfig[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.100.500.1.100

String that identifies an endpoint in other tables.

Activation (Config Parameter) | Table: ForwardUnconditionalConfig

Type	ActiveInactive
Range	
Default	Inactive
Script/CLI	EpServ.ForwardUnconditionalConfig[].Activation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.100.500.1.200

Activation state of the unconditional call forward service.
Using the DTMF maps configured for this service, the user can use his/her handset to activate or deactivate this service. In that case, the parameter is automatically updated to reflect the activation status.

This service can also be activated or deactivated by setting the value of this parameter.

ForwardingAddress (Config Parameter) | Table: ForwardUnconditionalConfig

Type	Text
Range	Size(0..127)
Default	
Script/CLI	EpServ.ForwardUnconditionalConfig[].ForwardingAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.100.500.1.300

Address or telephone number to which the user wants to forward calls.

DefaultForwardOnBusyEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.DefaultForwardOnBusyEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.200.100

Enables/Disables the call forward on busy service.
This service allows a user to forward incoming calls to a specified target when the user is already participating in another call.

The user does not have any feedback that a call was forwarded.

If enabled, the user can dial the DTMF maps for enabling and disabling this service.

See the **ForwardingAddress**, **DefaultForwardOnBusyDtmfMapActivation**, and **DefaultForwardOnBusyDtmfMapDeactivation** parameters.

If a specific configuration is set in the **EpSpecificForwardOnBusy.Enable** parameter and the **EpSpecificForwardOnBusy.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultForwardOnBusyDtmfMapActivation (Config Parameter)

Type	DigitMap
Range	
Default	
Script/CLI	EpServ.DefaultForwardOnBusyDtmfMapActivation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.200.300

DTMF map the user can dial to enable the application of the service.
This DTMF map must follow the syntax for DTMF maps as declared in the DTMF maps configuration.

Note that dialing this DTMF map does not have any effect unless the service's status is 'enabled'.

See the **DefaultForwardOnBusyEnable** parameter.

DefaultForwardOnBusyDtmfMapDeactivation (Config Parameter)

Type	DigitMap
Range	
Default	
Script/CLI	EpServ.DefaultForwardOnBusyDtmfMapDeactivation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.200.400

DTMF map the user can dial to disable the application of the service.
This DTMF map must follow the syntax for DTMF maps as declared in the DTMF maps configuration.

Note that dialing this DTMF map does not have any effect unless the service's status is 'enabled'.

See the **DefaultForwardOnBusyEnable** parameter.

EpSpecificForwardOnBusy (Table)

EpId (Index) | Table: EpSpecificForwardOnBusy

Type	Text
Range	
Script/CLI	EpServ.EpSpecificForwardOnBusy[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.200.500.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificForwardOnBusy

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.EpSpecificForwardOnBusy[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.200.500.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultForwardOnBusyEnable** parameter.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificForwardOnBusy.Enable** parameter.

Enable (Config Parameter) | Table: EpSpecificForwardOnBusy

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.EpSpecificForwardOnBusy[].Enable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.200.500.1.300

Enables/Disables the call forward on busy service.
This service allows a user to forward incoming calls to a specified target when the user is already participating in another call.

The user does not have any feedback that a call was forwarded.

If enabled, the user can dial the DTMF maps for enabling and disabling this service.

See the **ForwardingAddress** parameter.

This configuration overrides the default configuration set in the **DefaultForwardOnBusyEnable** parameter if the **EpSpecificForwardOnBusy.EnableConfig** parameter is set to 'Enable'.

ForwardOnBusyConfig (Table)

A table of the call forward on busy activation for the endpoint, indexed by the endpoint ID.

EpId (Index) | Table: ForwardOnBusyConfig

Type	Text
Range	
Script/CLI	EpServ.ForwardOnBusyConfig[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.200.600.1.100

String that identifies an endpoint in other tables.

Activation (Config Parameter) | Table: ForwardOnBusyConfig

Type	ActiveInactive
Range	
Default	Inactive
Script/CLI	EpServ.ForwardOnBusyConfig[].Activation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.200.600.1.200

Activation status of the call forward on busy service.
Using the DTMF maps configured for this service, the user can use his/her handset to activate or deactivate this service. In that case, the parameter is automatically updated to reflect the activation status.

This service can also be activated or deactivated by setting the value of this parameter.

ForwardingAddress (Config Parameter) | Table: ForwardOnBusyConfig

Type	Text
Range	Size(0..127)
Default	
Script/CLI	EpServ.ForwardOnBusyConfig[].ForwardingAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.200.600.1.300

Address or telephone number to which the user wants to forward calls.

DefaultForwardNoAnswerEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.DefaultForwardNoAnswerEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.300.100

Enables/Disables the call forward on no answer service.
This service allows a user to forward incoming calls to a specified target when the user is unable to pick up the call before the timeout, specified by the **DefaultForwardNoAnswerTimeout** parameter, expires.

The user does not have any feedback that a call was forwarded.

If enabled, the user can dial the DTMF maps for enabling and disabling this service.

See the **ForwardingAddress**, **Timeout**, **DefaultForwardNoAnswerDtmfMapActivation** and **DefaultForwardNoAnswerDtmfMapDeactivation** parameters.

If a specific configuration is set in the **EpSpecificForwardNoAnswer.Enable** parameter and the **EpSpecificForwardNoAnswer.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultForwardNoAnswerTimeout (Config Parameter)

Type	UInt32
Range	200..120000
Default	5000
Script/CLI	EpServ.DefaultForwardNoAnswerTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.300.200

Time, in milliseconds, the telephone keeps ringing before the call forwarding activates.
If a specific configuration is set in the **EpSpecificForwardNoAnswer.Timeout** parameter and the **EpSpecificForwardNoAnswer.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultForwardNoAnswerDtmfMapActivation (Config Parameter)

Type	DigitMap
Range	
Default	
Script/CLI	EpServ.DefaultForwardNoAnswerDtmfMapActivation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.300.300

DTMF map the user can dial to enable the application of the service.
This DTMF map must follow the syntax for DTMF maps as declared in the DTMF maps configuration.

Note that dialing this DTMF map does not have any effect unless the service's status is 'enabled'.

See the **DefaultForwardNoAnswerEnable** parameter.

DefaultForwardNoAnswerDtmfMapDeactivation (Config Parameter)

Type	DigitMap
Range	
Default	
Script/CLI	EpServ.DefaultForwardNoAnswerDtmfMapDeactivation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.300.400

DTMF map the user can dial to disable the application of the service.

This DTMF map must follow the syntax for DTMF maps as declared in the DTMF maps configuration. Note that dialing this DTMF map does not have any effect unless the service's status is 'enabled'. See the **DefaultForwardNoAnswerEnable** parameter.

EpSpecificForwardNoAnswer (Table)

EpId (Index) | Table: EpSpecificForwardNoAnswer

Type	Text
Range	
Script/CLI	EpServ.EpSpecificForwardNoAnswer[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.300.500.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificForwardNoAnswer

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.EpSpecificForwardNoAnswer[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.300.500.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultForwardNoAnswerEnable** and **DefaultForwardNoAnswerTimeout** parameters.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificForwardNoAnswer.Enable** and **EpSpecificForwardNoAnswer.Timeout** parameters.

Enable (Config Parameter) | Table: EpSpecificForwardNoAnswer

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.EpSpecificForwardNoAnswer[].Enable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.300.500.1.300

Enables/Disables the call forward on no answer service.
This service allows a user to forward incoming calls to a specified target when the user is unable to pick up the call before the timeout, specified by Timeout, expires.

The user does not have any feedback that a call was forwarded.

If enabled, the user can dial the DTMF maps for enabling and disabling this service.

See the **ForwardingAddress** and **Timeout** parameters.

This configuration overrides the default configuration set in the **DefaultForwardNoAnswerEnable** parameter if the **EpSpecificForwardNoAnswer.EnableConfig** parameter is set to 'Enable'.

Timeout (Config Parameter) | Table: EpSpecificForwardNoAnswer

Type	UInt32
Range	200..120000
Default	5000
Script/CLI	EpServ.EpSpecificForwardNoAnswer[].Timeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.300.500.1.400

Time, in milliseconds, the telephone keeps ringing before the call forwarding activates.
This configuration overrides the default configuration set in the **DefaultForwardNoAnswerTimeout** parameter if the **EpSpecificForwardNoAnswer.EnableConfig** parameter is set to 'Enable'.

ForwardNoAnswerConfig (Table)

A table of the call forward no answer activation for the endpoint, indexed by the endpoint ID.

EpId (Index) | Table: ForwardNoAnswerConfig

Type	Text
Range	
Script/CLI	EpServ.ForwardNoAnswerConfig[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.300.600.1.100

String that identifies an endpoint in other tables.

Activation (Config Parameter) | Table: ForwardNoAnswerConfig

Type	ActiveInactive
Range	
Default	Inactive
Script/CLI	EpServ.ForwardNoAnswerConfig[].Activation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.300.600.1.200

Activation status of the call forward on no answer service.
Using the DTMF maps configured for this service, the user can use his/her handset to activate or deactivate this service. In that case, the parameter is automatically updated to reflect the activation status.

This service can also be activated or deactivated by setting the value of this parameter.

ForwardingAddress (Config Parameter) | Table: ForwardNoAnswerConfig

Type	Text
Range	Size(0..127)
Default	
Script/CLI	EpServ.ForwardNoAnswerConfig[].ForwardingAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.800.300.600.1.300

Address or telephone number to which the user wants to forward calls.

DefaultCallCompletionBusySubscriberEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.DefaultCallCompletionBusySubscriberEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.900.100

Enables/Disables the completion of calls to busy subscriber (CCBS) service.
This service allows a caller to establish a call with a 'busy' called as soon as this called is available to take the call.

If a specific configuration is set in the **EpSpecificCallCompletion.BusySubscriberEnable** parameter and the **EpSpecificCallCompletion.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultCallCompletionBusySubscriberDtmfMapActivation (Config Parameter)

Type	DigitMap
Range	
Default	
Script/CLI	EpServ.DefaultCallCompletionBusySubscriberDtmfMapActivation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.900.200

DTMF map the user can dial to enable the application of the completion of calls to busy subscriber (CCBS) service.
This DTMF map must follow the syntax for DTMF maps as declared in the DTMF maps configuration.

The same code can be used in **DefaultCallCompletionBusySubscriberDtmfMapActivation** and **DefaultCallCompletionNoReplyDtmfMapActivation** parameters.

Note that dialing this DTMF map does not have any effect unless the service's status is 'enabled'.

See the **DefaultCallCompletionBusySubscriberEnable** parameter.

DefaultCallCompletionNoReplyEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.DefaultCallCompletionNoReplyEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.900.300

Enables/Disables the completion of calls on no reply (CCNR) service.
This service allows a caller to establish a call with an 'idle' called right after this called uses his phone and is available to take the call.

If a specific configuration is set in the **EpSpecificCallCompletion.NoReplyEnable** parameter and the **EpSpecificCallCompletion.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultCallCompletionNoReplyDtmfMapActivation (Config Parameter)

Type	DigitMap
Range	
Default	
Script/CLI	EpServ.DefaultCallCompletionNoReplyDtmfMapActivation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.900.400

DTMF map the user can dial to enable the application of the completion of calls on no reply (CCNR) service.
This DTMF map must follow the syntax for DTMF maps as declared in the DTMF maps configuration.

The same code can be used in **DefaultCallCompletionBusySubscriberDtmfMapActivation** and **DefaultCallCompletionNoReplyDtmfMapActivation** parameters.

Note that dialing this DTMF map does not have any effect unless the service's status is 'enabled'.

See the **DefaultCallCompletionNoReplyEnable** parameter.

DefaultCallCompletionDtmfMapDeactivation (Config Parameter)

Type	DigitMap
Range	
Default	
Script/CLI	EpServ.DefaultCallCompletionDtmfMapDeactivation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.900.500

DTMF map the user can dial to disable the application of the completion of calls to busy subscriber (CCBS) and completion of calls on no reply (CCNR) services.
This DTMF map must follow the syntax for DTMF maps as declared in the DTMF maps configuration.

Note that dialing this DTMF map does not have any effect unless the service's status is 'enabled'.

See the **DefaultCallCompletionBusySubscriberEnable** parameter and **DefaultCallCompletionNoReplyEnable**.

DefaultCallCompletionExpirationTimeout (Config Parameter)

Type	UInt32
Range	1..1440
Default	180
Script/CLI	EpServ.DefaultCallCompletionExpirationTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.900.600

Defines the delay after the call completion activation to automatically deactivate the call completion if the call is not completed.
This value is expressed in minutes (m).

DefaultCallCompletionMethod (Config Parameter)

Type	Enum
Range	MonitoringOnly(100) | MonitoringAndPolling(200)
Default	MonitoringOnly
Script/CLI	EpServ.DefaultCallCompletionMethod
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.900.650

Selects the call completion method to detect that the call completion destination is ready to complete the call.

- MonitoringOnly: The call completion only uses the monitoring method to detect that the destination is ready to complete the call.
- MonitoringAndPolling: The call completion only uses the monitoring method to detect that the destination is ready to complete the call. The polling mechanism is used if the call completion destination cannot be monitored.

The monitoring method consists of using the protocol signalling to detect the destination state without using the call. When the destination is ready to complete the call, the local user is notified that the call is ready to be completed and the call to the destination is initiated when the user is ready to initiate the call.

The polling method consists of using periodic calls to the call completion destination until the destination responds with a ringing or connect. Upon receiving these responses, the local user is notified that the call is ready to be completed.

The polling mechanism can only be used for call completion to busy subscriber (CCBS).

The retransmission of the polling mechanism is configurable with **DefaultCallCompletionPollingInterval**.

DefaultCallCompletionAutoReactivateEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.DefaultCallCompletionAutoReactivateEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.900.700

Enables/Disables the call completion auto reactivation.
When enabled, the completion of calls to busy is automatically activated if the call initiated by a completion of calls to busy or a completion of calls on no reply fails because of a busy destination.

DefaultCallCompletionAutoReactivateDelay (Config Parameter)

Type	UInt32
Range	0..600
Default	30
Script/CLI	EpServ.DefaultCallCompletionAutoReactivateDelay
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.900.750

Defines the minimal delay to wait before executing a call completion after its activation. This delay only applies to call completion activated via the call completion auto reactivation feature.
It is recommended to set a delay when the method to monitor the target state is based on the target calls instead of its ability to answer a call.

This parameter is not used if the **DefaultCallCompletionAutoReactivateEnable** parameter is set to 'Disable'.

This value is expressed in seconds (s).

DefaultCallCompletionEarlyMediaBehaviour (Config Parameter)

Type	Enum
Range	None(100) | Ccbs(200) | Ccnr(300)
Default	None
Script/CLI	EpServ.DefaultCallCompletionEarlyMediaBehaviour
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.900.775

Defines how the call completion service needs to interpret the reception of a progress message with early media.

- None: The progress message with early media is not considered as a busy or a ringing response.
- Ccbs: The progress message with early media is interpreted as a busy response and the CCBS can be activated on the call.
- Ccnr: The progress message with early media is interpreted as a ringing response and the CCNR can be activated on the call.

EpSpecificCallCompletion (Table)

EpId (Index) | Table: EpSpecificCallCompletion

Type	Text
Range	
Script/CLI	EpServ.EpSpecificCallCompletion[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.900.800.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificCallCompletion

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.EpSpecificCallCompletion[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.900.800.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultCallCompletionBusySubscriberEnable** and **DefaultCallCompletionNoReplyEnable** parameters.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificCallCompletion.BusySubscriberEnable** and **EpSpecificCallCompletion.NoReplyEnable** parameters.

BusySubscriberEnable (Config Parameter) | Table: EpSpecificCallCompletion

Type	EnableDisable
Range	
Default	Enable
Script/CLI	EpServ.EpSpecificCallCompletion[].BusySubscriberEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.900.800.1.300

Enables/Disables the completion of calls to busy subscriber (CCBS) service.
This service allows a caller to establish a call with a 'busy' called as soon as this called is available to take the call.

This configuration overrides the default configuration set in the **DefaultCallCompletionBusySubscriberEnable** parameter if the **EpSpecificCallCompletion.EnableConfig** parameter is set to 'Enable'.

NoReplyEnable (Config Parameter) | Table: EpSpecificCallCompletion

Type	EnableDisable
Range	
Default	Enable
Script/CLI	EpServ.EpSpecificCallCompletion[].NoReplyEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.900.800.1.400

Enables/Disables the completion of calls on no reply (CCNR) service.
This service allows a caller to establish a call with an 'idle' called right after this called uses his phone and is available to take the call.

This configuration overrides the default configuration set in the **DefaultCallCompletionNoReplyEnable** parameter if the **EpSpecificCallCompletion.EnableConfig** parameter is set to 'Enable'.

CallCompletionConfig (Table)

A table of the call completion configuration on the unit.

Index (Index) | Table: CallCompletionConfig

Type	UInt32
Range	
Script/CLI	EpServ.CallCompletionConfig[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.900.900.1.100

Unique identifier of the row.

EpId (Status Parameter) | Table: CallCompletionConfig

Type	Text
Range	
Script/CLI	EpServ.CallCompletionConfig[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.900.900.1.200

Identification of the endpoint using this call completion service.

Type (Status Parameter) | Table: CallCompletionConfig

Type	Enum
Range	Ccbs(100) | Ccnr(200)
Script/CLI	EpServ.CallCompletionConfig[].Type
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.900.900.1.300

The type of the call completion.

- Ccbs : Completion of calls to busy subscriber.
- Ccnr : Completion of calls on no reply.

TargetAddress (Status Parameter) | Table: CallCompletionConfig

Type	Text
Range	
Script/CLI	EpServ.CallCompletionConfig[].TargetAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.900.900.1.400

The target address of the call completion.
This address is the final address after manipulation of the call router.

TargetState (Status Parameter) | Table: CallCompletionConfig

Type	Enum
Range	Unknown(100) | Idle(200) | Busy(300)
Script/CLI	EpServ.CallCompletionConfig[].TargetState
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.900.900.1.500

The state of the call completion target.

- Unknown : The destination state is unknown.
- Idle : The destination is currently idle.
- Busy : The destination is currently busy.

DefaultCallCompletionPollingInterval (Config Parameter)

Type	UInt32
Range	5..3600
Default	5
Script/CLI	EpServ.DefaultCallCompletionPollingInterval
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.900.10000.780

Defines the delay between the calls to the call completion target used for the polling mechanism. This parameter is used only if the **DefaultCallCompletionMethod** is set to 'MonitoringAndPolling'.

This value is expressed in second (s).

DefaultDelayedHotlineEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.DefaultDelayedHotlineEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.1000.100

Enables/Disables the delayed hotline service. This service is also called warm line.
The delayed hotline allows the user to call a particular destination without dialling. The configured destination is called by picking up the phone and waiting for a configurable number of seconds without dialling.

The delayed hotline can also be configured to be initiated if the user does not dial a complete sequence of digits in an allowed time period.

The condition to execute the delayed hotline is configurable with the **DefaultDelayedHotlineCondition** parameter and the destination with the **DefaultDelayedHotlineTargetAddress** parameter.

If a specific configuration is set in the **EpSpecificDelayedHotline.Enable** parameter and the **EpSpecificDelayedHotline.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultDelayedHotlineCondition (Config Parameter)

Type	Enum
Range	FirstDtmfTimeout(100) | InterDtmfOrCompletionTimeout(200) | AnyTimeout(300)
Default	FirstDtmfTimeout
Script/CLI	EpServ.DefaultDelayedHotlineCondition
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.1000.200

Selects the condition(s) that activate the delayed hotline.

- FirstDtmfTimeout: The delayed hotline is activated when the timeout configured in **DtmfMapTimeoutFirstDtmf** elapse.
- InterDtmfOrCompletionTimeout: The delayed hotline is activated when the timeout configured in **DtmfMapTimeoutCompletion** elapses or the DTMFs collection fails because the **DtmfMapTimeoutInterDtmf** elapses.
- AnyTimeout: The delayed hotline is activated for the condition of 'FirstDtmfTimeout' and 'InterDtmfOrCompletionTimeout'.

If a specific configuration is set in the **EpSpecificDelayedHotline.Condition** parameter and the **EpSpecificDelayedHotline.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultDelayedHotlineTargetAddress (Config Parameter)

Type	Text
Range	Size(0..127)
Default	
Script/CLI	EpServ.DefaultDelayedHotlineTargetAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.1000.300

Address or telephone number of the target of the delayed hotline.
If a specific configuration is set in the **EpSpecificDelayedHotline.TargetAddress** parameter and the **EpSpecificDelayedHotline.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

EpSpecificDelayedHotline (Table)

A table of the telephony features configuration for the dlayed hotline, indexed by the endpoint ID.

EpId (Index) | Table: EpSpecificDelayedHotline

Type	Text
Range	
Script/CLI	EpServ.EpSpecificDelayedHotline[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.1000.1000.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificDelayedHotline

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.EpSpecificDelayedHotline[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.1000.1000.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultDelayedHotlineEnable**, **DefaultDelayedHotlineCondition** and **DefaultDelayedHotlineTargetAddress** parameters.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificDelayedHotline.Enable**, **EpSpecificDelayedHotline.Condition** and **EpSpecificDelayedHotline.TargetAddress** parameters.

Enable (Config Parameter) | Table: EpSpecificDelayedHotline

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.EpSpecificDelayedHotline[].Enable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.1000.1000.1.300

Enables/Disables the delayed hotline service. This service is also called warm line.
The delayed hotline allows the user to call a particular destination without dialling. The configured destination is called by picking up the phone and waiting for a configurable number of seconds without dialling.

The delayed hotline can also be configured to be initiated if the user does not dial a complete sequence of digits in an allowed time period.

The condition to execute the delayed hotline is configurable with the parameter **DefaultDelayedHotlineCondition** and the destination with the parameter **DefaultDelayedHotlineTargetAddress**.

This configuration overrides the default configuration set in the **DefaultDelayedHotlineEnable** parameter if the **EpSpecificDelayedHotline.EnableConfig** parameter is set to 'Enable'.

Condition (Config Parameter) | Table: EpSpecificDelayedHotline

Type	Enum
Range	FirstDtmfTimeout(100) | InterDtmfOrCompletionTimeout(200) | AnyTimeout(300)
Default	FirstDtmfTimeout
Script/CLI	EpServ.EpSpecificDelayedHotline[].Condition
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.1000.1000.1.400

Select the condition(s) that activate the delayed hotline.

- FirstDtmfTimeout: The delayed hotline is activated when the timeout configured in **DtmfMapTimeoutFirstDtmf** elapse.
- InterDtmfOrCompletionTimeout: The delayed hotline is activated when the timeout configured in **DtmfMapTimeoutCompletion** elapses or the DTMFs collection fails because the **DtmfMapTimeoutInterDtmf** elapses.
- AnyTimeout: The delayed hotline is activated for the condition of 'FirstDtmfTimeout' and 'InterDtmfOrCompletionTimeout'.

This configuration overrides the default configuration set in the **DefaultDelayedHotlineCondition** parameter if the **EpSpecificDelayedHotline.EnableConfig** parameter is set to 'Enable'.

TargetAddress (Config Parameter) | Table: EpSpecificDelayedHotline

Type	Text
Range	Size(0..127)
Default	
Script/CLI	EpServ.EpSpecificDelayedHotline[].TargetAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.1000.1000.1.500

Address or telephone number of the target of the delayed hotline.
This configuration overrides the default configuration set in the **DefaultDelayedHotlineTargetAddress** parameter if the **EpSpecificDelayedHotline.EnableConfig** parameter is set to 'Enable'.

CallStatistics (Table)

Call statistics per endpoint.

EpId (Index) | Table: CallStatistics

Type	Text
Range	
Script/CLI	EpServ.CallStatistics[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.1200.100.1.100

String that identifies an endpoint in other tables.

IncomingCallsReceived (Status Parameter) | Table: CallStatistics

Type	UInt32
Range	
Script/CLI	EpServ.CallStatistics[].IncomingCallsReceived
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.1200.100.1.200

Number of incoming IP calls received on the endpoint since service start. This value is updated at the end of the call.

IncomingCallsAnswered (Status Parameter) | Table: CallStatistics

Type	UInt32
Range	
Script/CLI	EpServ.CallStatistics[].IncomingCallsAnswered
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.1200.100.1.300

Number of incoming IP calls answered on the endpoint since service start. This value is updated at the end of the call.

IncomingCallsConnected (Status Parameter) | Table: CallStatistics

Type	UInt32
Range	
Script/CLI	EpServ.CallStatistics[].IncomingCallsConnected
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.1200.100.1.400

Number of incoming IP calls that successfully completed call setup signaling on the endpoint since service start. This value is updated at the end of the call.

IncomingCallsFailed (Status Parameter) | Table: CallStatistics

Type	UInt32
Range	
Script/CLI	EpServ.CallStatistics[].IncomingCallsFailed
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.1200.100.1.500

Number of incoming IP calls that failed to complete call setup signaling on the endpoint since service start. This value is updated at the end of the call.

OutgoingCallsAttempted (Status Parameter) | Table: CallStatistics

Type	UInt32
Range	
Script/CLI	EpServ.CallStatistics[].OutgoingCallsAttempted
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.1200.100.1.600

Number of outgoing IP calls attempted for the endpoint since service start. This value is updated at the end of the call.

OutgoingCallsAnswered (Status Parameter) | Table: CallStatistics

Type	UInt32
Range	
Script/CLI	EpServ.CallStatistics[].OutgoingCallsAnswered
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.1200.100.1.700

Number of outgoing IP calls answered by the called party for the endpoint since service start. This value is updated at the end of the call.

OutgoingCallsConnected (Status Parameter) | Table: CallStatistics

Type	UInt32
Range	
Script/CLI	EpServ.CallStatistics[].OutgoingCallsConnected
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.1200.100.1.800

Number of outgoing IP calls that successfully completed call setup signaling for the endpoint since service start. This value is updated at the end of the call.

OutgoingCallsFailed (Status Parameter) | Table: CallStatistics

Type	UInt32
Range	
Script/CLI	EpServ.CallStatistics[].OutgoingCallsFailed
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.1200.100.1.900

Number of outgoing IP calls that failed to complete call setup signaling for the endpoint since service start. This value is updated at the end of the call.

CallsDropped (Status Parameter) | Table: CallStatistics

Type	UInt32
Range	
Script/CLI	EpServ.CallStatistics[].CallsDropped
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.1200.100.1.1000

Number of IP calls, on the endpoint since service start, that were successfully connected (incoming or outgoing), but dropped unexpectedly while in progress without explicit user termination.

TotalCallTime (Status Parameter) | Table: CallStatistics

Type	UInt32
Range	
Script/CLI	EpServ.CallStatistics[].TotalCallTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.1200.100.1.1100

Cumulative duration of all IP calls on the endpoint since service start, in seconds. This value is updated at the end of the call.

Reset (Row Command) | Table: CallStatistics

Script/CLI:	EpServ.CallStatistics[].Reset
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.1200.100.1.1200

Sets all the values in the row to zero.

DtmfMapTimeoutCompletion (Config Parameter)

Type	UInt32
Range	1000..180000
Default	60000
Script/CLI	EpServ.DtmfMapTimeoutCompletion
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.20000.100

Total time the user has to dial the DTMF sequence. The timer starts when the dial tone is played. When the timer expires, the receiver off-hook tone is played.
This value is expressed in milliseconds (ms).

If a specific configuration is set in the **EpSpecificDtmfMapTimeout.Completion** parameter and the **EpSpecificDtmfMapTimeout.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DtmfMapTimeoutFirstDtmf (Config Parameter)

Type	UInt32
Range	1000..180000
Default	20000
Script/CLI	EpServ.DtmfMapTimeoutFirstDtmf
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.20000.200

Time the user has to enter the first DTMF after the dial tone. A receiver off-hook is played when the time has elapsed.
This value is expressed in milliseconds (ms).

If a specific configuration is set in the **EpSpecificDtmfMapTimeout.FirstDtmf** parameter and the **EpSpecificDtmfMapTimeout.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DtmfMapTimeoutInterDtmf (Config Parameter)

Type	UInt32
Range	500..10000
Default	3000
Script/CLI	EpServ.DtmfMapTimeoutInterDtmf
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.20000.300

Value of the 'T' DTMF in the DTMF map strings.
The 'T' DTMF is used to express a time lapse between the detection of two DTMFs.

This value is expressed in milliseconds (ms).

If a specific configuration is set in the **EpSpecificDtmfMapTimeout.InterDtmf** parameter and the **EpSpecificDtmfMapTimeout.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

EpSpecificDtmfMapTimeout (Table)

A table of the DTMF Map timeout configuration, indexed by the endpoint ID.

EpId (Index) | Table: EpSpecificDtmfMapTimeout

Type	Text
Range	
Script/CLI	EpServ.EpSpecificDtmfMapTimeout[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.20000.1000.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificDtmfMapTimeout

Type	EnableDisable
Range	
Default	Disable
Script/CLI	EpServ.EpSpecificDtmfMapTimeout[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.20000.1000.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DtmfMapTimeoutCompletion**, **DtmfMapTimeoutFirstDtmf** and **DtmfMapTimeoutInterDtmf** parameters.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificDtmfMapTimeout.Completion**, **EpSpecificDtmfMapTimeout.FirstDtmf** and **EpSpecificDtmfMapTimeout.InterDtmf** parameters.

Completion (Config Parameter) | Table: EpSpecificDtmfMapTimeout

Type	UInt32
Range	1000..180000
Default	60000
Script/CLI	EpServ.EpSpecificDtmfMapTimeout[].Completion
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.20000.1000.1.300

Total time the user has to dial the DTMF sequence. The timer starts when the dial tone is played. When the timer expires, the receiver off-hook tone is played.
This value is expressed in milliseconds (ms).

This configuration overrides the default configuration set in the **DtmfMapTimeoutCompletion** parameter if the **EpSpecificDtmfMapTimeout.EnableConfig** parameter is set to 'Enable'.

FirstDtmf (Config Parameter) | Table: EpSpecificDtmfMapTimeout

Type	UInt32
Range	1000..180000
Default	20000
Script/CLI	EpServ.EpSpecificDtmfMapTimeout[].FirstDtmf
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.20000.1000.1.400

Time the user has to enter the first DTMF after the dial tone. A receiver off-hook is played when the time has elapsed.
This value is expressed in milliseconds (ms).

This configuration overrides the default configuration set in the **DtmfMapTimeoutFirstDtmf** parameter if the **EpSpecificDtmfMapTimeout.EnableConfig** parameter is set to 'Enable'.

InterDtmf (Config Parameter) | Table: EpSpecificDtmfMapTimeout

Type	UInt32
Range	500..10000
Default	3000
Script/CLI	EpServ.EpSpecificDtmfMapTimeout[].InterDtmf
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.20000.1000.1.500

Value of the 'T' DTMF in the DTMF map strings.
The 'T' DTMF is used to express a time lapse between the detection of two DTMFs.

This value is expressed in milliseconds (ms).

This configuration overrides the default configuration set in the **DtmfMapTimeoutInterDtmf** parameter if the **EpSpecificDtmfMapTimeout.EnableConfig** parameter is set to 'Enable'.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	EpServ.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	EpServ.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1700.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the EpServ service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.1700.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	The endpoint %1$s holds the call %2$d.	Debug	The endpoint has put the call on hold.
20	The endpoint %1$s unholds the call %2$d.	Debug	The endpoint has put the call off hold.
30	The endpoint %1$s receives the call %2$d on call waiting.	Debug	The endpoint received a new call while it already has an active call. The call waiting feature is used to alert the user that a new call is waiting for an answer.
40	The endpoint %1$s initiates a second call.	Debug	The endpoint has a call on hold and initiates a second call.
50	The endpoint %1$s initiates a blind transfer between call %2$d and %3$d.	Debug	The endpoint initiates a blind transfer between the call on hold and the second call.
55	The endpoint %1$s initiates a blind transfer from call %2$d to destination %3$s.	Debug	The endpoint initiates a blind transfer of the call on hold to the dialed destination.
60	The endpoint %1$s initiates an attended transfer between call %2$d and %3$d.	Debug	The endpoint initiates an attended transfer between the call on hold and the second call.
70	The endpoint %1$s initiates a conference with call %2$d and call %3$d.	Debug	The endpoint initiates a conference between the call on hold and the second call.
75	The endpoint %1$s failed to initiates a conference because no resource is available.	Error	The endpoint cannot initiate a conference because they cannot allocate the supplementary resource required to perform a conference.
80	The endpoint %1$s terminates the conference with call %2$d and call %3$d.	Debug	The endpoint terminates the conference between the call on hold and the second call.
85	The conference service is disabled on the endpoint %1$s due to a wrong configuration.	Error	The EpServ service cannot enable the conference service. This occurs when the **EpServ.DefaultConferenceType** parameter is set to 'ConferenceServer' and no conference server was set in the **SipEp.DefaultStaticConferenceServerUri** parameter.

NumKey	Message	Severity	Description
90	The endpoint %1$s forwards to %2$s a call on busy.	Debug	The endpoint has forwarded an incoming call because it was busy. This action can only occur when the call forward on busy is enabled.
100	The endpoint %1$s forwards to %2$s a call on no answer.	Debug	The endpoint has forwarded an incoming call because the user did not respond within the required time. This action can only occur when the call forward on no answer is enabled.
110	The endpoint %1$s forwards to %2$s a call unconditional.	Debug	The endpoint has forwarded an incoming call. This action can only occur when the call forward unconditional is enabled.
120	The endpoint %1$s activates the completion of calls to busy subscriber to %2$s.	Debug	The endpoint has activated the completion of calls to busy subscriber service to the specified destination.
130	The endpoint %1$s deactivates the completion of calls to busy subscriber to %2$s.	Debug	The endpoint has deactivated the completion of calls to busy subscriber service to the specified destination.
140	The endpoint %1$s completed the completion of calls to busy subscriber to %2$s.	Debug	The endpoint has completed the completion of calls to busy subscriber by calling the specified destination.
150	The completion of calls to busy subscriber to %2$s on the endpoint %1$s is expired.	Debug	The completion of calls to busy subscriber is deactivated because the timeout is expired.
160	The endpoint %1$s activates the completion of calls on no reply to %2$s.	Debug	The endpoint has activated the completion of calls on no reply service to the specified destination.
170	The endpoint %1$s deactivates the completion of calls on no reply to %2$s.	Debug	The endpoint has deactivated the completion of calls on no reply service to the specified destination.
180	The endpoint %1$s completed the completion of calls on no reply to %2$s.	Debug	The endpoint has completed the completion of calls on no reply by calling the specified destination.

NumKey	Message	Severity	Description
190	The completion of calls on no reply to %2$s on the endpoint %1$s is expired.	Debug	The completion of calls on no reply is deactivated because the timeout is expired.
200	The endpoint %1$s reactivated the call completion to %2$s.	Debug	The endpoint has reactivated the call completion service to the specified destination. The endpoint is now using a completion of call to busy subscriber.
210	The endpoint %1$s fails to monitor the status of %2$s.	Error	The endpoint cannot activate the call completion service to the destination because the monitoring of the destination state cannot be initiated.
220	The %1$s endpoint activates the call waiting service using the configured DTMF map.	Debug	The endpoint activates the call waiting service by dialing the configured DTMF map.
230	The %1$s endpoint deactivates the call waiting service using the configured DTMF map.	Debug	The endpoint deactivates the call waiting service by dialing the configured DTMF map.
240	The %1$s endpoint deactivates the call waiting service for the next call using the configured DTMF map.	Debug	The endpoint deactivates the call waiting service before making the call by dialing the configured DTMF map.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.

NumKey	Message	Severity	Description
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.

NumKey	Message	Severity	Description
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to EpServ.

Message	Severity	Description
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.

Message	Severity	Description
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Ethernet Manager (Eth)

The Ethernet Manager (Eth) service is a DGW system service that manages the unit Ethernet link interfaces.

Parameters

LinkStatus (Table)

This table displays the status of all available Ethernet links.

LinkName (Index) | Table: LinkStatus

Type	Text
Range	
Script/CLI	Eth.LinkStatus[].LinkName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.25.1.100

Name of the link interface.

LinkType (Status Parameter) | Table: LinkStatus

Type	Text
Range	
Script/CLI	Eth.LinkStatus[].LinkType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.25.1.200

Type of link interface.

LinkState (Status Parameter) | Table: LinkStatus

Type	Enum
Range	Disconnected(100) | Up(200)
Script/CLI	Eth.LinkStatus[].LinkState
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.25.1.300

Indicates the status of the Ethernet link interface.

- Disconnected: The link interface is physically disconnected.
- Up: The link interface is physically connected and considered as usable by network interfaces.

Links (Table)

This table allows configuring the Ethernet links of the unit.

Name (Index) | Table: Links

Type	Text
Range	
Script/CLI	Eth.Links[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.50.1.100

The name of the Ethernet link.

Mtu (Config Parameter) | Table: Links

Type	UInt32
Range	576..1500
Default	1500
Script/CLI	Eth.Links[].Mtu
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.50.1.200

To configure the MTU (Maximum Transmission Unit) of a specific Ethernet link. All VLAN connections use the MTU size configured on the Ethernet link they are linked to.
The MTU value applied to a PPPoE connection is the smallest value chosen between the value negotiated with the server and the value configured here.

Range: 576 to 1500 bytes.

Ieee8021XAuthentication (Config Parameter) | Table: Links

Type	Enum
Range	Disable(100) | Enable(200)
Default	Disable
Script/CLI	Eth.Links[].Ieee8021XAuthentication
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.50.1.300

To configure the IEEE 802.1x authentication protocol activation on the Ethernet link interface. Possible values are:

- Disable: The IEEE 802.1x authentication protocol is disabled on the Ethernet link interface.
- Enable: The IEEE 802.1x authentication protocol using the EAP-TLS authentication method is enabled on the Ethernet link to allow the access to secured network(s) through an IEEE 802.1x EAP-TLS authenticator (such as an IEEE 802.1x capable network device). The Ethernet link interface remains always 'UP' whatever the result of the IEEE 802.1x authentication.

VirtualSwitch (Config Parameter) | Table: Links

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Eth.Links[].VirtualSwitch
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.50.1.400

To configure the link as a virtual switch. Possible values are:

- Disable: The link cannot be used to provide network access to virtual machines.
- Enable: The link can be used to provide network access to virtual machines.

The Virtual Switch parameter can only be enabled on Sentinel 400 units that support the Virtual Machine (VM) service.

IgnoreLinkDown (Config Parameter) | Table: Links

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Eth.Links[].IgnoreLinkDown
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.50.1.500

To configure the Ignore Link Down feature.

- Disable: The Link state and events are reported normally to the application. Normal behavior.
- Enable: Cable disconnections (Link Down) events are ignored and the link appears Up for the application.

The overall behavior is similar to having the unit connected to an ethernet switch that gets disconnected from the network: the ethernet interface stays Up while network connection is lost.

This feature solves a problem in configurations where two parts of Dgw communicate together through a "real" ethernet interface instead of the loopback. For instance in a survivability use case where the calls flow between a gateway and the SBC. Normally, when the link is down, communication is lost between them. Using this feature, communication still works.

Notes:

- Static IP addresses must be used on the links configured with this feature.

- If using the loopback interface is possible instead of using this feature, it is likely a better choice.
- This feature is not supported on the Sentinel CS.

PortsStatus (Table)

This table displays the status of all Ethernet connectors of the unit.

Name (Index) | Table: PortsStatus

Type	Text
Range	
Script/CLI	Eth.PortsStatus[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.100.1.100

The name of the Ethernet port.

LinkName (Status Parameter) | Table: PortsStatus

Type	Text
Range	
Script/CLI	Eth.PortsStatus[].LinkName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.100.1.200

The link interface associated with the Ethernet port.

Connection (Status Parameter) | Table: PortsStatus

Type	Enum
Range	Disconnected(0) | Half10(100) | Full10(200) | Half100(300) | Full100(400) | Full1000(500) | LinkIgnored(600)
Script/CLI	Eth.PortsStatus[].Connection
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.100.1.300

The speed, duplex, and state of the connection. The possible values are:

- Disconnected: This port is physically disconnected.

- Half10: This port is connected at 10 Mbit/s Half-duplex.
- Full10: This port is connected at 10 Mbit/s Full-duplex.
- Half100: This port is connected at 100 Mbit/s Half-duplex.
- Full100: This port is connected at 100 Mbit/s Full-duplex.
- Full1000: This port is connected at 1 Gbit/s Full-duplex.
- LinkIgnored: This port is disconnected, but the **IgnoreLinkDown** feature makes it appear as connected.

Ports (Table)

This table allows the configuration of the unit Ethernet ports.

Name (Index) | Table: Ports

Type	Text
Range	
Script/CLI	Eth.Ports[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.200.1.100

The name of the Ethernet port.

Speed (Config Parameter) | Table: Ports

Type	Enum
Range	Auto(100) | Half10(200) | Full10(300) | Half100(400) | Full100(500) | Full1000(600)
Default	Auto
Script/CLI	Eth.Ports[].Speed
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.200.1.200

To configure the speed and duplex of the connection. Possible values are:

- Auto: Automatic negociation of speed and duplex.
- Half10: 10 Mbit/s Half-duplex.
- Full10: 10 Mbit/s Full-duplex.
- Half100: 100 Mbit/s Half-duplex.
- Full100: 100 Mbit/s Full-duplex.

- Full1000: 1 Gbit/s Full-duplex.

Vlan (Table: user-defined, 16 lines max.)

This table allows the configuration of the Ethernet Virtual LAN interfaces of the system.

Idx (Index) | Table: Vlan

Type	UInt32
Range	
Script/CLI	Eth.Vlan[].Idx
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.300.1.50

Unique identifier of the row in the table.

LinkName (Config Parameter) | Table: Vlan

Type	Text
Range	Size(0..10)
Default	
Script/CLI	Eth.Vlan[].LinkName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.300.1.100

Name of the Ethernet link used by the VLAN interface.

VlanId (Config Parameter) | Table: Vlan

Type	UInt32
Range	0..4094
Default	0
Script/CLI	Eth.Vlan[].VlanId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.300.1.200

VLAN ID used by the VLAN interface.

DefaultUserPriority (Config Parameter) | Table: Vlan

Type	UInt32
Range	0..7
Default	0
Script/CLI	Eth.Vlan[].DefaultUserPriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.300.1.300

Default User Priority value the interface uses when tagging packets. Specific service class values may be set in the Local Quality of Service (LQos) in the **LQos.ServiceClasses** table.

ConfigStatus (Status Parameter) | Table: Vlan

Type	Enum
Range	ValidConfig(100)| InvalidLinkName(200) | InvalidVlanId(300) | DuplicateLinkVlanId(400)
Script/CLI	Eth.Vlan[].ConfigStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.300.1.350

Configuration status of the row.
It indicates whether the configuration of the row is valid or not. Possible values are:

- ValidConfig: This entry is valid.
- InvalidLinkName: The entry is not valid because the **Eth.LinkName** parameter is either empty or refers to a link that does not exists.
- InvalidVlanId: This entry is not valid because VlanId 0 is invalid.
- DuplicateLinkVlanId: This entry is not valid because the VLAN ID is already used.

Delete (Row Command) | Table: Vlan

Script/CLI:	Eth.Vlan[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.300.1.400

Deletes the VLAN interface and removes it from the system.

Eap (Table)

This table allows the configuration of the EAP settings.

Name (Index) | Table: Eap

Type	Text
Range	
Script/CLI	Eth.Eap[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.10000.100.1.100

The name of the Ethernet link.

Username (Config Parameter) | Table: Eap

Type	Text
Range	Size(0..64)
Default	
Script/CLI	Eth.Eap[].Username
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.10000.100.1.200

Username used to authenticate each Ethernet link interfaces during the IEEE 802.1x EAP-TLS authentication process. This parameter is used only when the IEEE 802.1x authentication is enabled (**Links.Ieee8021XAuthentication** set to Enabled).

CertificateValidation (Config Parameter) | Table: Eap

Type	Enum
Range	NoValidation(100) | TrustedAndValid(200)
Default	TrustedAndValid
Script/CLI	Eth.Eap[].CertificateValidation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.10000.100.1.300

Level of validation used by the device to authenticate the IEEE 802.1x EAP-TLS peer's certificate. This parameter also controls the criteria used to select the host certificate sent during the authentitication handshake. Possible values are:

- NoValidation: No validation is performed on the peer's certificate. Authentication with the peer is attempted even if the system time is not synchronised. If more than one host certificate is configured for an EAP-TLS usage, the one with the latest expiration date is used.
- TrustedAndValid: Allow a connection to the network by validating if the authentication peer's certificate is trusted and valid. The IEEE 802.1x authentication is attempted only if the system time is synchronised. If more than one host certificate is configured for an EAP-TLS usage, the one that is currently valid and with the latest expiration date is used.

Ieee8021XVersion (Config Parameter)

Type	Enum
Range	Ieee8021X2001(100) | Ieee8021X2004(200)
Default	Ieee8021X2001
Script/CLI	Eth.Ieee8021XVersion
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.10000.200

Version of IEEE 802.1X used by the unit.

EapTlsCipherSuite (Config Parameter)

Type	Enum
Range	CS1(100) | CS2(200) | CS3(300)
Default	CS1
Script/CLI	Eth.EapTlsCipherSuite
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.10000.300

Defines the allowed TLS cipher suites used during the IEEE 802.1X EAP-TLS authentication process.

- CS1:
  - TLS_DHE_DSS_WITH_AES_128_CBC_SHA
  - TLS_DHE_DSS_WITH_AES_256_CBC_SHA
  - Also includes ciphers from CS2 and CS3 below

- CS2:
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - Also includes ciphers from CS3 below
- CS3:
  - The following are TLS 1.2 ciphers:
  - TLS_RSA_WITH_AES_128_CBC_SHA256
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_CBC_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
  - The following are TLS 1.3 ciphers:
  - TLS_AES_256_GCM_SHA384
  - TLS_AES_128_GCM_SHA256
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_CCM_8_SHA256
  - TLS_AES_128_CCM_SHA256

Any IEEE 802.1X EAP-TLS authentication attempt using a cipher that is not allowed by the cipher suite will result in a failure to establish the connection.

EapTlsVersion (Config Parameter)

Type	Enum
Range	TLSv1(200) | TLSv1_1(300) | TLSv1_2 (400) | TLSv1_3 (500)
Default	TLSv1
Script/CLI	Eth.EapTlsVersion
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.10000.400

Defines the allowed TLS versions for the network security settings when using the IEEE 802.1X EAP-TLS authentication process.

- TLSv1: Allow TLS versions 1 and up.
- TLSv1_1: Allow TLS versions 1.1 and up.
- TLSv1_2: Allow TLS versions 1.2 and up.
- TLSv1_3: Allow TLS version 1.3 only.

Any IEEE 802.1X EAP-TLS authentication attempt using a TLS version that is not allowed will result in a failure to establish the connection.

RedundantPorts (Config Parameter)

Type	Enum
Range	Disable(0) | Eth4Eth5(100)
Default	Disable
Script/CLI	Eth.RedundantPorts
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.10100.100

Controls whether or not the ETH4 and ETH5 ports are redundant and connected to the same subnet.

- Disable: Redundant Ports is disabled.
- Eth4Eth5: Redundant Ports is enabled.

Configuring "Eth4Eth5" means that the traffic of the ETH4 port will automatically switchover to the ETH5 port in case of a link failure on the ETH4 port. To prevent network loop issues, the two ports are never active at the same time – meaning the ETH5 port is disabled while ETH4 is up and running.

Note: This feature is not supported on all hardware platforms.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Eth.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Eth.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

AddVlan (Command)

Adds a new virtual LAN.

Idx (Argument) | Command: AddVlan

Type	UInt32
Range	0..2147483647
Default	0

Index to use in Vlan table for this row.

LinkName (Argument) | Command: AddVlan

Type	Text
Range	Size(0..10)
Default	

Name of the Ethernet link over which to create the VLAN

VlanId (Argument) | Command: AddVlan

Type	UInt32
Range	0..4094
Default	0

VLAN ID of the VLAN to create.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Eth service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.2400.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	There are no valid certificates for the IEEE 802.1x EAP-TLS authentication usage on the Ethernet Link %1$s.	Error	This message is issued when IEEE 802.1x EAP-TLS authentication cannot start because no valid certificates are installed on the unit.
20	There is no IEEE 802.1x authenticator responding to the IEEE 802.1x EAP-TLS authentication requests on the Ethernet Link %1$s.	Error	This message is issued when the IEEE 802.1x EAP-TLS authentication cannot reach an IEEE 802.1x authenticator (such as an IEEE 802.1x capable network device).
30	The IEEE 802.1x EAP-TLS invalid certificates on the Ethernet Link %1$s.	Error	This message is issued when the IEEE 802.1x EAP-TLS authentication fails due to invalid certificates. Usually, this message means that the Ethernet Link did not get authorisation or access to the secured network(s).
40	The IEEE 802.1x EAP-TLS authentication failed on the Ethernet Link %1$s.	Error	This message is issued when the IEEE 802.1x EAP-TLS authentication requests failed because of an invalid EAP username or because no IEEE 802.1x authentication server could be reached.
50	The IEEE 802.1x EAP-TLS authentication succeeded on the Ethernet Link %1$s.	Debug	This message is issued when the Ethernet link interface succeeded in getting authorisation from a IEEE 802.1x EAP-TLS authentication server through an authenticator. Usually, this message means that the Ethernet Link received authorisation and access to the secured network(s).
80	%1$s link down detected.	Warning	This message is issued when the Eth.RedundantPorts parameter is enabled, and a link failure is detected on one of the redundant port.
90	%1$s link up detected.	Warning	This message is issued when the Eth.RedundantPorts parameter is enabled, and the link is back up on one of the redundant port.
100	Switching over from %1$s to redundant port %2$s.	Warning	This message is issued when the Eth.RedundantPorts parameter is enabled, and a link failure is detected on the primary port.
110	Switching back from %2$s to primary port %1$s.	Warning	This message is issued when the Eth.RedundantPorts parameter is enabled, and the primary port is back up and running.

NumKey	Message	Severity	Description
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.

NumKey	Message	Severity	Description
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Eth.

Message	Severity	Description
The '%1$s' link does not support VLAN.	Error	This message is issued when the user creates a VLAN on a link interface not supporting this type of network.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.

Message	Severity	Description
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

File Manager (File)

The File service allows the administrator to manage the files stored on the unit.

Parameters

Files (Table)

This table contains all the factory or user installed files.

Index (Index) | Table: Files

Type	UInt32
Range	
Script/CLI	File.Files[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2600.1.100.1.101

Unique identifier of the row in the table.

FileName (Status Parameter) | Table: Files

Type	Text
Range	SIZE(1..510)
Script/CLI	File.Files[].FileName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2600.1.100.1.201

Relative path and name of the file (directories are split with '/').

FileDescription (Status Parameter) | Table: Files

Type	Text
Range	SIZE(0..255)
Script/CLI	File.Files[].FileDescription
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2600.1.100.1.400

Textual description describing the content of the file.
The file description uses special tags in the file to build the description string.

FileSize (Status Parameter) | Table: Files

Type	UInt32
Range	
Script/CLI	File.Files[].FileSize
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2600.1.100.1.500

File size of the associated file.
This value is expressed in kilobytes (KB).

VmImagesFiles (Table)

This table contains all the virtual machine files under the /vm/images/ folder (factory or user-installed).
Available only on the Sentinel 400.

Index (Index) | Table: VmImagesFiles

Type	UInt32
Range	
Script/CLI	File.VmImagesFiles[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2600.1.150.1.100

Unique identifier of the row in the table.

FileName (Status Parameter) | Table: VmImagesFiles

Type	Text
Range	SIZE(1..510)
Script/CLI	File.VmImagesFiles[].FileName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2600.1.150.1.200

Relative path and name of the file (directories are separated with '/').

FileDescription (Status Parameter) | Table: VmImagesFiles

Type	Text
Range	SIZE(0..255)
Script/CLI	File.VmImagesFiles[].FileDescription
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2600.1.150.1.300

Textual description describing the content of the file.

FileSize (Status Parameter) | Table: VmImagesFiles

Type	UInt32
Range	
Script/CLI	File.VmImagesFiles[].FileSize
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2600.1.150.1.400

File size of the associated file.

This value is expressed in kilobytes (KB).

FileSystemQuotaSize (Status Parameter)

Type	UInt32
Range	
Script/CLI	File.FileSystemQuotaSize
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2600.1.200

This value indicates the total storage size allocated to the File service.
This value is expressed in kilobytes (KB).

FileSystemAvailableSize (Status Parameter)

Type	UInt32
Range	
Script/CLI	File.FileSystemAvailableSize
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2600.1.250

This value indicates the remaining storage size available for the File service.
This value is expressed in kilobytes (KB).

VmImagesAvailableSize (Status Parameter)

Type	UInt32
Range	
Script/CLI	File.VmImagesAvailableSize
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2600.1.280

This value indicates the storage size available in vm/images/ folder.
This value is expressed in kilobytes (KB).

Available only on the Sentinel 400.

TransferHttpsCipherSuite (Config Parameter)

Type	Enum
Range	CS1(100) | CS2(200) | CS3(300)
Default	CS1
Script/CLI	File.TransferHttpsCipherSuite
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2600.1.500.100

Defines the allowed cipher suites for the network security settings when using the HTTPS transfer protocol. When the device initiates an HTTPS connection to a server it will negotiate the cipher suite according to its configuration.

- CS1:
  - TLS_DHE_DSS_WITH_AES_128_CBC_SHA
  - TLS_DHE_DSS_WITH_AES_256_CBC_SHA
  - Also includes ciphers from CS2 and CS3 below
- CS2:
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - Also includes ciphers from CS3 below

- CS3:
  - The following are TLS 1.2 ciphers:
  - TLS_RSA_WITH_AES_128_CBC_SHA256
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_CBC_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
  - The following are TLS 1.3 ciphers:
  - TLS_AES_256_GCM_SHA384
  - TLS_AES_128_GCM_SHA256
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_CCM_8_SHA256
  - TLS_AES_128_CCM_SHA256

TransferHttpsTlsVersion (Config Parameter)

Type	Enum
Range	TLSv1(200) | TLSv1_1(300) | TLSv1_2 (400) | TLSv1_3 (500)
Default	TLSv1
Script/CLI	File.TransferHttpsTlsVersion
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2600.1.500.200

Defines the allowed TLS version for the network security settings when using the HTTPS transfer protocol. When the device initiates an HTTPS connection to a server it will negotiate the TLS version according to its configuration.

- TLSv1: Allow TLS versions 1 and up.
- TLSv1_1: Allow TLS versions 1.1 and up.
- TLSv1_2: Allow TLS versions 1.2 and up.
- TLSv1_3: Allow TLS version 1.3 only.

The device will always send its highest supported TLS version in the ClientHello message. The server will select the highest supported TLS version it supports from the ClientHello message. The device will then validate that the selected version is allowed. If the version is not allowed, the device will close the connection.

StatLastDownloadFileResult (Status Parameter)

Type	Enum
Range	None(100) | Downloading(200) | Success(300) | Failed(400)
Script/CLI	File.StatLastDownloadFileResult
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2600.1.600.100

Result of the last file download command that was successfully launched.

- None: No file download operation has been performed since the last reset to default settings.
- Downloading: A file download operation is currently in progress.
- Success: The last file download operation succeeded.
- Failed: The last file download operation failed.

StatLastUploadFileResult (Status Parameter)

Type	Enum
Range	None(100) | Uploading(200) | Success(300) | Failed(400)
Script/CLI	File.StatLastUploadFileResult
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2600.1.600.200

Result of the last file upload command that was successfully launched.

- None: No file upload operation has been performed since the last reset to default settings.
- Uploading: A file upload operation is currently in progress.
- Success: The last file upload operation succeeded.
- Failed: The last file upload operation failed.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	File.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2600.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	File.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2600.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

Delete (Command)

Deletes the specified file.

FileName (Argument) | Command: Delete

Type	Text
Range	SIZE(1..510)
Default	

Relative path and name of the file to delete.

DownloadFile (Command)

Launches the download of the specified file.

FileUrl (Argument) | Command: DownloadFile

Type	Text
Range	
Default	

URL to a file that is loaded upon executing the `Download` command. The supported transfer protocols are:

- HTTP
- HTTPS
- TFTP
- FTP

Examples of valid URLs:

- http://www.myserver.com/myfile
- tftp://myserver.com:69/myfolder/myfile

When the port is not included in the URL, the default port for the chosen protocol is used, i.e.

- HTTP, port 80
- HTTPS, port 443
- TFTP, port 69
- FTP, port 21

The filename part may only be composed of alphanumerical and '-._%$' characters.

ServiceName (Argument) | Command: DownloadFile

Type	Text
Range	
Default	Conf

Name of the service that uses the file. The service name is used as the top-level directory in the directory hierarchy managed by the File manager.

DestinationDirectory (Argument) | Command: DownloadFile

Type	Text
Range	
Default	

Destination directory on the device where to save the file.

UserName (Argument) | Command: DownloadFile

Type	Text
Range	Size(0..63)
Default	

When authentication is required by the remote file server, this parameter is used as the username.

Password (Argument) | Command: DownloadFile

Type	Text
Range	Size(0..63)
Default	

When authentication is required by the remote file server, this parameter is used as the password.

InstallFile (Command)

Install the file received in the **FileContent** argument at the path specified in the **Path** argument.

Note: Is it recommended to use this command within a configuration script file. Although it is possible to use this command through the CLI, the command total length must be kept under 8 KB, and may take considerable time to complete on some platforms.

Name (Argument) | Command: InstallFile

Type	Text
Range	Size(0..254)
Default	

The name to be given to the file.

Path (Argument) | Command: InstallFile

Type	Text
Range	
Default	

Path where to install the file. Two paths are supported:

- sbc/rulesets: SBC call agent and routing rulesets (only .crs and .rrs file extensions are allowed).
- conf: Configuration files

FileContent (Argument) | Command: InstallFile

Type	Text
Range	
Default	

The file content, encoded in Base64.
Note: Double quotes must be used around the Base64 value.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

UploadFile (Command)

Launches the upload of the specified file.

Url (Argument) | Command: UploadFile

Type	Text
Range	
Default	

URL to a remote entity where the selected file is sent to. The supported transfer protocols are:

- TFTP
- FTP

Example of a valid URL: tftp://myserver.com:69/myfolder/myfile
When the port is not included in the URL, the default port for the chosen protocol is used, i.e.:

- TFTP, port 69
- FTP, port 21

ServiceName (Argument) | Command: UploadFile

Type	Text
Range	
Default	

Name of the service that uses the file. The service name is used as the top-level directory in the directory hierarchy managed by the File manager.

SourceDirectory (Argument) | Command: UploadFile

Type	Text
Range	
Default	

Optional destination directory under the service directory.

FileName (Argument) | Command: UploadFile

Type	Text
Range	
Default	

File name to upload.

UserName (Argument) | Command: UploadFile

Type	Text
Range	Size(0..63)
Default	

When authentication is required by the remote file server, this parameter is used as the username.

Password (Argument) | Command: UploadFile

Type	Text
Range	Size(0..63)
Default	

When authentication is required by the remote file server, this parameter is used as the password.

Notification Messages

This section describes all the notification messages relevant to the File service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.2600.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	File %1$s has been deleted.	Info	This message is issued when the service successfully deletes a file. **Note:** This notification is platform-specific.
20	Not enough space to store file.	Error	This message is issued when the service does not have enough space in the file system to store the specified file. **Note:** This notification is platform-specific.
30	Download failed, a download is currently in progress.	Error	The download has failed since a download is currently being performed. A download must be stopped or completed before another download can be triggered. **Note:** This notification is platform-specific.
35	Upload failed, an upload is currently in progress.	Error	The upload has failed since an upload is currently being performed. An upload must be stopped or completed before another upload can be triggered. **Note:** This notification is platform-specific.
40	Unable to transfer the requested file because the connection failed.	Error	This message is issued when the File service fails to transfer the requested file because the connection could not be established. If using HTTPS file transfers, this error may be due to mismatched security certificates.
50	Unable to transfer the requested file, reason: file not found.	Error	This message is issued when the Cert service fails to transfer the requested file because the host reports it does not exist.
60	Unable to transfer the requested file, reason: access denied.	Error	This message is issued when the Cert service fails to transfer the requested file because the server authentication failed.
70	Unable to transfer the requested file, reason: timed out.	Error	This message is issued when the Cert service fails to transfer the requested file because a timeout occurred.
80	Unable to transfer the requested file, reason: internal error.	Error	This message is issued when the Cert service fails to transfer the requested file and an unexpected situation happened.

NumKey	Message	Severity	Description
90	Unable to transfer the requested file, reason: could not resolve host name.	Error	This message is issued when the Cert service fails to transfer the requested file because the host name cannot be resolved.
100	Unable to transfer the requested file, reason: host or port unreachable.	Error	This message is issued when the Cert service fails to transfer the requested file because the host or port cannot be reached.
110	File %1$s successfully downloaded.	Info	This message is issued when the file is successfully downloaded and successfully stored. **Note:** This notification is platform-specific.
120	File %1$s successfully stored.	Info	This message is issued when the file is successfully stored. **Note:** This notification is platform-specific.
130	File %1$s failed to store.	Error	This message is issued when the file failed to be stored. **Note:** This notification is platform-specific.
140	File %1$s cannot be opened.	Error	This message is issued when the file cannot be opened. **Note:** This notification is platform-specific.
150	Maximum number of files reached, cannot store file %1$s.	Error	This message is issued when the service has reached the maximum allowed number of files in the file system and cannot store the specified file. **Note:** This notification is platform-specific.
160	No write permission on the destination folder %1$s.	Error	This message is issued when the connected user did not have the write permission on the destination folder. **Note:** This notification is platform-specific.
170	No Erase permission on the destination folder %1$s.	Error	This message is issued when the connected user did not have the erase permission on the destination folder. **Note:** This notification is platform-specific.

NumKey	Message	Severity	Description
180	No Read permission on the destination folder %1$s.	Error	This message is issued when the connected user did not have the read permission on the destination folder. **Note:** This notification is platform-specific.
190	Unable to download the file %1$s, file not found.	Error	This message is issued when the service failed to download the requested file because it does not exist. **Note:** This notification is platform-specific.
200	Unable to upload the file %1$s, file not found.	Error	This message is issued when the service failed to upload the requested file because it does not exist. **Note:** This notification is platform-specific.
210	File %1$s cannot be read.	Error	This message is issued when the file cannot be read. **Note:** This notification is platform-specific.
220	File %1$s successfully uploaded.	Info	This message is issued when the file is successfully uploaded. **Note:** This notification is platform-specific.
230	Invalid Base64 file content.	Error	This message is issued when the `File.InstallFile` command failed because the Base64 file content could not be decoded.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.

NumKey	Message	Severity	Description
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.

NumKey	Message	Severity	Description
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to File.

Message	Severity	Description
Unable to delete the file %1$s, file not found.	Error	This message is issued when the service failed to delete the requested file because it does not exist.
URL %1$s is invalid, transfer failed.	Error	URL format is invalid and the transfer has failed.
The Ruleset file name is invalid. It may be too long or contains unauthorised characters or has an incorrect extension.	Error	The Ruleset file name is invalid and the transfer has failed.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.

Message	Severity	Description
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Firmware Pack Updater (Fpu)

The Firmware Pack Updater (FPU) service manages firmware upgrade, downgrade and rollback operations.

Parameters

MfpInstalledInfo (Table)

List of Firmware Packs that are currently installed on the unit.

Index (Index) | Table: MfpInstalledInfo

Type	UInt32
Range	
Script/CLI	Fpu.MfpInstalledInfo[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1300.1.100.1.50

Index of the currently installed MFPs.

MfpName (Status Parameter) | Table: MfpInstalledInfo

Type	Text
Range	
Script/CLI	Fpu.MfpInstalledInfo[].MfpName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1300.1.100.1.100

Name of the MFP.

MfpVersion (Status Parameter) | Table: MfpInstalledInfo

Type	Text
Range	
Script/CLI	Fpu.MfpInstalledInfo[].MfpVersion
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1300.1.100.1.200

Version of the MFP installed.

MfpBank (Status Parameter) | Table: MfpInstalledInfo

Type	Enum
Range	None(100) | Main(200) | Recovery(300) | MainInUse(400) | RecoveryInUse(500)
Script/CLI	Fpu.MfpInstalledInfo[].MfpBank
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1300.1.100.1.300

Bank where the MFP is installed.

MfpProfileName (Status Parameter) | Table: MfpInstalledInfo

Type	Text
Range	Size(0..255)
Script/CLI	Fpu.MfpInstalledInfo[].MfpProfileName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1300.1.100.1.400

Name of the profile.

Status (Status Parameter)

Type	Enum
Range	WaitingSystemReady(100) | Idle(200) | Updating(300) | Retrying(350) | WaitingManualRestart(400) | Rollbacking(500) | WaitingForGracefulRestart(600)
Script/CLI	Fpu.Status
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1300.1.110

Indicates the current status of the Firmware Pack Updater.

- WaitingSystemReady: Waiting for the system restart to complete.
- Idle: Ready to process a command.
- Updating: Currently downloading and installing a firmware.
- Retrying: Retry downloading and installing a firmware, after a first failure.
- WaitingManualRestart: Waiting for a manual restart to complete a firmware update.
- WaitingForGracefulRestart: Waiting for graceful shutdown of services before completing a firmware update.

MfpLastInstallationResult (Status Parameter)

Type	Enum
Range	None(100) | Success(200) | Fail(300)
Script/CLI	Fpu.MfpLastInstallationResult
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1300.1.125

Result of the last `Install` command.

- None: No installation result available.
- Success: The last installation succeeded.
- Fail: The last installation failed.

MfpLastInstallationDetailedResult (Status Parameter)

Type	Enum
Range	None(10) | Success(20) | FailUnknown(30) | FailConnectionError(40) | FailFileNotFound(41) | FailUnreachableFile(42) | FailAccessDenied(43) | FailUntrustedCertificate(44) | FailFileParsing(45) | FailIncompatibleFile(46) | FailInvalidConfig(50) | FailCancelled(60) | FailOccupied(70)
Script/CLI	Fpu.MfpLastInstallationDetailedResult
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1300.1.130

Detailed result of the last `Install` command.

- None: No installation result available.
- Success: The last installation succeeded.
- FailUnknown: An unknown firmware update failure.
- FailConnectionError: A connection error occured (e.g. could not connect, the connection timeout or an internal error).
- FailFileNotFound: The file on the remote server is not found.
- FailUnreachableFile: The host or the port is unreachable, or a bad hostname is given.
- FailAccessDenied: The authentication failed (username/password).
- FailUntrustedCertificate: The TLS certificate is untrusted or has a bad hostname.
- FailFileParsing: The parsing of the file failed.
- FailIncompatibleFile: Firmware incompatible or corrupted (e.g. wrong platform firmware).
- FailInvalidConfig: The URL or the configuration of the Fpu service is invalid.
- FailCancelled: The installation operation was cancelled by the user.
- FailOccupied: An installation operation is already in progress.

MfpLastInstallationDateTime (Status Parameter)

Type	Text
Range	Size(0..255)
Script/CLI	Fpu.MfpLastInstallationDateTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1300.1.150

Date and time when the firmware was installed.

MfpRollbackAvailable (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Fpu.MfpRollbackAvailable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1300.1.175

Indicates whether or not a MFP rollback operation is available.

MfpTransferUsername (Config Parameter)

Type	Text
Range	Size(0..63)
Default	
Script/CLI	Fpu.MfpTransferUsername
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1300.1.400.200.200

User name used for transfer authentication, if required.

MfpTransferPassword (Config Parameter)

Type	Text
Range	Size(0..255)
Default	
Script/CLI	Fpu.MfpTransferPassword
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1300.1.400.200.300

Password used for transfer authentication, if required.
Password encryption is supported via the **Dcm.PasswordEncryption** table.

When **Dcm.PasswordEncryption** is enabled clear text passwords will be automatically encrypted.

Unencrypted password maximal length is 63.

Encrypted password maximal length is 113.

MfpTransferCertificateValidation (Config Parameter)

Type	Enum
Range	NoValidation(100) | HostName(200)
Default	HostName
Script/CLI	Fpu.MfpTransferCertificateValidation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1300.1.400.200.500

When downloading a MFP from an HTTPS server, this parameter defines the level of security to use when validating the server's certificate.

- NoValidation: Allow a connection to the server without validating its certificate. The only condition is to receive a certificate from the server. This option provides partial security and should be selected with care.
- HostName: Allow a connection to the server by validating its certificate is trusted and valid. The validations performed on the certificate include the expiration date and that the Subject Alternate Name (SAN) or Common Name (CN) matches the FQDN or IP address of the server.

MfpTransferCertificateTrustLevel (Config Parameter)

Type	Enum
Range	LocallyTrusted(100) | OcspOptional(200) | OcspMandatory(300)
Default	LocallyTrusted
Script/CLI	Fpu.MfpTransferCertificateTrustLevel
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1300.1.400.200.600

Define how a peer certificate is considered trusted for a HTTPS connection.

- LocallyTrusted: A certificate is considered trusted when the certificate authority (CA) that signed the peer certificate is present in the **Cert.OthersCertificatesInfo** table. The certificate revocation status is not verified.
- OcspOptional: A certificate is considered trusted when it is locally trusted and is not revoked by its certificate authority (CA). The certificate revocation status is queried using the Online Certificate Status Protocol (OCSP). If the OCSP server is not available or the verification status is unknown, the certificate is considered trusted.
- OcspMandatory: A certificate is considered trusted when it is locally trusted and is not revoked by its certificate authority (CA). The certificate revocation status is queried using the Online Certificate Status Protocol (OCSP). If the OCSP server is not available or the verification status is unknown, the certificate is considered not trusted.

MfpTransferCipherSuite (Config Parameter)

Type	Enum
Range	CS1(100) | CS2(200) | CS3(300)
Default	CS1
Script/CLI	Fpu.MfpTransferCipherSuite
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1300.1.400.200.700

Defines the allowed cipher suites for the network security settings when using the HTTPS transfer protocol. When the device initiates an HTTPS connection to a server it will negotiate the cipher suite according to its configuration.

- CS1:
  - TLS_DHE_DSS_WITH_AES_128_CBC_SHA
  - TLS_DHE_DSS_WITH_AES_256_CBC_SHA
  - Also includes ciphers from CS2 and CS3 below

- CS2:
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - Also includes ciphers from CS3 below
- CS3:
  - The following are TLS 1.2 ciphers:
  - TLS_RSA_WITH_AES_128_CBC_SHA256
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_CBC_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
  - The following are TLS 1.3 ciphers:
  - TLS_AES_256_GCM_SHA384
  - TLS_AES_128_GCM_SHA256
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_CCM_8_SHA256
  - TLS_AES_128_CCM_SHA256

MfpTransferTlsVersion (Config Parameter)

Type	Enum
Range	TLSv1(200) | TLSv1_1(300) | TLSv1_2(400) | TLSv1_3(500)
Default	TLSv1
Script/CLI	Fpu.MfpTransferTlsVersion
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1300.1.400.200.800

Defines the allowed TLS version for the network security settings when using the HTTPS transfer protocol. When the device initiates an HTTPS connection to a server it will negotiate the TLS version according to its configuration.

- TLSv1: Allow TLS versions 1 and up.
- TLSv1_1: Allow TLS versions 1.1 and up.
- TLSv1_2: Allow TLS versions 1.2 and up.
- TLSv1_3: Allow TLS version 1.3 only.

The device will always send its highest supported TLS version in the ClientHello message. The server will select the highest supported TLS version it supports from the ClientHello message. The device will then validate that the selected version is allowed. If the version is not allowed the device will close the connection.

MfpUrl (Config Parameter)

Type	Text
Range	
Default	
Script/CLI	Fpu.MfpUrl
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1300.1.450

URL of the MFP 'single file' to install. The supported transfer protocols are:

- HTTP
- HTTPS
- TFTP
- FTP

Examples of valid URLs:

- http://www.myserver.com/myfile.bin

- tftp://myserver.com:69/myfolder/myfile.bin

When the port is not included in the URL, the default port for the chosen protocol is used.

For authentication, it is recommended to use the **Fpu.MfpTransferUsername** and **Fpu.MfpTransferPassword** parameters. The credentials may also be provisioned directly in the URL using the syntax protocol://[username[:password]@]hostname[:port]/[path/]filename with the following constraints:

- No "/", ":" and "@" characters should be present in username or password.
- No percent escaping.
- The password will appear in clear in the URL field in the Web page.

If a username/password is specified both in the URL and in the provisioning parameters, values specified in the URL will have precedence over the ones specified in the parameters.

This parameter may contain some macros that are substituted by the actual value at the moment of fetching the MFP file.

The supported macros are:

- %mac% - the MAC address of the unit.
- %product% - the product name of the unit.
- %productseries% - the product series name of the unit.
- %serial% - the serial number of the unit.
- %version% - the version number of the unit.
- %profile% - the profile name of the unit.

AutomaticRestartEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Fpu.AutomaticRestartEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1300.1.500

Enables the firmware pack updater to automatically restart the system when needed for completing a firmware update operation.
Also see the **AutomaticRestartGraceDelay** parameter.

AutomaticRestartGraceDelay (Config Parameter)

Type	UInt32
Range	0..10080
Default	0
Script/CLI	Fpu.AutomaticRestartGraceDelay
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1300.1.600

Configures the grace delay in minutes that the unit waits for all telephony calls to be terminated before the automatic restart can occur.
This value is expressed in minutes. The maximum value is set to 10080 minutes (7 days).

Also see the **AutomaticRestartEnable** parameter.

DefaultSettingsOnInstall (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Fpu.DefaultSettingsOnInstall
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1300.1.700

When set to "Enable", the unit automatically executes a factory reset upon completion of a firmware installation.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Fpu.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1300.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.

- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Fpu.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1300.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

CancelInstall (Command)

Cancels any firmware update currently in progress.
This command may restart the system.

DefaultSettings (Command)

Resets the entire system configuration to the factory defaults.

Install (Command)

Launches the installation of the selected MFPs.
Unless the **AutomaticRestartEnable** parameter is disabled, the system restarts when the installation is completed.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

Rollback (Command)

Launches the rollback of the previously installed MFP found in recovery bank.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Fpu service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.1300.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
1000	Executing on recovery firmware.	Critical	Because of repeated failures, the backup firmware was used to restart the unit. Perform a firmware update to avoid this message being repeated every time the unit is restarted. **Note:** This notification is platform-specific.
1100	Bad signature, bad construction, or corruption for file %1$s in MFP %2$s.	Error	The file contains an invalid digital signature, a bad file construction or is corrupted.
1200	%1$s MFP is incompatible or has unresolved dependencies.	Error	The MFP could not be installed because some required hardware or software modules could not be found.
1300	Installation operation could not complete successfully, retrying.	Warning	An installation operation failed. The installation process is now restarted.
1400	Installation operation could not complete successfully.	Error	An installation operation failed. The maximum number of incomplete update is reached. The installation process is now aborted.
1500	Installation of whole MFP selection succeeded.	Info	This message occurs at the end of the installation process, when no error occurred.
1600	Installation already in progress.	Warning	This message occurs when an installation operation is requested while a previous operation is not completed.
1700	Installation operation starting.	Info	This message occurs when an installation operation is starting.
2000	Installation is already up-to-date.	Info	This message occurs when the current installation is already in sync with the requested installation operation.
2900	The system is now restarting to complete the firmware update.	Info	This message occurs when the installation operation requested by the user requires a restart to take effect and the **AutomaticRestartEnable** parameter is set to "enable".
3000	Manual restart is required to complete the firmware update.	Info	This message occurs when the installation operation requested by the user requires a manual restart to take effect and the **AutomaticRestartEnable** parameter is set to "disable".

NumKey	Message	Severity	Description
3100	Firmware recovery required. Restarting system.	Warning	This message occurs when a firmware recovery is required because an error occurred while updating the firmware. It indicates that the system is about to restart.
3200	Transferring the %1$s file.	Debug	This message occurs when the service transfers a file during the update process.
3300	The firmware update was cancelled by user.	Info	This message occurs when a firmware update is canceled by the `CancelInstall` command.
3400	Cancelling the firmware update and reverting the unit's configuration to default values.	Info	This message occurs when a firmware update is cancelled due to a default settings command.
3700	Freeing some storage space for the new firmware to install. This may take several minutes.	Debug	This message occurs when an update is triggered by the user. The old firmware backup is erased to make some space for the target firmware. The firmware currently running is kept as a backup in case of an installation failure. This operation may take several minutes.
3800	Default reset initiated via the Reset switch.	Info	This message is issued when the FPU receives a request to apply the default settings to the unit because the user pressed the Reset switch.
3900	Default reset operation was ignored because the FPU is currently busy.	Warning	This message is issued when the FPU receives a request to apply the default settings while it is not ready to process it. The default settings operation was ignored.
4000	Rollback operation is starting.	Info	This message occurs when a rollback operation is starting. **Note:** This notification is platform-specific.
4100	Rollback already in progress.	Warning	This message occurs when a rollback operation is requested while a previous operation is not completed. **Note:** This notification is platform-specific.
4200	Rollback operation could not complete successfully.	Error	A rollback operation failed. The maximum number of incomplete rollbacks is reached. The rollback process is now aborted. **Note:** This notification is platform-specific.

NumKey	Message	Severity	Description
4300	Rollback operation could not complete successfully, retrying.	Warning	A rollback operation failed. The rollback process is now restarted. **Note:** This notification is platform-specific.
4400	Rollback to previously installed MFP succeeded.	Info	This message occurs at the end of the rollback process, when no error occurred. **Note:** This notification is platform-specific.
4500	The system is now restarting to complete the firmware rollback.	Info	This message occurs when the rollback operation requested by the user requires a system restart to complete. **Note:** This notification is platform-specific.
4600	Rollback operation is not available.	Error	A rollback operation cannot be started because there is no usable MFP to revert to.
4700	Unit is waiting for all calls to complete before restarting.	Info	The unit is waiting for all calls to complete (up to the timeout value configured in the **AutomaticRestartGraceDelay** parameter) before restarting the unit.
4800	The allowed time for graceful restart expired. Forcing a unit restart.	Warning	The time allowed for a graceful restart in **AutomaticRestartGraceDelay** expired. Forcing a unit restart.
4900	Unit is executing an automatic factory reset after firmware installation.	Info	This message is issued when the unit executes an automatic factory reset upon successful completion of a firmware installation. This occurs only if the unit is configured to have this behavior.
15100	Unable to transfer, reason: host or port unreachable.	Error	This message is issued when FPU fails to transfer the requested file because the host or port cannot be reached.
15200	Unable to transfer the requested file because the connection failed.	Error	This message is issued when the Fpu service fails to transfer the requested file because the connection could not be established. If using HTTPS file transfers, this error may be due to mismatched security certificates.
15300	Unable to transfer, reason: file not found.	Error	This message is issued when FPU fails to transfer the requested file because the host reports it does not exist.

NumKey	Message	Severity	Description
15350	Unable to transfer the requested file, reason: file already exists.	Error	This message is issued when FPU fails to transfer the requested file because the host reports it already exists.
15400	Unable to transfer, reason: access denied.	Error	This message is issued when FPU fails to transfer the requested file because authentication failed.
15500	Unable to transfer, reason: timed out.	Error	This message is issued when FPU fails to transfer the requested file, a timeout occurred.
15600	Unable to transfer, reason: internal error.	Error	This message is issued when FPU fails to transfer the requested file, an unexpected situation happened.
15700	Unable to transfer, reason: transfer parameters are invalid.	Error	This message is issued when FPU fails to transfer the requested file because of invalid configuration parameters.
15710	Transfer aborted, reason: Error when decompressing the file.	Error	This message is issued when the FPU fails to transfer the requested file because of an error when decompressing the files.
15720	Transfer aborted, reason: Error when untaring the file.	Error	This message is issued when hte FPU fails to transfer the requested file because of an error when untaring the files.
15730	Transfer aborted, reason: Error when parsing the file header.	Error	This message is issued when the FPU fails to parse the file header.
16200	Unable to transfer, reason: cannot resolve the host name (FQDN).	Error	This message is issued when FPU fails to transfer the requested file because the host name cannot be resolved.
16400	Invalid configuration, no valid file provided.	Error	This message occurs when the configuration contains no valid file to download.
16600	The %1$s file is valid.	Debug	This message occurs when the newly transferred file was correctly validated by the Firmware Pack Updater.
16700	The %1$s file is erroneous.	Error	This message occurs when the Firmware Pack Updater found an error in the newly retrieved file.
20100	Unable to encrypt the file.	Error	This message is issued when the FPU fails to encrypt a backup image.
20200	Unable to decrypt file.	Error	This message is issued when the FPU fails to decrypt either a script or a restore image.
20300	Missing password for cryptographic operation.	Error	Encryption or decryption was requested, but no password was specified.

NumKey	Message	Severity	Description
20400	Unable to transfer, reason: untrusted certificate.	Error	This message is issued when the FPU fails to transfer the requested file because the remote certificate is not trusted by any of the certificates in the unit.
20500	Unable to transfer, reason: hostname does not match the certificate.	Error	This message is issued when the FPU fails to transfer the requested file, the hostname used to connect to the server does not match the hostname configured in the certificate.
20600	OCSP verification of the certificate of %1$s with responder %2$s URL completed with %3$s status.	Info	This message is issued every time an OCSP request is completed (successfully or not).
20700	Certificate revocation status cannot be verified for HTTPS connection with %1$s remote host because the OCSP %2$s responder is unreachable.	Warning	This message is issued when the certificate revocation status cannot be verified because the received peer certificate does not include the Authority Information Access extension providing the URI for the OCSP responder or the OCSP responder cannot be reached.
20800	Certificate revocation status cannot be verified for HTTPS connection with %1$s remote host because the response from OCSP %2$s responder could not be accepted.	Warning	This message is issued when the response obtained from the OCSP responder cannot be accepted. Possible causes include: failure to match the response with the request, response delay too large, response cannot be parsed, and response fails verification.
20900	Certificate revocation status cannot be verified on the certificate of %1$s because the responder %2$s URL is not valid.	Warning	This message is issued when the responder URL does not follow the supported syntax.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.

NumKey	Message	Severity	Description
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.

NumKey	Message	Severity	Description
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Fpu.

Message	Severity	Description
No server specified.	Error	This message is issued when a firmware installation is requested but no server hostname is specified.
No MFP specified.	Error	This message is issued when a firmware installation is requested but no MFP name is specified.
No MFP version specified.	Error	This message is issued when a firmware installation is requested but no MFP version is specified.
Service is busy installing.	Error	This message is issued when a command cannot be executed because the Firmware Pack Updater is currently installing an MFP.
No installation to cancel.	Warning	This message is issued when a `CancelInstall` command cannot be executed because the Firmware Pack Updater is not currently installing an MFP.
The command could not be executed because the FPU is currently busy.	Error	This message is issued when a command can not be executed because the Firmware Pack Updater is currently busy.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.

Message	Severity	Description
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

High Availability (Ha)

The High availability (Ha) service enables a shared/floating IP address between two devices (Master and Backup). High availability is achieved by the Virtual Redundancy Routing Protocol (VRRP).

Parameters

VrrpInstance (Table: user-defined, 10 lines max.)

This table contains configuration parameters for VRRP instances. A VRRP instance is an entity that manages the VRRP protocol for a Virtual Router. VRRP instances with an invalid configuration are not started.

Id (Index) | Table: VrrpInstance

Type	UInt32
Range	0..255
Script/CLI	Ha.VrrpInstance[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4800.1.100.1.100

Unique numerical identifier for the instance.

Name (Config Parameter) | Table: VrrpInstance

Type	Text
Range	Size(0..20)
Default	
Script/CLI	Ha.VrrpInstance[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4800.1.100.1.200

Name of the VRRP instance. Accepted characters are alphanumeric and underscore.

InitialState (Config Parameter) | Table: VrrpInstance

Type	Enum
Range	Master(100) | Backup(200)
Default	Master
Script/CLI	Ha.VrrpInstance[].InitialState
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4800.1.100.1.300

Initial state of the VRRP state machine.

- Master: The VRRP state machine starts in the Master state.
- Backup: The VRRP state machine starts in the Backup state.

CurrentState (Status Parameter) | Table: VrrpInstance

Type	Enum
Range	Master(100) | Backup(200) | Fault(300) | Unknown(400) | InvalidConfig(500) | Error(600)
Script/CLI	Ha.VrrpInstance[].CurrentState
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4800.1.100.1.350

Current state of the VRRP state machine.

- Master: The VRRP state machine is currently in the Master state.
- Backup: The VRRP state machine is currently in the Backup state.
- Fault: The VRRP state machine is currently in the Fault state.
- Unknown: The VRRP state machine is currently in the Unknown state.
- InvalidConfig: The VRRP state machine configuration is invalid.
- Error: The VRRP state machine is experiencing some error.

Link (Config Parameter) | Table: VrrpInstance

Type	Text
Range	Size(0..20)
Default	
Script/CLI	Ha.VrrpInstance[].Link
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4800.1.100.1.400

Link on which the VRRP instance operates.

VirtualIpAddress (Config Parameter) | Table: VrrpInstance

Type	IpAddrMask
Range	
Default	
Script/CLI	Ha.VrrpInstance[].VirtualIpAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4800.1.100.1.500

Virtual Ip Address of the VRRP instance.

Priority (Config Parameter) | Table: VrrpInstance

Type	UInt32
Range	1..255
Default	100
Script/CLI	Ha.VrrpInstance[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4800.1.100.1.600

Priority of the VRRP instance. This priority is used for electing the Master.

VirtualRouterId (Config Parameter) | Table: VrrpInstance

Type	UInt32
Range	1..255
Default	197
Script/CLI	Ha.VrrpInstance[].VirtualRouterId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4800.1.100.1.700

Arbitrary unique number used to identify a instances of VRRP belonging to the same Virtual Router. The default value was chosen to minimize the possibility of conflict with a Virtual Router from another vendor.

No more than one VRRP instance can have the same pair Virtual Router ID + Link. VRRP instances having the same Virtual Router ID and Link are considered to have an invalid configuration.

Preemption (Config Parameter) | Table: VrrpInstance

Type	Enum
Range	PreemptionAllowed(100) | NoPreemption(200)
Default	PreemptionAllowed
Script/CLI	Ha.VrrpInstance[].Preemption
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4800.1.100.1.800

Configures the preemption behavior for the VRRP instance. Preemption is the action of taking over the MASTER role from a lower priority VRRP instance when becoming online.

- PreemptionAllowed: PreemptionAllowed: Enables preemption for the VRRP instance. When the VRRP instance becomes online while a lower-priority VRRP instance currently owns the MASTER role, it will take over the MASTER role from it. This configuration allows to return the MASTER role to a "preferred" VRRP instance when it comes back online, but the current calls are lost when doing so.
- NoPreemption: Disables preemption for the VRRP instance. When the VRRP instance becomes online while a lower-priority VRRP instance currently owns the MASTER role, it will not attempt to take over the MASTER role from it. Use this configuration when you want to minimize the impact on active calls, by reducing the number of times that the MASTER role is exchanged between VRRP instances. NOTE: For this to work, the initial state MUST NOT be MASTER.

Group (Config Parameter) | Table: VrrpInstance

Type	Text
Range	Size(0..20)
Default	
Script/CLI	Ha.VrrpInstance[].Group
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4800.1.100.1.850

Dictates which group the VRRP instance belongs to.

ConfigStatus (Status Parameter) | Table: VrrpInstance

Type	Enum
Range	Valid(100) | Invalid(200)
Script/CLI	Ha.VrrpInstance[].ConfigStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4800.1.100.1.900

Configuration status of the row.

Delete (Row Command) | Table: VrrpInstance

Script/CLI:	Ha.VrrpInstance[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.4800.1.100.1.950

Delete this **VrrpInstance** table entry.

StartupStatus (Status Parameter)

Type	Enum
Range	Ok(100) | ConfigurationIssue(200) | FailedStarting(300) | InProgress(400)
Script/CLI	Ha.StartupStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4800.1.1000

Indicates the service startup status.

1. Ok: The service started correctly.
2. InProgress: Start is not yet completed.
3. ConfigurationIssue: The service could not start properly because an issue was found in the configuration.
4. FailedStarting: The service could not start properly for another reason.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Ha.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4800.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Ha.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4800.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

AddVrrpInstance (Command)

Add a row in the **VrrpInstance** table.

Id (Argument) | Command: AddVrrpInstance

Type	UInt32
Range	0..255
Default	0

Unique numerical identifier for the instance.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Ha service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.4800.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.

NumKey	Message	Severity	Description
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Ha.

Message	Severity	Description
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.

Message	Severity	Description
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Host Configuration (Hoc)

The Host Configuration (Hoc) service manages the IP host parameters and other system settings.

Parameters

ManagementInterface (Config Parameter)

Type	Text
Range	Size(1..50)
Default	Lan1
Script/CLI	Hoc.ManagementInterface
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.100

Specifies to which network interface the system management services are bound. The name specified here must match an existing **InterfaceName** in the **NetworkInterfacesStatus** table of the Bni service. The special value 'All' means to bind all network interfaces.

Note that this parameter is case-sensitive.

Note that Advance IP Routing could be required to forward the packet over the correct network.

AutomaticConfigurationInterface (Config Parameter)

Type	Text
Range	Size(0..50)
Default	
Script/CLI	Hoc.AutomaticConfigurationInterface
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.150

The network interface that provides the IPv4 automatic configuration (Default Router, domain name, DNS servers, and NTP server) used by the unit. Please note that some connection types (for example ipStatic and pppIpcp) cannot obtain information about the domain name, DNS servers, and NTP server from the network, and therefore lead to no domain name being applied to the system.

Ipv6AutomaticConfigurationInterface (Config Parameter)

Type	Text
Range	Size(0..50)
Default	
Script/CLI	Hoc.Ipv6AutomaticConfigurationInterface
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.175

The network interface that provides the IPv6 automatic configuration (Default Router, domain name, DNS servers, and NTP server) used by the unit. Please note that some connection types (for example ip6Static) cannot obtain information about the domain name, DNS servers, and NTP server from the network, and therefore lead to no domain name being applied to the system.

HostName (Config Parameter)

Type	IpHostName
Range	Size(0..63)
Default	
Script/CLI	Hoc.HostName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.200

Host name of the unit. Certain restrictions apply to this name:

- It must be shorter than 64 characters.
- It must not start with a space or a period.
- It must not contain double quotes, semicolons, curly braces and commas.

SystemTime (Status Parameter)

Type	Text
Range	
Script/CLI	Hoc.SystemTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.250.100

Current system date and time configured in the unit.
This local time is computed from the Time Zone defined in the **StaticTimeZone** parameter.
If the time seems not valid, verify the SNTP configuration in the Sntp group.

SystemUptime (Status Parameter)

Type	Text
Range	
Script/CLI	Hoc.SystemUptime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.250.150

Time elapsed since the last system restart in a D:HH:MM:SS format.

StaticTimeZone (Config Parameter)

Type	Text
Range	Size(0..255)
Default	EST5EDT4,M3.2.0/02:00:00,M11.1.0/02:00:00
Script/CLI	Hoc.StaticTimeZone
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.250.200

Specifies the time zone in which the system is located.
The parameter contains two parts separated by a semicolon:

- The first part, mandatory, is the system timezone expressed in the IEEE 1003.1 POSIX format as defined in https://tools.ietf.org/html/draft-ietf-dhc-timezone-03.
- The second part, optional, is the timezone used by the web pages of the Sbc service. This part is only useful for units with the Sbc service, and defaults to UTC if not present. This string must be expressed in the IANA format.

The following are examples of IEEE 1003.1 POSIX strings for the first part:

- Pacific Time (Canada and US) : PST8PDT,M3.2.0,M11.1.0
- Mountain Time (Canada and US) : MST7MDT,M3.2.0,M11.1.0
- Central Time (Canada and US) : CST6CDT,M3.2.0,M11.1.0
- Eastern Time (Canada and US) : EST5EDT,M3.2.0,M11.1.0
- Atlantic Time (Canada) : AST4ADT,M3.2.0,M11.1.0
- Greenwich Mean Time : GMT0BST,M3.5.0/1,M10.5.0
- Western Europe Time : WET0WEST,M3.5.0/1,M10.5.0
- Central European Time : CET-1CEST,M3.5.0,M10.5.0/3
- China Standard Time : CST-8
- Japan Standard Time : JST-9
- Australia Eastern Standard Time : AEST-10AEDT,M10.1.0,M4.1.0/3
- UTC (Coordinated Universal Time) : UTC0

The following are examples of IANA strings for the second part:

- America/Los_Angeles
- Asia/Dubai
- Europe/Stockholm
- Etc/GMT+3

Examples of allowed combinations:

- Timezones matching the same place:

  EST5EDT,M3.2.0,M11.1.0;America/Toronto

  UTC5;America/Lima

- Only first part present:

  CST6CDT,M4.1.0,M10.5.0

Notes:

- Both parts are independent from each other and validated separately.
- Input validation requires both parts to be validated successfully. In case of validation failure on either part, the whole input value is rejected.

DomainNameConfigSource (Config Parameter)

Type	Enum
Range	Automatic(100) | AutomaticIpv6(150) | Static(200)
Default	Automatic
Script/CLI	Hoc.DomainNameConfigSource
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.300.100

Configuration source for the domain name.

- Automatic: The domain name is automatically obtained from the IPv4 network defined in the **AutomaticConfigurationInterface** parameter.
- AutomaticIpv6: The domain name is automatically obtained from the IPv6 network defined in the **Ipv6AutomaticConfigurationInterface** parameter.
- Static: The domain name is specified in the **StaticDomainName** parameter.

When switching from a Static to an Automatic or AutomaticIpv6 configuration source, the last value correctly obtained from the network (if any) is applied to the system.

DomainNameInfo (Status Parameter)

Type	IpHostName
Range	Size(0..64)
Script/CLI	Hoc.DomainNameInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.300.200

Current domain name.

StaticDomainName (Config Parameter)

Type	IpHostName
Range	Size(0..64)
Default	
Script/CLI	Hoc.StaticDomainName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.300.300

Static domain name. This domain name is used as the current domain name when the **DomainNameConfigSource** parameter is set to 'Static'.

SntpConfigSource (Config Parameter)

Type	Enum
Range	Automatic(100) | AutomaticIpv6(150) | Static(200) | AutomaticWithFallback(300)
Default	Automatic
Script/CLI	Hoc.SntpConfigSource
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.400.100

Configuration source for the SNTP parameters.

- Automatic: The SNTP parameters are automatically obtained from the IPv4 network defined in the **AutomaticConfigurationInterface** parameter.
- AutomaticIpv6: The SNTP parameters are automatically obtained from the IPv6 network defined in the **Ipv6AutomaticConfigurationInterface** parameter.
- Static: The SNTP parameters are specified in the **StaticSntpServers** table.
- AutomaticWithFallback: The SNTP parameters are automatically obtained from the IPv4 network with a fallback to the **StaticSntpServers** table.

When switching from a Static to an Automatic or AutomaticIpv6 configuration source, the last values correctly obtained from the network (if any) are applied to the system.

SntpSynchronizationPeriod (Config Parameter)

Type	UInt32
Range	1..1440
Default	1440
Script/CLI	Hoc.SntpSynchronizationPeriod
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.400.200

Time interval between system time synchronisation cycles. Each time this interval expires, a SNTP request is sent to the SNTP server and the result is used to set the system time. This value is expressed in minutes. The maximum value is set to 1 440 minutes, which corresponds to 24 hours.

SntpSynchronizationPeriodOnError (Config Parameter)

Type	UInt32
Range	1..1440
Default	60
Script/CLI	Hoc.SntpSynchronizationPeriodOnError
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.400.300

Time interval between retries after an unsuccessful request to the SNTP server. This value is expressed in minutes. The maximum value is set to 1 440 minutes, which corresponds to 24 hours.

SntpTimeZone (Config Parameter)

Type	Text
Range	Size(0..255)
Default	EST5EDT4,M3.2.0/02:00:00,M11.1.0/02:00:00
Script/CLI	Hoc.SntpTimeZone
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.400.400

This parameter is obsolete and has been replaced by **TimeGroup.StaticTimeZone** parameter.

SntpServerHostInfo (Status Parameter)

Type	IpHostNamePort
Range	
Script/CLI	Hoc.SntpServerHostInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.400.500

This parameter is obsolete and has been replaced by **Hoc.SntpServersInfo.HostName** parameter.

StaticSntpServerHost (Config Parameter)

Type	IpHostNamePort
Range	
Default	192.168.10.10:123
Script/CLI	Hoc.StaticSntpServerHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.400.700

This parameter is obsolete and has been replaced by the **Hoc.StaticSntpServers.HostName** parameter.

SntpCurrentSource (Status Parameter)

Type	IpHostNamePort
Range	
Script/CLI	Hoc.SntpCurrentSource
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.400.750

The IP address and port of the last NTP server used to synchronise the system time. An empty value indicates that no servers have been successfully contacted since the last service restart.

SntpServersInfo (Table)

This table contains the list of current SNTP servers. The SNTP servers are sorted by priority. The list can contain static servers, dynamic servers (DHCP) or both depending on how the **SntpConfigSource** parameter is set. When a server does not respond, there is a delay of several seconds before attempting to use the next one.

Priority (Index) | Table: SntpServersInfo

Type	UInt32
Range	1..8
Script/CLI	Hoc.SntpServersInfo[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.400.800.1.100

Priority number for this SNTP server. The lower the number is, the higher the priority is.

HostName (Status Parameter) | Table: SntpServersInfo

Type	IpHostNamePort
Range	
Script/CLI	Hoc.SntpServersInfo[].HostName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.400.800.1.200

SNTP server host name and port.

StaticSntpServers (Table)

This table contains the list of static SNTP servers. The SNTP servers are sorted by priority. These SNTP servers are used as the current SNTP servers when the **SntpConfigSource** parameter is set to 'Static'.

Priority (Index) | Table: StaticSntpServers

Type	UInt32
Range	1..4
Script/CLI	Hoc.StaticSntpServers[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.400.900.1.100

Priority number of this static SNTP server. The lower the number is, the higher the priority is.

HostName (Config Parameter) | Table: StaticSntpServers

Type	IpHostNamePort
Range	
Default	
Script/CLI	Hoc.StaticSntpServers[].HostName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.400.900.1.200

SNTP server host name and port.

DefaultRouterConfigSource (Config Parameter)

Type	Enum
Range	Automatic(100) | Static(200)
Default	Automatic
Script/CLI	Hoc.DefaultRouterConfigSource
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.500.100

Configuration source for the default router.

- Automatic: The default IPv4 router is automatically obtained from the IPv4 network defined in the **AutomaticConfigurationInterface**.
- Static: The default router is specified in the **StaticDefaultRouter** parameter.

When switching from a Static to an Automatic configuration source, the last value correctly obtained from the network (if any) is applied to the system.

DefaultIpv6RouterConfigSource (Config Parameter)

Type	Enum
Range	AutomaticIpv6(150) | Static(200)
Default	AutomaticIpv6
Script/CLI	Hoc.DefaultIpv6RouterConfigSource
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.500.150

Configuration source for the default IPv6 router.

- AutomaticIpv6: The default IPv6 router is automatically obtained from the IPv6 network defined in the **Ipv6AutomaticConfigurationInterface** parameter.
- Static: The default router is specified in the **StaticDefaultIpv6Router** parameter.

When switching from a Static to an AutomaticIpv6 configuration source, the last value correctly obtained from the network (if any) is applied to the system.

DefaultRouterInfo (Status Parameter)

Type	IpAddr
Range	
Script/CLI	Hoc.DefaultRouterInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.500.200

Current default router address.

DefaultIpv6RouterInfo (Status Parameter)

Type	IpAddress
Range	
Script/CLI	Hoc.DefaultIpv6RouterInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.500.250

Current default IPv6 router address.

StaticDefaultRouter (Config Parameter)

Type	IpAddr
Range	
Default	192.168.10.10
Script/CLI	Hoc.StaticDefaultRouter
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.500.300

Static default router address. This address is used as the current default router address when the **DefaultRouterConfigSource** parameter is set to 'Static'.

StaticDefaultIpv6Router (Config Parameter)

Type	IpAddress
Range	
Default	
Script/CLI	Hoc.StaticDefaultIpv6Router
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.500.350

Static default IPv6 router address. This address is used as the current default router address when the **DefaultIPv6RouterConfigSource** parameter is set to 'Static'.

DnsServersConfigSource (Config Parameter)

Type	Enum
Range	Automatic(100) | AutomaticIpv6(150) | Static(200)
Default	Automatic
Script/CLI	Hoc.DnsServersConfigSource
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.600.100

Configuration source for the DNS servers.

- Automatic: The DNS servers are automatically obtained from the IPv4 network defined in the **AutomaticConfigurationInterface** parameter.
- AutomaticIpv6: The DNS servers are automatically obtained from the IPv6 network defined in the **Ipv6AutomaticConfigurationInterface** parameter.
- Static: The DNS servers are specified in the **StaticDnsServers** table.

When switching from a Static to an Automatic or AutomaticIpv6 configuration source, the last values correctly obtained from the network (if any) are applied to the system.

DnsCacheRandomization (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Hoc.DnsCacheRandomization
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.600.150

Configuration of the DNS records randomisation of the device's internal DNS Cache.

- Enable: When DNS A/AAAA records are accessed from the cache, they are sent to the requesting service in a randomised order.
- Disable: When DNS A/AAAA records are accessed from the cache, they are sent to the requesting service in the same order they were originally received from the network.

DnsServersInfo (Table)

This table contains the list of current DNS servers. The DNS servers are sorted by priority.

Priority (Index) | Table: DnsServersInfo

Type	UInt32
Range	1..4
Script/CLI	Hoc.DnsServersInfo[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.600.200.1.100

Priority number for this DNS server. The lower the number is, the higher the priority is.

IpAddress (Status Parameter) | Table: DnsServersInfo

Type	IpAddress
Range	
Script/CLI	Hoc.DnsServersInfo[].IpAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.600.200.1.200

DNS server IP address.

StaticDnsServers (Table)

This table contains the list of static DNS servers. The DNS servers are sorted by priority. These DNS servers are used as the current DNS servers when the **DnsServersConfigSource** parameter is set to 'Static'.

Priority (Index) | Table: StaticDnsServers

Type	UInt32
Range	1..4
Script/CLI	Hoc.StaticDnsServers[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.600.300.1.100

Priority number of this static DNS server. The lower the number is, the higher the priority is.

IpAddress (Config Parameter) | Table: StaticDnsServers

Type	IpAddress
Range	
Default	
Script/CLI	Hoc.StaticDnsServers[].IpAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.600.300.1.200

Static DNS server IP address.

StaticHosts (Table: user-defined, 10 lines max.)

This table contains a list of static hosts. Each host is configured with an FQDN and its static ip addresses. This table is used by the Hoc service to locally resolve an FQDN and obtain its ip address without performing a DNS request.

Index (Index) | Table: StaticHosts

Type	UInt32
Range	
Script/CLI	Hoc.StaticHosts[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.650.100.1.100

Unique identifier of the row in the table.

Name (Config Parameter) | Table: StaticHosts

Type	Text
Range	Size(0..253)
Default	
Script/CLI	Hoc.StaticHosts[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.650.100.1.200

Name (FQDN) of the static host. The Hoc service does not perform DNS queries to resolve this FQDN. It returns the static ip addresses defined in the **StaticHosts.IpAddress** parameter. This name must be unique across the table.

IpAddresses (Config Parameter) | Table: StaticHosts

Type	Text
Range	Size(0..255)
Default	
Script/CLI	Hoc.StaticHosts[].IpAddresses
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.650.100.1.300

List of static IP addresses associated with the FQDN specified in the **StaticHosts.Name** parameter. This list contains numerical IPv4 or IPv6 addresses. IP addresses MUST be separated by a comma (,).

Delete (Row Command) | Table: StaticHosts

Script/CLI:	Hoc.StaticHosts[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.650.100.1.1000

Deletes this row.

SystemContact (Config Parameter)

Type	Text
Range	Size(0..255)
Default	
Script/CLI	Hoc.SystemContact
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.800.100

Indicates the contact information for the device. This information is for display purposes only and does not affect the behavior of the device. The value of this parameter is also returned by the "sysContact" object in SNMPv2-MIB.

SystemName (Config Parameter)

Type	Text
Range	Size(0..255)
Default	
Script/CLI	Hoc.SystemName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.800.200

Indicates the name of the device. This information is for display purposes only and does not affect the behavior of the device. The value of this parameter is also returned by the "sysName" object in SNMPv2-MIB.

SystemLocation (Config Parameter)

Type	Text
Range	Size(0..255)
Default	
Script/CLI	Hoc.SystemLocation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.800.300

Indicates the physical location of the device. This information is for display purposes only and does not affect the behavior of the device. The value of this parameter is also returned by the "sysLocation" object in SNMPv2-MIB.

HttpUaHeaderFormat (Config Parameter)

Type	Text
Range	
Default	%product%/v%version% %profile%
Script/CLI	Hoc.HttpUaHeaderFormat
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.800.1000.100

The text to display in the HTTP User-Agent Header. Macros can be used to include information specific to the unit.
The supported macros are:

- %version% - Application version.
- %mac% - MAC address.
- %macDash% - MAC address with dash separators.
- %product% - Product name.
- %profile% - Profile.
- %serial% - Serial number.
- %% - Insert % character.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Hoc.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Hoc.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.700.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

ClearDnsCache (Command)

Clears the DNS cache information.

InsertStaticHost (Command)

Inserts a new static host in the **StaticHosts** table.

Name (Argument) | Command: InsertStaticHost

Type	Text
Range	Size(1..253)
Default	

Contains the host name (FQDN). Cannot be empty.

IpAddresses (Argument) | Command: InsertStaticHost

Type	Text
Range	Size(0..255)
Default	

List of static IP addresses associated with the specified FQDN. This list contains numerical IPv4 or IPv6 addresses. IP addresses MUST be separated by a comma (,).

Index (Argument) | Command: InsertStaticHost

Type	UInt32
Range	
Default	0

Index in the table. A value of zero (default) causes automatic selection of the largest current index value + 1. If the index value already exists in the table, the insertion is refused.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

SetCurrentDateTime (Command)

Manually sets the system date/time to the specified value. If a SNTP server is configured, the time set by this command can be overriden at any time. This command must be used with local time. To control the timezone, use the **StaticTimeZone** parameter.

Note: The configured date/time will be lost after a reboot on devices with no real-time clock.

DateTime (Argument) | Command: SetCurrentDateTime

Type	Text
Range	Size(19..19)
Default	

Contains the date/time in the format "YYYY-MM-DD HH:MM:SS".

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Hoc service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.700.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	System management network interface is now %1$s.	Info	This message is issued when a new network interface is designated to become the system management interface.
12	Partial reset: system management network interface is now %1$s.	Warning	This message is issued when a new network interface is designated to become the system management interface after a partial reset is performed.
20	Host name is now: %1$s.	Info	This message is issued when the host name is changed.
30	Unable to set host name: %1$s.	Error	This message is issued when the host name cannot be set.
40	Current SNTP server list has been modified: %1$s.	Info	This message is issued when the current SNTP server list is changed. Depending on the value of **SnmpConfigSource** the list of NTP servers can be set automatically (by DHCP for example) or statically.
45	Current SNTP configuration is invalid. Therefore no SNTP request will be issued.	Warning	This message is issued when the current SNTP configuration is changed and invalid. The reason can be an invalid combination of **SntpConfigSource** and Basic Network Interface (Bni) automatic network interface ConnectionType, if any.
50	Static time zone is now: %1$s.	Debug	This message is issued when the static time zone is changed.
60	SNTP configuration source is now %1$s.	Debug	This message is issued when the SNTP configuration source is changed.
70	Static SNTP server list has been modified: %1$s.	Debug	This message is issued when the static SNTP server list is changed.
72	System clock is now synchronised to %1$s with SNTP server %2$s: %3$d.	Debug	This notification is issued everytime the system time is synchronised. It indicates the IP address of the actual NTP server that provided the time source.
75	System clock is now synchronised with %1$s.	Info	This message is issued when the system clock is synchronised.

NumKey	Message	Severity	Description
77	System clock is resynchronised from %1$s to %2$s.	Warning	This message is issued when the clock is resynchronised. This message is sent when the difference between the current time and the synchronized time is more than 7 seconds. Note that an abnormal difference between the current time and the synchronised time could mean a possible attack.
78	System clock is desynchronised.	Error	This message is issued when the system clock is desynchronised. Some security protocols (TLS, HTTPS) do not work when the system clock is desynchronised.
79	System clock is set to a previously saved date and time.	Warning	This message is sent when the time server could not be initially reached and a fallback time is applied to the system clock. The chosen fallback time is the most recent time among the "previously saved time", the "firmware build date", and the "unit production date".
80	Current default router is now: %1$s.	Info	This message is issued when the current default router is changed.
85	Current default router is invalid.	Warning	This message is issued when the current default router is not reachable. The reason can be an invalid combination of **DefaultRouterConfigSource** and Basic Network Interface (Bni) automatic network interface ConnectionType, if any.
88	No current default router defined.	Warning	This message is issued when the current default router is not defined. The reason can be an invalid combination of **DefaultRouterConfigSource** and Basic Network Interface (Bni) automatic network interface ConnectionType, if any.
90	Default router configuration source is now %1$s.	Debug	This message is issued when the default router configuration source is changed.
100	Static default router is now: %1$s.	Debug	This message is issued when the static default router is changed.
101	Current default IPv6 router is now: %1$s.	Info	This message is issued when the current default IPv6 router is changed.

NumKey	Message	Severity	Description
102	Current default IPv6 router is invalid.	Warning	This message is issued when the current default IPv6 router is not reachable. The reason can be an invalid combination of **DefaultIPv6RouterConfigSource** and Basic Network Interface (Bni) IPv6 automatic network interface ConnectionType, if any.
103	No current default IPv6 router defined.	Warning	This message is issued when the current default IPv6 router is not defined. The reason can be an invalid combination of **DefaultIPv6RouterConfigSource** and Basic Network Interface (Bni) IPv6 automatic network interface ConnectionType, if any.
104	Default IPv6 router configuration source is now %1$s.	Debug	This message is issued when the default IPv6 router configuration source is changed.
105	Static default IPv6 router is now: %1$s.	Debug	This message is issued when the static default IPv6 router is changed.
110	Current DNS server list has been modified.	Info	This message is issued when the current DNS server list is changed.
115	Current DNS configuration is invalid. Therefore no DNS request will be issued.	Warning	This message is issued when the current DNS configuration is changed and invalid. The reason can be an invalid combination of **DnsServersConfigSource** and Basic Network Interface (Bni) automatic network interface ConnectionType, if any.
120	DNS server configuration source is now %1$s.	Debug	This message is issued when the DNS servers configuration source is changed.
130	Static DNS server list has been modified.	Debug	This message is issued when the static DNS server list is changed.
200	Current domain name is now: %1$s.	Info	This message is issued when the current domain name is changed.
210	Unable to set domain name: %1$s.	Error	This message is issued when the current domain name cannot be set.
220	Domain name configuration source is now %1$s.	Debug	This message is issued when the domain name configuration source is changed.
230	Static domain name is now: %1$s.	Debug	This message is issued when the static domain name is changed.

NumKey	Message	Severity	Description
240	System management network interface named %1$s is invalid. Automatically updated to %2$s.	Warning	This message is issued when a network interface with an invalid name is encountered at service startup. An invalid name starts with a character that is not a letter or contains a character other than a letter, number or underscore.
250	SNTP server list is empty or the device has no real-time clock.	Warning	This message is issued when the SNTP server list is empty, or if there is no real-time clock, and the user manually sets a date/time. The date/time will be lost after a reboot on devices with no real-time clock.
260	SNTP server list is not empty.	Warning	This message is issued when the SNTP server list is not empty and the date/time is manually set. The date/time can be overriden by the SNTP server.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.

NumKey	Message	Severity	Description
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.

NumKey	Message	Severity	Description
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Hoc.

Message	Severity	Description
Trying to assign an inexistent network interface (%1$s) as system management interface.	Warning	This message is issued when an inexistent network interface is designated to become the system management interface. This would result in incapacity to connect to management services.
Operation successful but the host name does not follow the RFC 1035 preferred syntax.	Warning	This message is issued when the host name is RFC 1035 compliant but does not follow its preferred syntax.
Static host %1$s already exists.	Error	Creation of this static host is unauthorized because it already exists.
It is not allowed to modify the FQDN (%1$s) of an existing entry in table StaticHosts.	Error	The FQDN of the static host of an existing table entry cannot be modified.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.

Message	Severity	Description
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

IP routing (IpRouting)

The IP Routing (IpRouting) service manages the unit's IP routing table.

Parameters

AdvancedIpRoutes (Table: user-defined, 4 lines max.)

This table shows the configured routes in the table.

Id (Index) | Table: AdvancedIpRoutes

Type	UInt32
Range	
Script/CLI	IpRouting.AdvancedIpRoutes[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.200.1.50

Unique identifier of the row in the table.

Priority (Config Parameter) | Table: AdvancedIpRoutes

Type	UInt32
Range	1..252
Default	1
Script/CLI	IpRouting.AdvancedIpRoutes[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.200.1.100

Priority of the ip route execution.

Activation (Config Parameter) | Table: AdvancedIpRoutes

Type	EnableDisable
Range	
Default	Disable
Script/CLI	IpRouting.AdvancedIpRoutes[].Activation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.200.1.200

Activates this route.

- Enable: Activate this route.
- Disable: Do not activate this route.

SourceAddress (Config Parameter) | Table: AdvancedIpRoutes

Type	Text
Range	Size(0..51)
Default	
Script/CLI	IpRouting.AdvancedIpRoutes[].SourceAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.200.1.300

Specifies the source IP address criteria an incoming packet must have to match this rule. When left empty, any source address matches this rule. The supported format for the source network is: IP address[/mask].
When specifying a network name, it is mandatory to use the '/' format.

- Example: 192.168.1.0
- Example: 192.168.1.0/24
- Example: Lan1/

SourceLink (Config Parameter) | Table: AdvancedIpRoutes

Type	Text
Range	Size(0..51)
Default	
Script/CLI	IpRouting.AdvancedIpRoutes[].SourceLink
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.200.1.400

Specifies the source link criteria an incoming packet must have to match this rule. When left empty, packets received on any link match this rule.

ForwardToNetwork (Config Parameter) | Table: AdvancedIpRoutes

Type	Text
Range	Size(0..51)
Default	
Script/CLI	IpRouting.AdvancedIpRoutes[].ForwardToNetwork
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.200.1.500

Network on which the packet is forwarded.

Delete (Row Command) | Table: AdvancedIpRoutes

Script/CLI:	IpRouting.AdvancedIpRoutes[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.200.1.900

Deletes this row.

StaticIpRoutes (Table: user-defined, 50 lines max.)

This table shows the configured IPv4 static routes in the table.

Index (Index) | Table: StaticIpRoutes

Type	UInt32
Range	
Script/CLI	IpRouting.StaticIpRoutes[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.600.1.100

Unique identifier of the row in the table.

Link (Config Parameter) | Table: StaticIpRoutes

Type	Text
Range	Size(0..51)
Default	
Script/CLI	IpRouting.StaticIpRoutes[].Link
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.600.1.200

Output link (interface) name. When left empty, the link is selected automatically.

Destination (Config Parameter) | Table: StaticIpRoutes

Type	Text
Range	Size(0..51)
Default	
Script/CLI	IpRouting.StaticIpRoutes[].Destination
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.600.1.300

Specifies the destination IP address criteria that an outgoing packet must have to match this route.
The supported format for the destination is: IP address[/mask].
When specifying a network as a destination, it is mandatory to use the "/" format.

- Example: 192.168.1.5 specifies an IP address as the destination.
- Example: 192.168.1.0/24 specifies a network address as the destination.

Gateway (Config Parameter) | Table: StaticIpRoutes

Type	Text
Range	Size(0..51)
Default	
Script/CLI	IpRouting.StaticIpRoutes[].Gateway
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.600.1.400

Specifies the IP address of the gateway used by the route.

Delete (Row Command) | Table: StaticIpRoutes

Script/CLI:	IpRouting.StaticIpRoutes[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.600.1.500

Deletes this row.

Ipv4ForwardingEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	IpRouting.Ipv4ForwardingEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.800

Enables/disables IPv4 forwarding.
1. Enable: Forwarding is enabled.
2. Disable: Forwarding is disabled.

ConfigModifiedStatus (Status Parameter)

Type	Enum
Range	Yes(100) | No(200)
Script/CLI	IpRouting.ConfigModifiedStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.10000.100

Shows whether or not the routing table configuration has been modified without being applied.
1. Yes: The configuration has been modified but it has not been applied.
2. No: The IP routing service uses the configured rules.

Use the command `IpRouting.ApplyConfig` to apply the configuration.

AdvancedIpRoutesStatus (Table)

This table shows the current advanced routes used by the unit.

Id (Index) | Table: AdvancedIpRoutesStatus

Type	UInt32
Range	
Script/CLI	IpRouting.AdvancedIpRoutesStatus[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.10000.200.1.50

Unique identifier of the row in the table.

Priority (Status Parameter) | Table: AdvancedIpRoutesStatus

Type	UInt32
Range	
Script/CLI	IpRouting.AdvancedIpRoutesStatus[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.10000.200.1.100

Unique identifier of the row in the table.

SourceAddress (Status Parameter) | Table: AdvancedIpRoutesStatus

Type	Text
Range	
Script/CLI	IpRouting.AdvancedIpRoutesStatus[].SourceAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.10000.200.1.200

Source address[/mask] criteria used to match the rule.

SourceLink (Status Parameter) | Table: AdvancedIpRoutesStatus

Type	Text
Range	
Script/CLI	IpRouting.AdvancedIpRoutesStatus[].SourceLink
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.10000.200.1.300

Source link criteria used to match the rule.

ForwardToNetwork (Status Parameter) | Table: AdvancedIpRoutesStatus

Type	Text
Range	
Script/CLI	IpRouting.AdvancedIpRoutesStatus[].ForwardToNetwork
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.10000.200.1.350

Network on which the packet is forwarded.

Status (Status Parameter) | Table: AdvancedIpRoutesStatus

Type	Enum
Range	Disabled(100) | InvalidConfig(200) | Active(300) | DuplicatePriority(400)
Script/CLI	IpRouting.AdvancedIpRoutesStatus[].Status
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.10000.200.1.400

Status of the rule

- Disabled: The advanced IP route is disabled.
- InvalidConfig: The advanced IP route cannot be applied.
- Active: The advanced IP route is currently active.
- DuplicatePriority: The entered Priority level already exists.

IpRoutesStatus (Table)

This table shows the current IPv4 routes used by the unit.

Index (Index) | Table: IpRoutesStatus

Type	UInt32
Range	
Script/CLI	IpRouting.IpRoutesStatus[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.10000.300.1.100

Unique identifier of the row in the table.

Link (Status Parameter) | Table: IpRoutesStatus

Type	Text
Range	
Script/CLI	IpRouting.IpRoutesStatus[].Link
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.10000.300.1.200

Link (interface) ID.

Destination (Status Parameter) | Table: IpRoutesStatus

Type	Text
Range	
Script/CLI	IpRouting.IpRoutesStatus[].Destination
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.10000.300.1.300

Destination IP address or network address.
When the address is a network address, the format is 'address/mask length'

- Example: 192.168.1.25 for an IP address.
- Example: 192.168.1.0/24 for a network address with a mask length of 24 bits.

Gateway (Status Parameter) | Table: IpRoutesStatus

Type	Text
Range	
Script/CLI	IpRouting.IpRoutesStatus[].Gateway
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.10000.300.1.400

Specifies the gateway IP address.

Protocol (Status Parameter) | Table: IpRoutesStatus

Type	Enum
Range	Other(100) | Kernel(200) | Static(300) | Dhcp(400)
Script/CLI	IpRouting.IpRoutesStatus[].Protocol
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.10000.300.1.500

Identifies the entity that installed the route.

- Dhcp: The route was installed dynamically by the DHCP protocol.
- Static: The route was installed by the administrator of the unit.
- Kernel: The route was installed by the operating system.
- Other: The route was installed by another entity.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	IpRouting.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	IpRouting.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3500.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

ApplyConfig (Command)

Applies the configured routes.

InsertAdvancedRoute (Command)

Inserts a new row at the end of the **AdvancedIpRoutes** table.

Id (Argument) | Command: InsertAdvancedRoute

Type	UInt32
Range	0..2147483647
Default	0

Unique numerical identifier for this Route table entry.
The special value '0' (default value) generates an ID equal to the largest current ID value + 1.

Priority (Argument) | Command: InsertAdvancedRoute

Type	UInt32
Range	0..252
Default	0

Priority of the ip route execution.
When the special value '0' (default value) is used, the IpRouting service generates a priority equal to the highest value of the existing priorities + 1

Note: when the generated priority exceeds 252, the IpRouting service uses the default value of the **AdvancedIpRoutes.Priority** (1).

InsertStaticIpRoute (Command)

Inserts a new row at the end of the **StaticIpRoutes** table.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

RollbackConfig (Command)

Rolls back the current configuration to the running configuration as showed in the status. The current configuration is lost.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the IpRouting service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.3500.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
5	Unable to add route to %1$s via %2$s on link %3$s.	Error	Unable to add the route to the routing table.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.

NumKey	Message	Severity	Description
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to IpRouting.

Message	Severity	Description
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.

Message	Severity	Description
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Integrated Services Digital Network (Isdn)

The Integrated Services Digital Network (ISDN) service manages the ISDN parameters for BRI and PRI telephony interfaces.

Parameters

PrimaryRateInterface (Table)

Configuration parameters related to the Primary Rate interfaces on this managed device.

Name (Index) | Table: PrimaryRateInterface

Type	Text
Range	
Script/CLI	Isdn.PrimaryRateInterface[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.100.1.100

Name that identifies the interface.

EndpointType (Config Parameter) | Table: PrimaryRateInterface

Type	Enum
Range	Te(100) | Nt(200)
Default	Te
Script/CLI	Isdn.PrimaryRateInterface[].EndpointType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.100.1.200

Defines the endpoint type:

- Te: Terminal Equipment
- Nt: Network Termination

When the **SignalingChannel.Protocol** parameter is set to QSIG, the endpoint type will only be used in the second layer (LAPD) since it is a concept that does not exist within QSIG.

PortPinout (Config Parameter) | Table: PrimaryRateInterface

Type	Enum
Range	Auto(100) | Te(200) | Nt(300)
Default	Auto
Script/CLI	Isdn.PrimaryRateInterface[].PortPinout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.100.1.250

Defines the port pinout:

- Auto: The pinout is set according to the endpoint type.
- Te: Force the pinout to TE regardless of the endpoint type.
- Nt: Force the pinout to NT regardless of the endpoint type.

See **PrimaryRateInterface.EndpointType** parameter for a description of the endpoint type.

LineCoding (Config Parameter) | Table: PrimaryRateInterface

Type	Enum
Range	B8zs(100) | Hdb3(200) | Ami(300)
Default	Hdb3
Script/CLI	Isdn.PrimaryRateInterface[].LineCoding
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.100.1.400

Defines the transmission encoding of bits:

- B8ZS: Bipolar with 8-Zeros Substitution (T1 lines)
- HDB3: High-Density Bipolar with 3-zeros (E1 lines)
- AMI: Alternate Mark Inversion (E1 and T1 lines)

For further information, see ITU-T Recommendation G.703.

LineFraming (Config Parameter) | Table: PrimaryRateInterface

Type	Enum
Range	Sf(100) | Esf(200) | Crc4(300) | NoCrc4(400)
Default	Crc4
Script/CLI	Isdn.PrimaryRateInterface[].LineFraming
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.100.1.500

Defines the frame format:

- SF: Super frame. Sometimes known as D4 (T1 lines)
- ESF: Extended super frame (T1 lines)
- CRC4: Cyclic redundancy check 4 (E1 lines)
- NO-CRC4: No Cyclic redundancy check 4 (E1 lines)

For further information, see ITU-T Recommendation G.704.

NetworkLocation (Config Parameter) | Table: PrimaryRateInterface

Type	Enum
Range	User(100) | Private(200) | Public(300) | Transit(400) | International(500)
Default	User
Script/CLI	Isdn.PrimaryRateInterface[].NetworkLocation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.100.1.600

Defines the value of the network location in the progress indicator messages sent by the unit.

PreferredEncodingScheme (Config Parameter) | Table: PrimaryRateInterface

Type	Enum
Range	G711alaw(100) | G711ulaw(200)
Default	G711alaw
Script/CLI	Isdn.PrimaryRateInterface[].PreferredEncodingScheme
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.100.1.700

Defines the preferred data encoding scheme in the bearer capabilities (user information layer 1 protocol). This encoding scheme is used when initiating a call on the ISDN side.

FallbackEncodingScheme (Config Parameter) | Table: PrimaryRateInterface

Type	Enum
Range	G711alaw(100) | G711ulaw(200)
Default	G711ulaw
Script/CLI	Isdn.PrimaryRateInterface[].FallbackEncodingScheme
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.100.1.750

Defines the fallback data encoding scheme in the bearer capabilities (user information layer 1 protocol).

ChannelRange (Config Parameter) | Table: PrimaryRateInterface

Type	Text
Range	Size(1..10)
Default	1-30
Script/CLI	Isdn.PrimaryRateInterface[].ChannelRange
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.100.1.800

Defines the range of active bearer channels.

IncomingChannelRange (Config Parameter) | Table: PrimaryRateInterface

Type	Text
Range	Size(0..255)
Default	
Script/CLI	Isdn.PrimaryRateInterface[].IncomingChannelRange
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.100.1.830

Bearer channels are by default usable for both incoming and outgoing calls. Use this range to reserve channels for incoming calls.
NOTE: Channels outside of the range defined by **ChannelRange** are ignored.

NOTE: Channels reserved in both **IncomingChannelRange** and **OutgoingChannelRange** parameters are considered usable for both incoming and outgoing calls.

The string has the following syntax:

- ',': Separator between non-consecutive lists of channels or single channel.
- 'n': A single channel, where n is the channel number.
- 'm-n': List of channels where m is the start channel number and n is the end channel number.

NOTE: The space character is ignored and duplication is not allowed. Channels must be specified in low to high order.

Example: '1,12-15': The accepted channels are 1, 12, 13, 14 and 15.

OutgoingChannelRange (Config Parameter) | Table: PrimaryRateInterface

Type	Text
Range	Size(0..255)
Default	
Script/CLI	Isdn.PrimaryRateInterface[].OutgoingChannelRange
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.100.1.860

Bearer channels are by default usable for both incoming and outgoing calls. Use this range to reserve channels for outgoing calls.
NOTE: Channels outside of the range defined by ChannelRange are ignored.

NOTE: Channels reserved in both **IncomingChannelRange** and **OutgoingChannelRange** parameters are considered usable for both incoming and outgoing calls.

The string has the following syntax:

- ',': Separator between non-consecutive lists of channels or single channel.
- 'n': A single channel, where n is the channel number.
- 'm-n': List of channels where m is the start channel number and n is the end channel number.

NOTE: The space character is ignored and duplication is not allowed. Channels must be specified in low to high order.

Example: '1,12-15': The accepted channels are 1, 12, 13, 14 and 15.

ChannelAllocationStrategy (Config Parameter) | Table: PrimaryRateInterface

Type	Enum
Range	Ascending(100) | Descending(200) | RoundRobinAscending(300) | RoundRobinDescending(400)
Default	Ascending
Script/CLI	Isdn.PrimaryRateInterface[].ChannelAllocationStrategy
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.100.1.900

Defines the strategy for selecting bearer channels. Available strategies are:

- Ascending: select the lowest-numbered non-busy bearer channel
- Descending: select the highest-numbered non-busy bearer channel

- RoundRobinAscending: use a cyclic round-robin search; starting from the bearer channel that follows the bearer channel used for the last call, select the lowest-numbered non-busy bearer channel
- RoundRobinDescending: use a cyclic round-robin search; starting from the bearer channel that precedes the bearer channel used for the last call, select the highest-numbered non-busy bearer channel

MaxActiveCalls (Config Parameter) | Table: PrimaryRateInterface

Type	UInt32
Range	0..30
Default	0
Script/CLI	Isdn.PrimaryRateInterface[].MaxActiveCalls
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.100.1.1000

Defines the maximum number of active calls on the interface.
Note: The special value 0 indicates no maximum number of active calls.

SignalInformationElementEnable (Config Parameter) | Table: PrimaryRateInterface

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Isdn.PrimaryRateInterface[].SignalInformationElementEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.100.1.1050

Defines whether the signal information element is enabled on the interface. When activated at the Network UNI-side (**PrimaryRateInterfaceEndpointType** parameter set to Nt), the signal information element is sent to the User UNI-side. When activated at the User UNI-side (**PrimaryRateInterfaceEndpointType** parameter set to Te), the tone indicated in the signal information element is played in the IP direction.

InbandToneGenerationEnable (Config Parameter) | Table: PrimaryRateInterface

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.PrimaryRateInterface[].InbandToneGenerationEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.100.1.1100

Defines whether inband tone generation is enabled on the interface.
When activated at the User UNI-side (**PrimaryRateInterfaceEndpointType** parameter set to Te), only the ringback tone is generated.

When the **SignalingChannel.Protocol** parameter is set to 'QSIG' and this parameter is activated, the incoming side of the call plays the tones inband.

InbandDtmfDialingEnable (Config Parameter) | Table: PrimaryRateInterface

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.PrimaryRateInterface[].InbandDtmfDialingEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.100.1.1200

Defines whether inband DTMF dialing is enabled.

OverlapDialingEnable (Config Parameter) | Table: PrimaryRateInterface

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.PrimaryRateInterface[].OverlapDialingEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.100.1.1300

Defines whether overlap dialing is enabled on the interface.

CallingNameMaxLength (Config Parameter) | Table: PrimaryRateInterface

Type	UInt32
Range	0..82
Default	34
Script/CLI	Isdn.PrimaryRateInterface[].CallingNameMaxLength
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.100.1.1400

Defines the maximum length of the calling party name for calls from SIP to ISDN on the interface.

ExclusiveBChannelSelectionEnable (Config Parameter) | Table: PrimaryRateInterface

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Isdn.PrimaryRateInterface[].ExclusiveBChannelSelectionEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.100.1.1500

Defines whether exclusive B-Channel selection is enabled for calls from SIP to ISDN on the interface.

SendingCompleteEnable (Config Parameter) | Table: PrimaryRateInterface

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.PrimaryRateInterface[].SendingCompleteEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.100.1.1600

Defines whether the Sending Complete information element in SETUP messages is enabled for calls from SIP to ISDN on the interface.

ClipEnable (Config Parameter) | Table: PrimaryRateInterface

Type	Enum
Range	UserOnly(0) | Enable(1) | Disable(2)
Default	UserOnly
Script/CLI	Isdn.PrimaryRateInterface[].ClipEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.100.1.1700

Enables the CLIP service, which is offered to the called party to see the calling party's ISDN number. CLIP is complemented by privacy rules controlled by the **ClirEnable** and **ClirOverrideEnable** parameters. The **ClipEnable** parameter has the following effect:

- UserOnly: Sends a Calling Number IE which contains the calling number digits when acting as the User UNI-side (**PrimaryRateInterfaceEndpointType** parameter set to Te) otherwise the Calling Number IE is not sent.
- Enable: Sends a Calling Number IE which contains the calling number digits.
- Disable: The Calling Number IE is never sent.

ClirEnable (Config Parameter) | Table: PrimaryRateInterface

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Isdn.PrimaryRateInterface[].ClirEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.100.1.1725

Enables the CLIR service, which is offered to the calling party to restrict presentation of the calling party's ISDN number to the called party.
Setting this parameter to "Disable" disables the CLIR service.

Setting this parameter to "Enable" enables the CLIR service. This has the following effects:

For all ISDN signaling protocols except QSIG:

- On a TE interface at the originating network side, when sending a SETUP message with a Calling Party Number (CPN) IE, the Presentation Indicator (PI) is set to "Restricted". The calling party number itself is included in the CPN IE if available.
- On a NT interface at the originating network side, when receiving a SETUP message with a CPN IE, the PI is set to "Restricted". The calling party number itself is forwarded.

For the QSIG signaling protocol:

- Sending a SETUP message: The PI is set to "Restricted" in the CPN IE inserted in the SETUP message sent to the ISDN, unless the CLIR override option is set. However, even if PI is set to "Restricted", the calling number is included in the CPN IE.
- Receiving a SETUP message: If PI is set in the received message, the calling party number is removed, unless the CLIR override option is set.

ClirOverrideEnable (Config Parameter) | Table: PrimaryRateInterface

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Isdn.PrimaryRateInterface[].ClirOverrideEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.100.1.1750

Enables the CLIR override option. This option allows the calling party number to be presented to the destination party even when the Calling Party Number (CPN) IE's Presentation Indicator (PI) is set to "Restricted". This option is typically used for police or emergency services.
Setting this parameter to "Disable" disables the CLIR Override option.

Setting this parameter to "Enable" enables the CLIR Override option. This has the following effects:

For all ISDN signaling protocols except QSIG:

- The override option acts on the NT interface of the destination network side. It prevents the number to be removed from the CPN IE inserted in the SETUP message sent to the destination TE.

For the QSIG signaling protocol:

- The override option prevents the calling name to be removed from the CPN IE in a received SETUP message.

SendRestartOnStartupEnable (Config Parameter) | Table: PrimaryRateInterface

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.PrimaryRateInterface[].SendRestartOnStartupEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.100.1.1800

Defines whether the RESTART message is sent upon a signaling channel "UP" event

PrimaryRateInterfaceInterop (Table)

Interop configuration parameters related to the Primary Rate interfaces on this managed device.

Name (Index) | Table: PrimaryRateInterfaceInterop

Type	Text
Range	
Script/CLI	Isdn.PrimaryRateInterfaceInterop[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.50000.100.1.100

Name that identifies the interface.

ProgressIndicatorInSetupEnable (Config Parameter) | Table: PrimaryRateInterfaceInterop

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.PrimaryRateInterfaceInterop[].ProgressIndicatorInSetupEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.50000.100.1.200

Defines whether or not the Progress Indicator information element is allowed in the SETUP message when acting as the originating side.
See the **SignalingChannel.SendProgressIndicatorIE** parameter for other conditions for sending Progress Indicator IE.

ProgressIndicatorInSetupAckEnable (Config Parameter) | Table: PrimaryRateInterfaceInterop

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.PrimaryRateInterfaceInterop[].ProgressIndicatorInSetupAckEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.50000.100.1.300

Defines whether or not the Progress Indicator information element is allowed in the SETUP ACK when acting as the terminating side.
See the **SignalingChannel.SendProgressIndicatorIE** parameter for other conditions for sending Progress Indicator IE.

ProgressIndicatorInCallProgressForSetupEnable (Config Parameter) | Table: PrimaryRateInterfaceInterop

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.PrimaryRateInterfaceInterop[].ProgressIndicatorInCallProgressForSetupEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.50000.100.1.400

Defines whether or not the Progress Indicator information element is allowed in the CALL PROCEEDING message in response to a SETUP message when acting as the terminating side.
See the **SignalingChannel.SendProgressIndicatorIE** parameter for other conditions for sending Progress Indicator IE.

ProgressIndicatorInProgressEnable (Config Parameter) | Table: PrimaryRateInterfaceInterop

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.PrimaryRateInterfaceInterop[].ProgressIndicatorInProgressEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.50000.100.1.450

Defines whether or not the Progress Indicator information element is allowed in the PROGRESS message in response to a SETUP message when acting as the terminating side.
See the **SignalingChannel.SendProgressIndicatorIE** parameter for other conditions for sending Progress Indicator IE.

ProgressIndicatorInAlertingEnable (Config Parameter) | Table: PrimaryRateInterfaceInterop

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.PrimaryRateInterfaceInterop[].ProgressIndicatorInAlertingEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.50000.100.1.500

Defines whether or not the Progress Indicator information element is allowed in the ALERTING message.
See the **SignalingChannel.SendProgressIndicatorIE** parameter for other conditions for sending Progress Indicator IE.

ProgressIndicatorInConnectEnable (Config Parameter) | Table: PrimaryRateInterfaceInterop

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.PrimaryRateInterfaceInterop[].ProgressIndicatorInConnectEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.50000.100.1.600

Defines whether or not the Progress Indicator information element is allowed in the CONNECT message.
See the **SignalingChannel.SendProgressIndicatorIE** parameter for other conditions for sending Progress Indicator IE.

MaximumFacilityWaitingDelay (Config Parameter) | Table: PrimaryRateInterfaceInterop

Type	UInt32
Range	0..1500
Default	0
Script/CLI	Isdn.PrimaryRateInterfaceInterop[].MaximumFacilityWaitingDelay
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.50000.100.1.700

Defines the maximum amount of time to wait for a FACILITY message, after receiving a SETUP message, before going on with normal call processing.

After receiving a SETUP message, the system waits for this amount of time for a FACILITY message. As soon as it receives a FACILITY message or the delay expires, it goes on with normal call processing.

A FACILITY message can contain useful information for the call. For example, it can contain a Calling Name.

In order for this to be effective, the **SignalingChannel.FacilityServicesEnable** parameter must be enabled.

The value 0 deactivates this waiting delay.

This value is expressed in milliseconds (ms).

UseImplicitInbandInfoEnable (Config Parameter) | Table: PrimaryRateInterfaceInterop

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.PrimaryRateInterfaceInterop[].UseImplicitInbandInfoEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.200.50000.100.1.800

This parameter defines how to interpret an incoming ISDN response message with a Progress Indicator information element No. 1 (the call is not end-to-end ISDN; further call progress information may be available in-band).
Inband information generation is only applied for outgoing ISDN calls. For incoming calls, this parameter does not apply, however it can interact with ISDN disconnect timers (Early/Late) depending on RTP and ISDN Progress indicators.

- Disable: The Inband information towards the SIP gateway is always locally generated, regardless if Inband information is received on the ISDN call.
- Enable: The Inband information towards the SIP gateway is always provided by the called ISDN peer and the NT side shall activate the B-channel connection with Inband information.

BasicRateInterface (Table)

Configuration and operational parameters for all physical Basic Rate interfaces on this managed device.

Name (Index) | Table: BasicRateInterface

Type	Text
Range	
Script/CLI	Isdn.BasicRateInterface[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.100

The physical interface name.

EndpointType (Config Parameter) | Table: BasicRateInterface

Type	Enum
Range	Te(100) | Nt(200)
Default	Te
Script/CLI	Isdn.BasicRateInterface[].EndpointType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.200

Defines the endpoint type:

- Te: Terminal Equipment
- Nt: Network Termination

When the **SignalingChannel.Protocol** parameter is set to QSIG, the endpoint type will only be used in the second layer (LAPD) since it is a concept that does not exist within QSIG.

ConnectionType (Config Parameter) | Table: BasicRateInterface

Type	Enum
Range	PointToPoint(100) | PointToMultiPoint(200)
Default	PointToMultiPoint
Script/CLI	Isdn.BasicRateInterface[].ConnectionType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.300

Defines the connection type:

- PointToPoint: Can only attach one device (for instance a PABX or PSTN)
- PointToMultiPoint: Can attach more than one device

PointToMultiPoint configuration is not available in QSIG.

NetworkLocation (Config Parameter) | Table: BasicRateInterface

Type	Enum
Range	User(100) | Private(200) | Public(300) | Transit(400) | International(500)
Default	User
Script/CLI	Isdn.BasicRateInterface[].NetworkLocation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.600

Defines the value of the network location in the progress indicator messages sent by the unit.

PreferredEncodingScheme (Config Parameter) | Table: BasicRateInterface

Type	Enum
Range	G711alaw(100) | G711ulaw(200)
Default	G711alaw
Script/CLI	Isdn.BasicRateInterface[].PreferredEncodingScheme
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.700

Defines the preferred data encoding scheme in the bearer capabilities (user information layer 1 protocol). This encoding scheme is used when initiating a call on the ISDN side.

FallbackEncodingScheme (Config Parameter) | Table: BasicRateInterface

Type	Enum
Range	G711alaw(100) | G711ulaw(200)
Default	G711ulaw
Script/CLI	Isdn.BasicRateInterface[].FallbackEncodingScheme
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.750

Defines the fallback data encoding scheme in the bearer capabilities (user information layer 1 protocol).

ChannelAllocationStrategy (Config Parameter) | Table: BasicRateInterface

Type	Enum
Range	Ascending(100) | Descending(200) | RoundRobinAscending(300) | RoundRobinDescending(400)
Default	Ascending
Script/CLI	Isdn.BasicRateInterface[].ChannelAllocationStrategy
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.900

Defines the strategy for selecting bearer channels. Available strategies are:

- Ascending: select the lowest-numbered non-busy bearer channel
- Descending: select the highest-numbered non-busy bearer channel
- RoundRobinAscending: use a cyclic round-robin search; starting from the bearer channel that follows the bearer channel used for the last call, select the lowest-numbered non-busy bearer channel
- RoundRobinDescending: use a cyclic round-robin search; starting from the bearer channel that precedes the bearer channel used for the last call, select the highest-numbered non-busy bearer channel

MaxActiveCalls (Config Parameter) | Table: BasicRateInterface

Type	UInt32
Range	0..2
Default	0
Script/CLI	Isdn.BasicRateInterface[].MaxActiveCalls
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.1000

Defines the maximum number of active calls on the interface.
Note: The special value 0 indicates no maximum number of active calls.

SignalInformationElementEnable (Config Parameter) | Table: BasicRateInterface

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Isdn.BasicRateInterface[].SignalInformationElementEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.1050

Defines whether the signal information element is enabled on the interface. When activated at the Network UNI-side (**BasicRateInterfaceEndpointType** parameter set to Nt), the signal information element is sent to the User UNI-side. When activated at the User UNI-side (**BasicRateInterfaceEndpointType** parameter set to Te), the tone indicated in the signal information element is played in the IP direction.

InbandToneGenerationEnable (Config Parameter) | Table: BasicRateInterface

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.BasicRateInterface[].InbandToneGenerationEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.1100

Defines whether inband tone generation is enabled on the interface. When activated at the User UNI-side (**BasicRateInterfaceEndpointType** parameter set to Te), only the ringback tone is generated.

When the **SignalingChannel.Protocol** parameter is set to 'QSIG' and this parameter is activated, the incoming side of the call plays the tones inband.

InbandDtmfDialingEnable (Config Parameter) | Table: BasicRateInterface

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.BasicRateInterface[].InbandDtmfDialingEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.1200

Defines whether inband DTMF dialing is enabled.

OverlapDialingEnable (Config Parameter) | Table: BasicRateInterface

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.BasicRateInterface[].OverlapDialingEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.1300

Defines whether overlap dialing is enabled on the interface.

CallingNameMaxLength (Config Parameter) | Table: BasicRateInterface

Type	UInt32
Range	0..82
Default	34
Script/CLI	Isdn.BasicRateInterface[].CallingNameMaxLength
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.1400

Defines the maximum length of the calling party name for calls from SIP to ISDN on the interface.

ExclusiveBChannelSelectionEnable (Config Parameter) | Table: BasicRateInterface

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Isdn.BasicRateInterface[].ExclusiveBChannelSelectionEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.1500

Defines whether exclusive B-Channel selection is enabled for calls from SIP to ISDN on the interface.

SendingCompleteEnable (Config Parameter) | Table: BasicRateInterface

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.BasicRateInterface[].SendingCompleteEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.1600

Defines whether the Sending Complete information element in SETUP messages is enabled for calls from SIP to ISDN on the interface.

ClipEnable (Config Parameter) | Table: BasicRateInterface

Type	Enum
Range	UserOnly(0) | Enable(1) | Disable(2)
Default	UserOnly
Script/CLI	Isdn.BasicRateInterface[].ClipEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.1700

Enables the CLIP service, which is offered to the called party to see the calling party's ISDN number. CLIP is complemented by privacy rules controlled by the **ClirEnable** and **ClirOverrideEnable** parameters. The **ClipEnable** parameter has the following effect:

- UserOnly: Sends a Calling Number IE which contains the calling number digits when acting as the User UNI-side (**PrimaryRateInterfaceEndpointType** parameter set to Te) otherwise the Calling Number IE is not sent.
- Enable: Sends a Calling Number IE which contains the calling number digits.
- Disable: The Calling Number IE is never sent.

ClirEnable (Config Parameter) | Table: BasicRateInterface

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Isdn.BasicRateInterface[].ClirEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.1725

Enables the CLIR service, which is offered to the calling party to restrict presentation of the calling party's ISDN number to the called party.
Setting this parameter to "Disable" disables the CLIR service.

Setting this parameter to "Enable" enables the CLIR service. This has the following effects:

For all ISDN signaling protocols except QSIG:

- On a TE interface at the originating network side, when sending a SETUP message with a Calling Party Number (CPN) IE, the Presentation Indicator (PI) is set to "Restricted". The calling party number itself is included in the CPN IE if available.
- On a NT interface at the originating network side, when receiving a SETUP message with a CPN IE, the PI is set to "Restricted". The calling party number itself is forwarded.

For the QSIG signaling protocol:

- Sending a SETUP message: The PI is set to "Restricted" in the CPN IE inserted in the SETUP message sent to the ISDN, unless the CLIR override option is set. However, even if PI is set to "Restricted", the calling number is included in the CPN IE.
- Receiving a SETUP message: If PI is set in the received message, the calling party number is removed, unless the CLIR override option is set.

ClirOverrideEnable (Config Parameter) | Table: BasicRateInterface

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Isdn.BasicRateInterface[].ClirOverrideEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.1750

Enables the CLIR override option. This option allows the calling party number to be presented to the destination party even when the Calling Party Number (CPN) IE's Presentation Indicator (PI) is set to "Restricted". This option is typically used for police or emergency services.

Setting this parameter to "Disable" disables the CLIR Override option.

Setting this parameter to "Enable" enables the CLIR Override option. This has the following effects:

For all ISDN signaling protocols except QSIG:

- The override option acts on the NT interface of the destination network side. It prevents the number to be removed from the CPN IE inserted in the SETUP message sent to the destination TE.

For the QSIG signaling protocol:

- The override option prevents the calling name to be removed from the CPN IE in a received SETUP message.

SendRestartOnStartupEnable (Config Parameter) | Table: BasicRateInterface

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.BasicRateInterface[].SendRestartOnStartupEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.1800

Defines whether the RESTART message is sent upon a signaling channel "UP" event

HookFlashKeypad (Config Parameter) | Table: BasicRateInterface

Type	Text
Range	Size(0..32)
Default	
Script/CLI	Isdn.BasicRateInterface[].HookFlashKeypad
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.1900

The actual keypad string that is to be considered as a hook-flash.
Setting this parameter to an empty string disables the hook-flash detection.

The permitted keypad must be made up of IA5 characters. See ITU-T Recommendation T.50.

KeypadReceptionTimeout (Config Parameter) | Table: BasicRateInterface

Type	UInt32
Range	0..4
Default	2
Script/CLI	Isdn.BasicRateInterface[].KeypadReceptionTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.2000

The actual time to wait before considering the keypad reception over.
The value is expressed in seconds.

Setting this parameter to 0 disables the timeout, thus assuming that all keypads will be received in a single Information message.

Msn (Config Parameter) | Table: BasicRateInterface

Type	Text
Range	Size(0..255)
Default	
Script/CLI	Isdn.BasicRateInterface[].Msn
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.2200

This enables the MSN supplementary service with a comma separated list of numbers.
The MSN supplementary service shall enable each individual terminal on one access to have one or more identities.

If the Called E.164 received from a call does not match any MSN numbers, the call is silently discarded.

This service is available only for a BRI interface configured in TE Point To Multipoint. This service is also disabled when all fields are blank. This field must contain numeric values.

The comma separated list must use the following syntax: 777, 888, 999, 555, 444

Msn2 (Config Parameter) | Table: BasicRateInterface

Type	Text
Range	Size(0..32)
Default	
Script/CLI	Isdn.BasicRateInterface[].Msn2
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.2300

Deprecated: Use **Isdn.BasicRateInterface.Msn** instead. This enables the MSN supplementary service with these numbers.

The MSN supplementary service shall enable each individual terminal on one access to have one or more identities.

If the Called E.164 received from a call does not match any MSN numbers, the call is silently discarded.

This service is available only for a BRI interface configured in TE Point To Multipoint. This service is also disabled when all fields are blank. This field must contain numeric values.

Msn3 (Config Parameter) | Table: BasicRateInterface

Type	Text
Range	Size(0..32)
Default	
Script/CLI	Isdn.BasicRateInterface[].Msn3
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.2400

Deprecated: Use **Isdn.BasicRateInterface.Msn** instead. This enables the MSN supplementary service with these numbers.

The MSN supplementary service shall enable each individual terminal on one access to have one or more identities.

If the Called E.164 received from a call does not match any MSN numbers, the call is silently discarded.

This service is available only for a BRI interface configured in TE Point To Multipoint. This service is also disabled when all fields are blank. This field must contain numeric values.

TeiNegotiation (Config Parameter) | Table: BasicRateInterface

Type	Enum
Range	LinkUp(100) | PowerUp(200) | SignalingUp(300)
Default	LinkUp
Script/CLI	Isdn.BasicRateInterface[].TeiNegotiation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.100.1.2500

Sets the Terminal Endpoint Identifier (TEI) negotiation strategy.

- LinkUp: Each time the physical link comes up, the unit renegotiates the TEI value.
- PowerUp: When the physical link comes up, the unit does not renegotiate the TEI value. The value obtained at power-up is reused.
- SignalingUp: Each time the signaling link comes up, the unit renegotiates the TEI value.

NOTE: only applies on Point To Multipoint connections.

BasicRateInterfaceInterop (Table)

Interop configuration parameters related to the Basic Rate interfaces on this managed device.

Name (Index) | Table: BasicRateInterfaceInterop

Type	Text
Range	
Script/CLI	Isdn.BasicRateInterfaceInterop[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.50000.100.1.100

Name that identifies the interface.

ProgressIndicatorInSetupEnable (Config Parameter) | Table: BasicRateInterfaceInterop

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.BasicRateInterfaceInterop[].ProgressIndicatorInSetupEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.50000.100.1.200

Defines whether or not the Progress Indicator information element is allowed in the SETUP message when acting as the originating side.
See the **SignalingChannel.SendProgressIndicatorIE** parameter for other conditions for sending Progress Indicator IE.

ProgressIndicatorInSetupAckEnable (Config Parameter) | Table: BasicRateInterfaceInterop

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.BasicRateInterfaceInterop[].ProgressIndicatorInSetupAckEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.50000.100.1.300

Defines whether or not the Progress Indicator information element is allowed in the SETUP ACK when acting as the terminating side.
See the **SignalingChannel.SendProgressIndicatorIE** parameter for other conditions for sending Progress Indicator IE.

ProgressIndicatorInCallProgressForSetupEnable (Config Parameter) | Table: BasicRateInterfaceInterop

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.BasicRateInterfaceInterop[].ProgressIndicatorInCallProgressForSetupEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.50000.100.1.400

Defines whether or not the Progress Indicator information element is allowed in the CALL PROCEEDING message in response to a SETUP message when acting as the terminating side.
See the **SignalingChannel.SendProgressIndicatorIE** parameter for other conditions for sending Progress Indicator IE.

ProgressIndicatorInProgressEnable (Config Parameter) | Table: BasicRateInterfaceInterop

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.BasicRateInterfaceInterop[].ProgressIndicatorInProgressEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.50000.100.1.450

Defines whether or not the Progress Indicator information element is allowed in the PROGRESS message in response to a SETUP message when acting as the terminating side.
See the **SignalingChannel.SendProgressIndicatorIE** parameter for other conditions for sending Progress Indicator IE.

ProgressIndicatorInAlertingEnable (Config Parameter) | Table: BasicRateInterfaceInterop

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.BasicRateInterfaceInterop[].ProgressIndicatorInAlertingEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.50000.100.1.500

Defines whether or not the Progress Indicator information element is allowed in the ALERTING message.
See the **SignalingChannel.SendProgressIndicatorIE** parameter for other conditions for sending Progress Indicator IE.

ProgressIndicatorInConnectEnable (Config Parameter) | Table: BasicRateInterfaceInterop

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.BasicRateInterfaceInterop[].ProgressIndicatorInConnectEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.50000.100.1.600

Defines whether or not the Progress Indicator information element is allowed in the CONNECT message.
See the **SignalingChannel.SendProgressIndicatorIE** parameter for other conditions for sending Progress Indicator IE.

MaximumFacilityWaitingDelay (Config Parameter) | Table: BasicRateInterfaceInterop

Type	UInt32
Range	0..1500
Default	0
Script/CLI	Isdn.BasicRateInterfaceInterop[].MaximumFacilityWaitingDelay
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.50000.100.1.700

Defines the maximum amount of time to wait for a FACILITY message, after receiving a SETUP message, before going on with normal call processing.
After receiving a SETUP message, the system waits for this amount of time for a FACILITY message. As soon as it receives a FACILITY message or the delay expires, it goes on with normal call processing.

A FACILITY message can contain useful information for the call. For example, it can contain a Calling Name.

In order for this to be effective, the **SignalingChannel.FacilityServicesEnable** parameter must be enabled.

The value 0 deactivates this waiting delay.

This value is expressed in milliseconds (ms).

UseImplicitInbandInfoEnable (Config Parameter) | Table: BasicRateInterfaceInterop

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.BasicRateInterfaceInterop[].UseImplicitInbandInfoEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.50000.100.1.800

This parameter defines how to interpret an incoming ISDN response message with a Progress Indicator information element No. 1 (the call is not end-to-end ISDN; further call progress information may be available in-band).
Inband information generation is only applied for outgoing ISDN calls. For incoming calls, this parameter does not apply, however it can interact with ISDN disconnect timers (Early/Late) depending on RTP and ISDN Progress indicators.

- Disable: The Inband information towards the SIP gateway is always locally generated, regardless if Inband information is received on the ISDN call.
- Enable: The Inband information towards the SIP gateway is always provided by the called ISDN peer and the NT side shall activate the B-channel connection with Inband information.

AllowTeiBroadcastInPtpEnable (Config Parameter) | Table: BasicRateInterfaceInterop

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.BasicRateInterfaceInterop[].AllowTeiBroadcastInPtpEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.300.50000.100.1.900

Defines whether or not an ISDN message with a TEI broadcast needs to be interpreted as a TEI 0 when the connection type is 'PointToPoint' (see **BasicRateInterfaceGroup.ConnectionType** parameter).

BearerChannelInfo (Table)

Port-specific operational, statistics, and active call data for ISDN B channels.

Index (Index) | Table: BearerChannelInfo

Type	Text
Range	
Script/CLI	Isdn.BearerChannelInfo[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.400.100.1.100

Identifies the Bearer Channel..

State (Status Parameter) | Table: BearerChannelInfo

Type	Enum
Range	Idle(100) | InUse(200) | Maintenance(300) | Error(400) | Disabled(500)
Script/CLI	Isdn.BearerChannelInfo[].State
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.400.100.1.200

The current call control state for this channel:

- Idle: The channel is available
- InUse: The channel is currently used
- Maintenance: Maintenance state, temporarily unavailable
- Error: Error on this channel
- Disabled: The channel is disabled

SignalingChannel (Table)

ISDN signaling table containing configuration and operational parameters for all ISDN signaling channels on this managed device.

InterfaceName (Index) | Table: SignalingChannel

Type	Text
Range	
Script/CLI	Isdn.SignalingChannel[].InterfaceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.100

Identifies the interface.

Protocol (Config Parameter) | Table: SignalingChannel

Type	Enum
Range	Dss1(100) | Dms100(200) | Ni2(300) | Ess5(400) | QSig(500)
Default	Dss1
Script/CLI	Isdn.SignalingChannel[].Protocol
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.200

Defines the protocol to use for the signaling channel:

- DSS1: Digital Subscriber Signaling System No.1
- DMS100: Digital Multiplex System 100
- NI2: National ISDN No.2
- ESS5: 5 Electronic Switching System (5ESS)
- QSIG: ECMA's protocol for Private Integrated Services Networks

FacilityServicesEnable (Config Parameter) | Table: SignalingChannel

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Isdn.SignalingChannel[].FacilityServicesEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.250

Defines whether or not supplementary services FACILITY messages and FACILITY information elements should be enabled on the ISDN interface.
Disable: Facility information elements are disabled in both directions (send and receive). No Facility information element can be inserted in sent messages. When receiving a FACILITY message containing supplementary services information, reply with a STATUS message saying the FACILITY is not supported.

Enable: Facility information elements are enabled in both directions (send and receive). Facility information elements can be inserted in sent messages. When receiving a FACILITY message containing supplementary services information, accept and interpret the message, processing supported supplementary service messages and silently discarding unsupported supplementary service messages.

Generic procedures for the control of ISDN supplementary services are defined in the recommendation ITU-T Q.932.

ColpEnable (Config Parameter) | Table: SignalingChannel

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Isdn.SignalingChannel[].ColpEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.300

Defines the Connected Number Information Element at the originating ISDN side:

- Enable: Sends a Connected Number IE within the CONNECT message, which contains the connected number digits once the transformation of the routing table has been applied.
- Disable: The Connected Number IE is never sent.

ColrEnable (Config Parameter) | Table: SignalingChannel

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Isdn.SignalingChannel[].ColrEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.400

Defines the Connected Number Information Element restriction at the destination ISDN side:

- enable: When activated at the User UNI-side (Te), marks the Connected Number IE with a "restricted" Presentation Indicator, which keeps privacy over the connected number digits. This option has no effect when activated at the Network UNI-side (Nt).
- disable: No restriction is applied.

When the **SignalingChannel.Protocol** parameter is set to 'QSIG', the effect of this parameter does not depend on the **PrimaryRateInterface.EndpointType** parameter (Nt or Te).

- Enable: The Presentation Indicator of the Connected Number IE is set to "restricted" in replies to incoming calls.
- Disable: There is no restriction on the connected user number.

ColrOverrideEnable (Config Parameter) | Table: SignalingChannel

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Isdn.SignalingChannel[].ColrOverrideEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.500

Defines the Connected Number Information Element restriction override at the originating ISDN side:

- enable: When activated at the Network UNI-side (Nt), the connected number digits are delivered even if the Presentation Indicator is set to "restricted". This option has no effect when activated at the User UNI-side (Te). This is a national option designed for emergency services.
- disable: The restriction is not overridden.

When the **SignalingChannel.Protocol** parameter is set to 'QSIG', the effect of this parameter does not depend on the **PrimaryRateInterface.EndpointType** parameter (Nt or Te).

- enable: When the Presentation Indicator of the Connected Number IE is set to "restricted", the restriction is overridden and the connected user number is presented to the calling user.
- disable: The restriction is not overridden.

ConpEnable (Config Parameter) | Table: SignalingChannel

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Isdn.SignalingChannel[].ConpEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.510

Connected Name identification Presentation (CONP) is a supplementary service which provides the name of the answering or alerting user to the calling user.

- Enable: When acting as the terminating side, sends the name of the user who has answered the call in a FACILITY IE within the CONNECT message or the name of the alerted user within the ALERTING or PROGRESS message. The called name and connected name will be set from the P-Asserted-Identity SIP header value. If the name of the user is not available, the NameNotAvailable value is sent in the FACILITY IE. When acting as the originating side, sets the value used to build the P-Asserted-Identity SIP header from the name of the user who has

answered the call in the received FACILITY IE within the CONNECT message or the name of the alerted user received from the ALERTING or PROGRESS message.

- Disable: No answered or alerted user name information is provided.

When acting as the originating side, the user name will be provided to the requesting network even if the presentation indicator in the name presentation argument of the CONP service is set to restricted.

CONP is only available for QSIG and NI-2 protocols.

OutgoingNotifyEnable (Config Parameter) | Table: SignalingChannel

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Isdn.SignalingChannel[].OutgoingNotifyEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.600

Defines if NOTIFY messages can be sent.

- Enable: NOTIFY messages can be sent.
- Disable: NOTIFY messages are never sent.

The following NOTIFY messages are supported:

- REMOTE HOLD: Sent when the remote peer holds the call.
- REMOTE RETRIEVAL: Sent when the remote peer retrieves the call.

AcceptedProgressCauses (Config Parameter) | Table: SignalingChannel

Type	Text
Range	Size(0..255)
Default	1-127
Script/CLI	Isdn.SignalingChannel[].AcceptedProgressCauses
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.700

Sets the range of PROGRESS causes accepted by the unit. Causes excluded from this range trigger call disconnections.
The string has the following syntax:

- ',': Separator between non-consecutive lists of causes or single cause.

- 'n': A single cause, where n is the cause number.
- 'm-n': List of causes where m is the start cause number and n is the end cause number.

NOTE: The space character are ignored and cause duplication is not allowed. Causes must be specified in low to high order.

Example: '1,124-127': The accepted causes are 1, 124, 125, 126 and 127.

AutoCancelTimeout (Config Parameter) | Table: SignalingChannel

Type	UInt32
Range	0..180
Default	0
Script/CLI	Isdn.SignalingChannel[].AutoCancelTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.800

Time, in seconds, the endpoint rings before the call is automatically cancelled.
Setting this parameter to 0 disables the timeout. Calls will not be automatically cancelled.

DateTimeIeSupport (Config Parameter) | Table: SignalingChannel

Type	Enum
Range	None(100) | LocalTime(200) | Utc(300)
Default	None
Script/CLI	Isdn.SignalingChannel[].DateTimeIeSupport
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.900

Defines if the optional Date/Time Information Element (IE) can be sent into the CONNECT and SETUP messages issued over BRI and PRI.

- None: Date/Time IE is not sent.
- LocalTime: Date/Time IE is sent, containing the local time according to the configured time zone in HOC.
- Utc: Date/Time IE is sent, containing the Coordinated Universal Time (UTC).

Refer to the HOC service for time zones and time server configuration. Without an SNTP synchronized connection, Date/Time IE is not sent.

MaintenanceServiceCallTermination (Config Parameter) | Table: SignalingChannel

Type	Enum
Range	Graceful(100) | Abrupt(200)
Default	Graceful
Script/CLI	Isdn.SignalingChannel[].MaintenanceServiceCallTermination
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.10000

Describes the call termination strategy after reception of a service message requesting a maintenance on the associated bearer channel.

- Graceful: The call proceeds normally until the user clears the call. The associated bearer is then set to maintenance.
- Abrupt: The call is terminated immediately and set to maintenance.

LinkEstablishment (Config Parameter) | Table: SignalingChannel

Type	Enum
Range	OnDemand(100) | Permanent(200)
Default	OnDemand
Script/CLI	Isdn.SignalingChannel[].LinkEstablishment
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.10100

Sets the link establishment strategy.

- OnDemand: When the data link is shut down, the unit establishes a new link only when required.
- Permanent: When the data link is shut down, the unit attempts to establish a new link.

LinkEstablishmentTimer (Config Parameter) | Table: SignalingChannel

Type	UInt32
Range	0..30000
Default	100
Script/CLI	Isdn.SignalingChannel[].LinkEstablishmentTimer
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.10110

Sets the link establishment timer.
This parameter has no effect if the **LinkEstablishment** parameter is set to 'OnDemand'.

AcceptedStatusCauses (Config Parameter) | Table: SignalingChannel

Type	Text
Range	Size(0..255)
Default	
Script/CLI	Isdn.SignalingChannel[].AcceptedStatusCauses
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.10200

Sets the STATUS causes that can be received without automatically clearing the call.
The default action is to clear the call upon the receipt of a STATUS message. If a STATUS message is received indicating a compatible call state and containing the supplied STATUS causes, the clearing of the call is prevented

The string has the following syntax:

- ',': Separator between non-consecutive lists of causes or single cause.
- 'n': A single cause, where n is the cause number.
- 'm-n': List of causes where m is the start cause number and n is the end cause number.

NOTE: The space character are ignored and cause duplication is not allowed. Causes must be specified in low to high order.

Example: '1,124-127': The accepted causes are 1, 124, 125, 126 and 127.

SendIsdnProgress (Config Parameter) | Table: SignalingChannel

Type	Enum
Range	SendAll(100) | SendInband(200) | SendAlerting(300)
Default	SendAll
Script/CLI	Isdn.SignalingChannel[].SendIsdnProgress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.10300

Sets the strategy for sending ISDN Progress messages.

- SendAll: Send an ISDN Progress message in all situations where call progression is signaled.
- SendInband: Send an ISDN Progress message only when call progression contains an indication of in-band information.
- SendAlerting: Send an ISDN Alerting message only when call progression contains an indication of in-band information.

The strategy for sending Progress messages should be adapted to the configuration of the peer ISDN switch. Some switches may terminate calls when receiving one or many ISDN progress messages.

SendProgressIndicatorIE (Config Parameter) | Table: SignalingChannel

Type	Enum
Range	SendAll(100) | SendInbandOnly(200)
Default	SendAll
Script/CLI	Isdn.SignalingChannel[].SendProgressIndicatorIE
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.10400

Sets the strategy for sending the Progress Indicator Information Element.

- SendAll: Send the Progress Indicator IE in all situations.
- SendInbandOnly: Send the Progress Indicator only when the Progress Description contains an indication of in-band information.

The strategy for the Progress Indicator IE should be adapted to the configuration of the peer ISDN switch.

This parameter controls sending of a Progress Indicator IE in ISDN messages where Progress Indicators are allowed. See the parameters in the **BasicRateInterfaceInterop** and **PrimaryRateInterfaceInterop** tables for a control over which ISDN messages allow Progress Indicators.

AocESupport (Config Parameter) | Table: SignalingChannel

Type	Enum
Range	No(100) | Transparent(200) | Automatic(300) | Explicit(400)
Default	No
Script/CLI	Isdn.SignalingChannel[].AocESupport
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.10600

Send the total charge at the (E)nd of the call in AOC-E messages.

- no: The AOC-E support is disabled. No information is forwarded to the peer interface.
- transparent: On an NT interface, the information is sent as received from the network. No information is sent if the network does not provide information. On a TE interface, the information is forwarded to the peer interface if AOC messages are received from the network.
- automatic: On an NT interface, always send the information. If the network does not provide information, 'noChargeAvailable' is sent. On a TE interface, the information is forwarded to the peer interface if AOC messages are received from the network.
- explicit: On an NT interface, always send the information if the phone requests AOC on a per-call basis. 'noChargeAvailable' is sent if the network does not provide information. If the phone does not request AOC on a per-call basis, no information is sent. On a TE interface, send an AOC request to the network. If the network rejects the request, no information is forwarded to the peer interface. Otherwise, the information is forwarded to the peer interface if AOC messages are received from the network.

AocDSupport (Config Parameter) | Table: SignalingChannel

Type	Enum
Range	No(100) | Transparent(200) | Automatic(300) | Explicit(400)
Default	No
Script/CLI	Isdn.SignalingChannel[].AocDSupport
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.10620

Send the current charge (D)uring the call in AOC-D messages.

- no: The AOC-D support is disabled. No information is forwarded to the peer interface.
- transparent: On an NT interface, the information is sent as received from the network. No information is sent if the network does not provide information. On a TE interface, the information is forwarded to the peer interface if AOC messages are received from the network.

- automatic: On an NT interface, always send the information. If the network does not provide information, 'noChargeAvailable' is sent. On a TE interface, the information is forwarded to the peer interface if AOC messages are received from the network.
- explicit: On an NT interface, always send the information if the phone requests AOC on a per-call basis. 'noChargeAvailable' is sent if the network does not provide information. If the phone does not request AOC on a per-call basis, no information is sent. On a TE interface, send an AOC request to the network. If the network rejects the request, no information is forwarded to the peer interface. Otherwise, the information is forwarded to the peer interface if AOC messages are received from the network.

CallReroutingBehavior (Config Parameter) | Table: SignalingChannel

Type	Enum
Range	Unsupported(100) | RelayReroute(200) | ProcessLocally(300)
Default	Unsupported
Script/CLI	Isdn.SignalingChannel[].CallReroutingBehavior
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.10700

Defines how the call rerouting request received from the private network side is supported. Rerouting requests are received in a Facility IE.

- Unsupported: Rerouting requests received are rejected. A reject answer is sent to the private network.
- RelayReroute: Rerouting requests are relayed as received to the public network side. If the peer rejects or does not support the reroute request, the ISDN service may initiate a new call to process the rerouting request locally.
- ProcessLocally: Received Rerouting requests are not relayed to the public network side. The ISDN service attempts to connect to the rerouted address by initiating a new call.

DefaultCallingTon (Config Parameter) | Table: SignalingChannel

Type	Enum
Range	Unknown(100) | International(200) | National(300) | NetworkSpecific(400) | Subscriber(500) | Abbreviated(600)
Default	Unknown
Script/CLI	Isdn.SignalingChannel[].DefaultCallingTon
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.10800

Default value to insert in the "Type of Number" parameter of the "Calling Party Number" IE when "Type of Number" is not already defined in the call properties. A call property set by the "Properties

Manipulation" feature of the Call Router has precedence over this default value. This parameter applies to the outgoing ISDN calls.
Possible values are:

- Unknown: Default value of Type of Number is set to Unknown.
- International: Default value of Type of Number is set to International.
- National: Default value of Type of Number is set to National.
- NetworkSpecific: Default value of Type of Number is set to Network-Specific.
- Subscriber: Default value of Type of Number is set to Subscriber.
- Abbreviated: Default value of Type of Number is set to Abbreviated.

DefaultCallingNpi (Config Parameter) | Table: SignalingChannel

Type	Enum
Range	Unknown(100) | IsdnTelephony(200) | Data(300) | Telex(400) | NationalStandard(500) | Private(600)
Default	Unknown
Script/CLI	Isdn.SignalingChannel[].DefaultCallingNpi
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.10900

Default value to insert in the "Numbering Plan Identification" parameter of the "Calling Party Number" IE when "Numbering Plan Identification" is not already defined in the call properties. A call property set by the "Properties Manipulation" feature of the Call Router has precedence over this default value. This parameter applies to the outgoing ISDN calls.
Possible values are:

- Unknown: Default value of Numbering Plan Identification is set to Unknown.
- IsdnTelephony: Default value of Numbering Plan Identification is set to ISDN Telephony.
- Data: Default value of Numbering Plan Identification is set to Data.
- Telex: Default value of Numbering Plan Identification is set to Telex.
- NationalStandard: Default value of Numbering Plan Identification is set to National Standard.
- Private: Default value of Numbering Plan Identification is set to Private.

DefaultCallingPi (Config Parameter) | Table: SignalingChannel

Type	Enum
Range	PresentationAllowed(100) | PresentationRestricted(200) | NotAvailable(300)
Default	PresentationAllowed
Script/CLI	Isdn.SignalingChannel[].DefaultCallingPi
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.11000

Default value to insert in the "Presentation Indicator" parameter of the "Calling Party Number" IE when "Presentation Indicator" is not already defined in the call properties. A call property set by the "Properties Manipulation" feature of the Call Router has precedence over this default value. If "Presentation Indicator" is not provided by the call properties, its value is determined by the following two steps. First, it is set to the default value defined by "DefaultCallingPi". Second, the "Presentation Indicator" can be overridden by the CLIP and CLIR services: the value can be set to "Restricted" by the CLIR service and the value can be set to "NotAvailable" if there is no number to forward. This parameter applies to the outgoing ISDN calls.
Possible values are:

- PresentationAllowed: Default value of Presentation Indicator is set to Presentation Allowed.
- PresentationRestricted: Default value of Presentation Indicator is set to Presentation Restricted.
- NotAvailable: Default value of Presentation Indicator is set to Not Available.

DefaultCallingSi (Config Parameter) | Table: SignalingChannel

Type	Enum
Range	UserProvidedNotScreened(100) | UserProvidedVerifiedAndPassed(200) | UserProvidedVerifiedAndFailed(300) | NetworkProvided(400) | ContextDependent(500)
Default	ContextDependent
Script/CLI	Isdn.SignalingChannel[].DefaultCallingSi
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.11100

Default value to insert in the "Screening Indicator" parameter of the "Calling Party Number" IE when "Screening Indicator" is not already defined in the call properties. A call property set by the "Properties Manipulation" feature of the Call Router has precedence over this default value. This parameter applies to the outgoing ISDN calls.
Possible values are:

- UserProvidedNotScreened: Default value of Screening Indicator is set to User Provided Not Screened.
- UserProvidedVerifiedAndPassed: Default value of Screening Indicator is set to User Provided Verified And Passed.
- UserProvidedVerifiedAndFailed: Default value of Screening Indicator is set to User Provided Verified And Failed.
- NetworkProvided: Default value of Screening Indicator is set to Network Provided.
- ContextDependent: Screening Indicator is set to the value that makes the most sense according to run-time context.

DefaultCalledTon (Config Parameter) | Table: SignalingChannel

Type	Enum
Range	Unknown(100) | International(200) | National(300) | NetworkSpecific(400) | Subscriber(500) | Abbreviated(600)
Default	Unknown
Script/CLI	Isdn.SignalingChannel[].DefaultCalledTon
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.11200

Default value to insert in the "Type of Number" parameter of the "Called Party Number" IE when "Type of Number" is not already defined in the call properties. A call property set by the "Properties Manipulation" feature of the Call Router has precedence over this default value. This parameter applies to the outgoing ISDN calls.
Possible values are:

- Unknown: Default value of Type of Number is set to Unknown.
- International: Default value of Type of Number is set to International.
- National: Default value of Type of Number is set to National.
- NetworkSpecific: Default value of Type of Number is set to Network-Specific.
- Subscriber: Default value of Type of Number is set to Subscriber.
- Abbreviated: Default value of Type of Number is set to Abbreviated.

DefaultCalledNpi (Config Parameter) | Table: SignalingChannel

Type	Enum
Range	Unknown(100) | IsdnTelephony(200) | Data(300) | Telex(400) | NationalStandard(500) | Private(600)
Default	Unknown
Script/CLI	Isdn.SignalingChannel[].DefaultCalledNpi
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.11300

Default value to insert in the "Numbering Plan Identification" parameter of the "Called Party Number" IE when "Numbering Plan Identification" is not already defined in the call properties. A call property set by the "Properties Manipulation" feature of the Call Router has precedence over this default value. This parameter applies to the outgoing ISDN calls.
Possible values are:

- Unknown: Default value of Numbering Plan Identification is set to Unknown.
- IsdnTelephony: Default value of Numbering Plan Identification is set to ISDN Telephony.
- Data: Default value of Numbering Plan Identification is set to Data.
- Telex: Default value of Numbering Plan Identification is set to Telex.
- NationalStandard: Default value of Numbering Plan Identification is set to National Standard.
- Private: Default value of Numbering Plan Identification is set to Private.

UserSuspendedHandling (Config Parameter) | Table: SignalingChannel

Type	Enum
Range	Ignore(100) | Disconnect(200)
Default	Ignore
Script/CLI	Isdn.SignalingChannel[].UserSuspendedHandling
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.11400

Defines the unit's behaviour when it receives a Notification Indicator IE with the description set to User suspended.
Possible values are:

- Ignore: Ignore the Notification Indicator IE with description set to User suspended.
- Disconnect: Disconnect the call on Notification Indicator IE with description set to User suspended.

StrictHandlingErrorConditions (Config Parameter) | Table: SignalingChannel

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Isdn.SignalingChannel[].StrictHandlingErrorConditions
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.11500

When activated, validation of Information Elements is applied to every received messages.

Detailed error handling procedures are protocol dependent and may vary from network-to-network. The handling of error conditions follows procedures described in ITU-T Q.931 subclause 5.8.

McidEnable (Config Parameter) | Table: SignalingChannel

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Isdn.SignalingChannel[].McidEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.100.1.11600

Defines if the Malicious Call Identification (MCID) request sent from the user or network side is supported. Malicious Call Identification (MCID) requests are sent in a Facility IE.

On the reception of a SIP INFO message containing the "P-Call-Info: malicious" proprietary header, the associated call will send an ISDN FACILITY message indicating that this call is tagged as malicious.

This parameter only applies to the DSS1 signaling protocol.

- Enable: MCID requests are sent.
- Disable: MCID requests are never sent.

SignalingChannelInfo (Table)

ISDN signaling table containing configuration and operational parameters for all ISDN signaling channels on this managed device.

InterfaceName (Index) | Table: SignalingChannelInfo

Type	Text
Range	
Script/CLI	Isdn.SignalingChannelInfo[].InterfaceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.200.1.100

Identifies the interface.

State (Status Parameter) | Table: SignalingChannelInfo

Type	Enum
Range	Up(100) | Down(200)
Script/CLI	Isdn.SignalingChannelInfo[].State
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.200.1.200

The current call control state for this channel:

- Up:
- Down:

SignalingChannelInterop (Table)

Interop configuration parameters related to the Signaling Channel on this managed device.

InterfaceName (Index) | Table: SignalingChannelInterop

Type	Text
Range	
Script/CLI	Isdn.SignalingChannelInterop[].InterfaceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.50000.100.1.100

Name that identifies the interface.

CallProceedingDelay (Config Parameter) | Table: SignalingChannelInterop

Type	UInt32
Range	0..4000
Default	0
Script/CLI	Isdn.SignalingChannelInterop[].CallProceedingDelay
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.50000.100.1.200

Defines the maximum time to wait after receiving a SETUP message before sending a CALL PROCEEDING message and going on with normal call processing.
After receiving a SETUP message, the system waits for a message from the called party. If the message maps to a User Busy cause, a DISCONNECT message is sent instead of the CALL PROCEEDING otherwise it goes on with normal call processing.

The value 0 deactivates this feature.

This value is expressed in milliseconds (ms).

CallingNameDelivery (Config Parameter) | Table: SignalingChannelInterop

Type	Enum
Range	FacilityIe(100) | DisplayIe(200) | UserUserIe(300) | SignalingProtocol(400)
Default	SignalingProtocol
Script/CLI	Isdn.SignalingChannelInterop[].CallingNameDelivery
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.50000.100.1.300

Defines how the Calling Name is delivered.

- FacilityIe: Use a Facility Information Element for delivering the Calling Name.
- DisplayIe: Use a Display Information Element for delivering the Calling Name.
- UserUserIe: Use a User-User Information Element for delivering the Calling Name.
- SignalingProtocol: Use the delivery method defined by the signaling protocol.

CallingNameHandling (Config Parameter) | Table: SignalingChannelInterop

Type	Enum
Range	SignalingProtocol(100) | IgnoreUserUserIe(200)
Default	SignalingProtocol
Script/CLI	Isdn.SignalingChannelInterop[].CallingNameHandling
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.50000.100.1.350

Defines how to handle the received ISDN Calling Name.

- SignalingProtocol: Use the signaling protocol method.
- IgnoreUserUserIe: Use the signaling protocol method, excepting the User-User IE.

InteropPlayLocalRingbackWhenNoMediaStream (Config Parameter) | Table: SignalingChannelInterop

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Isdn.SignalingChannelInterop[].InteropPlayLocalRingbackWhenNoMediaStream
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.50000.100.1.500

Forces local ringback generation when early-media is enabled but no media stream has been received yet.

- Enable: The local ringback is played after sending an ALERTING and no media stream has been received yet from the outgoing interface.
- Disable: Do not play local ringback when doing early-media.

Note that this parameter only applies to 180 SIP responses when early-media is enabled.

Note that this parameter only affects incoming call on the ISDN interface.

InteropConsecutiveChannelIndicator (Config Parameter) | Table: SignalingChannelInterop

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Isdn.SignalingChannelInterop[].InteropConsecutiveChannelIndicator
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.50000.100.1.600

To choose which numbering is used in the channel indicator.

- Enable: Channel indicator use logical numbering (1-30).
- Disable: Channel indicator use physical time slot number as defined in ISDN (1-15, 17-31).

Note that when enabling this parameter, the ISDN standard is no longer followed. This parameter applies only for a PRI interface in E1.

InteropAddReleaseSecondCauseOnExpiry (Config Parameter) | Table: SignalingChannelInterop

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.SignalingChannelInterop[].InteropAddReleaseSecondCauseOnExpiry
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.50000.100.1.700

Specifies if an optional second cause information element with No. 102 cause (recovery on timer expiry) should be sent in the Release message with the original Disconnect cause number.

- Enable: The unit will send a RELEASE message with the cause number originally contained in the DISCONNECT message and indicate a second Cause information element with No. 102 cause (recovery on timer expiry).
- Disable: The No. 102 cause (recovery on timer expiry) is not sent with the original Disconnect cause.

This parameter only applies to timers T305, T306, and T308, for endpoint type TE or NT.

Some implementations compliant to TBR-3 require this parameter to be disabled.

InteropQsigIeInterpretation (Config Parameter) | Table: SignalingChannelInterop

Type	Enum
Range	Ecma143(100) | Itutq931(200)
Default	Ecma143
Script/CLI	Isdn.SignalingChannelInterop[].InteropQsigIeInterpretation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.500.50000.100.1.800

Specifies the standard to apply while interpreting the Information Elements (IE) under QSIG signaling protocol.

- Ecma143: The IE is interpreted following the ECMA-143 standard (QSIG)
- Itutq931: The IE is interpreted following the ITU-T Q.931 standard (ISDN)

The Channel Identification IE is affected by this parameter following the selected standard:

- Ecma143: the bits [7:6] of the octet 3 are hardcoded, the interface is always explicitly identified and the channels are numbered from 1 upwards
- Itutq931: the interface is identified following the defined interface type (BRI or PRI) and the channel number equals the timeslot number

This parameter only applies to QSIG signalling on BRI interface.

PhysicalLinkInfo (Table)

The ISDN physical link information table contains status information for all ISDN interfaces on this managed device.

InterfaceName (Index) | Table: PhysicalLinkInfo

Type	Text
Range	
Script/CLI	Isdn.PhysicalLinkInfo[].InterfaceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.600.100.1.100

Identifies the interface.

State (Status Parameter) | Table: PhysicalLinkInfo

Type	Enum
Range	Up(100) | Down(200)
Script/CLI	Isdn.PhysicalLinkInfo[].State
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.600.100.1.200

The layer 1 state for this interface:

- Up: Layer 1 connectivity.
- Down: No layer 1 connectivity. The interface might be in this state because no cable is plugged in or a pinout problem is detected.

PhysicalLink (Table)

The ISDN physical link table containing configuration and operational parameters for all ISDN interfaces on this managed device.

InterfaceName (Index) | Table: PhysicalLink

Type	Text
Range	
Script/CLI	Isdn.PhysicalLink[].InterfaceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.600.200.1.100

Identifies the interface.

L1TimerT3 (Config Parameter) | Table: PhysicalLink

Type	UInt32
Range	0..30000
Default	3000
Script/CLI	Isdn.PhysicalLink[].L1TimerT3
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.600.200.1.200

Timer 3 (T3) is a supervisory timer that has to take into account the overall time to activate. This time includes the time it takes to activate both the TE-NT and the NT-TE portion of the customer access. The expiry of Timer T3 is intended to provide an indication that the network side cannot complete the activation procedure, probably due to a failure condition or the terminal cannot detect INFO 4.

This value is expressed in milliseconds (ms).

ClockMode (Config Parameter) | Table: PhysicalLink

Type	Enum
Range	Auto(100) | Master(200) | Slave(300)
Default	Auto
Script/CLI	Isdn.PhysicalLink[].ClockMode
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.600.200.1.300

An ISDN port can either generate the clocking for the line or accept the clock from the line. The options master or slave determine the clocking method:

- Auto: Derived from the endpoint type (NT: clock master, TE: clock slave)
- Master: Generates clock
- Slave: Accepts clock

Note: For BRI interfaces with the endpoint type configured in TE the clock mode is always slave (even if configuration is set to master).

MonitorLinkStateEnable (Config Parameter) | Table: PhysicalLink

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Isdn.PhysicalLink[].MonitorLinkStateEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.600.200.1.400

Monitors the physical link state of an ISDN interface.
Enable: An ISDN endpoint's operational state is affected by its interface physical link state. When the link state of an ISDN interface is down, the operational state of its matching endpoint becomes "disable".

Disable: An ISDN endpoint's operational state is not affected by its interface physical link state.

AutoConfigureStatus (Status Parameter)

Type	Enum
Range	Idle(100) | Sensing(200)
Script/CLI	Isdn.AutoConfigureStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.700.100

Indicates the current status of the ISDN automatic configuration mechanism.

- Idle: The automatic configuration mechanism is ready to be started.
- Sensing: The automatic configuration mechanism is currently started and is testing different ISDN configurations to obtain a link up.

LastAutoConfigureResult (Status Parameter)

Type	Enum
Range	None(100) | Success(200) | Fail(300) | Aborted(400)
Script/CLI	Isdn.LastAutoConfigureResult
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.700.200

Result of the last ISDN automatic configuration.

- None: No result is available.
- Success: The last automatic configuration succeeded.
- Fail: The last automatic configuration failed.
- Aborted: The last automatic configuration has been cancelled by the user.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Isdn.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Isdn.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1850.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

AutoConfigure (Command)

Auto-detect and auto-configure the ISDN interfaces.

Interface (Argument) | Command: AutoConfigure

Type	Text
Range	Size(0..48)
Default	

The specific ISDN Interface on which the AutoConfigure command will be executed. See the **Isdn.PhysicalLinkInfo** table for the exact interface name to use. Take note that the argument value is case-sensitive.

This argument is optional. If no value is provided, the command will be executed on all ISDN interfaces.

CancelAutoConfigure (Command)

Stops and cancels the automatic detection and configuration mechanism.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Isdn service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.1850.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
5	%1$s: Physical link state changed to up.	Info	The physical link state has changed to up.
10	%1$s: Signaling channel state changed to up.	Info	The signaling channel state has changed to up.
15	%1$s: Physical link state changed to down.	Info	The physical link state has changed to down.
20	%1$s: Signaling channel state changed to down.	Info	The signaling channel state has changed to down.
30	%1$s, B-channel %2$d: State changed to free.	Info	The B-channel state has changed to free.
40	%1$s, B-channel %2$d: State changed to used.	Info	The B-channel state has changed to used.
50	%1$s: Graceful lock initiated.	Info	A graceful lock has been initiated.
60	%1$s: Abrupt lock initiated.	Info	An abrupt lock has been initiated.
70	%1$s: Locked successfully.	Info	Locked successfully.
80	%1$s, Unlocked successfully.	Info	Unlocked successfully.
90	%1$s: Cannot allocate B-channel, line is locked.	Warning	The unit cannot allocate a B-channel because the line is locked.
95	%1$s: The unit cannot allocate a DSP channel to process the call: all DSP resources are currently in use.	Warning	The unit rejected the call: the endpoint could not allocate a DSP channel to process the call.
100	%1$s: Cannot allocate B-channel, maximum number of calls (%2$d) reached.	Warning	The unit cannot allocate a B-channel because the maximum number of calls has been reached.
105	%1$s: Cannot allocate B-channel, no more bearer available.	Error	The unit cannot allocate a B-channel because no more bearer are available, due to high demand.
107	%1$s: Cannot allocate B-channel %2$s on this interface. B-Channel does not exist.	Error	The unit cannot allocate a specific B-channel because it does not exist on the interface.

NumKey	Message	Severity	Description
110	%1$s, Timer %2$s expired once, retransmitting %3$s.	Warning	The timer has expired once, the unit is retransmitting.
120	%1$s, B-channel %2$d: Timer %3$s expired once, retransmitting %4$s.	Warning	The timer has expired once, the unit is retransmitting.
130	%1$s, B-channel %2$d: Timer %3$s expired once, releasing call.	Error	The timer has expired once, the unit is releasing the call.
140	%1$s, B-channel %2$d: Timer %3$s expired twice.	Error	The timer has expired twice.
150	%1$s, B-channel %2$d: Timer %3$s expired twice, releasing call.	Error	The timer has expired twice, the unit is releasing the call.
155	%1$s, B-channel %2$d: Automatically cancelling call on no answer.	Info	The unit is cancelling the call because it was not answered within the auto cancel timeout period.
160	%1$s, B-channel %2$d: Rejecting incoming call because received SETUP message is missing expected bearer capability information element.	Warning	The unit is rejecting the incoming call because the received SETUP message is missing an expected bearer capability information element.
170	%1$s, B-channel %2$d: Rejecting incoming call because received SETUP message contains bearer capabilities that are not implemented.	Warning	The unit is rejecting the incoming call because the received SETUP message contains bearer capabilities that are not implemented.
180	%1$s, B-channel %2$d: Rejecting incoming call because received SETUP message contains incompatible bearer capabilities at the destination.	Warning	The unis is rejecting the incoming call because the received SETUP message contains incompatible bearer capabilities at the destination.
185	%1$s: ISDN frame slip detected.	Warning	This message is issued when the physical link detects a frame slip. This happens when there is a problem with clock synchronization.

NumKey	Message	Severity	Description
190	%1$s, B-channel %2$d: No called number received from SIP for called user, using none.	Warning	No called number has been received from SIP for the called user, using none.
200	%1$s, B-channel %2$d: Received number (%3$s) does not match any existing DTMF map.	Warning	The received number does not match any existing DTMF map.
210	%1$s, B-channel %2$d: Received invalid IA5 digits (%3$s) in calling party number.	Warning	Received invalid IA5 digits in the calling party number.
220	%1$s, B-channel %2$d: Releasing call following Q.931 RESTART.	Warning	Releasing the call following Q.931 RESTART.
230	%1$s, B-channel %2$d: Releasing call following D-channel down.	Warning	Releasing the call following D-channel down.
240	%1$s, B-channel %2$d: Call destroyed.	Warning	The call has been destroyed.
250	%1$s, B-channel %2$d: Received DISCONNECT message without cause.	Error	Received a DISCONNECT message without cause.
300	%1$s: Ignoring received Q.931 RESTART message with badly coded channel identification information element (no interface ID nor B-channel ID specified).	Error	Ignoring a received Q.931 RESTART message with badly coded channel identification information element (no interface ID nor B-channel ID has been specified).
305	%1$s, Invalid clock mode detected according to the endpoint type.	Warning	A clock mode can be invalid for a specific endpoint type. See the **PhysicalLink.ClockMode** parameter for more information.
310	%1$s: Received unhandled ISDN message %2$s.	Warning	Received an unhandled ISDN message.
320	%1$s: ISDN HOLD request was rejected because the Hold Service is disabled.	Info	An ISDN HOLD message was received but the Hold Telephony Service is disabled. The HOLD request has been rejected.

NumKey	Message	Severity	Description
330	%1$s: ISDN HOLD request was rejected.	Error	An ISDN HOLD message was received but it has been refused by the remote peer. The HOLD request has been rejected.
340	%1$s: ISDN RETRIEVE request was rejected because no B-channel is available.	Error	An ISDN RETRIEVE message was received but no B-channel is available. The RETRIEVE request has been rejected.
350	%1$s: ISDN HOLD request was rejected because a transfer is currently in progress.	Error	An ISDN HOLD message was received but the call is currently being transferred. The HOLD request has been rejected.
360	The ISDN auto-configuration process has started.	Info	An auto-configuration process has started on ISDN interfaces.
370	The ISDN auto-configuration process has been cancelled.	Info	The ISDN auto-configuration process has been cancelled by the user.
380	The ISDN auto-configuration process has completed successfully.	Info	The ISDN auto-configuration process has completed successfully. NOTE: This does not mean that the auto-configuration process has succeeded on all interfaces.
390	The ISDN auto-configuration process has failed.	Error	The ISDN auto-configuration process has terminated because of an error.
400	%1$s: Auto-configuration has succeeded.	Info	The auto-configuration process has succeeded on the specified ISDN interface.
410	%1$s: Auto-configuration has failed.	Error	The auto-configuration process has failed on the specified ISDN interface.
500	Usage of deprecated ISDN Msn parameters on %1$s is not recommended.	Warning	Usage of the deprecated **Isdn.BasicRateInterface.Msn2** and **Isdn.BasicRateInterface.Msn3** parameters is not recommended. It is recommended to use the **Isdn.BasicRateInterface.Msn** parameter instead.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.

NumKey	Message	Severity	Description
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.

NumKey	Message	Severity	Description
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Isdn.

Message	Severity	Description
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.

Message	Severity	Description
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Local Firewall (Lfw)

The Local Firewall (LFW) service allows the administrator to filter the network with the unit as final destination.

Parameters

ConfigModifiedStatus (Status Parameter)

Type	Enum
Range	Yes(100) | No(200)
Script/CLI	Lfw.ConfigModifiedStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.100

Shows whether or not the Local Firewall configuration has been modified without being applied.

1. Yes: The configuration has been modified but it has not been applied.
2. No: The Local Firewall service uses the configured rules.

Use the `Lfw.ApplyConfig` command to apply the configuration.

LocalRulesStatus (Table)

This table shows the local rules applied in the firewall.

Priority (Index) | Table: LocalRulesStatus

Type	UInt32
Range	
Script/CLI	Lfw.LocalRulesStatus[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.200.1.100

Unique identifier of the row in the table.

SourceAddress (Status Parameter) | Table: LocalRulesStatus

Type	Text
Range	
Script/CLI	Lfw.LocalRulesStatus[].SourceAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.200.1.200

Source address[/mask] criteria an incoming packet must have to match this rule.
An empty string matches any address.

SourcePort (Status Parameter) | Table: LocalRulesStatus

Type	Text
Range	
Script/CLI	Lfw.LocalRulesStatus[].SourcePort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.200.1.300

Source port[-port] criteria an incoming packet must have to match this rule.
MinPort-MaxPort specifies a port range.

An empty string means that no filtering is applied on the source port thus matching any port.

This parameter is only effective when the **LocalRulesStatus.Protocol** parameter is set to Tcp or Udp.

DestinationAddress (Status Parameter) | Table: LocalRulesStatus

Type	Text
Range	
Script/CLI	Lfw.LocalRulesStatus[].DestinationAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.200.1.400

Destination address[/mask] criteria an incoming packet must have to match this rule.
An empty string matches any address.

DestinationPort (Status Parameter) | Table: LocalRulesStatus

Type	Text
Range	
Script/CLI	Lfw.LocalRulesStatus[].DestinationPort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.200.1.500

Destination port[-port] criteria an incoming packet must have to match this rule.
MinPort-MaxPort specifies a port range.

An empty string means that no filtering is applied on the destination port thus matching any port.

This parameter is only effective when the **LocalRulesStatus.Protocol** parameter is set to Tcp or Udp.

Protocol (Status Parameter) | Table: LocalRulesStatus

Type	Enum
Range	All(100) | Tcp(200) | Udp(300) | Icmp(400)
Script/CLI	Lfw.LocalRulesStatus[].Protocol
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.200.1.600

Protocol criteria an incoming packet must have to match this rule.
The protocol can be one of the following:

- All: Match packets using any protocols.
- Tcp: Only match TCP packets.
- Udp: Only match UDP packets.

- Icmp: Only match ICMP packets.

BlacklistEnable (Status Parameter) | Table: LocalRulesStatus

Type	EnableDisable
Range	
Script/CLI	Lfw.LocalRulesStatus[].BlacklistEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.200.1.620

Indicates if blacklisting is enabled for this rule.

- Enable: When a packet establishing a connection matches this rule, the action is executed and the source IP address is added to the blacklist.
- Disable: When a packet establishing a connection matches this rule, the action is executed but the source IP address is not added to the blacklist.

Note: If rate limiting is enabled for this rule, blacklisted IP addresses are added to the rate limit blacklist.

RateLimitValue (Status Parameter) | Table: LocalRulesStatus

Type	UInt32
Range	1..5000
Script/CLI	Lfw.LocalRulesStatus[].RateLimitValue
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.200.1.650

Number of new connections allowed to match this rule from a single source IP address within a certain time period.

RateLimitTimePeriod (Status Parameter) | Table: LocalRulesStatus

Type	UInt32
Range	1..86400
Script/CLI	Lfw.LocalRulesStatus[].RateLimitTimePeriod
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.200.1.680

The time period on which to base the rate limit. This period is expressed in seconds.
Ex.: a **RateLimitValue** of 10 and a **RateLimitTimePeriod** of 60 means a limit of 10 new connections per minute.

Action (Status Parameter) | Table: LocalRulesStatus

Type	Enum
Range	Accept(100) | Reject(200) | Drop(300) | RateLimitPerSource(400)
Script/CLI	Lfw.LocalRulesStatus[].Action
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.200.1.700

Action taken when this rule matches a packet.
Action can be one of the following:

- Accept: Let the packet through.
- Reject: Send back an ICMP port unreachable in response to the matched packet, the packet is then dropped.
- Drop: The packet is dropped without any notification.
- RateLimitPerSource: Drop the packets received from a given source IP address when it exceeds a configurable rate. The rate is set using the **RateLimitValue** and **RateLimitTimePeriod** parameters.
  Note: This action is only allowed when the **ConnectionState** parameter is set to 'New'.

DefaultPolicy (Config Parameter)

Type	Enum
Range	Accept(100) | Drop(300)
Default	Accept
Script/CLI	Lfw.DefaultPolicy
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.550

Action taken when a packet does not match any rule.
Default policy can be one of the following:

- Accept: Let the packet through.
- Drop: The packet is dropped without any notification.

Make sure that there are some rules with Action set to 'Accept' in the local firewall BEFORE applying changes that will set the default policy to 'Drop'. Failing to comply with this warning results in losing contact with the unit and a partial or factory reset is required.

To have no filtering applied to incoming packets, set the default policy to 'Accept' and remove all rules from the local firewall.

LocalRules (Table: user-defined, 20 lines max.)

This table shows the configured local rules for the firewall.

Priority (Index) | Table: LocalRules

Type	UInt32
Range	
Script/CLI	Lfw.LocalRules[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.600.1.100

Unique identifier of the row in the table.

Activation (Config Parameter) | Table: LocalRules

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Lfw.LocalRules[].Activation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.600.1.200

Current activation state for this rule.

- Enable: This rule is active in the firewall.
- Disable: This rule is not in the firewall.

SourceAddress (Config Parameter) | Table: LocalRules

Type	Text
Range	Size(0..51)
Default	
Script/CLI	Lfw.LocalRules[].SourceAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.600.1.300

Source address of the incoming packet using the following format: address[/mask] or network interface name/.

The address can either be a network IP address (using /mask) or one of the host IP addresses.

When specifying a network interface name, it is mandatory to use the suffix "/". Doing so indicates that the network address of this interface is used instead of the host address. Also, it must match one of the values in the **networkInterfacesStatusTable.InterfaceName** parameter from the Basic Network Interface (BNI) service. Note that if the specified network interface is disabled or removed, the rule is automatically disabled thus removed from the firewall. When the network interface is enabled or added back, the rule is automatically enabled and applied in the firewall.

Mask must be a plain number specifying the number of binary 1s at the left side of the network mask. E.g.: a mask of 24 specifies a network mask of 255.255.255.0.

Leaving the default empty string matches any address.

SourcePort (Config Parameter) | Table: LocalRules

Type	Text
Range	Size(0..11)
Default	
Script/CLI	Lfw.LocalRules[].SourcePort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.600.1.400

Source port of the incoming packet using the following format: port[-port].
MinPort-MaxPort specifies a port range.

The default empty string means that no filtering is applied on the source port thus matching any port.

This parameter is only effective when the **LocalRules.Protocol** parameter is set to Tcp or Udp.

DestinationAddress (Config Parameter) | Table: LocalRules

Type	Text
Range	Size(0..51)
Default	
Script/CLI	Lfw.LocalRules[].DestinationAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.600.1.500

Destination address of the incoming packet using the following format: address or network interface name.
The address must be one of the host IP addresses. Specifying a network address here is invalid since this is a local firewall.

When specifying a network interface name, the host address of this interface is used. Also, it must match one of the values in the **networkInterfacesStatusTable.InterfaceName** parameter from the Basic Network Interface (BNI) service. Note that if the specified network interface is disabled or removed, the rule is automatically disabled thus removed from the firewall. When the network interface is enabled or added back, the rule is automatically enabled and applied in the firewall.

Leaving the default empty string matches any address.

DestinationPort (Config Parameter) | Table: LocalRules

Type	Text
Range	Size(0..11)
Default	
Script/CLI	Lfw.LocalRules[].DestinationPort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.600.1.600

Destination port of the incoming packet using the following format: port[-port].
MinPort-MaxPort specifies a port range.

The default empty string means that no filtering is applied on the destination port thus matching any port.

This parameter is only effective when the **LocalRules.Protocol** parameter is set to Tcp or Udp.

Protocol (Config Parameter) | Table: LocalRules

Type	Enum
Range	All(100) | Tcp(200) | Udp(300) | Icmp(400)
Default	All
Script/CLI	Lfw.LocalRules[].Protocol
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.600.1.700

Protocol of the incoming packet.
The protocol can be one of the following:

- All: Match packets using any protocols.
- Tcp: Only match TCP packets.
- Udp: Only match UDP packets.
- Icmp: Only match ICMP packets.

BlacklistEnable (Config Parameter) | Table: LocalRules

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Lfw.LocalRules[].BlacklistEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.600.1.720

Indicates if blacklisting is enabled for this rule.

- Enable: When a packet establishing a connection matches this rule, the action is executed and the source IP address is added to the blacklist.
- Disable: When a packet establishing a connection matches this rule, the action is executed but the source IP address is not added to the blacklist.

Note: If rate limiting is enabled for this rule, blacklisted IP addresses are added to the rate limit blacklist.

RateLimitValue (Config Parameter) | Table: LocalRules

Type	UInt32
Range	1..5000
Default	10
Script/CLI	Lfw.LocalRules[].RateLimitValue
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.600.1.750

Number of new connections allowed to match this rule from a single source IP address within a certain time period.

RateLimitTimePeriod (Config Parameter) | Table: LocalRules

Type	UInt32
Range	1..86400
Default	60
Script/CLI	Lfw.LocalRules[].RateLimitTimePeriod
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.600.1.780

The time period on which to base the rate limit. This period is expressed in seconds.
Ex.: a **RateLimitValue** of 10 and a **RateLimitTimePeriod** of 60 means a limit of 10 new connections per minute.

Action (Config Parameter) | Table: LocalRules

Type	Enum
Range	Accept(100) | Reject(200) | Drop(300) | RateLimitPerSource(400)
Default	Accept
Script/CLI	Lfw.LocalRules[].Action
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.600.1.800

Action taken when this rule matches a packet.
Action can be one of the following:

- Accept: Let the packet through.
- Reject: Send back an ICMP port unreachable in response to the matched packet, the packet is then dropped.
- Drop: The packet is dropped without any notification.
- RateLimitPerSource: Drop the packets received from a given source IP address when it exceeds a configurable rate. The rate is set using the **RateLimitValue** and **RateLimitTimePeriod** parameters.
  Note: This action is only allowed when the **ConnectionState** parameter is set to 'New'.

Up (Row Command) | Table: LocalRules

Script/CLI:	Lfw.LocalRules[].Up
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.600.1.900

Moves the current row upwards.

Down (Row Command) | Table: LocalRules

Script/CLI:	Lfw.LocalRules[].Down
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.600.1.1000

Moves the current row downwards.

Insert (Row Command) | Table: LocalRules

Script/CLI:	Lfw.LocalRules[].Insert
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.600.1.1100

Inserts a new row before this row.

Delete (Row Command) | Table: LocalRules

Script/CLI:	Lfw.LocalRules[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.600.1.1200

Deletes this row.

BlacklistTimeout (Config Parameter)

Type	UInt32
Range	1..86400
Default	60
Script/CLI	Lfw.BlacklistTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.700.100

The time an address stays in the blacklist. If Lfw receives a packet from a blacklisted source, the packet is dropped and the remaining blacklist time is reset to this value.
The time units are seconds.

BlacklistRateLimitTimeout (Config Parameter)

Type	UInt32
Range	1..86400
Default	60
Script/CLI	Lfw.BlacklistRateLimitTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.700.200

The time an address stays in the 'rate limit' blacklist. If Lfw receives a packet from a 'rate limit' blacklisted source, the packet is dropped but the remaining blacklist time is not reset.
The time units are seconds.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Lfw.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Lfw.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2200.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

ApplyConfig (Command)

Applies the configured rules.

InsertRule (Command)

Inserts a new row at the end of the **LocalRules** table.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

RollbackConfig (Command)

Rolls back the current configuration to the running configuration as showed in the status.
The current configuration is lost.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Lfw service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.2200.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	Blacklisting is ignored in Rule with priority = %1$d.	Warning	Blacklisting is only allowed when the **NetworkRules** Action parameter is set to 'Drop' or 'RateLimitPerSource'. Otherwise the rule is still active but blacklisting is disabled.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.

NumKey	Message	Severity	Description
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Lfw.

Message	Severity	Description
At least one of the rules applied is ambiguous.	Warning	This message is sent when apply is called and at least one of the rule is ambiguous Ex.: Blacklisting is on and Action is accept.
Blacklist will be ignored because his use with the current action is ambiguous.	Warning	This message is sent when a set will put the rule in an ambiguous state.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.

Message	Severity	Description
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Link Layer Discovery Protocol (Lldp)

The Link Layer Discovery Protocol (LLDP) service is used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802.1AB local area network, usually wired Ethernet. LLDP cannot be activated on more than one network interface at a time.

Parameters

RemoteMediaPolicyState (Table)

This table holds the LLDP network policies received from the network interface on which LLPD was enabled.

AppType (Index) | Table: RemoteMediaPolicyState

Type	Enum
Range	Unknown(0) | Voice(1) | VoiceSignaling(2) | GuestVoice(3) | GuestVoiceSignaling(4) | SoftPhoneVoice(5) | VideoConferencing(6) | StreamingVideo(7) | VideoSignaling(8)
Script/CLI	Lldp.RemoteMediaPolicyState[].AppType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4100.1.100.100.1.100

The application type for which the LLPD network policies were received.
The supported application types are only:

- Voice
- VoiceSignaling

All other LLPD network policies received from other types of applications are ignored.

VlanId (Status Parameter) | Table: RemoteMediaPolicyState

Type	UInt32
Range	0..4094
Script/CLI	Lldp.RemoteMediaPolicyState[].VlanId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4100.1.100.100.1.200

The requested VLAN ID for the specified application type.

Priority (Status Parameter) | Table: RemoteMediaPolicyState

Type	UInt32
Range	0..7
Script/CLI	Lldp.RemoteMediaPolicyState[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4100.1.100.100.1.300

The requested 802.1Q User Priority for the specified application type.

Dscp (Status Parameter) | Table: RemoteMediaPolicyState

Type	UInt32
Range	0..255
Script/CLI	Lldp.RemoteMediaPolicyState[].Dscp
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4100.1.100.100.1.400

The requested DSCP (DiffServ) for the specified application type.

PolicyFlag (Status Parameter) | Table: RemoteMediaPolicyState

Type	Enum
Range	Defined(100) | Unknown(200)
Script/CLI	Lldp.RemoteMediaPolicyState[].PolicyFlag
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4100.1.100.100.1.500

The Policy Flag indicating if an Endpoint Device will explicitly advertise that the network policy for a specific application type is required but currently unknown.

- Defined: The network policy is defined.
- Unknown: The network policy for the specified application type is currently unknown. In this case, the values of the **Llpd.RemoteMediaPolicyState.VlanId** , **Llpd.RemoteMediaPolicyState.Priority**, and **Llpd.RemoteMediaPolicyState.Dscp** parameters are ignored.

TaggedFlag (Status Parameter) | Table: RemoteMediaPolicyState

Type	Enum
Range	Untagged(100) | Tagged(200)
Script/CLI	Lldp.RemoteMediaPolicyState[].TaggedFlag
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4100.1.100.100.1.600

The Tagged flag.

- Untagged: An untagged value indicates that the device is using an untagged frame format and does not include a tag header. In this case, both **Llpd.RemoteMediaPolicyState.VlanId** and **Llpd.RemoteMediaPolicyState.Priority** parameters are ignored and only the **Llpd.RemoteMediaPolicyState.Dscp** parameter is relevant.

- Tagged: A tagged value indicates that the device is using the tagged frame format and the values of the **Llpd.RemoteMediaPolicyState.VlanId**, **Llpd.RemoteMediaPolicyState.Priority**, and **Llpd.RemoteMediaPolicyState.Dscp** parameters are being used.

NetworkInterface (Config Parameter)

Type	Text
Range	Size(0..50)
Default	
Script/CLI	Lldp.NetworkInterface
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4100.1.200

The network interface name on which LLDP network policies should be enabled.
The LLDP cannot be activated on multiple network interfaces simultaneously.

ChassisId (Config Parameter)

Type	Enum
Range	MacAddress(100) | NetworkAddress(200)
Default	NetworkAddress
Script/CLI	Lldp.ChassisId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4100.1.300

The address type to populate the chassis ID.

- MacAddress: The MAC address.
- NetworkAddress: The IP address (or 0.0.0.0 if DHCP is not yet obtained).

OverrideNetworkPolicyEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Lldp.OverrideNetworkPolicyEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4100.1.400

Enables the LLDP-MED protocol override of the values of the VLAN ID, User Priority and DiffServ values.

- Enable: The service listens for LLDP advertisements and the values received for the VLAN ID, User Priority and DiffServ are applied while any previously configured value for the **Eth.Vlan.VlanId**, **Eth.Vlan.DefaultUserPriority**, and **LQos.DefaultDiffServ** parameters are ignored.
- Disable: The service only publishes its characteristics and configurations by LLDP, and does not override any parameter.

OverrideNetworkPolicyRefresh (Config Parameter)

Type	Enum
Range	Disable(100) | OnNetworkPolicyChanges(200)
Default	Disable
Script/CLI	Lldp.OverrideNetworkPolicyRefresh
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4100.1.410

Allows received Network Policies to refresh the VLAN ID, User Priority and DiffServ values of an overridden network. The **Lldp.RemoteMediaPolicyState** status table will reflect the new values.

- Disable: The service applies only the first received Network Policy TLV. If a change occurs, the current Network Policy still applies.
- OnNetworkPolicyChanges: The service applies the newly received Network Policy TLV, but only if the LLDPDU shares the same **Lldp.ChassisId** and Port ID.

This parameter has no effect if the **Lldp.OverrideNetworkPolicyEnable** parameter is set to 'Disable'.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Lldp.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4100.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.

- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Lldp.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4100.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Lldp service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.4100.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	Conflicting VLAN ID between voice and signaling. Using the VLAN ID %1$d for both.	Info	This message is issued when the VLAN ID received by LLDP is different for the voice class and signaling class, in which case the voice VLAN ID is taken.
20	The VLAN for the network interface %1$s is overridden with a VLAN ID of %2$d.	Info	This message is issued when the network policy override is enabled and a VLAN ID has been received by LLDP with QoS configuration.
30	The LLDP network interface has no IP address assigned.	Info	This message is issued when there is no IP address assigned on the LLDP network interface at the time the LLDP PDU was sent. In this case, the PDU contains no IP address.
40	The configured LLDP network interface %1$s is not active.	Warning	This message is issued when the LLDP service starts with a disabled or non-existing network interface.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.

NumKey	Message	Severity	Description
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.

NumKey	Message	Severity	Description
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Lldp.

Message	Severity	Description
The network %1$s is not active.	Warning	This message is issued when the user assigns a disabled or non-existing network interface name to the LLDP service.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.

Message	Severity	Description
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Local Quality of Service (LQos)

The Local Quality of Service (LQOS) service manages the QOS parameters applicable to the unit.

Parameters

DefaultDiffServ (Config Parameter)

Type	UInt32
Range	0..255
Default	184
Script/CLI	LQos.DefaultDiffServ
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2500.1.100

Default Differentiated Services value used by the unit for all generated IPv4 packets. Specific service class values may be set in the **ServiceClasses** table. This 8-bit value is directly set in the TOS field (2nd byte) of the header of transmitted IPv4 packets, allowing the administrator to use either DiffServ or TOS mapping.

Note: The TOS values for TCP packets are equal to the closest multiple of 4 value that is not greater than the configured value.

DefaultTrafficClass (Config Parameter)

Type	UInt32
Range	0..255
Default	0
Script/CLI	LQos.DefaultTrafficClass
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2500.1.150

Default Traffic Class value used by the unit for all generated IPv6 packets. Specific service class values may be set in the **ServiceClasses** table. The 8-bit Traffic Class field in the IPv6 header is available for use by originating nodes and/or forwarding routers to identify and distinguish between different classes or priorities of IPv6 packets.

Ethernet8021QTagging (Table)

This table lists all Ethernet interfaces and allows to configure 802.1Q tagging for them.

InterfaceName (Index) | Table: Ethernet8021QTagging

Type	Text
Range	
Script/CLI	LQos.Ethernet8021QTagging[].InterfaceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2500.1.200.1.100

Name of the Ethernet interface

EnablePriorityTagging (Config Parameter) | Table: Ethernet8021QTagging

Type	EnableDisable
Range	
Default	Disable
Script/CLI	LQos.Ethernet8021QTagging[].EnablePriorityTagging
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2500.1.200.1.200

Enables or disables user priority tagging on the interface. The VLAN ID part of the 802.1Q tag is always set to 0. VLANs may be configured in service Ethernet (Eth)'s VLAN table.

DefaultUserPriority (Config Parameter) | Table: Ethernet8021QTagging

Type	UInt32
Range	0..7
Default	0
Script/CLI	LQos.Ethernet8021QTagging[].DefaultUserPriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2500.1.200.1.300

Default User Priority value the interface uses when tagging packets. Specific service class values may be set in the **ServiceClasses** table.

ServiceClasses (Table)

This table allows to set specific values of DiffServ, traffic class and User Priority by service class.

Id (Index) | Table: ServiceClasses

Type	UInt32
Range	
Script/CLI	LQos.ServiceClasses[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2500.1.300.1.100

Unique identifier of the row in the table.

Description (Status Parameter) | Table: ServiceClasses

Type	Text
Range	SIZE(0..127)
Script/CLI	LQos.ServiceClasses[].Description
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2500.1.300.1.200

Description of the service class.

DiffServ (Config Parameter) | Table: ServiceClasses

Type	UInt32
Range	0..255
Default	184
Script/CLI	LQos.ServiceClasses[].DiffServ
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2500.1.300.1.300

Differentiated Services value for this service class. This value overrides the **DefaultDiffServ** parameter. This 8-bit value is directly set in the TOS field (2nd byte) of the header of transmitted IPv4 packets, allowing the administrator to use either DiffServ or TOS mapping.

Note: The TOS values for TCP packets are equal to the closest multiple of 4 value that is not greater than the configured value.

TrafficClass (Config Parameter) | Table: ServiceClasses

Type	UInt32
Range	0..255
Default	0
Script/CLI	LQos.ServiceClasses[].TrafficClass
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2500.1.300.1.350

Default Traffic Class value used in IPv6 packets. The 8-bit Traffic Class field in the IPv6 header is available for use by originating nodes and/or forwarding routers to identify and distinguish between different classes or priorities of IPv6 packets.

UserPriority (Config Parameter) | Table: ServiceClasses

Type	UInt32
Range	0..7
Default	6
Script/CLI	LQos.ServiceClasses[].UserPriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2500.1.300.1.400

User priority for this service class. This value overrides the **DefaultUserPriority** parameter from the **Ethernet8021QTagging** table.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	LQos.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2500.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	LQos.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2500.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the LQos service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.2500.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	Default DiffServ value is now %1$d for link %2$s.	Info	This message is issued when the default DiffServ value for a link is modified.
15	Default IPv6 traffic class value is now %1$d for link %2$s.	Info	This message is issued when the default IPv6 traffic class value for a link is modified.
20	Error setting default DiffServ %1$d value for link %2$s.	Error	This message is issued when an error occurs when setting the default DiffServ value for a link.
25	Error setting default IPv6 traffic class %1$d value for link %2$s.	Error	This message is issued when an error occurs when setting the default IPv6 traffic class value for a link.
30	Default user priority value is now %1$d for link %2$s.	Info	This message is issued when the default user priority value for a link is modified.
40	Error setting default user priority %1$d value for link %2$s.	Error	This message is issued when an error occurs when setting the default user priority value for a link.
50	Overriding service class %1$s (%2$d) with user priority (%3$d) and DiffServ (%4$d) from LLDP values received.	Info	This message is issued when the service class information received from LLDP have been applied, overriding the configured user priority and DiffServ values.
60	Error overriding service class info from LLDP; cannot find class id %1$d.	Error	This message is issued when an error occurs when overriding the service class information from LLDP values.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.

NumKey	Message	Severity	Description
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.

NumKey	Message	Severity	Description
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to LQos.

Message	Severity	Description
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.

Message	Severity	Description
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Media IP Transport (Mipt)

The Media IP Transport (MIPT) service manages the voice and data encodings over the IP network.

Parameters

DefaultCodecGenericVoiceActivityDetection (Config Parameter)

Type	Enum
Range	Disable(100) | Transparent(200) | Conservative(300)
Default	Conservative
Script/CLI	Mipt.DefaultCodecGenericVoiceActivityDetection
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.100

If Voice Activity Detection (VAD) is enabled, then speech frames are only sent during talkspurts (periods of audio activity).
During silence periods, no speech frames are sent, but Comfort Noise (CN) packets containing information about background noise may be sent (see draft-ietf-avt-rtp-cn-05.txt). This parameter specifies the sensitivity of the VAD algorithm to silence periods.

The generic VAD is used by codecs without built-in VAD like G.711, G.722, and G.726.

- Disable: VAD disabled.
- Transparent: VAD enabled - low sensitivity to silence periods.

- Conservative: VAD enabled - normal sensitivity to silence periods.

If a specific value is set for the **EpSpecificCodec.GenericVoiceActivityDetection** parameter and the **EpSpecificCodec.EnableConfig** parameter is set to 'Enable', then it overrides the current default value.

EpSpecificCodec (Table)

Endpoint specific configuration.

EpId (Index) | Table: EpSpecificCodec

Type	Text
Range	
Script/CLI	Mipt.EpSpecificCodec[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.200.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificCodec

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodec[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.200.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultCodecGenericVoiceActivityDetection** parameter.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificCodec.GenericVoiceActivityDetection** parameter.

GenericVoiceActivityDetection (Config Parameter) | Table: EpSpecificCodec

Type	Enum
Range	Disable(100) | Transparent(200) | Conservative(300)
Default	Conservative
Script/CLI	Mipt.EpSpecificCodec[].GenericVoiceActivityDetection
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.200.1.300

If Voice Activity Detection (VAD) is enabled, then speech frames are only sent during talkspurts (periods of audio activity).
During silence periods, no speech frames are sent, but Comfort Noise (CN) packets containing information about background noise may be sent (see draft-ietf-avt-rtp-cn-05.txt). This parameter specifies the sensitivity of the VAD algorithm to silence periods.

The generic VAD is used by codecs without built-in VAD like G.711, G.722, and G.726.

- Disable: VAD disabled.
- Transparent: VAD enabled - low sensitivity to silence periods.
- Conservative: VAD enabled - normal sensitivity to silence periods.

This configuration overrides the default configuration set in the **DefaultCodecGenericVoiceActivityDetection** parameter if the **EpSpecificCodec.EnableConfig** parameter is set to 'Enable'.

DefaultCodecG711MulawVoiceEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Mipt.DefaultCodecG711MulawVoiceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.100.100

Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.
PCMA and PCMU are specified in ITU-T Recommendation G.711. Audio data is encoded as eight bits per sample, after logarithmic scaling. PCMU denotes mu-law scaling, PCMA A-law scaling.

This codec uses generic voice activity detection. See the **DefaultCodecGenericVoiceActivityDetection** and **EpSpecificCodec.GenericVoiceActivityDetection** parameters.

This codec always uses the RTP transport.

If a specific value is set for the **EpSpecificCodecG711Mulaw.VoiceEnable** parameter and the **EpSpecificCodecG711Mulaw.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG711MulawVoicePriority (Config Parameter)

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.DefaultCodecG711MulawVoicePriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.100.200

Indicates the priority of this voice codec versus the other voice codecs. The voice codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming call.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

If a specific value is set for the **EpSpecificCodecG711Mulaw.VoicePriority** parameter and the **EpSpecificCodecG711Mulaw.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG711MulawDataEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Mipt.DefaultCodecG711MulawDataEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.100.300

Indicates if the codec can be selected for data transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.
If a specific value is set for the **EpSpecificCodecG711Mulaw.DataEnable** parameter and the **EpSpecificCodecG711Mulaw.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG711MulawDataPriority (Config Parameter)

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.DefaultCodecG711MulawDataPriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.100.400

Indicates the priority of this data codec versus the other data codecs. The data codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming call.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

If a specific value is set for the **EpSpecificCodecG711Mulaw.DataPriority** parameter and the **EpSpecificCodecG711Mulaw.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG711MulawMinPTime (Config Parameter)

Type	UInt32
Range	10..30
Default	20
Script/CLI	Mipt.DefaultCodecG711MulawMinPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.100.500

Lower boundary for the packetization period of the given codec.
PCMU -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

If a specific value is set for the **EpSpecificCodecG711Mulaw.MinPTime** parameter and the **EpSpecificCodecG711Mulaw.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG711MulawMaxPTime (Config Parameter)

Type	UInt32
Range	10..30
Default	30
Script/CLI	Mipt.DefaultCodecG711MulawMaxPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.100.600

Upper boundary for the packetization period of the given codec.
PCMU -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

If a specific value is set for the **EpSpecificCodecG711Mulaw.MaxPTime** parameter and the **EpSpecificCodecG711Mulaw.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

EpSpecificCodecG711Mulaw (Table)

Endpoint specific configuration.

EpId (Index) | Table: EpSpecificCodecG711Mulaw

Type	Text
Range	
Script/CLI	Mipt.EpSpecificCodecG711Mulaw[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.100.700.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificCodecG711Mulaw

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecG711Mulaw[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.100.700.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultCodecG711MulawVoiceEnable**, **DefaultCodecG711MulawVoicePriority**, **DefaultCodecG711MulawDataEnable**, **DefaultCodecG711MulawDataPriority**, **DefaultCodecG711MulawMinPTime** and **DefaultCodecG711MulawMaxPTime** parameters.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificCodecG711Mulaw.VoiceEnable**, **EpSpecificCodecG711Mulaw.VoicePriority**, **EpSpecificCodecG711Mulaw.DataEnable**, **EpSpecificCodecG711Mulaw.DataPriority**, **EpSpecificCodecG711Mulaw.MinPTime** and **EpSpecificCodecG711Mulaw.MaxPTime** parameters.

VoiceEnable (Config Parameter) | Table: EpSpecificCodecG711Mulaw

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Mipt.EpSpecificCodecG711Mulaw[].VoiceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.100.700.1.300

Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.
PCMA and PCMU are specified in ITU-T Recommendation G.711. Audio data is encoded as eight bits per sample, after logarithmic scaling. PCMU denotes mu-law scaling, PCMA A-law scaling.

This codec uses generic voice activity detection. See the **DefaultCodecGenericVoiceActivityDetection** and **EpSpecificCodec.GenericVoiceActivityDetection** parameters.

This codec always uses the RTP transport.

This configuration overrides the default configuration set in the **DefaultCodecG711MulawVoiceEnable** parameter if the **EpSpecificCodecG711Mulaw.EnableConfig** parameter is set to 'Enable'.

VoicePriority (Config Parameter) | Table: EpSpecificCodecG711Mulaw

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.EpSpecificCodecG711Mulaw[].VoicePriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.100.700.1.400

Indicates the priority of this voice codec versus the other voice codecs. The voice codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

This configuration overrides the default configuration set in the **DefaultCodecG711MulawVoicePriority** parameter if the **EpSpecificCodecG711Mulaw.EnableConfig** parameter is set to 'Enable'.

DataEnable (Config Parameter) | Table: EpSpecificCodecG711Mulaw

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Mipt.EpSpecificCodecG711Mulaw[].DataEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.100.700.1.500

Indicates if the codec can be selected for data transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.
This configuration overrides the default configuration set in the **DefaultCodecG711MulawDataEnable** parameter if the **EpSpecificCodecG711Mulaw.EnableConfig** parameter is set to 'Enable'.

DataPriority (Config Parameter) | Table: EpSpecificCodecG711Mulaw

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.EpSpecificCodecG711Mulaw[].DataPriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.100.700.1.600

Indicates the priority of this data codec versus the other data codecs. The data codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

This configuration overrides the default configuration set in the **DefaultCodecG711MulawDataPriority** parameter if the **EpSpecificCodecG711Mulaw.EnableConfig** parameter is set to 'Enable'.

MinPTime (Config Parameter) | Table: EpSpecificCodecG711Mulaw

Type	UInt32
Range	10..30
Default	20
Script/CLI	Mipt.EpSpecificCodecG711Mulaw[].MinPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.100.700.1.700

Lower boundary for the packetization period of the given codec.
PCMU -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

This configuration overrides the default configuration set in the **DefaultCodecG711MulawMinPTime** parameter if the **EpSpecificCodecG711Mulaw.EnableConfig** parameter is set to 'Enable'.

MaxPTime (Config Parameter) | Table: EpSpecificCodecG711Mulaw

Type	UInt32
Range	10..30
Default	30
Script/CLI	Mipt.EpSpecificCodecG711Mulaw[].MaxPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.100.700.1.800

Upper boundary for the packetization period of the given codec.
PCMU -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

This configuration overrides the default configuration set in the **DefaultCodecG711MulawMaxPTime** parameter if the **EpSpecificCodecG711Mulaw.EnableConfig** parameter is set to 'Enable'.

DefaultCodecG711AlawVoiceEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Mipt.DefaultCodecG711AlawVoiceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.200.100

Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.
PCMA and PCMU are specified in ITU-T Recommendation G.711. Audio data is encoded as eight bits per sample, after logarithmic scaling. PCMU denotes mu-law scaling, PCMA A-law scaling.

This codec uses generic voice activity detection. See the **DefaultCodecGenericVoiceActivityDetection** and **EpSpecificCodec.GenericVoiceActivityDetection** parameters.

This codec always uses the RTP transport.

If a specific value is set for the **EpSpecificCodecG711Alaw.VoiceEnable** parameter and the **EpSpecificCodecG711Alaw.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG711AlawVoicePriority (Config Parameter)

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.DefaultCodecG711AlawVoicePriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.200.200

Indicates the priority of this voice codec versus the other voice codecs. The voice codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

If a specific value is set for the **EpSpecificCodecG711Alaw.VoicePriority** parameter and the **EpSpecificCodecG711Alaw.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG711AlawDataEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Mipt.DefaultCodecG711AlawDataEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.200.300

Indicates if the codec can be selected for data transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.
If a specific value is set for the **EpSpecificCodecG711Alaw.DataEnable** parameter and the **EpSpecificCodecG711Alaw.EnableConfig** parameters is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG711AlawDataPriority (Config Parameter)

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.DefaultCodecG711AlawDataPriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.200.400

Indicates the priority of this data codec versus the other data codecs. The data codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

If a specific value is set for the **EpSpecificCodecG711Alaw.DataPriority** parameter and the **EpSpecificCodecG711Alaw.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG711AlawMinPTime (Config Parameter)

Type	UInt32
Range	10..30
Default	20
Script/CLI	Mipt.DefaultCodecG711AlawMinPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.200.500

Lower boundary for the packetization period of the given codec.
PCMA -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

If a specific value is set for the **EpSpecificCodecG711Alaw.MinPTime** parameter and the **EpSpecificCodecG711Alaw.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG711AlawMaxPTime (Config Parameter)

Type	UInt32
Range	10..30
Default	30
Script/CLI	Mipt.DefaultCodecG711AlawMaxPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.200.600

Upper boundary for the packetization period of the given codec.
PCMA -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100m s with increments of 1 ms only if the stream is not encrypted (SRTP).

If a specific value is set for the **EpSpecificCodecG711Alaw.MaxPTime** parameter and the **EpSpecificCodecG711Alaw.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

EpSpecificCodecG711Alaw (Table)

Endpoint specific configuration.

EpId (Index) | Table: EpSpecificCodecG711Alaw

Type	Text
Range	
Script/CLI	Mipt.EpSpecificCodecG711Alaw[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.200.700.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificCodecG711Alaw

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecG711Alaw[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.200.700.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultCodecG711AlawVoiceEnable**, **DefaultCodecG711AlawVoicePriority**, **DefaultCodecG711AlawDataEnable**, **DefaultCodecG711AlawDataPriority**, **DefaultCodecG711AlawMinPTime** and **DefaultCodecG711AlawMaxPTime** parameters.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificCodecG711Alaw.VoiceEnable**, **EpSpecificCodecG711Alaw.VoicePriority**, **EpSpecificCodecG711Alaw.DataEnable**, **EpSpecificCodecG711Alaw.DataPriority**, **EpSpecificCodecG711Alaw.MinPTime** and **EpSpecificCodecG711Alaw.MaxPTime** parameters.

VoiceEnable (Config Parameter) | Table: EpSpecificCodecG711Alaw

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Mipt.EpSpecificCodecG711Alaw[].VoiceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.200.700.1.300

Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.
PCMA and PCMU are specified in ITU-T Recommendation G.711. Audio data is encoded as eight bits per sample, after logarithmic scaling. PCMU denotes mu-law scaling, PCMA A-law scaling.

This codec uses generic voice activity detection. See the **DefaultCodecGenericVoiceActivityDetection** and **EpSpecificCodec.GenericVoiceActivityDetection** parameters.

This codec always uses the RTP transport.

This configuration overrides the default configuration set in the **DefaultCodecG711AlawVoiceEnable** parameter if the **EpSpecificCodecG711Alaw.EnableConfig** parameter is set to 'Enable'.

VoicePriority (Config Parameter) | Table: EpSpecificCodecG711Alaw

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.EpSpecificCodecG711Alaw[].VoicePriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.200.700.1.400

Indicates the priority of this voice codec versus the other voice codecs. The voice codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

This configuration overrides the default configuration set in the **DefaultCodecG711AlawVoicePriority** parameter if the **EpSpecificCodecG711Alaw.EnableConfig** parameter is set to 'Enable'.

DataEnable (Config Parameter) | Table: EpSpecificCodecG711Alaw

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Mipt.EpSpecificCodecG711Alaw[].DataEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.200.700.1.500

Indicates if the codec can be selected for data transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.
This configuration overrides the default configuration set in the **DefaultCodecG711AlawDataEnable** parameter if the **EpSpecificCodecG711Alaw.EnableConfig** parameter is set to 'Enable'.

DataPriority (Config Parameter) | Table: EpSpecificCodecG711Alaw

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.EpSpecificCodecG711Alaw[].DataPriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.200.700.1.600

Indicates the priority of this data codec versus the other data codecs. The data codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

This configuration overrides the default configuration set in the **DefaultCodecG711AlawDataPriority** parameter if the **EpSpecificCodecG711Alaw.EnableConfig** parameter is set to 'Enable'.

MinPTime (Config Parameter) | Table: EpSpecificCodecG711Alaw

Type	UInt32
Range	10..30
Default	20
Script/CLI	Mipt.EpSpecificCodecG711Alaw[].MinPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.200.700.1.700

Lower boundary for the packetization period of the given codec.
PCMA -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

This configuration overrides the default configuration set in the **DefaultCodecG711AlawMinPTime** parameter if the **EpSpecificCodecG711Alaw.EnableConfig** parameter is set to 'Enable'.

MaxPTime (Config Parameter) | Table: EpSpecificCodecG711Alaw

Type	UInt32
Range	10..30
Default	30
Script/CLI	Mipt.EpSpecificCodecG711Alaw[].MaxPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.300.200.700.1.800

Upper boundary for the packetization period of the given codec.
PCMA -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

This configuration overrides the default configuration set in the **DefaultCodecG711AlawMaxPTime** parameter if the **EpSpecificCodecG711Alaw.EnableConfig** parameter is set to 'Enable'.

DefaultCodecG722VoiceEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Mipt.DefaultCodecG722VoiceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.350.100

Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.
G.722 is specified in ITU Recommendation G.722, 7 kHz audio-coding within 64 kbit/s. This Recommendation describes the characteristics of an audio wideband (50 to 7 000 Hz) coding system used for higher quality speech applications.

Although G.722 is a wideband codec, the perceived audio quality would be limited by the telephony interfaces, which only support narrowband audio (50 to 4 000 Hz).

Note: Supports only a bitrate of 64 kbps.

This codec always uses the RTP transport.

If a specific value is set for the **EpSpecificCodecG722.VoiceEnable** parameter and the **EpSpecificCodecG722.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG722VoicePriority (Config Parameter)

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.DefaultCodecG722VoicePriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.350.200

Indicates the priority of this voice codec versus the other voice codecs. The voice codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

If a specific value is set for the **EpSpecificCodecG722.VoicePriority** parameter and the **EpSpecificCodecG722.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG722MinPTime (Config Parameter)

Type	UInt32
Range	10..10 | 20..20 | 30..30
Default	20
Script/CLI	Mipt.DefaultCodecG722MinPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.350.300

Lower boundary for the packetization period of the given codec.
G.722 -> (10 ms|20 ms|30 ms)

This value is expressed in ms, with increments of 10 ms.

If a specific value is set for the **EpSpecificCodecG722.MinPTime** parameter and the **EpSpecificCodecG722.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG722MaxPTime (Config Parameter)

Type	UInt32
Range	10..10 | 20..20 | 30..30
Default	20
Script/CLI	Mipt.DefaultCodecG722MaxPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.350.400

Upper boundary for the packetization period of the given codec.
G.722 -> (10 ms|20 ms|30 ms)

This value is expressed in ms, with increments of 10 ms.

If a specific value is set for the **EpSpecificCodecG722.MaxPTime** parameter and the **EpSpecificCodecG722.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

EpSpecificCodecG722 (Table)

Endpoint specific configuration.

EpId (Index) | Table: EpSpecificCodecG722

Type	Text
Range	
Script/CLI	Mipt.EpSpecificCodecG722[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.350.500.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificCodecG722

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecG722[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.350.500.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultCodecG722VoiceEnable**, **DefaultCodecG722VoicePriority**, **DefaultCodecG722MinPTime** and **DefaultCodecG722MaxPTime** parameters.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificCodecG722.VoiceEnable**, **EpSpecificCodecG722.VoicePriority**, **EpSpecificCodecG722.MinPTime** and **EpSpecificCodecG722.MaxPTime** parameters.

VoiceEnable (Config Parameter) | Table: EpSpecificCodecG722

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Mipt.EpSpecificCodecG722[].VoiceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.350.500.1.300

Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.
G.722 is specified in ITU Recommendation G.722, 7 kHz audio-coding within 64 kbit/s. This Recommendation describes the characteristics of an audio wideband (50 to 7 000 Hz) coding system used for higher quality speech applications.

Although G.722 is a wideband codec, the perceived audio quality would be limited by the telephony interfaces, which only support narrowband audio (50 to 4 000 Hz).

Note: Supports only a bitrate of 64 kbps.

This codec always uses the RTP transport.

This configuration overrides the default configuration set in the **DefaultCodecG722VoiceEnable** parameter if the **EpSpecificCodecG722.EnableConfig** parameter is set to 'Enable'.

VoicePriority (Config Parameter) | Table: EpSpecificCodecG722

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.EpSpecificCodecG722[].VoicePriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.350.500.1.400

Indicates the priority of this voice codec versus the other voice codecs. The voice codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

This configuration overrides the default configuration set in the **DefaultCodecG722VoicePriority** parameter if the **EpSpecificCodecG722.EnableConfig** parameter is set to 'Enable'.

MinPTime (Config Parameter) | Table: EpSpecificCodecG722

Type	UInt32
Range	10..10 | 20..20 | 30..30
Default	20
Script/CLI	Mipt.EpSpecificCodecG722[].MinPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.350.500.1.500

Lower boundary for the packetization period of the given codec.
G.722 -> (10 ms|20 ms|30 ms)

This value is expressed in ms, with increments of 10 ms.

This configuration overrides the default configuration set in the **DefaultCodecG722MinPTime** parameter if the **EpSpecificCodecG722.EnableConfig** parameter is set to 'Enable'.

MaxPTime (Config Parameter) | Table: EpSpecificCodecG722

Type	UInt32
Range	10..10 | 20..20 | 30..30
Default	20
Script/CLI	Mipt.EpSpecificCodecG722[].MaxPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.350.500.1.600

Upper boundary for the packetization period of the given codec.
G.722 -> (10 ms|20 ms|30 ms)

This value is expressed in ms, with increments of 10 ms.

This configuration overrides the default configuration set in the **DefaultCodecG722MaxPTime** parameter if the **EpSpecificCodecG722.EnableConfig** parameter is set to 'Enable'.

DefaultCodecG723VoiceEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Mipt.DefaultCodecG723VoiceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.400.100

Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.
G.723.1 is specified in ITU Recommendation G.723.1, Dual-rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s. This Recommendation specifies a coded representation that can be used for compressing the speech signal component of multi-media services at a very low bit rate. Audio is encoded in 30 ms frames. A G.723.1 frame can be one of three sizes: 24 octets (6.3 kb/s frame), 20 octets (5.3 kb/s frame), or 4 octets. These 4-octet frames are called SID frames (Silence Insertion Descriptor) and are used to specify comfort noise parameters.

This codec always uses the RTP transport.

If a specific value is set for the **EpSpecificCodecG723.VoiceEnable** parameter and the **EpSpecificCodecG723.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG723VoicePriority (Config Parameter)

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.DefaultCodecG723VoicePriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.400.200

Indicates the priority of this voice codec versus the other voice codecs. The voice codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

If a specific value is set for the **EpSpecificCodecG723.VoicePriority** parameter and the **EpSpecificCodecG723.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG723Bitrate (Config Parameter)

Type	Enum
Range	Rate53kbps(100) | Rate63kbps(200)
Default	Rate63kbps
Script/CLI	Mipt.DefaultCodecG723Bitrate
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.400.300

Indicates the G.723.1 bit rate to use.
If a specific value is set for the **EpSpecificCodecG723.Bitrate** parameter and the **EpSpecificCodecG723.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG723MinPTime (Config Parameter)

Type	UInt32
Range	30..30 | 60..60
Default	30
Script/CLI	Mipt.DefaultCodecG723MinPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.400.400

Lower boundary for the packetization period of the given codec.
G.723.1 -> (30 ms|60 ms)

For reception, the range is extended from 30 ms to 120 ms with increments of 30 ms only if the stream is not encrypted (SRTP).

If a specific value is set for the **EpSpecificCodecG723.MinPTime** parameter and the **EpSpecificCodecG723.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG723MaxPTime (Config Parameter)

Type	UInt32
Range	30..30 | 60..60
Default	60
Script/CLI	Mipt.DefaultCodecG723MaxPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.400.500

Upper boundary for the packetization period of the given codec.
G.723.1 -> (30 ms|60 ms)

For reception, the range is extended from 30 ms to 120 ms with increments of 30 ms only if the stream is not encrypted (SRTP).

If a specific value is set for the **EpSpecificCodecG723.MaxPTime** parameter and the **EpSpecificCodecG723.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

EpSpecificCodecG723 (Table)

Endpoint specific configuration.

EpId (Index) | Table: EpSpecificCodecG723

Type	Text
Range	
Script/CLI	Mipt.EpSpecificCodecG723[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.400.700.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificCodecG723

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecG723[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.400.700.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultCodecG723VoiceEnable**, **DefaultCodecG723VoicePriority**, **DefaultCodecG723Bitrate**, **DefaultCodecG723MinPTime**, **DefaultCodecG723MaxPTime** and **DefaultCodecG723VoiceActivityDetection** parameters.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificCodecG723.VoiceEnable**, **EpSpecificCodecG723.VoicePriority**, **EpSpecificCodecG723.Bitrate**, **EpSpecificCodecG723.MinPTime**, **EpSpecificCodecG723.MaxPTime** and **EpSpecificCodecG723.VoiceActivityDetection** parameters.

VoiceEnable (Config Parameter) | Table: EpSpecificCodecG723

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Mipt.EpSpecificCodecG723[].VoiceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.400.700.1.300

Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.
G.723.1 is specified in ITU Recommendation G.723.1, Dual-rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s. This Recommendation specifies a coded representation that can be used for compressing the speech signal component of multi-media services at a very low bit rate. Audio is encoded in 30 ms frames. A G.723.1 frame can be one of three sizes: 24 octets (6.3 kb/s frame), 20 octets (5.3 kb/s frame), or 4 octets. These 4-octet frames are called SID frames (Silence Insertion Descriptor) and are used to specify comfort noise parameters.

This codec always uses the RTP transport.

This configuration overrides the default configuration set in the **DefaultCodecG723VoiceEnable** parameter if the **EpSpecificCodecG723.EnableConfig** parameter is set to 'Enable'.

VoicePriority (Config Parameter) | Table: EpSpecificCodecG723

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.EpSpecificCodecG723[].VoicePriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.400.700.1.400

Indicates the priority of this voice codec versus the other voice codecs. The voice codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

This configuration overrides the default configuration set in the **DefaultCodecG723VoicePriority** parameter if the **EpSpecificCodecG723.EnableConfig** parameter is set to 'Enable'.

Bitrate (Config Parameter) | Table: EpSpecificCodecG723

Type	Enum
Range	Rate53kbps(100) | Rate63kbps(200)
Default	Rate63kbps
Script/CLI	Mipt.EpSpecificCodecG723[].Bitrate
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.400.700.1.500

Indicates the G.723.1 bit rate to use.
This configuration overrides the default configuration set in the **DefaultCodecG723Bitrate** parameter if the **EpSpecificCodecG723.EnableConfig** parameter is set to 'Enable'.

MinPTime (Config Parameter) | Table: EpSpecificCodecG723

Type	UInt32
Range	30..30 | 60..60
Default	30
Script/CLI	Mipt.EpSpecificCodecG723[].MinPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.400.700.1.600

Lower boundary for the packetization period of the given codec.
G.723.1 -> (30 ms|60 ms)

For reception, the range is extended from 30 ms to 120 ms with increments of 30 ms only if the stream is not encrypted (SRTP).

This configuration overrides the default configuration set in the **DefaultCodecG723MinPTime** parameter if the **EpSpecificCodecG723.EnableConfig** parameter is set to 'Enable'.

MaxPTime (Config Parameter) | Table: EpSpecificCodecG723

Type	UInt32
Range	30..30 | 60..60
Default	60
Script/CLI	Mipt.EpSpecificCodecG723[].MaxPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.400.700.1.700

Upper boundary for the packetization period of the given codec.
G.723.1 -> (30 ms|60 ms)

For reception, the range is extended from 30 ms to 120 ms with increments of 30 ms only if the stream is not encrypted (SRTP).

This configuration overrides the default configuration set in the **DefaultCodecG723MaxPTime** parameter if the **EpSpecificCodecG723.EnableConfig** parameter is set to 'Enable'.

DefaultCodecG726r16kbpsVoiceEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.DefaultCodecG726r16kbpsVoiceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.100.100

Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

- Disable: Disable G.726 at 16 kbps.
- Enable: Enable G.726 at 16 kbps.

G.726 is specified in ITU-T Recommendation G.726: 40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM). It describes the algorithm recommended for conversion of a single 64 kbit/s A-law or U-law PCM channel encoded at 8000 samples/sec to and from a 40, 32, 24, or 16 kbit/s channel. The conversion is applied to the PCM stream using an Adaptive Differential Pulse Code Modulation (ADPCM) transcoding technique.

This codec uses generic voice activity detection. See the **DefaultCodecGenericVoiceActivityDetection** and **EpSpecificCodec.GenericVoiceActivityDetection** parameters.

This codec always uses the RTP transport.

If a specific value is set for the **EpSpecificCodecG726r16kbps.VoiceEnable** parameter and the **EpSpecificCodecG726r16kbps.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG726r16kbpsVoicePriority (Config Parameter)

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.DefaultCodecG726r16kbpsVoicePriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.100.200

Indicates the priority of this voice codec versus the other voice codecs. The voice codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

If a specific value is set for the **EpSpecificCodecG726r16kbps.VoicePriority** parameter and the **EpSpecificCodecG726r16kbps.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG726r16kbpsPayloadType (Config Parameter)

Type	UInt32
Range	96..127
Default	97
Script/CLI	Mipt.DefaultCodecG726r16kbpsPayloadType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.100.300

Determines the actual RTP dynamic payload type used in an initial offer when enabling G.726 at 16 kbps for voice and data transmission.
The payload types available are as per RFC 3551.

If a specific value is set for the **EpSpecificCodecG726r16kbps.PayloadType** parameter and the **EpSpecificCodecG726r16kbps.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG726r16kbpsMinPTime (Config Parameter)

Type	UInt32
Range	10..30
Default	20
Script/CLI	Mipt.DefaultCodecG726r16kbpsMinPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.100.400

Lower boundary for the packetization period of the given codec.
G.726 at 16 kbps -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

If a specific value is set for the **EpSpecificCodecG726r16kbps.MinPTime** parameter and the **EpSpecificCodecG726r16kbps.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG726r16kbpsMaxPTime (Config Parameter)

Type	UInt32
Range	10..30
Default	30
Script/CLI	Mipt.DefaultCodecG726r16kbpsMaxPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.100.500

Upper boundary for the packetization period of the given codec.
G.726 at 16 kbps -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

If a specific value is set for the **EpSpecificCodecG726r16kbps.MaxPTime** parameter and the **EpSpecificCodecG726r16kbps.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

EpSpecificCodecG726r16kbps (Table)

Endpoint specific configuration.

EpId (Index) | Table: EpSpecificCodecG726r16kbps

Type	Text
Range	
Script/CLI	Mipt.EpSpecificCodecG726r16kbps[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.100.600.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificCodecG726r16kbps

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecG726r16kbps[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.100.600.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultCodecG726r16kbpsVoiceEnable**, **DefaultCodecG726r16kbpsVoicePriority**, **DefaultCodecG726r16kbpsPayloadType**, **DefaultCodecG726r16kbpsMinPTime** and **DefaultCodecG726r16kbpsMaxPTime** parameters.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificCodecG726r16kbps.VoiceEnable**, **EpSpecificCodecG726r16kbps.VoicePriority**, **EpSpecificCodecG726r16kbps.PayloadType**, **EpSpecificCodecG726r16kbps.MinPTime** and **EpSpecificCodecG726r16kbps.MaxPTime** parameters.

VoiceEnable (Config Parameter) | Table: EpSpecificCodecG726r16kbps

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecG726r16kbps[].VoiceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.100.600.1.300

Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

- Disable: Disable G.726 at 16 kbps.
- Enable: Enable G.726 at 16 kbps.

G.726 is specified in ITU-T Recommendation G.726: 40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM). It describes the algorithm recommended for conversion of a single 64 kbit/s A-law or U-law PCM channel encoded at 8000 samples/sec to and from a 40, 32, 24, or 16 kbit/s channel. The conversion is applied to the PCM stream using an Adaptive Differential Pulse Code Modulation (ADPCM) transcoding technique.

This codec uses generic voice activity detection. See the **DefaultCodecGenericVoiceActivityDetection** and **EpSpecificCodec.GenericVoiceActivityDetection** parameters.

This codec always uses the RTP transport.

This configuration overrides the default configuration set in the **DefaultCodecG726r16kbpsVoiceEnable** parameter if the **EpSpecificCodecG726r16kbps.EnableConfig** parameter is set to 'Enable'.

VoicePriority (Config Parameter) | Table: EpSpecificCodecG726r16kbps

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.EpSpecificCodecG726r16kbps[].VoicePriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.100.600.1.400

Indicates the priority of this voice codec versus the other voice codecs. The voice codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

This configuration overrides the default configuration set in the **DefaultCodecG726r16kbpsVoicePriority** parameter if the **EpSpecificCodecG726r16kbps.EnableConfig** parameter is set to 'Enable'.

PayloadType (Config Parameter) | Table: EpSpecificCodecG726r16kbps

Type	UInt32
Range	96..127
Default	97
Script/CLI	Mipt.EpSpecificCodecG726r16kbps[].PayloadType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.100.600.1.500

Determines the actual RTP dynamic payload type used in an initial offer when enabling G.726 at 16 kbps for voice and data transmission.
The payload types available are as per RFC 3551.

This configuration overrides the default configuration set in the **DefaultCodecG726r16kbpsPayloadType** parameter if the **EpSpecificCodecG726r16kbps.EnableConfig** parameter is set to 'Enable'.

MinPTime (Config Parameter) | Table: EpSpecificCodecG726r16kbps

Type	UInt32
Range	10..30
Default	20
Script/CLI	Mipt.EpSpecificCodecG726r16kbps[].MinPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.100.600.1.600

Lower boundary for the packetization period of the given codec.
G.726 at 16 kbps -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

This configuration overrides the default configuration set in the **DefaultCodecG726r16kbpsMinPTime** parameter if the **EpSpecificCodecG726r16kbps.EnableConfig** parameter is set to 'Enable'.

MaxPTime (Config Parameter) | Table: EpSpecificCodecG726r16kbps

Type	UInt32
Range	10..30
Default	30
Script/CLI	Mipt.EpSpecificCodecG726r16kbps[].MaxPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.100.600.1.700

Upper boundary for the packetization period of the given codec.
G.726 at 16 kbps -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

This configuration overrides the default configuration set in the **DefaultCodecG726r16kbpsMaxPTime** parameter if the **EpSpecificCodecG726r16kbps.EnableConfig** parameter is set to 'Enable'.

DefaultCodecG726r24kbpsVoiceEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.DefaultCodecG726r24kbpsVoiceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.200.100

Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

- Disable: Disable G.726 at 24 kbps.
- Enable: Enable G.726 at 24 kbps.

G.726 is specified in ITU-T Recommendation G.726: 40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM). It describes the algorithm recommended for conversion of a single 64 kbit/s A-law or U-law PCM channel encoded at 8000 samples/sec to and from a 40, 32, 24, or 16 kbit/s channel. The conversion is applied to the PCM stream using an Adaptive Differential Pulse Code Modulation (ADPCM) transcoding technique.

This codec uses generic voice activity detection. See the **DefaultCodecGenericVoiceActivityDetection** and **EpSpecificCodec.GenericVoiceActivityDetection** parameters.

This codec always uses the RTP transport.

If a specific value is set for the **EpSpecificCodecG726r24kbps.VoiceEnable** parameter and the **EpSpecificCodecG726r24kbps.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG726r24kbpsVoicePriority (Config Parameter)

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.DefaultCodecG726r24kbpsVoicePriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.200.200

Indicates the priority of this voice codec versus the other voice codecs. The voice codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

If a specific value is set for the **EpSpecificCodecG726r24kbps.VoicePriority** parameter and the **EpSpecificCodecG726r24kbps.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG726r24kbpsPayloadType (Config Parameter)

Type	UInt32
Range	96..127
Default	98
Script/CLI	Mipt.DefaultCodecG726r24kbpsPayloadType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.200.300

When enabling G.726 at 24 kbps for voice and data transmission, this parameter determines the actual RTP dynamic payload type used in an initial offer.
The payload types available are as per RFC 3551.

If a specific value is set for the **EpSpecificCodecG726r24kbps.PayloadType** parameter and the **EpSpecificCodecG726r24kbps.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG726r24kbpsMinPTime (Config Parameter)

Type	UInt32
Range	10..30
Default	20
Script/CLI	Mipt.DefaultCodecG726r24kbpsMinPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.200.400

Lower boundary for the packetization period of the given codec.
G.726 at 24 kbps -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

If a specific value is set for the **EpSpecificCodecG726r24kbps.MinPTime** parameter and the **EpSpecificCodecG726r24kbps.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG726r24kbpsMaxPTime (Config Parameter)

Type	UInt32
Range	10..30
Default	30
Script/CLI	Mipt.DefaultCodecG726r24kbpsMaxPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.200.500

Upper boundary for the packetization period of the given codec.
G.726 at 24 kbps -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

If a specific value is set for the **EpSpecificCodecG726r24kbps.MaxPTime** parameter and the **EpSpecificCodecG726r24kbps.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

EpSpecificCodecG726r24kbps (Table)

Endpoint specific configuration.

EpId (Index) | Table: EpSpecificCodecG726r24kbps

Type	Text
Range	
Script/CLI	Mipt.EpSpecificCodecG726r24kbps[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.200.600.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificCodecG726r24kbps

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecG726r24kbps[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.200.600.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultCodecG726r24kbpsVoiceEnable**, **DefaultCodecG726r24kbpsVoicePriority**, **DefaultCodecG726r24kbpsPayloadType**, **DefaultCodecG726r24kbpsMinPTime** and **DefaultCodecG726r24kbpsMaxPTime** parameters.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificCodecG726r24kbps.VoiceEnable**, **EpSpecificCodecG726r24kbps.VoicePriority**, **EpSpecificCodecG726r24kbps.PayloadType**, **EpSpecificCodecG726r24kbps.MinPTime** and **EpSpecificCodecG726r24kbps.MaxPTime** parameter.

VoiceEnable (Config Parameter) | Table: EpSpecificCodecG726r24kbps

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecG726r24kbps[].VoiceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.200.600.1.300

Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

- Disable: Disable G.726 at 24 kbps.
- Enable: Enable G.726 at 24 kbps.

G.726 is specified in ITU-T Recommendation G.726: 40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM). It describes the algorithm recommended for conversion of a single 64 kbit/s A-law or U-law PCM channel encoded at 8000 samples/sec to and from a 40, 32, 24, or 16 kbit/s channel. The conversion is applied to the PCM stream using an Adaptive Differential Pulse Code Modulation (ADPCM) transcoding technique.

This codec uses generic voice activity detection. See the **DefaultCodecGenericVoiceActivityDetection** and **EpSpecificCodec.GenericVoiceActivityDetection** parameters.

This codec always uses the RTP transport.

This configuration overrides the default configuration set in the **DefaultCodecG726r24kbpsVoiceEnable** parameter if the **EpSpecificCodecG726r24kbps.EnableConfig** parameter is set to 'Enable'.

VoicePriority (Config Parameter) | Table: EpSpecificCodecG726r24kbps

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.EpSpecificCodecG726r24kbps[].VoicePriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.200.600.1.400

Indicates the priority of this voice codec versus the other voice codecs. The voice codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

This configuration overrides the default configuration set in the **DefaultCodecG726r24kbpsVoicePriority** parameter if the **EpSpecificCodecG726r24kbps.EnableConfig** parameter is set to 'Enable'.

PayloadType (Config Parameter) | Table: EpSpecificCodecG726r24kbps

Type	UInt32
Range	96..127
Default	98
Script/CLI	Mipt.EpSpecificCodecG726r24kbps[].PayloadType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.200.600.1.500

Determines the actual RTP dynamic payload type used in an initial offer when enabling G.726 at 24 kbps for voice and data transmission.
The payload types available are as per RFC 3551.

This configuration overrides the default configuration set in the **DefaultCodecG726r24kbpsPayloadType** parameter if the **EpSpecificCodecG726r24kbps.EnableConfig** parameter is set to 'Enable'.

MinPTime (Config Parameter) | Table: EpSpecificCodecG726r24kbps

Type	UInt32
Range	10..30
Default	20
Script/CLI	Mipt.EpSpecificCodecG726r24kbps[].MinPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.200.600.1.600

Lower boundary for the packetization period of the given codec.
G.726 at 24 kbps -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

This configuration overrides the default configuration set in the **DefaultCodecG726r24kbpsMinPTime** parameter if the **EpSpecificCodecG726r24kbps.EnableConfig** parameter is set to 'Enable'.

MaxPTime (Config Parameter) | Table: EpSpecificCodecG726r24kbps

Type	UInt32
Range	10..30
Default	30
Script/CLI	Mipt.EpSpecificCodecG726r24kbps[].MaxPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.200.600.1.700

Upper boundary for the packetization period of the given codec.
G.726 at 24 kbps -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

This configuration overrides the default configuration set in the **DefaultCodecG726r24kbpsMaxPTime** parameter if the **EpSpecificCodecG726r24kbps.EnableConfig** parameter is set to 'Enable'.

DefaultCodecG726r32kbpsVoiceEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.DefaultCodecG726r32kbpsVoiceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.300.100

Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

- Disable: Disable G.726 at 32 kbps.
- Enable: Enable G.726 at 32 kbps.

G.726 is specified in ITU-T Recommendation G.726: 40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM). It describes the algorithm recommended for conversion of a single 64 kbit/s A-law or U-law PCM channel encoded at 8000 samples/sec to and from a 40, 32, 24, or 16 kbit/s channel. The conversion is applied to the PCM stream using an Adaptive Differential Pulse Code Modulation (ADPCM) transcoding technique.

This codec uses generic voice activity detection. See the **DefaultCodecGenericVoiceActivityDetection** and **EpSpecificCodec.GenericVoiceActivityDetection** parameters.

This codec always uses the RTP transport.

DefaultCodecG726r32kbpsVoicePriority (Config Parameter)

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.DefaultCodecG726r32kbpsVoicePriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.300.200

Indicates the priority of this voice codec versus the other voice codecs. The voice codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

If a specific value is set for the **EpSpecificCodecG726r32kbps.VoiceEnable** parameter and the **EpSpecificCodecG726r32kbps.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG726r32kbpsDataEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.DefaultCodecG726r32kbpsDataEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.300.300

Indicates if the codec can be selected for data transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

- Disable: Disable G.726 at 32 kbps.
- Enable: Enable G.726 at 32 kbps.

If a specific value is set for the **EpSpecificCodecG726r32kbps.DataEnable** parameter and the **EpSpecificCodecG726r32kbps.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG726r32kbpsDataPriority (Config Parameter)

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.DefaultCodecG726r32kbpsDataPriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.300.400

Indicates the priority of this data codec versus the other data codecs. The data codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

If a specific value is set for the **EpSpecificCodecG726r32kbps.DataPriority** parameter and the **EpSpecificCodecG726r32kbps.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG726r32kbpsPayloadType (Config Parameter)

Type	UInt32
Range	96..127
Default	99
Script/CLI	Mipt.DefaultCodecG726r32kbpsPayloadType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.300.500

Determines the actual RTP dynamic payload type used in an initial offer when enabling G.726 at 32 kbps for voice and data transmission.
The payload types available are as per RFC 3551.

If a specific value is set for the **EpSpecificCodecG726r32kbps.PayloadType** parameter and the **EpSpecificCodecG726r32kbps.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG726r32kbpsMinPTime (Config Parameter)

Type	UInt32
Range	10..30
Default	20
Script/CLI	Mipt.DefaultCodecG726r32kbpsMinPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.300.600

Lower boundary for the packetization period of the given codec.
G.726 at 32 kbps -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

If a specific value is set for the **EpSpecificCodecG726r32kbps.MinPTime** parameter and the **EpSpecificCodecG726r32kbps.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG726r32kbpsMaxPTime (Config Parameter)

Type	UInt32
Range	10..30
Default	30
Script/CLI	Mipt.DefaultCodecG726r32kbpsMaxPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.300.700

Upper boundary for the packetization period of the given codec.
G.726 at 32 kbps -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

If a specific value is set for the **EpSpecificCodecG726r32kbps.MaxPTime** parameter and the **EpSpecificCodecG726r32kbps.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

EpSpecificCodecG726r32kbps (Table)

Endpoint specific configuration.

EpId (Index) | Table: EpSpecificCodecG726r32kbps

Type	Text
Range	
Script/CLI	Mipt.EpSpecificCodecG726r32kbps[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.300.800.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificCodecG726r32kbps

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecG726r32kbps[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.300.800.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultCodecG726r32kbpsVoiceEnable**, **DefaultCodecG726r32kbpsVoicePriority**, **DefaultCodecG726r32kbpsDataEnable**, **DefaultCodecG726r32kbpsDataPriority**, **DefaultCodecG726r32kbpsPayloadType**, **DefaultCodecG726r32kbpsMinPTime** and **DefaultCodecG726r32kbpsMaxPTime** parameters.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificCodecG726r32kbps.VoiceEnable**, **EpSpecificCodecG726r32kbps.VoicePriority**, **EpSpecificCodecG726r32kbps.DataEnable**, **EpSpecificCodecG726r32kbps.DataPriority**, **EpSpecificCodecG726r32kbps.PayloadType**, **EpSpecificCodecG726r32kbps.MinPTime** and **EpSpecificCodecG726r32kbps.MaxPTime** parameters.

VoiceEnable (Config Parameter) | Table: EpSpecificCodecG726r32kbps

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecG726r32kbps[].VoiceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.300.800.1.300

Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

- Disable: Disable G.726 at 32 kbps.
- Enable: Enable G.726 at 32 kbps.

G.726 is specified in ITU-T Recommendation G.726: 40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM). It describes the algorithm recommended for conversion of a single 64 kbit/s A-law or U-law PCM channel encoded at 8000 samples/sec to and from a 40, 32, 24, or 16 kbit/s channel. The conversion is applied to the PCM stream using an Adaptive Differential Pulse Code Modulation (ADPCM) transcoding technique.

This codec uses generic voice activity detection. See the **DefaultCodecGenericVoiceActivityDetection** and **EpSpecificCodec.GenericVoiceActivityDetection** parameters.

This codec always uses the RTP transport.

This configuration overrides the default configuration set in the **DefaultCodecG726r32kbpsVoiceEnable** parameter if the **EpSpecificCodecG726r32kbps.EnableConfig** parameter is set to 'Enable'.

VoicePriority (Config Parameter) | Table: EpSpecificCodecG726r32kbps

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.EpSpecificCodecG726r32kbps[].VoicePriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.300.800.1.400

Indicates the priority of this voice codec versus the other voice codecs. The voice codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

This configuration overrides the default configuration set in the **DefaultCodecG726r32kbpsVoicePriority** parameter if the **EpSpecificCodecG726r32kbps.EnableConfig** parameter is set to 'Enable'.

DataEnable (Config Parameter) | Table: EpSpecificCodecG726r32kbps

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecG726r32kbps[].DataEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.300.800.1.500

Indicates if the codec can be selected for data transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

- Disable: Disable G.726 at 32 kbps.
- Enable: Enable G.726 at 32 kbps.

This configuration overrides the default configuration set in the **DefaultCodecG726r32kbpsDataEnable** parameter if the **EpSpecificCodecG726r32kbps.EnableConfig** parameter is set to 'Enable'.

DataPriority (Config Parameter) | Table: EpSpecificCodecG726r32kbps

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.EpSpecificCodecG726r32kbps[].DataPriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.300.800.1.600

Indicates the priority of this data codec versus the other data codecs. The data codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

This configuration overrides the default configuration set in the **DefaultCodecG726r32kbpsDataPriority** parameter if the **EpSpecificCodecG726r32kbps.EnableConfig** parameter is set to 'Enable'.

PayloadType (Config Parameter) | Table: EpSpecificCodecG726r32kbps

Type	UInt32
Range	96..127
Default	99
Script/CLI	Mipt.EpSpecificCodecG726r32kbps[].PayloadType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.300.800.1.700

Determines the actual RTP dynamic payload type used in an initial offer when enabling G.726 at 32 kbps for voice and data transmission.
The payload types available are as per RFC 3551.

This configuration overrides the default configuration set in the **DefaultCodecG726r32kbpsPayloadType** parameter if the **EpSpecificCodecG726r32kbps.EnableConfig** parameter is set to 'Enable'.

MinPTime (Config Parameter) | Table: EpSpecificCodecG726r32kbps

Type	UInt32
Range	10..30
Default	20
Script/CLI	Mipt.EpSpecificCodecG726r32kbps[].MinPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.300.800.1.800

Lower boundary for the packetization period of the given codec.
G.726 at 32 kbps -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

This configuration overrides the default configuration set in the **DefaultCodecG726r32kbpsMinPTime** parameter if the **EpSpecificCodecG726r32kbps.EnableConfig** parameter is set to 'Enable'.

MaxPTime (Config Parameter) | Table: EpSpecificCodecG726r32kbps

Type	UInt32
Range	10..30
Default	30
Script/CLI	Mipt.EpSpecificCodecG726r32kbps[].MaxPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.300.800.1.900

Upper boundary for the packetization period of the given codec.
G.726 at 32 kbps -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

This configuration overrides the default configuration set in the **DefaultCodecG726r32kbpsMaxPTime** parameter if the **EpSpecificCodecG726r32kbps.EnableConfig** parameter is set to 'Enable'.

DefaultCodecG726r40kbpsVoiceEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.DefaultCodecG726r40kbpsVoiceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.400.100

Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

- Disable: Disable G.726 at 40 kbps.
- Enable: Enable G.726 at 40 kbps.

G.726 is specified in ITU-T Recommendation G.726: 40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM). It describes the algorithm recommended for conversion of a single 64 kbit/s A-law or U-law PCM channel encoded at 8000 samples/sec to and from a 40, 32, 24, or 16 kbit/s channel. The conversion is applied to the PCM stream using an Adaptive Differential Pulse Code Modulation (ADPCM) transcoding technique.

This codec uses generic voice activity detection. See the **DefaultCodecGenericVoiceActivityDetection** and **EpSpecificCodec.GenericVoiceActivityDetection** parameters.

This codec always uses the RTP transport.

If a specific value is set for the **EpSpecificCodecG726r40kbps.VoiceEnable** parameter and the **EpSpecificCodecG726r40kbps.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG726r40kbpsVoicePriority (Config Parameter)

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.DefaultCodecG726r40kbpsVoicePriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.400.200

Indicates the priority of this voice codec versus the other voice codecs. The voice codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

If a specific value is set for the **EpSpecificCodecG726r40kbps.VoicePriority** parameter and the **EpSpecificCodecG726r40kbps.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG726r40kbpsDataEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.DefaultCodecG726r40kbpsDataEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.400.300

Indicates if the codec can be selected for data transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

- Disable: Disable G.726 at 40 kbps.
- Enable: Enable G.726 at 40 kbps.

If a specific value is set for the **EpSpecificCodecG726r40kbps.DataEnable** parameter and the **EpSpecificCodecG726r40kbps.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG726r40kbpsDataPriority (Config Parameter)

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.DefaultCodecG726r40kbpsDataPriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.400.400

Indicates the priority of this data codec versus the other data codecs. The data codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

If a specific value is set for the **EpSpecificCodecG726r40kbps.DataPriority** parameter and the **EpSpecificCodecG726r40kbps.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG726r40kbpsPayloadType (Config Parameter)

Type	UInt32
Range	96..127
Default	100
Script/CLI	Mipt.DefaultCodecG726r40kbpsPayloadType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.400.500

Setermines the actual RTP dynamic payload type used in an initial offer when enabling G.726 at 40 kbps for voice and data transmission.
The payload types available are as per RFC 3551.

If a specific value is set for the **EpSpecificCodecG726r40kbps.PayloadType** parameter and the **EpSpecificCodecG726r40kbps.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG726r40kbpsMinPTime (Config Parameter)

Type	UInt32
Range	10..30
Default	20
Script/CLI	Mipt.DefaultCodecG726r40kbpsMinPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.400.600

Lower boundary for the packetization period of the given codec.
G.726 at 40 kbps -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

If a specific value is set for the **EpSpecificCodecG726r40kbps.MinPTime** parameter and the **EpSpecificCodecG726r40kbps.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG726r40kbpsMaxPTime (Config Parameter)

Type	UInt32
Range	10..30
Default	30
Script/CLI	Mipt.DefaultCodecG726r40kbpsMaxPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.400.700

Upper boundary for the packetization period of the given codec.
G.726 at 40 kbps -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

If a specific value is set for the **EpSpecificCodecG726r40kbps.MaxPTime** parameter and the **EpSpecificCodecG726r40kbps.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

EpSpecificCodecG726r40kbps (Table)

Endpoint specific configuration.

EpId (Index) | Table: EpSpecificCodecG726r40kbps

Type	Text
Range	
Script/CLI	Mipt.EpSpecificCodecG726r40kbps[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.400.800.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificCodecG726r40kbps

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecG726r40kbps[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.400.800.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultCodecG726r40kbpsVoiceEnable**, **DefaultCodecG726r40kbpsVoicePriority**, **DefaultCodecG726r40kbpsDataEnable**, **DefaultCodecG726r40kbpsDataPriority**, **DefaultCodecG726r40kbpsPayloadType**, **DefaultCodecG726r40kbpsMinPTime** and **DefaultCodecG726r40kbpsMaxPTime** parameters.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificCodecG726r40kbps.VoiceEnable**, **EpSpecificCodecG726r40kbps.VoicePriority**, **EpSpecificCodecG726r40kbps.DataEnable**, **EpSpecificCodecG726r40kbps.DataPriority**, **EpSpecificCodecG726r40kbps.PayloadType**, **EpSpecificCodecG726r40kbps.MinPTime** and **EpSpecificCodecG726r40kbps.MaxPTime** parameter.

VoiceEnable (Config Parameter) | Table: EpSpecificCodecG726r40kbps

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecG726r40kbps[].VoiceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.400.800.1.300

Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

- Disable: Disable G.726 at 40 kbps.
- Enable: Enable G.726 at 40 kbps.

G.726 is specified in ITU-T Recommendation G.726: 40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM). It describes the algorithm recommended for conversion of a single 64 kbit/s A-law or U-law PCM channel encoded at 8000 samples/sec to and from a 40, 32, 24, or 16 kbit/s channel. The conversion is applied to the PCM stream using an Adaptive Differential Pulse Code Modulation (ADPCM) transcoding technique.

This codec uses generic voice activity detection. See the **DefaultCodecGenericVoiceActivityDetection** and **EpSpecificCodec.GenericVoiceActivityDetection** parameters.

This codec always uses the RTP transport.

This configuration overrides the default configuration set in the **DefaultCodecG726r40kbpsVoiceEnable** parameter if the **EpSpecificCodecG726r40kbps.EnableConfig** parameter is set to 'Enable'.

VoicePriority (Config Parameter) | Table: EpSpecificCodecG726r40kbps

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.EpSpecificCodecG726r40kbps[].VoicePriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.400.800.1.400

Indicates the priority of this voice codec versus the other voice codecs. The voice codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

This configuration overrides the default configuration set in the **DefaultCodecG726r40kbpsVoicePriority** parameter if the **EpSpecificCodecG726r40kbps.EnableConfig** parameter is set to 'Enable'.

DataEnable (Config Parameter) | Table: EpSpecificCodecG726r40kbps

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecG726r40kbps[].DataEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.400.800.1.500

Indicates if the codec can be selected for data transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

- Disable: Disable G.726 at 40 kbps.
- Enable: Enable G.726 at 40 kbps.

This configuration overrides the default configuration set in the **DefaultCodecG726r40kbpsDataEnable** parameter if the **EpSpecificCodecG726r40kbps.EnableConfig** parameter is set to 'Enable'.

DataPriority (Config Parameter) | Table: EpSpecificCodecG726r40kbps

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.EpSpecificCodecG726r40kbps[].DataPriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.400.800.1.600

Indicates the priority of this data codec versus the other data codecs. The data codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

This configuration overrides the default configuration set in the **DefaultCodecG726r40kbpsDataPriority** parameter if the **EpSpecificCodecG726r40kbps.EnableConfig** parameter is set to 'Enable'.

PayloadType (Config Parameter) | Table: EpSpecificCodecG726r40kbps

Type	UInt32
Range	96..127
Default	100
Script/CLI	Mipt.EpSpecificCodecG726r40kbps[].PayloadType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.400.800.1.700

Determines the actual RTP dynamic payload type used in an initial offer when enabling G.726 at 40 kbps for voice and data transmission.
The payload types available are as per RFC 3551.

This configuration overrides the default configuration set in the **DefaultCodecG726r40kbpsPayloadType** parameter if the **EpSpecificCodecG726r40kbps.EnableConfig** parameter is set to 'Enable'.

MinPTime (Config Parameter) | Table: EpSpecificCodecG726r40kbps

Type	UInt32
Range	10..30
Default	20
Script/CLI	Mipt.EpSpecificCodecG726r40kbps[].MinPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.400.800.1.800

Lower boundary for the packetization period of the given codec.
G.726 at 40 kbps -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

This configuration overrides the default configuration set in the **DefaultCodecG726r40kbpsMinPTime** parameter if the **EpSpecificCodecG726r40kbps.EnableConfig** parameter is set to 'Enable'.

MaxPTime (Config Parameter) | Table: EpSpecificCodecG726r40kbps

Type	UInt32
Range	10..30
Default	30
Script/CLI	Mipt.EpSpecificCodecG726r40kbps[].MaxPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.500.400.800.1.900

Upper boundary for the packetization period of the given codec.
G.726 at 40 kbps -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

This configuration overrides the default configuration set in the **DefaultCodecG726r40kbpsMaxPTime** parameter if the **EpSpecificCodecG726r40kbps.EnableConfig** parameter is set to 'Enable'.

DefaultCodecG729VoiceEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Mipt.DefaultCodecG729VoiceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.600.100

Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.
G729 is specified in ITU-T Recommendation G.729, Coding of speech at 8 kbit/s using conjugate structure-algebraic code excited linear prediction (CS-ACELP). For all data rates, the sampling frequency (and RTP timestamp clock rate) is 8000 Hz. A voice activity detector (VAD) and comfort noise generator (CNG) algorithm in Annex B of G.729 is RECOMMENDED for digital simultaneous voice and data applications and can be used in conjunction with G.729 or G.729 Annex A. A G.729 or G.729 Annex A frame contains 10 octets, while the G.729 Annex B comfort noise frame occupies 2 octets.

This codec always uses the RTP transport.

If a specific value is set for the **EpSpecificCodecG729.VoiceEnable** parameter and the **EpSpecificCodecG729.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG729VoicePriority (Config Parameter)

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.DefaultCodecG729VoicePriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.600.200

Indicates the priority of this voice codec versus the other voice codecs. The voice codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

If a specific value is set for the **EpSpecificCodecG729.VoicePriority** parameter and the **EpSpecificCodecG729.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG729MinPTime (Config Parameter)

Type	UInt32
Range	20..20 | 30..30 | 40..40 | 50..50 | 60..60 | 70..70 | 80..80
Default	20
Script/CLI	Mipt.DefaultCodecG729MinPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.600.300

Lower boundary for the packetization period of the given codec.
G.729 -> (20 ms|30 ms|40 ms|50 ms|60 ms|70 ms|80 ms)

For reception, the range is extended from 10 ms to 100 ms with increments of 10 ms only if the stream is not encrypted (SRTP).

If a specific value is set for the **EpSpecificCodecG729.MinPTime** parameter and the **EpSpecificCodecG729.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG729MaxPTime (Config Parameter)

Type	UInt32
Range	20..20 | 30..30 | 40..40 | 50..50 | 60..60 | 70..70 | 80..80
Default	80
Script/CLI	Mipt.DefaultCodecG729MaxPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.600.400

Upper boundary for the packetization period of the given codec.
G.729 -> (20 ms|30 ms|40 ms|50 ms|60 ms|70 ms|80 ms)

For reception, the range is extended from 10 ms to 100 ms with increments of 10 ms only if the stream is not encrypted (SRTP).

If a specific value is set for the **EpSpecificCodecG729.MaxPTime** parameter and the **EpSpecificCodecG729.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecG729VoiceActivityDetection (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Mipt.DefaultCodecG729VoiceActivityDetection
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.600.500

If Voice Activity Detection (VAD) is enabled, then speech frames are only sent during talkspurts (periods of audio activity).
During silence periods, no speech frames are sent, but Comfort Noise (CN) packets containing information about background noise may be sent in accordance with annex B of G.729.

- Disable: G.729 uses annex A only.
- Enable: G.729 annex A is used with annex B.

If a specific value is set for the **EpSpecificCodecG729.VoiceActivityDetection** parameter and the **EpSpecificCodecG729.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

EpSpecificCodecG729 (Table)

Endpoint specific configuration.

EpId (Index) | Table: EpSpecificCodecG729

Type	Text
Range	
Script/CLI	Mipt.EpSpecificCodecG729[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.600.600.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificCodecG729

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecG729[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.600.600.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultCodecG729VoiceEnable**, **DefaultCodecG729VoicePriority**, **DefaultCodecG729MinPTime**, **DefaultCodecG729MaxPTime** and **DefaultCodecG729VoiceActivityDetection** parameters.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificCodecG729.EnableVoice EpSpecificCodecG729.VoicePriority**, **EpSpecificCodecG729.MinPTime**, **EpSpecificCodecG729.MaxPTime** and **EpSpecificCodecG729.VoiceActivityDetection** parameters.

VoiceEnable (Config Parameter) | Table: EpSpecificCodecG729

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Mipt.EpSpecificCodecG729[].VoiceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.600.600.1.300

Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.
G729 is specified in ITU-T Recommendation G.729, Coding of speech at 8 kbit/s using conjugate structure-algebraic code excited linear prediction (CS-ACELP). For all data rates, the sampling frequency (and RTP timestamp clock rate) is 8000 Hz. A voice activity detector (VAD) and comfort noise generator (CNG) algorithm in Annex B of G.729 is RECOMMENDED for digital simultaneous voice and data applications and can be used in conjunction with G.729 or G.729 Annex A. A G.729 or G.729 Annex A frame contains 10 octets, while the G.729 Annex B comfort noise frame occupies 2 octets.

This codec always uses the RTP transport.

This configuration overrides the default configuration set in the **DefaultCodecG729VoiceEnable** parameter if the **EpSpecificCodecG729.EnableConfig** parameter is set to 'Enable'.

VoicePriority (Config Parameter) | Table: EpSpecificCodecG729

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.EpSpecificCodecG729[].VoicePriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.600.600.1.400

Indicates the priority of this voice codec versus the other voice codecs. The voice codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

This configuration overrides the default configuration set in the **DefaultCodecG729VoicePriority** parameter if the **EpSpecificCodecG729.EnableConfig** parameter is set to 'Enable'.

MinPTime (Config Parameter) | Table: EpSpecificCodecG729

Type	UInt32
Range	20..20 | 30..30 | 40..40 | 50..50 | 60..60 | 70..70 | 80..80
Default	20
Script/CLI	Mipt.EpSpecificCodecG729[].MinPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.600.600.1.500

Lower boundary for the packetization period of the given codec.
G.729 -> (20 ms|30 ms|40 ms|50 ms|60 ms|70 ms|80 ms)

For reception, the range is extended from 10 ms to 100 ms with increments of 10 ms only if the stream is not encrypted (SRTP).

This configuration overrides the default configuration set in the **DefaultCodecG729MinPTime** parameter if the **EpSpecificCodecG729.EnableConfig** parameter is set to 'Enable'.

MaxPTime (Config Parameter) | Table: EpSpecificCodecG729

Type	UInt32
Range	20..20 | 30..30 | 40..40 | 50..50 | 60..60 | 70..70 | 80..80
Default	80
Script/CLI	Mipt.EpSpecificCodecG729[].MaxPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.600.600.1.600

Upper boundary for the packetization period of the given codec.
G.729 -> (20 ms|30 ms|40 ms|50 ms|60 ms|70 ms|80 ms)

For reception, the range is extended from 10 ms to 100 ms with increments of 10 ms only if the stream is not encrypted (SRTP).

This configuration overrides the default configuration set in the **DefaultCodecG729MaxPTime** parameter if the **EpSpecificCodecG729.EnableConfig** parameter is set to 'Enable'.

VoiceActivityDetection (Config Parameter) | Table: EpSpecificCodecG729

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Mipt.EpSpecificCodecG729[].VoiceActivityDetection
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.600.600.1.700

If Voice Activity Detection (VAD) is enabled, then speech frames are only sent during talkspurts (periods of audio activity).
During silence periods, no speech frames are sent, but Comfort Noise (CN) packets containing information about background noise may be sent in accordance with annex B of G.729.

- Disable: G.729 uses annex A only.
- Enable: G.729 annex A is used with annex B.

This configuration overrides the default configuration set in the **DefaultCodecG729VoiceActivityDetection** parameter if the **EpSpecificCodecG729.EnableConfig** parameter is set to 'Enable'.

DefaultCodecT38DataEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Mipt.DefaultCodecT38DataEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.700.100

If enabled, the T.38 protocol is used for fax transmission.
If a specific value is set for the **EpSpecificCodecT38.DataEnable** parameter and the **EpSpecificCodecT38.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecT38DataPriority (Config Parameter)

Type	UInt32
Range	10..10
Default	10
Script/CLI	Mipt.DefaultCodecT38DataPriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.700.200

Indicates the priority of this data codec versus the other data codecs. The data codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

If a specific value is set for the **EpSpecificCodecT38.DataPriority** parameter and the **EpSpecificCodecT38.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecT38RedundancyLevel (Config Parameter)

Type	UInt32
Range	1..5
Default	3
Script/CLI	Mipt.DefaultCodecT38RedundancyLevel
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.700.400

Number of redundancy packets. This is the standard redundancy offered by T.38.
Refer to the **DefaultCodecT38FinalFramesRedundancy** parameter for additional T.38 reliability options.

If a specific value is set for the **EpSpecificCodecT38.RedundancyLevel** parameter and the **EpSpecificCodecT38.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecT38FinalFramesRedundancy (Config Parameter)

Type	UInt32
Range	0..3
Default	0
Script/CLI	Mipt.DefaultCodecT38FinalFramesRedundancy
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.700.500

Defines the number of times T.38 packets will be retransmitted. This only applies to the T.38 packets where the PrimaryUDPTL contains the following T.38 data type: HDLC_SIG_END, HDLC_FCS_OK_SIG_END, HDLC_FCS_BAD_SIG_END and T4_NON_ECM_SIG_END.
Refer to the **DefaultCodecT38ProtectionLevel** parameter for standard T.38 reliability options.

DefaultCodecT38NoSignalEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.DefaultCodecT38NoSignalEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.700.600

Enables/disables the sending of T.38 no-signal packets. When enabled, the unit ensures that, during a T.38 fax transmission, data is sent out at least every time the **DefaultCodecT38NoSignalTimeout** delay expires. In the absence of meaningful data to send, no-signal packets are output.

DefaultCodecT38NoSignalTimeout (Config Parameter)

Type	UInt32
Range	1..2147483647
Default	1
Script/CLI	Mipt.DefaultCodecT38NoSignalTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.700.700

The period, in seconds, at which no-signal packets are sent during a T.38 transmission, in the absence of valid data.

DefaultCodecT38DetectionThreshold (Config Parameter)

Type	Enum
Range	Default(100) | Low(200) | Lowest(300)
Default	Default
Script/CLI	Mipt.DefaultCodecT38DetectionThreshold
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.700.750

Sets the T.38 input signal detection threshold. Lowering the threshold allows detecting lower amplitude fax signals.

- Default: (-26dB)
- Low: (-31dB)
- Lowest: (-43dB)

If a specific value is set for the **EpSpecificCodecT38.DetectionThreshold** parameter and the **EpSpecificCodecT38.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

EpSpecificCodecT38 (Table)

Endpoint specific configuration.

EpId (Index) | Table: EpSpecificCodecT38

Type	Text
Range	
Script/CLI	Mipt.EpSpecificCodecT38[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.700.800.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificCodecT38

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecT38[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.700.800.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultCodecT38DataEnable**, **DefaultCodecT38DataPriority** and **DefaultCodecT38RedundancyLevel** parameters.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificCodecT38.DataEnable**, **EpSpecificCodecT38.DataPriority** and **EpSpecificCodecT38.RedundancyLevel** parameters.

DataEnable (Config Parameter) | Table: EpSpecificCodecT38

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Mipt.EpSpecificCodecT38[].DataEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.700.800.1.300

If enabled, the T.38 protocol is used for fax transmission.

This configuration overrides the default configuration set in the **DefaultCodecT38DataEnable** parameter if the **EpSpecificCodecT38.EnableConfig** parameter is set to 'Enable'.

DataPriority (Config Parameter) | Table: EpSpecificCodecT38

Type	UInt32
Range	10..10
Default	10
Script/CLI	Mipt.EpSpecificCodecT38[].DataPriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.700.800.1.400

Indicates the priority of this data codec versus the other data codecs. The data codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

This configuration overrides the default configuration set in the **DefaultCodecT38DataPriority** parameter if the **EpSpecificCodecT38.EnableConfig** parameter is set to 'Enable'.

RedundancyLevel (Config Parameter) | Table: EpSpecificCodecT38

Type	UInt32
Range	1..5
Default	3
Script/CLI	Mipt.EpSpecificCodecT38[].RedundancyLevel
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.700.800.1.600

Number of redundancy packets. This is the standard redundancy offered by T.38.
Refer to the **DefaultCodecT38FinalFramesRedundancy** parameter for additional T.38 reliability options.

This configuration overrides the default configuration set in the **DefaultCodecT38RedundancyLevel** parameter if the **EpSpecificCodecT38.EnableConfig** parameter is set to 'Enable'.

DetectionThreshold (Config Parameter) | Table: EpSpecificCodecT38

Type	Enum
Range	Default(100) | Low(200) | Lowest(300)
Default	Default
Script/CLI	Mipt.EpSpecificCodecT38[].DetectionThreshold
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.700.800.1.700

Sets the T.38 input signal detection threshold. Lowering the threshold allows detecting lower amplitude fax signals.

- Default: (-26dB)
- Low: (-31dB)
- Lowest: (-43dB)

This configuration overrides the default configuration set in the **DefaultCodecT38DetectionThreshold** parameter if the **EpSpecificCodecT38.EnableConfig** parameter is set to 'Enable'.

DefaultCodecClearModeVoiceEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.DefaultCodecClearModeVoiceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.800.100

Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.
Clear Mode is a method to carry 64 kbit/s channel data transparently in RTP packets as defined in RFC 4040.

This codec always uses the RTP transport.

If a specific value is set for the **EpSpecificCodecClearMode.VoiceEnable** parameter and the **EpSpecificCodecClearMode.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecClearModeVoicePriority (Config Parameter)

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.DefaultCodecClearModeVoicePriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.800.200

Indicates the priority of this voice codec versus the other voice codecs. The voice codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

If a specific value is set for the **EpSpecificCodecClearMode.VoicePriority** parameter and the **EpSpecificCodecClearMode.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecClearModeDataEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.DefaultCodecClearModeDataEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.800.300

If enabled, the Clear Mode protocol is used for data transmission.
The data transmission for this codec can be triggered by the detection of a fax/modem tone or if the properties of the call indicate that it was for data.

Clear Mode is a method to carry 64 kbit/s channel data transparently in RTP packets as defined in RFC 4040.

This codec always uses the RTP transport.

If a specific value is set for the **EpSpecificCodecClearMode.DataEnable** parameter and the **EpSpecificCodecClearMode.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecClearModeDataPriority (Config Parameter)

Type	UInt32
Range	0..10
Default	10
Script/CLI	Mipt.DefaultCodecClearModeDataPriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.800.400

Indicates the priority of this data codec versus the other data codecs. The data codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

If a specific value is set for the **EpSpecificCodecClearMode.DataPriority** parameter and the **EpSpecificCodecClearMode.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecClearModePayloadType (Config Parameter)

Type	UInt32
Range	96..127
Default	124
Script/CLI	Mipt.DefaultCodecClearModePayloadType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.800.500

When enabling Clear Mode for voice and data transmission, this parameter determines the actual RTP dynamic payload type used in an initial offer.
The payload types available are as per RFC 3551.

If a specific value is set for the **EpSpecificCodecClearMode.PayloadType** parameter and the **EpSpecificCodecClearMode.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecClearModeMinPTime (Config Parameter)

Type	UInt32
Range	10..30
Default	10
Script/CLI	Mipt.DefaultCodecClearModeMinPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.800.600

Lower boundary for the packetization period of the given codec.
Clear Mode -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

If a specific value is set for the **EpSpecificCodecClearMode.MinPTime** parameter and the **EpSpecificCodecClearMode.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecClearModeMaxPTime (Config Parameter)

Type	UInt32
Range	10..30
Default	30
Script/CLI	Mipt.DefaultCodecClearModeMaxPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.800.700

Upper boundary for the packetization period of the given codec.
Clear Mode -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

If a specific value is set for the **EpSpecificCodecClearMode.MaxPTime** parameter and the **EpSpecificCodecClearMode.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

EpSpecificCodecClearMode (Table)

Endpoint specific configuration.

EpId (Index) | Table: EpSpecificCodecClearMode

Type	Text
Range	
Script/CLI	Mipt.EpSpecificCodecClearMode[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.800.800.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificCodecClearMode

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecClearMode[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.800.800.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultCodecClearModeVoiceEnable**, **DefaultCodecClearModeVoicePriority**, **DefaultCodecClearModeDataEnable**, **DefaultCodecClearModeDataPriority**, **DefaultCodecClearModePayloadType**, **DefaultCodecClearModeMinPTime** and **DefaultCodecClearModeMaxPTime**.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificCodecClearMode.VoiceEnable**, **EpSpecificCodecClearMode.VoicePriority**, **EpSpecificCodecClearMode.DataPriority**, **EpSpecificCodecClearMode.DataPriority**, **EpSpecificCodecClearMode.PayloadType**, **EpSpecificCodecClearMode.MinPTime** and **EpSpecificCodecClearMode.MaxPTime**.

VoiceEnable (Config Parameter) | Table: EpSpecificCodecClearMode

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecClearMode[].VoiceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.800.800.1.300

Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.
Clear Mode is a method to carry 64 kbit/s channel data transparently in RTP packets as defined in RFC 4040.

This codec always uses the RTP transport.

This configuration overrides the default configuration set in the **DefaultCodecClearModeVoiceEnable** parameter if the **EpSpecificCodecClearMode.EnableConfig** parameter is set to 'Enable'.

VoicePriority (Config Parameter) | Table: EpSpecificCodecClearMode

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.EpSpecificCodecClearMode[].VoicePriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.800.800.1.400

Indicates the priority of this voice codec versus the other voice codecs. The voice codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

This configuration overrides the default configuration set in the **DefaultCodecClearModeVoicePriority** parameter if the **EpSpecificCodecClearMode.EnableConfig** parameter is set to 'Enable'.

DataEnable (Config Parameter) | Table: EpSpecificCodecClearMode

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecClearMode[].DataEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.800.800.1.500

If enabled, the Clear Mode protocol is used for fax transmission.
This configuration overrides the default configuration set in the **DefaultCodecClearModeDataEnable** parameter if the **EpSpecificCodecClearMode.EnableConfig** parameter is set to 'Enable'.

DataPriority (Config Parameter) | Table: EpSpecificCodecClearMode

Type	UInt32
Range	0..10
Default	10
Script/CLI	Mipt.EpSpecificCodecClearMode[].DataPriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.800.800.1.600

Indicates the priority of this data codec versus the other data codecs. The data codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

This configuration overrides the default configuration set in the **DefaultCodecClearModeDataPriority** parameter if the **EpSpecificCodecClearMode.EnableConfig** parameter is set to 'Enable'.

PayloadType (Config Parameter) | Table: EpSpecificCodecClearMode

Type	UInt32
Range	96..127
Default	124
Script/CLI	Mipt.EpSpecificCodecClearMode[].PayloadType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.800.800.1.700

When enabling Clear Mode for voice and data transmission, this parameter determines the actual RTP dynamic payload type used in an initial offer.
The payload types available are as per RFC 3551.

This configuration overrides the default configuration set in the **DefaultCodecClearModePayloadType** parameter if the **EpSpecificCodecClearMode.EnableConfig** parameter is set to 'Enable'.

MinPTime (Config Parameter) | Table: EpSpecificCodecClearMode

Type	UInt32
Range	10..30
Default	10
Script/CLI	Mipt.EpSpecificCodecClearMode[].MinPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.800.800.1.800

Lower boundary for the packetization period of the given codec.
Clear Mode -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

This configuration overrides the default configuration set in the **DefaultCodecClearModeMinPTime** parameter if the **EpSpecificCodecClearMode.EnableConfig** parameter is set to 'Enable'.

MaxPTime (Config Parameter) | Table: EpSpecificCodecClearMode

Type	UInt32
Range	10..30
Default	30
Script/CLI	Mipt.EpSpecificCodecClearMode[].MaxPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.800.800.1.900

Upper boundary for the packetization period of the given codec.
Clear Mode -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

This configuration overrides the default configuration set in the **DefaultCodecClearModeMaxPTime** parameter if the **EpSpecificCodecClearMode.EnableConfig** parameter is set to 'Enable'.

DefaultCodecClearChannelVoiceEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.DefaultCodecClearChannelVoiceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.900.100

Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.
Clear Channel is a method to carry 64 kbit/s channel data transparently in RTP packets. This codec behaves like the Clear Mode as defined in RFC 4040, but it uses 'X-CLEAR-CHANNEL' instead of 'CLEARMODE' in the codec negotiation.

This codec always uses the RTP transport.

If a specific value is set for the **EpSpecificCodecClearChannel.VoiceEnable** parameter and the **EpSpecificCodecClearChannel.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecClearChannelVoicePriority (Config Parameter)

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.DefaultCodecClearChannelVoicePriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.900.200

Indicates the priority of this voice codec versus the other voice codecs. The voice codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

If a specific value is set for the **EpSpecificCodecClearChannel.VoicePriority** parameter and the **EpSpecificCodecClearChannel.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecClearChannelDataEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.DefaultCodecClearChannelDataEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.900.300

If enabled, the Clear Channel protocol is used for data transmission.
Clear Channel is a method to carry 64 kbit/s channel data transparently in RTP packets. This codec behaves like the Clear Mode as defined in RFC 4040, but it uses 'X-CLEAR-CHANNEL' instead of 'CLEARMODE' in the codec negotiation.

Clear Channel is a method to carry 64 kbit/s channel data transparently in RTP packets as defined in RFC 4040.

This codec always uses the RTP transport.

If a specific value is set for the **EpSpecificCodecClearChannel.DataEnable** parameter and the **EpSpecificCodecClearChannel.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecClearChannelDataPriority (Config Parameter)

Type	UInt32
Range	0..10
Default	10
Script/CLI	Mipt.DefaultCodecClearChannelDataPriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.900.400

Indicates the priority of this data codec versus the other data codecs. The data codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

If a specific value is set for the **EpSpecificCodecClearChannel.DataPriority** parameter and the **EpSpecificCodecClearChannel.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecClearChannelPayloadType (Config Parameter)

Type	UInt32
Range	96..127
Default	125
Script/CLI	Mipt.DefaultCodecClearChannelPayloadType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.900.500

When enabling Clear Channel for voice and data transmission, this parameter determines the actual RTP dynamic payload type used in an initial offer.
The payload types available are as per RFC 3551.

If a specific value is set for the **EpSpecificCodecClearChannel.PayloadType** parameter and the **EpSpecificCodecClearChannel.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecClearChannelMinPTime (Config Parameter)

Type	UInt32
Range	10..30
Default	10
Script/CLI	Mipt.DefaultCodecClearChannelMinPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.900.600

Lower boundary for the packetization period of the given codec.
Clear Channel -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

If a specific value is set for the **EpSpecificCodecClearChannel.MinPTime** parameter and the **EpSpecificCodecClearChannel.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecClearChannelMaxPTime (Config Parameter)

Type	UInt32
Range	10..30
Default	30
Script/CLI	Mipt.DefaultCodecClearChannelMaxPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.900.700

Upper boundary for the packetization period of the given codec.
Clear Channel -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

If a specific value is set for the **EpSpecificCodecClearChannel.MaxPTime** parameter and the **EpSpecificCodecClearChannel.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

EpSpecificCodecClearChannel (Table)

Endpoint specific configuration.

EpId (Index) | Table: EpSpecificCodecClearChannel

Type	Text
Range	
Script/CLI	Mipt.EpSpecificCodecClearChannel[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.900.800.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificCodecClearChannel

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecClearChannel[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.900.800.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultCodecClearChannelVoiceEnable**, **DefaultCodecClearChannelVoicePriority**, **DefaultCodecClearChannelDataEnable**, **DefaultCodecClearChannelDataPriority**, **DefaultCodecClearChannelPayloadType**, **DefaultCodecClearChannelMinPTime** and **DefaultCodecClearChannelMaxPTime**.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificCodecClearChannel.VoiceEnable**, **EpSpecificCodecClearChannel.VoicePriority**, **EpSpecificCodecClearChannel.DataPriority**, **EpSpecificCodecClearChannel.DataPriority**, **EpSpecificCodecClearChannel.PayloadType**, **EpSpecificCodecClearChannel.MinPTime** and **EpSpecificCodecClearChannel.MaxPTime**.

VoiceEnable (Config Parameter) | Table: EpSpecificCodecClearChannel

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecClearChannel[].VoiceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.900.800.1.300

Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.
X Clear Cahnnel is a method to carry 64 kbit/s channel data transparently in RTP packets. This codec behaves like the Clear Mode as defined in RFC 4040, but it uses 'X-CLEAR-CHANNEL' instead of 'CLEARMODE' the in codec negotiation.

This codec always uses the RTP transport.

This configuration overrides the default configuration set in the **DefaultCodecClearChannelVoiceEnable** parameter if the **EpSpecificCodecClearChannel.EnableConfig** parameter is set to 'Enable'.

VoicePriority (Config Parameter) | Table: EpSpecificCodecClearChannel

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.EpSpecificCodecClearChannel[].VoicePriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.900.800.1.400

Indicates the priority of this voice codec versus the other voice codecs. The voice codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

This configuration overrides the default configuration set in the **DefaultCodecClearChannelVoicePriority** parameter if the **EpSpecificCodecClearChannel.EnableConfig** parameter is set to 'Enable'.

DataEnable (Config Parameter) | Table: EpSpecificCodecClearChannel

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecClearChannel[].DataEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.900.800.1.500

If enabled, the Clear Channel protocol is used for fax transmission.
Clear Channel is a method to carry 64 kbit/s channel data transparently in RTP packets. This codec behaves like the Clear Mode as defined in RFC 4040, but it uses 'X-CLEAR-CHANNEL' instead of 'CLEARMODE' the in codec negotiation.

This configuration overrides the default configuration set in the **DefaultCodecClearChannelDataEnable** parameter if the **EpSpecificCodecClearChannel.EnableConfig** parameter is set to 'Enable'.

DataPriority (Config Parameter) | Table: EpSpecificCodecClearChannel

Type	UInt32
Range	0..10
Default	10
Script/CLI	Mipt.EpSpecificCodecClearChannel[].DataPriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.900.800.1.600

Indicates the priority of this data codec versus the other data codecs. The data codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

This configuration overrides the default configuration set in the **DefaultCodecClearChannelDataPriority** parameter if the **EpSpecificCodecClearChannel.EnableConfig** parameter is set to 'Enable'.

PayloadType (Config Parameter) | Table: EpSpecificCodecClearChannel

Type	UInt32
Range	96..127
Default	125
Script/CLI	Mipt.EpSpecificCodecClearChannel[].PayloadType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.900.800.1.700

When enabling Clear Channel for voice and data transmission, this parameter determines the actual RTP dynamic payload type used in an initial offer.
The payload types available are as per RFC 3551.

This configuration overrides the default configuration set in the **DefaultCodecClearChannelPayloadType** parameter if the **EpSpecificCodecClearChannel.EnableConfig** parameter is set to 'Enable'.

MinPTime (Config Parameter) | Table: EpSpecificCodecClearChannel

Type	UInt32
Range	10..30
Default	10
Script/CLI	Mipt.EpSpecificCodecClearChannel[].MinPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.900.800.1.800

Lower boundary for the packetization period of the given codec.
Clear Channel -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

This configuration overrides the default configuration set in the **DefaultCodecClearChannelMinPTime** parameter if the **EpSpecificCodecClearChannel.EnableConfig** parameter is set to 'Enable'.

MaxPTime (Config Parameter) | Table: EpSpecificCodecClearChannel

Type	UInt32
Range	10..30
Default	30
Script/CLI	Mipt.EpSpecificCodecClearChannel[].MaxPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.900.800.1.900

Upper boundary for the packetization period of the given codec.
Clear Channel -> (10 ms..30 ms)

This value is expressed in ms, with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

This configuration overrides the default configuration set in the **DefaultCodecClearChannelMaxPTime** parameter if the **EpSpecificCodecClearChannel.EnableConfig** parameter is set to 'Enable'.

DefaultCodecXCCDVoiceEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.DefaultCodecXCCDVoiceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.1000.100

Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.
X-CCD clear channel is a method to carry 64 kbit/s channel data transparently in RTP packets as defined in RFC 4040.

This codec always uses the RTP transport.

If a specific value is set for the **EpSpecificCodecXCCD.VoiceEnable** parameter and the **EpSpecificCodecXCCD.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecXCCDVoicePriority (Config Parameter)

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.DefaultCodecXCCDVoicePriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.1000.200

Indicates the priority of this voice codec versus the other voice codecs. The voice codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

If a specific value is set for the **EpSpecificCodecXCCD.VoicePriority** parameter and the **EpSpecificCodecXCCD.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecXCCDDataEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.DefaultCodecXCCDDataEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.1000.300

If enabled, the X-CCD Clear Channel protocol is used for data transmission.
The data transmission for this codec can be triggered by the detection of a fax/modem tone or if the properties of the call indicate that it was for data.

X-CCD Clear Channel is a method to carry 64 kbit/s channel data transparently in RTP packets as defined in RFC 4040.

This codec always uses the RTP transport.

If a specific value is set for the **EpSpecificCodecXCCD.DataEnable** parameter and the **EpSpecificCodecXCCD.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecXCCDDataPriority (Config Parameter)

Type	UInt32
Range	0..10
Default	10
Script/CLI	Mipt.DefaultCodecXCCDDataPriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.1000.400

Indicates the priority of this data codec versus the other data codecs. The data codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

If a specific value is set for the **EpSpecificCodecXCCD.DataPriority** parameter and the **EpSpecificCodecXCCD.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecXCCDPayloadType (Config Parameter)

Type	UInt32
Range	96..127
Default	126
Script/CLI	Mipt.DefaultCodecXCCDPayloadType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.1000.500

When enabling X-CCD Clear Channel for voice and data transmission, this parameter determines the actual RTP dynamic payload type used in an initial offer.
The payload types available are as per RFC 3551.

If a specific value is set for the **EpSpecificCodecXCCD.PayloadType** parameter and the **EpSpecificCodecXCCD.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecXCCDMinPTime (Config Parameter)

Type	UInt32
Range	10..30
Default	10
Script/CLI	Mipt.DefaultCodecXCCDMinPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.1000.600

Lower boundary for the packetization period of the given codec.
X-CCD Clear Channel -> (10 ms..30 ms)

This value is expressed in ms, with increments of 1 ms.

If a specific value is set for the **EpSpecificCodecXCCD.MinPTime** parameter and the **EpSpecificCodecXCCD.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultCodecXCCDMaxPTime (Config Parameter)

Type	UInt32
Range	10..30
Default	30
Script/CLI	Mipt.DefaultCodecXCCDMaxPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.1000.700

Upper boundary for the packetization period of the given codec.
X-CCD Clear Channel -> (10 ms..30 ms)

This value is expressed in ms, with increments of 1 ms.

If a specific value is set for the **EpSpecificCodecXCCD.MaxPTime** parameter and the **EpSpecificCodecXCCD.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

EpSpecificCodecXCCD (Table)

Endpoint specific configuration.

EpId (Index) | Table: EpSpecificCodecXCCD

Type	Text
Range	
Script/CLI	Mipt.EpSpecificCodecXCCD[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.1000.800.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificCodecXCCD

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecXCCD[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.1000.800.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultCodecXCCDVoiceEnable**, **DefaultCodecXCCDVoicePriority**, **DefaultCodecXCCDDataEnable**, **DefaultCodecXCCDDataPriority**, **DefaultCodecXCCDPayloadType**, **DefaultCodecXCCDMinPTime** and **DefaultCodecXCCDMaxPTime**.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificCodecXCCD.VoiceEnable**, **EpSpecificCodecXCCD.VoicePriority**, **EpSpecificCodecXCCD.DataPriority**, **EpSpecificCodecXCCD.DataPriority**, **EpSpecificCodecXCCD.PayloadType**, **EpSpecificCodecXCCD.MinPTime** and **EpSpecificCodecXCCD.MaxPTime**.

VoiceEnable (Config Parameter) | Table: EpSpecificCodecXCCD

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecXCCD[].VoiceEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.1000.800.1.300

Indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.
X-CCD Clear Channel is a method to carry 64 kbit/s channel data transparently in RTP packets as defined in RFC 4040.

This codec always uses the RTP transport.

This configuration overrides the default configuration set in the **DefaultCodecXCCDVoiceEnable** parameter if the **EpSpecificCodecXCCD.EnableConfig** parameter is set to 'Enable'.

VoicePriority (Config Parameter) | Table: EpSpecificCodecXCCD

Type	UInt32
Range	0..10
Default	0
Script/CLI	Mipt.EpSpecificCodecXCCD[].VoicePriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.1000.800.1.400

Indicates the priority of this voice codec versus the other voice codecs. The voice codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

This configuration overrides the default configuration set in the **DefaultCodecXCCDVoicePriority** parameter if the **EpSpecificCodecXCCD.EnableConfig** parameter is set to 'Enable'.

DataEnable (Config Parameter) | Table: EpSpecificCodecXCCD

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificCodecXCCD[].DataEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.1000.800.1.500

If enabled, the X-CCD Clear Channel protocol is used for fax transmission.
This configuration overrides the default configuration set in the **DefaultCodecXCCDDataEnable** parameter if the **EpSpecificCodecXCCD.EnableConfig** parameter is set to 'Enable'.

DataPriority (Config Parameter) | Table: EpSpecificCodecXCCD

Type	UInt32
Range	0..10
Default	10
Script/CLI	Mipt.EpSpecificCodecXCCD[].DataPriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.1000.800.1.600

Indicates the priority of this data codec versus the other data codecs. The data codec with the highest priority will be offered first when an outgoing call is initiated. This priority is not used in incoming calls.
The application uses an internal order for codecs with the same priority.

10 is the highest priority and 0 the lowest.

This configuration overrides the default configuration set in the **DefaultCodecXCCDDataPriority** parameter if the **EpSpecificCodecXCCD.EnableConfig** parameter is set to 'Enable'.

PayloadType (Config Parameter) | Table: EpSpecificCodecXCCD

Type	UInt32
Range	96..127
Default	126
Script/CLI	Mipt.EpSpecificCodecXCCD[].PayloadType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.1000.800.1.700

When enabling X-CCD Clear Channel for voice and data transmission, this parameter determines the actual RTP dynamic payload type used in an initial offer.
The payload types available are as per RFC 3551.

This configuration overrides the default configuration set in the **DefaultCodecXCCDPayloadType** parameter if the **EpSpecificCodecXCCD.EnableConfig** parameter is set to 'Enable'.

MinPTime (Config Parameter) | Table: EpSpecificCodecXCCD

Type	UInt32
Range	10..30
Default	10
Script/CLI	Mipt.EpSpecificCodecXCCD[].MinPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.1000.800.1.800

Lower boundary for the packetization period of the given codec.
X-CCD Clear Channel -> (10 ms..30 ms)

This value is expressed in ms, with increments of 1 ms.

This configuration overrides the default configuration set in the **DefaultCodecXCCDMinPTime** parameter if the **EpSpecificCodecXCCD.EnableConfig** parameter is set to 'Enable'.

MaxPTime (Config Parameter) | Table: EpSpecificCodecXCCD

Type	UInt32
Range	10..30
Default	30
Script/CLI	Mipt.EpSpecificCodecXCCD[].MaxPTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.100.1000.800.1.900

Upper boundary for the packetization period of the given codec.
X-CCD Clear Channel -> (10 ms..30 ms)

This value is expressed in ms, with increments of 1 ms.

This configuration overrides the default configuration set in the **DefaultCodecXCCDMaxPTime** parameter if the **EpSpecificCodecXCCD.EnableConfig** parameter is set to 'Enable'.

DefaultJitterBufferLevel (Config Parameter)

Type	Enum
Range	OptimizeLatency(100) | Normal(200) | OptimizeQuality(300) | FaxModem(400) | Custom(500)
Default	Normal
Script/CLI	Mipt.DefaultJitterBufferLevel
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.200.100

Jitter is an abrupt and unwanted variation of one or more signal characteristics, such as the interval between successive pulses or the frequency or phase of successive cycles. An adaptive jitter buffer usually consists of an elastic buffer in which the signal is temporarily stored and then retransmitted at a rate based on the average rate of the incoming signal.

- OptimizeLatency: The jitter buffer is set to the lowest effective value to minimize the latency. Voice cut can be heard if the network is not optimal. (min = 10 ms, max = 40 ms)
- Normal: The jitter buffer tries to find a good compromise between the latency and the voice quality. This setting is recommended in private networks. (min = 30 ms, max = 90 ms)
- OptimizeQuality: The jitter buffer is set to a high value to minimize the voice cuts at cost of high latency. This setting is recommended in public networks. (min = 50 ms, max = 125 ms)
- FaxModem: The jitter buffer is set to a larger value. The Fax/Modem transmission is very sensitive to voice cuts but not to latency, so the fax has a better chance of success with a high buffer. (min = 70 ms, max = 135 ms)
- Custom: The jitter buffer uses the configuration of the **DefaultJitterBufferCustomMinLength** and **DefaultJitterBufferCustomMaxLength** parameters.

If a specific value is set for the **EpSpecificJitterBuffer.Level** parameter and the **EpSpecificJitterBuffer.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultJitterBufferCustomMinLength (Config Parameter)

Type	UInt32
Range	0..900
Default	30
Script/CLI	Mipt.DefaultJitterBufferCustomMinLength
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.200.200

The jitter buffer minimal length (in milliseconds) is the delay the jitter buffer tries to maintain.

The minimal jitter buffer MUST be equal to or smaller than the maximal jitter buffer.

The minimal jitter buffer should be a multiple of ptime.

The maximum allowed value for this parameter is platform dependent.

This value is used only when the **DefaultJitterBufferLevel** parameter is set to 'Custom'

If a specific value is set for the **EpSpecificJitterBuffer.CustomMinLength** parameter and the **EpSpecificJitterBuffer.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultJitterBufferCustomNomLength (Config Parameter)

Type	UInt32
Range	0..900
Default	0
Script/CLI	Mipt.DefaultJitterBufferCustomNomLength
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.200.210

The jitter buffer nominal length (in milliseconds) is the delay the jitter buffer uses when a call begins. The delay then varies according to network conditions.
If this parameter is set to 0, the nominal jitter is set to (minimal jitter buffer + maximal jitter buffer) / 2.

The nominal jitter buffer should be a multiple of ptime.

This value is used only when the **DefaultJitterBufferLevel** parameter is set to 'Custom'

The maximum allowed value for this parameter is platform dependent.

If this value is smaller than the value set in the **DefaultJitterBufferCustomMinLength** parameter, it will be accepted, however the value set in the **DefaultJitterBufferCustomMinLength** parameter will instead be used.

If a specific value is set for the **EpSpecificJitterBuffer.CustomNomLength** parameter and the **EpSpecificJitterBuffer.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultJitterBufferCustomMaxLength (Config Parameter)

Type	UInt32
Range	0..900
Default	125
Script/CLI	Mipt.DefaultJitterBufferCustomMaxLength
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.200.300

The jitter buffer maximal length (in milliseconds) is the highest delay the jitter buffer is allowed to introduce.
The maximal jitter buffer MUST be equal to or greater than the minimal jitter buffer.

The maximal jitter buffer should be a multiple of ptime.

The maximal jitter buffer should be equal to or greater than the minimal jitter buffer + (4 * ptime).

The maximum allowed value for this parameter is platform dependent.

This value is used only when the **DefaultJitterBufferLevel** parameter is set to 'Custom'

If this value is smaller than the value set in the **DefaultJitterBufferCustomNomLength** parameter, it will be accepted, however the value set in the **DefaultJitterBufferCustomNomLength** parameter will instead be used.

If a specific value is set for the **EpSpecificJitterBuffer.CustomMaxLength** parameter and the **EpSpecificJitterBuffer.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultVbdJitterBufferCustomMinLength (Config Parameter)

Type	UInt32
Range	0..900
Default	0
Script/CLI	Mipt.DefaultVbdJitterBufferCustomMinLength
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.200.310

The jitter buffer minimal length (in milliseconds) is the delay the jitter buffer tries to maintain.
See the **DefaultVbdJitterBufferType** description for an explanation of the adaptive jitter buffer.

The minimal jitter buffer MUST be equal to or smaller than the voiceband data maximal jitter buffer.

The minimal jitter buffer should be a multiple of ptime.

This value is used only when the **DefaultJitterBufferLevel** parameter is set to 'Custom'

The maximum allowed value for this parameter is platform dependent.

This value is ignored when the **DefaultVbdJitterBufferType** parameter is set to 'Fixed'

If a specific value is set for the **EpSpecificJitterBuffer.CustomVbdMinLength** parameter and the **EpSpecificJitterBuffer.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultVbdJitterBufferCustomNomLength (Config Parameter)

Type	UInt32
Range	0..900
Default	67
Script/CLI	Mipt.DefaultVbdJitterBufferCustomNomLength
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.200.320

The jitter buffer nominal length (in milliseconds) is the delay the jitter buffer uses when a call begins. The delay then varies depending on the type of jitter buffer.
See the **DefaultVbdJitterBufferType** description for an explanation of the fixed and adaptive jitter buffer.

In adaptive mode, the nominal jitter buffer should be equal to (voice band data minimal jitter buffer + voice band data maximal jitter buffer) / 2.

The maximum allowed value for this parameter is platform dependent.

This value is used only when the **DefaultJitterBufferLevel** parameter is set to 'Custom'

If a specific value is set for the **EpSpecificJitterBuffer.CustomVbdNomLength** parameter and the **EpSpecificJitterBuffer.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultVbdJitterBufferCustomMaxLength (Config Parameter)

Type	UInt32
Range	0..900
Default	135
Script/CLI	Mipt.DefaultVbdJitterBufferCustomMaxLength
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.200.330

The jitter buffer maximal length (in milliseconds) is the highest delay the jitter buffer is allowed to introduce.
The maximal jitter buffer MUST be equal to or greater than the minimal jitter buffer.

The maximal jitter buffer should be a multiple of ptime.

The maximal jitter buffer should be equal to or greater than voiceband data minimal jitter buffer + (4 * ptime) in adaptive mode.

The maximum allowed value for this parameter is platform dependent.

This value is used only when the **DefaultJitterBufferLevel** parameter is set to 'Custom'

If this value is smaller than the value set in the **DefaultVbdJitterBufferCustomNomLength** parameter, it will be accepted, however the value set in the **DefaultVbdJitterBufferCustomNomLength** parameter will instead be used.

If a specific value is set for the **EpSpecificJitterBuffer.CustomVbdMaxLength** parameter and the **EpSpecificJitterBuffer.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

DefaultVbdJitterBufferType (Config Parameter)

Type	Enum
Range	AdaptiveImmediately(100) | AdaptiveSilence(200) | Fixed(300)
Default	Fixed
Script/CLI	Mipt.DefaultVbdJitterBufferType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.200.340

Algorithm to use for managing the jitter buffer during a call. **DefaultVbdJitterBufferCustomNomLength** serves as the delay at the beginning of the call and might be adapted afterwards based on the selected algorithm.

- AdaptiveImmediately: The nominal delay varies based on the estimated packet jitter. Playout adjustment is done immediately when the actual delay goes out of bounds of a small window around the moving nominal delay.
- AdaptiveSilence: The nominal delay varies based on the estimated packet jitter. Playout adjustment is done based on the actual delay going out of bounds of a small window around the moving nominal delay. The adjustment is deferred until silence is detected (either from playout buffer underflow or by analysis of packet content). Playout adjustment is also done when overflow or underflow events occur.
- Fixed: The nominal delay is fixed to the value of **DefaultVbdJitterBufferCustomNomLength** and does not change thereafter. Playout adjustment is done when overflow or underflow events occur.

If a specific value is set for the **EpSpecificJitterBuffer.CustomVbdJitterBufferType** parameter and the **EpSpecificJitterBuffer.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

EpSpecificJitterBuffer (Table)

Endpoint specific configuration.

EpId (Index) | Table: EpSpecificJitterBuffer

Type	Text
Range	
Script/CLI	Mipt.EpSpecificJitterBuffer[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.200.400.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificJitterBuffer

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificJitterBuffer[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.200.400.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultJitterBufferLevel**, **DefaultJitterBufferCustomMinLength** and **DefaultJitterBufferCustomMaxLength** parameters.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificJitterBuffer.Level**, **EpSpecificJitterBuffer.CustomMinLength** and **EpSpecificJitterBuffer.CustomMaxLength** parameters.

Level (Config Parameter) | Table: EpSpecificJitterBuffer

Type	Enum
Range	OptimizeLatency(100) | Normal(200) | OptimizeQuality(300) | FaxModem(400) | Custom(500)
Default	Normal
Script/CLI	Mipt.EpSpecificJitterBuffer[].Level
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.200.400.1.300

Jitter is an abrupt and unwanted variation of one or more signal characteristics, such as the interval between successive pulses or the frequency or phase of successive cycles. An adaptive jitter buffer

usually consists of an elastic buffer in which the signal is temporarily stored and then retransmitted at a rate based on the average rate of the incoming signal.

- OptimizeLatency: The jitter buffer is set to the lowest effective value to minimize the latency. Voice cut can be heard if the network is not optimal. (min = 10 ms, max = 40 ms)
- Normal: The jitter buffer tries to find a good compromise between the latency and the voice quality. This setting is recommended in private networks. (min = 30 ms, max = 90 ms)
- OptimizeQuality: The jitter buffer is set to a high value to minimize the voice cuts at cost of high latency. This setting is recommended in public networks. (min = 50 ms, max = 120 ms)
- FaxModem: The jitter buffer is set to a larger value. The Fax/Modem transmission is very sensitive to voice cuts but not to latency, so the fax has a better chance of success with a high buffer. (min = 70 ms, max = 135 ms)
- Custom: The jitter buffer uses the configuration of the **DefaultJitterBufferCustomMinLength** and **DefaultJitterBufferCustomMaxLength** parameters.

This configuration overrides the default configuration set in the **DefaultJitterBufferLevel** parameter if the **EpSpecificJitterBuffer.EnableConfig** parameter is set to 'Enable'.

CustomMinLength (Config Parameter) | Table: EpSpecificJitterBuffer

Type	UInt32
Range	0..900
Default	30
Script/CLI	Mipt.EpSpecificJitterBuffer[].CustomMinLength
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.200.400.1.400

The jitter buffer minimal length (in milliseconds) is the delay the jitter buffer tries to maintain. The minimal jitter buffer MUST be equal to or smaller than the maximal jitter buffer.

The minimal jitter buffer should be a multiple of ptime.

This value is used only when the **Level** parameter is set to 'Custom'.

The maximum allowed value for this parameter is platform dependent.

This configuration overrides the default configuration set in the **DefaultJitterBufferCustomMinLength** parameter if the **EpSpecificJitterBuffer.EnableConfig** parameter is set to 'Enable'.

CustomNomLength (Config Parameter) | Table: EpSpecificJitterBuffer

Type	UInt32
Range	0..900
Default	0
Script/CLI	Mipt.EpSpecificJitterBuffer[].CustomNomLength
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.200.400.1.410

The jitter buffer nominal length (in milliseconds) is the delay the jitter buffer uses when a call begins. The delay then varies according to network conditions.
If this parameter is set to 0, the nominal jitter is set to (minimal jitter buffer + maximal jitter buffer) / 2.

The nominal jitter buffer MUST be equal to or smaller than the maximal jitter buffer.

The nominal jitter buffer should be a multiple of ptime.

This value is used only when the **Level** parameter is set to 'Custom'.

The maximum allowed value for this parameter is platform dependent.

If this value is smaller than the value set in the **EpSpecificJitterBuffer.CustomMinLength** parameter, it will be accepted, however the value set in the **EpSpecificJitterBuffer.CustomMinLength** parameter will instead be used.

This configuration overrides the default configuration set in the **DefaultJitterBufferCustomNomLength** parameter if the **EpSpecificJitterBuffer.EnableConfig** parameter is set to 'Enable'.

CustomMaxLength (Config Parameter) | Table: EpSpecificJitterBuffer

Type	UInt32
Range	0..900
Default	125
Script/CLI	Mipt.EpSpecificJitterBuffer[].CustomMaxLength
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.200.400.1.500

The jitter buffer maximal length (in milliseconds) is the highest delay the jitter buffer is allowed to introduce.
The maximal jitter buffer MUST be equal to or greater than the minimal jitter buffer.

The maximal jitter buffer should be a multiple of ptime.

The maximal jitter buffer should be equal to or greater than minimal jitter buffer + 4 * ptime.

This value is used only when the **Level** parameter is set to 'Custom'.

The maximum allowed value for this parameter is platform dependent.

If this value is smaller than the value set in the **EpSpecificJitterBuffer.CustomNomLength** parameter, it will be accepted, however the value set in the **EpSpecificJitterBuffer.CustomNomLength** parameter will instead be used.

This configuration overrides the default configuration set in the **DefaultJitterBufferCustomMaxLength** parameter if the **EpSpecificJitterBuffer.EnableConfig** parameter is set to 'Enable'.

CustomVbdMinLength (Config Parameter) | Table: EpSpecificJitterBuffer

Type	UInt32
Range	0..900
Default	0
Script/CLI	Mipt.EpSpecificJitterBuffer[].CustomVbdMinLength
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.200.400.1.600

The jitter buffer minimal length (in milliseconds) is the delay the jitter buffer tries to maintain. See the **CustomVbdJitterBufferType** description for an explanation of the adaptive jitter buffer.

The minimal jitter buffer MUST be equal to or smaller than the voiceband data maximal jitter buffer.

The minimal jitter buffer should be a multiple of ptime.

This value is used only when the **Level** parameter is set to 'Custom'.

The maximum allowed value for this parameter is platform dependent.

This value is ignored when the **CustomVbdJitterBufferType** parameter is set to 'Fixed'

This configuration overrides the default configuration set in the **DefaultVbdJitterBufferCustomMinLength** parameter if the **EpSpecificJitterBuffer.EnableConfig** parameter is set to 'Enable'.

CustomVbdNomLength (Config Parameter) | Table: EpSpecificJitterBuffer

Type	UInt32
Range	0..900
Default	67
Script/CLI	Mipt.EpSpecificJitterBuffer[].CustomVbdNomLength
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.200.400.1.700

The jitter buffer nominal length (in milliseconds) is the delay the jitter buffer uses when a call begins. The delay then varies depending on the type of jitter buffer.
See the **CustomVbdJitterBufferType** description for an explanation of the fixed and adaptive jitter buffer.

In adaptive mode, the nominal jitter buffer should be equal to (voice band data minimal jitter buffer + voice band data maximal jitter buffer) / 2.

The maximum allowed value for this parameter is platform dependent.

This value is used only when the **Level** parameter is set to 'Custom'.

This configuration overrides the default configuration set in the **DefaultVbdJitterBufferCustomNomLength** parameter if the **EpSpecificJitterBuffer.EnableConfig** parameter is set to 'Enable'.

CustomVbdMaxLength (Config Parameter) | Table: EpSpecificJitterBuffer

Type	UInt32
Range	0..900
Default	125
Script/CLI	Mipt.EpSpecificJitterBuffer[].CustomVbdMaxLength
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.200.400.1.800

The jitter buffer maximal length (in milliseconds) is the highest delay the jitter buffer is allowed to introduce.
The maximal jitter buffer MUST be equal to or greater than the minimal jitter buffer.

The maximal jitter buffer should be a multiple of ptime.

The maximal jitter buffer should be equal to or greater than voiceband data minimal jitter buffer + (4 * ptime) in adaptive mode.

The maximum allowed value for this parameter is platform dependent.

This value is used only when the **Level** parameter is set to 'Custom'.

If this value is smaller than the value set in the **EpSpecificJitterBuffer.CustomVbdNomLength** parameter, it will be accepted, however the value set in the **EpSpecificJitterBuffer.CustomVbdNomLength** parameter will instead be used.

This configuration overrides the default configuration set in the **DefaultVbdJitterBufferCustomMaxLength** parameter if the **EpSpecificJitterBuffer.EnableConfig** parameter is set to 'Enable'.

CustomVbdJitterBufferType (Config Parameter) | Table: EpSpecificJitterBuffer

Type	Enum
Range	AdaptiveImmediately(100) | AdaptiveSilence(200) | Fixed(300)
Default	Fixed
Script/CLI	Mipt.EpSpecificJitterBuffer[].CustomVbdJitterBufferType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.200.400.1.900

Algorithm to use for managing the jitter buffer during a call. **CustomVbdNomLength** serves as the delay at the beginning of the call and might be adapted afterwards based on the selected algorithm.

- AdaptiveImmediately: The nominal delay varies based on the estimated packet jitter. Playout adjustment is done immediately when the actual delay goes out of bounds of a small window around the moving nominal delay.
- AdaptiveSilence: The nominal delay varies based on the estimated packet jitter. Playout adjustment is done based on the actual delay going out of bounds of a small window around the moving nominal delay. The adjustment is deferred until silence is detected (either from playout buffer underflow or by analysis of packet content). Playout adjustment is also done when overflow or underflow events occur.
- Fixed: The nominal delay is fixed to the value of **DefaultVbdJitterBufferCustomNomLength** and does not change thereafter. Playout adjustment is done when overflow or underflow events occur.

This configuration overrides the default configuration set in the **DefaultVbdJitterBufferType** parameter if the **EpSpecificJitterBuffer.EnableConfig** parameter is set to 'Enable'.

DefaultDtmfTransportMethod (Config Parameter)

Type	Enum
Range	InBand(100) | OutOfBandUsingRtp(200) | OutOfBandUsingSignalingProtocol(300) | SignalingProtocolDependent(400)
Default	InBand
Script/CLI	Mipt.DefaultDtmfTransportMethod
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.300.100

Selects the preferred DTMF transport method.

- InBand: The DTMFs and the voice are mixed together within the RTP audio stream. This method is not reliable when a compressed codec (e.g. G.722, G.723, G.726, G.729) is used.

- OutOfBandUsingRtp: The DTMFs are transmitted Out-of-Band along the RTP stream, as per RFC-2833, if the peer supports it. Otherwise, DTMF transport falls back to Inband. This also applies when using SRTP.
- OutOfBandUsingSignalingProtocol: The DTMF are transmitted Out-of-Band following a signaling method set in the **SipEp.InteropDtmfTransportMethod** parameter.
- SignalingProtocolDependent: The signaling protocol has the control to select the DTMF transport mode. The behavior depends on the **SipEp.InteropDtmfTransportMethod** parameter.

If a specific value is set for the **EpSpecificDtmfTransport.Method** parameter and the **EpSpecificDtmfTransport.EnableConfig** parameter is set to *Enable*, then the specific value will override the current default value.

DefaultDtmfTransportPayloadType (Config Parameter)

Type	UInt32
Range	96..127
Default	96
Script/CLI	Mipt.DefaultDtmfTransportPayloadType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.300.200

Determines the actual RTP dynamic payload type used for telephone-event in an initial offer when selecting the 'OutOfBandUsingRtp' DTMF transport mode (see the **DefaultDtmfTransportMethod** parameter). The payload types available are as per RFC 1890.

If a specific value is set for the **EpSpecificDtmfTransport.PayloadType** parameter and the **EpSpecificDtmfTransport.EnableConfig** parameter is set to 'Enable', then the specific value will override the current default value.

EpSpecificDtmfTransport (Table)

Endpoint specific configuration.

EpId (Index) | Table: EpSpecificDtmfTransport

Type	Text
Range	
Script/CLI	Mipt.EpSpecificDtmfTransport[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.300.300.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificDtmfTransport

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificDtmfTransport[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.300.300.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultDtmfTransportMethod** and **DefaultDtmfTransportPayloadType** parameters.
- Enable: The endpoint uses the specific configuration as defined in the **EpSpecificDtmfTransport.Method** and **EpSpecificDtmfTransport.PayloadType** parameters.

Method (Config Parameter) | Table: EpSpecificDtmfTransport

Type	Enum
Range	InBand(100) | OutOfBandUsingRtp(200) | OutOfBandUsingSignalingProtocol(300) | SignalingProtocolDependent(400)
Default	InBand
Script/CLI	Mipt.EpSpecificDtmfTransport[].Method
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.300.300.1.300

Selects the preferred DTMF transport method.

- InBand: The DTMFs and the voice are mixed together within the RTP audio stream. This method is not reliable when a compressed codec (e.g. G.722, G.723, G.726, G.729) is used.
- OutOfBandUsingRtp: The DTMFs are transmitted Out-of-Band along the RTP stream, as per RFC-2833, if the peer supports it. Otherwise, DTMF transport falls back to Inband. This also applies when using SRTP.
- OutOfBandUsingSignalingProtocol: The DTMF are transmitted Out-of-Band following a signaling method set in the **SipEp.InteropDtmfTransportMethod** parameter.
- SignalingProtocolDependent: The signaling protocol has the control to select the DTMF transport mode. The behavior depends on the **SipEp.InteropDtmfTransportMethod** parameter.

This configuration overrides the default configuration set in the **DefaultDtmfTransportMethod** parameter if the **EpSpecificDtmfTransport.EnableConfig** parameter is set to *Enable*.

PayloadType (Config Parameter) | Table: EpSpecificDtmfTransport

Type	UInt32
Range	96..127
Default	96
Script/CLI	Mipt.EpSpecificDtmfTransport[].PayloadType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.300.300.1.400

Determines the actual RTP dynamic payload type used for telephone-event in an initial offer when selecting the *OutOfBandUsingRtp* DTMF transport mode (see the **Method** parameter). The payload types available are as per RFC 1890.

This configuration overrides the default configuration set in the **DefaultDtmfTransportPayloadType** parameter if the **EpSpecificDtmfTransport.EnableConfig** parameter is set to *Enable*.

IpTransportRtpBasePort (Config Parameter)

Type	UInt32
Range	1025..65435
Default	5004
Script/CLI	Mipt.IpTransportRtpBasePort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.400.100.100

UDP base port for the RTP/RTCP protocols.
The RTP/RTCP ports are allocated starting from this base port. RTP ports number are even and RTCP ports number are odd.

The unit may use two or four RTP/RTCP ports per FXS/FXO endpoint.

It uses two ports in case of a standard call, while it uses four ports in other types of calls such as a conference call, a call transfer, etc.

Example: let's say that a unit has two FXS endpoints and the base port is defined on 5004:

- if there is currently no ongoing call and FXS endpoint 1 has an incoming or outgoing call, it will use the RTP/RTCP ports 5004 and 5005.
- if there is currently a standard call on FXS endpoint 1 and FXS endpoint 2 has a conference call, then FXS endpoint 2 will use the RTP/RTCP ports 5006, 5007, 5008, and 5009, which are the next available ports.

The range of ports reserved for RTP must not overlap the ranges of ports reserved for T.38.

IpTransportSrtpBasePort (Config Parameter)

Type	UInt32
Range	0..0 | 1025..65435
Default	5004
Script/CLI	Mipt.IpTransportSrtpBasePort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.400.100.200

UDP base port for the SRTP/SRTCP protocols.
The SRTP/SRTCP ports are allocated starting from this base port. SRTP ports number are even and SRTCP ports number are odd.

Using the same base port for **IpTransportRtpBasePort** and **IpTransportSrtpBasePort** does not conflict.

Base Port equal to 0 means that the SRTP connection will use the same base port as the one used for **IpTransportRtpBasePort**, and when the transport is configured as Secure with Fallback, the same audio port is used for RTP and SRTP in SDP offer.

Refer to the documentation of **IpTransportRtpBasePort** for more details.

The range of ports reserved for SRTP must not overlap the ranges of ports reserved for T.38.

IpTransportT38BasePort (Config Parameter)

Type	UInt32
Range	1025..65435
Default	6004
Script/CLI	Mipt.IpTransportT38BasePort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.400.200.100

T.38 base port.
The T.38 ports are allocated starting from this base port. The units use as many T.38 ports as the number of FXS/FXO endpoints.

Example: let's say that a unit has two FXS endpoints and the base port is defined on 6004:

- if there is currently no ongoing call and FXS endpoint 1 has an incoming or outgoing call, it will use the T.38 port 6004.
- if there is currently a call on FXS endpoint 1 and FXS endpoint 2 has an incoming or outgoing call, then FXS endpoint 2 will use the T.38 port 6005.

The range of ports reserved for T.38 must not overlap the ranges of ports reserved for RTP and SRTP.

DefaultCodecVsBearerCapabilitiesMapping (Table)

Codec to prioritize in the outgoing INVITE when the incoming SETUP's ITC matches the configured one. The ITC value to set in the outgoing SETUP's bearer capabilities when the incoming INVITE's codec matches the configured one.

Index (Index) | Table: DefaultCodecVsBearerCapabilitiesMapping

Type	UInt32
Range	1..3
Script/CLI	Mipt.DefaultCodecVsBearerCapabilitiesMapping[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.500.100.1.100

Index of the current Codec vs. Bearer match.

EnableMap (Config Parameter) | Table: DefaultCodecVsBearerCapabilitiesMapping

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.DefaultCodecVsBearerCapabilitiesMapping[].EnableMap
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.500.100.1.200

Defines if the outgoing codecs priority or selection should reflect the incoming ITC and vice versa.

- Disable: The codecs order in the outgoing INVITE follows the codec priority. The ITC in the outgoing SETUP is not modified.
- Enable: When the ITC value in the incoming SETUP matches **DefaultCodecVsBearerCapabilitiesMapping.InformationTransferCap** and the **DefaultCodecVsBearerCapabilitiesMapping.MappingType** parameter is set to Prioritize the first codec in the outgoing INVITE is **DefaultCodecVsBearerCapabilitiesMapping.Codec**. With a **DefaultCodecVsBearerCapabilitiesMapping.MappingType** set to Select, then the outgoing INVITE contains only the **DefaultCodecVsBearerCapabilitiesMapping.Codec**. If the first codec in the incoming INVITE matches **DefaultCodecVsBearerCapabilitiesMapping.Codec**, the ITC value in the outgoing SETUP is **DefaultCodecVsBearerCapabilitiesMapping.InformationTransferCap**.

Codec (Config Parameter) | Table: DefaultCodecVsBearerCapabilitiesMapping

Type	Enum
Range	G711alaw(100) | G711ulaw(200) | G722(250) | G723(300) | G72616kbps(400) | G72624kbps(500) | G72632kbps(600) | G72640kbps(700) | G729(800) | ClearMode(900) | ClearChannel(1000) | XCCD(1100)
Default	G729
Script/CLI	Mipt.DefaultCodecVsBearerCapabilitiesMapping[].Codec
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.500.100.1.300

The codec to be prioritized or selected in an outgoing INVITE when the incoming SETUP's ITC matches **DefaultCodecVsBearerCapabilitiesMapping.InformationTransferCap**. This codec is also checked against an incoming INVITE's priority codec. If it matches, then the outgoing SETUP's ITC is set to **DefaultCodecVsBearerCapabilitiesMapping.InformationTransferCap**. See the **DefaultCodecVsBearerCapabilitiesMapping.MappingType** parameter for a description of prioritization versus selection of a codec.

InformationTransferCap (Config Parameter) | Table: DefaultCodecVsBearerCapabilitiesMapping

Type	Enum
Range	Audio31kHz(100) | Speech(200) | Unrestricted(300)
Default	Speech
Script/CLI	Mipt.DefaultCodecVsBearerCapabilitiesMapping[].InformationTransferCap
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.500.100.1.400

The ITC value to be set in the outgoing SETUP when the incoming INVITE's priority codec matches **DefaultCodecVsBearerCapabilitiesMapping.Codec**. This value is also checked against an incoming SETUP's bearer capabilities. If it matches, then the outgoing INVITE's prioritized or selected codec is set to **DefaultCodecVsBearerCapabilitiesMapping.Codec**. See the **DefaultCodecVsBearerCapabilitiesMapping.MappingType** parameter for a description of prioritization versus selection of a codec.

There is one exception to the above description; any incoming ISDN call using UDI (Unrestricted Digital) will ignore the **DefaultCodecVsBearerCapabilitiesMapping** entries with the **InformationTransferCap** set to Unrestricted(300). When such an ISDN call is incoming, the outgoing SIP INVITE will offer PCMA or PCMU, depending on the ISDN port 'Preferred Encoding Scheme' value.

MappingType (Config Parameter) | Table: DefaultCodecVsBearerCapabilitiesMapping

Type	Enum
Range	Prioritize(100) | Select(200)
Default	Prioritize
Script/CLI	Mipt.DefaultCodecVsBearerCapabilitiesMapping[].MappingType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.500.100.1.500

- Prioritize: the **DefaultCodecVsBearerCapabilitiesMapping.Codec** is set on top of the list in an outgoing INVITE when the incoming SETUP's ITC matches **DefaultCodecVsBearerCapabilitiesMapping.InformationTransferCap**.
- Select: the **DefaultCodecVsBearerCapabilitiesMapping.Codec** is the only codec offered in an outgoing INVITE when the incoming SETUP's ITC matches **DefaultCodecVsBearerCapabilitiesMapping.InformationTransferCap**.

DefaultSecurityRtpMode (Config Parameter)

Type	Enum
Range	Unsecure(100) | Secure(200) | SecureWithFallback(300)
Default	Unsecure
Script/CLI	Mipt.DefaultSecurityRtpMode
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.600.100

Defines the RTP payload mode (secure or not secure).

- Unsecure: Only RTP.
- Secure: Only SRTP.
- SecureWithFallback: SRTP with RTP fallback if the peer does not support security.

DefaultSecurityKeyManagement (Config Parameter)

Type	Enum
Range	Mikey(100) | Sdes(200)
Default	Mikey
Script/CLI	Mipt.DefaultSecurityKeyManagement
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.600.150

Defines the key management protocol for SRTP.

- Mikey: Use MIKEY (Multimedia Internet KEYing - RFC 3830).
- Sdes: Use SDES (Security DEScriptions - RFC 4568).

Note that this parameter has no effect if the **RtpMode** parameter is set to "Unsecure".

DefaultSecurityRtpEncryption (Config Parameter)

Type	Enum
Range	AesCm128(200)
Default	AesCm128
Script/CLI	Mipt.DefaultSecurityRtpEncryption
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.600.200

Defines the encryption type to be used with SRTP.

- AesCm128: AES (Advanced Encryption Standard) Counter Mode 128 bits.

Note that this parameter has no effect if the **RtpMode** parameter is set to "Unsecure".

AllowUnsecureT38WithSrtp (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.AllowUnsecureT38WithSrtp
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.600.300

Enables T38 even if the call has been established previously in SRTP.

- Disable: T38 disabled for SRTP calls.
- Enable: T38 enabled for SRTP calls. Beware that enabling this parameter opens a security hole, because T38 is an unsecure protocol.

Note that this parameter has no effect if the **RtpMode** parameter is set to "Unsecure".

SessionUpdateCryptoMode (Config Parameter)

Type	Enum
Range	Regenerate(100) | Keep(200)
Default	
Script/CLI	Mipt.SessionUpdateCryptoMode
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.600.350

Deprecated: This parameter has been split in three (3) different parameters for more granularity.

Configuring to "Regenerate" will set the following parameters:

- **Mipt.CryptoModeWhenSendingOffer** = RegenerateAlways
- **Mipt.CryptoModeWhenSendingAnswer** = RegenerateAlways
- **Mipt.CryptoContextBehavior** = ResetAlways

Configuring to "Keep" will set the following parameters:

- **Mipt.CryptoModeWhenSendingOffer** = KeepAlways
- **Mipt.CryptoModeWhenSendingAnswer** = KeepAlways
- **Mipt.CryptoContextBehavior** = ResetAlways

Note: This parameter is write-only, so trying to read its value would return an error.

CryptoModeWhenSendingOffer (Config Parameter)

Type	Enum
Range	RegenerateAlways(100) | KeepAlways(200)
Default	RegenerateAlways
Script/CLI	Mipt.CryptoModeWhenSendingOffer
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.600.360

Specifies if the cryptographic attribute in the SDP offer should be regenerated or not for a new SDP offer with secured RTP (SRTP) streams. A cryptographic attribute includes the cryptographic suite, the key parameters, and the session parameters.
An SDP offer is sent during the following call scenarios:

- Hold and Resume
- Session timers (i.e. session expires)
- Forking
- Call Transfer
- Conference call

Of this list is excluded establisment or termination of a call.

The possible configuration values are:

- RegenerateAlways: Always regenerate a new cryptographic attribute for the SDP offer to be sent.
- KeepAlways: Keep the same cryptographic attribute for the SDP offer to be sent.

When the sent or received cryptographic attribute changes, the behavior of the associated cryptographic context can be adjusted according to the **CryptoContextBehavior** parameter.

This parameter is effective only when the **Mipt.KeyManagement** parameter is set to *SDES*.

Note: This parameter does not apply to SIP session refresh, whose session timers re-INVITEs or UPDATEs should not affect the SRTP crypto at all.

CryptoModeWhenSendingAnswer (Config Parameter)

Type	Enum
Range	RegenerateAlways(100) | KeepUnlessCryptoChanged(130) | KeepAlways(200)
Default	RegenerateAlways
Script/CLI	Mipt.CryptoModeWhenSendingAnswer
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.600.370

Specifies if the cryptographic attribute in the SDP answer with secured RTP (SRTP) streams should be regenerated. A cryptographic attribute includes the cryptographic suite, the key parameters, and the session parameters.
The possible configuration values are:

- RegenerateAlways: Always regenerate a new cryptographic attribute for the SDP answer to be sent, regardless of the content of the received SDP offer.
- KeepUnlessCryptoChanged: Keep the same cryptographic attribute for the SDP answer to be sent, unless the matching cryptographic attribute of the received SDP offer changed.

- KeepAlways: Keep the same cryptographic attribute for the SDP answer to be sent, regardless of the content of the received SDP offer.

When the sent or received cryptographic attribute changes, the behavior of the associated cryptographic context can be adjusted according to the **CryptoContextBehavior** parameter.

This parameter is effective only when the **Mipt.KeyManagement** parameter is set to *SDES*.

Note: This parameter does not apply to SIP session refresh, whose session timers re-INVITEs or UPDATEs should not affect the SRTP crypto at all.

CryptoContextBehavior (Config Parameter)

Type	Enum
Range	ResetAlways(100) | ResetOnNewCrypto(150) | ResetNever(200)
Default	ResetAlways
Script/CLI	Mipt.CryptoContextBehavior
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.600.380

Specifies whether or not the cryptographic context, more specifically the rollover counter (ROC), must be reset after a SDP renegotiation.
The ROC is an internal counter that tracks how many times the sequence number went over 65535.

Both endpoints must have an identical behavior, else this will lead to decryption problems.

The possible behaviors are:

- ResetAlways: Reset the cryptographic context on every renegociation, even if the crypto key has not changed.
- ResetOnNewCrypto: Reset the cryptographic context when the negotiated crypto key has changed.
- ResetNever: The cryptographic context is never reset after a renegotiation. The context is updated with the new crypto key and the ROC keeps its current value.

Note: When the cryptographic context is reset, the sequence number, timestamp and SSRC of the stream are also reset to new randomized values.

Note: In any case, the cryptographic context is automatically reset when the stream destination changes, regardless of the config of this parameter.

Refer to the **CryptoModeWhenSendingOffer** and **CryptoModeWhenSendingAnswer** parameters for more details how crypto attributes are negotiated.

EpSpecificSecurity (Table)

Endpoint specific configuration.

EpId (Index) | Table: EpSpecificSecurity

Type	Text
Range	
Script/CLI	Mipt.EpSpecificSecurity[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.600.400.1.100

String that identifies an endpoint in other tables.

EnableConfig (Config Parameter) | Table: EpSpecificSecurity

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EpSpecificSecurity[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.600.400.1.200

Defines the configuration to use for a specific endpoint.

- Disable: The endpoint uses the default configuration as defined in the **DefaultSecurity**.
- Enable: The endpoint uses the specific configuration.

RtpMode (Config Parameter) | Table: EpSpecificSecurity

Type	Enum
Range	Unsecure(100) | Secure(200) | SecureWithFallback(300)
Default	Unsecure
Script/CLI	Mipt.EpSpecificSecurity[].RtpMode
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.600.400.1.300

Defines the RTP payload mode (secure or not secure).

- Unsecure: Only RTP.
- Secure: Only SRTP.
- SecureWithFallback: SRTP with RTP fallback if the peer does not support security.

KeyManagement (Config Parameter) | Table: EpSpecificSecurity

Type	Enum
Range	Mikey(100) | Sdes(200)
Default	Mikey
Script/CLI	Mipt.EpSpecificSecurity[].KeyManagement
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.600.400.1.350

Defines the key management protocol for SRTP.

- Mikey: Use MIKEY (Multimedia Internet KEYing - RFC 3830).
- Sdes: Use SDES (Security DEScriptions - RFC 4568).

Note that this parameter has no effect if the **RtpMode** parameter is set to "Unsecure".

RtpEncryption (Config Parameter) | Table: EpSpecificSecurity

Type	Enum
Range	AesCm128(200)
Default	AesCm128
Script/CLI	Mipt.EpSpecificSecurity[].RtpEncryption
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.600.400.1.400

Defines the encryption type to be used with SRTP.

- AesCm128: AES (Advanced Encryption Standard) Counter Mode 128 bits.

Note that this parameter has no effect if the **RtpMode** parameter is set to "Unsecure".

LastConnectionsStats (Table)

Last 10 connections statistics.

ConnectionsIndex (Index) | Table: LastConnectionsStats

Type	UInt32
Range	1..10
Script/CLI	Mipt.LastConnectionsStats[].ConnectionsIndex
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.100.1.100

Last 10 connections identificator.

OctetsTransmitted (Status Parameter) | Table: LastConnectionsStats

Type	UInt64
Range	
Script/CLI	Mipt.LastConnectionsStats[].OctetsTransmitted
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.100.1.200

Number of octets transmitted during the connection.

OctetsReceived (Status Parameter) | Table: LastConnectionsStats

Type	UInt64
Range	
Script/CLI	Mipt.LastConnectionsStats[].OctetsReceived
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.100.1.300

Number of octets received during the connection.

PacketsTransmitted (Status Parameter) | Table: LastConnectionsStats

Type	UInt64
Range	
Script/CLI	Mipt.LastConnectionsStats[].PacketsTransmitted
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.100.1.400

Number of packets transmitted during the connection..

PacketsReceived (Status Parameter) | Table: LastConnectionsStats

Type	UInt64
Range	
Script/CLI	Mipt.LastConnectionsStats[].PacketsReceived
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.100.1.500

Number of packets received during the connection.

PacketsLost (Status Parameter) | Table: LastConnectionsStats

Type	UInt32
Range	
Script/CLI	Mipt.LastConnectionsStats[].PacketsLost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.100.1.600

Number of packets lost during the connection. This value is obtained by substracting the expected number of packets based on the sequence number from the number of packets received.

MinimumInterarrivalJitter (Status Parameter) | Table: LastConnectionsStats

Type	UInt32
Range	
Script/CLI	Mipt.LastConnectionsStats[].MinimumInterarrivalJitter
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.100.1.700

Minimum interarrival time, in milliseconds, during the connection. All RTP packets belonging to the connection and received at the RTP level are considered in the calculation.

MaximumInterarrivalJitter (Status Parameter) | Table: LastConnectionsStats

Type	UInt32
Range	
Script/CLI	Mipt.LastConnectionsStats[].MaximumInterarrivalJitter
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.100.1.800

Maximum interarrival time, in milliseconds, during the connection. All RTP packets belonging to the connection and received at the RTP level are considered in the calculation.

AverageInterarrivalJitter (Status Parameter) | Table: LastConnectionsStats

Type	UInt32
Range	
Script/CLI	Mipt.LastConnectionsStats[].AverageInterarrivalJitter
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.100.1.900

Average interarrival time, in milliseconds, during the connection. All RTP packets belonging to the connection and received at the RTP level are considered in the calculation.

MinimumLatency (Status Parameter) | Table: LastConnectionsStats

Type	UInt32
Range	
Script/CLI	Mipt.LastConnectionsStats[].MinimumLatency
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.100.1.1000

Minimum latency, in milliseconds, during the connection.
The latency value is computed as one half of the round-trip time, as measured through RTCP.

MaximumLatency (Status Parameter) | Table: LastConnectionsStats

Type	UInt32
Range	
Script/CLI	Mipt.LastConnectionsStats[].MaximumLatency
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.100.1.1100

Maximum latency, in milliseconds, during the connection.
The latency value is computed as one half of the round-trip time, as measured through RTCP.

AverageLatency (Status Parameter) | Table: LastConnectionsStats

Type	UInt32
Range	
Script/CLI	Mipt.LastConnectionsStats[].AverageLatency
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.100.1.1200

Average latency, in milliseconds, during the connection.
The latency value is computed as one half of the round-trip time, as measured through RTCP

LastPeriodsStats (Table)

Last 10 periods statistics.

PeriodIndex (Index) | Table: LastPeriodsStats

Type	UInt32
Range	1..10
Script/CLI	Mipt.LastPeriodsStats[].PeriodIndex
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.200.1.100

Period identificator.

OctetsTransmitted (Status Parameter) | Table: LastPeriodsStats

Type	UInt64
Range	
Script/CLI	Mipt.LastPeriodsStats[].OctetsTransmitted
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.200.1.200

Number of octets transmitted during the collection period. This value is obtained by cumulating the octets transmitted in all connections that were active during the collection period.

OctetsReceived (Status Parameter) | Table: LastPeriodsStats

Type	UInt64
Range	
Script/CLI	Mipt.LastPeriodsStats[].OctetsReceived
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.200.1.300

Number of octets received during the collection period. This value is obtained by cumulating the octets received in all connections that were active during the collection period.

PacketsTransmitted (Status Parameter) | Table: LastPeriodsStats

Type	UInt64
Range	
Script/CLI	Mipt.LastPeriodsStats[].PacketsTransmitted
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.200.1.400

Number of packets transmitted during the collection period. This value is obtained by cumulating the packets transmitted in all connections that were active during the collection period.

PacketsReceived (Status Parameter) | Table: LastPeriodsStats

Type	UInt64
Range	
Script/CLI	Mipt.LastPeriodsStats[].PacketsReceived
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.200.1.500

Number of packets received during the collection period. This value is obtained by cumulating the packets received in all connections that were active during the collection period.

PacketsLost (Status Parameter) | Table: LastPeriodsStats

Type	UInt32
Range	
Script/CLI	Mipt.LastPeriodsStats[].PacketsLost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.200.1.600

Number of packets lost during the collection period. This value is obtained by cumulating the packets lost in all connections that were active during the collection period.

MinimumInterarrivalJitter (Status Parameter) | Table: LastPeriodsStats

Type	UInt32
Range	
Script/CLI	Mipt.LastPeriodsStats[].MinimumInterarrivalJitter
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.200.1.700

Minimum interarrival time, in milliseconds, during the collection period. This value is the lowest interarrival jitter for all connections that were active during the collection period.

MaximumInterarrivalJitter (Status Parameter) | Table: LastPeriodsStats

Type	UInt32
Range	
Script/CLI	Mipt.LastPeriodsStats[].MaximumInterarrivalJitter
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.200.1.800

Maximum interarrival time, in milliseconds, during the collection period. This value is the highest interarrival jitter for all connections that were active during the collection period.

AverageInterarrivalJitter (Status Parameter) | Table: LastPeriodsStats

Type	UInt32
Range	
Script/CLI	Mipt.LastPeriodsStats[].AverageInterarrivalJitter
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.200.1.900

Average interarrival time, in milliseconds, during the collection period. This value is the weighted average of the interarrival jitter for all connections that were active during the collection period. For each connection, the total jitter of packets received during the collection period and the total number of packets received during the collection period are used in the weighted average calculation.

MinimumLatency (Status Parameter) | Table: LastPeriodsStats

Type	UInt32
Range	
Script/CLI	Mipt.LastPeriodsStats[].MinimumLatency
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.200.1.1000

Minimum latency, in milliseconds, during the collection period. This value is the lowest latency for all connections that were active during the collection period.

MaximumLatency (Status Parameter) | Table: LastPeriodsStats

Type	UInt32
Range	
Script/CLI	Mipt.LastPeriodsStats[].MaximumLatency
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.200.1.1100

Maximum latency, in milliseconds, during the collection period. This value is the highest latency for all connections that were active during the collection period.

AverageLatency (Status Parameter) | Table: LastPeriodsStats

Type	UInt32
Range	
Script/CLI	Mipt.LastPeriodsStats[].AverageLatency
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.200.1.1200

Average latency, in milliseconds, during the collection period. This value is the weighted average of the latency for all connections that were active during the collection period. For each connection, the total latency of packets received during the collection period and the total number of packets received during the collection period are used in the weighted average calculation.

PeriodBeginning (Status Parameter) | Table: LastPeriodsStats

Type	Text
Range	
Script/CLI	Mipt.LastPeriodsStats[].PeriodBeginning
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.200.1.1300

Date and time of the collection period beginning.

PeriodEnd (Status Parameter) | Table: LastPeriodsStats

Type	Text
Range	
Script/CLI	Mipt.LastPeriodsStats[].PeriodEnd
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.200.1.1400

Date and time of the collection period end.

ChannelStatistics (Table)

Statistics per endpoint/channel since last reboot or statistics reset.

EpChannelId (Index) | Table: ChannelStatistics

Type	Text
Range	
Script/CLI	Mipt.ChannelStatistics[].EpChannelId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.250.1.100

String that identifies the combination of an endpoint and a channel. The endpoint name is the same as the EpId used to refer to endpoints in other tables. On endpoints with multiple channels, the channel number must be appended at the end of the endpoint name, separated with a dash. Here are a few examples:

- Slot3/E1T1-12 refers to endpoint Slot3/E1T1, channel 12.
- Phone-Fax1 refers to FXS endpoint Phone-Fax1. No channel number is appended because FXS lines do not support multiple channels.

PacketsSent (Status Parameter) | Table: ChannelStatistics

Type	UInt32
Range	
Script/CLI	Mipt.ChannelStatistics[].PacketsSent
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.250.1.200

Number of packets transmitted on the channel since service start. This value is obtained by cumulating the packets transmitted in all the connections that ended during the collection period.

PacketsReceived (Status Parameter) | Table: ChannelStatistics

Type	UInt32
Range	
Script/CLI	Mipt.ChannelStatistics[].PacketsReceived
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.250.1.300

Number of packets received on the channel since service start. This value is obtained by cumulating the packets received in all the connections that ended during the collection period.

BytesSent (Status Parameter) | Table: ChannelStatistics

Type	UInt32
Range	
Script/CLI	Mipt.ChannelStatistics[].BytesSent
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.250.1.400

Number of bytes transmitted on the channel since service start. This value is obtained by cumulating the bytes transmitted in all the connections that ended during the collection period.

BytesReceived (Status Parameter) | Table: ChannelStatistics

Type	UInt32
Range	
Script/CLI	Mipt.ChannelStatistics[].BytesReceived
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.250.1.500

Number of bytes received on the channel since service start. This value is obtained by cumulating the bytes received in all the connections that ended during the collection period.

AverageReceiveInterarrivalJitter (Status Parameter) | Table: ChannelStatistics

Type	UInt32
Range	
Script/CLI	Mipt.ChannelStatistics[].AverageReceiveInterarrivalJitter
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.250.1.600

Average interarrival time, in microseconds, for the channel since service start. This value is based on the average interarrival jitter of each call ended during the collection period. The value is weighted by the duration of the calls.

Reset (Row Command) | Table: ChannelStatistics

Script/CLI:	Mipt.ChannelStatistics[].Reset
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.250.1.900

Sets all the values of the row to zero.

StatsCollectionPeriodDuration (Config Parameter)

Type	UInt32
Range	0..44640
Default	0
Script/CLI	Mipt.StatsCollectionPeriodDuration
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.300

Specifies the collection period duration (in minutes).

StatsPerConnectionNotificationEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.StatsPerConnectionNotificationEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.400

Enables the generation of connection end statistics notification.

- Enable: Notifications are generated.
- Disable: Notifications are not generated.

StatsPerPeriodNotificationEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.StatsPerPeriodNotificationEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.700.500

Enables the generation of period statistics notification.

- Enable: Notifications are generated.
- Disable: Notifications are not generated.

EnforceSymmetricRtpEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.EnforceSymmetricRtpEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.40000.100

For each bi-directional RTP streams, enforce that incoming RTP packets are from the same source as the destination of outgoing RTP packets.

- Enable: Silently discard incoming RTP packets with source address and port differing from the destination address and port of outgoing packets.
- Disable: Accept packets from all sources.

Enforcing symmetric RTP may prevent legitimate RTP streams coming from a media server from being processed, for example: Music and conferencing servers.

InteropDtmfRtpInitialPacketQty (Config Parameter)

Type	UInt32
Range	1..3
Default	3
Script/CLI	Mipt.InteropDtmfRtpInitialPacketQty
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.40000.200

Specifies the quantity of packets sent at the beginning of an Out-of-Band DTMF using RTP. This parameter also specifies the quantity of terminating packets that are sent at the end of the DTMF transmission.
Note that this parameter has an effect only if the **DtmfTransportMethod** parameter is set to 'OutOfBandUsingRtp'.

InteropPacketReceptionMode (Config Parameter)

Type	Enum
Range	Mode0(100) | Mode1(200)
Default	Mode1
Script/CLI	Mipt.InteropPacketReceptionMode
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.40000.300

The following modes control the type of processing applied at the reception of RTP packets.

- Mode0: Legacy mode. Supports receiving RTP packets with a wider range of packetisation times (ptime), however the call quality will be overly deteriorated on poor network conditions such as high jitter or packet loss.
- Mode1: Supports receiving RTP packets with a smaller range of packetisation times (ptime), however it will have an overall better call quality. During SRTP communications, this mode will be automatically applied regardless of the mode configured.

Refer to the Codec documentation for more details (e.g. DefaultCodecG711MulawMaxPTime).

The Mode0 extends the supported ptime range in reception only, as per the following:

- G.711: 10 - 100 ms, in increments of 1 ms.
- G.726: 10 - 100 ms, in increments of 1 ms.
- G.729: 10 - 100 ms, in increments of 10 ms.
- G.723.1: 30 - 120 ms, in increments of 30 ms.

PcmCaptureEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.PcmCaptureEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.50000.100.100

Enables PCM capture for the endpoint specified by the **PcmCaptureEndpoint** parameter and sends the capture to the host configured in the **PcmCaptureIpAddr** parameter.

The captured PCM received from the peer is sent to port 5001 and the captured PCM sent to the peer is sent to port 6001.

The PCM capture can be enabled/disabled on-the-fly. The capture starts right away if the endpoint is already in a call, or will be started the next time a call is established.

PcmCaptureEndpoint (Config Parameter)

Type	Text
Range	Size(0..64)
Default	
Script/CLI	Mipt.PcmCaptureEndpoint
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.50000.100.200

Unit's endpoint on which the PCM capture must be performed.
The endpoint name must match one of the epAdm/endpointTable/endpointEpId list. For digital interfaces (like ISDN), a "-Channel#" must be appended for the requested channel.

The list of endpoints is available under **EpAdm.EndpointTable**. Valid examples (depending of the platform) are:

- PCM capture is to be done on channel #3 of a PRI interface located in slot #2: Slot2/E1T1-3
- PCM capture is to be done on channel #2 of a BRI interface: Bri1-2
- PCM capture is to be done on the 16th FXS port: FXS16

Note that PCM capture does not support capturing on multiple endpoints simultaneously.

PcmCaptureIpAddr (Config Parameter)

Type	IpAddress
Range	
Default	
Script/CLI	Mipt.PcmCaptureIpAddr
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.50000.100.300

IP address where the captured PCM packets should be sent.

DspTracingEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.DspTracingEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.50000.200.100

Activates the DSP tracing.
When enabled, DSP debugging traces are sent to the syslog. The Diagnostic Traces must be enabled and the DSP trace level set to Debug in order to see these DSP traces. Refer to the Notifications and Logging Manager (Nlm) service's parameters **DiagnosticTracesEnable** and **DiagnosticTracesFilter**.

WARNING: Sensitive information may be sent in these traces. Use them only for debugging. Leaving them enabled for a long time is a security hole, and may also reduce system performance and affect voice quality.

DspStatsEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Mipt.DspStatsEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.50000.300.100

Activates the DSP channel statistics.
When enabled, in-call statistics from the DSP channels are sent to the syslog. The Diagnostic Traces must be enabled and the "Line/Line Engine" trace level set to Debug or All (nlmMIB/TacGroup) in order to see these statistics.

See the following **DspStatsInterval** and **DspStatsFilter** parameters for more configuration.

WARNING: Enabling the DSP channel statistics might slow down the system and reduce voice quality. Use only for debugging or troubleshooting.

DspStatsInterval (Config Parameter)

Type	UInt32
Range	0..3600
Default	0
Script/CLI	Mipt.DspStatsInterval
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.50000.300.200

The time interval, in seconds, between each statistics request.
When greater than 0, it outputs the statistics at the interval specified, and at channel closing.

When the interval is 0, it outputs the statistics only at channel closing.

DspStatsFilter (Config Parameter)

Type	UInt32
Range	0..255
Default	0
Script/CLI	Mipt.DspStatsFilter
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.50000.300.300

Sum the values of the statistics groups wanted:

- DIM_STAT_ID_EC_DBG (1): Echo Canceller.
- DIM_STAT_ID_ERROR (2): Error.
- DIM_STAT_ID_FAX_RELAY (4): Fax T38.
- DIM_STAT_ID_RX_TX (8): Transmit/Receive.
- DIM_STAT_ID_SEC_RTP (16): Security SRTP.
- DIM_STAT_ID_VAD (32): Voice Activity Detection.
- DIM_STAT_ID_VQMON (64): Voice Quality Monitor.
- DIM_STAT_ID_VP (128): Voice Playout.

For example a value of 8 means DIM_STAT_ID_RX_TX statistics only, a value of 12 means DIM_STAT_ID_FAX_RELAY and DIM_STAT_ID_RX_TX, and a value of 255 means all groups.

This feature is not available on all products. Refer to the Software Configuration Guide for more details.

WARNING: Requesting a lot of statistics might slow down the system and reduce voice quality. Use only for debugging or troubleshooting.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Mipt.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Mipt.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1600.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

ResetPeriod (Command)

The `ResetPeriod` command is used to reset only the statistics of the current period. The previous periods are left unchanged.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Mipt service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.1600.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	The call %1$d on endpoint %2$s cannot be initiated because there are no codecs enabled.	Error	The call cannot be initiated because all codecs are disabled. Enable at least one codec to solve this problem.
20	The call %1$d on endpoint %2$s detects a fax/modem transmission.	Debug	A fax or modem transmission is detected on the endpoint. The endpoint will swtich to data mode according to the configuration.
30	The call %1$d on endpoint %2$s cannot be initiated because the selected codec in the codec versus bearer capabilities mapping table is disabled.	Error	The call cannot be initiated because the selected codec in the codec versus bearer capabilities mapping table is disabled. Enable at least one codec in the codec versus bearer capabilities mapping table to solve this problem.
40	The call %1$d on endpoint %2$s uses unsecure RTP because the peer does not support secure RTP.	Warning	This message is sent when both RTP secure and unsecure is enabled locally and the peer does not support secure RTP.
50	The call %1$d on endpoint %2$s cannot be initiated because the peer did not offer secure RTP.	Error	This message is sent when only secure RTP is enabled locally and receiving an offer from the peer that does not contain a secure RTP stream.
60	The call %1$d on endpoint %2$s cannot be initiated because the peer did not offer unsecure RTP.	Error	This message is sent when only unsecure RTP is enabled locally and receiving an offer from the peer that does not contain an unsecure RTP stream.
70	The call %1$d on endpoint %2$s detected a MIKEY protocol error in the SDP received from the peer.	Warning	This message is sent when a protocol error occurs with MIKEY (syntax error, invalid timestamp, incompatible security policies, invalid key-management ids, etc.).
75	The call %1$d on endpoint %2$s detected a SDES protocol error in the SDP received from the peer.	Warning	This message is sent when a protocol error occurs with SDES (invalid crypto attributes, unsupported crypto suite, invalid keys, etc.).

NumKey	Message	Severity	Description
80	Last connection statistics: PT=%d PR= %d PL=%d OT=%d OR= %d JMIN=%d JMAX= %d JAVG=%d LMIN=%d LMAX=%d LAVG=%d.	Info	The statistics of the last terminated connection. The parameters are: • PT: Packets Transmitted; • PR: Packets Received; • PL: Packets Lost; • OT: Octets Transmitted; • OR: Octets Received; • JMIN: Minimum Jitter; • JMAX: Maximum Jitter; • JAVG: Average Jitter; • LMIN: Minimum Latency; • LMAX: Maximum Latency; • LAVG: Average Latency.

NumKey	Message	Severity	Description
90	Last collection period: PT=%d PR=%d PL=%d OT=%d OR=%d JMIN=%d JMAX=%d JAVG=%d LMIN=%d LMAX=%d LAVG=%d PB=%s PE=%s.	Info	The statistics of the last completed collection period. The parameters are: • PT: Packets Transmitted; • PR: Packets Received; • PL: Packets Lost; • OT: Octets Transmitted; • OR: Octets Received; • JMIN: Minimum Jitter; • JMAX: Maximum Jitter; • JAVG: Average Jitter; • LMIN: Minimum Latency; • LMAX: Maximum Latency; • LAVG: Average Latency. • PB: Period Beginning. • PE: Period End.
100	The call %1$d on endpoint %2$s is configured for %3$s but received %4$s from the peer.	Warning	This happens from a key management protocol misconfiguration. Change the key management protocol to reflect the one used by the peer. Not doing so will result in calls that cannot be secured.

NumKey	Message	Severity	Description
110	The call %1$d on endpoint %2$s detected an SRTP cryptographic error. The secured RTP stream is not properly decoded.	Error	This message is sent when a cryptographic error occurs with the SRTP cryptographic context (invalid crypto session, invalid keys, invalid sequence number, etc.).
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.

NumKey	Message	Severity	Description
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.

NumKey	Message	Severity	Description
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Mipt.

Message	Severity	Description
The %1$d base port value is too close to the upper boundary limit to accommodate all the telephony ports. Please reduce its value.	Warning	When using all features such as second call and/or call conference, the number of ports may exceed the upper boundary limit (65535), which would cause the UDP ports to start over at number 1.
Usage of deprecated SessionUpdateCryptoMode should be avoided.	Warning	A deprecated parameter should be avoided, since it will eventually be removed completely. Please use the **Mipt.CryptoModeWhenSendingOffer**, **Mipt.CryptoModeWhenSendingAnswer** and **Mipt.CryptoContextBehavior** parameters instead.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.

Message	Severity	Description
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Music on Hold (Moh)

The Music on Hold (MOH) service manages the option to play an audio file when a telephony endpoint is on hold.

Parameters

FileUrl (Config Parameter)

Type	Text
Range	
Default	
Script/CLI	Moh.FileUrl
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1550.1.100

URL to a MP3 file that is loaded at unit startup and reloaded every time the **ReloadInterval** elapses. The supported transfer protocols are:

- HTTP
- TFTP
- FTP
- FILE

Examples of valid URLs:

- http://www.myserver.com/myfile.mp3
- tftp://myserver.com:69/myfolder/myfile.mp3
- file://myfile.mp3

When the port is not included in the URL, the default port for the chosen protocol is used.

Username (Config Parameter)

Type	Text
Range	
Default	
Script/CLI	Moh.Username
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1550.1.200

When authentication is required by the remote file server, this parameter is used as the username.

Password (Config Parameter)

Type	Text
Range	Size(0..255)
Default	
Script/CLI	Moh.Password
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1550.1.300

When authentication is required by the remote file server, this parameter is used as the password. Password encryption is supported via the **Dcm.PasswordEncryption** table.

When **Dcm.PasswordEncryption** is enabled clear text passwords will be automatically encrypted.

Unencrypted password maximal length is 63.

Encrypted password maximal length is 113.

ReloadInterval (Config Parameter)

Type	UInt32
Range	0..6000
Default	0
Script/CLI	Moh.ReloadInterval
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1550.1.400

Time, in hours, between attempts to load the MP3 file. A value of 0 loads the file only once at unit startup. Any other value between 1 and 6000 is the number of hours between automatic reloads of the file. When a manual file download is triggered, the counter is not reset so the next reload will happen at the same time.

FileStatus (Status Parameter)

Type	Enum
Range	NoFile(100) | FileReady(200) | Downloading(300) | InvalidFormat(400) | FileTooLarge(500)
Script/CLI	Moh.FileStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1550.1.500

Status of the MP3 file in the unit.

- NoFile: No file is currently loaded in the unit.
- FileReady: A valid file is currently loaded in the unit.
- Downloading: A file is currently being downloaded.
- InvalidFormat: The downloaded file as an invalid format.
- FileTooLarge: The downloaded file is too large.

LastTransferStatus (Status Parameter)

Type	Enum
Range	Success(100) | Failed(200)
Script/CLI	Moh.LastTransferStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1550.1.600

Status of the last file transfer attempt.

- Success: Last file transfer succeeded.
- Failed: Last file transfer failed.

LastTransferDateTime (Status Parameter)

Type	Text
Range	Size(0..255)
Script/CLI	Moh.LastTransferDateTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1550.1.700

Date and time of the last successful music file transfer.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Moh.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1550.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Moh.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1550.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

CancelTransfer (Command)

When a file transfer is in progress, it stops it. Nothing is done otherwise.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

Transfer (Command)

Launches the download of the MP3 file.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Moh service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.1550.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	The MP3 file has been loaded successfully.	Info	The MP3 file has been loaded successfully during unit startup.
15	The MP3 file transfer has been cancelled successfully.	Info	Could not complete the download because the process is cancelled.
20	The MP3 file is too large. The maximum allowed size is %1$d kilobytes.	Error	The MP3 file to be loaded is too large and has not been loaded in the unit.
30	The file downloaded has an invalid format.	Error	The file downloaded does not follow the format required by the unit.
40	%1$s URL is invalid, download cancelled.	Error	URL format is invalid and the download has been cancelled.
50	Download cancelled, a download is currently in progress.	Error	The download has been cancelled since a download is currently being performed. A download must be stopped or completed before another download can be triggered.
60	Download cancellation failed, there are no downloads in progress.	Warning	Could not complete the download cancellation because there is no download currently in progress.
70	Unable to transfer the requested file, reason: trying to access forbidden path.	Error	This message is issued when the MOH service fails to transfer the requested file because the specified path points to a forbidden location.
80	Unable to transfer the requested file because the connection failed.	Error	This message is issued when the Moh service fails to transfer the requested file because the connection could not be established.
90	Unable to transfer the requested file, because no file was found.	Error	This message is issued when Moh fails to transfer the requested file because the host reports it does not exist.
100	Unable to transfer the requested file, because access was denied.	Error	This message is issued when Moh fails to transfer the requested file because authentication failed.
110	Unable to transfer the requested file, because connection timed out.	Error	This message is issued when Moh fails to transfer the requested file, a timeout occurred.
120	Unable to transfer the requested file, because there was an internal error.	Error	This message is issued when Moh fails to transfer the requested file, an unexpected situation happened.

NumKey	Message	Severity	Description
130	Unable to transfer the requested file, because host name could not be resolved.	Error	This message is issued when Moh fails to transfer the requested file because the host name cannot be resolved.
140	Unable to transfer the requested file, because either host or port are unreachable.	Error	This message is issued when Moh fails to transfer the requested file because the host or port cannot be reached.
150	MP3 file decoding could not be started successfully.	Error	This message is sent when MP3 file decoding could not be started successfully.
160	MP3 file decoding could not be stopped successfully.	Error	This message is sent when MP3 file decoding could not be stopped successfully.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.

NumKey	Message	Severity	Description
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.

NumKey	Message	Severity	Description
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Moh.

Message	Severity	Description
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.

Message	Severity	Description
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Network Address Translation (Nat)

The Network Address Translation (NAT) service allows the administrator to change the source or destination IP address of a packet.

Parameters

ConfigModifiedStatus (Status Parameter)

Type	Enum
Range	Yes(100) | No(200)
Script/CLI	Nat.ConfigModifiedStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.100

Shows whether or not the Network Address Translation configuration has been modified without being applied.

1. Yes: The configuration has been modified but it has not been applied.
2. No: The Network Address Translation service uses the configured rules.

Use the command `Nat.ApplyConfig` to apply the configuration.

SNatRulesStatus (Table)

This table shows the rules applied in the source NAT.

Priority (Index) | Table: SNatRulesStatus

Type	UInt32
Range	
Script/CLI	Nat.SNatRulesStatus[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.200.1.100

Unique identifier of the row in the table.

SourceAddress (Status Parameter) | Table: SNatRulesStatus

Type	Text
Range	
Script/CLI	Nat.SNatRulesStatus[].SourceAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.200.1.200

Source address[/mask] criteria an incoming packet must have to match this rule.
An empty string matches any address.

Cannot be an empty string if the destination address is already empty.

SourcePort (Status Parameter) | Table: SNatRulesStatus

Type	Text
Range	
Script/CLI	Nat.SNatRulesStatus[].SourcePort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.200.1.300

Source port[-port] criteria an incoming packet must have to match this rule.
MinPort-MaxPort specifies a port range.

An empty string means that no filtering is applied on the source port thus matching any port.

This parameter is only effective when the **SNatRulesStatus.Protocol** parameter is set to Tcp or Udp.

DestinationAddress (Status Parameter) | Table: SNatRulesStatus

Type	Text
Range	
Script/CLI	Nat.SNatRulesStatus[].DestinationAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.200.1.400

Destination address[/mask] criteria an incoming packet must have to match this rule.
An empty string matches any address.

Cannot be an empty string if the source address is already empty.

DestinationPort (Status Parameter) | Table: SNatRulesStatus

Type	Text
Range	
Script/CLI	Nat.SNatRulesStatus[].DestinationPort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.200.1.500

Destination port[-port] criteria an incoming packet must have to match this rule.
MinPort-MaxPort specifies a port range.

An empty string means that no filtering is applied on the destination port thus matching any port.

This parameter is only effective when the **SNatRulesStatus.Protocol** parameter is set to Tcp or Udp.

Protocol (Status Parameter) | Table: SNatRulesStatus

Type	Enum
Range	All(100) | Tcp(200) | Udp(300) | Icmp(400)
Script/CLI	Nat.SNatRulesStatus[].Protocol
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.200.1.600

Protocol criteria an incoming packet must have to match this rule.
The protocol can be one of the following:

- All: Match packets using any protocol.
- Tcp: Only match TCP packets.
- Udp: Only match UDP packets.

- Icmp: Only match ICMP packets.

NewAddress (Status Parameter) | Table: SNatRulesStatus

Type	Text
Range	
Script/CLI	Nat.SNatRulesStatus[].NewAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.200.1.700

New address[:port] applied to the source of the packet.
When specifying a port number, it is mandatory to have the protocol set to TCP or UDP.

SNatRules (Table: user-defined, 20 lines max.)

This table shows the configured rules for source NAT.

Priority (Index) | Table: SNatRules

Type	UInt32
Range	
Script/CLI	Nat.SNatRules[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.700.1.100

Unique identifier of the row in the table.

Activation (Config Parameter) | Table: SNatRules

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Nat.SNatRules[].Activation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.700.1.200

Activates this rule.

- Enable: This rule is active in the SNAT.

- Disable: This rule is not in the SNAT.

SourceAddress (Config Parameter) | Table: SNatRules

Type	Text
Range	Size(0..51)
Default	
Script/CLI	Nat.SNatRules[].SourceAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.700.1.300

Source address of the incoming packet using the following format: address[/mask] or network interface name/.
Address can be either a network IP address (using /mask) or one of the host IP addresses.

When specifying a network interface name, it is mandatory to use the suffix "/". Doing so indicates that the network address of this interface is used instead of the host address. Also, it must match one of the values in the parameter **networkInterfacesStatusTable.InterfaceName** from the Basic Network Interface (BNI) service. Note that if the specified network interface is disabled or removed, the rule is automatically disabled thus removed from the NAT. When the network interface is enabled or added back, the rule is automatically enabled and applied in the NAT.

Mask must be a plain number specifying the number of binary 1s at the left side of the network mask. E.g.: a mask of 24 specifies a network mask of 255.255.255.0.

Leaving the default empty string matches any address.

Cannot be an empty string if the destination address is already empty.

SourcePort (Config Parameter) | Table: SNatRules

Type	Text
Range	Size(0..11)
Default	
Script/CLI	Nat.SNatRules[].SourcePort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.700.1.400

Source port of the incoming packet using the following format: port[-port].
MinPort-MaxPort specifies a port range.

The default empty string means that no filtering is applied on the source port thus matching any port.

This parameter is only effective when the **SNatRules.Protocol** parameter is set to Tcp or Udp.

DestinationAddress (Config Parameter) | Table: SNatRules

Type	Text
Range	Size(0..51)
Default	
Script/CLI	Nat.SNatRules[].DestinationAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.700.1.500

Destination address of the incoming packet using the following format: address[/mask] or network interface name/.
Address can be either a network IP address (using /mask) or one of the host IP addresses.

When specifying a network interface name, it is mandatory to use the suffix "/". Doing so indicates that the network address of this interface is used instead of the host address. Also, it must match one of the values in the parameter **networkInterfacesStatusTable.InterfaceName** from the Basic Network Interface (BNI) service. Note that if the specified network interface is disabled or removed, the rule is automatically disabled thus removed from the NAT. When the network interface is enabled or added back, the rule is automatically enabled and applied in the NAT.

Mask must be a plain number specifying the number of binary 1s at the left side of the network mask. E.g.: a mask of 24 specifies a network mask of 255.255.255.0.

Leaving the default empty string matches any address.

Cannot be an empty string if the source address is already empty.

DestinationPort (Config Parameter) | Table: SNatRules

Type	Text
Range	Size(0..11)
Default	
Script/CLI	Nat.SNatRules[].DestinationPort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.700.1.600

Destination port of the incoming packet using the following format: port[-port].
MinPort-MaxPort specifies a port range.

The default empty string means that no filtering is applied on the destination port thus matching any port.

This parameter is only effective when the **SNatRules.Protocol** parameter is set to Tcp or Udp.

Protocol (Config Parameter) | Table: SNatRules

Type	Enum
Range	All(100) | Tcp(200) | Udp(300) | Icmp(400)
Default	All
Script/CLI	Nat.SNatRules[].Protocol
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.700.1.700

Protocol of the incoming packet.
The protocol can be one of the following:

- All: Match packets using any protocol.
- Tcp: Only match TCP packets.
- Udp: Only match UDP packets.
- Icmp: Only match ICMP packets.

NewAddress (Config Parameter) | Table: SNatRules

Type	Text
Range	Size(0..51)
Default	
Script/CLI	Nat.SNatRules[].NewAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.700.1.800

New address applied to the source of the packet using the following syntax: address[:port].
When specifying a port number, it is mandatory to have the protocol set to TCP or UDP.

Up (Row Command) | Table: SNatRules

Script/CLI:	Nat.SNatRules[].Up
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.700.1.900

Moves the current row upside.

Down (Row Command) | Table: SNatRules

Script/CLI:	Nat.SNatRules[].Down
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.700.1.1000

Moves the current row downside.

Insert (Row Command) | Table: SNatRules

Script/CLI:	Nat.SNatRules[].Insert
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.700.1.1100

Inserts a new row before this row.

Delete (Row Command) | Table: SNatRules

Script/CLI:	Nat.SNatRules[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.700.1.1200

Deletes this row.

DNatRulesStatus (Table)

This table shows the rules applied in the destination NAT.

Priority (Index) | Table: DNatRulesStatus

Type	UInt32
Range	
Script/CLI	Nat.DNatRulesStatus[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.800.1.100

Unique identifier of the row in the table.

SourceAddress (Status Parameter) | Table: DNatRulesStatus

Type	Text
Range	
Script/CLI	Nat.DNatRulesStatus[].SourceAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.800.1.200

Source address[/mask] criteria an incoming packet must have to match this rule.
An empty string matches any address.

Cannot be an empty string if the destination address is already empty.

SourcePort (Status Parameter) | Table: DNatRulesStatus

Type	Text
Range	
Script/CLI	Nat.DNatRulesStatus[].SourcePort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.800.1.300

Source port[-port] criteria an incoming packet must have to match this rule.
MinPort-MaxPort specifies a port range.

An empty string means that no filtering is applied on the source port thus matching any port.

This parameter is only effective when the **DNatRulesStatus.Protocol** parameter is set to Tcp or Udp.

DestinationAddress (Status Parameter) | Table: DNatRulesStatus

Type	Text
Range	
Script/CLI	Nat.DNatRulesStatus[].DestinationAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.800.1.400

Destination address[/mask] criteria an incoming packet must have to match this rule.
An empty string matches any address.

Cannot be an empty string if the source address is already empty.

DestinationPort (Status Parameter) | Table: DNatRulesStatus

Type	Text
Range	
Script/CLI	Nat.DNatRulesStatus[].DestinationPort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.800.1.500

Destination port[-port] criteria an incoming packet must have to match this rule.
MinPort-MaxPort specifies a port range.

An empty string means that no filtering is applied on the destination port thus matching any port.

This parameter is only effective when the **DNatRulesStatus.Protocol** parameter is set to Tcp or Udp.

Protocol (Status Parameter) | Table: DNatRulesStatus

Type	Enum
Range	All(100) | Tcp(200) | Udp(300) | Icmp(400)
Script/CLI	Nat.DNatRulesStatus[].Protocol
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.800.1.600

Protocol criteria an incoming packet must have to match this rule.
The protocol can be one of the following:

- All: Match packets using any protocol.
- Tcp: Only match TCP packets.
- Udp: Only match UDP packets.
- Icmp: Only match ICMP packets.

NewAddress (Status Parameter) | Table: DNatRulesStatus

Type	Text
Range	
Script/CLI	Nat.DNatRulesStatus[].NewAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.800.1.700

New address[:port] applied to the destination of the packet.

When specifying a port number, it is mandatory to have the protocol set to TCP or UDP.

DNatRules (Table: user-defined, 20 lines max.)

This table shows the configured rules for destination NAT.

Priority (Index) | Table: DNatRules

Type	UInt32
Range	
Script/CLI	Nat.DNatRules[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.900.1.100

Unique identifier of the row in the table.

Activation (Config Parameter) | Table: DNatRules

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Nat.DNatRules[].Activation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.900.1.200

Activations this rule.

- Enable: This rule is active in the DNAT.
- Disable: This rule is not in the DNAT.

SourceAddress (Config Parameter) | Table: DNatRules

Type	Text
Range	Size(0..51)
Default	
Script/CLI	Nat.DNatRules[].SourceAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.900.1.300

Source address of the incoming packet using the following format: address[/mask] or network interface name/.
Address can be either a network IP address (using /mask) or one of the host IP addresses.

When specifying a network interface name, it is mandatory to use the suffix "/". Doing so indicates that the network address of this interface is used instead of the host address. Also, it must match one of the values in the parameter **networkInterfacesStatusTable.InterfaceName** from the Basic Network Interface (BNI) service. Note that if the specified network interface is disabled or removed, the rule is automatically disabled thus removed from the NAT. When the network interface is enabled or added back, the rule is automatically enabled and applied in the NAT.

Mask must be a plain number specifying the number of binary 1s at the left side of the network mask. E.g.: a mask of 24 specifies a network mask of 255.255.255.0.

Leaving the default empty string matches any address.

Cannot be an empty string if the destination address is already empty.

SourcePort (Config Parameter) | Table: DNatRules

Type	Text
Range	Size(0..11)
Default	
Script/CLI	Nat.DNatRules[].SourcePort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.900.1.400

Source port of the incoming packet using the following format: port[-port].
MinPort-MaxPort specifies a port range.

The default empty string means that no filtering is applied on the source port thus matching any port.

This parameter is only effective when the **DNatRules.Protocol** parameter is set to Tcp or Udp.

DestinationAddress (Config Parameter) | Table: DNatRules

Type	Text
Range	Size(0..51)
Default	
Script/CLI	Nat.DNatRules[].DestinationAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.900.1.500

Destination address of the incoming packet using the following format: address[/mask] or network interface name/.

Address can be either a network IP address (using /mask) or one of the host IP addresses.

When specifying a network interface name, it is mandatory to use the suffix "/". Doing so indicates that the network address of this interface is used instead of the host address. Also, it must match one of the values in the parameter **networkInterfacesStatusTable.InterfaceName** from the Basic Network Interface (BNI) service. Note that if the specified network interface is disabled or removed, the rule is automatically disabled thus removed from the NAT. When the network interface is enabled or added back, the rule is automatically enabled and applied in the NAT.

Mask must be a plain number specifying the number of binary 1s at the left side of the network mask. E.g.: a mask of 24 specifies a network mask of 255.255.255.0.

Leaving the default empty string matches any address.

Cannot be an empty string if the source address is already empty.

DestinationPort (Config Parameter) | Table: DNatRules

Type	Text
Range	Size(0..11)
Default	
Script/CLI	Nat.DNatRules[].DestinationPort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.900.1.600

Destination port of the incoming packet using the following format: port[-port].
MinPort-MaxPort specifies a port range.

The default empty string means that no filtering is applied on the destination port thus matching any port.

This parameter is only effective when the **DNatRules.Protocol** parameter is set to Tcp or Udp.

Protocol (Config Parameter) | Table: DNatRules

Type	Enum
Range	All(100) | Tcp(200) | Udp(300) | Icmp(400)
Default	All
Script/CLI	Nat.DNatRules[].Protocol
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.900.1.700

Protocol of the incoming packet.
The protocol can be one of the following:

- All: Match packets using any protocol.

- Tcp: Only match TCP packets.
- Udp: Only match UDP packets.
- Icmp: Only match ICMP packets.

NewAddress (Config Parameter) | Table: DNatRules

Type	Text
Range	Size(0..51)
Default	
Script/CLI	Nat.DNatRules[].NewAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.900.1.800

New address applied to the destination of the packet using the following syntax: address[:port]. When specifying a port number, it is mandatory to have the protocol set to TCP or UDP.

Up (Row Command) | Table: DNatRules

Script/CLI:	Nat.DNatRules[].Up
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.900.1.900

Moves the current row upside.

Down (Row Command) | Table: DNatRules

Script/CLI:	Nat.DNatRules[].Down
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.900.1.1000

Moves the current row downside.

Insert (Row Command) | Table: DNatRules

Script/CLI:	Nat.DNatRules[].Insert
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.900.1.1100

Inserts a new row before this row.

Delete (Row Command) | Table: DNatRules

Script/CLI:	Nat.DNatRules[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.900.1.1200

Deletes this row.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Nat.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Nat.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2275.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

ApplyConfig (Command)

Applies the configured rules.

InsertDestinationRule (Command)

Inserts a new row at the end of the **NatRules** table.

InsertSourceRule (Command)

Inserts a new row at the end of the **NatRules** table.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

RollbackConfig (Command)

Rolls back the current configuration to the running configuration as showed in the status.
The current configuration is lost.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Nat service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.2275.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.

NumKey	Message	Severity	Description
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Nat.

Message	Severity	Description
Specify a source or destination address.	Error	Need at least a source address or a destination address defined.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.

Message	Severity	Description
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Network Firewall (Nfw)

The Network Firewall (NFW) service allows the administrator to filter traffic that is routed between networks.

Parameters

ConfigModifiedStatus (Status Parameter)

Type	Enum
Range	Yes(100) | No(200)
Script/CLI	Nfw.ConfigModifiedStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.100

Shows whether or not the Network Firewall configuration has been modified without being applied.

1. Yes: The configuration has been modified but it has not been applied.
2. No: The Network Firewall service uses the configured rules.

Use the `Nfw.ApplyConfig` command to apply the configuration.

NetworkRulesStatus (Table)

This table shows the network rules applied in the firewall.

Priority (Index) | Table: NetworkRulesStatus

Type	UInt32
Range	
Script/CLI	Nfw.NetworkRulesStatus[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.200.1.100

Unique identifier of the row in the table.

SourceAddress (Status Parameter) | Table: NetworkRulesStatus

Type	Text
Range	
Script/CLI	Nfw.NetworkRulesStatus[].SourceAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.200.1.200

Source address[/mask] criteria an incoming packet must have to match this rule.
An empty string matches any address.

SourcePort (Status Parameter) | Table: NetworkRulesStatus

Type	Text
Range	
Script/CLI	Nfw.NetworkRulesStatus[].SourcePort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.200.1.300

Source port[-port] criteria an incoming packet must have to match this rule.
MinPort-MaxPort specifies a port range.

An empty string means that no filtering is applied on the source port thus matching any port.

This parameter is only effective when the **NetworkRulesStatus.Protocol** parameter is set to Tcp or Udp.

DestinationAddress (Status Parameter) | Table: NetworkRulesStatus

Type	Text
Range	
Script/CLI	Nfw.NetworkRulesStatus[].DestinationAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.200.1.400

Destination address[/mask] criteria an incoming packet must have to match this rule.
An empty string matches any address.

DestinationPort (Status Parameter) | Table: NetworkRulesStatus

Type	Text
Range	
Script/CLI	Nfw.NetworkRulesStatus[].DestinationPort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.200.1.500

Destination port[-port] criteria an incoming packet must have to match this rule.
MinPort-MaxPort specifies a port range.

An empty string means that no filtering is applied on the destination port thus matching any port.

This parameter is only effective when the **NetworkRulesStatus.Protocol** parameter is set to Tcp or Udp.

Protocol (Status Parameter) | Table: NetworkRulesStatus

Type	Enum
Range	All(100) | Tcp(200) | Udp(300) | Icmp(400)
Script/CLI	Nfw.NetworkRulesStatus[].Protocol
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.200.1.600

Protocol criteria an incoming packet must have to match this rule.
The protocol can be one of the following:

- All: Match packets using any protocols.
- Tcp: Only match TCP packets.
- Udp: Only match UDP packets.

- Icmp: Only match ICMP packets.

ConnectionState (Status Parameter) | Table: NetworkRulesStatus

Type	Enum
Range	All(100) | New(200) | EstablishedOrRelated(300)
Script/CLI	Nfw.NetworkRulesStatus[].ConnectionState
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.200.1.650

Connection state associated with the incoming packet.
The connection state can be one of the following:

- All: Match packets in any state.
- New: Match packets that are not part of an existing connection.
- EstablishedOrRelated: Match packets that are part of an existing connection.

BlacklistEnable (Status Parameter) | Table: NetworkRulesStatus

Type	EnableDisable
Range	
Script/CLI	Nfw.NetworkRulesStatus[].BlacklistEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.200.1.660

Indicates if blacklisting is enabled for this rule.

- Enable: When a packet establishing a connection matches this rule, the action is executed and the source IP address is added to the blacklist.
- Disable: When a packet establishing a connection matches this rule, the action is executed but the source IP address is not added to the blacklist.

Note: If rate limiting is enabled for this rule, blacklisted IP addresses are added to the rate limit blacklist.

RateLimitValue (Status Parameter) | Table: NetworkRulesStatus

Type	UInt32
Range	1..5000
Script/CLI	Nfw.NetworkRulesStatus[].RateLimitValue
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.200.1.670

Number of packets allowed to match this rule from a single source IP address within a certain time period.

RateLimitTimePeriod (Status Parameter) | Table: NetworkRulesStatus

Type	UInt32
Range	1..86400
Script/CLI	Nfw.NetworkRulesStatus[].RateLimitTimePeriod
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.200.1.680

The time period on which to base the rate limit. This period is expressed in seconds.
Ex.: a **RateLimitValue** of 10 and a **RateLimitTimePeriod** of 60 means a limit of 10 new connections per minute.

Action (Status Parameter) | Table: NetworkRulesStatus

Type	Enum
Range	Accept(100) | Reject(200) | Drop(300) | RateLimitPerSource(400)
Script/CLI	Nfw.NetworkRulesStatus[].Action
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.200.1.700

Action taken when this rule matches a packet.
Action can be one of the following:

- Accept: Let the packet through.
- Reject: Send back an ICMP port unreachable in response to the matched packet, the packet is then dropped.
- Drop: The packet is dropped without any notification.

DefaultPolicy (Config Parameter)

Type	Enum
Range	Accept(100) | Drop(300)
Default	Drop
Script/CLI	Nfw.DefaultPolicy
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.550

Action taken when a packet does not match any rule.
Default policy can be one of the following:

- Accept: Let the packet through.
- Drop: The packet is dropped without any notification.

To have no filtering applied to forwarded packets, set the default policy to 'Accept' and remove all rules from the network firewall.

NetworkRules (Table: user-defined, 20 lines max.)

This table shows the configured network rules for the firewall.

Priority (Index) | Table: NetworkRules

Type	UInt32
Range	
Script/CLI	Nfw.NetworkRules[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.600.1.100

Unique identifier of the row in the table.

Activation (Config Parameter) | Table: NetworkRules

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Nfw.NetworkRules[].Activation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.600.1.200

Activates this rule.

- Enable: This rule is active in the firewall.
- Disable: This rule is not in the firewall.

SourceAddress (Config Parameter) | Table: NetworkRules

Type	Text
Range	Size(0..51)
Default	
Script/CLI	Nfw.NetworkRules[].SourceAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.600.1.300

Source address of the incoming packet using the following format: address[/mask] or network interface name/.
Address can be either a network IP address (using /mask) or one of the host IP addresses.

When specifying a network interface name, it is mandatory to use the suffix "/". Doing so indicates that the network address of this interface is used instead of the host address. Also, it must match one of the values in the **networkInterfacesStatusTable.InterfaceName** parameter from the Basic Network Interface (BNI) service. Note that if the specified network interface is disabled or removed, the rule is automatically disabled thus removed from the firewall. When the network interface is enabled or added back, the rule is automatically enabled and applied in the firewall.

Mask must be a plain number specifying the number of binary 1s at the left side of the network mask. E.g.: a mask of 24 specifies a network mask of 255.255.255.0.

Leaving the default empty string matches any address.

SourcePort (Config Parameter) | Table: NetworkRules

Type	Text
Range	Size(0..11)
Default	
Script/CLI	Nfw.NetworkRules[].SourcePort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.600.1.400

Source port of the incoming packet using the following format: port[-port].
MinPort-MaxPort specifies a port range.

The default empty string means that no filtering is applied on the source port thus matching any port.

This parameter is only effective when the **NetworkRules.Protocol** parameter is set to Tcp or Udp.

DestinationAddress (Config Parameter) | Table: NetworkRules

Type	Text
Range	Size(0..51)
Default	
Script/CLI	Nfw.NetworkRules[].DestinationAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.600.1.500

Destination address of the incoming packet using the following format: address[/mask] or network interface name/.
The address can either be a network IP address (using /mask) or one of the host IP addresses.

When specifying a network interface name, it is mandatory to use the suffix "/". Doing so indicates that the network address of this interface is used instead of the host address. Also, it must match one of the values in the **networkInterfacesStatusTable.InterfaceName** parameter from the Basic Network Interface (BNI) service. Note that if the specified network interface is disabled or removed, the rule is automatically disabled thus removed from the firewall. When the network interface is enabled or added back, the rule is automatically enabled and applied in the firewall.

Mask must be a plain number specifying the number of binary 1s at the left side of the network mask. E.g.: a mask of 24 specifies a network mask of 255.255.255.0.

Leaving the default empty string matches any address.

DestinationPort (Config Parameter) | Table: NetworkRules

Type	Text
Range	Size(0..11)
Default	
Script/CLI	Nfw.NetworkRules[].DestinationPort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.600.1.600

Destination port of the incoming packet using the following format: port[-port].
MinPort-MaxPort specifies a port range.

The default empty string means that no filtering is applied on the destination port thus matching any port.

This parameter is only effective when the **NetworkRules.Protocol** parameter is set to Tcp or Udp.

Protocol (Config Parameter) | Table: NetworkRules

Type	Enum
Range	All(100) | Tcp(200) | Udp(300) | Icmp(400)
Default	All
Script/CLI	Nfw.NetworkRules[].Protocol
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.600.1.700

Protocol of the incoming packet.
The protocol can be one of the following:

- All: Match packets using any protocols.
- Tcp: Only match TCP packets.
- Udp: Only match UDP packets.
- Icmp: Only match ICMP packets.

BlacklistEnable (Config Parameter) | Table: NetworkRules

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Nfw.NetworkRules[].BlacklistEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.600.1.720

Indicates if blacklisting is enabled for this rule.

- Enable: When a packet establishing a connection matches this rule, the action is executed and the source IP address is added to the blacklist.
- Disable: When a packet establishing a connection matches this rule, the action is executed but the source IP address is not added to the blacklist.

Note: If rate limiting is enabled for this rule, blacklisted IP addresses are added to the rate limit blacklist.

RateLimitValue (Config Parameter) | Table: NetworkRules

Type	UInt32
Range	1..5000
Default	10
Script/CLI	Nfw.NetworkRules[].RateLimitValue
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.600.1.730

Number of packets allowed to match this rule from a single source IP address within a certain time period.

RateLimitTimePeriod (Config Parameter) | Table: NetworkRules

Type	UInt32
Range	1..86400
Default	60
Script/CLI	Nfw.NetworkRules[].RateLimitTimePeriod
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.600.1.740

The time period on which to base the rate limit. This period is expressed in seconds.
Ex.: a **RateLimitValue** of 10 and a **RateLimitTimePeriod** of 60 means a limit of 10 packets per minute.

ConnectionState (Config Parameter) | Table: NetworkRules

Type	Enum
Range	All(100) | New(200) | EstablishedOrRelated(300)
Default	All
Script/CLI	Nfw.NetworkRules[].ConnectionState
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.600.1.750

Connection state associated with the incoming packet.
The connection state can be one of the following:

- All: Match packets in any state.
- New: Match packets that are not part of an existing connection.
- EstablishedOrRelated: Match packets that are part of an existing connection.

Action (Config Parameter) | Table: NetworkRules

Type	Enum
Range	Accept(100) | Reject(200) | Drop(300) | RateLimitPerSource(400)
Default	Accept
Script/CLI	Nfw.NetworkRules[].Action
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.600.1.800

Action taken when this rule matches a packet.
Action can be one of the following:

- Accept: Let the packet through.
- Reject: Send back an ICMP port unreachable in response to the matched packet, the packet is then dropped.
- Drop: The packet is dropped without any notification.
- RateLimitPerSource: Drop the packets received from a given source IP address when it exceeds a configurable rate. The rate is set using the **RateLimitValue** and **RateLimitTimePeriod** parameters.
  Note: This action is only allowed when the **ConnectionState** parameter is set to 'New'.

Up (Row Command) | Table: NetworkRules

Script/CLI:	Nfw.NetworkRules[].Up
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.600.1.900

Moves the current row upwards.

Down (Row Command) | Table: NetworkRules

Script/CLI:	Nfw.NetworkRules[].Down
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.600.1.1000

Moves the current row downwards.

Insert (Row Command) | Table: NetworkRules

Script/CLI:	Nfw.NetworkRules[].Insert
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.600.1.1100

Inserts a new row before this row.

Delete (Row Command) | Table: NetworkRules

Script/CLI:	Nfw.NetworkRules[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.600.1.1200

Deletes this row.

BlacklistTimeout (Config Parameter)

Type	UInt32
Range	1..86400
Default	60
Script/CLI	Nfw.BlacklistTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.700.100

The time an address stays in the blacklist. If Nfw receives a packet from a blacklisted source, the packet is dropped and the remaining blacklist time is reset to this value.
The time units are seconds.

BlacklistRateLimitTimeout (Config Parameter)

Type	UInt32
Range	1..86400
Default	60
Script/CLI	Nfw.BlacklistRateLimitTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.700.200

The time an address stays in the 'rate limit' blacklist. If Nfw receives a packet from a 'rate limit' blacklisted source, the packet is dropped and the remaining blacklist time stays the same.
The time units are seconds.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Nfw.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Nfw.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2250.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

ApplyConfig (Command)

Applies the configured rules.

InsertRule (Command)

Inserts a new row at the end of the **NetworkRules** table.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

RollbackConfig (Command)

Rolls back the current configuration to the running configuration as showed in the status.
The current configuration is lost.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Nfw service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.2250.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	Blacklisting is ignored in Rule with priority = %1$d.	Warning	Blacklisting is only allowed when the **NetworkRules.Action** parameter is set to 'Drop' or 'RateLimitPerSource'. Otherwise the rule is still active but blacklisting is disabled.
20	Rate limit action is not allowed. Rule with priority = %1$d has no effect.	Error	When the **NetworkRules.Action** parameter is set to 'RateLimitPerSource' the corresponding **NetworkRules.ConnectionState** must be set to 'New'. Otherwise the rule has no effect.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.

NumKey	Message	Severity	Description
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.

NumKey	Message	Severity	Description
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Nfw.

Message	Severity	Description
At least one of the rules applied is ambiguous.	Warning	This message is sent when apply is called and at least one of the rule is ambiguous Ex.: Blacklisting is on and Action is accept.
Blacklist will be ignored because his use with the current action is ambiguous.	Warning	This message is sent when blacklisting puts the rule in an ambiguous state.
Rate limit with this connection state is ambiguous.	Warning	This message is sent when an action puts the rule in an ambiguous state.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.

Message	Severity	Description
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Notifications and Logging Manager (Nlm)

The Notifications and Logging Manager (Nlm) service manages the routing and filtering of the unit's event notification messages.

Parameters

SyslogRemoteHost (Config Parameter)

Type	IpHostNamePort
Range	
Default	
Script/CLI	Nlm.SyslogRemoteHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.100.100

Host name and port number of the device that archives log entries sent by syslog transport. Specifying no port (or port 0) sends notification to port 514.

SyslogMessageTimestamp (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Nlm.SyslogMessageTimestamp
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.100.150

Enable syslog timestamp as per RFC5424.

- Enable: Timestamp is present in syslog.
- Disable: Timestamp is not present in syslog.

SyslogMessageFormat (Config Parameter)

Type	Text
Range	Size(0..1024)
Default	%servicetextkey: %serviceid-%servicename: %msgid-%message
Script/CLI	Nlm.SyslogMessageFormat
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.100.200

Specifies the format of a syslog notification.
Formal Syntax Description:

- Precision = DIGIT
- Width = DIGIT
- MacroId = (ALPHA / "_")
- Macro = %[Width]|[.Precision]|[Width.Precision]MacroId

The Width field is the minimum width of the converted argument. If the converted argument has fewer characters than the specified field width, then it is padded with spaces. If the converted argument has more characters than the specified field width, the field width is extended to whatever is required. The Precision field specifies the maximum number of characters to be printed from a string.

Examples: message = "The button is pressed."

- Syslog : %message --> "The button is pressed."
- Syslog : %25message --> "The button is pressed. "

- Syslog : %10.5message --> "The b "
- Syslog : %5.10message --> "The button"
- Syslog : %.5message --> "The b"

Syslog Notification predefined macros:

Control characters

- %% : %

Syslog notification macros

- %msgid : The notification numkey.
- %mac : Lowercase MAC address of the device.
- %serial : Serial number of the device.
- %serviceid : The numkey of the service that issued the notification.
- %servicetextkey : The textkey of the service that issued the notification.
- %servicename : The display name of the service that issued the notification.
- %message : The message text of the notification.
- %mfpname : The firmware name.
- %version : The firmware version.
- %profile : The firmware profile.

For example, syslog compliant to RFC 5424 may use a format similar to:

- 1 - %mac DGW-2.0 %servicetextkey %msgid %message

Events (Table: user-defined, 100 lines max.)

This table contains the rules that define how events are filtered and routed.

Index (Index) | Table: Events

Type	UInt32
Range	
Script/CLI	Nlm.Events[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.200.1.100

Unique identifier of the row in the table.

Activation (Config Parameter) | Table: Events

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Nlm.Events[].Activation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.200.1.200

Current activation state for the routing rule defined in this table entry.

- Enable: This action is enabled for this table entry.
- Disable: This action is disabled for this table entry.

Type (Config Parameter) | Table: Events

Type	Enum
Range	Notification(100)
Default	Notification
Script/CLI	Nlm.Events[].Type
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.200.1.300

Type of system event for which the routing rule applies.
Currently, the only type of supported event is the system notification.

Criteria (Config Parameter) | Table: Events

Type	Text
Range	Size(0..512)
Default	
Script/CLI	Nlm.Events[].Criteria
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.200.1.400

Expression that an event must match in order to apply the specified action. An expression can contain several 'basic' criteria, separated by commas. The syntax accepts a group of inclusion criteria followed by a group of exclusion criteria. The group of exclusion criteria begins with a hyphen (-).
A basic criteria has the following syntax:

(Service NumKey || All).(Notification Numkey || Severity level || All).

- Keyword All can be used to specify a criteria that applies to all services or all notifications.
- Severity level is specified using a single letter: W for Warnings, I for Information, C for Critical, D for Debug, and E for Error.
- Several basic criteria can be specified on the same line, separated by commas.
- Criteria can specify inclusion or exclusion. A group of exclusion criteria can follow the group of inclusion criteria. The group of exclusion criteria must begin with a hyphen (-).
- Matching an inclusion criteria causes the action to be executed unless an exclusion criteria is also matched.
- Exclusion criteria have precedence over inclusion criteria.

Instead of using an expression such as described above, the single keyword 'All' can be used to accept any notification from any service.

If the whole expression is empty, the criteria never matches any notification and no action is executed.

Spaces can be present before or after a basic criteria. However, spaces are not accepted within a basic criteria, i.e. before or after the dot.

Examples

Basic criteria for the ISDN Service (service number key = 1850), Message 'Physical link state changed to up' (message number key = 5): Basic criteria is 1850.5.

Expression 1850.All,1600.200,1600.W,-1850.500,1600.300.

- 1850.All,1600.200,1600.W are inclusion criteria and -1850.500,1600.300 are exclusion criteria.
- All notifications from service 1850, except notification 500, will match the expression.
- All notifications from service 1600 with Warning level, except notification 300, will match the expression.
- Notification 200 from service 1600 will match the expression, no matter the severity level.

Action (Config Parameter) | Table: Events

Type	Enum
Range	SendViaSyslog(100) | SendViaSip(200) | SendViaSnmp(250) | LogLocally(300) | LogToFile(400)
Default	SendViaSyslog
Script/CLI	Nlm.Events[].Action
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.200.1.500

Action to apply to the system event if the criteria matches.
The possible actions are:

- SendViaSyslog: The event notification is sent using syslog as transport.
- SendViaSip: The event notification is sent using SIP Notify as transport.
- SendViaSnmp: The event notification is sent using SNMP as transport.
- LogLocally: The event notification is logged in LocalLog.
- LogToFile: The event notification is logged into a file.

ConfigStatus (Status Parameter) | Table: Events

Type	Enum
Range	Valid(100) | Invalid(200) | NotSupported(300)
Script/CLI	Nlm.Events[].ConfigStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.200.1.600

Configuration status of the row.
It indicates whether the configuration of the row is valid.

- Valid: The current content of Criteria and Action fields is valid.
- Invalid: The current content of Criteria and Action fields is not valid.
- NotSupported: The current content Criteria and Action fields is valid but not supported. A possible reason could be, for instance, a resource limitation.

Delete (Row Command) | Table: Events

Script/CLI:	Nlm.Events[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.200.1.10000

Delete this row.

LocalLogMaxNbEntries (Status Parameter)

Type	UInt32
Range	
Script/CLI	Nlm.LocalLogMaxNbEntries
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.300.100

Maximum number of entries that the local log can contain. When adding a new entry while the local log is full, the oldest entry is erased to make room for the new one.

LocalLogNbErrorEntries (Status Parameter)

Type	UInt32
Range	
Script/CLI	Nlm.LocalLogNbErrorEntries
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.300.200

Current number of error entries in the local log.

LocalLogNbCriticalEntries (Status Parameter)

Type	UInt32
Range	
Script/CLI	Nlm.LocalLogNbCriticalEntries
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.300.300

Current number of critical entries in the local log.

LocalLogMessages (Table: user-defined, 100 lines max.)

This table contains the entries of the local log.

Index (Index) | Table: LocalLogMessages

Type	UInt32
Range	
Script/CLI	Nlm.LocalLogMessages[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.300.500.1.100

Unique identifier of the row in the table.

LocalTime (Status Parameter) | Table: LocalLogMessages

Type	Text
Range	
Script/CLI	Nlm.LocalLogMessages[].LocalTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.300.500.1.200

Local date and time at which the log entry was inserted. Format is YYYY-MM-DD HH:MM:SS.

ServiceNumkey (Status Parameter) | Table: LocalLogMessages

Type	UInt32
Range	
Script/CLI	Nlm.LocalLogMessages[].ServiceNumkey
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.300.500.1.300

Numerical identifier of the service that issued the log entry.

NotificationId (Status Parameter) | Table: LocalLogMessages

Type	UInt32
Range	
Script/CLI	Nlm.LocalLogMessages[].NotificationId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.300.500.1.400

Numerical identifier of the notification message.

Severity (Status Parameter) | Table: LocalLogMessages

Type	Enum
Range	Critical(500) | Error(400) | Warning(300) | Information(200) | Debug(100)
Script/CLI	Nlm.LocalLogMessages[].Severity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.300.500.1.500

Severity of the log entry.

ServiceTextkey (Status Parameter) | Table: LocalLogMessages

Type	Text
Range	
Script/CLI	Nlm.LocalLogMessages[].ServiceTextkey
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.300.500.1.600

Textual identifier of the service that issued the log entry.

Message (Status Parameter) | Table: LocalLogMessages

Type	Text
Range	
Script/CLI	Nlm.LocalLogMessages[].Message
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.300.500.1.700

The readable content of the log message.

LogFileBaseName (Config Parameter)

Type	Text
Range	Size(0..40)
Default	Notifications
Script/CLI	Nlm.LogFileBaseName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.400.100

Base name of the log file. This base name is postfixed by a time-stamp when a log file is created.

LogFileMaxSize (Config Parameter)

Type	UInt32
Range	1..2048
Default	200
Script/CLI	Nlm.LogFileMaxSize
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.400.200

Maximum size, in KB, that a single log file can have. A new file is created if an entry is added to a full log file. Note that the maximum size can be different depending on the size of user storage, it is limited to 50% of the quota defined in the **FileSystemQuotaSize** parameter.

LogFileMaxNb (Config Parameter)

Type	UInt32
Range	1..10
Default	2
Script/CLI	Nlm.LogFileMaxNb
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.400.300

Maximum number of log files to keep. When the maximum number of files is reached, the oldest file is deleted.

PCaptureState (Status Parameter)

Type	Enum
Range	None(100) | Requested(200) | Completed(300) | UndefinedFailure(400) | UrlFailure(500) | FilterFailure(600) | AuthenticationFailure(700) | HostUnreachableFailure(800) | TlsCertificateFailure(900) | SizeLimitFailure(1000) | LinkFailure(1100)
Script/CLI	Nlm.PCaptureState
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.500.100

State of the packet capture. The state is reset to 'None' when the Nlm service start.

- None: No packet capture was requested since the start of the Nlm service.

- Requested: A packet capture is currently in progress.
- Completed: The last packet capture was completed without failure.
- UndefinedFailure: The last packet capture was terminated by an undefined failure.
- UrlFailure: The last packet capture was terminated because the **PCaptureFileUrl** parameter is empty.
- FilterFailure: The last packet capture was terminated because the value of the **PCaptureFilter** parameter is invalid.
- AuthenticationFailure: The last packet capture was terminated because the username/password of the **PCaptureFileUrl** parameter are rejected by the server.
- HostUnreachableFailure: The last packet capture was terminated because the server is unreachable.
- TlsCertificateFailure: The last packet capture was terminated because the server certificate was not trusted.
- SizeLimitFailure: The last packet capture was terminated because of a size limit failure. Only part of the packet capture file will have been saved on the server or the File service.
- LinkFailure: The last packet capture was stopped because the PCaptureLinkName parameter is empty or the link interface is unavailable.

PCaptureNbFrames (Config Parameter)

Type	UInt32
Range	0..2147483648
Default	0
Script/CLI	Nlm.PCaptureNbFrames
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.500.200

Specifies the maximum number of frames after which the packet capture is automatically stopped. 0 means no limit.

PCaptureNbSecs (Config Parameter)

Type	UInt32
Range	0..2678400
Default	0
Script/CLI	Nlm.PCaptureNbSecs
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.500.300

Specifies the maximum number of seconds after which the packet capture is automatically stopped. 0 means no limit.

PCaptureFilter (Config Parameter)

Type	Text
Range	Size(0..1024)
Default	
Script/CLI	Nlm.PCaptureFilter
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.500.400

Selects which packets will be ignored. If no expression is given, all packets on the net will be captured. Otherwise, only packets for which expression value is 'true' will be captured. For the expression syntax, see pcap-filter(7) (http://www.tcpdump.org/manpages/pcap-filter.7.txt).

PCaptureFileUrl (Config Parameter)

Type	Text
Range	Size(0..512)
Default	
Script/CLI	Nlm.PCaptureFileUrl
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.500.500

URL where to send the packet capture. The URL should follow this format: protocol://[user[:password]@]hostname[:port]/[path/]filename

The brackets [] indicate an optional parameter.

The filename may only be composed of alphanumerical and '-._%$' characters as well as macros. The macros used in this field are replaced by the unit's MAC address or date/time of when the capture was started.

The supported macros are:

- %mac% - the MAC address of the unit.
- %date% - the date if the capture start in format YYYYMMDD.
- %time% - the time if the capture start in format hhmmss.

The supported transfer protocols are:

- HTTP
- HTTPS

- FILE

Examples of valid URLs:

- http://httpserver.com:69/folder/capture.pcap
- http://guest@httpserver.com/capture_%mac%_%date%_%time%.pcap
- https://username:password@httpserver.com/capture.pcap
- file://capture.pcap

The protocol default port is used if none is specified.

PCaptureLinkName (Config Parameter)

Type	Text
Range	Size(0..50)
Default	
Script/CLI	Nlm.PCaptureLinkName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.500.550

Name of the link interface to capture.
Select "any" to capture on all interfaces simultaneously.

PCaptureTransferCertificateValidation (Config Parameter)

Type	Enum
Range	NoValidation(100) | HostName(200)
Default	HostName
Script/CLI	Nlm.PCaptureTransferCertificateValidation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.500.800.100

When saving a packet capture to a HTTPS server, this parameter defines the level of security to use when validating the server's certificate.

- NoValidation: Allow a connection to the server without validating its certificate. The only condition is to receive a certificate from the server. This option provides partial security and should be selected with care.
- HostName: Allow a connection to the server by validating if its certificate is trusted and valid. The validations performed on the certificate include the expiration date and indicates if the Subject Alternate Name (SAN) or Common Name (CN) matches the FQDN or IP address of the server.

PCaptureTransferCertificateTrustLevel (Config Parameter)

Type	Enum
Range	LocallyTrusted(100) | OcspOptional(200) | OcspMandatory(300)
Default	LocallyTrusted
Script/CLI	Nlm.PCaptureTransferCertificateTrustLevel
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.500.800.200

Define how a peer certificate is considered trusted for a HTTPS connection.

- LocallyTrusted: A certificate is considered trusted when the certificate authority (CA) that signed the peer certificate is present in the **Cert.OthersCertificatesInfo** table. The certificate revocation status is not verified.
- OcspOptional: A certificate is considered trusted when it is locally trusted and is not revoked by its certificate authority (CA). The certificate revocation status is queried using the Online Certificate Status Protocol (OCSP). If the OCSP server is not available or the verification status is unknown, the certificate is considered trusted.
- OcspMandatory: A certificate is considered trusted when it is locally trusted and is not revoked by its certificate authority (CA). The certificate revocation status is queried using the Online Certificate Status Protocol (OCSP). If the OCSP server is not available or the verification status is unknown, the certificate is considered not trusted.

PCaptureTransferCipherSuite (Config Parameter)

Type	Enum
Range	CS1(100) | CS2(200) | CS3(300)
Default	CS1
Script/CLI	Nlm.PCaptureTransferCipherSuite
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.500.800.300

Defines the allowed cipher suites for the network security settings when using the HTTPS transfer protocol. When the device initiates an HTTPS connection to a server, it will negotiate the cipher suite according to its configuration.

- CS1:
  - TLS_DHE_DSS_WITH_AES_128_CBC_SHA
  - TLS_DHE_DSS_WITH_AES_256_CBC_SHA
  - Also includes ciphers from CS2 and CS3 below

- CS2:
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - Also includes ciphers from CS3 below
- CS3:
  - The following are TLS 1.2 ciphers:
  - TLS_RSA_WITH_AES_128_CBC_SHA256
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_CBC_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
  - The following are TLS 1.3 ciphers:
  - TLS_AES_256_GCM_SHA384
  - TLS_AES_128_GCM_SHA256
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_CCM_8_SHA256
  - TLS_AES_128_CCM_SHA256

PCaptureTransferTlsVersion (Config Parameter)

Type	Enum
Range	TLSv1(200) | TLSv1_1(300) | TLSv1_2(400) | TLSv1_3(500)
Default	TLSv1
Script/CLI	Nlm.PCaptureTransferTlsVersion
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.500.800.400

Defines the allowed TLS version for the network security settings when using the HTTPS transfer protocol. When the device initiates an HTTPS connection to a server, it will negotiate the TLS version according to its configuration.

- TLSv1: Allow TLS versions 1 and up.
- TLSv1_1: Allow TLS versions 1.1 and up.
- TLSv1_2: Allow TLS versions 1.2 and up.
- TLSv1_3: Allow TLS version 1.3 only.

The device will always send its highest supported TLS version in the ClientHello message. The server will select the highest supported TLS version it supports from the ClientHello message. The device will then validate that the selected version is allowed. If the version is not allowed the device will close the connection.

DiagLogAutomaticDump (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Nlm.DiagLogAutomaticDump
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.600.100

Enables or disables the automatic dump of diagnostic logs when the system crashes.
The diagnostic log files are located under the **File** service.

Available on all platforms, excluding the Mediatrix 4102S rev1.

DiagnosticTracesEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Nlm.DiagnosticTracesEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.10000.100

Enables the traces used by the Technical Assistance Centre to further assist in resolving some issues. Enabling this feature issues a lot of messages to the syslog host. These messages may be filtered using the **DiagnosticTracesFilter** parameter.

DiagnosticTracesFilter (Config Parameter)

Type	Text
Range	Size(0..512)
Default	
Script/CLI	Nlm.DiagnosticTracesFilter
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.10000.200

Filter applied to diagnostic traces. An empty filter means that all diagnostic traces are enabled.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Nlm.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.

- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Nlm.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1100.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

DumpDiagLog (Command)

Generate a diagnostic log file. The file is written in the persistent memory, using the **File** service under the **nlm/diag** directory.
Oldest diagnostic log files may be removed if space is insufficient.

Available on all platforms, excluding the Mediatrix 4102S rev1.

InsertEvent (Command)

Insert a routing rule in table **Events**.

Type (Argument) | Command: InsertEvent

Type	Enum
Range	Notification(100)
Default	Notification

Type of system event for which the routing rule applies.

Criteria (Argument) | Command: InsertEvent

Type	Text
Range	Size(0..256)
Default	

Expression criteria for the event to match in order to apply the specified action.

Action (Argument) | Command: InsertEvent

Type	Enum
Range	SendViaSyslog(100) | SendViaSip(200) | SendViaSnmp(250) | LogLocally(300) | LogToFile(400)
Default	SendViaSyslog

Action to apply if the criteria matches.

Activation (Argument) | Command: InsertEvent

Type	EnableDisable
Range	
Default	Enable

Activation state for the routing rule.

Index (Argument) | Command: InsertEvent

Type	UInt32
Range	
Default	0

Index in the table. A value of zero (default) causes automatic selection of the largest current index value + 1. If the index value already exists in the table, the insertion is refused.

LocalLogReset (Command)

Removes all the entries in the local log.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

PCaptureStart (Command)

Start the packet capture.
The start packet capture command fails if:

- The **PCaptureFileUrl** or **PCaptureLinkName** parameter is empty.
- The link name in PCaptureLinkName parameter is unavailable.
- A capture is already in progress.

PCaptureStop (Command)

Stop the packet capture.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Nlm service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.1100.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
1000	Packet capture started.	Info	This message is issued when a packet capture is started.
1100	Packet capture stopped. Stop requested by the command PCaptureStop.	Info	This message is issued when a packet capture is stopped by executing the `PCaptureStop` command.
1200	Packet capture stopped. Maximum number of frames reached.	Info	This message is issued when a packet capture is stopped because the maximum number of frames was reached.
1300	Packet capture stopped. Maximum delay reached.	Info	This message is issued when a packet capture is stopped because the maximum delay was reached.
1400	Packet capture stopped. The Nlm service is stopped.	Error	This message is issued when a packet capture is stopped because the Nlm service was stopped.
1500	Packet capture stopped. An undefined failure occur.	Error	This message is issued when a packet capture is stopped because an undefined failure occurred.
1600	Packet capture stopped. URL defined in the PCaptureFileUrl parameter is empty.	Error	This message is issued when a packet capture is stopped because the URL is empty.
1700	Packet capture stopped. Filter defined in the PCaptureFilter parameter is invalid.	Error	This message is issued when a packet capture is stopped because the filter is invalid.
1800	Packet capture stopped. Fail to authentication to the server.	Error	This message is issued when a packet capture is stopped because of an authentication failure.
1900	Packet capture stopped. The server is unreachable.	Error	This message is issued when a packet capture is stopped because the server is unreachable.
2000	Packet capture stopped. The server certificate is not trusted.	Error	This message is issued when a packet capture is stopped because the server certificate is not trusted.
2100	Packet capture stopped. The captured file is too large for the File service.	Error	This message is issued when a packet capture is stopped because the captured file reached the size limit in the File service.

NumKey	Message	Severity	Description
2200	Packet capture stopped. The link interface name defined in the PCaptureLinkName parameter is empty.	Error	This message is issued when a packet capture is stopped because the link interface name is empty.
2300	Packet capture stopped. The link interface defined in the PCaptureLinkName parameter is unavailable.	Error	This message is issued when a packet capture is stopped because the link interface is unavailable.
2400	Diagnostic logs are successfully transfered to persistent storage.	Info	This message is issued when the **DumpDiagLog** command successfully transferred the logs files to persistent storage.
2500	Diagnostic logs transfer failed due to insufficient storage space.	Error	This message is issued when the **DumpLogs** command transfer fails due to insufficient storage space.
2600	Diagnostic logs transfer failed due to an error reading the configuration file.	Error	This message is issued when the **DumpLogs** command transfer fails due to an error reading the configuration file.
2700	Diagnostic logs transfer failed due to an undefine failure.	Error	This message is issued when the **DumpLogs** command transfer fails due to an undefined failure.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.

NumKey	Message	Severity	Description
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.

NumKey	Message	Severity	Description
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Nlm.

Message	Severity	Description
The Nlm event table exceeds the maximum size allowed.	Error	This message is issued when the Nlm event table has reached the maximum size allowed. Subsequent events are not added to the table.
The Nlm event router failed to remove rule.	Error	This message is issued when the Nlm event router is unable to remove a rule in the table.
The Nlm event router failed to insert new rule.	Error	This message is issued when the Nlm event router is unable to insert a new rule in the table.
The Nlm event expression criteria is invalid.	Error	This message is issued when the Nlm event expression criteria is invalid.
The Log To File action is not supported.	Error	This message is issued when the Log To File action is selected and the user storage is less than 1 MB.
Cannot start packet capture because the destination URL is not defined in PCaptureFileUrl parameter.	Error	This message is issued when the **PCaptureStart** command is executed and **PCaptureFileUrl** parameter is empty.
A packet capture is already in progress.	Error	This message is issued when the **PCaptureStart** command is executed and a packet capture is already in progress.
Cannot start the packet capture because the link interface name is not defined in the PCaptureLinkName parameter.	Error	This message is issued when the PCaptureStart command is executed and PCaptureLinkName parameter is empty.
Cannot start the packet capture because the link interface defined in the PCaptureLinkName parameter is unavailable.	Error	This message is issued when the PCaptureStart command is executed and the link interface defined in PCaptureLinkName parameter is unavailable.
There is no packet capture in progress.	Warning	This message is issued when the **PCaptureStop** command is executed and there is no packet capture in progress.
A dump of the diagnostic logs is already in progress.	Error	This message is issued when the **DumpLogs** command is executed and a dump is already in progress.
The dump diagnostic logs fails because of an undefined failure.	Error	This message is issued when a dump diagnostic logs failed because of an undefined failure.

Message	Severity	Description
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.

Message	Severity	Description
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Network Traffic Control (Ntc)

The Network Traffic Control (NTC) service allows the administrator to perform traffic shaping on the network interfaces.

Parameters

LinkBandwidthControl (Table)

This table shows the bandwidth limitation applied on the network interfaces.

LinkName (Index) | Table: LinkBandwidthControl

Type	Text
Range	
Script/CLI	Ntc.LinkBandwidthControl[].LinkName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3700.1.100.1.100

Name of the Ethernet link over which the bandwidth limitation is applied.

EgressLimit (Config Parameter) | Table: LinkBandwidthControl

Type	Int32
Range	0..0 | 64..1000000
Default	0
Script/CLI	Ntc.LinkBandwidthControl[].EgressLimit
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3700.1.100.1.200

Indicates the egress bandwidth limitation for the selected link interface. The range is from 64 to 1000000 kilobits per second (kbps).
The value 0 means no bandwidth limitation and no prioritization.

This value must be set according to the upstream bandwidth limit of the network on this link. Set to 0 (disable) if the network bandwidth exceeds 1000000 kbps or if it exceeds the effective limit of this device.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Ntc.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3700.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Ntc.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.3700.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Ntc service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.3700.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	Applied %1$d kbps bandwidth limit on interface %2$s.	Info	This message is issued when NTC applied a bandwidth limit to an interface.
20	Bandwidth limit disabled on interface %1$s.	Info	This message is issued when the NTC service removes the bandwidth limit of an interface.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.

NumKey	Message	Severity	Description
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.

NumKey	Message	Severity	Description
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Ntc.

Message	Severity	Description
Configured Bandwidth limit exceeded the hardware maximum value of '%1$d' kbps on '%2$s' interface. The maximum value is applied.	Warning	This message is issued when the NTC service exceeded the hardware bandwidth limit of an interface.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.

Message	Severity	Description
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Process Control Manager (Pcm)

The Process Control Manager (PCM) service manages the startup and shutdown sequence of the system.

Parameters

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Pcm.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.300.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.

- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Pcm.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.300.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

Restart (Command)

Stops and restarts the unit.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Pcm service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.300.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	Restarting the unit.	Info	This message is issued when the PCM receives a request to restart the unit.
20	Restarting of the unit initiated via button.	Info	This message is issued when the PCM receives a request to restart the unit because the user pressed the button.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.

NumKey	Message	Severity	Description
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.

NumKey	Message	Severity	Description
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Pcm.

Message	Severity	Description
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.

Message	Severity	Description
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Plain Old Telephony System Line (Pots)

The Plain Old Telephony System (POTS) service manages the FXS and FXO analog telephony interfaces.

Parameters

Line (Table)

This table shows the current available lines and allows their basic configuration.

Id (Index) | Table: Line

Type	Text
Range	
Script/CLI	Pots.Line[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.100.1.100

String that identifies a line in other tables.

TypeStatus (Status Parameter) | Table: Line

Type	Enum
Range	Fxs(100) | Fxo(200)
Script/CLI	Pots.Line[].TypeStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.100.1.200

The status POTS type of the line.

State (Status Parameter) | Table: Line

Type	Enum
Range	Idle(100) | InUse(200) | Disabled(300) | Bypass(400) | Down(500)
Script/CLI	Pots.Line[].State
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.100.1.300

The current call control state for this channel:

- Idle: The line is available
- InUse: The line is currently used
- Disabled: The line is disabled
- Bypass: The line is on bypass
- Down: The power of the line is down

CallerIdCustomization (Config Parameter)

Type	Enum
Range	Country(100) | EtsiDtmf(200) | TelebrasDtmf(210) | TdkDtmf(220) | EtsiFsk(300) | Bell202Fsk(310)
Default	Country
Script/CLI	Pots.CallerIdCustomization
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.200

Overrides the modulation of the Caller ID.

When using this parameter, both the reception and transmission are affected. If an FSK modulation is selected, the received DTMF-based Caller ID will not be recognised. If a DTMF modulation is selected, the received FSK-based Caller ID will not be recognised.

- Country: Use the Caller ID modulation of the country selected by the **TelIf.CountrySelection** parameter.
- EtsiDtmf: ETSI 300 659-1 (DTMF string)
- TelebrasDtmf: Telebras 220-250-713 (DTMF string)
- TdkDtmf: TS 900 301-1 (DTMF string)
- EtsiFsk: ETSI 300 659-1 (FSK V.23)
- Bell202Fsk: Bellcore (FSK Bell 202)

DtmfMapDigitDetection (Config Parameter)

Type	Enum
Range	WhenPressed(100) | WhenReleased(200)
Default	WhenPressed
Script/CLI	Pots.DtmfMapDigitDetection
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.300

Determines when a digit is processed through the DTMF maps.

- WhenPressed : Digits are processed as soon as they are pressed. This can lead to a digit leak in the RTP at the beginning of a call if the voice stream is established before the last digit is released.
- WhenReleased : Digits are processed only when released. This option increases the delay needed to match a dialed string to a DTMF map. There is also an impact on **EpServ.DtmfMapTimeoutInterDtmf**, **EpServ.DtmfMapTimeoutFirstDtmf** and **EpServ.DtmfMapTimeoutCompletion** since the timers are stopped at the end of a digit instead of the beginning.

VocalUnitInformation (Config Parameter)

Type	Enum
Range	None(100) | All(200)
Default	All
Script/CLI	Pots.VocalUnitInformation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.400

Determines the type of vocal information that can be obtained by dialing a pre-defined digit map.

- None: The vocal information feature is disabled.
- All: Enable all vocal information digit maps.

The supported vocal information digit maps are:

- '*#*0': The list of IP addresses of the device.
- '*#*1': The MAC address of the device.
- '*#*8': The firmware version number of the device.

CallerIdTransmission (Config Parameter)

Type	Enum
Range	Country(100) | FirstRing(200) | RingPulse(300) | LineReversalRingPulse(400) | DtAs(500) | LineReversalDtAs(600) | NoRingPulse(700)
Default	Country
Script/CLI	Pots.CallerIdTransmission
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.500

Overrides the transmission method of the generated Caller ID.

- Country : Use the Caller ID transmission of the country selected by the **TelIf.CountrySelection** parameter.
- FirstRing : Caller ID is sent after the first ring.
- RingPulse : Caller ID is sent between a brief ring pulse and the first ring.
- LineReversalRingPulse : Caller ID is sent between a brief ring pulse and the first ring on an inverted polarity line.
- DtAs : Caller ID is sent after the dual tone alerting state tone.
- LineReversalDtAs : Caller ID is sent after the dual tone alerting state tone on an inverted polarity line.
- NoRingPulse : Caller ID is sent before the first ring.

FxsLineSupervisionMode (Config Parameter)

Type	Enum
Range	None(100) | DropOnDisconnect(200) | ReversalOnIdle(300) | ReversalOnEstablished(400)
Default	DropOnDisconnect
Script/CLI	Pots.FxsLineSupervisionMode
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.100

Determines how the power drop and line polarity are used to signal the state of a line.

- None: Don't use power drop or polarity reversal to signal the state of the line.
- DropOnDisconnect: Activates the Power Drop on Disconnect feature. A short power drop is made at the end of a call when the call is disconnected by the remote party. The drop duration can be configured in the **FxsPowerDropOnDisconnectDuration** parameter.
- ReversalOnIdle: Activates the Polarity Reversal on Idle feature. The polarity of the line is initially in reversed state. The polarity of the line returns to the normal state when the user seizes the line or when the line rings for an incoming call. The polarity of the line is reversed again when the call is disconnected.
- ReversalOnEstablished: Activates the Polarity Reversal on Established option. The polarity of the line is initially in the normal state. The polarity of the line is reversed when the call is established and returns to the normal state when the call is disconnected.

Note: Power drop and polarity reversal are also called battery drop and battery reversal.

FxsDisconnectDelay (Config Parameter)

Type	UInt32
Range	0..300
Default	0
Script/CLI	Pots.FxsDisconnectDelay
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.200

Determines whether or not call clearing occurs as soon as the called user is the first to hang up a received call. This parameter has no effect when the user acts as the calling party.
If the value is set to 0, the call is disconnected as soon as the called user hangs up the call.

If the value is greater than 0, that value is the amount of time, in seconds, the unit waits after the called user hangs up before signalling the end of the call.

FxsInbandRingback (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Pots.FxsInbandRingback
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.300

Determines whether or not the FXS endpoint needs to generate a ringback for incoming ringing call.

- Disable: The FXS endpoint does not play local ringback to the remote party.
- Enable: The FXS endpoint plays local ringback to the remote party via the negotiated media stream.

FxsShutdownBehavior (Config Parameter)

Type	Enum
Range	DisabledTone(100) | PowerDrop(200)
Default	DisabledTone
Script/CLI	Pots.FxsShutdownBehavior
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.400

Determines the FXS endpoint behavior when it becomes shut down.

- DisabledTone: A disabled tone is played when the user picks up the telephone and the FXS endpoint is shut down.
- PowerDrop: The loop current is interrupted when the FXS endpoint is shut down and no tone is played when the user picks up the telephone.

A FXS endpoint becomes shut down when the operational state of the endpoint becomes 'Disabled' (see the **EpAdm.OperationalState** parameter) and the **EpAdm.EndpointAutomaticShutdownEnable** parameter is set to 'Enable'.

This parameter is not used by FXS endpoints related to bypass when the **FxsBypass.Activation** parameter is set to 'EndpointDisabled'.

FxsPowerDropOnDisconnectDuration (Config Parameter)

Type	UInt32
Range	100..5000
Default	1000
Script/CLI	Pots.FxsPowerDropOnDisconnectDuration
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.500

Determines the power drop duration that is made at the end of a call when the call is disconnected by the remote party.
This value is expressed in milliseconds (ms).

This parameter only has an effect when the **FxsLineSupervisionMode** parameter is set to 'DropOnDisconnect'.

FxsServiceActivation (Config Parameter)

Type	Enum
Range	FlashHook(100) | FlashHookAndDigit(200)
Default	FlashHook
Script/CLI	Pots.FxsServiceActivation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.600

Selects the method used by the user to activate supplementary services like call hold, second call, call waiting, call transfer and conference call.

- FlashHook: Service activation is performed by flash hook or hanging up.
- FlashHookAndDigit: Service activation is performed by flash hook, flash hook followed by a digit or hanging up.

Flash hook and digits commands when a call is waiting or a call is on hold:

- [Flash+1] or [hang-up] : End active call and switch to call on hold/waiting.
- [Flash+2] : Hold the active call and switch to call on hold/waiting.
- [Flash+3] : Enter in 3-party conference mode.
- [Flash+4] : Transfer call on hold to the active call (not available on call waiting).

Flash hook and digits commands when in 3-party conference:

- [hang-up] : End all calls.
- [Flash+1] : Exit from 3-party conference mode. 3rd party is active, 2nd party call is ended.

- [Flash+2] : Exit from 3-party conference mode. 2nd party is active, 3rd party is on hold.

FxsCallerIdPrivateCallingPartyName (Config Parameter)

Type	Text
Range	Size(0..50)
Default	Anonymous
Script/CLI	Pots.FxsCallerIdPrivateCallingPartyName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.700

Sets the Calling Party Name of the caller ID (CLIP) when the calling party is tagged as private.

- When empty, no Calling Party Name parameter is sent.
- When set to 'P', no Calling Party Name parameter is sent but a Reason for Absence of Caller Party Name parameter is sent with the value 0x50 (Private).

FxsSipMessageAlertingEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Pots.FxsSipMessageAlertingEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.800

Determines whether or not the FXS endpoints should handle a SIP MESSAGE notification.

- Disable: The FXS endpoints will ignore all SIP MESSAGE notifications.
- Enable: A SIP message notification will trigger an alert on the FXS endpoint by generating a short ring and sending the message content through the Caller ID.

The FXS ports needs to be on-hook for the alert to be generated, otherwise the notification is ignored.

The SIP message notifications are received only if the **SipEp.SipMessageSupport** parameter is set to "AcceptPlainText".

FxsCountryCustomizationOverride (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Pots.FxsCountryCustomizationOverride
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.10000.100

Allows to override FXS-related default country settings.

- Disable: The line uses the default country FXS settings.
- Enable: The line uses the FXS country configuration set in the **FxsCountryCustomizationLoopCurrent** parameter and the **FxsCountryCustomizationFlashHookDetectionRange** parameter.

FxsCountryCustomizationLoopCurrent (Config Parameter)

Type	UInt32
Range	20..32
Default	30
Script/CLI	Pots.FxsCountryCustomizationLoopCurrent
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.10000.200

Loop current generated by the FXS port in milliamperes(mA).
This configuration is used only if the **FxsCountryCustomizationOverride** parameter is set to 'Enable'.

FxsCountryCustomizationFlashHookDetectionRange (Config Parameter)

Type	Text
Range	Size(5..9)
Default	100-1200
Script/CLI	Pots.FxsCountryCustomizationFlashHookDetectionRange
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.10000.300

The range in which the hook switch must remain pressed to perform a flash hook.

The range consists of the minimal delay and maximal delay expressed in ms separated by a '-'. The minimal value allowed is 10 ms and the maximum value allowed is 1200 ms. The space character is not allowed.

This configuration is used only if the **FxsCountryCustomizationOverride** parameter is set to 'Enable'.

FxsBypass (Table)

This table shows the current available FXS bypass and allows their basic configuration.

Id (Index) | Table: FxsBypass

Type	Text
Range	
Script/CLI	Pots.FxsBypass[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.10100.1000.1.100

String that identifies a line in other tables.

Activation (Config Parameter) | Table: FxsBypass

Type	Enum
Range	PowerOff(100) | EndpointDisabled(200) | OnDemand(300)
Default	EndpointDisabled
Script/CLI	Pots.FxsBypass[].Activation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.10100.1000.1.200

Specifies when the bypass needs to be activated.

- PowerOff: The bypass is activated only when the unit power is off or the POTS service is not started.
- EndpointDisabled: The bypass is activated when the operational state of the endpoint is 'Disable' and the **EpAdm.EndpointAutomaticShutdownEnable** parameter is set to 'Enable'. The bypass is also activated for the same conditions as the ones defined in 'PowerOff'.
- OnDemand: The bypass is activated when the user enters the DTMF map configured in the **FxsBypass.ActivationDtmfMap** parameter. The bypass is deactivated when the user on hooks the phone for at least the number of time configured in the **FxsBypass.DeactivationTimeout** parameter. The bypass is also activated for the same conditions as the ones defined in 'PowerOff'.

ActivationDtmfMap (Config Parameter) | Table: FxsBypass

Type	DigitMap
Range	
Default	
Script/CLI	Pots.FxsBypass[].ActivationDtmfMap
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.10100.1000.1.300

Specifies the DTMF to signal to enable the bypass.
This parameter is only used when the **FxsBypass.Activation** parameter is set to 'OnDemand'.

DeactivationTimeout (Config Parameter) | Table: FxsBypass

Type	UInt32
Range	0..3600
Default	32
Script/CLI	Pots.FxsBypass[].DeactivationTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.10100.1000.1.400

Specifies the delay to wait before deactivating the bypass after an on hook if the bypass is activated on demand. The delay is restarted after each on hook. The bypass is not deactivated if the delay expires while the FXS endpoint is off hook.
This parameter is only used when the **FxsBypass.Activation** parameter is set to 'OnDemand' and the bypass is activated using the DTMFs configured in the **FxsBypass.ActivationDtmfMap** parameter.

This value is expressed in seconds (s).

FxsDefaultMessageWaitingIndicatorActivation (Config Parameter)

Type	Enum
Range	Disabled(100) | Tone(200) | Visual(300) | ToneAndVisual(400)
Default	ToneAndVisual
Script/CLI	Pots.FxsDefaultMessageWaitingIndicatorActivation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.10200.100

Configure the Message Waiting Indicator service available on FXS lines.
When used in conjunction with a voice-messaging system, the Message Waiting Indicator allows the user to be notified when new messages are awaiting attention on the messaging server.

- Disabled: The user is not alerted of messages awaiting attention.
- Tone: When messages are awaiting attention, the user is alerted by a message waiting tone when picking up the handset.
- Visual: When messages are awaiting attention, the user is alerted by a Visual Message Waiting Indicator such as a blinking LED on the phone.
- ToneAndVisual: When messages are awaiting attention, the user is alerted by a Visual Message Waiting Indicator such as a blinking LED on the phone, and a message waiting tone when picking up the handset.

If a specific configuration is set in the **FxsSpecificMessageWaitingIndicator.Activation** parameter and the **FxsSpecificMessageWaitingIndicator.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

FxsDefaultVisualMessageWaitingIndicatorType (Config Parameter)

Type	Enum
Range	Fsk(100) | FskAndVoltage(200)
Default	Fsk
Script/CLI	Pots.FxsDefaultVisualMessageWaitingIndicatorType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.10200.150

Configures how the Visual Message Waiting Indicator is sent on FXS lines.

- Fsk: A FSK signal is sent to activate the VMWI on the phone.
- FskAndVoltage: Both FSK signal and high voltage signal are used to activate the VMWI on the phone.

Note: FskAndVoltage is not supported on all devices.

FxsSpecificMessageWaitingIndicator (Table)

This table allows to configure the message waiting indicator feature for a specific FXS line.

Id (Index) | Table: FxsSpecificMessageWaitingIndicator

Type	Text
Range	
Script/CLI	Pots.FxsSpecificMessageWaitingIndicator[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.10200.200.1.100

String that identifies a line in other tables.

EnableConfig (Config Parameter) | Table: FxsSpecificMessageWaitingIndicator

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Pots.FxsSpecificMessageWaitingIndicator[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.10200.200.1.200

Defines the configuration to use for a specific line.

- Disable: The line uses the default configuration as defined in the **FxsDefaultMessageWaitingIndicatorActivation** parameter.
- Enable: The line uses the specific configuration as defined in the **FxsSpecificMessageWaitingIndicator.Activation** parameter.

Activation (Config Parameter) | Table: FxsSpecificMessageWaitingIndicator

Type	Enum
Range	Disabled(100) | Tone(200) | Visual(300) | ToneAndVisual(400)
Default	ToneAndVisual
Script/CLI	Pots.FxsSpecificMessageWaitingIndicator[].Activation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.10200.200.1.300

Configure the Message Waiting Indicator for a specific FXS line.
When used in conjunction with a voice-messaging system, the Message Waiting Indicator allows the user to be notified when new messages are awaiting attention on the messaging server.

- Disabled: The user is not alerted of messages awaiting attention.

- Tone: When messages are awaiting attention, the user is alerted by a message waiting tone when picking up the handset.
- Visual: When messages are awaiting attention, the user is alerted by a Visual Message Waiting Indicator such as a blinking LED on the phone.
- ToneAndVisual: When messages are awaiting attention, the user is alerted by a Visual Message Waiting Indicator such as a blinking LED on the phone, and a message waiting tone when picking up the handset.

This configuration overrides the default configuration set in the **FxsDefaultMessageWaitingIndicatorActivation** parameter if the **FxsSpecificMessageWaitingIndicator.EnableConfig** parameter is set to 'Enable'.

FxsDefaultAutoCancelTimeout (Config Parameter)

Type	UInt32
Range	0..600
Default	0
Script/CLI	Pots.FxsDefaultAutoCancelTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.10300.100

Time, in seconds, the endpoint rings before the call is automatically cancelled.
Setting this parameter to 0 disables the timeout. Calls will not be automatically cancelled.

FxsEmergencyCallOverride (Config Parameter)

Type	Enum
Range	NoOverride(100) | NoServices(200) | NoDisconnect(300)
Default	NoOverride
Script/CLI	Pots.FxsEmergencyCallOverride
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.10400.100

Overrides the set of services that are activated during an emergency call.

- NoOverride: The set of services for emergency calls remains the same as configured.
- NoServices: Ignores any service requiring a flash-hook. Call waiting and all other related services are deactivated.
- NoDisconnect: Same as 'NoServices' and, in addition, automatically re-establish a call that was disconnected by the originator.

Refer to the service 'EpServ' for telephony services configuration.

FxsEmergencyRingTimeout (Config Parameter)

Type	UInt32
Range	0..180000
Default	2000
Script/CLI	Pots.FxsEmergencyRingTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.10400.200

When the **FxsEmergencyCallOverride** parameter is set to 'NoDisconnect', this parameter sets the grace period before ringing the phone in the event where the originator of an emergency call hangs-up before the emergency call center disconnects the call.

This value is expressed in milliseconds (ms).

FxsDistinctiveRing (Table)

This table allows to override the default country ring configuration. The configuration applies to all interfaces.

Index (Index) | Table: FxsDistinctiveRing

Type	UInt32
Range	1..4
Script/CLI	Pots.FxsDistinctiveRing[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.10500.100.1.100

Unique identifier of the row in the table.

RingId (Config Parameter) | Table: FxsDistinctiveRing

Type	Text
Range	Size(0..512)
Default	
Script/CLI	Pots.FxsDistinctiveRing[].RingId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.10500.100.1.200

Identification of the distinctive ring. When the **RingId** parameter is defined and the incoming call property 'distinctive-ring' matches with it, the corresponding ring pattern is used. Otherwise, the country ring pattern is used.

Example:

- An "Alert-Info: <http://127.0.0.1/Bellcore-dr2>" matches with a "//127.0.0.1/Bellcore-dr2" RingId

Pattern (Config Parameter) | Table: FxsDistinctiveRing

Type	Text
Range	Size(0..512)
Default	
Script/CLI	Pots.FxsDistinctiveRing[].Pattern
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.10500.100.1.300

Pattern description of the distinctive ring. Used only if the **RingId** parameter is not empty.

The format for a cadence is 'on, off, on, off, ...' where 'on' and 'off', respectively are numerical values representing the time in milliseconds. Up to three 'on, off' pairs can be specified. Allowed range for the 'on' and 'off' values are 0 to 32767. A cadence starting with a value of zero (0) is invalid.

Examples:

- Bellcore-dr2: "800,400,800,4000"
- Bellcore-dr4: "300,200,1000,200,300,4000"

FxsCallerId (Table)

This table activates the Caller ID generation. The Caller ID activation is endpoint specific.

Id (Index) | Table: FxsCallerId

Type	Text
Range	
Script/CLI	Pots.FxsCallerId[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.10600.100.1.150

String that identifies a line in other tables.

Activation (Config Parameter) | Table: FxsCallerId

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Pots.FxsCallerId[].Activation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.10600.100.1.300

Enables or disables the Caller ID generation on the FXS endpoint.

FxsInteropPlayLocalRingbackWhenNoMediaStream (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Pots.FxsInteropPlayLocalRingbackWhenNoMediaStream
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.10000.50000.100

Forces local ringback generation when early-media is enabled but no media stream has been received yet.

- Enable: Upon reception of an early-media provisional response (i.e. SIP 18x with SDP), play a local ringback tone if no RTP packet is received after 1 second. At any moment, if an RTP packet is received, the early-media stream is played right away, thus aborting definitely the local ringback.
- Disable: Never play local ringback in early-media use-cases.

Applies to outgoing calls only.

FxoPreDialDelay (Config Parameter)

Type	UInt32
Range	0..10000
Default	0
Script/CLI	Pots.FxoPreDialDelay
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.100

The delay between the time the line is successfully seized, or dial tone detected, and the moment the destination phone number is dialed.
A value of '0' indicates to use a value that is specific to the country specification as set in the **TelIf.CountrySelection** parameter.

This value is expressed in milliseconds (ms).

Note: Some country specifications require a mandatory pre-dial delay. In that case, the highest value between the mandatory pre-dial delay and the value set in this parameter is used.

FxoDialToneDetectionMode (Config Parameter)

Type	Enum
Range	Disable(100) | CountryTone(200)
Default	CountryTone
Script/CLI	Pots.FxoDialToneDetectionMode
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.200

When dial tone detection is enabled, the unit waits for a dial tone on the FXO line before initiating the dialling sequence. If no dial tone is detected, the line is considered as busy with an incoming call. This mechanism helps avoid collisions between incoming and outgoing calls.

- Disable: Dial tone detection is disabled.
- CountryTone: The unit tries to detect the tone specified for this purpose in the current country's tone specification. Some country specifications omit this information. In that case, the unit behaves as if the **FxoDialToneDetectionMode** parameter is 'disable'.

See the **TelIf.CountrySelection** parameter.

FxoDialToneDetectionTimeout (Config Parameter)

Type	UInt32
Range	1300..10000
Default	3000
Script/CLI	Pots.FxoDialToneDetectionTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.300

Indicates how long the unit waits for a dial tone before considering the line is busy with an incoming FXO call.
This value is expressed in milliseconds (ms).

FxoAnsweringDelay (Table)

This table holds the answering delay configuration. Each row in this table configures the answering delay of a line.

Id (Index) | Table: FxoAnsweringDelay

Type	Text
Range	
Script/CLI	Pots.FxoAnsweringDelay[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.5000.1.100

String that identifies a FXO line.

WaitBeforeAnsweringDelay (Config Parameter) | Table: FxoAnsweringDelay

Type	UInt32
Range	0..30000
Default	8000
Script/CLI	Pots.FxoAnsweringDelay[].WaitBeforeAnsweringDelay
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.5000.1.200

The waiting period before answering an incoming FXO call.
If this delay expires before the caller ID signal is decoded, the call proceeds without caller ID information.

If a minimal waiting period is required for the selected country, the highest of both values is used. See the **TelIf.CountrySelection** parameter.

This value is expressed in milliseconds (ms).

AnsweringOnCallerIdDetection (Config Parameter) | Table: FxoAnsweringDelay

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Pots.FxoAnsweringDelay[].AnsweringOnCallerIdDetection
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.5000.1.300

Enables answering upon caller ID detection instead of the waiting delay configured by **WaitBeforeAnsweringDelay**.

When enabled, an incoming FXO call is answered on the first occurrence of either

- The reception of the caller ID signal.
- The expiration of the delay configured by the **WaitBeforeAnsweringDelay** parameter and the country wait before answering delay. See the **TelIf.CountrySelection** parameter.

WaitForCalleeToAnswer (Config Parameter) | Table: FxoAnsweringDelay

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Pots.FxoAnsweringDelay[].WaitForCalleeToAnswer
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.5000.1.400

When the endpoint is set up for automatic call (see the **EpServ.DefaultAutoCallEnable** parameter), enabling this parameter makes the endpoint wait until the called party connection is established before answering the incoming call.

FxoIncomingCallBehavior (Table)

Table that defines how each line behaves when there is an incoming call.

Id (Index) | Table: FxoIncomingCallBehavior

Type	Text
Range	
Script/CLI	Pots.FxoIncomingCallBehavior[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.5100.1.100

String that identifies a FXO line.

NotAllowedBehavior (Config Parameter) | Table: FxoIncomingCallBehavior

Type	Enum
Range	DoNotAnswer(100) | PlayCongestionTone(200)
Default	PlayCongestionTone
Script/CLI	Pots.FxoIncomingCallBehavior[].NotAllowedBehavior
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.5100.1.200

Under certain circumstances (locked port, configuration, etc...), incoming FXO calls are not allowed. When that is the case, the FXO endpoint behaves in one of the manners below.

- DoNotAnswer: The incoming call is left unanswered.
- PlayCongestionTone: The incoming call is answered, a congestion tone is played for 10 seconds, and then the call is terminated.

FxoOutgoingCallBehavior (Table)

This table defines each line behavior on outgoing calls.

Id (Index) | Table: FxoOutgoingCallBehavior

Type	Text
Range	
Script/CLI	Pots.FxoOutgoingCallBehavior[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.5150.1.100

String that identifies a FXO line.

AnswerSupervisionMode (Config Parameter) | Table: FxoOutgoingCallBehavior

Type	Enum
Range	None(100) | Reversal(200)
Default	None
Script/CLI	Pots.FxoOutgoingCallBehavior[].AnswerSupervisionMode
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.5150.1.200

Sets the answer supervision mode to use on outgoing FXO calls.

- None: No answer supervision, the IP call is established immediately after signalling the digits on the PSTN.
- Reversal: The IP call is established after receiving a polarity reversal from the PSTN.

Note: Polarity reversal is also called battery reversal.

FxoCustomBasicParameters (Table)

This table allows to override the default country basic parameters for the FXO lines. This table is effective only if the **OverrideDefaultCountryParameters** parameter is enabled. If the **OverrideDefaultCountryParameters** parameter is disabled, the values set in the current row are not applied.

This parameters override is not supported on all hardware.

Id (Index) | Table: FxoCustomBasicParameters

Type	Text
Range	
Script/CLI	Pots.FxoCustomBasicParameters[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.5200.1.100

String that identifies a FXO line.

OverrideDefaultCountryParameters (Config Parameter) | Table: FxoCustomBasicParameters

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Pots.FxoCustomBasicParameters[].OverrideDefaultCountryParameters
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.5200.1.200

Overrides the default country basic parameters for this FXO line.

- Disable: The FXO line uses the default country values. The values set in the current row are not applied.
- Enable: The FXO line uses the custom values as defined in the current row. To reset the parameter values to the default country values, use the Reset row command.

This setting is not supported on all hardware.

Impedance (Config Parameter) | Table: FxoCustomBasicParameters

Type	Enum
Range	I600(100) | I600LongLoop(200) | I900(300) | Australia(400) | Australia2(420) | Austria(500) | Belgium(600) | Brazil(700) | China(800) | CzechRepublic(900) | Denmark(1000) | Finland(1100) | France(1200) | Germany(1300) | Greece(1400) | Italy(1500) | Japan(1600) | Netherlands(1700) | NewZealand(1800) | Norway(1900) | Russia(2000) | Slovakia(2100) | Spain(2200) | Sweden(2300) | UK(2400)
Default	I600
Script/CLI	Pots.FxoCustomBasicParameters[].Impedance
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.5200.1.300

AC Impedance for the FXO line.
Not all values are supported on all hardware.

Impedance values are:

- I600: 600 ohms.
- I600LongLoop: 350 ohms + (1000 ohms || 210 nF).
- I900: 900 ohms.
- Australia: 220 ohms + (820 ohms || 115 nF).
- Australia2: 220 ohms + (820 ohms || 115 nF) with Spark Quenching.

- Others: Refer to the FXO properties section of the Country Specifications document.

For more details, refer to the Country Specifications document published on the Media5 documentation portal.

DigitalHybrid (Config Parameter) | Table: FxoCustomBasicParameters

Type	Text
Range	Size(0..512)
Default	
Script/CLI	Pots.FxoCustomBasicParameters[].DigitalHybrid
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.5200.1.400

The digital hybrid filter is applied over the Impedance, and helps reduce near-end echo.
Contact the Media5 Technical Assistance Center for support on how to use this parameter.

Reset (Row Command) | Table: FxoCustomBasicParameters

Script/CLI:	Pots.FxoCustomBasicParameters[].Reset
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.5200.1.10000

Resets the FXO basic parameter values with the default country values. This command is used to retrieve the default country values.

FxoLinkState (Table)

A table of link state updated by the link state verification mechanism.

Id (Index) | Table: FxoLinkState

Type	Text
Range	
Script/CLI	Pots.FxoLinkState[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.10100.100.1.100

String that identifies a FXO line.

LinkState (Status Parameter) | Table: FxoLinkState

Type	Enum
Range	Unknown(100) | Up(200) | Down(300)
Script/CLI	Pots.FxoLinkState[].LinkState
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.10100.100.1.200

Link state as reported by the link state verification mechanism. The link state verification can be enabled by using the **FxoLinkStateVerification** parameter object.

The unit does not automatically detect when a previously connected port has changed to the disconnected status. The unit only detects the change of status when it attempts to use the port or after a restart.

The unit automatically detects within seconds when a disconnected port becomes connected.

- Unknown: The line fault detection is disabled.
- Up: When last polled, the line was connected.
- Down: When last polled, the line was disconnected.

FxoLinkStateVerification (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Pots.FxoLinkStateVerification
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.10100.200

The link state verification mechanism allows the detection of defective or down lines based on the absence of current when closing the loop. The link state is reported in the **FxoLinkState** parameter.

FxoLinkStateVerificationTimeout (Config Parameter)

Type	UInt32
Range	500..10000
Default	5000
Script/CLI	Pots.FxoLinkStateVerificationTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.10100.300

Indicates how long the unit waits to successfully take the line before considering the line is *Down*. The link state is reported in the **FxoLinkState** parameter.
This value is expressed in milliseconds (ms).

FxoLinkStateVerificationPowerDenial (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Pots.FxoLinkStateVerificationPowerDenial
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.10100.400

When enabled, the link state verification mechanism can detect, through power denial events, if the FXO link is not powered.

The process can take between 5 seconds and 15 seconds to complete before declaring the link state as *Down*. The link state is reported in the **FxoLinkState** parameter.

This parameter has no effect if the **FxoLinkStateVerification** parameter is disabled.

FxoFeocOnCallFailureEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Pots.FxoFeocOnCallFailureEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.10200.100

Enables forced-end-of-call on call failure.

This feature forcefully terminates a call that stayed in an error state for some time. When the line falls in an error state where a SIT, a ROH, a BUSY or any error tone is played outbound to the FXO line, the unit waits for the timeout specified by the **FxoFeocOnCallFailureTimeout** parameter and then hangs up.

FxoFeocOnCallFailureTimeout (Config Parameter)

Type	UInt32
Range	0..180
Default	30
Script/CLI	Pots.FxoFeocOnCallFailureTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.10200.200

The waiting period before terminating a call in an error state. See the **FxoFeocOnCallFailure** parameter.

This value is expressed in seconds (sec).

FxoFeocOnSilenceDetectionMode (Config Parameter)

Type	Enum
Range	Disable(100) | InbountAndOutboundSilent(400)
Default	Disable
Script/CLI	Pots.FxoFeocOnSilenceDetectionMode
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.10200.300

Enables forced-end-of-call on silence detection.
This feature forcefully terminates a call that stayed silent for some time. When silence is detected on the inbound and/or outbound media for an amount of time specified by **FxoFeocOnSilenceDetectionTimeout**, the call is terminated.

- Disable: Forced-end-of-call on silence detection is disabled.
- InbountAndOutboundSilent: The call is terminated if both inbound and outbound media are silent at the same time.

This feature is useful to free resources in the event of a network failure preventing the end-of-call to be detected or when the FXO end-of-call tone was not detected.

FxoFeocOnSilenceDetectionTimeout (Config Parameter)

Type	UInt32
Range	1..300
Default	300
Script/CLI	Pots.FxoFeocOnSilenceDetectionTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.10200.400

Maximum amount of time that a call can remain silent, as specified by **FxoFeocOnSilenceDetectionMode**, before it is terminated and the line is released.

This value is expressed in seconds (sec).

FxoFeocOnToneDetectionMode (Config Parameter)

Type	Enum
Range	Disable(100) | CountryTone(200) | CustomTone(300)
Default	CountryTone
Script/CLI	Pots.FxoFeocOnToneDetectionMode
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.10200.500

Enables forced-end-of-call upon tone detection.
This feature terminates a call on detection of an end-of-call tone on the inbound from the FXO line.

- Disable: Force-end-of-call upon tone detection is disabled.
- CountryTone: The unit tries to detect the tone specified for this purpose in the current country's tone specification. Some country specifications omit this information. In that case, the unit behaves as if the **FxoFeocOnToneDetectionMode** parameter is 'disable'. See the **TelIf.CountrySelection** parameter.
- CustomTone: Terminates a call upon detection of a custom tone. This custom tone is configured with the **FxoFeocToneCustomFrequency**, **FxoFeocToneCustomCadence**, and **FxoFeocToneCustomRepetition** parameters.

FxoFeocToneCustomFrequency (Config Parameter)

Type	UInt32
Range	350..620
Default	440
Script/CLI	Pots.FxoFeocToneCustomFrequency
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.10200.10000.100

Frequency to detect in the custom cadence.
A customised tone detection can only detect a single frequency. To detect tones made of multiple frequencies, create the cadence for only one of the frequencies found in the tone.

This value is expressed in hertz (Hz).

FxoFeocToneCustomCadence (Config Parameter)

Type	Text
Range	Size(0..128)
Default	
Script/CLI	Pots.FxoFeocToneCustomCadence
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.10200.10000.200

A cadence is a series of frequencies that are played for a specified time, making up a tone. The format for a cadence is 'on, off, on, off, ...' where 'on' and 'off', respectively are numerical values representing the time in milliseconds that the frequency can and cannot be detected.
Example: '2000, 1000, 2000, 0' is a cadence where the frequency will play for 2 seconds, stop for 1 second, and play for two more seconds. This example is also equivalent to setting the string '2000, 1000, 2000'.

Up to four 'on, off' pairs can be specified. Specifying less than those eight values results in '0' values being added as necessary. When specifying more than eight, only the eight first values are used.

A cadence starting with a value of zero (0) is invalid. The first zero (0) found in the string signals the end of the cadence (i.e. '200, 0, 300' is the same as '200').

The allowed range for the 'on' and 'off' values are 0 to 32767. These values are expressed in milliseconds (ms).

See the **FxoFeocToneCustomFrequency** and **FxoFeocToneCustomRepetition** parameters.

FxoFeocToneCustomRepetition (Config Parameter)

Type	UInt32
Range	2..10
Default	3
Script/CLI	Pots.FxoFeocToneCustomRepetition
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.10200.10000.300

Repetition of the cadence. See the **FxoFeocToneCustomCadence** parameter.

Number of times the custom cadence must be detected to consider the custom end-of-call tone has been detected.

FxoInteropNormalizeFskCallerId (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Pots.FxoInteropNormalizeFskCallerId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.10300.100

The signal strength of an FSK Caller ID should be constant. Enabling this parameter will help to properly detect a Caller ID when the signal sent by the service provider is not stable enough.

- Disable: The FSK signal strength is left unchanged.
- Enable: The FSK signal strength is normalised by the Caller ID detector.

FxoInteropIgnoreInvalidCallerIdChecksum (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Pots.FxoInteropIgnoreInvalidCallerIdChecksum
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.20000.10300.200

Enabling this parameter may help to detect a received FSK Caller ID even when the decoded data is slightly corrupted.

- Disable: The FSK Caller ID data is rejected if decoding errors occurred.
- Enable: The FSK Caller ID data is accepted even if the checksum is invalid or its end-bit is missing.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Pots.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Pots.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1800.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Pots service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.1800.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	The endpoint %1$s power protection goes in power denial for %2$d seconds.	Error	The endpoint power protection goes in power denial.
20	The endpoint %1$s power protection exited power denial.	Error	The endpoint power protection exited power denial.
30	The endpoint %1$s power protection lowered the loop current to %2$dmA.	Error	The endpoint power protection lowered the loop current.
40	Message is awaiting attention for endpoint %1$s.	Debug	The endpoint has at least one message awaiting attention on the voice-messaging system. The message waiting feature is used to alert the user that a new message is waiting for an attention.
50	No more messages are awaiting attention for endpoint %1$s.	Debug	The endpoint does not have any more messages awaiting attention on the voice-messaging system.
60	Endpoint %1$s: Automatically cancelling call on no answer.	Info	The unit is cancelling the call because it was not answered within the auto cancel timeout period.
70	Disconnection of emergency call %1$d was denied on endpoint %2$s	Info	This notification occurs in the event where the grace period expired after the originator of an emergency call hangs-up before the emergency call center disconnects the call. See also parameter **FxsEmergencyRingTimeout**
80	The endpoint %1$s off-hooks the emergency call %2$d	Debug	This notification occurs when an endpoint re-connects to an emergency call after trying to disconnect
90	Endpoint %1$s: The unit cannot allocate a DSP channel to process the call: all DSP resources are currently in use.	Warning	The unit rejected the call: the endpoint could not allocate a DSP channel to process the call.
95	Endpoint %1$s: Received a caller-id with mismatched modulation.	Info	This notification occurs when the endpoint has received a Caller ID with a different modulation than the one configured in the **Pots.CallerIdCustomization** parameter.
100	Text message is sent as caller-id to %1$s Endpoint.	Info	This notification occurs when the unit receives a text message notification and succesfully sends it to the corresponding endpoint as the caller id.

NumKey	Message	Severity	Description
110	Text message cannot be sent to %1$s Endpoint: Invalid state.	Warning	This notification occurs when the unit receives a text message notification and fails to send it to the corresponding endpoint because the state is invalid.
120	Endpoint %1$s: Polarity reversal not detected (timeout); automatically answering the call.	Warning	Answer supervision usually notifies that the call has been answered via a line polarity reversal.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.

NumKey	Message	Severity	Description
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.

NumKey	Message	Severity	Description
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Pots.

Message	Severity	Description
Unsupported Visual Message Waiting Indicator type.	Error	The requested Visual Message Waiting Indicator type is not supported by the device.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.

Message	Severity	Description
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

R2 Channel Associated Signaling (R2)

The R2 Channel Associated Signaling (R2) service manages the E1 CAS telephony interfaces.

Parameters

R2 (Table)

Configuration parameters related to the R2 channel associated signaling (R2 CAS) on this managed device.

Name (Index) | Table: R2

Type	Text
Range	
Script/CLI	R2.R2[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.100.1.100

Name that identifies the interface.

ChannelRange (Config Parameter) | Table: R2

Type	Text
Range	Size(1..10)
Default	1-30
Script/CLI	R2.R2[].ChannelRange
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.100.1.200

Defines the range of active bearer channels.

ChannelAllocationStrategy (Config Parameter) | Table: R2

Type	Enum
Range	Ascending(100) | Descending(200) | RoundRobinAscending(300) | RoundRobinDescending(400)
Default	Ascending
Script/CLI	R2.R2[].ChannelAllocationStrategy
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.100.1.300

Defines the strategy for selecting bearer channels. Available strategies are:

- Ascending: select the lowest-numbered non-busy bearer channel
- Descending: select the highest-numbered non-busy bearer channel
- RoundRobinAscending: use a cyclic round-robin search; starting from the bearer channel that follows the bearer channel used for the last call, select the lowest-numbered non-busy bearer channel
- RoundRobinDescending: use a cyclic round-robin search; starting from the bearer channel that precedes the bearer channel used for the last call, select the highest-numbered non-busy bearer channel

MaxActiveCalls (Config Parameter) | Table: R2

Type	UInt32
Range	0..30
Default	0
Script/CLI	R2.R2[].MaxActiveCalls
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.100.1.400

Defines the maximum number of active calls on the interface.
Note: The special value 0 indicates no maximum number of active calls.

EncodingScheme (Config Parameter) | Table: R2

Type	Enum
Range	G711alaw(100) | G711ulaw(200)
Default	G711alaw
Script/CLI	R2.R2[].EncodingScheme
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.100.1.500

Defines the voice encoding scheme in the bearer capabilities.This encoding scheme is used when initiating a call on the R2 side. The supported encoding schemes are G.711 u-Law and G.711 A-Law.

LineSignaling (Config Parameter) | Table: R2

Type	Enum
Range	Q4212BitsSignaling(100)
Default	Q4212BitsSignaling
Script/CLI	R2.R2[].LineSignaling
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.100.1.600

Defines the protocol to use for the line signaling:

- Q421-2BitsSignaling: R2 line signaling type ITU-U Q.421. Typically used for PCM systems.

This signaling protocol must match the one used by the connected equipment or network.

IncomingDigitSignaling (Config Parameter) | Table: R2

Type	Enum
Range	MfcR2(100) | DtmfR2(200)
Default	MfcR2
Script/CLI	R2.R2[].IncomingDigitSignaling
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.100.1.750

Defines the R2 incoming digit signaling method.

- MfcR2: Multi Frequency Compelled - R2.
- DtmfR2: Dual Tone Multi Frequency - R2.

Digit signaling is also known as Address Signaling, Selection Signals, and Register Signaling. The digits are used primarily to indicate the called number, but can also have other meanings, as documented in the ITU-T Q.441 specification.

OutgoingDigitSignaling (Config Parameter) | Table: R2

Type	Enum
Range	MfcR2(100) | DtmfR2(200)
Default	MfcR2
Script/CLI	R2.R2[].OutgoingDigitSignaling
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.100.1.760

Defines the R2 outgoing digit signaling method.

- MfcR2: Multi Frequency Compelled - R2.
- DtmfR2: Dual Tone Multi Frequency - R2.

Digit signaling is also known as Address Signaling, Selection Signals, and Register Signaling. The digits are used primarily to indicate the called number, but can also have other meanings, as documented in the ITU-T Q.441 specification.

CountrySelection (Config Parameter) | Table: R2

Type	Enum
Range	BrazilR2(100) | MexicoR2(200) | ArgentinaR2(300) | SaudiArabiaR2(400) | VenezuelaR2(500) | PhilippinesR2(600) | ITUTR2(700)
Default	BrazilR2
Script/CLI	R2.R2[].CountrySelection
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.100.1.800

Identifies the country.

- Brazil-R2: Brazil R2 setting.
- Mexico-R2: Mexico R2 setting.
- Argentina-R2: Argentina R2 setting.
- SaudiArabia-R2: SaudiArabia R2 setting.
- Venezuela-R2: Venezuela R2 setting.
- Philippines-R2: Philippines R2 setting.
- ITU-T-R2: ITU-T R2 setting.

DigitAttenuation (Config Parameter) | Table: R2

Type	UInt32
Range	0..20
Default	0
Script/CLI	R2.R2[].DigitAttenuation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.100.1.900

Additional attenuation in dB for MFR2/DTMF digit generation. By default, MFR2/DTMF digit generation power is determined by country selection. This parameter provides a mean to reduce this power.

R2SignalingVariants (Table)

This table allows to override or retrieve the default country settings for R2 signaling parameters. This table is effective only if the **OverrideDefault** parameter is Enabled. If the **OverrideDefault** parameter is Disabled, any change in this table have no effects.

InterfaceName (Index) | Table: R2SignalingVariants

Type	Text
Range	
Script/CLI	R2.R2SignalingVariants[].InterfaceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.200.1.100

Identifies the interface.

OverrideDefault (Config Parameter) | Table: R2SignalingVariants

Type	EnableDisable
Range	
Default	Disable
Script/CLI	R2.R2SignalingVariants[].OverrideDefault
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.200.1.300

Overrides the default settings of R2 Signaling parameters for the **CountrySelection** and **InterfaceName**.

- Disable: The interface uses the default country configuration. The configuration set in the current row has no effect on the default country configuration. Refer to the technical documentation to get the default country variants configuration.
- Enable: The interface uses the specific country configuration as defined in the current row. To retrieve the default configuration associated with the current country, the parameter reset MUST be enabled.

BitsCD (Config Parameter) | Table: R2SignalingVariants

Type	Int32
Range	0..12
Default	1
Script/CLI	R2.R2SignalingVariants[].BitsCD
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.200.1.400

Settings of the C and D bits when the device transmits line signals. C and D bits of received line signals are ignored by the device.

DnisLength (Config Parameter) | Table: R2SignalingVariants

Type	UInt32
Range	0..20
Default	0
Script/CLI	R2.R2SignalingVariants[].DnisLength
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.200.1.500

This parameter specifies the expected length of the DNIS. DNIS (Dialed Number Identification Service) is the called party or the destination number. If a variable length is defined, then the I-15 digit is used to indicate the end of DNIS.

- 0: Variable DNIS length used.
- 1..20: Number indicates the specific DNIS expected length.

AniLength (Config Parameter) | Table: R2SignalingVariants

Type	UInt32
Range	0..20
Default	0
Script/CLI	R2.R2SignalingVariants[].AniLength
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.200.1.600

Defines the length of ANI (Automatic Number Identification) to be requested or sent. If a variable length ANI is used, the tone set in the **R2ToneVariants.FwdGroup1EndOfAni** parameter is sent to indicate the end of the ANI digits. When fixed length ANI is used and the available ANI digits are longer than the requested length, the last n digits are sent. If available ANI digits are shorter, then the **R2ToneVariants.FwdGroup1EndOfAni** parameter tone is sent.

- 0: Variable ANI length.
- 1..20: Specific ANI length.

AniRequestEnable (Config Parameter) | Table: R2SignalingVariants

Type	EnableDisable
Range	
Default	Enable
Script/CLI	R2.R2SignalingVariants[].AniRequestEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.200.1.700

Defines whether or not ANI should be requested. ANI (Automatic Number Identification) is the calling party number. When ANI is requested, the calling party category followed by the actual ANI is sent. If this parameter is enabled, the ANI request is sent after the nth DNIS digits (defined in the **SendAniRequestAfterDnisDigits** parameter) received.

SendAniRequestAfterDnisDigits (Config Parameter) | Table: R2SignalingVariants

Type	UInt32
Range	0..10
Default	0
Script/CLI	R2.R2SignalingVariants[].SendAniRequestAfterDnisDigits
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.200.1.800

When the **AniRequestEnable** parameter is Enabled, this parameter defines the number of DNIS (Dialed Number Identification Service) digits to be received before sending the ANI request. If a variable number is used, the ANI request is sent after all DNIS digits have been received.

- 0: Variable number of DNIS digits.
- 1..10: Specific number of DNIS digits.

CollectCallBlocked (Config Parameter) | Table: R2SignalingVariants

Type	EnableDisable
Range	
Default	Enable
Script/CLI	R2.R2SignalingVariants[].CollectCallBlocked
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.200.1.900

Defines if the Collect Call Blockage Option is used.
Two methods actually exist to do Collect Call Blockage. The first method refers to R2 signaling and how, through the use of signals, collect calls can be blocked. The second method refers to how, through the use of double answer, the same ends can be achieved.

For an incoming collect call, a signal of Group II-8 is sent forward from the caller to the called party. The called party implements the collect call blockage (when the **CollectCallBlocked** parameter is enabled) by sending backward to the caller a signal of Group B-7 indicating that the collect calls are not being accepted by the called party. Consequently, the originator of the call gets a busy tone and the local calling party circuit that has been used for the call is dropped when the originator puts the phone on hook.

The double answer allows the destination side to reject or accept a collect call (toll). Since the owner of the collect call is the person being called, the CO recognizes that the call is being dropped just by the fact that the call was dropped. For regular, non-collect calls, the owner of the call is the person calling and not the party being called. So, if the receiver of the call decides to refuse the call, a double answer is generated within a specified time. If the receiver wants to answer the call, a double answer is not generated and the receiver is then billed for the incoming call.

- Enable: The signal of Group B-7 is sent if a Group II-8 (Collect Call) signal is received from the caller or a double answer is generated within a specified time depending on the value defined in the **R2TimerVariants** table.
- Disable: No signal is sent in response to a Group II-8 (Collect Call) signal and/or no double answer is generated by the called side upon incoming calls.

AniCategory (Config Parameter) | Table: R2SignalingVariants

Type	Enum
Range	NatSubscriberNoPrio(100) | NatSubscriberPrio(200) | NatMaintenance(300) | NatSpare(400) | NatOperator(500) | NatData(600) | IntSubscriberNoPrio(700) | IntData(800) | IntSubscriberPrio(900) | IntOperator(1000) | CollectCall(1100)
Default	NatSubscriberNoPrio
Script/CLI	R2.R2SignalingVariants[].AniCategory
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.200.1.920

Specifies the group II forward signal to be sent on receiving a calling party category request. This tone indicates the category of the calling party.

- NatSubscriberNoPrio: Call is set up from a national subscriber's line and is not a priority.
- NatSubscriberPrio: Call is set up from a national subscriber's line to which priority treatment of calls has been granted.
- NatMaintenance: Call comes from a national maintenance equipment.
- NatSpare: Spare.

- NatOperator: Call is set up from a national operator's position.
- NatData: Call will be used for national data transmission.
- IntSubscriberNoPrio: Call is set up from an international subscriber's line and is not a priority.
- IntData: Call will be used for international data transmission.
- IntSubscriberPrio: Call is set up from an international subscriber's line to which priority treatment of calls has been granted.
- IntOperator: Call is set up from an international operator's position.
- CollectCall: Call is set up for Call Collect.

LineFreeCategory (Config Parameter) | Table: R2SignalingVariants

Type	Enum
Range	LineFreeCharge(100) | LineFreeNoCharge(200)
Default	LineFreeCharge
Script/CLI	R2.R2SignalingVariants[].LineFreeCategory
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.200.1.930

Specifies the group B backward signal to be sent by the incoming R2 register to indicate line free condition of the destination party.

- LineFreeCharge : Called party's line is free but is to be charged on answer.
- LineFreeNoCharge: Called party's line is free but is not to be charged on answer.

AniRestrictedEnable (Config Parameter) | Table: R2SignalingVariants

Type	EnableDisable
Range	
Default	Enable
Script/CLI	R2.R2SignalingVariants[].AniRestrictedEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.200.1.950

This parameter specifies the behaviour of the unit following the reception of a reject request after sending the Send next digit (ANI) request. The request is generally rejected when the calling party is unable to send its identification.

- Enable: A congestion tone is sent in response to the reject request and the call should be dropped by the caller.
- Disable: The unit uses the same behaviour as the End of ANI Tone and the call continues.

IncomingDeclineMethod (Config Parameter) | Table: R2SignalingVariants

Type	Enum
Range	Release(100) | ClearBack(200)
Default	Release
Script/CLI	R2.R2SignalingVariants[].IncomingDeclineMethod
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.200.1.970

Sets how to cancel a call attempt from R2 if the called party rejects the call when in Seizure Acknowledged state (waiting for answer).

- Release: B bit is set to 0 and state is set to Released.
- ClearBack: B bit is set to 0 until decline guard expires then B bit is set to 1 and state is set to Clear-back.

See also **R2TimerVariants.DeclineGuardTimeout** parameter.

ResetSpecific (Row Command) | Table: R2SignalingVariants

Script/CLI:	R2.R2SignalingVariants[].ResetSpecific
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.200.1.1000

Resets specific settings of R2 Signaling parameters with the default country settings. This command is used to retrieve the default country configuration set in the **CountrySelection** parameter.

R2TimerVariants (Table)

This table allows to override or retrieve the default country setting for R2 Timers.

InterfaceName (Index) | Table: R2TimerVariants

Type	Text
Range	
Script/CLI	R2.R2TimerVariants[].InterfaceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.100

Identifies the interface.

OverrideDefault (Config Parameter) | Table: R2TimerVariants

Type	EnableDisable
Range	
Default	Disable
Script/CLI	R2.R2TimerVariants[].OverrideDefault
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.300

Overrides the default setting of R2 Timers for the **CountrySelection** and **InterfaceName**.

- Disable: The interface uses the default country configuration. The configuration set in the current row has no effects on the default country configuration. Refer to the technical documentation to get the default country timers configuration.
- Enable: The interface uses the specific country configuration as defined in the current row. To retrieve the default configuration associated with the current country, the parameter reset MUST be enabled.

SeizureAckTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	0..10000
Default	2000
Script/CLI	R2.R2TimerVariants[].SeizureAckTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.400

Maximum time an outgoing R2 register waits for the seizure acknowledgement signal after sending a seizure signal.
This value is expressed in milliseconds (ms).

FaultSeizureAckTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	0..100000
Default	60000
Script/CLI	R2.R2TimerVariants[].FaultSeizureAckTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.500

Maximum time an incoming R2 register waits for a seizure acknowledge failure condition to clear.
This value is expressed in milliseconds (ms).

DoubleSeizureTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	0..1000
Default	100
Script/CLI	R2.R2TimerVariants[].DoubleSeizureTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.600

Minimum time an outgoing R2 register waits after a double seizure is recognized before releasing the connection.
This value is expressed in milliseconds (ms).

DoubleAnswerTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	0..90000
Default	1500
Script/CLI	R2.R2TimerVariants[].DoubleAnswerTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.700

Maximum time an outgoing R2 register waits after receiving a clear-backward signal before releasing the connection.
This value is expressed in milliseconds (ms).

AnswerTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	0..8000
Default	0
Script/CLI	R2.R2TimerVariants[].AnswerTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.710

Maximum time the answer signal AB=01 is applied before the clear backward signal AB=11 is sent. This parameter is generally used to reject collect calls (toll) and is only available if the **CollectCallBlocked** parameter is enabled.

A value of 0 means that the signal is applied until the call is disconnected. However, if a special event (flash hook) is detected in the answered state then the clear backward signal AB=11 is immediately applied for a period corresponding to **ReAnswerTimeout**.

This value is expressed in milliseconds (ms).

ReAnswerTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	0..8000
Default	1000
Script/CLI	R2.R2TimerVariants[].ReAnswerTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.720

Maximum time the clear backward signal AB=11 is applied before the answer signal AB=01 is reapplied again. This parameter is generally used to reject collect calls (toll) and is only available if the **CollectCallBlocked** parameter is enabled.

The **ReAnswerTimeout** parameter is only applied if the **AnswerTimeout** or an event generating the clear backward signal is triggered.

This value is expressed in milliseconds (ms).

ReleaseGuardTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	0..4000
Default	100
Script/CLI	R2.R2TimerVariants[].ReleaseGuardTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.800

Maximum time an incoming R2 register waits after sending an idle line signal to prevent a new seizure of the line when a clear forward line signal is received.
This value is expressed in milliseconds (ms).

InterCallGuardTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	0..15000
Default	100
Script/CLI	R2.R2TimerVariants[].InterCallGuardTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.820

Maximum time an outgoing R2 register waits after receiving an idle line signal before attempting a new seizure of the line.
This value is expressed in milliseconds (ms).

NoDigitTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	0..120000
Default	0
Script/CLI	R2.R2TimerVariants[].NoDigitTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.830

Maximum time an incoming R2 register waits before sending the congestion tone when no digits are received.
This value is expressed in milliseconds (ms).

CongestionToneGuardTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	0..200000
Default	1000
Script/CLI	R2.R2TimerVariants[].CongestionToneGuardTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.850

Maximum time an incoming R2 register waits after sending a congestion tone before sending a clear forward line signal and transits to the idle state.
This value is expressed in milliseconds (ms).

UnblockingTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	0..4000
Default	100
Script/CLI	R2.R2TimerVariants[].UnblockingTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.900

Maximum time a both-way trunk waits before assuming an idle state when a blocking condition is removed. This will prevent a too aggressive seizure of the trunk.
This value is expressed in milliseconds (ms).

AddressCompleteTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	0..120000
Default	8000
Script/CLI	R2.R2TimerVariants[].AddressCompleteTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.1000

The Address Complete Timeout is the maximum time that the caller waits for a reception of AddressComplete Tone after sending all ANI or DNIS Digits.
This value is expressed in milliseconds (ms).

WaitAnswerTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	0..600000
Default	60000
Script/CLI	R2.R2TimerVariants[].WaitAnswerTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.1100

The maximal time that the caller waits for an Answer signal (ANSW) after receiving a Group B Line Free Signal Tone. This timer is effective only when the line is free.
This value is expressed in milliseconds (ms).

DigitCompleteTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	0..10000
Default	4000
Script/CLI	R2.R2TimerVariants[].DigitCompleteTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.1200

The maximal time that the caller waits for a Group I forward tone after sending either a Group A next Dnis digit, next Ani digit or next calling category Tone.
This value is expressed in milliseconds (ms).

WaitGroupBResponseCompleteTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	0..30000
Default	3000
Script/CLI	R2.R2TimerVariants[].WaitGroupBResponseCompleteTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.1300

The maximal time that the caller waits for the confirmation of the end of the compelled sequence after receiving a Group B Signal Tone. The end of the compelled sequence is detected by a transition of the backward tone to off.

This value is expressed in milliseconds (ms).

WaitImmediateResponseCompleteTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	0..10000
Default	1000
Script/CLI	R2.R2TimerVariants[].WaitImmediateResponseCompleteTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.1400

The maximal time that the caller waits for the confirmation of the end of the compelled sequence after receiving a Group B Signal Tone. The end of the compelled sequence is detected by a transition of the backward tone to off. This timer is specific to the immediate accept Signal Tone.
This value is expressed in milliseconds (ms).

PlayToneGuardTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	0..2000
Default	70
Script/CLI	R2.R2TimerVariants[].PlayToneGuardTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.1500

The maximum time an incoming R2 registers waits after receiving the confirmation of the reception of the Group B Signal Tone before playing one of the calling tones in the caller direction.
This value is expressed in milliseconds (ms).

AcceptCallTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	0..10000
Default	2000
Script/CLI	R2.R2TimerVariants[].AcceptCallTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.1600

Time that the unit waits to accept a R2 CAS call.

This value is expressed in milliseconds (ms).

ClearForwardGuardTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	0..600000
Default	1500
Script/CLI	R2.R2TimerVariants[].ClearForwardGuardTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.1700

The maximum time an outgoing R2 register waits after sending a clear forward line signal before transiting to the idle state.
This value is expressed in milliseconds (ms).

ClearBackwardGuardTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	0..600000
Default	1500
Script/CLI	R2.R2TimerVariants[].ClearBackwardGuardTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.1800

The maximum time an incoming R2 register waits after sending a clear backward line signal before sending the idle line signal and transit in the idle state.
This value is expressed in milliseconds (ms).

FaultOnAnsweredGuardTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	0..86400000
Default	250
Script/CLI	R2.R2TimerVariants[].FaultOnAnsweredGuardTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.1900

The maximum time an outgoing R2 register waits for the fault to clear before sending the clear forward line signal. In the case of recognition of bb = 0 while in the answered state, no immediate

action is taken. However, the clear forward signal will be sent if bb = 1 is restored or the answered guard timeout is reached.
This value is expressed in milliseconds (ms).

FaultOnClearBackwardGuardTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	0..86400000
Default	250
Script/CLI	R2.R2TimerVariants[].FaultOnClearBackwardGuardTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.2000

The maximum time an outgoing R2 register waits for the fault to clear before sending the clear forward line signal. In the case of recognition of bb = 0 while in the clear backward state, no immediate action is taken. However, the clear forward signal will be sent if bb = 1 is restored or the clear backward guard timeout is reached.
This value is expressed in milliseconds (ms).

FaultOnSeizeAckGuardTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	0..86400000
Default	250
Script/CLI	R2.R2TimerVariants[].FaultOnSeizeAckGuardTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.2100

The maximum time an outgoing R2 register waits for the fault to clear before sending the clear forward line signal. In the case of recognition of bb = 0 while in the seize acknowledge state prior to the answer signal, no immediate action is taken. However, the clear forward signal will be sent if bb = 1 is restored or the seize acknowledge guard timeout is reached.
This value is expressed in milliseconds (ms).

FaultOnSeizeGuardTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	0..86400000
Default	250
Script/CLI	R2.R2TimerVariants[].FaultOnSeizeGuardTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.2200

The maximum time an outgoing R2 register waits for the fault to clear before sending the clear forward line signal. In the case of recognition of bb = 0 while in the seize state, no immediate action is taken. However, when the seize acknowledgement signal is recognized after the seize ack timeout period has elapsed or the seize guard timeout, the clear forward signal will be sent.
This value is expressed in milliseconds (ms).

DeclineGuardTimeout (Config Parameter) | Table: R2TimerVariants

Type	Int32
Range	1000..2000
Default	1500
Script/CLI	R2.R2TimerVariants[].DeclineGuardTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.2250

Maximum time the AB=10 release signal is applied before sending the AB=11 clearback signal. This parameter applies when the **IncomingDeclineMethod** parameter is set to 'ClearBack' while declining a call.

This value is expressed in milliseconds (ms).

ResetSpecific (Row Command) | Table: R2TimerVariants

Script/CLI:	R2.R2TimerVariants[].ResetSpecific
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.300.1.2300

Resets specific settings of R2 Timers parameters with the default country settings. This command is used to retrieve the default country configuration set in the **CountrySelection** parameter.

R2DigitTimerVariants (Table)

This table allows to override or retrieve the default country setting for R2 Digit Timers.

InterfaceName (Index) | Table: R2DigitTimerVariants

Type	Text
Range	
Script/CLI	R2.R2DigitTimerVariants[].InterfaceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.400.1.100

Identifies the interface.

OverrideDefault (Config Parameter) | Table: R2DigitTimerVariants

Type	EnableDisable
Range	
Default	Disable
Script/CLI	R2.R2DigitTimerVariants[].OverrideDefault
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.400.1.300

Overrides the default setting of R2 Digit timers for the **CountrySelection** and **InterfaceName**.

- Disable: The interface uses the default country configuration. The configuration set in the current row has no effects on the default country configuration. Refer to the technical documentation to get the default country timers configuration.
- Enable: The interface uses the specific country configuration as defined in the current row. To retrieve the default configuration associated with the current country, the parameter reset MUST be enabled.

MfCongestionToneDuration (Config Parameter) | Table: R2DigitTimerVariants

Type	Int32
Range	0..120000
Default	0
Script/CLI	R2.R2DigitTimerVariants[].MfCongestionToneDuration
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.400.1.350

Allows the administrator to specifically configures the duration of the transmission of the congestion tone. The special value '0' sets the duration according to the **R2DigitTimerVariants.MfcPulseMinOnTimeout** parameter, which sets the minimum duration of all backward tones.

This value is expressed in milliseconds (ms).

MfcPulseInterDigitTimeout (Config Parameter) | Table: R2DigitTimerVariants

Type	Int32
Range	0..1000
Default	100
Script/CLI	R2.R2DigitTimerVariants[].MfcPulseInterDigitTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.400.1.400

The minimum delay between the end of transmission of the last signal of the compelled cycle and the start of the next one.
This value is expressed in milliseconds (ms).

MfcPulseMinOnTimeout (Config Parameter) | Table: R2DigitTimerVariants

Type	Int32
Range	0..1000
Default	150
Script/CLI	R2.R2DigitTimerVariants[].MfcPulseMinOnTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.400.1.500

The minimum time a backward tone can be on from the backward perspective.

This value is expressed in milliseconds (ms).

MfcMaxSequenceTimeout (Config Parameter) | Table: R2DigitTimerVariants

Type	Int32
Range	0..70000
Default	10000
Script/CLI	R2.R2DigitTimerVariants[].MfcMaxSequenceTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.400.1.600

The maximum time for a complete compelled signaling cycle from the forward perspective.
This value is expressed in milliseconds (ms).

MfcMaxOnTimeout (Config Parameter) | Table: R2DigitTimerVariants

Type	Int32
Range	0..35000
Default	5000
Script/CLI	R2.R2DigitTimerVariants[].MfcMaxOnTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.400.1.700

The maximum time a forward tone can be on from the forward perspective.
This value is expressed in milliseconds (ms).

MfcMaxOffTimeout (Config Parameter) | Table: R2DigitTimerVariants

Type	Int32
Range	0..35000
Default	5000
Script/CLI	R2.R2DigitTimerVariants[].MfcMaxOffTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.400.1.800

The maximum time a forward tone can be off from the forward perspective.
This value is expressed in milliseconds (ms).

ResetSpecific (Row Command) | Table: R2DigitTimerVariants

Script/CLI:	R2.R2DigitTimerVariants[].ResetSpecific
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.400.1.900

Resets specific settings of R2 Digit Timers parameters with the default country settings. This command is used to retrieve the default country configuration set in the **CountrySelection** parameter.

R2LinkTimerVariants (Table)

This table allows to override or retrieve the default country setting for R2 Link Timers.

InterfaceName (Index) | Table: R2LinkTimerVariants

Type	Text
Range	
Script/CLI	R2.R2LinkTimerVariants[].InterfaceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.500.1.100

Identifies the interface.

OverrideDefault (Config Parameter) | Table: R2LinkTimerVariants

Type	EnableDisable
Range	
Default	Disable
Script/CLI	R2.R2LinkTimerVariants[].OverrideDefault
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.500.1.300

Overrides the default setting of R2 Link timers for the **CountrySelection** and **InterfaceName**.

- Disable: The interface uses the default country configuration. The configuration set in the current row has no effects on the default country configuration. Refer to the technical documentation to get the default country timers configuration.

- Enable: The interface uses the specific country configuration as defined in the current row. To retrieve the default configuration associated with the current country, the parameter reset MUST be enabled.

LinkActivationTimeout (Config Parameter) | Table: R2LinkTimerVariants

Type	Int32
Range	0..10000
Default	1000
Script/CLI	R2.R2LinkTimerVariants[].LinkActivationTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.500.1.400

The maximum time the unit waits for an activation indication coming from the physical link. The activation indication is used to indicate that the physical layer connection has been activated.
This value is expressed in milliseconds (ms).

LinkActivationRetryTimeout (Config Parameter) | Table: R2LinkTimerVariants

Type	Int32
Range	0..10000
Default	3000
Script/CLI	R2.R2LinkTimerVariants[].LinkActivationRetryTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.500.1.500

The maximum time the unit waits before attempting to reestablish the physical link. The attempt is made when the physical layer connection has been deactivated.
This value is expressed in milliseconds (ms).

ResetSpecific (Row Command) | Table: R2LinkTimerVariants

Script/CLI:	R2.R2LinkTimerVariants[].ResetSpecific
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.500.1.600

Resets specific settings of R2 Link Timers parameters with the default country settings. This command is used to retrieve the default country configuration set in the **CountrySelection** parameter.

R2ToneVariants (Table)

This table allows to override or retrieve the default country setting for R2 Tone variants in forward and backward group.

InterfaceName (Index) | Table: R2ToneVariants

Type	Text
Range	
Script/CLI	R2.R2ToneVariants[].InterfaceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.100

Identifies the interface.

OverrideDefault (Config Parameter) | Table: R2ToneVariants

Type	EnableDisable
Range	
Default	Disable
Script/CLI	R2.R2ToneVariants[].OverrideDefault
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.300

Overrides the default setting of R2 tone variants for the **CountrySelection** and **InterfaceName**.

- Disable: The interface uses the default country configuration. The configuration set in the current row has no effects on the default country configuration. Refer to the technical documentation to get the default country tones configuration.
- Enable: The interface uses the specific country configuration as defined in the current row. To retrieve the default configuration associated with the current country, the parameter reset MUST be enabled.

FwdGroup1EndOfDnis (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | I1(200) | I2(300) | I3(400) | I4(500) | I5(600) | I6(700) | I7(800) | I8(900) | I9(1000) | I10(1100) | I11(1200) | I12(1300) | I13(1400) | I14(1500) | I15(1600)
Default	I15
Script/CLI	R2.R2ToneVariants[].FwdGroup1EndOfDnis
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.400

Specifies the forward Group 1 tone used to send after the DNIS digits.

- None: No tone used.
- I1..I15: Group 1 forward signal MF Tones

FwdGroup1EndOfAni (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | I1(200) | I2(300) | I3(400) | I4(500) | I5(600) | I6(700) | I7(800) | I8(900) | I9(1000) | I10(1100) | I11(1200) | I12(1300) | I13(1400) | I14(1500) | I15(1600)
Default	I15
Script/CLI	R2.R2ToneVariants[].FwdGroup1EndOfAni
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.500

Specifies the forward Group 1 tone used to send after the ANI digits.

- None: No tone used.
- I1..I15: Group 1 forward signal MF Tones

FwdGroup1RestrictedAni (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | I1(200) | I2(300) | I3(400) | I4(500) | I5(600) | I6(700) | I7(800) | I8(900) | I9(1000) | I10(1100) | I11(1200) | I12(1300) | I13(1400) | I14(1500) | I15(1600)
Default	I12
Script/CLI	R2.R2ToneVariants[].FwdGroup1RestrictedAni
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.520

Specifies the forward Group 1 tone used to reject a send next digit (ANI). This tone is generally used in response to the identification request when the caller party is unable to send his identification to the called party. If no tone is defined, the **FwdGroup1EndOfAni** tone is sent to the caller.

- None: No tone used.
- I1..I15: Group 1 forward signal MF Tones

BwdGroupASendNextDnisDigit (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | A1(200) | A2(300) | A3(400) | A4(500) | A5(600) | A6(700) | A7(800) | A8(900) | A9(1000) | A10(1100) | A11(1200) | A12(1300) | A13(1400) | A14(1500) | A15(1600)
Default	A15
Script/CLI	R2.R2ToneVariants[].BwdGroupASendNextDnisDigit
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.600

Specifies the backward Group A tone used to request the next DNIS digit.

- None: No tone used.
- A1..A15: Group A backward signal MF Tones

BwdGroupASendPreviousDnisDigit (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | A1(200) | A2(300) | A3(400) | A4(500) | A5(600) | A6(700) | A7(800) | A8(900) | A9(1000) | A10(1100) | A11(1200) | A12(1300) | A13(1400) | A14(1500) | A15(1600)
Default	A15
Script/CLI	R2.R2ToneVariants[].BwdGroupASendPreviousDnisDigit
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.700

Specifies the backward Group A tone used to request the previous DNIS digit.

- None: No tone used.
- A1..A15: Group A backward signal MF Tones

BwdGroupASwitchToGroupII (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | A1(200) | A2(300) | A3(400) | A4(500) | A5(600) | A6(700) | A7(800) | A8(900) | A9(1000) | A10(1100) | A11(1200) | A12(1300) | A13(1400) | A14(1500) | A15(1600)
Default	A15
Script/CLI	R2.R2ToneVariants[].BwdGroupASwitchToGroupII
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.800

Specifies the backward Group A tone used to request to the caller a switch of Group II signals.

- None: No tone used.
- A1..A15: Group A backward signal MF Tones

BwdGroupANetworkCongestion (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | A1(200) | A2(300) | A3(400) | A4(500) | A5(600) | A6(700) | A7(800) | A8(900) | A9(1000) | A10(1100) | A11(1200) | A12(1300) | A13(1400) | A14(1500) | A15(1600)
Default	A15
Script/CLI	R2.R2ToneVariants[].BwdGroupANetworkCongestion
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.900

Specifies the backward Group A tone to be sent when a congestion network is detected.

- None: No tone used.
- A1..A15: Group A backward signal MF Tones

BwdGroupASendCallingPartyCategory (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | A1(200) | A2(300) | A3(400) | A4(500) | A5(600) | A6(700) | A7(800) | A8(900) | A9(1000) | A10(1100) | A11(1200) | A12(1300) | A13(1400) | A14(1500) | A15(1600)
Default	A15
Script/CLI	R2.R2ToneVariants[].BwdGroupASendCallingPartyCategory
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.1000

Specifies the backward Group A tone sent when the backward group requests the calling party category.

- None: No tone used.
- A1..A15: Group A backward signal MF Tones

BwdGroupAImmediateAccept (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | A1(200) | A2(300) | A3(400) | A4(500) | A5(600) | A6(700) | A7(800) | A8(900) | A9(1000) | A10(1100) | A11(1200) | A12(1300) | A13(1400) | A14(1500) | A15(1600)
Default	A15
Script/CLI	R2.R2ToneVariants[].BwdGroupAImmediateAccept
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.1100

Specifies the backward Group A tone sent when the backward group accepts the call immediatly.

- None: No tone used.
- A1..A15: Group A backward signal MF Tones

BwdGroupASendDnisDigitNMinus2 (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | A1(200) | A2(300) | A3(400) | A4(500) | A5(600) | A6(700) | A7(800) | A8(900) | A9(1000) | A10(1100) | A11(1200) | A12(1300) | A13(1400) | A14(1500) | A15(1600)
Default	A15
Script/CLI	R2.R2ToneVariants[].BwdGroupASendDnisDigitNMinus2
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.1200

Specifies the backward Group A tone used to request the previous - 1 DNIS digit.

- None: No tone used.
- A1..A15: Group A backward signal MF Tones

BwdGroupASendDnisDigitNMinus3 (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | A1(200) | A2(300) | A3(400) | A4(500) | A5(600) | A6(700) | A7(800) | A8(900) | A9(1000) | A10(1100) | A11(1200) | A12(1300) | A13(1400) | A14(1500) | A15(1600)
Default	A15
Script/CLI	R2.R2ToneVariants[].BwdGroupASendDnisDigitNMinus3
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.1300

Specifies the backward Group A tone used to request the previous - 2 DNIS digit.

- None: No tone used.
- A1..A15: Group A backward signal MF Tones

BwdGroupARepeatAllDnis (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | A1(200) | A2(300) | A3(400) | A4(500) | A5(600) | A6(700) | A7(800) | A8(900) | A9(1000) | A10(1100) | A11(1200) | A12(1300) | A13(1400) | A14(1500) | A15(1600)
Default	A15
Script/CLI	R2.R2ToneVariants[].BwdGroupARepeatAllDnis
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.1400

Specifies the backward Group A tone used to request all DNIS digits.

- None: No tone used.
- A1..A15: Group A backward signal MF Tones

BwdGroupASendNextAniDigit (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | A1(200) | A2(300) | A3(400) | A4(500) | A5(600) | A6(700) | A7(800) | A8(900) | A9(1000) | A10(1100) | A11(1200) | A12(1300) | A13(1400) | A14(1500) | A15(1600)
Default	A15
Script/CLI	R2.R2ToneVariants[].BwdGroupASendNextAniDigit
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.1500

Specifies the backward Group A tone used to request the next ANI digit.

- None: No tone used.
- A1..A15: Group A backward signal MF Tones

BwdGroupASendCallingPartyCategorySwitchGroupC (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | A1(200) | A2(300) | A3(400) | A4(500) | A5(600) | A6(700) | A7(800) | A8(900) | A9(1000) | A10(1100) | A11(1200) | A12(1300) | A13(1400) | A14(1500) | A15(1600)
Default	A15
Script/CLI	R2.R2ToneVariants[].BwdGroupASendCallingPartyCategorySwitchGroupC
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.1550

Specifies the backward Group A tone used to request the calling party category and then switch to Group C signals.

- None: No tone used.
- A1..A15: Group A backward signal MF Tones

BwdGroupBSendSit (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | B1(200) | B2(300) | B3(400) | B4(500) | B5(600) | B6(700) | B7(800) | B8(900) | B9(1000) | B10(1100) | B11(1200) | B12(1300) | B13(1400) | B14(1500) | B15(1600)
Default	B15
Script/CLI	R2.R2ToneVariants[].BwdGroupBSendSit
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.1600

Specifies the backward Group B tone used to send a special information tone.

- None: No tone used.
- B1..B15: Group B backward signal MF Tones

BwdGroupBUserBusy (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | B1(200) | B2(300) | B3(400) | B4(500) | B5(600) | B6(700) | B7(800) | B8(900) | B9(1000) | B10(1100) | B11(1200) | B12(1300) | B13(1400) | B14(1500) | B15(1600)
Default	B15
Script/CLI	R2.R2ToneVariants[].BwdGroupBUserBusy
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.1700

Specifies the backward Group B tone used to signal a user busy.

- None: No tone used.
- B1..B15: Group B backward signal MF Tones

BwdGroupBNetworkCongestion (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | B1(200) | B2(300) | B3(400) | B4(500) | B5(600) | B6(700) | B7(800) | B8(900) | B9(1000) | B10(1100) | B11(1200) | B12(1300) | B13(1400) | B14(1500) | B15(1600)
Default	B15
Script/CLI	R2.R2ToneVariants[].BwdGroupBNetworkCongestion
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.1800

Specifies the backward Group B tone used to signal a network congestion.

- None: No tone used.
- B1..B15: Group B backward signal MF Tones

BwdGroupBUnassignedNumber (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | B1(200) | B2(300) | B3(400) | B4(500) | B5(600) | B6(700) | B7(800) | B8(900) | B9(1000) | B10(1100) | B11(1200) | B12(1300) | B13(1400) | B14(1500) | B15(1600)
Default	B15
Script/CLI	R2.R2ToneVariants[].BwdGroupBUnassignedNumber
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.1900

Specifies the backward Group B tone used to signal an unassigned number.

- None: No tone used.
- B1..B15: Group B backward signal MF Tones

BwdGroupBLineFreeCharge (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | B1(200) | B2(300) | B3(400) | B4(500) | B5(600) | B6(700) | B7(800) | B8(900) | B9(1000) | B10(1100) | B11(1200) | B12(1300) | B13(1400) | B14(1500) | B15(1600)
Default	B15
Script/CLI	R2.R2ToneVariants[].BwdGroupBLineFreeCharge
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.2000

Specifies the backward Group B tone used to signal that the line is free and charge must be applied.

- None: No tone used.
- B1..B15: Group B backward signal MF Tones

BwdGroupBSupplementaryLineFreeCharge (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | B1(200) | B2(300) | B3(400) | B4(500) | B5(600) | B6(700) | B7(800) | B8(900) | B9(1000) | B10(1100) | B11(1200) | B12(1300) | B13(1400) | B14(1500) | B15(1600)
Default	B15
Script/CLI	R2.R2ToneVariants[].BwdGroupBSupplementaryLineFreeCharge
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.2100

Specifies a supplementary backward Group B tone used to detect that the line is free and charge must be applied. This is a supplementary (optionnal) tone used on the reception only.

- None: No tone used.
- B1..B15: Group B backward signal MF Tones

BwdGroupBLineFreeNoCharge (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | B1(200) | B2(300) | B3(400) | B4(500) | B5(600) | B6(700) | B7(800) | B8(900) | B9(1000) | B10(1100) | B11(1200) | B12(1300) | B13(1400) | B14(1500) | B15(1600)
Default	B15
Script/CLI	R2.R2ToneVariants[].BwdGroupBLineFreeNoCharge
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.2200

Specifies the backward Group B tone used to signal that the line is free and no charges must be applied.

- None: No tone used.
- B1..B15: Group B backward signal MF Tones

BwdGroupBLineOutOfOrder (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | B1(200) | B2(300) | B3(400) | B4(500) | B5(600) | B6(700) | B7(800) | B8(900) | B9(1000) | B10(1100) | B11(1200) | B12(1300) | B13(1400) | B14(1500) | B15(1600)
Default	B15
Script/CLI	R2.R2ToneVariants[].BwdGroupBLineOutOfOrder
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.2300

Specifies the backward Group B tone used to signal that the line is out of order.

- None: No tone used.
- B1..B15: Group B backward signal MF Tones

BwdGroupBChangedNumber (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | B1(200) | B2(300) | B3(400) | B4(500) | B5(600) | B6(700) | B7(800) | B8(900) | B9(1000) | B10(1100) | B11(1200) | B12(1300) | B13(1400) | B14(1500) | B15(1600)
Default	B15
Script/CLI	R2.R2ToneVariants[].BwdGroupBChangedNumber
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.2350

Specifies the backward Group B tone used to signal that the subscriber has changed number.

- None: No tone used.
- B1..B15: Group B backward signal MF Tones

BwdGroupCSendNextAniDigit (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | C1(200) | C2(300) | C3(400) | C4(500) | C5(600) | C6(700) | C7(800) | C8(900) | C9(1000) | C10(1100) | C11(1200) | C12(1300) | C13(1400) | C14(1500) | C15(1600)
Default	C15
Script/CLI	R2.R2ToneVariants[].BwdGroupCSendNextAniDigit
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.2355

Specifies the backward Group C tone used to request the next ANI digit.

- None: No tone used.
- C1..C15: Group C backward signal MF Tones

BwdGroupCRepeatAllDnisSwitchGroupA (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | C1(200) | C2(300) | C3(400) | C4(500) | C5(600) | C6(700) | C7(800) | C8(900) | C9(1000) | C10(1100) | C11(1200) | C12(1300) | C13(1400) | C14(1500) | C15(1600)
Default	C15
Script/CLI	R2.R2ToneVariants[].BwdGroupCRepeatAllDnisSwitchGroupA
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.2360

Specifies the backward Group C tone used to request all DNIS digits and then switch to Group A signals.

- None: No tone used.
- C1..C15: Group C backward signal MF Tones

BwdGroupCSendNextDnisDigitSwitchGroupA (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | C1(200) | C2(300) | C3(400) | C4(500) | C5(600) | C6(700) | C7(800) | C8(900) | C9(1000) | C10(1100) | C11(1200) | C12(1300) | C13(1400) | C14(1500) | C15(1600)
Default	C15
Script/CLI	R2.R2ToneVariants[].BwdGroupCSendNextDnisDigitSwitchGroupA
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.2365

Specifies the backward Group C tone used to request the next DNIS digit and then switch to Group A signals.

- None: No tone used.
- C1..C15: Group C backward signal MF Tones

BwdGroupCNetworkCongestion (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | C1(200) | C2(300) | C3(400) | C4(500) | C5(600) | C6(700) | C7(800) | C8(900) | C9(1000) | C10(1100) | C11(1200) | C12(1300) | C13(1400) | C14(1500) | C15(1600)
Default	C15
Script/CLI	R2.R2ToneVariants[].BwdGroupCNetworkCongestion
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.2370

Specifies the backward Group C tone used to signal a network congestion.

- None: No tone used.
- C1..C15: Group C backward signal MF Tones

BwdGroupCSendPreviousDnisDigitSwitchGroupA (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | C1(200) | C2(300) | C3(400) | C4(500) | C5(600) | C6(700) | C7(800) | C8(900) | C9(1000) | C10(1100) | C11(1200) | C12(1300) | C13(1400) | C14(1500) | C15(1600)
Default	C15
Script/CLI	R2.R2ToneVariants[].BwdGroupCSendPreviousDnisDigitSwitchGroupA
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.2375

Specifies the backward Group C tone used to request the previous DNIS digit and then switch to Group A signals.

- None: No tone used.
- C1..C15: Group C backward signal MF Tones

BwdGroupCSwitchGroupII (Config Parameter) | Table: R2ToneVariants

Type	Enum
Range	None(100) | C1(200) | C2(300) | C3(400) | C4(500) | C5(600) | C6(700) | C7(800) | C8(900) | C9(1000) | C10(1100) | C11(1200) | C12(1300) | C13(1400) | C14(1500) | C15(1600)
Default	C15
Script/CLI	R2.R2ToneVariants[].BwdGroupCSwitchGroupII
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.2380

Specifies the backward Group C tone used to request to the caller a switch of Group II signals.

- None: No tone used.
- C1..C15: Group C backward signal MF Tones

ResetSpecific (Row Command) | Table: R2ToneVariants

Script/CLI:	R2.R2ToneVariants[].ResetSpecific
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.100.600.1.2400

Resets specific settings of R2 Tones parameters with the default country settings. This command is used to retrieve the default country configuration set in the **CountrySelection** parameter.

BearerChannelInfo (Table)

Port-specific operational, statistics, and active call data for B channels.

Index (Index) | Table: BearerChannelInfo

Type	Text
Range	
Script/CLI	R2.BearerChannelInfo[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.200.100.1.100

Identifies the Bearer Channel..

State (Status Parameter) | Table: BearerChannelInfo

Type	Enum
Range	Idle(100) | InUse(200) | Maintenance(300) | Error(400) | Disabled(500)
Script/CLI	R2.BearerChannelInfo[].State
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.200.100.1.200

The current call control state for this channel:

- Idle: The channel is available
- InUse: The channel is currently used
- Maintenance: Maintenance state, temporarily unavailable
- Error: Error on this channel
- Disabled: The channel is disabled

PhysicalLinkInfo (Table)

The physical link information table contains status information for all interfaces on this managed device.

InterfaceName (Index) | Table: PhysicalLinkInfo

Type	Text
Range	
Script/CLI	R2.PhysicalLinkInfo[].InterfaceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.300.100.1.100

Identifies the interface.

State (Status Parameter) | Table: PhysicalLinkInfo

Type	Enum
Range	Up(100) | Down(200)
Script/CLI	R2.PhysicalLinkInfo[].State
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.300.100.1.200

The layer 1 state for this interface:

- Up: Layer 1 connectivity.
- Down: No layer 1 connectivity. The interface might be in this state because no cable is plugged in or a pinout problem is detected.

PhysicalLink (Table)

The physical link table containing configuration and operational parameters for all interfaces on this managed device.

InterfaceName (Index) | Table: PhysicalLink

Type	Text
Range	
Script/CLI	R2.PhysicalLink[].InterfaceName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.300.200.1.100

Identifies the interface.

LineCoding (Config Parameter) | Table: PhysicalLink

Type	Enum
Range	B8zs(100) | Hdb3(200) | Ami(300)
Default	Hdb3
Script/CLI	R2.PhysicalLink[].LineCoding
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.300.200.1.200

Defines the transmission encoding of bits:

- B8ZS: Bipolar with 8-Zeros Substitution (T1 lines)
- HDB3: High-Density Bipolar Order 3 (E1 lines)
- AMI: Alternate Mark Inversion (E1 and T1 lines)

For further information, see ITU-T G.703 Recommendation.

LineFraming (Config Parameter) | Table: PhysicalLink

Type	Enum
Range	Sf(100) | Esf(200) | Crc4(300) | NoCrc4(400)
Default	Crc4
Script/CLI	R2.PhysicalLink[].LineFraming
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.300.200.1.300

Defines the frame format:

- SF: Super frame. Sometimes known as D4 (T1 lines)
- ESF: Extended super frame (T1 lines)
- CRC4: Cyclic redundancy check 4 (E1 lines)
- NO-CRC4: No Cyclic redundancy check 4 (E1 lines)

For further information, see ITU-T G.704 Recommendation.

ClockMode (Config Parameter) | Table: PhysicalLink

Type	Enum
Range	Master(100) | Slave(200)
Default	Slave
Script/CLI	R2.PhysicalLink[].ClockMode
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.300.200.1.400

A port can either generate the clocking for the line or accept the clock from the line. The options master or slave determine the clocking method:

- Master: Generates clock
- Slave: Accepts clock

MonitorLinkStateEnable (Config Parameter) | Table: PhysicalLink

Type	EnableDisable
Range	
Default	Enable
Script/CLI	R2.PhysicalLink[].MonitorLinkStateEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.300.200.1.500

Monitors the physical link state of an R2 interface.
Enable: An R2 endpoint's operational state is affected by its interface physical link state. When the link state of an R2 interface is down, the operational state of its matching endpoint becomes "disable".

Disable: An R2 endpoint's operational state is not affected by its interface physical link state.

PortPinout (Config Parameter) | Table: PhysicalLink

Type	Enum
Range	Auto(100) | Master(200) | Slave(300)
Default	Auto
Script/CLI	R2.PhysicalLink[].PortPinout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.300.200.1.600

Defines the port pinout:

- Auto: The pinout is set according to the clock mode.
- Master: Force the pinout to Master regardless of the clock mode.
- Slave: Force the pinout to Slave regardless of the clock mode.

See the **PhysicalLink.ClockMode** parameter for a description of the clock mode.

AutoConfigureStatus (Status Parameter)

Type	Enum
Range	Idle(100) | Sensing(200)
Script/CLI	R2.AutoConfigureStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.400.100

Indicates the current status of the R2 automatic configuration mechanism.

- Idle: The automatic configuration mechanism is ready to be started.
- Sensing: The automatic configuration mechanism is currently started and is testing different R2 configurations to obtain a link up.

LastAutoConfigureResult (Status Parameter)

Type	Enum
Range	None(100) | Success(200) | Fail(300) | Aborted(400)
Script/CLI	R2.LastAutoConfigureResult
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.400.200

Result of the last R2 automatic configuration.

- None: No result is available.
- Success: The last automatic configuration succeeded.
- Fail: The last automatic configuration failed.
- Aborted: The last automatic configuration has been cancelled by the user.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	R2.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	R2.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1875.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

AutoConfigure (Command)

Auto-detect and auto-configure the R2 interfaces.

Interface (Argument) | Command: AutoConfigure

Type	Text
Range	Size(0..48)
Default	

The specific R2 Interface on which the AutoConfigure command will be executed. See the **R2.PhysicalLinkInfo** table for the exact interface name to use. Take note that the argument value is case-sensitive.
This argument is optional. If no value is provided, the command will be executed on all R2 interfaces.

CancelAutoConfigure (Command)

Stops and cancels the automatic detection and configuration mechanism.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the R2 service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.1875.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
5	%1$s: Physical link state changed to up.	Info	The physical link state has changed to up.
10	%1$s: Physical link state changed to down.	Info	The physical link state has changed to down.
15	%1$s, channel %2$d: State changed to free.	Info	The channel state has changed to free.
20	%1$s, channel %2$d: State changed to used.	Info	The channel state has changed to used.
22	%1$s: Alarm condition %2$d is detected.	Warning	An alarm condition is detected on The R2 interface.
25	%1$s: Graceful lock initiated.	Info	A graceful lock has been initiated.
30	%1$s: Abrupt lock initiated.	Info	An abrupt lock has been initiated.
35	%1$s: Locked successfully.	Info	Locked successfully.
40	%1$s, Unlocked successfully.	Info	Unlocked successfully.
45	%1$s: Cannot allocate channel, line is locked.	Warning	The unit cannot allocate a channel because the line is locked.
48	%1$s: The unit cannot allocate a DSP channel to process the call: all DSP resources are currently in use.	Warning	The unit rejected the call: the endpoint could not allocate a DSP channel to process the call.
50	%1$s: Cannot allocate channel, maximum number of calls (%2$d) reached.	Warning	The unit cannot allocate a channel because the maximum number of calls has been reached.
55	%1$s: R2 frame slip detected.	Warning	This message is issued when the physical link detects a frame slip. This happens when there is a problem with clock synchronization.
60	%1$s: Received unhandled R2 message %2$s.	Warning	Received an unhandled R2 message.

NumKey	Message	Severity	Description
65	%1$s, interface %2$d, channel %3$d: Requested number %4$s does not match any dial map.	Info	The requested number does not match any dial map.
70	Cannot find a R2 interface for outgoing call.	Info	Cannot find a R2 interface for outgoing call.
100	The R2 auto-configuration process has started.	Info	An auto-configuration process has started on R2 interfaces.
110	The R2 auto-configuration process has been cancelled.	Info	The R2 auto-configuration process has been cancelled by the user.
120	The R2 auto-configuration process has completed successfully.	Info	The R2 auto-configuration process has completed successfully. NOTE: This does not mean that the auto-configuration process has succeeded on all interfaces.
130	The R2 auto-configuration process has failed.	Error	The R2 auto-configuration process has terminated because of an error.
140	%1$s: Auto-configuration has succeeded.	Info	The auto-configuration process has succeeded on the specified R2 interface.
150	%1$s: Auto-configuration has failed.	Error	The auto-configuration process has failed on the specified R2 interface.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.

NumKey	Message	Severity	Description
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.

NumKey	Message	Severity	Description
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to R2.

Message	Severity	Description
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.

Message	Severity	Description
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Session Border Controller (Sbc)

The Session Border Controller (SBC) service allows the administrator to perform SIP to SIP normalization, call routing, NAT traversal, and survivability.

Parameters

CallAgent (Table: user-defined, 50 lines max.)

This table contains the parameter used to configure the Call Agents.
The changes to this table are applied on execution of the `ApplyConfiguration` command or when the service is restarted.

Id (Index) | Table: CallAgent

Type	UInt32
Range	
Script/CLI	Sbc.CallAgent[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.100.1.100

Unique numerical identifier for a Call Agent. The Call Agent ID is used by other parameters included in the Configuration Group to refer to a Call Agent.

Name (Config Parameter) | Table: CallAgent

Type	Text
Range	Size(0..100)
Default	
Script/CLI	Sbc.CallAgent[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.100.1.200

Call Agent name.
Alpha-numerics as well as '.', '-' and '_' are valid characters.

Enable (Config Parameter) | Table: CallAgent

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Sbc.CallAgent[].Enable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.100.1.300

Activate/deactivate the Call Agent.

SignalingInterface (Config Parameter) | Table: CallAgent

Type	UInt32
Range	
Default	0
Script/CLI	Sbc.CallAgent[].SignalingInterface
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.100.1.400

ID of the Signaling Interface used by this Call Agent.

MediaInterface (Config Parameter) | Table: CallAgent

Type	Text
Range	Size(0..6)
Default	
Script/CLI	Sbc.CallAgent[].MediaInterface
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.100.1.500

ID of the Media Interface used by this Call Agent.

Gateway (Config Parameter) | Table: CallAgent

Type	Text
Range	Size(0..100)
Default	
Script/CLI	Sbc.CallAgent[].Gateway
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.100.1.600

Name of the local gateway to be used by this Call Agent. When no local gateway is selected, the Call Agent will use an external peer.
When the **Gateway** parameter is set to a local gateway,

- the **PeerHost** and **PeerNetwork** parameters are ignored
- the **CallAgent.SignalingInterface** parameter is ignored and is replaced by the loop_s signaling interface
- the **CallAgent.MediaInterface** parameter can be left empty in which case the loop_m media interface is used

A few consistency checks are also performed when the **CallAgent.Gateway** parameter is configured:

- The gateway must exist in the SipEp service.
- The gateway's network interface must be set to 'SBC'.
- The gateway's media network must be configured on the same network as the Call Agent.

When these consistency checks fail, warning notifications are issued but the configuration is not refused.

PeerHost (Config Parameter) | Table: CallAgent

Type	IpHostNamePort
Range	
Default	
Script/CLI	Sbc.CallAgent[].PeerHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.100.1.700

FQDN / IP addr and port of the SIP peer for this Call Agent.

PeerNetwork (Config Parameter) | Table: CallAgent

Type	IpAddrMask
Range	
Default	
Script/CLI	Sbc.CallAgent[].PeerNetwork
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.100.1.800

Network address of the SIP peers for this Call Agent.

ForceTransport (Config Parameter) | Table: CallAgent

Type	Enum
Range	None(100) | TCP(200) | UDP(300) | TLS(400)
Default	None
Script/CLI	Sbc.CallAgent[].ForceTransport
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.100.1.900

Force the Call Agent to use the selected transport protocol when initiating SIP dialogs.

- None: Transport is not forced. Will use UDP if the use of another transport protocol is not forced elsewhere.
- TCP: The outbound SIP signalling will be transported over TCP on the normal port.
- UDP: The outbound SIP signalling will be transported over UDP on the normal port.
- TLS: The outbound SIP signalling will be transported over TLS on the secure port.

Note: To force TLS and guarantee that no other transport protocol can be used, you must also set the **SignalingInterface.AllowedTransports** parameter to TlsOnly.

ConfigStatus (Status Parameter) | Table: CallAgent

Type	Enum
Range	Valid(100) | UnknownSignalingInterface(200) | UnknownMediaInterface(300) | InvalidGatewayBinding(400) | InvalidConfig(500) | NoMediaInterface(600)
Script/CLI	Sbc.CallAgent[].ConfigStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.100.1.1000

Configuration status of the row.
Indicates if the configuration of this Call Agent is valid and ready to be applied.

- Valid: The current content of the row is valid.
- UnknownSignalingInterface: The Signaling Interface is not set or has an unknown ID.
- UnknownMediaInterface: The Media Interface has an unknown ID.
- InvalidGatewayBinding: The parameters binding the gateway to the Call Agent are not configured properly.
- InvalidConfig: The configuration is not valid.
- NoMediaInterface: The Media Interface is not set.

Delete (Row Command) | Table: CallAgent

Script/CLI:	Sbc.CallAgent[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.100.1.10000

Delete this **CallAgent** table entry.

CallAgentRuleset (Table: user-defined, 60 lines max.)

This table allows the user/administrator to associate Rulesets to Call Agents.
The changes to this table are applied when the `ApplyConfiguration` command is executed or when the service is restarted.

The changes to the ruleset files are applied when the `ApplyConfiguration` command is executed or when the service is restarted.

Note: Even if the **ConfigModifiedStatus** parameter does not indicate 'yes', after modifying the **CallAgentRuleset** table, you must execute the `ApplyConfiguration` command.

Id (Index) | Table: CallAgentRuleset

Type	UInt32
Range	
Script/CLI	Sbc.CallAgentRuleset[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.200.1.100

Unique numerical identifier for this Ruleset association.

CallAgent (Config Parameter) | Table: CallAgentRuleset

Type	UInt32
Range	
Default	0
Script/CLI	Sbc.CallAgentRuleset[].CallAgent
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.200.1.200

ID of the **CallAgent** table entry to which this Ruleset is attached.

Priority (Config Parameter) | Table: CallAgentRuleset

Type	UInt32
Range	1..2147483647
Default	1
Script/CLI	Sbc.CallAgentRuleset[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.200.1.300

Execution priority of this Ruleset for the Call Agent.
Inbound rules of the Ruleset are executed in ascending priority order. Outbound rules are executed in descending priority order.

Ruleset (Config Parameter) | Table: CallAgentRuleset

Type	Text
Range	Size(0..48)
Default	
Script/CLI	Sbc.CallAgentRuleset[].Ruleset
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.200.1.400

Name of the Ruleset to which the Call Agent is attached.
This name must match the name of a Call Agent ruleset file in the local storage of this device (see the File Service). This file must have the exact same name with a '.crs' extension. For example: 'my_ruleset.crs'.

Parameters (Config Parameter) | Table: CallAgentRuleset

Type	Text
Range	Size(0..512)
Default	
Script/CLI	Sbc.CallAgentRuleset[].Parameters
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.200.1.500

List of named parameters (parameter=value) for the Ruleset.
General format: parameter1=value1 parameter2=value2 parameter3=value3

Each parameter-value pair must be separated by a space.

The values can contain any character, with the following constraints:

- Values that contain space characters must be enclosed within double quotes.
- Within the values, double quotes and backslash characters must be escaped with a backslash.

The maximum length for a value is 100 characters.

Example: FirstValue=1 SecondValue = 192.168.0.1:5060 ThirdValue ='A more complex string'

ConfigStatus (Status Parameter) | Table: CallAgentRuleset

Type	Enum
Range	Valid(100) | UnknownRuleset(200) | InvalidConfig(300)
Script/CLI	Sbc.CallAgentRuleset[].ConfigStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.200.1.600

Configuration status of the Ruleset.
Indicates whether this Ruleset is valid and ready to be applied.

- Valid: The current content of the row is valid.
- UnknownRuleset: The ruleset file is not found.
- InvalidConfig: The configuration is not valid.

Delete (Row Command) | Table: CallAgentRuleset

Script/CLI:	Sbc.CallAgentRuleset[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.200.1.10000

Delete this entry from the table.

CallAgentRulesetCatalog (Table)

This table displays the call agent Rulesets installed on this device.

Id (Index) | Table: CallAgentRulesetCatalog

Type	UInt32
Range	
Script/CLI	Sbc.CallAgentRulesetCatalog[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.250.1.100

Unique identifier of the row in the table.

Name (Status Parameter) | Table: CallAgentRulesetCatalog

Type	Text
Range	Size(0..100)
Script/CLI	Sbc.CallAgentRulesetCatalog[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.250.1.200

Ruleset name.
The Ruleset name is based on the file name from which the extension '.crs' was removed.

Description (Status Parameter) | Table: CallAgentRulesetCatalog

Type	Text
Range	Size(0..512)
Script/CLI	Sbc.CallAgentRulesetCatalog[].Description
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.250.1.300

Description of the Ruleset.

Origin (Status Parameter) | Table: CallAgentRulesetCatalog

Type	Enum
Range	Factory(100) | Custom(200)
Script/CLI	Sbc.CallAgentRulesetCatalog[].Origin
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.250.1.400

Origin of the Ruleset.

- Factory: Read only Ruleset delivered with the application.
- Custom: User defined Ruleset.

A custom Ruleset has priority over a factory Ruleset. If a custom Ruleset is created with the same name as a factory Ruleset, it is the custom Ruleset that will be shown and used. Once the custom Ruleset is deleted, the factory Ruleset will be reactivated.

Cloning, editing and saving a factory Ruleset will create a custom Ruleset without modifying the factory Ruleset.

RoutingRules (Table: user-defined, 30 lines max.)

This table allows the user/administrator to configure the Routing Rulesets.
The changes to this table are applied when the `ApplyConfiguration` command is executed or when the service is restarted.

The changes to the ruleset files are applied when the `ApplyConfiguration` command is executed or when the service is restarted.

Note: Even if the **ConfigModifiedStatus** parameter does not indicate 'yes' after modifying the **RoutingRules** table, you must execute the `ApplyConfiguration` command.

Id (Index) | Table: RoutingRules

Type	UInt32
Range	
Script/CLI	Sbc.RoutingRules[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.300.1.100

Unique numerical identifier for this **RoutingRules** table entry.

Priority (Config Parameter) | Table: RoutingRules

Type	UInt32
Range	1..2147483647
Default	1
Script/CLI	Sbc.RoutingRules[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.300.1.200

Priority of execution of the Routing Rulesets.

Ruleset (Config Parameter) | Table: RoutingRules

Type	Text
Range	Size(0..48)
Default	
Script/CLI	Sbc.RoutingRules[].Ruleset
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.300.1.300

Name of the Routing Ruleset.
This name must have the exact same name with the same extension ('.rrs') as the name of the routing ruleset file located in the local storage of this device (see the File Service). For example: 'my_routing_ruleset.rrs'.

Parameters (Config Parameter) | Table: RoutingRules

Type	Text
Range	Size(0..512)
Default	
Script/CLI	Sbc.RoutingRules[].Parameters
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.300.1.400

List of parameters with their value (parameter=value) for the Routing Ruleset.
General format: parameter1=value1 parameter2=value2 parameter3=value3

Each parameter-value pair must be separated by a space.

The values can contain any character, with the following constraints:

- Values that contain space characters must be enclosed within double quotes.
- Within the values, double quotes and backslash characters must be escaped with a backslash.

The maximum length for a value is 100 characters.

Example: FirstValue=1 SecondValue = 192.168.0.1:5060 ThirdValue ='A more complex string'

ConfigStatus (Status Parameter) | Table: RoutingRules

Type	Enum
Range	Valid(100) | UnknownRuleset(200) | InvalidConfig(300)
Script/CLI	Sbc.RoutingRules[].ConfigStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.300.1.500

Configuration status of this routing entry.
Indicates whether the **RoutingRules** table entry is valid and ready to be applied.

- Valid: The current content of the row is valid.
- UnknownRuleset: The ruleset file is not found.
- InvalidConfig: The configuration is not valid.

Delete (Row Command) | Table: RoutingRules

Script/CLI:	Sbc.RoutingRules[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.300.1.10000

Delete this entry from the table.

RoutingRulesetCatalog (Table)

This table displays the routing Rulesets installed on this device.

Id (Index) | Table: RoutingRulesetCatalog

Type	UInt32
Range	
Script/CLI	Sbc.RoutingRulesetCatalog[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.350.1.100

Unique identifier of the row in the table.

Name (Status Parameter) | Table: RoutingRulesetCatalog

Type	Text
Range	Size(0..100)
Script/CLI	Sbc.RoutingRulesetCatalog[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.350.1.200

Ruleset name.
The Ruleset name is based on the file name from which the extension '.rrs' was removed.

Description (Status Parameter) | Table: RoutingRulesetCatalog

Type	Text
Range	Size(0..512)
Script/CLI	Sbc.RoutingRulesetCatalog[].Description
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.350.1.300

Description of the Ruleset.

Origin (Status Parameter) | Table: RoutingRulesetCatalog

Type	Enum
Range	Factory(100) | Custom(200)
Script/CLI	Sbc.RoutingRulesetCatalog[].Origin
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.350.1.400

Origin of the Ruleset.

- Factory: Read only Ruleset delivered with the application.
- Custom: User defined Ruleset.

A custom Ruleset has priority over a factory Ruleset. If a custom Ruleset is created with the same name as a factory Ruleset, it is the custom Ruleset that will be shown and used. Once the custom Ruleset is deleted, the factory Ruleset will be reactivated.

Cloning, editing and saving a factory Ruleset will create a custom Ruleset without modifying the factory Ruleset.

SignalingInterface (Table: user-defined, 25 lines max.)

This table allows the user/administrator to configure the Signaling Interfaces.
To apply the changes made to this table, the service must be restarted.

Id (Index) | Table: SignalingInterface

Type	UInt32
Range	
Script/CLI	Sbc.SignalingInterface[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.400.1.100

Unique numerical identifier for a Signaling Interface. The Signaling Interface ID is used by other parameters included in the Configuration Group to refer to this Signaling Interface.

Name (Config Parameter) | Table: SignalingInterface

Type	Text
Range	Size(0..100)
Default	
Script/CLI	Sbc.SignalingInterface[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.400.1.200

Signaling Interface name.
Alpha-numerics as well as '.', '-' and '_' are valid characters.

NetworkInterface (Config Parameter) | Table: SignalingInterface

Type	Text
Range	Size(0..50)
Default	
Script/CLI	Sbc.SignalingInterface[].NetworkInterface
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.400.1.300

The name of the BNI Network Interface this Signaling Interface is linked to.

Port (Config Parameter) | Table: SignalingInterface

Type	UInt32
Range	0..65535
Default	0
Script/CLI	Sbc.SignalingInterface[].Port
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.400.1.400

Signaling port number on which to receive and send requests. A value of '0' uses the default SIP port.

SecurePort (Config Parameter) | Table: SignalingInterface

Type	UInt32
Range	0..65535
Default	0
Script/CLI	Sbc.SignalingInterface[].SecurePort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.400.1.450

Signaling port number used to receive and send Secure SIP requests. A value of '0' uses the default Secure SIP port.

ForceLocalClientPort (Config Parameter) | Table: SignalingInterface

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Sbc.SignalingInterface[].ForceLocalClientPort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.400.1.460

Traditionally a TCP or TLS client connection uses a local ephemeral port (i.e. randomly chosen) to create a connection to a remote server.

When this parameter is enabled, the local client connection will not use an ephemeral port for this Signaling Interface, but will share the same port number as the local server port specified in the **Port** or **SecurePort** parameters.

This parameter has no effect for UDP, and for TLS when the **TlsMode** parameter is set to "server".

Note: When disabling this parameter, please stop the Sbc service for at least 60 seconds before starting it back. Otherwise the Sbc service may need to be restarted a second time, due to listening port number conflict.

TlsMode (Config Parameter) | Table: SignalingInterface

Type	Enum
Range	Both(100) | Client(200) | Server(300) | BothMutualAuth(400) | ServerMutualAuth(500)
Default	Client
Script/CLI	Sbc.SignalingInterface[].TlsMode
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.400.1.475

The TLS mode that this signaling interface uses.

- Both: Permits both client and server connections.
- Client: This Signaling Interface can only be used as a TLS client. If no host certificate is present on the unit only this mode is enabled
- Server: This Signaling Interface can only be used as a TLS server. This mode requires a valid host certificate on the unit.
- BothMutualAuth: Permits both client and server connections. Server connections require mutual authentication.
- ServerMutualAuth: This Signaling Interface can only be used as a TLS server and requires mutual authentication. This mode requires a valid host certificate on the unit.

Note: In mutual authentication mode, peer certificate validation is limited to verifying that the certificate is trusted and has not expired. If **CertificateValidation** is set to NoValidation, peer certificate validation is skipped and mutual authentication will not take effect, even when a mutual authentication mode is selected.

AllowedTransports (Config Parameter) | Table: SignalingInterface

Type	Enum
Range	All(100) | TlsOnly(200)
Default	All
Script/CLI	Sbc.SignalingInterface[].AllowedTransports
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.400.1.480

This parameter configures which transport protocols are allowed on the Sinaling Interface. The possible values are:

- All: The Signaling Interface has no restriction on the transport protocol. It supports all transport protocols supported by the SBC.
- TlsOnly: The Signaling Interface only supports TLS. Incoming SIP requests that are not in TLS are not directed to this Signaling Interface. Outgoing SIP requests are forced to TLS, even when the **ForceTransport** parameter is set to another transport protocol or when the Contact received when establishing a dialog specifies another transport protocol.

PublicIpAddr (Config Parameter) | Table: SignalingInterface

Type	IpHostName
Range	
Default	
Script/CLI	Sbc.SignalingInterface[].PublicIpAddr
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.400.1.500

Public IP address of this Signaling Interface.
Use this parameter when the interface is located on the 'private' side of a NAT and must be contacted from the 'public' side.

This parameter must be set to the public FQDN or public IP address of the NAT.

The NAT must be configured with port forwarding to the 'private' IP address of this Interface, e.g. as per the **NetworkInterface** parameter.

Note: A FQDN in this parameter will be used as-is, without being resolved.

TcpConnectTimeout (Config Parameter) | Table: SignalingInterface

Type	UInt32
Range	1..127000
Default	10000
Script/CLI	Sbc.SignalingInterface[].TcpConnectTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.400.1.600

TCP connection timeout, in milliseconds, for connections initiated by the SBC service.

TcpIdleTimeout (Config Parameter) | Table: SignalingInterface

Type	UInt32
Range	0..300000
Default	0
Script/CLI	Sbc.SignalingInterface[].TcpIdleTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.400.1.700

Idle timeout, in milliseconds, after which a TCP connection is closed. A value of '0' means there is no idle timeout.

DiffServ (Config Parameter) | Table: SignalingInterface

Type	UInt32
Range	0..255
Default	184
Script/CLI	Sbc.SignalingInterface[].DiffServ
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.400.1.750

In general, Differentiated Services (DiffServ) control the Quality of Service (QoS) tagging of IP network traffic. In this case it controls the tagging of IPv4 packets transmitted by this interface.
This 8-bit value is directly set in the TOS field (2nd byte) of the IPv4 header, allowing the use of either DiffServ or TOS mapping.

The RFC 4594 recommends a DSCP value of 46 for Telephony (VoIP), which means a DiffServ value of 184 (the default in DGW)

ConfigStatus (Status Parameter) | Table: SignalingInterface

Type	Enum
Range	Valid(100) | UnknownNetworkInterface(200) | PortConflict(300) | InvalidTlsMode(350) | InvalidTransportMode(380) | InvalidConfig(400)
Script/CLI	Sbc.SignalingInterface[].ConfigStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.400.1.800

Configuration status of this Signaling Interface.
Indicates if the Signaling Interface configuration is valid and ready to be applied.

- Valid: The current content of the row is valid.
- UnknownNetworkInterface: The **NetworkInterface** parameter is either empty or unknown.
- PortConflict: The selected port is in conflict with another usage.
- InvalidTlsMode: The selected port is in conflict with another usage.
- InvalidTransportMode: The Signaling Interface is configured to use only TLS transport and host validation is required by configuration but no CA certificate is present.
- InvalidConfig: The configuration of this Signaling Interface is invalid.

Delete (Row Command) | Table: SignalingInterface

Script/CLI:	Sbc.SignalingInterface[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.400.1.10000

Delete this entry from the table.

MediaInterface (Table: user-defined, 25 lines max.)

This table allows the user/administrator to configure the Media Interfaces.
To apply the changes made to this table, the service must be restarted.

Id (Index) | Table: MediaInterface

Type	UInt32
Range	
Script/CLI	Sbc.MediaInterface[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.500.1.100

Unique numerical identifier for a Media Interface. The Media Interface ID is used by other parameters included in the Configuration Group to refer to this Media Interface.

Name (Config Parameter) | Table: MediaInterface

Type	Text
Range	Size(0..100)
Default	
Script/CLI	Sbc.MediaInterface[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.500.1.200

Media Interface name.
Alpha-numerics as well as '.', '-' and '_' are valid characters.

NetworkInterface (Config Parameter) | Table: MediaInterface

Type	Text
Range	Size(0..50)
Default	
Script/CLI	Sbc.MediaInterface[].NetworkInterface
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.500.1.300

The name of the BNI Network Interface the Signaling Interface is linked to.

PortRange (Config Parameter) | Table: MediaInterface

Type	Text
Range	Size(0..20)
Default	
Script/CLI	Sbc.MediaInterface[].PortRange
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.500.1.400

Range of ports assigned to send and receive media traffic.

PublicIpAddr (Config Parameter) | Table: MediaInterface

Type	IpHostName
Range	
Default	
Script/CLI	Sbc.MediaInterface[].PublicIpAddr
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.500.1.500

Public IP address of this Media Interface.
Use this parameter when the interface is located on the 'private' side of a NAT and must be contacted from the 'public' side.

This parameter must be set to the public FQDN or public IP address of the NAT.

The NAT must be configured with port forwarding to the 'private' IP address of this Interface, e.g. as per the **NetworkInterface** parameter.

Note: A FQDN in this parameter will internally be resolved to an IP address before usage.

DiffServ (Config Parameter) | Table: MediaInterface

Type	UInt32
Range	0..255
Default	184
Script/CLI	Sbc.MediaInterface[].DiffServ
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.500.1.550

In general, Differentiated Services (DiffServ) control the Quality of Service (QoS) tagging of IP network traffic. In this case it controls the tagging of IPv4 packets transmitted by this interface.
This 8-bit value is directly set in the TOS field (2nd byte) of the IPv4 header, allowing the use of either DiffServ or TOS mapping.

The RFC 4594 recommends a DSCP value of 46 for Telephony (VoIP), which means a DiffServ value of 184 (the default in DGW)

ConfigStatus (Status Parameter) | Table: MediaInterface

Type	Enum
Range	Valid(100) | UnknownNetworkInterface(200) | PortConflict(300) | InvalidConfig(400)
Script/CLI	Sbc.MediaInterface[].ConfigStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.500.1.600

Configuration status of the row.
Indicates if this Media Interface is valid and ready to be applied.

- Valid: The current content of the row is valid.
- UnknownNetworkInterface: The **NetworkIterface** parameter is either empty or unknown.
- PortConflict: The selected port is in conflict with another usage.
- InvalidConfig: The configuration of this Media Interface is invalid.

Delete (Row Command) | Table: MediaInterface

Script/CLI:	Sbc.MediaInterface[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.500.1.10000

Delete this entry from the table.

RegistrationAgent (Table: user-defined, 50 lines max.)

This table allows the user/administrator to configure the Registration Agent.
The changes to this table take effect immediately.

Id (Index) | Table: RegistrationAgent

Type	UInt32
Range	
Script/CLI	Sbc.RegistrationAgent[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.600.1.100

Unique numerical identifier for this Registration Agent.

Username (Config Parameter) | Table: RegistrationAgent

Type	Text
Range	Size(0..100)
Default	
Script/CLI	Sbc.RegistrationAgent[].Username
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.600.1.200

User name in the Address of Record (AoR) of this registration entry.

Domain (Config Parameter) | Table: RegistrationAgent

Type	Text
Range	Size(0..100)
Default	
Script/CLI	Sbc.RegistrationAgent[].Domain
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.600.1.300

Domain in the Address of Record (AoR) of this registration entry.

FriendlyName (Config Parameter) | Table: RegistrationAgent

Type	Text
Range	Size(0..100)
Default	
Script/CLI	Sbc.RegistrationAgent[].FriendlyName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.600.1.400

Friendly name of this registration entry.

Contact (Config Parameter) | Table: RegistrationAgent

Type	Text
Range	Size(0..100)
Default	
Script/CLI	Sbc.RegistrationAgent[].Contact
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.600.1.500

SIP Contact to register.
This field accepts the syntax of standard expressions of the SIP contact header. Also it supports a Call Agent macro format %capubip(ca_name)% that is substituted by the actual address and port values of the Call Agent designated by ca_name. Note that the public address is used when the Signaling Interface associated with the Call Agent is configured with the public address. Otherwise, the network interface address of the Signaling Interface is used.

The macro can be used alone or within a contact expression:

- %capubip(ca_name)% - the macro is replaced by the IP address and port and prefixed by 'sip:'.
- sip:user@%CallAgentName%;uri-parameters?headers - the macro is replaced by the IP address and port within the contact expression.

Examples of using this macro:

- %capubip(wan_ip_trunk_ca)% --> sip:1.1.1.1:5060
- sip:user@%capubip(wan_ip_trunk_ca)% --> sip:user@1.1.1.1:5060
- sips:user@%capubip(wan_ip_trunk_ca)%;uri-parameters?headers --> sips:user@1.1.1.1:5060;uri-parameters?headers

Where 1.1.1.1:5060 are the IP address and port of the Signaling Interface associated with the wan_ip_trunk_ca Call Agent.

RegistrationType (Config Parameter) | Table: RegistrationAgent

Type	Enum
Range	Normal(100) | RFC6140(200)
Default	Normal
Script/CLI	Sbc.RegistrationAgent[].RegistrationType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.600.1.550

Selects the type of registrations made by this Registration Agent.

- Normal: Registrations made by this Registration Agent are regular registrations for single users.
- RFC6140: Registrations made by this Registration Agent are bulk registrations as defined in RFC 6140.

ExpireValue (Config Parameter) | Table: RegistrationAgent

Type	UInt32
Range	1..86400
Default	3600
Script/CLI	Sbc.RegistrationAgent[].ExpireValue
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.600.1.600

Registration expiration, in seconds.

RetryInterval (Config Parameter) | Table: RegistrationAgent

Type	UInt32
Range	1..86400
Default	600
Script/CLI	Sbc.RegistrationAgent[].RetryInterval
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.600.1.700

Interval, in seconds, to retry an unsuccessful registration.

ConfigStatus (Status Parameter) | Table: RegistrationAgent

Type	Enum
Range	Valid(100) | InvalidConfig(200)| InvalidContact(300)
Script/CLI	Sbc.RegistrationAgent[].ConfigStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.600.1.800

Configuration status of the Registration Agent.
Indicates if the Registration Agent entry is valid. A valid entry is applied immediately when entering it.

- Valid: The current content of the row is valid.
- InvalidConfig: The configuration is not valid.

- InvalidContact: The contact is not valid. Possible causes are:
  - The macro used as the contact refers to a Call Agent that is not active or non-existent.
  - The Registration Type is RFC 6140 and the contact has a user part.

Delete (Row Command) | Table: RegistrationAgent

Script/CLI:	Sbc.RegistrationAgent[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.600.1.10000

Delete this entry from the table.

PeerMonitoring (Table)

This table extends the **CallAgent** table with the configuration of the Blacklisting and the Peer Server Monitoring.

Blacklisting is the mechanism through which SIP server availability is managed. Unresponsive servers are put in a blacklist for a duration of **BlackListingDuration** and are not used during that time.

To complement Blacklisting, Peer Monitoring can be used to actively verify if servers are responsive. This allows detecting unresponsive servers before they are used. Peer Monitoring is done by sending SIP OPTIONs to the monitored servers.

A server can be blacklisted as a result of Peer Monitoring or in the course of normal SIP signaling.

During 'normal' SIP signaling, a server can be blacklisted on dialog-opening transactions or on out-of-dialog transactions. The in-dialog transactions that fail do not cause blacklisting.

Peer Monitoring is based on the value of **CallAgent.PeerHost**.

If the value of the **CallAgent.PeerHost** parameter is an IP address, then the Peer Monitoring is made on this address.

If the value of the **CallAgent.PeerHost** parameter is an FQDN, all the address:port values obtained from the DNS are monitored independently. The Call Agent is considered blacklisted only when all the address:port values obtained from the DNS are blacklisted.

Peer Monitoring is done using the transport protocol configured in the **CallAgent.ForceTransport** parameter. If this parameter is not configured, the default SIP transport (UDP) is used.

Peer Monitoring is performed independently of the rules defined in the Routing Rulesets.

The changes to this table are applied when the `ApplyConfiguration` command is executed or when the service is restarted.

Id (Index) | Table: PeerMonitoring

Type	UInt32
Range	
Script/CLI	Sbc.PeerMonitoring[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.700.1.100

ID of the **CallAgent** table entry used to configure the Peer Monitoring.

KeepAliveInterval (Config Parameter) | Table: PeerMonitoring

Type	UInt32
Range	0..3600
Default	0
Script/CLI	Sbc.PeerMonitoring[].KeepAliveInterval
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.700.1.200

Interval, in seconds, for sending Keep-Alive OPTIONS to monitor the Call Agent's peer.
Special value '0' means the Peer Monitoring feature is disabled.

BlackListingDuration (Config Parameter) | Table: PeerMonitoring

Type	UInt32
Range	0..86400
Default	0
Script/CLI	Sbc.PeerMonitoring[].BlackListingDuration
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.700.1.300

Duration, in seconds, that a peer host remains blacklisted when it appears to be down.
Special value '0' means a peer host is never blacklisted.

BlackListingDelay (Config Parameter) | Table: PeerMonitoring

Type	UInt32
Range	0..60000
Default	0
Script/CLI	Sbc.PeerMonitoring[].BlackListingDelay
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.700.1.400

Delay, in milliseconds, after which the peer is considered to be 'down' following expiration of the transaction timer.
A value of '0' means the peer host is blacklisted immediately after expiration of the transaction timer.

BlackListingErrorCodes (Config Parameter) | Table: PeerMonitoring

Type	Text
Range	Size(0..200)
Default	
Script/CLI	Sbc.PeerMonitoring[].BlackListingErrorCodes
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.700.1.500

Comma-separated list of SIP response codes indicating the peer is down.
After sending a monitoring request or any other message to the peer, if the Call Agent receives one of these response codes, the peer host is immediately blacklisted.

CustomHeader (Config Parameter) | Table: PeerMonitoring

Type	Text
Range	Size(0..500)
Default	
Script/CLI	Sbc.PeerMonitoring[].CustomHeader
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.700.1.600

Additional SIP header added in the OPTIONS request sent for monitoring purposes. The header string must respect the usual format: Header-Name: header-value.
Macros can be used to include information specific to the unit. The supported macros are:

- %mac% - the MAC address of the unit.
- %version% - the MFP version of the unit.
- %product% - the product name of the unit.
- %productseries% - the product series name of the unit.
- %profile% - the MFP profile of the unit.
- %serial% - the serial number of the unit.

ConfigModifiedStatus (Status Parameter)

Type	Enum
Range	Yes(100) | No(200)
Script/CLI	Sbc.ConfigModifiedStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.800

Indicates that some configuration changes need the `ApplyConfiguration` command to be executed in order to take effect or to be validated. Restarting the service will also apply these changes.

1. Yes: The configuration has been modified but has not been applied.
2. No: The configuration has not been modified.

Use the `ApplyConfiguration` command to apply the configuration.

HaStatus (Status Parameter)

Type	Enum
Range	Disabled(0) | Master(100) | Backup(200) | Unknown(300)
Script/CLI	Sbc.HaStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.10000.100

HA Status:

- Disabled: HA is disabled.
- Master: HA is in master mode.
- Backup: HA is in backup mode.
- Unknown: HA is in unknown mode.

HaNetworkInterface (Config Parameter)

Type	Text
Range	Size(0..255)
Default	
Script/CLI	Sbc.HaNetworkInterface
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.10000.200

When empty, the Sbc HA support is disabled.

The Ha service network interface used by the Sbc service to implement the Sbc HA feature. The interface name corresponds to an "Ha_" prefixed entry in the Ha.VrrpInstance table (e.g. "Ha_MyInstance")

When multiple instances within the Ha.VrrpInstance share the same group, another option containing all of them in sequence (e.g. "Ha_MyInst1,Ha_MyInst2") is provided such that the Sbc service can follow over the entire group, rather than a singular instance

NOTE: The Sbc service must be configured accordingly, no validation is performed.

HaLocalSyncNetworkInterface (Config Parameter)

Type	Text
Range	Size(0..50)
Default	
Script/CLI	Sbc.HaLocalSyncNetworkInterface
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.10000.300

The network interface used to synchronize with the peer call database.

HaPeerSyncIpAddr (Config Parameter)

Type	IpAddress
Range	
Default	
Script/CLI	Sbc.HaPeerSyncIpAddr
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.100.10000.400

The peer IP address to synchronize the call database with.

PrefixBasedRouting (Table: user-defined, 100 lines max.)

This table contains the prefix-based routing rules.
The changes to this table take effect immediately.

RuleId (Index) | Table: PrefixBasedRouting

Type	UInt32
Range	
Script/CLI	Sbc.PrefixBasedRouting[].RuleId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.150.100.1.100

Unique numerical identifier for this rule.

Prefix (Config Parameter) | Table: PrefixBasedRouting

Type	Text
Range	Size(0..50)
Default	
Script/CLI	Sbc.PrefixBasedRouting[].Prefix
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.150.100.1.200

Prefix to match in order to apply the rule.
A rule is selected using the longest-prefix-match algorithm.

DestinationCa (Config Parameter) | Table: PrefixBasedRouting

Type	UInt32
Range	
Default	0
Script/CLI	Sbc.PrefixBasedRouting[].DestinationCa
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.150.100.1.300

Id of a Call Agent in the **CallAgent** table. This Call Agent is used for sending the request.

RoutingMethod (Config Parameter) | Table: PrefixBasedRouting

Type	Enum
Range	NextHop(100) | OutboundProxy(200) | RequestUri(300)
Default	NextHop
Script/CLI	Sbc.PrefixBasedRouting[].RoutingMethod
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.150.100.1.400

Method used for routing.

- NextHop: This method allows sending the request directly to this next hop, without necessarily modifying the outbound message. The next hop is used for all requests within a given SIP dialog, thus ignoring data from the dialog state (remote URI, route set). If the target Call Agent is defined with a peer host, the next hop field default destination is the IP address or domain name and port of that host. Otherwise, it is mandatory to enter an override destination (domain name or IP address). When using the NextHop method, the **DestinationOveride** parameter supports multiple destinations by using a comma-separated list of destinations.
- OutboundProxy: This method adds a Route header field to the forwarded request, which will be considered for routing by the SIP transport layer. Similar to the NextHop method, the default destination is a URI built out of the IP address or domain name and port as defined by the Call Agent, if applicable.
- RequestUri: This method uses the Request URI (R-URI) to determine the next hop. Note that the target Call Agent set is still used to execute the outbound rulesets regardless of the host portion of the R-URI.

DestinationOverride (Config Parameter) | Table: PrefixBasedRouting

Type	Text
Range	Size(0..200)
Default	
Script/CLI	Sbc.PrefixBasedRouting[].DestinationOverride
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.150.100.1.500

String containing a coma-separated list of IP addresses or FQDNs to use as the next hop when the routing method is set to 'NextHop' or 'OutboundProxy'. This destination overrides the peer host that is configured in the target Call Agent. If the target Call Agent does not specify a peer host then using the destination override is mandatory.

RUriHandling (Config Parameter) | Table: PrefixBasedRouting

Type	Enum
Range	None(100) | Update(200) | Replace(300)
Default	None
Script/CLI	Sbc.PrefixBasedRouting[].RUriHandling
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.150.100.1.600

Indicates how to handle the host part of the Request URI.

- None: Leave the request URI unmodified.
- Update: Update the host part of the Request URI with the destination next hop or outbound proxy.
- Replace: Replace the Request URI by the (resolved) numeric IP address of the next hop.

ForceTransport (Config Parameter) | Table: PrefixBasedRouting

Type	Enum
Range	None(100) | TCP(200) | UDP(300) | TLS(400)
Default	None
Script/CLI	Sbc.PrefixBasedRouting[].ForceTransport
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.150.100.1.700

Force the use of a selected transport protocol when initiating SIP dialogs. Supersedes what is defined in the Call Agent.

- None: Transport is not forced. Will use UDP if the use of another transport protocol is not forced elsewhere.
- TCP: The outbound SIP signaling will be transported over TCP on the normal port.
- UDP: The outbound SIP signaling will be transported over UDP on the normal port.
- TLS: The outbound SIP signaling will be transported over TLS on the secure port.

Note: To force TLS and guarantee that no other transport protocol can be used, you must also set the **SignalingInterface.AllowedTransports** parameter to TlsOnly.

ConfigStatus (Status Parameter) | Table: PrefixBasedRouting

Type	Enum
Range	Valid(100) | InvalidCa(200) | NoPrefix(300) | InvalidDestination(400) | DestinationOverrideMandatory(500) | PrefixDuplicate(600) | InvalidConfig(700)
Script/CLI	Sbc.PrefixBasedRouting[].ConfigStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.150.100.1.1000

Configuration status of the row.
Indicates if the **PrefixBasedRouting** entry is valid and ready to be applied.

- Valid: The current content of the row is valid.
- InvalidCa: The Call Agent is not defined.
- NoPrefix: The prefix is not defined.
- InvalidDestination: The destination is not valid.
- DestinationOverrideMandatory: The destination override is missing.
- PrefixDuplicate: The prefix is already used by an other entry.
- InvalidConfig: The configuration is not valid.

Delete (Row Command) | Table: PrefixBasedRouting

Script/CLI:	Sbc.PrefixBasedRouting[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.150.100.1.10000

Delete this entry from the table.

StaticRegistration (Table: user-defined, 100 lines max.)

This table contains the Static Registration entries.
It is used by Rulesets to validate or to update, with the table's content, various fields of a SIP request.

The changes to this table take effect immediately.

RegistrationId (Index) | Table: StaticRegistration

Type	UInt32
Range	
Script/CLI	Sbc.StaticRegistration[].RegistrationId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.170.100.1.100

Unique numerical identifier for this registration entry.

Aor (Config Parameter) | Table: StaticRegistration

Type	Text
Range	Size(0..50)
Default	
Script/CLI	Sbc.StaticRegistration[].Aor
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.170.100.1.200

The address of record, in URI format, of this registration entry.
For example: sip:alice@example.com

This value must be unique within the table.

Contact (Config Parameter) | Table: StaticRegistration

Type	Text
Range	Size(0..50)
Default	
Script/CLI	Sbc.StaticRegistration[].Contact
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.170.100.1.300

The SIP contact, in URI format, used for this registration entry.
For example: sip:5551212@192.168.11.23:5060

ConfigStatus (Status Parameter) | Table: StaticRegistration

Type	Enum
Range	Valid(100) | AorDuplicate(200) |InvalidConfig(300)
Script/CLI	Sbc.StaticRegistration[].ConfigStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.170.100.1.1000

Configuration status of the row.
Indicates if the **StaticRegistration** entry is valid and ready to be applied.

- Valid: The current content of the row is valid.
- AorDuplicate: The Aor is identical to another one within the table.
- InvalidConfig: The configuration is not valid.

Delete (Row Command) | Table: StaticRegistration

Script/CLI:	Sbc.StaticRegistration[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.170.100.1.10000

Delete this entry from the table.

CallAgentStatus (Table)

This table displays the status and the active configuration of the Call Agents.

Id (Index) | Table: CallAgentStatus

Type	UInt32
Range	
Script/CLI	Sbc.CallAgentStatus[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.100.1.100

Unique numerical identifier for a Call Agent. The Call Agent ID is used by other parameters included in the Status Group to refer to a Call Agent.

Name (Status Parameter) | Table: CallAgentStatus

Type	Text
Range	Size(0..100)
Script/CLI	Sbc.CallAgentStatus[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.100.1.200

Call Agent name.
This name is displayed everywhere the Call Agent is used in the Management Interface.

SignalingInterface (Status Parameter) | Table: CallAgentStatus

Type	UInt32
Range	
Script/CLI	Sbc.CallAgentStatus[].SignalingInterface
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.100.1.300

ID of the Signaling Interface used by this Call Agent.

MediaInterface (Status Parameter) | Table: CallAgentStatus

Type	Text
Range	
Script/CLI	Sbc.CallAgentStatus[].MediaInterface
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.100.1.400

ID of the Media Interface used by this Call Agent.

Gateway (Status Parameter) | Table: CallAgentStatus

Type	Text
Range	Size(0..100)
Script/CLI	Sbc.CallAgentStatus[].Gateway
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.100.1.500

Name of the local gateway to be used by this Call Agent. When no local gateway is selected, the Call Agent will use an external peer.

PeerHost (Status Parameter) | Table: CallAgentStatus

Type	IpAddress
Range	
Script/CLI	Sbc.CallAgentStatus[].PeerHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.100.1.600

Resolved IP address of the peer.

State (Status Parameter) | Table: CallAgentStatus

Type	Enum
Range	Active(100) | NetworkDown(200)| InternalError(300) | PeerDown(400)
Script/CLI	Sbc.CallAgentStatus[].State
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.100.1.700

State of the call agent.

- Active: The Call Agent is active.
- NetworkDown: The Call Agent is inactive because the network is down.

SignalingInterfaceStatus (Table)

This table displays the active configuration of the Signaling Interfaces.

Id (Index) | Table: SignalingInterfaceStatus

Type	UInt32
Range	
Script/CLI	Sbc.SignalingInterfaceStatus[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.200.1.100

Unique numerical identifier for a Signaling Interface. The Signaling Interface ID is used by other parameters included in the Status Group to refer to this Signaling Interface.

Name (Status Parameter) | Table: SignalingInterfaceStatus

Type	Text
Range	Size(0..100)
Script/CLI	Sbc.SignalingInterfaceStatus[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.200.1.200

Signaling Interface name.
This name is displayed everywhere the Signaling Interface is used in the Management Interface.

NetworkInterface (Status Parameter) | Table: SignalingInterfaceStatus

Type	Text
Range	
Script/CLI	Sbc.SignalingInterfaceStatus[].NetworkInterface
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.200.1.300

The name of the BNI Network Interface on which this Signaling Interface is attached.

Port (Status Parameter) | Table: SignalingInterfaceStatus

Type	UInt32
Range	
Script/CLI	Sbc.SignalingInterfaceStatus[].Port
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.200.1.400

Signaling port number on which requests are sent and received.

SecurePort (Status Parameter) | Table: SignalingInterfaceStatus

Type	UInt32
Range	
Script/CLI	Sbc.SignalingInterfaceStatus[].SecurePort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.200.1.450

Signaling Secure Port number.

ForceLocalClientPort (Status Parameter) | Table: SignalingInterfaceStatus

Type	EnableDisable
Range	
Script/CLI	Sbc.SignalingInterfaceStatus[].ForceLocalClientPort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.200.1.460

ForceLocalClientPort value currently in use on this Signaling Interface.

TlsMode (Status Parameter) | Table: SignalingInterfaceStatus

Type	Enum
Range	Both(100) | Client(200) | Server(300) | BothMutualAuth(400) | ServerMutualAuth(500)
Script/CLI	Sbc.SignalingInterfaceStatus[].TlsMode
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.200.1.475

The TLS mode that this signaling interface uses.

AllowedTransports (Status Parameter) | Table: SignalingInterfaceStatus

Type	Enum
Range	All(100) | TlsOnly(200)
Script/CLI	Sbc.SignalingInterfaceStatus[].AllowedTransports
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.200.1.485

Transport protocols allowed on the Signaling Interface. The possible values are:

- All: The Signaling Interface has no restriction on the transport protocol. It supports all transport protocols supported by the SBC.
- TlsOnly: The Signaling Interface supports only TLS.

PublicIpAddr (Status Parameter) | Table: SignalingInterfaceStatus

Type	IpHostName
Range	
Script/CLI	Sbc.SignalingInterfaceStatus[].PublicIpAddr
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.200.1.500

Public FQDN or public IP address for near-end NAT traversal.

TcpConnectTimeout (Status Parameter) | Table: SignalingInterfaceStatus

Type	UInt32
Range	
Script/CLI	Sbc.SignalingInterfaceStatus[].TcpConnectTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.200.1.600

TCP connection timeout, in milliseconds, for connections initiated by the SBC.

TcpIdleTimeout (Status Parameter) | Table: SignalingInterfaceStatus

Type	UInt32
Range	
Script/CLI	Sbc.SignalingInterfaceStatus[].TcpIdleTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.200.1.700

Idle timeout, in milliseconds, after which a TCP connection is closed.
Special value '0' means there is no idle timeout.

DiffServ (Status Parameter) | Table: SignalingInterfaceStatus

Type	UInt32
Range	
Script/CLI	Sbc.SignalingInterfaceStatus[].DiffServ
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.200.1.750

DiffServ value currently in use on this Signaling Interface.

IpAddress (Status Parameter) | Table: SignalingInterfaceStatus

Type	IpAddress
Range	
Script/CLI	Sbc.SignalingInterfaceStatus[].IpAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.200.1.800

Current local IP address of this Signaling Interface.

State (Status Parameter) | Table: SignalingInterfaceStatus

Type	Enum
Range	Active(100) | NetworkDown(200) | NoIpAddress(300)
Script/CLI	Sbc.SignalingInterfaceStatus[].State
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.200.1.900

State

- Active: The Signaling Interface is active.
- NetworkDown: The Signaling Interface is inactive because the network is down.
- NoIpAddress: The Signaling Interface is inactive because it has no IP address.

MediaInterfaceStatus (Table)

This table displays the active configuration of the Media Interfaces.

Id (Index) | Table: MediaInterfaceStatus

Type	UInt32
Range	
Script/CLI	Sbc.MediaInterfaceStatus[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.300.1.100

Unique numerical identifier for a Media Interface. The Media Interface ID is used by other parameters in the Status Group to refer to this Media Interface.

Name (Status Parameter) | Table: MediaInterfaceStatus

Type	Text
Range	Size(0..100)
Script/CLI	Sbc.MediaInterfaceStatus[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.300.1.200

Media Interface name.
This name is displayed everywhere the Media Interface is used in the Management Interface.

NetworkInterface (Status Parameter) | Table: MediaInterfaceStatus

Type	Text
Range	
Script/CLI	Sbc.MediaInterfaceStatus[].NetworkInterface
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.300.1.300

The name of the BNI Network Interface the Signaling Interface is linked to.

PortRange (Status Parameter) | Table: MediaInterfaceStatus

Type	Text
Range	Size(0..20)
Script/CLI	Sbc.MediaInterfaceStatus[].PortRange
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.300.1.400

Range of ports assigned to send and receive media traffic.

PublicIpAddr (Status Parameter) | Table: MediaInterfaceStatus

Type	IpHostName
Range	
Script/CLI	Sbc.MediaInterfaceStatus[].PublicIpAddr
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.300.1.500

Public FQDN or public IP address for near-end NAT traversal.

DiffServ (Status Parameter) | Table: MediaInterfaceStatus

Type	UInt32
Range	
Script/CLI	Sbc.MediaInterfaceStatus[].DiffServ
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.300.1.550

DiffServ value currently in use on this Media Interface.

IpAddress (Status Parameter) | Table: MediaInterfaceStatus

Type	IpAddress
Range	
Script/CLI	Sbc.MediaInterfaceStatus[].IpAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.300.1.600

Current local IP address of this Media Interface.

State (Status Parameter) | Table: MediaInterfaceStatus

Type	Enum
Range	Active(100) | NetworkDown(200) | NoIpAddress(300)
Script/CLI	Sbc.MediaInterfaceStatus[].State
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.300.1.700

State

- Active: The Media Interface is active.
- NetworkDown: The Media Interface is inactive because the network is down.
- NoIpAddress: The Media Interface is inactive because it has no IP address.

CallAgentRulesetStatus (Table)

This table displays the association of Rulesets to Call Agents.

Id (Index) | Table: CallAgentRulesetStatus

Type	UInt32
Range	
Script/CLI	Sbc.CallAgentRulesetStatus[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.400.1.100

Unique numerical identifier for this Ruleset association.

CallAgent (Status Parameter) | Table: CallAgentRulesetStatus

Type	UInt32
Range	
Script/CLI	Sbc.CallAgentRulesetStatus[].CallAgent
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.400.1.200

ID of the **CallAgent** table entry to which this Ruleset is attached.

Priority (Status Parameter) | Table: CallAgentRulesetStatus

Type	UInt32
Range	
Script/CLI	Sbc.CallAgentRulesetStatus[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.400.1.300

Priority of execution of this Ruleset on that Call Agent.
Inbound rules of the Ruleset are executed in ascending priority order. Outbound rules are executed in descending priority order.

Ruleset (Status Parameter) | Table: CallAgentRulesetStatus

Type	Text
Range	Size(0..48)
Script/CLI	Sbc.CallAgentRulesetStatus[].Ruleset
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.400.1.400

Name of the Ruleset to which the Call Agent is attached.

Parameters (Status Parameter) | Table: CallAgentRulesetStatus

Type	Text
Range	Size(0..512)
Script/CLI	Sbc.CallAgentRulesetStatus[].Parameters
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.400.1.500

List of ruleset parameters and their value.

RoutingRulesStatus (Table)

This table contains the configuration of the routing rules.

Id (Index) | Table: RoutingRulesStatus

Type	UInt32
Range	
Script/CLI	Sbc.RoutingRulesStatus[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.500.1.100

Unique numerical identifier for this **RoutingRulesStatus** table entry.

Priority (Status Parameter) | Table: RoutingRulesStatus

Type	UInt32
Range	
Script/CLI	Sbc.RoutingRulesStatus[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.500.1.200

Priority of execution of the Routing Rulesets.

Ruleset (Status Parameter) | Table: RoutingRulesStatus

Type	Text
Range	Size(0..48)
Script/CLI	Sbc.RoutingRulesStatus[].Ruleset
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.500.1.300

Name of the routing ruleset.

Parameters (Status Parameter) | Table: RoutingRulesStatus

Type	Text
Range	Size(0..512)
Script/CLI	Sbc.RoutingRulesStatus[].Parameters
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.500.1.400

List of routing ruleset parameters and their value.

RegistrationAgentStatus (Table)

This table displays the state of the Registration Agent's Subscribers

Id (Index) | Table: RegistrationAgentStatus

Type	UInt32
Range	
Script/CLI	Sbc.RegistrationAgentStatus[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.600.1.100

Unique numerical identifier for a subscriber.

State (Status Parameter) | Table: RegistrationAgentStatus

Type	Enum
Range	Registering(200) | Registered(300) | Refreshing(400) | Unreachable(600) | Rejected(800) | InvalidResponse (1000) | NotFound (1100) | Unknown (1200)
Script/CLI	Sbc.RegistrationAgentStatus[].State
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.200.600.1.200

The current state of the registration.

- Registering: The registration is currently trying to register.
- Registered: The registration is successfully registered.
- Refreshing: The registration is trying to refresh.
- Unreachable: The last registration attempt failed because the registrar is unreachable.
- Rejected: The last registration attempt failed because the registrar rejected the registration.
- InvalidResponse: The received 200 OK response contact does not match the contact of the register. Or the 200 OK response for an un-register contains contact. This value is also used when the response doesn't match any other state.
- NotFound: The last registration attempt failed with SIP code 404. This can happen when the registrar does not find the user or if the Sbc service is not configured properly.
- Unknown: The state is not available. Please try again later.

NbActiveCalls (Status Parameter)

Type	UInt32
Range	
Script/CLI	Sbc.NbActiveCalls
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.300.100

Current number of active calls handled by the SBC service.

CallAgentStats (Table)

This table contains the statistics related to a Call Agent.
Statistics are collected as soon as the SBC service is started.

CallAgent (Index) | Table: CallAgentStats

Type	UInt32
Range	
Script/CLI	Sbc.CallAgentStats[].CallAgent
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.300.200.1.100

Id of the Call Agent associated with the statistics.

InboundCallAttempts (Status Parameter) | Table: CallAgentStats

Type	UInt32
Range	
Script/CLI	Sbc.CallAgentStats[].InboundCallAttempts
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.300.200.1.200

Number of inbound call attempts for this Call Agent.

OutboundCallAttempts (Status Parameter) | Table: CallAgentStats

Type	UInt32
Range	
Script/CLI	Sbc.CallAgentStats[].OutboundCallAttempts
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.300.200.1.300

Number of outbound call attempts for this Call Agent.

InboundCallCompleted (Status Parameter) | Table: CallAgentStats

Type	UInt32
Range	
Script/CLI	Sbc.CallAgentStats[].InboundCallCompleted
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.300.200.1.400

Number of completed inbound calls for this Call Agent.

OutboundCallCompleted (Status Parameter) | Table: CallAgentStats

Type	UInt32
Range	
Script/CLI	Sbc.CallAgentStats[].OutboundCallCompleted
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.300.200.1.500

Number of completed outbound calls for this Call Agent.

CertificateValidation (Config Parameter)

Type	Enum
Range	NoValidation(100) | HostName(200)
Default	HostName
Script/CLI	Sbc.CertificateValidation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.400.100

When establishing a TLS connection as a client, this parameter defines the level of security to use when validating the server's certificate.

- NoValidation: Allow a connection to the server without validating its certificate. This option provides partial security and should be selected with care. When used with mutual authentication modes in **SignalingInterface.TlsMode**, peer certificate validation will not take effect.
- HostName: Allow a connection to the server by validating if its certificate is trusted and valid. The validations performed on the certificate include the expiration date and indicate if the Subject Alternate Name (SAN) or Common Name (CN) matches the FQDN or IP address of the server.

TransportInteropMaxTlsVersion (Config Parameter)

Type	Enum
Range	TLSv1_2(400) | TLSv1_3(500)
Default	TLSv1_3
Script/CLI	Sbc.TransportInteropMaxTlsVersion
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.400.200

Sets the maximum version of TLS supported by the Sbc service.

"TLSv1_2" offers backward compatibility to SIP servers that do not support client requests with both TLS 1.2 and TLS 1.3 enabled.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Sbc.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.

- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Sbc.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4400.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

AddCallAgent (Command)

Insert a row in the **CallAgent** table.

Name (Argument) | Command: AddCallAgent

Type	Text
Range	Size(0..100)
Default	

Name of the Call Agent.
This name must be unique among all Call Agents.

Id (Argument) | Command: AddCallAgent

Type	UInt32
Range	0..2147483647
Default	0

Unique numerical identifier for a Call Agent.
The Call Agent ID is used by other entities to refer to a Call Agent.

The special value '0' (default value) generates an ID equal to the largest current ID value + 1.

AddCallAgentRuleset (Command)

Insert a row in the **CallAgentRuleset** association table.

Id (Argument) | Command: AddCallAgentRuleset

Type	UInt32
Range	0..2147483647
Default	0

Unique numerical identifier for this Ruleset association.
The special value '0' (default value) generates an ID equal to the largest current ID value + 1.

Ruleset (Argument) | Command: AddCallAgentRuleset

Type	Text
Range	Size(0..48)
Default	

Name of the Ruleset to attach to the Call Agent.
This name must match the name of a Call Agent ruleset file in the local storage of this device (see the File Service). This file must have the exact same name with the '.crs' extension. For example: 'my_ruleset.crs'.

CallAgent (Argument) | Command: AddCallAgentRuleset

Type	UInt32
Range	
Default	0

ID of the **CallAgent** table entry to attach this Ruleset to.

Priority (Argument) | Command: AddCallAgentRuleset

Type	UInt32
Range	0..2147483647
Default	0

Execution priority of this Ruleset for Call Agent.
When the special value '0' (default value) is used, the Sbc service generates a priority equal to the highest value of the existing priorities + 1.

AddMediaInterface (Command)

Add a Media Interface entry in the **MediaInterface** table.

Name (Argument) | Command: AddMediaInterface

Type	Text
Range	Size(0..100)
Default	

Name of the Media Interface.
This name must be unique among all Media Interfaces.

Id (Argument) | Command: AddMediaInterface

Type	UInt32
Range	0..2147483647
Default	0

Unique numerical identifier for a Media Interface.
The Media Interface ID is used by other parameters included in the **StatisticGroup** to refer to this Media Interface.

The special value '0' (default value) generates an ID equal to the largest current ID value + 1.

AddPrefixBasedRoutingRule (Command)

Insert a row in the **PrefixBasedRouting** table.

RuleId (Argument) | Command: AddPrefixBasedRoutingRule

Type	UInt32
Range	
Default	0

Unique numerical identifier for this rule.
The special value '0' (default value) generates an ID equal to the largest current ID value + 1.

AddRegistrationAgent (Command)

Insert a row in the **RegistrationAgent** table.

Id (Argument) | Command: AddRegistrationAgent

Type	UInt32
Range	0..2147483647
Default	0

Unique numerical identifier for this Registration Agent.

The special value '0' (default value) generates an ID equal to the largest current ID value + 1.

AddRouteRuleset (Command)

Insert a row in the **RoutingRules** table.

Id (Argument) | Command: AddRouteRuleset

Type	UInt32
Range	0..2147483647
Default	0

Unique numerical identifier for this Route table entry.
The special value '0' (default value) generates an ID equal to the largest current ID value + 1.

Ruleset (Argument) | Command: AddRouteRuleset

Type	Text
Range	Size(0..48)
Default	

Name of the Routing Ruleset.
This name must match the name of a routing ruleset file in the local storage of this device (see the File Service). This file must have the exact same name with the extension '.rrs'. For example: 'my_routing_ruleset.rrs'.

Priority (Argument) | Command: AddRouteRuleset

Type	UInt32
Range	0..2147483647
Default	0

Execution priority of this Ruleset.
When the special value '0' (default value) is used, the Sbc service generates a priority equal to the highest value of the existing priorities + 1.

AddSignalingInterface (Command)

Add a Signaling Interface entry in the **SignalingInterface** table.

Name (Argument) | Command: AddSignalingInterface

Type	Text
Range	Size(0..100)
Default	

Name of the Signaling Interface.
This name must be unique among all Signaling Interfaces.

Id (Argument) | Command: AddSignalingInterface

Type	UInt32
Range	0..2147483647
Default	0

Unique numerical identifier for a Signaling Interface.
The Signaling Interface ID is used by other parameters included in the **StatisticGroup** to refer to this Signaling Interface.

The special value '0' (default value) generates an ID equal to the largest current ID value + 1.

AddStaticRegistrationEntry (Command)

Insert a row in the **StaticRegistration** table.

RegistrationId (Argument) | Command: AddStaticRegistrationEntry

Type	UInt32
Range	
Default	0

Unique numerical identifier for this entry.

The special value '0' (default value) generates an ID equal to the largest current ID value + 1.

ApplyConfiguration (Command)

Apply any pending configuration changes.
The **ConfigModifiedStatus** parameter indicates whether or not some changes were made to the configuration but not yet applied.

Note that pending configuration changes are automatically applied when the Sbc service is restarted.

When editing the content of a ruleset, the changes made are immediately applied when the ruleset is saved. There is no pending state when editing Rulesets.

This command is ignored if the **NeedRestartInfo** indicates that the Sbc service requires a restart.

See also the `CancelEdits` command.

CancelEdits (Command)

Cancel any pending configuration changes.
See also the `ApplyConfiguration` command.

This command has no effect if the **ConfigModifiedStatus** parameter indicates there are no pending changes.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

RefreshRegistrationAgent (Command)

This command forces unregister and reregister of all Registration agent's registrations.

ResetRegistrationCache (Command)

Resets the Registration Cache.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Sbc service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	Port conflict detected on Media Interface %1$d ('%2$s').	Error	The **MediaInterface.PortRange** parameter refers to a port already in use.
20	Name duplication for Media Interface %1$d ('%2$s').	Error	The values of **MediaInterface.Name** must be unique in the **MediaInterface** table.
30	Media Interface at index %1$d has no name.	Error	A **MediaInterface** table entry must have its **Name** parameter configured.
40	The %1$s Network Interface used by the Media Interface %2$d ('%3$s') is not ready.	Warning	The Network Interface referred by the **MediaInterface.NetworkInterface** parameter is not ready. It may be either disconnected, its address may not be resolved or it can be unavailable for another reason. This can be a normal transient situation.
100	Port conflict detected on Signaling Interface %1$d ('%2$s').	Error	The **SignalingInterface.Port** parameter refers to a port already in use.
110	The name of the %1$s Signaling Interface is duplicated.	Error	The values of **SignalingInterface.Name** must be unique in the **SignalingInterface** table.
120	Signaling Interface at index %1$d has no name.	Error	A **SignalingInterface** table entry must have its **Name** parameter configured.
130	The %1$s Network Interface used by the Signaling Interface %2$d ('%3$s') is not ready.	Warning	The Network Interface is not ready. It may be either disconnected, its address may not be resolved or it can be unavailable for another reason. This can be a normal transient situation.
140	No Network Interface defined for the Signaling Interface %1$d ('%2$s').	Error	The **SignalingInterface.NetworkInterface** must be configured.
150	Signaling Interface at index %1$d is not in Client mode and no host certificate is available.	Error	For a Signaling Interface to operate in Server, ServerMutualAuth, Both or BothMutualAuth modes, a host certificate and a private key associated to the Sbc service in the Cert service are required.
180	Signaling Interface at index %1$d is TLS only and TLS is disabled.	Error	For a Signaling Interface to operate in TLS mode only, TLS needs to be enabled. TLS is disabled when the **CertificateValidation** parameter is enabled and no CA certificate is present.

NumKey	Message	Severity	Description
200	The Call Agent %1$d ('%2$s') refers to an undefined Media Interface %3$d.	Error	The **CallAgent.MediaInterface** parameter must refer to an existing Media Interface, unless the Call Agent is bound to a SipEp Gateway through the **CallAgent.Gateway** parameter.
205	The %1$s Call Agent has no Media Interface.	Error	When the **CallAgent.MediaInterface** parameter is empty, a Media Interface named loop_m needs to be configured in the Media Interface Configuration table.
210	The Call Agent %1$d ('%2$s') refers to an undefined Signaling Interface %3$d.	Error	The **CallAgent.SignalingInterface** parameter must refer to an existing Signaling Interface, unless the Call Agent is bound to a SipEp Gateway through the **CallAgent.Gateway** parameter.
230	No name defined for Call Agent %1$d.	Error	A **CallAgent** table entry must have its **Name** parameter configured.
240	The name of the %1$s Call Agent is duplicated.	Error	The values of **CallAgent.Name** must be unique in the **CallAgent** table.
270	Call Agent %1$d ('%2$s') has an ambiguous peer configuration.	Warning	The **CallAgent.PeerHost** and **CallAgent.PeerNetwork** parameters cannot be both configured. **PeerHost** has precedence over **PeerNetwork**
280	Peer FQDN or address configuration on the '%1$s'Call Agent is ignored.	Warning	The **CallAgent.PeerHost** and **CallAgent.PeerNetwork** parameters are ignored when the **CallAgent.Gateway** parameter is configured.
300	No peer defined for Call Agent %1$d ('%2$s').	Error	A peer must be defined for each Call Agent. The peer can be set through one of the following parameters: • **CallAgent.PeerHost** • **CallAgent.PeerNetwork** or • **CallAgent.Gateway**.

NumKey	Message	Severity	Description
410	The '%1$s' routing ruleset file is not found for the entry %2$d in the RoutingRules table.	Error	The ruleset file referred by the **RoutingRules.Ruleset** parameter is not found. The routing ruleset file must bear the same name as the ruleset with the extension '.rrs' and must be located in the File service under the 'sbc/rulesets' folder.
430	No Ruleset defined for CallAgentRuleset table entry %1$d.	Error	A **CallAgentRuleset** table entry must refer to a Ruleset.
440	Ruleset file '%1$s' not found for CallAgentRuleset table entry %2$d.	Error	The ruleset file referred by the **CallAgentRuleset.Ruleset** parameter is not found. The Call Agent ruleset file must bear the same name as the ruleset with the extension '.crs' and must be located in the File service under the 'sbc/rulesets' folder.
460	Call Agent Ruleset %1$d refers to an undefined Call Agent.	Error	The **CallAgentRuleset.CallAgent** parameter must refer to an existing Call Agent.
500	Internal error '%1$d'.	Critical	An internal error occurred. Check configuration. Restarting the unit may solve the issue.
510	Invalid interfaces configuration.	Error	A configuration issue in the **MediaInterface** or **SignalingInterface** tables prevents the SBC service to be fully started. Check interface configuration for correctness and port conflicts.
520	The Apply command was attempted on the configuration but failed.	Error	Check the configuration and the content of the ruleset files. Diagnostic traces may help to find the exact cause.
560	Invalid Configuration. No attempt to apply the configuration.	Error	The configuration validation failed. It cannot be applied.
570	The configuration was successfully loaded.	Info	This message is issued when the configuration is successfully loaded.
600	PrefixBasedRouting table entry %1$d refers to an undefined Call Agent.	Error	The **PrefixBasedRouting.DestinationCa** parameter must refer to an existing Call Agent.
610	Prefix '%1$s' is duplicated in the prefix-based routing table.	Error	The values of **PrefixBasedRouting.Prefix** must be unique in the **PrefixBasedRouting** table.

NumKey	Message	Severity	Description
630	The '%1$s' URI of the Static Registration AoR is duplicated.	Error	The values of **StaticRegistration.Aor** must be unique in the **StaticRegistration** table.
700	Call Start: call-id=%1$s, from=%2$s, to=%3$s ruri=%4$s, res=%5$s, src=%6$s:%7$s.	Info	This message is sent whenever a call has been established.
710	Call Attempt: call-id=%1$s, from=%2$s, to=%3$s ruri=%4$s, res=%5$s, src=%6$s:%7$s.	Info	This message is sent whenever a call failed or has been cancelled before getting established.

NumKey	Message	Severity	Description
720	Call End: call-id=%1$s, from=%2$s, to=%3$s ruri=%4$s, src=%5$s: %6$s, duration=%7$s, reason=%8$s.	Info	This message is sent whenever a call has been disconnected after being successfully established. Possible reasons: • reply: A SIP reply received in an inbound or outbound leg. • rtp-timer-terminated: RTP timeout. • session-timer-terminated: Session timeout. • no-ack: ACK not received. • caller-terminated: BYE from caller. • callee-terminated: BYE from callee. • admin-control-terminated: Call terminated from GUI. • call-length-terminated: Call length limit reached. • server-shutdown: Call terminated by the Sbc when terminating. • error: Internal error. • undefined: The reason is not available.
730	An error during session creation: source=%1$s: %2$s, ruri=%3$s, from=%4$s, to=%5$s, call-id=%6$s, reason=%7$s.	Error	This message indicates that a call failed due to a system error, often as result of an incorrect configuration. The administrator should fix the system configuration. For example, if a routing destination is incorrectly configured, an error such as 'routing failed: can't parse outbound proxy URI: 192.168.0.85' may appear.

NumKey	Message	Severity	Description
740	A limit is enforced: source=%1$s:%2$s, ruri=%3$s, from=%4$s, to=%5$s, call-id=%6$s, reason=%7$s.	Warning	This message is sent whenever a session is rejected because a limit is enforced. The Reason field describes the limit that has been enforced.
750	Drop request: source=%1$s:%2$s, ruri=%3$s, from=%4$s, to=%5$s, call-id=%6$s, reason=%7$s.	Info	This message is sent when the 'Drop request' action is executed.
770	Registration expired. aor=%1$s, to=%2$s, contact=%3$s, source=%4$s:%5$s, from-ua=%6$s.	Info	This message is sent when a register-cache or a registrar entry has expired due its UA-timer. This happens if a client does not re-register within the re-registration window enforced by the registrar or the SBC's registration cache. It may be a result of a transient client incapability to re-register. Please note that when register throttling is used with a remote registrar, the entry might still be valid from the point of view of the remote registrar. In this case, the AoR is still considered to be registered.
773	Registration record deleted from the registration cache. aor=%1$s, to=%2$s, contact=%3$s, source=%4$s:%5$s, from-ua=%6$s.	Info	This message is sent when a registration record was deleted from the registration cache. This happens when the SBC receives a register with an expiration value of 0 meaning that the sender wish to be unregistered.
776	The registration cache was cleared.	Info	This message is sent when the command to clear the registration cache was received by the SBC. The registration cache is emptied completely after this message
778	A new registration contact was added to the cache. aor=%1$s, to=%2$s, contact=%3$s, source=%4$s:%5$s.	Info	This message is sent when a new registration contact is created in the Sbc registration cache.

NumKey	Message	Severity	Description
780	Registration expired at the registrar. aor=%1$s, to=%2$s, contact=%3$s, source=%4$s:%5$s, from-ua=%6$s.	Info	This message is sent when registration throttling is in use and the client did not re-register within the re-registration window. When using registration throttling the SIP registrar window is typically longer than the client registration window and occurrence of this event usually indicates permanent incapability of a client to re-register.
790	Capture file: filename=%1$s, pcap-id=%2$s, from=%3$s, to=%4$s, call-id=%5$s.	Info	This message is sent when the 'Log received traffic' action is executed.
800	Alert. Reason=%1$s.	Error	This message is sent on an alert.
810	Sbc notification: source=%1$s:%2$s, reason=%3$s, ruri=%4$s, from=%5$s, to=%6$s, call-id=%7$s.	Info	This message is sent when various information concerning the connections are received (i.e. Tls connection was terminated).
820	A Tls connection to %1$s:%2$s was refused.	Error	This message is sent when a Tls connection with host failed because it is unreachable or not listening on the specified port.
830	A Tls connection to %1$s:%2$s failed because the received certificate is not trusted.	Error	This message is sent when a received certificate is not trusted. This could be because the certificate is malformed, the certificate authority is invalid or the certificate is expired.
840	A Tls connection to %1$s:%2$s failed for unspecified reason.	Error	This message is sent when a connection attempt failed for a reason different from the other notifications.
850	Tls connection to %1$s:%2$s was unexpectedly terminated.	Error	This message is sent when an ongoing Tls connection is unexpectedly stopped.
860	A Tls connection to %1$s:%2$s was successfully established.	Info	This message is sent when a connection attempt is successful and ready to be used.
870	Tls connection to %1$s:%2$s was gracefully terminated.	Info	This message is sent when a Tls is terminated successfully.
900	Call Agent %1$s is bound to non-existent SipEp gateway %2$s.	Warning	The **CallAgent.Gateway** parameter does not refer to an existing gateway in the **Gateway** table of the SipEp service.

NumKey	Message	Severity	Description
910	The '%1$s' Call Agent is bound to the '%2$s' SipEp gateway which is not configured for binding.	Warning	The **CallAgent.Gateway** parameter refers to a SipEp gateway that is not configured for SBC binding. See the **Gateway.SignalingInterface** parameter in the SipEp service for details.
920	The media networks of the '%1$s' Call Agent and the '%2$s' SipEp Gateway do not match.	Warning	When a binding exists between a Call Agent and a SipEp Gateway, the **Sbc.CallAgent.MediaInterface** and **SipEp.Gateway.MediaNetworks** parameters must refer to the same Network Interface. An empty **Sbc.callAgent.MediaInterface** parameter means the 'loop_m' Media Interface is used.
1020	The '%1$s' ruleset file cannot be open.	Error	Error trying to open the ruleset file. The ruleset files must be put in the 'sbc/rulesets' folder in the user storage.
1030	The '%1$s' Ruleset file has an invalid format.	Error	The ruleset file cannot be properly parsed. This could be caused by missing sections, unknown rule type, or other. Make sure the ruleset file is generated using the ruleset editor version that matches the application version.
1040	Missing ruleset filename.	Error	This message is sent when a ruleset filename is missing. Make sure that every Call Agent Ruleset has a name in the **CallAgentRuleset** table and every Routing Ruleset has a name in the **RoutingRules** table.
1050	No object to apply ruleset to. '%1$s' File,'%2$s' Ruleset,'%3$s' Object.	Error	The Ruleset refers to an undefined Call Agent. Make sure the Ruleset refers to valid entities. Also make sure that the required Call Agents are enabled. In some cases, this message can display the 'Object' as a 16-digit hexadecimal ID. This ID can be used to locate related diagnostic traces that may provide more information.
1060	Wrong usage of the '%1$s' ruleset.	Error	Trying to apply a Routing Ruleset as a Call Agent Ruleset, or the opposite. Make sure that Rulesets of the correct type are used. The Call Agent Rulesets have the '.crs' extension and the Routing Rulesets have the '.rrs' extension.

NumKey	Message	Severity	Description
1070	Unknown The '%1$s' Signaling Interface assigned to the '%2$s' Call Agent is unknown.	Error	An unknown Signaling Interface is assigned to the Call Agent. Make sure that the assigned Signaling Interfaces are valid.
1080	The '%1$s' Media Interface assigned to the '%2$s' Call Agent is unknown.	Error	An unknown Media Interface is assigned to the Call Agent. Make sure that the assigned Media Interfaces are valid.
1090	The '%1$s' action or condition used in the Ruleset is unknown.	Error	The Ruleset contains an unknown action or filter. Make sure the ruleset file is generated using the ruleset editor version that matches the application version.
1100	Error initializing the '%1$s' action or filter.	Error	The action or filter could not be initialized. Make sure the ruleset file is generated using the ruleset editor version that matches the application version.
1110	Missing value for the '%1$s' action/filter parameter.	Error	A value is missing for the identified action/filter parameter. Make sure the ruleset file is generated using the ruleset editor version that matches the application version.
1120	Invalid format for the '%1$s' action/filter parameter.	Error	The format is invalid for the identified action/filter parameter. Make sure the ruleset file is generated using the ruleset editor version that matches the application version.
1130	Unknown '%1$s' condition.	Error	The identified filter operation is unknown. Make sure the ruleset file is generated using the ruleset editor version that matches the application version.
1140	The '%1$s' Call Agent used in a Ruleset is unknown.	Error	This message is generated when a ruleset filter matches an unknown Call Agent. Check the Rulesets and make sure that the Rulesets refer to existing Call Agents. Also make sure that the required Call Agents are enabled. In some cases, this message can display the 'Call Agent' as a 16-digit hexadecimal ID. This ID can be used to locate related diagnostic traces that may provide more information.

NumKey	Message	Severity	Description
1150	The '%1$s' Call Agent used in a Ruleset is invalid.	Error	A Call Agent given as a filter argument is invalid. Make sure that the Call Agent configuration is valid and compatible with the use cases that it must support. Make sure the ruleset file is generated using the ruleset editor version that matches the application version. In some cases, this message can display the 'Call Agent' as a 16-digit hexadecimal ID. This ID can be used to locate related diagnostic traces that may provide more information.
1160	The '%1$s' right-hand-side operand found in a ruleset operation is unknown.	Error	This message is generated by operations with a limited set of right-hand-side operands. In the Rulesets, locate and verify the operations that use the operand shown in the message. Make sure the ruleset file is generated using the ruleset editor version that matches the application version.
1170	The '%1$s' right-hand-side operand found in a ruleset operation is invalid.	Error	This message is generated when a right-hand-side operand has an incorrect format. In the Rulesets, locate and fix the operations that use the operand shown in the message. Make sure the ruleset file is generated using the ruleset editor version that matches the application version.
1180	Error initializing Ruleset '%1$s' '%2$s'.	Error	Error while initializing a group of rules in a Ruleset. See the surrounding messages for more specific details. Make sure the ruleset file is generated using the ruleset editor version that matches the application version.
1190	Error initializing the Routing Ruleset.	Error	Error while initializing a rule in a Routing Ruleset. See the surrounding messages for more specific details. Make sure the ruleset file is generated using the ruleset editor version that matches the application version.

NumKey	Message	Severity	Description
1200	Error while initializing a rule in the '%1$s' Ruleset.	Error	Error while initializing a rule. See the surrounding messages for more specific details. Make sure the ruleset file is generated using the ruleset editor version that matches the application version.
1210	The '%1$s' next-hop is invalid.	Error	The format of a next-hop value is incorrect. Verify the next hop values in the Rulesets. Make sure the ruleset file is generated using the ruleset editor version that matches the application version.
1220	The '%1$s' routing method is invalid.	Error	The routing method shown in the message is invalid. Verify the routing methods in the ruleset files. Make sure the ruleset file is generated using the ruleset editor version that matches the application version.
1230	Missing destination Call Agent.	Error	The Call Agent attribute has not been set. Check the Rulesets and make sure that the destination Call Agent attributes are properly set.
1240	The destination of the '%1$s'Call Agent is non-existent.	Error	The Call Agent shown in the message was not found. Check the Rulesets and make sure that the Rulesets refer to existing call agents. Also make sure that the required call agents are enabled.
1250	The destination of the '%1$s' Call Agent is Invalid.	Error	This message is shown when the Call Agent definition does not allow proper routing in the current system configuration. For instance, when routing is configured as a next-hop but with no IP destination specified and the Call Agent peer is defined as a **PeerNetwork** instead of a **PeerHost**. Make sure the Call Agent configuration is compatible with the use cases that it must support.
1260	Licence activation parameters changed for the SBC service.	Warning	This message is sent when a new licence key has been activated on the device and the licence parameters have changed.

NumKey	Message	Severity	Description
1270	There is no adequately configured 'registration_ca' Call Agent.	Warning	The 'registration_ca' entry must be present, enabled and correctly configured in the **CallAgent** table. This Call Agent is required for proper operation of the SBC registrations. Its **SignalingInterface** parameter must be set to 'loop_s', its **MediaInterface** parameter must be set to 'loop_m' and its **PeerHost** parameter must be set to 127.0.0.1:5060.
1280	There is no adequately configured 'loop_s' Signaling Interface.	Warning	The 'loop_s' Signaling Interface is not found or is incorrectly configured. The 'loop_s' entry must be present and correctly configured in the **SignalingInterface** table for proper operation of the bindings between the Sbc and SipEp services. It must be configured on the Loop Network Interface on port 5060.
1290	802.1Q parameters changed for SBC service.	Warning	This message is sent when a 802.1Q parameter changes on the device. The SBC service needs to be restarted for the new parameters to take effect.
1300	An internal error has occurred. Please restart the SBC service.	Error	This message is sent when the SBC service takes too long to start. Sbc needs to be restarted to work properly.
1310	Invalid Call Agent Macro in registration agent, the '%1$s' Call Agent is not active or non-existent.	Error	The Call Agent shown in the message was not found. A **RegistrationAgent.Contact** parameter refers to a Call Agent that is either disabled or does not exist.
1320	Cannot use the network address of the '%1$s' Call Agent as a registration contact because the network is down.	Error	This message is sent when the Sbc service tries to use the network address of a Call Agent configured as a macro in a **RegistrationAgent.Contact** parameter and this network is down.
1330	%1$s	Info	This message is sent when a Ruleset issues an event using the 'Log Event' action.
1340	Force transport is set to TLS on the '%1$s' Call Agent and TLS is currently disabled.	Warning	This message is sent when a Call Agent force transport argument is set to TLS and TLS is disabled. This happens when there is no host certificate linked to the Sbc service.

NumKey	Message	Severity	Description
1350	Force transport is set to TLS on a Routing Ruleset and TLS is currently disabled.	Warning	This message is sent when the force transport argument of a Routing Ruleset is set to TLS and TLS is disabled. This happens when there is no host certificate linked to the Sbc service.
1360	The Sbc service has received too many events. The events queue will be truncated.	Warning	This message is sent when the Sbc service receives many events to log and the queue is full.
1370	The SIP transport was forced to TLS by the Signaling Interface when sending signaling to the %1$s:%2$s destination.	Warning	The **SignalingInterface.AllowedTransports** parameter is configured to TlsOnly and had to automatically change the transport protocol to TLS when requested to send a SIP message in a non-TLS transport protocol. This notification can appear in a few different situations: • The Contact, received in the SIP reply when establishing a dialog, specifies a transport different than TLS. Check if the peer can be configured to specify the correct transport in the Contact. • The transport protocol selected in a Routing Rule is not consistent with the configuration of **SignalingInterface.AllowedTransports**.
1380	Tls is disabled. Host Validation is required but there are no CA certificates.	Warning	This warning is sent when the **CertificateValidation** parameter is set to HostName but there are no CA certificates to verify the host name. Either set the parameter to NoValidation or add a CA certificate to the Cert service.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.

NumKey	Message	Severity	Description
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.

NumKey	Message	Severity	Description
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Sbc.

Message	Severity	Description
Cannot Cancel Edits.	Warning	The `CancelEdits` command cannot be performed because there is no active configuration that can be used to revert to.
The ApplyConfiguration command was refused because the service must be restarted.	Warning	When a change requires to restart the service (such as changes to the interface configuration), the `ApplyConfiguration` command is not allowed.
Invalid Configuration. Cannot apply.	Error	The configuration is not valid and cannot be applied. See the notification messages for details.
Invalid port range for Media Interface.	Error	The **MediaInterface.PortRange** parameter is invalid.
Invalid PeerHost.	Error	Check the definition and syntax of the **CallAgent.PeerHost** parameter.
Invalid PeerNetwork.	Error	Check the definition and syntax of the **CallAgent.PeerNetwork** parameter.
RoutingRules Ruleset parameters are invalid.	Error	The validation of the **RoutingRules.Parameters** parameter failed because of either the syntax, a duplicated parameter name or value check.
CallAgent Ruleset parameters are invalid.	Error	The validation of the **CallAgent.Parameters** parameter failed either because of syntax, duplicate parameter name or value check.
Call Agents do not support more than one Media Interface.	Error	The validation of the **CallAgent.MediaInterface** parameter failed because in the current firmware version, there is a maximum of one Media Interface per Call Agent.
CallAgent.ForceTransport parameter of the '%1$s' Call Agent is not compatible with the SignalingInterface.AllowedTransports parameter.	Error	The validation of the **CallAgent.ForceTransport** parameter failed because it is not compatible with the **SignalingInterface.AllowedTransports** parameter of its Signaling Interface.
Write Success.	Info	Configuration changes were applied successfully.

Message	Severity	Description
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.

Message	Severity	Description
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

SBC Conditions

This section describes the conditions that can be used in SBC's Call Agent or Routing Rules.

Name	Description	Operators
Source Call Agent	Checks the source Call Agent.	**==** , **!=**
Source IP	Checks the IP address the incoming request was sent from.	**==** , **!=** , **RegExp** , **does not match RegExp** , **begins with** , **does not begin with**
Source Port	Checks the port number the incoming request was sent from.	**==** , **!=** , **RegExp** , **does not match RegExp** , **begins with** , **does not begin with**
Inbound interface	Checks the local interface the incoming request was received from. Value is a Signaling Interface name.	**==** , **!=** , **RegExp** , **does not match RegExp** , **begins with** , **does not begin with**
R-URI	Checks the request URI.	**==** , **!=** , **RegExp** , **does not match RegExp** , **begins with** , **does not begin with**
R-URI user	Checks the user part of the request URI.	**==** , **!=** , **RegExp** , **does not match RegExp** , **begins with** , **does not begin with**

Name	Description	Operators
R-URI user parameter	Checks the parameter(s) in the username part of the request URI For example in the R-URI "sip:106;name=smith@domain.com", the parameter "name" can be checked for value "smith".	**==** , **!=** , **RegExp** , **does not match RegExp** , **begins with** , **does not begin with**
R-URI domain	Checks the host part of the request URI. The host part can contain a port number.	**==** , **!=** , **RegExp** , **does not match RegExp** , **begins with** , **does not begin with**
R-URI URI parameter	Checks the parameter(s) of the request URI.	**==** , **!=** , **RegExp** , **does not match RegExp** , **begins with** , **does not begin with**
From	Checks the 'From' header value.	**==** , **!=** , **RegExp** , **does not match RegExp** , **begins with** , **does not begin with**
From URI	Checks the value of the 'From' header URI.	**==** , **!=** , **RegExp** , **does not match RegExp** , **begins with** , **does not begin with**

Name	Description	Operators
From user	Checks the user part of the 'From' header URI.	**==** , **!=** , **RegExp** , **does not match RegExp** , **begins with** , **does not begin with**
From domain	Checks the host part of the 'From' header URI. The host part can contain a port number.	**==** , **!=** , **RegExp** , **does not match RegExp** , **begins with** , **does not begin with**
To	Checks the value of the 'To' header.	**==** , **!=** , **RegExp** , **does not match RegExp** , **begins with** , **does not begin with**
To URI	Checks the value of the 'To' header URI.	**==** , **!=** , **RegExp** , **does not match RegExp** , **begins with** , **does not begin with**
To user	Checks the user part of the 'To' header URI.	**==** , **!=** , **RegExp** , **does not match RegExp** , **begins with** , **does not begin with**

Name	Description	Operators
To domain	Checks the host part of the 'To' header URI. The host part can contain a port number.	**==** , **!=** , **RegExp** , **does not match RegExp** , **begins with** , **does not begin with**
Header	Checks the value of a given SIP header.	**==** , **!=** , **RegExp** , **does not match RegExp** , **begins with** , **does not begin with**
Codecs	Checks the presence/absence of specified codecs within de SDP payload. Codecs name must be specified according to IETF RTP payload types.	**Contain** , **Do not contain** , **Contain RegExp**
Media Types	Checks the presence/absence of a media type within the SDP. Right operand specifies the media type name (audio, video, image or text).	**Contain** , **Do not contain** , **Contain RegExp**
Call parameter	Checks the value of a call parameter using the selected operator. The call parameter must first be defined by the 'Set Call parameter' action. Any condition referring to an undefined value returns FALSE as result.	**==** , **!=** , **RegExp** , **does not match RegExp** , **begins with** , **does not begin with**
Call parameter existence	Tests if a call parameter exists or not. This is useful to accurately discriminate non-existing and empty values.	**Exists** , **Does not exist**
Method	Checks the SIP request method. The value is chosen from a list of allowed methods.	**==** , **!=**

Name	Description	Operators
Register cache	Checks the content of the registration cache.	**From URI (AoR + Contact + IP/port)** , **From URI (AoR + IP/port)** , **Contact URI (Contact + IP/port)** , **To URI (AoR)** , **R-URI (Alias)**
NAT	Checks if whether or not the sender is behind the NAT. Works only if the UA directly communicates with the SBC service.	**First Via Address**
Last Action Result	Returns true if the last action is completed successfully, false otherwise.	**==**
Blacklist	Checks if a Call Agent is on a blacklist (or not). A Call Agent is blacklisted when it is not reachable to make sure that no attempts to send traffic are done. If the value of the **CallAgent.PeerHost** parameter is an IP address without a port, this condition checks if the Call Agent is blacklisted on either standard SIP port (5060 and 5061). If either port is blacklisted, the Call Agent is considered blacklisted. See also **Sbc.PeerMonitoring**.	**Call Agent Blacklisted** , **Call Agent not Blacklisted**
Parallel Call Count	Tests if the number of parallel calls is below or above a threshold. The value refers to the number on ongoing calls that were evaluated by this rule, for a specific Call Agent. It does not refer to a global number of calls.	**Is below** , **Is equal or above**

SBC Operators

This section describes the operators that can be used with conditions in the SBC Call Agent or Routing Rules.

Name	Description
!=	The left operand does not equal the specified value.
==	The left operand equals the specified value.
Call Agent Blacklisted	The Call Agent specified with the right operand is blacklisted. If the value of the **CallAgent.PeerHost** parameter is an IP address without a port, this condition checks if the Call Agent is blacklisted on either standard SIP port (5060 and 5061). If either port is blacklisted, the Call Agent is considered blacklisted. See also **Sbc.PeerMonitoring**.
Call Agent not Blacklisted	The Call Agent specified with the right operand is not blacklisted.
Contact URI (Contact + IP/ port)	A user with specified 'Contact' URI is registered from specified IP:port.
Contain	The right operand is contained in.
Contain RegExp	Sample described by the right operand is contained in.
Do not contain	The right operand is not contained in.
Does not exist	The left operand does not exist within the specified string.
Exists	The left operand exists within the specified string.
First Via Address	Compares the SIP message source IP with the the first Via address.
From URI (AoR + Contact + IP/ port)	The user with matching 'From' URI and 'Contact' URI is registered from specified IP:port.
From URI (AoR + IP/port)	The user with matching 'From' URI is registered with any 'Contact' URI from specified IP:port.
Is below	The left operand is lower than the right operand.
Is equal or above	The left operand is higher or equal than the right operand.
R-URI (Alias)	The user with specified request URI is registered.
RegExp	The left operand matches the specified regular expression. The regular expression syntax is standard except that it supports the use of replacements. When a regular expression contains a '$' character that is not used to identify a replacement, then the '$' and backslash characters must be escaped with a backslash.
To URI (AoR)	The user with specified 'To' URI is registered.
begins with	The left operand starts with the specified string.
does not begin with	The left operand does not start with the specified string.

Name	Description
does not match RegExp	The left operand does not match the specified regular expression. The regular expression syntax is standard except that it supports the use of replacements. When a regular expression contains a '$' character that is not used to identify a replacement, then the '$' and backslash characters must be escaped with a backslash.

SBC Call Agent Rule Actions

SIP Mediation Actions

Manipulation of Identities, URIs, header fields and response codes.

Set RURI

Sets the request URI to a new value

Parameter	Description
new URI	The value of the new SIP request URI.

Prefix RURI user

Adds a prefix to the user part of the request URI.

Parameter	Description
prefix string	A value to insert as a prefix to the user part of the request URI.

Set RURI user

Replaces the user part of the request URI.

Parameter	Description
new userpart	Value of the new userpart to be used in the request URI field.

Append to RURI user

Adds a suffix to the user part of the request URI. Several suffixes can be added if the action is used several times.

Parameter	Description
suffix	Suffix to add to the request URI.

Strip RURI user

Removes the leading characters of the user part of the request URI.

Parameter	Description
number of leading characters	The number of leading characters to remove.

Set RURI host

Replaces the host part of the request URI.

Parameter	Description
new hostpart	The value of the new host part.

Set RURI parameter

Sets the request URI parameter.

Parameter	Description
parameter name	Parameter name
parameter value	Parameter value

Set From

Replaces the value of the 'From' header field.

Parameter	Description
From HF value	New value for the 'From' header field.

Set From display name

Replaces the display name part of the 'From' header field.

Parameter	Description
new From display name	New value for the display name.

Set From user

Replaces the user part of the 'From' URI.

Parameter	Description
new From userpart	New user part for the 'From' URI.

Set From host

Replaces the hostname of the 'From' URI.

Parameter	Description
new From hostname	New host name for the 'From' URI.

Set To

Replaces the 'To' header field value.

Parameter	Description
To HF value	The new value of the 'To' header field.

Set To display name

Replaces the display name part of the 'To' header field.

Parameter	Description
new To display name	The new value for the 'To' display name.

Set To user

Replaces the user part of 'To' URI.

Parameter	Description
new To userpart	The new user part of the 'To' URI.

Set To host

Replaces the host name of the 'To' URI.

Parameter	Description
new To hostname	The new host name of the 'To' URI.

Remove Header

Removes all occurrences of a specified Header from all requests and responses in a session. Headers added in subsequent rules are not removed by this action.

Note: Mandatory header fields (CallID, From, To, CSeq, Via, Route, Record-Route and Contact) are not removed by this action.

Parameter	Description
header field name	Name of the header to remove. This parameter is case-insensitive. Headers in compact name form must be removed separately.

Add Header

Adds a new header field to a request.

Parameter	Description
HF name	Header field name to add.
HF value	Value of the new header field.

Add Dialog contact parameter

Allows parameters to be added to the 'Contact' URI generated by the SBC on either side of the call.

Parameter	Description
Leg	Select inbound or outbound leg.
User part	If this option is enabled, the parameter will be added to the user part of the Contact-URI.
parameter name	Parameter name to add to the 'Contact' URI.
parameter value	Value of the new parameter.

Set Header whitelist

Removes all headers that are not specified in a list of headers. The headers are removed from all requests and responses in a session.
Headers are removed after all inbound and outbound rules have been processed.

Note: Mandatory header fields (CallID, From, To, CSeq, Via, Route, Record-Route and Contact) are not removed by this action.

Parameter	Description
comma-separated header-field name list	List of header field names. Names are comma-separated and case-insensitive. Names in compact form must be listed explicitly.

Set Header blacklist

Removes all occurrences of a list of headers from all requests and responses in a session.

Headers are removed after all inbound and outbound rules have been processed.

Note: Mandatory header fields (CallID, From, To, CSeq, Via, Route, Record-Route and Contact) are not removed by this action.

Parameter	Description
comma-separated header-field name list	List of header field names. Names are comma-separated and case-insensitive. Names in compact form must be listed explicitly.

Enable SIP Session timer callee-leg

Enforces the use of a session timer on the outbound leg.

Parameter	Description
session expiration(sec)	SIP session expiration value in seconds.
minimum expiration(sec)	The minimum value for the session interval, in units of delta-seconds. When used in an INVITE or UPDATE request, it indicates the smallest value of the session interval that can be used for that session. When present in a request or in a response, the session interval MUST NOT be less than 90 seconds.

Enable SIP Session timer caller-leg

Enforces the use of a session timer on the inbound leg.

Parameter	Description
session expiration(sec)	SIP session expiration value in seconds.
minimum expiration(sec)	The minimum value for the session interval, in units of delta-seconds. When used in an INVITE or UPDATE request, it indicates the smallest value of the session interval that can be used for that session. When present in a request or in a response, the session interval MUST NOT be less than 90 seconds.

Translate reply code

Translates a SIP reply code to another value and replaces the reason text.

Parameter	Description
matching reply code	SIP reply code to be replaced.
new reply code and reason phrase	New reply code and reason phrase.

Enable transparent dialog IDs

Enforces the use of the same dialog IDs on both legs of a call.

Parameter	Description
To-tag	Method of To-tag propagation.

Forward Via-HFs

Forces the SBC to keep the Via header fields when forwarding the request.

UAC auth

Responds to authentication requests using the specified credentials.

Parameter	Description
username	Authentication user name.
password	Authentication password.
towards	Towards caller or callee.

Diversion to history-info

Converts the SIP diversion header-field into the History-Info header-field by RFC 6044.

Call Transfer Handling

Defines the mode in which REFERs are handled: rejection, local processing, or forwarding.
Note: When this ruleset action is not used, the default REFER Processing Mode is 'REFER pass-through'.

Parameter	Description
mode	REFER Processing Mode. The choices available are 'REFER pass-through', 'Handle REFER internally' and 'Reject REFER'.
bye delay	Delay, in seconds, before issuing BYE to disconnect the original call leg. Applies only when the local processing mode is used.
remove allow refer	Remove the REFER method from the Allow header in requests and responses sent to the call agent's peer.

Refer-To URI translation

Translates the Refer-To URI of a REFER if it corresponds to an SBC generated Contact back into the original Contact.
This action must be executed at several places for the feature to work properly:

- All calls and requests that might send a REFER for which the translation is needed.
- Calls to which the Refer-To points to.

Set Contact Header parameter whitelist

Sets the whitelist of the Contact Header parameters.

Parameter	Description
comma-separated parameter name list	Comma-separated list of parameters to whitelist. Only the parameters defined in this list are relayed.

Set Contact Header parameter blacklist

Sets the blacklist of the Contact Header parameters.

Parameter	Description
comma-separated parameter name list	Comma-separated list of parameters to blacklist. Parameters defined in this list are not relayed.

Forward Contact Header parameters

Forwards the Contact Header parameters.

Set Content-Type whitelist

Keeps all message bodies whose content is in the whitelist Content-Type list; all other message bodies are removed. Multipart bodies are only removed when each single part inside has been removed. This field is case-insensitive.

Parameter	Description
comma-separated Content-Type names list	Specify the Content-Type names as comma-separated list, e.g. 'application/sdp,application/my-proprietary-ct'.

Set Content-Type blacklist

Removes all message bodies whose content is in the blacklist Content-Type list; all other message bodies are kept. Multipart bodies are only removed when each single part inside has been removed. This field is case-insensitive.

Parameter	Description
comma-separated Content-Type names list	Specify the Content-Type names as comma-separated list, e.g. 'application/sdp,application/my-proprietary-ct'.

Handle INVITE with Replaces header

Handle Replaces header in an incoming INVITE: incoming call is connected to an existing call leg.

SDP Mediation Actions

Manipulation of codec and early media negotiation.

Set CODEC whitelist

Removes all but listed codecs from the SDP payload.
If no media type is left in the SDP payload after applying the action, i.e. removing the non-listed codecs, the request is rejected with a 488 SIP response.

Parameter	Description
Value	Comma-separated list of codecs to be accepted in the SDP payload. Codec names are case-insensitive and must be specified according to IETF RTP payload types.

Set CODEC blacklist

Removes all listed codecs from the SDP payload.
If no media type is left in the SDP payload after applying the action, i.e. removing the listed codecs, the request is rejected with a 488 SIP response.

Parameter	Description
Value	Comma-separated list of codecs to remove from the SDP payload. Codec names are case-insensitive and must be specified according to IETF RTP payload types.

Set CODEC preferences

Promotes specified codecs in SDP negotiation.

Parameter	Description
inbound leg	Comma-separated list of codecs to promote in the SDP payload of the inbound leg. Codec names are case-insensitive and must be specified according to IETF RTP payload types.
outbound leg	Comma-separated list of codecs to promote in the SDP payload of the outbound leg. Codec names are case-insensitive and must be specified according to IETF RTP payload types.

Set Media whitelist

Removes all but listed media types from the SDP payload.
If no media type is left in the SDP payload after applying the action, i.e. removing the non-listed media types, the request is rejected with a 488 SIP response.

Parameter	Description
Value	Comma-separated list of media types (audio, video, image, text...) to be accepted in the SDP.

Set Media blacklist

Removes all listed media types from the SDP payload.
If no media type is left in the SDP payload after applying the action, i.e. removing the listed media types, the request is rejected with a 488 SIP response.

Parameter	Description
Value	Comma-separated list of media types (audio, video, image, text...) to be remove from the SDP.

Set SDP attributes whitelist

Sets the whitelist of SDP attributes.

Parameter	Description
comma-separated sdp attributes list	Comma-separated list of SDP attributes to whitelist. Only the parameters defined in this list are relayed. This whitelist has no effect on: • media direction attributes (sendrecv/sendonly/recvonly/inactive) • payload specific attributes (rtpmap/fmtp).

Set SDP attributes blacklist

Sets the blacklist of SDP attributes.

Parameter	Description
comma-separated sdp attributes list	Comma-separated list of SDP attributes to blacklist. Parameters defined in this list are not relayed. This blacklist has no effect on: • media direction attributes (sendrecv/sendonly/recvonly/inactive) • payload specific attributes (rtpmap/fmtp).

Drop early media

Drop RTP frames until the call is established.

Drop SDP from 1xx replies

Removes SDP payload from specific 1xx responses.

Parameter	Description
affected replies	Comma-separated list of SIP response codes.

Rectify SDP content

Rectify the content of relayed SDP payload.

Parameter	Description
Handle missing stream direction	Add explicitely the stream direction in relayed SDP payload. When disabled, the absence of stream direction may be considered as "a=sendrecv" by SIP peers. This is as RFC3264. When enabled, if the SDP answer to relay is positive, the absence of stream direction is detected and the relayed SDP will contain the matching stream direction: • The sent SDP offer contained "a=inactive", the relayed SDP answer will contain "a=inactive". • The sent SDP offer contained "a=sendrecv", the relayed SDP answer will contain "a=sendrecv". • The sent SDP offer contained "a=recvonly", the relayed SDP answer will contain "a=sendonly". • The sent SDP offer contained "a=sendonly", the relayed SDP answer will contain "a=recvonly".
Hold IP Connection Address	Rectify the Connection Address when its IP address is 0.0.0.0. The possibilities are: • No Action: The value of the Connection Address is not rectified. • Replaced by the RTP Anchoring IP: The advertised IP used to relay the media is used. This option requires having the "Enable RTP anchoring" action.

Management and Monitoring Actions

Logging packets and custom notifications.

Log received traffic

Logs SIP/RTP traffic into a capture file.
The capture file (in PCAP format) is stored in the 'sbc/logs' folder of the File service.

Note: The Log received traffic action can only be used in inbound rules.

Parameter	Description
Log type	Selects the type of packets to include in the capture file. • SIP only: Include SIP messages only. • SIP and RTP: Include SIP messages and RTP frames.
Show DNS queries	Show DNS queries in PCAP file
PCAP file name	Represents the name of the PCAP file. This name MUST be unique for each call. In order to link the PCAP file to a specific call, it is recommended to use the $ci-$ft expression as the PCAP file name. Using the expression creates a file name containing the SIP Call-ID and From-tag used to identify a unique call. When the PCAP file name parameter is empty, a unique file name is automatically generated. However, in this case, it is not possible to link the PCAP file to a specific call as the PCAP file name does not contain any Call ids.
Event attributes	Comma separated key=value attributes to be added in the 'message-log' event generated by this action

Log message

Generates a syslog message.

Parameter	Description
log level	Syslog severity level.
message text	Text of the syslog message.

Log event

Generates a notification.

Parameter	Description
event text	Message text of the notification event.

Traffic Shaping Actions

Sets a quota on SIP and RTP traffic and reports violations.

Limit parallel calls

Sets a quota on number of parallel calls.
The quota can be applied to a specific part of the traffic by using a key.

New calls arriving in excess of this limit are declined using the 403 SIP response.

The limit applies separately to inbound and outbound traffic respectively going through inbound and outbound rules, unless 'global key' is selected, in which case the limit will apply to both inbound and outbound traffic.

Parameter	Description
Parallel calls	Maximum number of parallel calls.
Key attribute	Optional key that identifies a subset traffic.
Is global key	• Checked: The limit applies to inbound and outbound traffic, on all Call Agents for which the key attribute matches. • Unchecked: The limit only applies to the traffic matching this rule and key attribute.
SIP Response code	The response code issued when calls are refused
SIP Response reason	The response reason in the response when calls are refused
SIP header	SIP header to add when call limit is reached. Ie: 'Warning: call limit reached'.
Soft limit	Generate a 'limit' event everytime the counter is greater than this value. Value of 0 disables the soft-limit.
Report abuse	Generate an abuse report for firewall blacklisting.

Limit CAPS

Sets a quota on number of call attempts within a certain time period.
The quota can be applied to a specific part of the traffic by using a key.

New calls arriving in excess of this limit are declined using the 403 SIP response.

The limit applies separately to inbound and outbound traffic respectively going through inbound and outbound rules, unless 'global key' is selected, in which case the limit will apply to both inbound and outbound traffic.

If a SIP call is challenged and a re-INVITE is sent with the same SIP alias, this is considered as being part of the same call and only increases CAPS by one.

Parameter	Description
Call Attemps per time unit	Maximum number of calls within the time period.
Time unit	Period of time (in seconds).
Key attribute	Optional key that identifies a subset traffic.
Is global key	• Checked: The limit applies to inbound and outbound traffic, on all Call Agents for which the key attribute matches. • Unchecked: The limit only applies to the traffic matching this rule and key attribute.
SIP Response code	SIP response code to use when the call limit is reached.
SIP Response reason	The response reason in the response when the call limit is reached.
SIP header	SIP header to add when call limit is reached. Ie: 'Warning: call limit reached'.
Soft limit	Generate a 'limit' event everytime the counter is greater than this value. Value of 0 disables the soft-limit.
Report abuse	Generate an abuse report for firewall blacklisting.

Limit Bandwidth

Sets a quota on RTP traffic bandwidth.
The quota can be applied to a specific part of the traffic by using a key.

New calls arriving in excess of this limit are declined using the 403 SIP response.

The limit applies separately to inbound and outbound traffic respectively going through inbound and outbound rules, unless 'global key' is selected, in which case the limit will apply to both inbound and outbound traffic.

Parameter	Description
Limit Bandwidth	The limit of bandwidth, in kbps, for the traffic matching this rule.
Key attribute	Optional key that identifies a subset traffic.
Is global key	• Checked: The limit applies to inbound and outbound traffic, on all Call Agents for which the key attribute matches. • Unchecked: The limit only applies to the traffic matching this rule and key attribute.
SIP Response code	The response code issued when calls are refused

Parameter	Description
SIP Response reason	The response reason in the response when calls are refused
SIP header	SIP header to add when the bandwidth limit is reached. Ie: 'Warning: bandwidth limit reached'.
Soft limit	Generate a 'limit' event everytime the counter is greater than this value. Value of 0 disables the soft-limit.
Report abuse	Generate an abuse report for firewall blacklisting.

Set call Timer

Disconnects a call if it exceeds a specified duration.

Parameter	Description
Call Timer	Set the maximum call duration, in seconds.

Media Processing Actions

Media Processing Actions.

Enable RTP Anchoring

Anchors RTP media to the SBC and centralises media forwarding. Additionally, ICE connectivity checks and RTP keep-alive can be introduced for anchored calls. If RTP timeout is introduced and no RTP packet appears, the call is disconnected.

Parameter	Description
Force symmetric media	When enabled, the SBC ignores the IP address advertised in the SDP payload and learns the IP address and UDP port number of the UA by observing RTP packets coming from the UA. It then starts sending the reverse RTP stream to that address.
Lock on addresses learned from RTP	When enabled, the SBC will not overwrite remote addresses learned fromRTP with addresses learned from signaling.
Enable intelligent relay (IR)	When enabled, the SBC detects that the caller and the callee are behind the same NAT and if so, bypasses the media relay. The test is done by comparing the source IP address of the incoming INVITE message with the intended destination of the request.
Source IP Header field for IR	When intelligent relay is enabled, this value configures a header field used to transport the information about the caller's network through additional proxies in the signaling path.
Offer ICE-lite	When enabled, the SBC adds the ICE-lite capabilities to the SDP offer.
Offer RTCP feedback	Adds additional RTCP capabilities for better QoS monitoring than the one available in traditional RTP implementations. When the option is enabled, the RTP profile is changed from AVP/SAVP to AVPF/SAVPF. When the option is disabled, the RTP profile is changed from AVPF/SAVPF to AVP/SAVP.
Offer RTCP Multiplexing	Multiplexing RTP and RTCP packets on a single port, negotiated as per RFC 5761. When enabled, offers sent will contain the "rtcp-mux" attribute in the SDP. Upon reception of an answer containing the "rtcp-mux" attribute, the RTCP packets will be relayed with the RTP packets through the same port. Regardless of the value of this option, whenever an offer is received with the "rtcp-mux" attribute, the answer sent will also contain the "rtcp-mux" attribute, and the RTCP packets will be relayed with the RTP packets through the same port.
Keepalive	When set to a time value, it allows the SBC to send keep-alive RTP traffic. This is useful if one side of a call detects and discontinues inactive calls whereas the other side suppresses RTP due to Voice Inactivity Detection or On Hold scenarios.
Keepalive method	Selects a format of RTP packets to be used as keep-alive RTP traffic.
Timeout	When set to a time value, allows the SBC to disconnect a call when no RTP traffic appears. This is useful to eliminate "hanging calls" due to abruptly disconnected SIP devices.

Parameter	Description
Change SSRC	When enabled, generates a new, non-zero, SSRC value for the RTP stream going towards the Call Agent peer. This option must be enabled on both inbound and outbound rules in order to convert the streams for both inbound and outbound calls.

SRTP Preferences

Configures SRTP Preferences.

Parameter	Description
Crypto Context Behavior	Specifies whether or not the cryptographic context, more specifically the rollover counter (ROC), must be reset after a SDP renegotiation. The ROC is an internal counter that tracks how many times the sequence number went over 65535. Both endpoints must have an identical behavior, else this will lead to decryption problems. The possible behaviors are: • ResetAlways: Reset the cryptographic context on every renegotiation, even if the crypto key has not changed. • ResetOnNewCrypto: Reset the cryptographic context when the negotiated crypto key has changed. • ResetNever: The cryptographic context is never reset after a renegotiation. The context is updated with the new crypto key and the ROC keeps its current value. Note: When the cryptographic context is reset, the sequence number, timestamp and SSRC of the stream are also reset to new randomized values. Note: In any case, the cryptographic context is automatically reset when the stream destination changes, regardless of the config of this parameter. Note: When this action is not used, the SBC default behavior is 'ResetNever'. Refer to the **Crypto Mode When Sending Offer** and **Crypto Mode When Sending Answer** parameters for more details how cryptographic attributes are negotiated.

Parameter	Description
Crypto Mode When Sending Answer	Specifies if the cryptographic attribute in the SDP answer with secured RTP (SRTP) streams should be regenerated or not. A cryptographic attribute includes the cryptographic suite, the key parameters, and the session parameters. The possible values are: • RegenerateAlways: Always regenerate new cryptographic attribute for the SDP answer to be sent, regardless of the content of the received SDP offer. • KeepUnlessCryptoChanged: Keep the same cryptographic attribute for the SDP answer to be sent, unless the matching cryptographic attribute of the received SDP offer changed. • KeepAlways: Keep the same cryptographic attribute for the SDP answer to be sent, regardless of the content of the received SDP offer When the sent or received cryptographic attribute change, the behavior of the associated cryptographic context can be adjusted according to the **Crypto Context On Change** parameter. This parameter is effective only when the **Key Exchange Mechanisms** is *SDES*. Note: When this action is not used, the SBC default behavior is 'KeepAlways'.

Parameter	Description
Crypto Mode When Sending Offer	Specifies if the cryptographic attribute in the SDP offer should be regenerated or not for a new SDP offer with secured RTP (SRTP) streams. A cryptographic attribute includes the cryptographic suite, the key parameters, and the session parameters. An SDP offer is sent during the following call scenarios: • Hold and Resume • Session timers (i.e. session expires) • Forking • Call Transfer • Conference call Of this list is excluded establisment or termination of a call. The possible values are: • RegenerateAlways: Always regenerate new cryptographic attribute for the SDP offer to be sent. • KeepUnlessMediaChanged: Keep the same cryptographic attribute for the SDP offer to be sent, unless the media stream state changed (e.g. a resume or call transfer situation). • KeepAlways: Keep the same cryptographic attribute for the SDP offer to be sent. When the sent or received cryptographic attribute changes, the behavior of the associated cryptographic context can be adjusted according to the **Crypto Context On Change** parameter. This parameter is effective only when the **Key Exchange Mechanisms** is *SDES*. Note: When this action is not used, the SBC default behavior is 'KeepAlways'.

Parameter	Description
SRTP lifetime	When selected, the lifetime is appended at the end of the cryptographic attribute.
Support AES_256_CM_HMAC_SHA1_80 Crypto Suite	When selected, the AES_256_CM_HMAC_SHA1_80 Crypto Suite is considered supported. Note: At least one suite must be selected to allow the communication to be established.
Support AES_CM_128_HMAC_SHA1_80 Crypto Suite	When selected, the AES_CM_128_HMAC_SHA1_80 Crypto Suite is considered supported. Note: At least one suite must be selected to allow the communication to be established.
Support AES_CM_128_HMAC_SHA1_32 Crypto Suite	When selected, the AES_CM_128_HMAC_SHA1_32 Crypto Suite is considered supported. Note: At least one suite must be selected to allow the communication to be established.

Force RTP/SRTP

Forces the media traffic to use secure or non-secure RTP.

RTP anchoring must be enabled in an inbound or an outbound rule otherwise this action is ignored.

The affected call leg depends on which rule the action is applied:

- on an inbound rule: the caller leg
- on an outbound rule: the callee leg

Offers sent by the SBC on the affected leg use forced transport.

Notes:

- Best effort SRTP from the call offeror is unsupported.
- A non-conforming offer received on the forced leg will be rejected with a 488.

Parameter	Description
Force plain RTP	When selected, forces/converts the side of the call it is used on to RTP. Selecting it disables "Force secure RTP".
Force secure RTP	When selected, forces/converts the side of the call it is used on to SRTP. Selecting it disables "Force plain RTP".
Key Exchange Mechanisms	Only usable when "Force secure RTP" is activated. Offers DTLS, SDES, or both, to secure the key exchange mechanism.
Filter forced transports	When selected, and when the same media type is offered both with and without the forced transport, the media lines not matching the forced transport are removed. In the answer sent back to the peer that made the offer, the removed lines are re-inserted but marked as rejected (port set to 0). Use this when the other side cannot handle two media streams of the same type.

DTMF conversion from INFO to avt

Convert DTMF from SIP INFO request into RTP AVT format according to RFC 2833.
This action is sensitive to the place where it is used:

- As an inbound rule on the caller side, it converts the DTMF sent by the caller.
- As an outbound rule on the callee side, it converts the DTMF sent by the callee.
- As an inbound rule on the callee side, or as an outbound rule on the caller side, it has no effect.

Example: Call Agent A handles peers that use SIP INFO, and Call Agent B handles peers that use RTP AVT. We want DTMF converted between Call Agents A and B in both directions. The following configuration works:

- Action dtmf_info2avt must be used as inbound and outbound rules on Call Agent A.
- Action dtmf_avt2info must be used as inbound and outbound rules on Call Agent B.

DTMF conversion from avt to INFO

Convert DTMF from RTP AVT format (RFC 2833) into SIP INFO request.
This action is sensitive to the place where it is used:

- As an inbound rule on the caller side, it converts the DTMF sent by the caller.
- As an outbound rule on the callee side, it converts the DTMF sent by the callee.

- As an inbound rule on the callee side, or as an outbound rule on the caller side, it has no effect.

Example: Call Agent A handles peers that use SIP INFO, and Call Agent B handles peers that use RTP AVT. We want DTMF converted between Call Agents A and B in both directions. The following configuration works:

- Action dtmf_info2avt must be used as inbound and outbound rules on Call Agent A.
- Action dtmf_avt2info must be used as inbound and outbound rules on Call Agent B.

SIP dropping Actions

Eliminating non-compliant traffic, either silently or with a SIP response.

Reply to request with reason and code

Sends a response to a SIP request.
When this action is executed, subsequent actions and rules are not executed.

Parameter	Description
Code	SIP error code
Reason phrase	Reason text Replacement expressions can be part of this value.
Optional header field	Header fields to include in the response message. Replacement expressions can be part of this value. Multiple headers can be added by inserting '\r\n' between them.

Allow unsolicited NOTIFYs

Allows forwarding NOTIFY requests without a prior subscription (either implicit with REFER, or explicit with SUBSCRIBE).

Drop request

Drops requests silently.
When this action is executed, subsequent actions and rules are not executed.

Parameter	Description
Event throttling key	A replacement expression. When a request is dropped, an event is generated for each different value of the replacement expression. For example: If the event throttling key is set to '$si', an event will be generated once for each different source IP address of the dropped request. When empty, an event is generated for each dropped request. When the key contains a constant string, an event is generated at most once every 10 seconds.
Blacklist by firewall if repeated	Include this action when considering blacklisting IP address in firewall.
Drop reason text	Drop reason text.

Scripting Actions

Processing of internal parameters that are used to link multiple actions together using intermediate results stored in parameters.

Set Call parameter

Stores a computing result in an parameter. The parameter can be tested using the 'Call parameter' condition and/or referred to from actions using the '$V(gui.varname)' replacement.

Parameter	Description
parameter name	Name of the parameter to set.
parameter value	Value of the parameter.Replacement expressions can be part of this value.

Registration Processing Actions

REGISTER caching, storing and throttling.

Enable REGISTER caching

Generates an alias for the contact URI of a REGISTER request and forwards the request with the alias instead of the original contact.
Upon successful answer to the request, the alias is stored together with the original contact and AOR in the registration cache.

Parameter	Description
Cookie method	Determines where the alias is located in the Contact header field. • User part: The contact is generated in the "<sip:[alias]@[SBC IP and port]>." form • reg_alias URI parameter: The contact is generated in the "<sip:[SBC IP and port];reg_alias=[alias]>" form. • Username (no alias): The contact username is used directly as the "cookie", and is not replaced by an "alias". This method has the limitation of not supporting multiple registrations per user. Only the last registration is saved in the cache for any given user. This method should only be used when the server replies without an alias in the SIP REGISTER responses.
With temporary aliases	This option will create temporary aliases when the REGISTER request is relayed so that requests sent by the registrar shortly after the REG/200 can be relayed to the registrering UA even if this request is processed before the 200/REG.

Retarget R-URI from cache

Lookup the registration cache to find an entry with an alias matching the user-part of the request's R-URI.
If a matching entry is found, the R-URI of the request is re-written with the original contact from the registration cache.

If no entry is found, the request is not modified and is processed with the next applicable rules.

Note that entries with aliases are saved in the registration cache when using 'Enable REGISTER caching'.

Parameter	Description
enable NAT handling	When enabled, the SBC sends subsequent SIP messages to the source IP and port of the REGISTERS request it received.
enable sticky transport	When enabled, the SBC uses the same interface and transport over which the REGISTER was received for sending subsequent SIP messages.

REGISTER throttling

Forces SIP user-agents to shorten the re-registration period while propagating the REGISTERs upstream to the registrar, at longer intervals.
Particularly useful to trigger REGISTER-based keep-alives to facilitate NAT traversal.

This action requires the use of "enable REGISTER caching" or "save REGISTER contact" actions and must precede any REGISTER processing action in order to take effect.

This action is executed immediately when the rule is evaluated. The reply is sent immediately.

The order of the rules is important. The rules and the actions are executed in the order in which they appear.

Registration requests are forwarded for UAS re-registration when the binding expires at the UAS or when the source IP/Port has changed.

Parameter	Description
minimum registrar expiration	Sets the minimum interval between registrations of the SBC unit to the registrar. This value is assigned to the **expires** parameter in the REGISTER sent to the registrar when the **expires** parameter in the REGISTER received from the user-agent is smaller or when the parameter is absent.
maximum UA expiration	Sets the maximum interval between registrations of the registering user to the SBC unit. This value is assigned to the **expires** parameter in the response sent to the user-agent when the **expires** parameter in the REGISTER received from the user-agent is larger or when the parameter is absent. This value must be smaller than the registrar expiration or at least twice as big.

Save REGISTER contact

Acts as a local registrar and stores the AOR and contact in the registration cache.
This contact overwrites any previously saved contact.

The REGISTER request is answered with a 200 OK and no further processing is done on that request.

Restore contact from registrar

Lookup the registration cache to find an entry with an AOR matching the request's request URI.
If a matching entry is found, the request URI of the request is re-written with the original contact from the registration cache.

If no entry is found, the request is not modified and is processed with the next applicable rules.

Note that this action will restore contacts that were saved using 'Save REGISTER contact' or 'Enable REGISTER caching'.

Fetch home-proxy IP

This action retrieves the routing information used for user registration and routes later requests to the user's 'home proxy', without re-targeting DNS lookup. This is useful in IMS use-cases when the user's signaling must be routed through the proxy previously used for registration.
This action sets an internal 'next-hop' value available for a routing rule that uses the 'next hop' routing method. This internal 'next-hop' value is set to the IP address, port and outbound interface to reach the proxy where the user was previously registered.

Please note that for this action to work, the 'source-alias' call parameter must be set. This can be done by a previous Register Cache condition targeting the caller (e.g. Register Cache / From URI (AoR +Contact+IP/port) / 'Is Registered').

External Interaction Actions

Queries to external servers by REST or ENUM.

ENUM query

Query an ENUM server and replaces the R-URI with the result of the query. If no source is entered, the R-URI user is used. The default domain suffix can also be overridden to query private ENUM servers or non E164 numbers.

Parameter	Description
queried value	Field to be queried by the Enum query.
domain suffix	DNS suffix used for the Enum query (ex: e164.arpa).
ENUM services	Semi-colon separated list of ENUM services (ex: sip;voice:sip;video:sip).

Read call parameters over REST

Do REST query to given URL and set call variables received in reply. Typically input to the query is specified as URI parameters that include substitution variables.

Parameter	Description
REST URL	REST server URL

NAT Handling Actions

Facilitates NAT traversal.

Enable dialog NAT handling

Remembers during the dialog duration where the initial dialog initiating request came from and sends all subsequent traffic to that IP address and port.

Disable rport field on outbound Via header

Removes the Via header field ";rport" on outbound requests (RFC 3581).
By default, ";rport" is added by the SBC so that the upstream peer returns responses to the source port the request was sent from. Use this rule when forwarding to peers that mishandle or reject Via headers containing the ";rport" field.

Other Actions

Miscellaneous Call Agent actions.

Fork

Duplicates a SIP request. When forking is used, extra sessions are required for the additional call legs involved. Make sure your licences support enough sessions.

Parameter	Description
New R-URI	Requests the URI of the new request.

Add Q.850 Reason Header

Add a Reason header with the Q.850 call termination reason, if no Reason header is present.

Parameter	Description
on inbound leg	Add the header on the inbound call leg.
on outbound leg	Add the header on the outbound call leg.

Reset dialog by 1xx replies

Allow early dialog to be reset when a downstream serial-forking proxy forwards a call to another destination without 181 reply and previous 1xx replies were not important (without SDP, not reliable).

SBC Routing Rule Actions

Routing Actions

Static and dynamic SIP request routing.

Prefix-based routing

This is frequently used when you have a number of PSTN gateways serving different regions. Technically you match area codes with the beginning of the user-part of the request URI.

Parameter	Description
Match	This parameter specifies an expression on which the prefix matching is done. This expression can be made of Replacement expressions, call parameters, backreferences to a regular expression evaluated in the rule condition, ... For instance, setting this parameter to $rU causes the match to be checked against the user part of the request URI. The prefix matching searches for the corresponding entry in the **PrefixBasedRouting** table. Then the routing is done according to the parameters in the matching entry in the **PrefixBasedRouting** table.
Update To-URI host	Update To-URI host
Replace To-URI host with the resolved destination IP address	Replace To-URI host with the resolved destination IP address

Static route

The Static Route is the simplest type of routing where the administrator explicitly chooses the destination Call Agent.
The next SIP hop is determined by either using the request URI or by directly using an IP address.

Whichever method is chosen, the Rulesets of the specified destination Call Agent are executed.

If the next hop yields multiple IP addresses (e.g. when using an FQDN), the SBC load-balances among them by their respective priorities.

Parameter	Description
Call Agent	The Call Agent to which the request will be forwarded.
Route via R-URI	The 'Route via R-URI' method uses the request URI to find out the next-hop IP address. That is particularly useful when Call Agent rules alter the request URI using actions like reverse registration cache or ENUM lookup. If the host part of the request URI includes a DNS name that resolves to multiple destinations per RFC 3263, the SBC load-balances among the respective destinations according to their priorities.
Set Next Hop	Uses the destination Call Agent's peer IP address(es) as the next-hop IP address. Optional sub-parameters: • Use another destination instead of Call Agent's destination(s): Overrides the CA's peer IP address by the provided IP address. • Use on first request only: This option changes the default behaviour for forwarding subsequent in-dialog requests. By default when turned off, all subsequent outbound requests will follow the path of the dialog-initiating request. However, if this option is turned on, the next-hop logic for subsequent requests is governed only by the SIP standard procedures. Particularly, if the next hop in the INVITE path was a non-record-routing proxy, it will not be included in the request path. • Update R-URI host: This option rewrites the host part of the request URI with the address of the next hop. By default it is turned off and the request URI is not modified when forwarded. • Add Route header field: This option is also known as "preloaded Route". It prints the next-hop destination in the Route header field. Use only if next SIP hop is known to require such a behaviour.

Parameter	Description
Replaces the DNS name in the request URI with the resolved IP address.	If a DNS name appears in the request URI, it is substituted by its resolved IP address before forwarding.
Update To-URI host	Update To-URI host
Replace To-URI host with the resolved destination IP address.	Replace To-URI host with the resolved destination IP address.
Force transport	Overrides the transport protocol to be used to initiate SIP dialogs with the next hop. The following protocols are supported: UDP, TCP, TLS and Websockets. Note: To force TLS and guarantee that no other transport protocol can be used, you must also set the **SignalingInterface.AllowedTransports** parameter to TlsOnly.
Enable redirect handing	If this option is enabled, incoming 302 SIP responses are not passed upstream. Instead, the SBC takes the content of the 'Contact' header field and uses it as another next-hop for forwarding the original request. Specifically, the contact URI in the 302 SIP response is used to rewrite the request URI, determine the next-hop IP address and looks up a Call Agent whose outbound rules are processed.

Call Agent based on R-URI

The SBC tries to find a Call Agent that matches the host in the request URI.
This can be particularly useful if a rule changes the hostname in a request URI, for example by ENUM lookup. If the lookup yields an address of a valid Call Agent, it is used for routing, otherwise it proceeds to the next rule.

Parameter	Description
Route via R-URI	The 'Route via R-URI' method uses the request URI to find out the next-hop IP address. That is particularly useful when Call Agent rules alter the request URI using actions such as 'Restore contact from registrar' or 'ENUM lookup'. If the host part of request URI includes a DNS name that resolves to multiple destinations per RFC 3263, the SBC load-balances among the respective destinations by their priorities.
Set Next Hop	Uses the destination Call Agent's peer IP address(es) as the next-hop IP address.
Replaces the DNS name in the request URI with the resolved IP address.	If a DNS name appears in the request URI, it is substituted by its resolved IP address before forwarding.
Update To-URI host	Update To-URI host
Replace To-URI host with the resolved destination IP address.	Replace To-URI host with the resolved destination IP address.
Force transport	Overrides the transport protocol to be used to initiate SIP dialogs with the next hop. The following protocols are supported: UDP, TCP, TLS and Websockets. Note: To force TLS and guarantee that no other transport protocol can be used, you must also set the **SignalingInterface.AllowedTransports** parameter to TlsOnly.
Enable redirect handing	If this option is enabled, incoming 302 SIP responses are not passed upstream. Instead, the SBC takes the content of the 'Contact' header field and uses it as another next-hop for forwarding the original request. Specifically, the contact URI in the 302 SIP response is used to rewrite the request URI, determine the next-hop IP address and look up a Call Agent whose outbound rules are processed.

SBC Replacement Expressions

$r

Request URI.

The expression refers to the current request URI which may be changed during the course of request processing.

Name	Description
$r.	Complete request URI.
$ru	user@host[:port] part of the request URI.
$rU	User part of the request URI.
$rd	Request-URI domain (host:port).
$rh	Host part of the request URI.
$rp	Port number of the request URI.
$rP	Request URI Parameters.

$f

From header

Name	Description
$f.	Complete 'From' header field.
$fu	user@host[:port] part of the 'From' URI.
$fU	User part of the 'From' URI.
$fd	'From' URI domain (host:port).
$fh	Host part of the 'From' URI.
$fp	Port number of the 'From' URI.
$fn	Display name of the 'From' header field.
$fP	URI parameters of the 'From' header field.
$fQ	Header parameters of the 'From' header field.
$ft	The tag of the 'From' header field.
$fH	The name of the 'From' header field, exactly as it is stated in the SIP request.

$t

To header

Name	Description
$t.	Complete 'To' header.
$tu	user@host[:port] part of the 'To' URI.
$tU	User part of the 'To' URI.
$td	'To' URI domain (host:port).
$th	Host part of the 'To' URI.
$tp	Port number of the 'To' URI.
$tn	Display name of the 'To' header field.
$tP	URI parameters of the 'To' header field.
$tQ	Header parameters of the 'To' header field.
$tt	The tag of the 'To' header.
$tH	The name of the 'To' header, exactly as it is stated in the SIP request.

$a

P-Asserted-Identity

Name	Description
$a.	Complete 'P-Asserted-Identity' header.
$au	user@host[:port] part of the 'P-Asserted-Identity' URI.
$aU	User part of the 'P-Asserted-Identity' URI.
$ad	'P-Asserted-Identity' URI Domain (host:port).
$ah	Host part of the 'P-Asserted-Identity' URI.
$ap	Port number of the 'P-Asserted-Identity' URI.
$aP	Parameters of the 'P-Asserted-Identity' header field. Does not include the parameters of the URI.
$at	The tag of the 'P-Asserted-Identity'.
$aH	The name of the 'P-Asserted-Identity' header field, exactly as it is stated in the SIP request.

$p

P-Preferred-Identity

Name	Description
$p.	Complete 'P-Preferred-Identity' header field.
$pu	user@host[:port] part of the 'P-Preferred-Identity' URI.
$pU	User part of the 'P-Preferred-Identity' URI.
$pd	'P-Preferred-Identity' URI Domain (host:port).
$ph	Host part of the 'P-Preferred-Identity' URI.
$pp	Port number of the 'P-Preferred-Identity' URI.
$pP	Parameters of the 'P-Preferred-Identity' header field. Does not include the parameters of the URI.
$pt	The tag of the 'P-Preferred-Identity' header field.
$pH	The name of the 'P-Preferred-Identity' header, exactly as it is stated in the SIP request.

$c

Call-ID

Name	Description
$ci	Call-ID of the SIP request.

$s

Source party

Name	Description
$si	Source IP address of the inbound SIP request.
$sp	Source port number of the inbound SIP request.

$d

Expected destination party

Name	Description
$di	Destination IP address of the outbound SIP request. This replacement expression is only available in outbound rules.
$dp	Destination port number of the outbound SIP request. This replacement expression is only available in outbound rules.

$R

Interface of the inbound SIP request

Name	Description
$Ri	IP address of the Signaling Interface on which the inbound SIP request was received.
$Rp	Port number of the Signaling Interface on which the inbound SIP request was received.
$Rf	ID of the Signaling Interface on which the inbound SIP request was received.
$Rn	Name of the Signaling Interface on which the inbound SIP request was received.
$RI	The configured address of the **SignalingInterface.PublicIpAddr** parameter on which the inbound SIP request was received.

$H

Arbitrary Headers
The replacement expressions in this group mention the name of an arbitrary header between parentheses.

The core headers (From, To, Call-ID, Via, Route, Record-Route, Contact) cannot be replaced.

Example: $H(Server) will be replaced by the value of the 'Server' header field.

Name	Description
$H(headername)	Value of the 'headername' header
$HU(headername)	User part of the URI in the 'headername' header.
$Hd(headername)	URI Domain (host:port) of the 'headername' header.
$Hu(headername)	user@host[:port] part of the URI in the 'headername' header.
$Hh(headername)	Host part of the URI in the 'headername' header.
$Hp(headername)	Port number of the URI in the 'headername' header.
$Hn(headername)	Display name of the 'headername' header.
$HP(headername)	Parameters of the 'headername' header field. Does not include the parameters of the URI.
$HH(headername)	Header headername (as URI) headers

$m

Request method

Name	Description
$m	The method of the request.

$V

Call parameter

Name	Description
$V(gui.varname)	Value of the 'varname' call parameter.

$B

Cnum and Rnum

Name	Description
$B(cnum.rnum)	Value of the regular expression backreference. • Rnum is the index of the rule condition containing the regular expression, starting at 1. • Cnum is the index of the subexpression within the regular expression, starting at 1.

$U

Register cache

Name	Description
$Ua	Originating AoR from the registration cache. This replacement expression can only be used after the execution of a‘Restore contact from registrar’ or a ‘Retarget R-URI from cache’ action.
$UA	Originating alias from the registration cache. This replacement expression can only be used after the execution of a ‘Restore contact from registrar’ or a ‘Retarget R-URI from cache’ action.

$_

Operations on Values

Name	Description
$_u(value)	Changes the value to uppercase.
$_l(value)	Changes the value to lowercase.
$_s(value)	Size of the value.
$_5(value)	MD5 sum of the value.
$_r(value)	Random number from 0 to 'value' - 1. Example: $_r(5) gives 0, 1, 2, 3 or 4.

$#

URL-encoded

Name	Description
$#(value)	Encodes the value into a URL format with appropriate escaping for characters outside the ASCII character set.

$attr

Global Attributes

Name	Description
$attr(version)	Version number of the DGW firmware. The returned value matches with the %version% macro in DGW firmware.
$attr(profile)	Profile identification of the DGW firmware. The returned value matches with the %profile% macro in DGW firmware.
$attr(serial)	Serial number of the Mediatrix unit. The returned value matches with the %serial% macro in DGW firmware.
$attr(mac)	MAC address of the Mediatrix unit. The returned value matches with the %mac% macro in DGW firmware.
$attr(product)	Product name of the Mediatrix unit. The returned value matches with the %product% macro in DGW firmware.
$attr(productseries)	Product series name of the Mediatrix unit. The returned value matches with the %productseries% macro in DGW firmware.

Service Controller Manager (Scm)

The Service Controller Manager (SCM) service allows the administrator to enable or disable services.

Parameters

ServicesInfo (Table)

This table contains information about each service within the system.

Name (Index) | Table: ServicesInfo

Type	Text
Range	
Script/CLI	Scm.ServicesInfo[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.400.1.100.1.100

Displays the service name.

Id (Status Parameter) | Table: ServicesInfo

Type	UInt32
Range	
Script/CLI	Scm.ServicesInfo[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.400.1.100.1.200

Shows the service identifier.

Class (Status Parameter) | Table: ServicesInfo

Type	Enum
Range	System(100) | User(200)
Script/CLI	Scm.ServicesInfo[].Class
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.400.1.100.1.400

Shows the service class.

- System: A system service is a core element of the system. It cannot be managed by the administrator.
- User: A user service is an element that can be managed by the administrator. This type of service is not essential to the system execution.

StartupType (Status Parameter) | Table: ServicesInfo

Type	Enum
Range	Auto(100) | Manual(200)
Script/CLI	Scm.ServicesInfo[].StartupType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.400.1.100.1.500

Shows the service startup type.

- Auto: The service is automatically started when the system restarts.
- Manual: The administrator manually starts the service.

ExecState (Status Parameter) | Table: ServicesInfo

Type	Enum
Range	Started(100) | Starting(200) | Stopped(300) | Stopping(400) | NotResponding(65000)
Script/CLI	Scm.ServicesInfo[].ExecState
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.400.1.100.1.600

Shows the execution state of the service.

- Started: Service started and executing normally.
- Starting: Service is being started.
- Stopped: Service has stopped its execution.
- Stopping: Service has been requested to stop and is freeing resource.
- NotResponding: Service has been requested to start or stop and has not responded within the allowed delay.

Comment (Status Parameter) | Table: ServicesInfo

Type	Text
Range	Size(0..255)
Script/CLI	Scm.ServicesInfo[].Comment
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.400.1.100.1.700

Displays comments on the service's current state.

ServiceCommands (Table)

This table contains commands that can be executed on services.

Name (Index) | Table: ServiceCommands

Type	Text
Range	
Script/CLI	Scm.ServiceCommands[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.400.1.200.1.100

Displays the service name.

Restart (Row Command) | Table: ServiceCommands

Script/CLI:	Scm.ServiceCommands[].Restart
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.400.1.200.1.200

Restarts the service.

Stop (Row Command) | Table: ServiceCommands

Script/CLI:	Scm.ServiceCommands[].Stop
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.400.1.200.1.300

Stops the service.

Start (Row Command) | Table: ServiceCommands

Script/CLI:	Scm.ServiceCommands[].Start
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.400.1.200.1.400

Starts the service.

ServicesConfig (Table)

This table configures each service within the system.

Name (Index) | Table: ServicesConfig

Type	Text
Range	
Script/CLI	Scm.ServicesConfig[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.400.1.400.1.100

Displays the service name.

StartupType (Config Parameter) | Table: ServicesConfig

Type	Enum
Range	Auto(100) | Manual(200)
Default	Auto
Script/CLI	Scm.ServicesConfig[].StartupType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.400.1.400.1.200

Selects the service startup type.

- Auto: The service is automatically started when the system starts.
- Manual: The administrator must manually start the service.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Scm.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.400.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Scm.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.400.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

CancelRestartRequiredServices (Command)

Cancel the restart during the grace delay period.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

RestartRequiredServices (Command)

Restart only the services that needed a restart for their configuration to be applied.

GraceDelay (Argument) | Command: RestartRequiredServices

Type	UInt32
Range	0..10080
Default	0

The delay (in minutes) allowed for telephony calls to be all completed.
At the expiration of this delay, the services are forced to restart.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Scm service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.400.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	Starting service <%1$s>.	Debug	This message is issued when the SCM starts a service.
20	Service <%1$s> started successfully.	Info	This message is issued when a service has successfully started.
40	Service <%1$s> is stopped.	Info	This message is issued when a service is in the stopped state.
50	Service <%1$s> is being stopped.	Debug	This message is issued when a service has been asked to stop its execution.
60	Service <%1$s> registers.	Debug	This message is issued when the service registers itself along with its dependencies.
70	Service <%1$s> unregisters.	Debug	This message is issued when the service unregisters itself.
80	SCM is restarting service <%1$s>.	Info	This message is issued when the user executes the `Restart` command on a service.
90	Restart of service(s) completed.	Info	This message is issued when SCM has finished restarting services.
100	Stop of service(s) completed.	Info	This message is issued when SCM has finished stopping services.
110	Service <%1$s> has not responded to the last Start request within the allowed delay.	Warning	This message is issued when a service did not respond to a start request before the allowed timeout has elapsed.
120	Service <%1$s> has not responded to the last Stop request within the allowed delay.	Warning	This message is issued when a service did not respond to a stop request before the allowed timeout has elapsed.
130	Received the restart required services command.	Info	This message is issued when the user or script executes the `RestartRequiredServices` command. This command will restart only the services that needed it.
135	Received the cancel restart required services command.	Info	This message is issued when the user or script executes the `CancelRestartRequiredServices` command.
140	SCM is starting service < %1$s>.	Info	This message is issued when the user executes the `Start` command on a service.
150	Start of service(s) completed.	Info	This message is issued when SCM has finished starting services.

NumKey	Message	Severity	Description
160	SCM is stopping service <%1$s>.	Info	This message is issued when the user executes the `Stop` command on a service.
170	The allowed time for graceful services restart expired. Forcing the services restart.	Warning	The time allowed for a graceful restart of services expired. Forcing the services restart.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.

NumKey	Message	Severity	Description
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.

NumKey	Message	Severity	Description
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Scm.

Message	Severity	Description
Cannot perform command on service < %1$s> because it is a system class service.	Error	This message is issued when the user tries to perform a command on a system class service.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.

Message	Severity	Description
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

SIP Endpoint (SipEp)

The SIP Endpoint (SipEp) service allows the administrator to associate telephony endpoints with SIP user agents.

Parameters

Gateway (Table: user-defined, 10 lines max.)

This table holds the basic configuration of the IP gateways.

Name (Index) | Table: Gateway

Type	Text
Range	
Script/CLI	SipEp.Gateway[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.100.1.100

Name of the SIP gateway. It identifies the gateway in other tables.

Type (Config Parameter) | Table: Gateway

Type	Enum
Range	TrunkGateway(100) | EndpointGateway(200)
Default	TrunkGateway
Script/CLI	SipEp.Gateway[].Type
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.100.1.150

Type of the SIP gateway.

NetworkInterface (Config Parameter) | Table: Gateway

Type	Text
Range	Size(1..50)
Default	Lan1
Script/CLI	SipEp.Gateway[].NetworkInterface
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.100.1.200

The network on which the gateway listens for incoming SIP traffic.
The value must match one of the **InterfaceName** values in the **NetworkInterfaces** or **NetworkInterfacesStatus** table of the BNI service.

The value must be set to 'Loop' when the Sbc service is set as a home domain or outbound proxy.

This value applies to all transports (e.g., UDP, TCP, etc.).

MediaNetworks (Config Parameter) | Table: Gateway

Type	Text
Range	Size(0..255)
Default	
Script/CLI	SipEp.Gateway[].MediaNetworks
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.100.1.250

List of networks (separated by ",") to use for the media (voice, fax, etc.) stream. The value must match one of the **InterfaceName** values in the **NetworkInterfacesStatus** table of the BNI service.

The order in the list defines the priority. If the list of media network is empty, the network defined in the **Gateway.NetworkInterface** parameter is used.

When the media stream is negotiated, only the first active network (**NetworkInterfacesStatus.Status** columnar of the network in the BNI service is active) of an IP address family (IPv4, IPv6) is used. All subsequent networks of the same IP family are ignored.

Note: When generating an offer and multiple networks are available for the media, ANAT grouping (RFC 4091) is automatically activated. When generating an answer, ANAT grouping is activated when it is detected in the offer. The SDP answer will always have only one active media with the preferred IP address family.

Port (Config Parameter) | Table: Gateway

Type	ExtIpPort
Range	
Default	0
Script/CLI	SipEp.Gateway[].Port
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.100.1.300

Port on which the gateway listens for incoming unsecure SIP traffic.
This is used only when UDP and/or TCP transports are enabled.

Notes:

- If set to 0, the unit uses the default SIP port 5060.
- This parameter applies to Trunk gateways only. 'Endpoint' gateways have no static listening port.

SecurePort (Config Parameter) | Table: Gateway

Type	ExtIpPort
Range	
Default	0
Script/CLI	SipEp.Gateway[].SecurePort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.100.1.325

Port on which the gateway listens for incoming secure SIP traffic.
This is used only when the TLS transport is enabled.

Notes:

- If set to 0, the unit uses the default SIP port 5061.

- This parameter applies to Trunk gateways only. 'Endpoint' gateways have no static listening port.

Domain (Config Parameter) | Table: Gateway

Type	Text
Range	SIZE(0..255)
Default	
Script/CLI	SipEp.Gateway[].Domain
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.100.1.350

SIP domain name. If not empty, it overrides the home domain proxy (refer to the **DefaultStaticProxyHomeDomainHost** parameter) in the following places:

In the address of record.

In the Request-URI. When the **Gateway.Domain** parameter overrides the home domain proxy in the Request-URI, the Request-URI also contain a maddr parameter with the resolved home domain proxy to make sure the requests are routable.

Delete (Row Command) | Table: Gateway

Script/CLI:	SipEp.Gateway[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.100.1.400

Deletes this row.

GatewayStatus (Table)

This table holds the status of the current IP gateways.

Name (Index) | Table: GatewayStatus

Type	Text
Range	
Script/CLI	SipEp.GatewayStatus[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.150.1.100

Name of the SIP gateway. It identifies the gateway in other tables.

NetworkInterface (Status Parameter) | Table: GatewayStatus

Type	Text
Range	
Script/CLI	SipEp.GatewayStatus[].NetworkInterface
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.150.1.200

The network on which the gateway listens for incoming SIP traffic.
This value applies to all transports (e.g., UDP, TCP, etc.).

MediaNetworks (Status Parameter) | Table: GatewayStatus

Type	Text
Range	
Script/CLI	SipEp.GatewayStatus[].MediaNetworks
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.150.1.250

List of networks (separated by ",") to use for the media (voice, fax, etc.) stream. Only the first active network of an IP address family (IPv4, IPv6) is present. The order in the list defines the priority.
Note: When generating an offer and multiple network are available for the media, ANAT grouping (RFC 4091) is automatically activated. When generating an answer, ANAT grouping is activated when it is detected in the offer. The SDP answer will always have only one active media with the preferred IP address family.

Port (Status Parameter) | Table: GatewayStatus

Type	ExtIpPort
Range	
Script/CLI	SipEp.GatewayStatus[].Port
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.150.1.300

Port on which the gateway listens for incoming unsecure SIP traffic.
This value applies to UDP and TCP transports only and for Trunk gateways.

Note: If set to 0, the unit uses the default SIP port 5060.

SecurePort (Status Parameter) | Table: GatewayStatus

Type	ExtIpPort
Range	
Script/CLI	SipEp.GatewayStatus[].SecurePort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.150.1.325

Port on which the gateway listens for incoming SIP traffic.
This value applies to TLS transport only and for Trunk gateways.

Note: If set to 0, the unit uses the default SIP port 5061.

Domain (Status Parameter) | Table: GatewayStatus

Type	Text
Range	
Script/CLI	SipEp.GatewayStatus[].Domain
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.150.1.350

SIP domain name. String used to build the address of record.

State (Status Parameter) | Table: GatewayStatus

Type	Text
Range	
Script/CLI	SipEp.GatewayStatus[].State
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.150.1.400

The current state of the gateway.

- Ready: The gateway is ready to make and receive calls.
- Cannot start, port already in use: The gateway cannot open its IP port because the port is already used by another service. This generally occurs when the administrator adds a new gateway but forgets to configure a different IP port.
- Network down: The SIP gateway is not started or the network interface on which the SIP gateway is associated does not have an IP address.
- Restarting: The SIP gateway cannot make or receive calls while it is restarting.

- Waiting for time synchronization: The gateway is started but it cannot open its SIP TLS port because the real-time clock is not synchronized. This generally occurs when the SNTP server is not set or is unreachable.
- Server unreachable: The gateway is started but it cannot make and receive calls because the SIP server is unreachable. This state is only reported when the **SipKeepAliveMethod** parameter is configured.
- Invalid Configuration: The gateway cannot start due to an inconsistent configuration.
- Waiting for telephony lines: The gateway is waiting for at least one E1T1 link to be up. This state is only available when the **EpAdm.DisableSipGatewaysWhenTrunkLinesDown** parameter is set to Enable.

UserAgent (Table)

This table holds the user agent configuration parameters. A user agent is a logical entity that can act as both a client and a server for the duration of a dialog. The information contained in this table will be used to dynamically create the To, From, and Contact headers used in the request sent by the UAC (User Agent Client).

EpId (Index) | Table: UserAgent

Type	Text
Range	
Script/CLI	SipEp.UserAgent[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.400.1.100

String that identifies an endpoint in other tables.

Username (Config Parameter) | Table: UserAgent

Type	Text
Range	SIZE(0..255)
Default	
Script/CLI	SipEp.UserAgent[].Username
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.400.1.200

A string that uniquely identifies this endpoint in the domain. For example, a telephone number. This string is used when creating the Contact and From headers. The SIP From header carries the permanent location (IP address, home domain) where the endpoint is. The SIP Contact header carries the CURRENT location (IP address) where the endpoint can be reached.

Contact headers are used in two ways:

First, contacts are registered to the SIP registrar. This enables external callers to be redirected to the endpoint's current location.

Second, a contact header is sent along with any request the UA sends (e.g.: INVITE), and is used by the target UA as a return address for later requests sent by the target to this endpoint.

FriendlyName (Config Parameter) | Table: UserAgent

Type	Text
Range	SIZE(0..255)
Default	
Script/CLI	SipEp.UserAgent[].FriendlyName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.400.1.300

Friendly name for SIP User Agent. A friendly name or display name is meant to contain a descriptive version of the URI and is intended to be displayed to a user interface.

Register (Config Parameter) | Table: UserAgent

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.UserAgent[].Register
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.400.1.400

Indicates if the endpoint needs to register to the registrar.
If set to Enable, the endpoint will become BY DEFAULT unavailable when not registered. The **RegistrationUnregisteredBehavior** parameter can modify this behaviour.

GatewayName (Config Parameter) | Table: UserAgent

Type	Text
Range	
Default	all
Script/CLI	SipEp.UserAgent[].GatewayName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.400.1.500

Selects on which SIP gateway the user configuration is applied. The value must match the gateway name as defined in the **Gateway.Name** parameter.
The value 'all' means all gateways.

MwiSubscribe (Config Parameter) | Table: UserAgent

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.UserAgent[].MwiSubscribe
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.400.1.700

Indicates if the endpoint needs to subscribe to messaging system. When set to Enable, an endpoint subscription is triggered.

ContactDomain (Config Parameter) | Table: UserAgent

Type	Text
Range	SIZE(0..127)
Default	
Script/CLI	SipEp.UserAgent[].ContactDomain
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.400.1.800

Indicates the host part of the SIP contact field. If an empty string is specified, the listening IP address is used.

AcceptLanguage (Config Parameter) | Table: UserAgent

Type	Text
Range	SIZE(0..255)
Default	
Script/CLI	SipEp.UserAgent[].AcceptLanguage
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.400.1.900

Indicates the preferred languages for reason phrases, session descriptions, or status responses carried as message bodies in the response. It is used to fill the Accept-Language SIP header field. The general syntax is a comma-separated list of language codes.

Example: en, fr

See ISO 639-1 for a list of language codes.

See RFC 3261 for the detailed syntax.

NOTE: When the string is empty, the Accept-Language header will not be added.

DefaultStaticProxyHomeDomainHost (Config Parameter)

Type	IpHostNamePort
Range	
Default	192.168.10.10:0
Script/CLI	SipEp.DefaultStaticProxyHomeDomainHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.500.100

SIP proxy server FQDN and port.
An intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. A proxy server primarily plays the role of routing, which means its job is to ensure that a request is passed on to another entity that can further process the request. Proxies are also useful for enforcing policy and for firewall traversal. A proxy interprets, and, if necessary, rewrites parts of a request message before forwarding it.

Special macros can be entered when the Sbc and/or SipProxy service are available:

- The special macro '%sbc%' can be entered to use the SBC as the destination host. This macro resolves to the IP address and port of the 'loop_s' signaling interface in the Sbc service.
- The special macro '%sipproxy%' can be entered to use the SipProxy service as the destination host. This macro resolves to the IP address and port of the SipProxy service.

If the special macro %sbc% is used in the home domain proxy, then the registration and messaging hosts must be either set to %sbc% or left empty.

Note: If the host corresponds to a domain name that is bound to a SRV record, the port must be set to 0 for the unit to perform DNS SRV queries; otherwise only A type record lookups will be used.

DefaultStaticProxyOutboundHost (Config Parameter)

Type	IpHostNamePort
Range	
Default	
Script/CLI	SipEp.DefaultStaticProxyOutboundHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.500.200

SIP outbound proxy server FQDN and port
To disable the outbound proxy, set it to '0.0.0.0'.

From RFC 3261: A proxy that receives requests from a client, even though it may not be the server resolved by the Request-URI. Typically, a UA is manually configured with an outbound proxy, or can learn about one through auto-configuration protocols.

When enabled, the initial route for all SIP requests will contain the outbound proxy address, suffixed with the loose routing parameter 'lr'. The Request-URI still contains the home domain proxy address. Requests are directed to the first route (the outbound proxy).

Special macros can be entered when the Sbc and/or SipProxy service are available:

- The special macro '%sbc%' can be entered to use the SBC as the destination host. This macro resolves to the IP address and port of the 'loop_s' signaling interface in the Sbc service.
- The special macro '%sipproxy%' can be entered to use the SipProxy service as the destination host. This macro resolves to the IP address and port of the SipProxy service.

Note: If the host corresponds to a domain name that is bound to a SRV record, the port must be set to 0 for the unit to perform DNS SRV queries; otherwise only A type record lookups will be used.

DefaultProxyOutboundType (Config Parameter)

Type	Enum
Range	LooseRouter(100) | StrictRouter(200) | NoRouteHeader(300)
Default	LooseRouter
Script/CLI	SipEp.DefaultProxyOutboundType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.500.300

Default type of routing that the configured outbound proxy does.

- LooseRouter: This is the most current method for SIP routing, as per RFC 3261, and will become the standard behaviour once RFC 3261 compliance is achieved. See the **DefaultStaticProxyOutboundHost** parameter for a description.
- StrictRouter: Pre-RFC 3261, RFC 2543 compatible SIP routing.
- NoRouteHeader: Removes the route header from all SIP packets sent to an outbound proxy. Does not modify persistent TLS connection headers.

The initial route for all SIP requests contains the home domain proxy address (the Request-URI). Requests are directed to the outbound proxy.

In other words, the Request-URI is constructed as usual by using the home domain proxy and the user name, but is used in the route set. The Request-URI is filled by the outbound proxy address.

Also see the **DefaultStaticProxyHomeDomainHost** parameter.

GwSpecificProxy (Table)

A table of the proxy configuration indexed by the SIP gateway name. It is used to override the default value.

GatewayName (Index) | Table: GwSpecificProxy

Type	Text
Range	
Script/CLI	SipEp.GwSpecificProxy[].GatewayName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.500.400.1.100

String that identifies a SIP gateway in other tables.

EnableConfig (Config Parameter) | Table: GwSpecificProxy

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.GwSpecificProxy[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.500.400.1.200

Defines the configuration to use for a specific SIP gateway.

- Disable: The SIP gateway uses the default configuration as defined in the **DefaultStaticProxyHomeDomainHost**, **DefaultStaticProxyOutboundHost**, and **DefaultProxyOutboundType** parameters.
- Enable: The SIP gateway uses the specific configuration as defined in the **GwSpecificProxy.HomeDomainHost**, **GwSpecificProxy.OutboundHost**, and **GwSpecificProxy.OutboundType** parameters.

HomeDomainHost (Config Parameter) | Table: GwSpecificProxy

Type	IpHostNamePort
Range	
Default	192.168.0.10:0
Script/CLI	SipEp.GwSpecificProxy[].HomeDomainHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.500.400.1.300

SIP proxy server FQDN and port for a specific SIP gateway.
An intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. A proxy server primarily plays the role of routing, which means its job is to ensure that a request is passed on to another entity that can further process the request. Proxies are also useful for enforcing policy and for firewall traversal. A proxy interprets, and, if necessary, rewrites parts of a request message before forwarding it.

Special macros can be entered when the Sbc and/or SipProxy service are available:

- The special macro '%sbc%' can be entered to use the SBC as the destination host. This macro resolves to the IP address and port of the 'loop_s' signaling interface in the Sbc service.
- The special macro '%sipproxy%' can be entered to use the SipProxy service as the destination host. This macro resolves to the IP address and port of the SipProxy service.

If the special macro %sbc% is used in the home domain proxy, then the registration and messaging hosts must be either set to %sbc% or left empty.

Note: If the host corresponds to a domain name that is bound to a SRV record, the port must be set to 0 for the unit to perform DNS SRV queries; otherwise, only A type record lookups will be used.

OutboundHost (Config Parameter) | Table: GwSpecificProxy

Type	IpHostNamePort
Range	
Default	0.0.0.0:0
Script/CLI	SipEp.GwSpecificProxy[].OutboundHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.500.400.1.400

SIP outbound proxy server FQDN and port for a specific SIP gateway.
To disable the outbound proxy, set it to '0.0.0.0'.

From RFC 3261: A proxy that receives requests from a client, even though it may not be the server resolved by the Request-URI. Typically, a UA is manually configured with an outbound proxy, or can learn about one through auto-configuration protocols.

When enabled, the initial route for all SIP requests will contain the outbound proxy address, suffixed with the loose routing parameter 'lr'. The Request-URI still contains the home domain proxy address. Requests are directed to the first route (the outbound proxy).

Special macros can be entered when the Sbc and/or SipProxy service are available:

- The special macro '%sbc%' can be entered to use the SBC as the destination host. This macro resolves to the IP address and port of the 'loop_s' signaling interface in the Sbc service.
- The special macro '%sipproxy%' can be entered to use the SipProxy service as the destination host. This macro resolves to the IP address and port of the SipProxy service.

Note: If the host corresponds to a domain name that is bound to a SRV record, the port must be set to 0 for the unit to perform DNS SRV queries; otherwise, only A type record lookups will be used.

OutboundType (Config Parameter) | Table: GwSpecificProxy

Type	Enum
Range	LooseRouter(100) | StrictRouter(200) | NoRouteHeader(300)
Default	LooseRouter
Script/CLI	SipEp.GwSpecificProxy[].OutboundType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.500.400.1.500

Type of routing that the configured outbound proxy does for a specific SIP gateway.

- LooseRouter: This is the most current method for SIP routing, as per RFC 3261, and will become the standard behaviour once RFC 3261 compliance is achieved. See the **DefaultStaticProxyOutboundHost** parameter for a description.
- StrictRouter: Pre-RFC 3261, RFC 2543 compatible SIP routing.
- NoRouteHeader: Removes the route header from all SIP packets sent to an outbound proxy. Does not modify persistent TLS connection headers.

The initial route for all SIP requests contains the home domain proxy address (the Request-URI). Requests are directed to the outbound proxy.

In other words, the Request-URI is constructed as usual by using the home domain proxy and the user name, but is used in the route set. The Request-URI is filled by the outbound proxy address.

Also see the **DefaultStaticProxyHomeDomainHost** parameter.

DefaultSessionTimerEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	SipEp.DefaultSessionTimerEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.600.100

Enables/Disables the session expiration services.
Disabling this service is not recommended since it will make 'dead' calls impossible to detect.

Questions and Answers:

Q - What is the session timer extension?

A - The session timer extension allows the detection of the premature end of a call caused by a network problem or a peer's failure.

The session timer mechanism sends a refresh request every n seconds. This refresh request is either an reINVITE or an UPDATE, according to configuration in the **SessionRefreshRequestMethod** parameter. A sucessful response (200 OK) to this refresh request means that the peer is still alive and reachable. A timeout to this refresh request may mean that there are problems in the signaling path, or that the peer is simply not there anymore. In that case the call will be shut down by using normal SIP means.

Q - SDP in Session Timer reINVITEs or UPDATEs:

A - If the reINVITE method is used, it is sent with the last SDP that was negotiated. Reception of a session timer reINVITE should not modify the connection characteristics. If the UPDATE method is used, it is sent without any SDP offer. The UPDATE method is recommended to improve SRTP interoperability.

Q - Relation between minimum and maximum values:

A - A UA that receives a Session-Expires header whose value is smaller than the minimum it is willing to accept will reply a 422 Timer too low to the INVITE and terminate the call. The phone will not ring.

It is up to the caller to decide what to do when it receives a 422 to its INVITE. The service will automatically retry the INVITE, with a Session-Expires value equal to the minimum value that the UAS was ready to accept (found in the Min-SE header). This means that the maximum value as set in the service might not be followed. This has the advantageous effect of establishing the call even if the two endpoints have conflicting values. The service will also keep retrying as long as it gets 422 answers with different Min-SE values.

Q - Who refreshes?

A - Sending a session timer reINVITE or UPDATE is referred to as refreshing the session. Normally, the UAS that receives the INVITE will have the last word on who refreshes. The service will always let the UAC (caller) do the refreshes if the caller supports session timers. In the case the caller does not support session timers, the service will assume the role of the refresher.

DefaultSessionTimerMinimumExpirationDelay (Config Parameter)

Type	UInt32
Range	180..86400
Default	1800
Script/CLI	SipEp.DefaultSessionTimerMinimumExpirationDelay
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.600.200

Minimum value for the periodical session refreshes.
This value is reflected in the Min-SE header.

The Min-SE value is a threshold under which proxies and/or UAs on the signaling path are not allowed.

Increasing the minimum helps to reduce network traffic, but also makes 'dead' calls longer to detect.

This value is expressed in seconds (s).

Also see the **DefaultSessionTimerMaximumExpirationDelay** parameter.

DefaultSessionTimerMaximumExpirationDelay (Config Parameter)

Type	UInt32
Range	180..86400
Default	3600
Script/CLI	SipEp.DefaultSessionTimerMaximumExpirationDelay
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.600.300

Suggested maximum time for the periodical session refreshes.
This value is reflected in the Session-Expires header.

Increasing the maximum helps to reduce network traffic, but also makes 'dead' calls longer to detect.

This value is expressed in seconds (s).

Also see the **DefaultSessionTimerMinimumExpirationDelay** parameter.

SessionRefreshRequestMethod (Config Parameter)

Type	Enum
Range	ReInvite(100) | Update(200)
Default	ReInvite
Script/CLI	SipEp.SessionRefreshRequestMethod
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.600.400

Selects the method used for sending Session Refresh Requests.

- ReInvite: Session Refresh Requests are sent with the INVITE method.
- Update: Session Refresh Requests are sent with the UPDATE method. This is the recommended method to improve SRTP interoperability, since it contains no SDP.

Session Refresh Requests can be received via both methods, regardless of how this parameter is configured.

Authentication (Table: user-defined, 500 lines max.)

This table holds the user agent authentication configuration parameters. Authentication information adds some level of security.

Index (Index) | Table: Authentication

Type	UInt32
Range	
Script/CLI	SipEp.Authentication[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.700.100.1.100

Authentication index for this row.
The table's entries are searched in ascending **Authentication.Index** order.

CriteriaSelection (Config Parameter) | Table: Authentication

Type	Enum
Range	Unit(100) | Endpoint(200) | Gateway(300) | Username(400)
Default	Unit
Script/CLI	SipEp.Authentication[].CriteriaSelection
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.700.100.1.200

Selects which criterion to use for matching an authentication request with an authentication entry.

- Unit: The authentication entry is used on all challenges that were not matched on a previous entry.
- Endpoint: The authentication entry is used for all challenges related to the endpoint specified in the **Authentication.EpId** parameter.
- Gateway: The authentication entry is used for all challenges related to the gateway specified in the **Authentication.GatewayName** parameter.
- Username: The authentication entry is used for all challenges related to the username specified in the **Authentication.UsernameCriteria** parameter.

EpId (Config Parameter) | Table: Authentication

Type	Text
Range	
Default	
Script/CLI	SipEp.Authentication[].EpId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.700.100.1.300

String that identifies an endpoint in the **UserAgent** table. Used only if the **CriteriaSelection** parameter is set to 'Endpoint'.

GatewayName (Config Parameter) | Table: Authentication

Type	Text
Range	
Default	
Script/CLI	SipEp.Authentication[].GatewayName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.700.100.1.350

String that identifies a SIP gateway in the **GatewayStatus** table. It is used only if the **CriteriaSelection** parameter is set to 'Gateway'.

UsernameCriteria (Config Parameter) | Table: Authentication

Type	Text
Range	Size(0..255)
Default	
Script/CLI	SipEp.Authentication[].UsernameCriteria
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.700.100.1.360

String that identifies a username in the SIP request to authenticate. It is used only if the **CriteriaSelection** parameter is set to 'Username'.

ValidateRealm (Config Parameter) | Table: Authentication

Type	EnableDisable
Range	
Default	Enable
Script/CLI	SipEp.Authentication[].ValidateRealm
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.700.100.1.375

Configures how to interpret the realm in the challenge.

- Disable: The credential defined in this row will be used with any realm given in the challenge.
- Enable: The credential defined in this row will be used only when the realm given in the challenge is the same as the one defined in the **Realm** parameter.

Realm (Config Parameter) | Table: Authentication

Type	Text
Range	Size(0..128)
Default	
Script/CLI	SipEp.Authentication[].Realm
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.700.100.1.400

When authentication informations are required from users, the realm identifies who requested the information.

Username (Config Parameter) | Table: Authentication

Type	Text
Range	Size(0..128)
Default	
Script/CLI	SipEp.Authentication[].Username
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.700.100.1.500

A string that uniquely identifies this entity in the realm, used for authentication purposes. The user name always maps to a password.

Password (Config Parameter) | Table: Authentication

Type	Text
Range	Size(0..255)
Default	
Script/CLI	SipEp.Authentication[].Password
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.700.100.1.600

User password.
Password encryption is supported via the **Dcm.PasswordEncryption** table.

When **Dcm.PasswordEncryption** is enabled clear text passwords will be automatically encrypted.

Unencrypted password maximal length is 128.

Encrypted password maximal length is 221.

Up (Row Command) | Table: Authentication

Script/CLI:	SipEp.Authentication[].Up
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.700.100.1.700

Moves the current row upside.

Down (Row Command) | Table: Authentication

Script/CLI:	SipEp.Authentication[].Down
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.700.100.1.800

Moves the current row downside.

Insert (Row Command) | Table: Authentication

Script/CLI:	SipEp.Authentication[].Insert
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.700.100.1.900

Inserts a new row before this row.

Delete (Row Command) | Table: Authentication

Script/CLI:	SipEp.Authentication[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.700.100.1.1000

Deletes this row.
The **Authentication** table has a minimum size of 20 rows. When calling the `DeleteAllRows` command on this table, all the rows are deleted and 20 new rows are added. When the user deletes a specific row, a new row is added at the end of the table if the number of rows is inferior to 20.

DefaultRegistrationRefreshTime (Config Parameter)

Type	UInt32
Range	0..600
Default	60
Script/CLI	SipEp.DefaultRegistrationRefreshTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.200

In SIP, a registration is valid for a period of time defined by the registrar. Once a unit is registered, the SIP protocol requires the User Agent to refresh this registration before the registration expires. Typically, this re-registration must be completed before the ongoing registration expires, so that the User Agent's registration state does not change (i.e., remains 'registered').
This parameter defines the time, relative to the end of the registration, at which a registered unit will begin updating its registration.

For example, if the registration lasts 60 minutes and the **RegistrationRefreshTime** parameter is set to 43, the unit will send new REGISTER requests 59 minutes and 17 seconds after the reception of the registration acknowledgement (43 seconds before the end of the registration period).

Setting the **RegistrationRefreshTime** parameter to 0 means that the User Agent will fall into the 'unregistered' state BEFORE sending the re-REGISTER requests.

This value is expressed in seconds (s).

If a specific configuration is set in the **GwSpecificRegistration.RefreshTime** parameter and the **GwSpecificRegistration.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultRegistrationExpirationValue (Config Parameter)

Type	UInt32
Range	1..86400
Default	3600
Script/CLI	SipEp.DefaultRegistrationExpirationValue
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.250

Configures the default registration expiration.
This value is used when the contact in a registration response contains no expires or the expires is badly formatted. In this case, the delay before a re-REGISTER is the value set in this parameter minus the value set in the **DefaultRegistrationRefreshTime** parameter.

See also the **DefaultRegistrationRefreshTime** parameter.

This value is expressed in seconds (s).

If a specific configuration is set in the **GwSpecificRegistration.ExpirationValue** parameter and the **GwSpecificRegistration.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultRegistrationProposedExpirationValue (Config Parameter)

Type	UInt32
Range	0..86400
Default	0
Script/CLI	SipEp.DefaultRegistrationProposedExpirationValue
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.300

Configures the suggested expiration delay of a contact in the SIP REGISTER.
Set the value to 0 to disable the expiration proposition.

This value does not modify the delay before a re-REGISTER. The delay is the expires of the contact in the 200 OK response to the REGISTER minus the value set in the **RegistrationRefreshTime** parameter. If the expires of the contact in the 200 OK response to the REGISTER is not present or badly formatted, then the delay is the default registration proposed expiration value minus the value set in the **RegistrationRefreshTime** parameter.

See also the **DefaultRegistrationRefreshTime** parameter.

This value is expressed in seconds (s).

If a specific configuration is set in the **GwSpecificRegistration.ProposedExpirationValue** parameter and the **GwSpecificRegistration.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultRegistrationRetryTime (Config Parameter)

Type	UInt32
Range	1..86400
Default	120
Script/CLI	SipEp.DefaultRegistrationRetryTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.350

Configures the interval on which a failed registration is retried.
This parameter defines the time, relative to the failure of the registration, at which the device retries the registration.

This value is expressed in seconds (s).

If a specific configuration is set in the **GwSpecificRegistration.RetryTime** parameter and the **GwSpecificRegistration.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultRegistrationUnregisteredBehavior (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.DefaultRegistrationUnregisteredBehavior
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.400

Specifies whether an endpoint should remain enabled or not when not registered.

- Disable: When an endpoint is not registered, it is disabled. This prevents the user from making or receiving calls. Picking up the handset yields a fast busy tone and incoming INVITEs receive a '403 Forbidden' response.
- Enable: When an endpoint is not registered, it is still enabled. The user can receive and initiate outgoing calls. Note that since the endpoint is not registered to a registrar, the public address of the endpoint is not available to the outside world, so the endpoint will most likely be unreachable except through direct IP calling.

If a specific configuration is set in the **GwSpecificRegistration.UnregisteredBehavior** parameter and the **GwSpecificRegistration.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultUnitRegistrationUnregisteredBehavior (Config Parameter)

Type	Enum
Range	NoEffect(100) | DisableGateway(200)
Default	NoEffect
Script/CLI	SipEp.DefaultUnitRegistrationUnregisteredBehavior
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.450

Specifies whether the SIP gateway state should be affected or not by the unit registrations state.

- NoEffect: The unit registrations state has no effect on the SIP gateway state.
- DisableGateway: The SIP gateway goes in the 'unregistered' state when all unit registrations are not in the 'registered' state.

DefaultStaticRegistrarServerHost (Config Parameter)

Type	IpHostNamePort
Range	
Default	192.168.10.10:0
Script/CLI	SipEp.DefaultStaticRegistrarServerHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.500

SIP registrar server FQDN and port.
A registrar is a server that accepts REGISTER requests and places the information it receives in those requests into the location service for the domain it handles.

Note: If the host corresponds to a domain name that is bound to a SRV record, the port must be set to 0 for the unit to perform DNS SRV queries; otherwise only type A record lookups will be used.

Special macros can be entered when the Sbc and/or SipProxy service are available:

- The special macro '%sbc%' can be entered to use the SBC as the destination host. This macro resolves to the IP address and port of the 'loop_s' signaling interface in the Sbc service.
- The special macro '%sipproxy%' can be entered to use the SipProxy service as the destination host. This macro resolves to the IP address and port of the SipProxy service.

If the special macro %sbc% is used in the home domain proxy, then the registration and messaging hosts must be either set to %sbc% or left empty.

If a specific configuration is set in the **GwSpecificRegistration.ServerHost** parameter and the **GwSpecificRegistration.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

GwSpecificRegistration (Table)

A table of the registration configuration indexed by the SIP gateway name. It is used to override the default value.

GatewayName (Index) | Table: GwSpecificRegistration

Type	Text
Range	
Script/CLI	SipEp.GwSpecificRegistration[].GatewayName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.600.1.100

String that identifies a SIP gateway in other tables.

EnableConfig (Config Parameter) | Table: GwSpecificRegistration

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.GwSpecificRegistration[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.600.1.200

Defines the configuration to use for a specific SIP gateway.

- Disable: The SIP gateway uses the default configuration as defined in the **DefaultStaticProxyHomeDomainHost**, **DefaultRegistrationRefreshTime**, **DefaultRegistrationProposedExpirationValue**, **DefaultRegistrationUnregisteredBehavior**, and **DefaultStaticRegistrarServerHost** parameters.
- Enable: The endpoint uses the specific configuration as defined in the **GwSpecificRegistration.RefreshTime**, **GwSpecificRegistration.ProposedExpirationValue**, **GwSpecificRegistration.UnregisteredBehavior**, and **GwSpecificRegistration.ServerHost** parameters.

RefreshTime (Config Parameter) | Table: GwSpecificRegistration

Type	UInt32
Range	0..600
Default	60
Script/CLI	SipEp.GwSpecificRegistration[].RefreshTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.600.1.300

Refresh registration time for a specific SIP gateway.
In SIP, a registration is valid for a period of time defined by the registrar. Once a unit is registered, the SIP protocol requires the User Agent to refresh this registration before the registration expires. Typically, this re-registration must be completed before the ongoing registration expires, so that the User Agent's registration state does not change (i.e., remains 'registered').

This parameter defines the time, relative to the end of the registration, at which a registered unit will begin updating its registration.

For instance, if the registration lasts 60 minutes and the **RegistrationRefreshTime** parameter is set to 43, the unit will send new REGISTER requests 59 minutes and 17 seconds after the reception of the registration acknowledgement (43 seconds before the end of the registration period).

Setting the **RegistrationRefreshTime** parameter to 0 means that the User Agent will fall into the 'unregistered' state BEFORE sending the re-REGISTER requests.

This value is expressed in seconds (s).

This configuration overrides the default configuration set in the **DefaultRegistrationRefreshTime** parameter if the **GwSpecificRegistration.EnableConfig** parameter is set to 'Enable'.

ExpirationValue (Config Parameter) | Table: GwSpecificRegistration

Type	UInt32
Range	1..86400
Default	3600
Script/CLI	SipEp.GwSpecificRegistration[].ExpirationValue
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.600.1.350

Configures the default registration expiration.
This value is used when the contact in a registration response contains no expires or the expires is badly formatted. In this case, the delay before a re-REGISTER is the value set in this parameter minus the value set in the **RefreshTime** parameter.

See also the **RefreshTime** parameter.

This value is expressed in seconds (s).

This configuration overrides the default configuration set in the **DefaultRegistrationExpirationValue** parameter if the **GwSpecificRegistration.EnableConfig** parameter is set to 'Enable'.

ProposedExpirationValue (Config Parameter) | Table: GwSpecificRegistration

Type	UInt32
Range	0..86400
Default	0
Script/CLI	SipEp.GwSpecificRegistration[].ProposedExpirationValue
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.600.1.400

Suggested expiration delay of a contact in the SIP REGISTER for a specific SIP gateway.
Set the value to 0 to disable the expiration proposal.

This value does not modify the delay before a re-REGISTER. The delay is the expires of the contact in the 200 OK response to the REGISTER minus the value set in the **RegistrationRefreshTime** parameter. If the expires of the contact in the 200 OK response to the REGISTER is not present

or badly formatted, then the delay is the default registration proposed expiration value minus the value set in the **RegistrationRefreshTime** parameter.

See also the **RefreshTime** parameter.

This value is expressed in seconds (s).

This configuration overrides the default configuration set in the **DefaultRegistrationProposedExpirationValue** parameter if the **GwSpecificRegistration.EnableConfig** parameter is set to 'Enable'.

RetryTime (Config Parameter) | Table: GwSpecificRegistration

Type	UInt32
Range	1..86400
Default	120
Script/CLI	SipEp.GwSpecificRegistration[].RetryTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.600.1.450

Configures the interval on which a failed registration retries on a specific SIP gateway.
This parameter defines the time, relative to the failure of the registration, at which the SIP gateway retries the registration.

This value is expressed in seconds (s).

This configuration overrides the default configuration set in the **DefaultRegistrationRetryTime** parameter if the **GwSpecificRegistration.EnableConfig** parameter is set to 'Enable'.

UnregisteredBehavior (Config Parameter) | Table: GwSpecificRegistration

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.GwSpecificRegistration[].UnregisteredBehavior
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.600.1.500

Specifies whether an endpoint should remain enabled or not when not registered for a specific SIP gateway.

- Disable: When an endpoint is not registered, it is disabled. This prevents the user from making or receiving calls. Picking up the handset yields a fast busy tone and incoming INVITEs receive a '403 Forbidden' response.
- Enable: When an endpoint is not registered, it is still enabled. The user can receive and initiate outgoing calls. Note that since the endpoint is not registered to a registrar, the public address

of the endpoint is not available to the outside world, so the endpoint will most likely be unreachable except through direct IP calling.

This configuration overrides the default configuration set in the **DefaultRegistrationUnregisteredBehavior** parameter if the **GwSpecificRegistration.EnableConfig** parameter is set to 'Enable'.

ServerHost (Config Parameter) | Table: GwSpecificRegistration

Type	IpHostNamePort
Range	
Default	192.168.0.10:0
Script/CLI	SipEp.GwSpecificRegistration[].ServerHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.600.1.600

SIP registrar server FQDN and port for a specific SIP gateway.
A registrar is a server that accepts REGISTER requests and places the information it receives in those requests into the location service for the domain it handles.

Note: If the host corresponds to a domain name that is bound to a SRV record, the port must be set to 0 for the unit to perform DNS SRV queries; otherwise, only type A record lookups will be used.

Special macros can be entered when the Sbc and/or SipProxy service are available:

- The special macro '%sbc%' can be entered to use the SBC as the destination host. This macro resolves to the IP address and port of the 'loop_s' signaling interface in the Sbc service.
- The special macro '%sipproxy%' can be entered to use the SipProxy service as the destination host. This macro resolves to the IP address and port of the SipProxy service.

If the special macro %sbc% is used in the home domain proxy, then the registration and messaging hosts must be either set to %sbc% or left empty.

This configuration overrides the default configuration set in the **DefaultRegistrarServerHost** parameter if the **GwSpecificRegistration.EnableConfig** parameter is set to 'Enable'.

UnitRegistrations (Table: user-defined, 500 lines max.)

This table holds a list of users to register. These users are not tied to a specifiic endpoint.
Note: Endpoint related registration can be specified in table UserAgent

Index (Index) | Table: UnitRegistrations

Type	UInt32
Range	
Script/CLI	SipEp.UnitRegistrations[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.700.1.100

Unique identifier of the row.

Username (Config Parameter) | Table: UnitRegistrations

Type	Text
Range	SIZE(0..255)
Default	
Script/CLI	SipEp.UnitRegistrations[].Username
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.700.1.200

A string that uniquely identifies this user in the domain.

GatewayName (Config Parameter) | Table: UnitRegistrations

Type	Text
Range	
Default	all
Script/CLI	SipEp.UnitRegistrations[].GatewayName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.700.1.250

Selects on which SIP gateway the unit registration is applied. The value must match the gateway name as defined in the **Gateway.Name** parameter.

The value 'all' means all gateways.

Delete (Row Command) | Table: UnitRegistrations

Script/CLI:	SipEp.UnitRegistrations[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.700.1.300

Delete this row.

BehaviorOnInitialRegistrationReception (Config Parameter)

Type	Enum
Range	NoRegistration(100) | EndpointRegistration(200) | UnitRegistration(300) | UnitAndEndpointRegistration(400)
Default	NoRegistration
Script/CLI	SipEp.BehaviorOnInitialRegistrationReception
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.900

Configures the behaviour upon reception of a 380 or 504 carrying an XML body with a specified 'initial-registration' action.

- NoRegistration: No registration refresh are sent upon reception of the message.
- EndpointRegistration: Registration refresh of the endpoint associated with the call is sent upon reception of the message.
- UnitRegistration: Registration refresh of all the usernames configured as 'unit registration' are sent upon reception of the message.
- UnitAndEndpointRegistration: Registration refresh of the endpoint associated with the call and of all the usernames configured as 'unit registration' are sent upon reception of the message.

If the registration(s) succeed, then the call is re-attempted. If the registration(s) fail, then the call is terminated.
See also the **RegistrationDelayOnInitialRegistrationReception** parameter.

RegistrationDelayOnInitialRegistrationReception (Config Parameter)

Type	UInt32
Range	0..5000
Default	0
Script/CLI	SipEp.RegistrationDelayOnInitialRegistrationReception
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.1000

This parameter is only used when the **BehaviorOnInitialRegistrationReception** parameter is configured to a value other than 'NoRegistration'. This parameter configures the time interval between the unregistration confirmation (or final response) and the registration attempt that follows.

Note: This parameter only applies on registration refresh triggered by the **BehaviorOnInitialRegistrationReception** feature.

This value is expressed in milliseconds (ms).

See also the **BehaviorOnInitialRegistrationReception** parameter.

RegistrationStatus (Table)

This table holds a list of current registration.

Index (Index) | Table: RegistrationStatus

Type	UInt32
Range	
Script/CLI	SipEp.RegistrationStatus[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.10000.1.100

Unique identifier of the row.

Gateway (Status Parameter) | Table: RegistrationStatus

Type	Text
Range	
Script/CLI	SipEp.RegistrationStatus[].Gateway
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.10000.1.200

The SIP gateway used to register.

Endpoint (Status Parameter) | Table: RegistrationStatus

Type	Text
Range	
Script/CLI	SipEp.RegistrationStatus[].Endpoint
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.10000.1.300

The endpoint related to this registration.
The parameter is empty for generic unit registration not related to an endpoint.

State (Status Parameter) | Table: RegistrationStatus

Type	Enum
Range	Unregistered(100) | Registering(200) | Registered(300) | Refreshing(400) | Unregistering(500) | Unreachable(600) | AuthFailed(700) | Rejected(800) | ConfigError(900) | InvalidResponse (1000)
Script/CLI	SipEp.RegistrationStatus[].State
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.10000.1.400

The current state of the registration.

- Unregistered: The registration is not registered and never tries to register. This case occurs if the network interface used by the SIP gateway is not up or the unit/endpoint is locked.
- Registering: The registration is currently trying to register.
- Registered: The registration is successfully registered.
- Refreshing: The registration is trying to refresh.
- Unreachable: The last registration attempt failed because the registrar is unreachable.

- AuthFailed: The last registration attempt failed because authentication was not successful.
- Rejected: The last registration attempt failed because the registrar rejects the registration.
- ConfigError: The last registration attempt failed because it was badly configured. Check if the username to register and the registrar host are not empty.
- InvalidResponse: The received 200 OK response contact do not match the contact of the register. Or the 200 OK response for an un-register contains contact.

Registrar (Status Parameter) | Table: RegistrationStatus

Type	Text
Range	
Script/CLI	SipEp.RegistrationStatus[].Registrar
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.10000.1.500

The host of the registrar currently used by the registration.

Username (Status Parameter) | Table: RegistrationStatus

Type	Text
Range	
Script/CLI	SipEp.RegistrationStatus[].Username
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.800.10000.1.600

The username currently used by the registration.

TransportAddRPortEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.TransportAddRPortEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.10

Indicates whether or not the rport parameter should be added to the Via header field, as defined in RFC 3581.
Enabling this parameter may help in some NAT-traversal use-cases (if supported by the server).

TransportPersistentBasePort (Config Parameter)

Type	UInt32
Range	1025..64535
Default	16000
Script/CLI	SipEp.TransportPersistentBasePort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.50

Base port used to establish persistent connections with SIP servers.
When the SipEp service creates a persistent connection, the local SIP port for that connection is the first available port starting from the last Persistent base port value used.

See also the **TransportPersistentPortInterval** parameter.

TransportPersistentPortInterval (Config Parameter)

Type	UInt32
Range	0..0 | 100..1000
Default	0
Script/CLI	SipEp.TransportPersistentPortInterval
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.55

Interval used to cycle through a range of ports. That last available port is the sum of **TransportPersistentBasePort** and **TransportPersistentPortInterval** values.

After a reboot, the last SIP port used is remembered and the following ports are used, instead starting from the base port.

If set to '0', the cycle mechanism is disabled.

See also the **TransportPersistentBasePort** parameter.

TransportPersistentDisconnectOnSipTransmissionError (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	SipEp.TransportPersistentDisconnectOnSipTransmissionError
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.60

When enabled, resets the persistent connection when a SIP transmission error occurs.

TransportPersistentDisconnectOnSipTransmissionErrorEpGw (Config Parameter)

Type	Enum
Range	All(100) | Register(200)
Default	Register
Script/CLI	SipEp.TransportPersistentDisconnectOnSipTransmissionErrorEpGw
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.62

Specifies which SIP request types transmission errors will trigger a disconnection of a TCP persistent connection.

- All: Disconnect on any SIP request type transmission error.
- Register: Disconnect on SIP REGISTER transmission error only.

TransportCriticalConnectionFailureMaxCount (Config Parameter)

Type	UInt32
Range	0..100
Default	0
Script/CLI	SipEp.TransportCriticalConnectionFailureMaxCount
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.65

Specifies the maximum number of consecutive network error occurrences (TCP reject or TCP timeout) to the same destination to trigger a critical network connection failure. When the failure is

trigggered, the associated SIP gateway is restarted to force the usage of a different local persistent port.

The new port is taken from the persistent port interval defined by the **TransportPersistentPortInterval** parameter.

A typical usage is in environments where a firewall can block the source port used by a gateway.

Setting the value to '0' disables the parameter.

Notes:

- This parameter only supports trunk gateways. It does not support endpoint gateways nor SipProxy.
- This parameter is ignored when the **TransportPersistentPortInterval** parameter is set 0.

TransportFailbackInterval (Config Parameter)

Type	UInt32
Range	5..3600
Default	15
Script/CLI	SipEp.TransportFailbackInterval
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.75

Time interval before retrying the establishment of a persistent connection.
This value is the interval that the device waits before retrying periodically to establish a persistent connection to the highest priority target. This timer is started when a persistent connection goes down or fails to connect to the destination.

See also the **DefaultSipFailoverConditions** and **GwSpecificFailover.SipFailoverConditions** parameters.

This value is expressed in seconds (s).

TransportTlsCertificateTrustLevel (Config Parameter)

Type	Enum
Range	LocallyTrusted(100) | OcspOptional(200) | OcspMandatory(300)
Default	LocallyTrusted
Script/CLI	SipEp.TransportTlsCertificateTrustLevel
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.85

Define how a peer certificate is considered trusted for a TLS connection.

- LocallyTrusted: A certificate is considered trusted when the certificate authority (CA) that signed the peer certificate is present in the **Cert.OthersCertificatesInfo** table. The certificate revocation status is not verified.
- OcspOptional: A certificate is considered trusted when it is locally trusted and is not revoked by its certificate authority (CA). The certificate revocation status is queried using the Online Certificate Status Protocol (OCSP). If the OCSP server is not available or the verification status is unknown, the certificate is considered trusted.
- OcspMandatory: A certificate is considered trusted when it is locally trusted and is not revoked by its certificate authority (CA). The certificate revocation status is queried using the Online Certificate Status Protocol (OCSP). If the OCSP server is not available or the verification status is unknown, the certificate is considered not trusted.

TransportTlsCipherSuite (Config Parameter)

Type	Enum
Range	CS1(100) | CS2(200) | CS3(300)
Default	CS1
Script/CLI	SipEp.TransportTlsCipherSuite
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.90

Defines the allowed cipher suites when using TLS persistent connections.

- CS1:
  - TLS_DHE_DSS_WITH_AES_128_CBC_SHA
  - TLS_DHE_DSS_WITH_AES_256_CBC_SHA
  - Also includes ciphers from CS2 and CS3 below
- CS2:
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - Also includes ciphers from CS3 below

- CS3:
  - The following are TLS 1.2 ciphers:
  - TLS_RSA_WITH_AES_128_CBC_SHA256
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_CBC_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
  - The following are TLS 1.3 ciphers:
  - TLS_AES_256_GCM_SHA384
  - TLS_AES_128_GCM_SHA256
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_CCM_8_SHA256
  - TLS_AES_128_CCM_SHA256

TransportTlsVersion (Config Parameter)

Type	Enum
Range	TLSv1(200) | TLSv1_1(300) | TLSv1_2 (400) | TLSv1_3 (500)
Default	TLSv1
Script/CLI	SipEp.TransportTlsVersion
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.95

Defines the allowed TLS versions when using TLS persistent connections.

- TLSv1: Allow TLS versions 1 and up.

- TLSv1_1: Allow TLS versions 1.1 and up.
- TLSv1_2: Allow TLS versions 1.2 and up.
- TLSv1_3: Allow TLS version 1.3 only.

The device will always send its highest supported TLS version in the ClientHello message. The server will select the highest supported TLS version it supports from the ClientHello message. The device will then validate that the selected version is allowed. If the version is not allowed the device will close the connection.

TransportConfig (Table)

This table contains the informations pertaining to the supported transports. It is indexed by gateway name.
Note that the transport used for the entire unit is always the transport configured in the first row of this table. Consequently when a transport is configured on a specific row (gateway), the configuration is also applied to all rows (gateways). This characteristic could possibly change when the unit will be able to support different transports.

GatewayName (Index) | Table: TransportConfig

Type	Text
Range	
Script/CLI	SipEp.TransportConfig[].GatewayName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.100.1.100

String that identifies a SIP gateway in other tables.

RegistrationEnable (Config Parameter) | Table: TransportConfig

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.TransportConfig[].RegistrationEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.100.1.200

Indicates whether or not the SIP Gateway must include its supported transports in its registrations. If enabled, then the gateway registers with one contact for each transport that is currently enabled. Each of these contacts contains a 'transport' parameter.

ContactEnable (Config Parameter) | Table: TransportConfig

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.TransportConfig[].ContactEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.100.1.300

Indicates whether or not the SIP Gateway must include its supported transport in all SIP messages that have the contact header, except for the REGISTER message (see the **RegistrationEnable** parameter).

If enabled, then the gateway sends SIP messages with the 'transport' parameter in the contact header.

When secure transport is not selected, it is either set to 'transport=tcp' when TCP is enabled and UDP is disabled, 'transport=udp' when UDP is enabled and TCP disabled or no transport parameter when both TCP and UDP are enabled. When secure transport is selected, it is set to 'transport=tls'.

UdpEnable (Config Parameter) | Table: TransportConfig

Type	EnableDisable
Range	
Default	Enable
Script/CLI	SipEp.TransportConfig[].UdpEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.100.1.400

Enables or disables the UDP transport.
Note that the UDP and TLS transports are mutually exclusive. The TLS transport cannot be used with the UDP transport.

UdpQValue (Config Parameter) | Table: TransportConfig

Type	Text
Range	Size(0..5)
Default	
Script/CLI	SipEp.TransportConfig[].UdpQValue
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.100.1.500

Indicates the priority of the UDP transport.
A qvalue parameter is added to each contact. This only applies if the transport-specific registration is enabled (see the **TransportRegistrationEnable** parameter).

Qvalues give each transport a weight, indicating the degree of preference for that transport. A higher value means higher preference.

The format of the qvalue string must follow the RFC 3261 ABNF (a floating point value between 0.000 and 1.000). If an empty string is specified, no qvalue is set in the contacts.

TcpEnable (Config Parameter) | Table: TransportConfig

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.TransportConfig[].TcpEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.100.1.600

Enables or disables the TCP transport.
Note that the TCP and TLS transports are mutually exclusive. The TLS transport cannot be used with the TCP transport.

TcpQValue (Config Parameter) | Table: TransportConfig

Type	Text
Range	Size(0..5)
Default	
Script/CLI	SipEp.TransportConfig[].TcpQValue
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.100.1.700

Indicates the priority of the TCP transport.
A qvalue parameter is added to each contact. This only applies if the transport-specific registration is enabled (see the **TransportRegistrationEnable** parameter).

Qvalues give each transport a weight, indicating the degree of preference for that transport. A higher value means higher preference.

The format of the qvalue string must follow the RFC 3261 ABNF (a floating point value between 0.000 and 1.000). If an empty string is specified, no qvalue is set in the contacts.

TlsEnable (Config Parameter) | Table: TransportConfig

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.TransportConfig[].TlsEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.100.1.800

Enables or disables the TLS transport.
Note that the TLS transport is exclusive to UDP and TCP transport. The TLS transport cannot be used with the TCP or UDP transport.

TlsQValue (Config Parameter) | Table: TransportConfig

Type	Text
Range	Size(0..5)
Default	
Script/CLI	SipEp.TransportConfig[].TlsQValue
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.100.1.900

Indicates the priority of the TLS transport.
A qvalue parameter is added to each contact. This only applies if the transport-specific registration is enabled (see the **TransportRegistrationEnable** parameter).

Qvalues give each transport a weight, indicating the degree of preference for that transport. A higher value means higher preference.

The format of the qvalue string must follow the RFC 3261 ABNF (a floating point value between 0.000 and 1.000). If an empty string is specified, no qvalue is set in the contacts.

TlsPersistentConnectionStatus (Table)

This table holds the status of the TLS persistent connections.

Index (Index) | Table: TlsPersistentConnectionStatus

Type	UInt32
Range	
Script/CLI	SipEp.TlsPersistentConnectionStatus[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.10000.1.100

Unique identifier of the row.

Gateway (Status Parameter) | Table: TlsPersistentConnectionStatus

Type	Text
Range	
Script/CLI	SipEp.TlsPersistentConnectionStatus[].Gateway
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.10000.1.200

The SIP gateway used to register.

LocalPort (Status Parameter) | Table: TlsPersistentConnectionStatus

Type	ExtIpPort
Range	
Script/CLI	SipEp.TlsPersistentConnectionStatus[].LocalPort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.10000.1.300

Local port used by the TLS persistent connection.

RemoteHost (Status Parameter) | Table: TlsPersistentConnectionStatus

Type	Text
Range	
Script/CLI	SipEp.TlsPersistentConnectionStatus[].RemoteHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.10000.1.400

The remote host used to establish the TLS persistent connection. The remote host can be a host name or an IP address of the proxy, outbound proxy or registrar.

RemoteHostIpAddr (Status Parameter) | Table: TlsPersistentConnectionStatus

Type	Text
Range	
Script/CLI	SipEp.TlsPersistentConnectionStatus[].RemoteHostIpAddr
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.10000.1.450

The resolved IP address of the remote host used to establish the TLS persistent connection.

State (Status Parameter) | Table: TlsPersistentConnectionStatus

Type	Enum
Range	Up(100) | Down(200) | WaitingShutdown(300) | WaitingUp(400)
Script/CLI	SipEp.TlsPersistentConnectionStatus[].State
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.900.10000.1.500

The current state of the TLS persistent connection.

- Up: The TLS connection is established and ready to be used.
- Down: The TLS connection is not established.
- WaitingShutdown: The TLS connection is established but in a graceful shutdown.
- WaitingUp: The TLS connection is established not yet ready to be used.

DefaultSipFailoverConditions (Config Parameter)

Type	Text
Range	Size(0..512)
Default	5xxOnRegistration
Script/CLI	SipEp.DefaultSipFailoverConditions
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.930.100

Configures additional SIP-level conditions for failover.
Expressed as a sequence of keywords separated by commas. Spaces and tabs are ignored.

Supported keyword list is:

- 5xxOnRegistration: 5xx (Server Failure, i.e. 500 to 599 inclusively) response received to a registration attempt.
- 500OnRegistration: 500 (Server Internal Error) response received to a registration attempt.
- 5xxOnInvite: 5xx (Server Failure, i.e. 500 to 599 inclusively) response received to an INVITE.
- 504OnInvite: 504 (Server Time-Out) response received to an INVITE.

The parameter can accept multiple values, comma-separated. When empty, only the connection-level failover conditions apply.

Note that 5xxOnRegistration and 500OnRegistration are mutually exclusive and cannot be selected together. Same applies to 5xxOnInvite and 504OnInvite.

Note: This parameter only applies to Endpoint gateways.

GwSpecificFailover (Table)

A table of the failover configuration indexed by the SIP gateway name. It is used to override the default value.

GatewayName (Index) | Table: GwSpecificFailover

Type	Text
Range	
Script/CLI	SipEp.GwSpecificFailover[].GatewayName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.930.500.1.100

String that identifies a SIP gateway in other tables.

EnableConfig (Config Parameter) | Table: GwSpecificFailover

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.GwSpecificFailover[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.930.500.1.200

Defines the configuration to use for a specific SIP gateway.

- Disable: The SIP gateway uses the default configuration as defined in the **DefaultSipFailoverCondition** parameter.
- Enable: The endpoint uses the specific configuration as defined in the **GwSpecificFailover.SipFailoverCondition** parameter.

SipFailoverConditions (Config Parameter) | Table: GwSpecificFailover

Type	Text
Range	Size(0..512)
Default	5xxOnRegistration
Script/CLI	SipEp.GwSpecificFailover[].SipFailoverConditions
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.930.500.1.300

Configures additional SIP-level conditions for failover.
Expressed as a sequence of keywords separated by commas. Spaces and tabs are ignored.

Supported keyword list is:

- 5xxOnRegistration: 5xx (Server Failure, i.e. 500 to 599 inclusively) response received to a registration attempt.
- 500OnRegistration: 500 (Server Internal Error) response received to a registration attempt.
- 5xxOnInvite: 5xx (Server Failure, i.e. 500 to 599 inclusively) response received to an INVITE.
- 504OnInvite: 504 (Server Time-Out) response received to an INVITE.

The parameter can accept multiple values, comma-separated. When empty, only the connection-level failover conditions apply.

Note that 5xxOnRegistration and 500OnRegistration are mutually exclusive and cannot be selected together. Same applies to 5xxOnInvite and 504OnInvite.

Note: This parameter only applies to Endpoint gateways.

PenaltyBoxEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.PenaltyBoxEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1000.100

Indicates whether the unit uses the penalty box feature.
The penalty box feature is used when a given host FQDN resolves to a non-responding address. When the address times out, it is put into the penalty box for a given amount of time. During that time, the address in question is considered as 'non-responding' for all requests.

This feature is most useful when using DNS requests returning multiple or varying server addresses. It makes sure that, when a host is down, users wait a minimal amount of time before trying a secondary host.

The penalty box is always 'active'. This means that even if the feature is disabled, IP addresses are marked as invalid, but they are still tried. The advantage is that when the feature is enabled, IP addresses that were already marked as invalid are instantly put into the penalty box.

When enabled, this feature takes effect immediately on the next call attempt.

The penalty box feature is applied only when using UDP or TCP connections established with a FQDN. A similar penalty box feature for the TLS connections is available via the **SipEp.TransportFailbackInterval** parameter.

See also the **PenaltyBoxTime** parameter.

PenaltyBoxTime (Config Parameter)

Type	UInt32
Range	30..7200
Default	300
Script/CLI	SipEp.PenaltyBoxTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1000.200

Amount of time that a host spends in the penalty box.
An IP address is put into the penalty box for the current **PenaltyBoxEnable** parameter. Changing the **PenaltyBoxTime** parameter does not affect IP addresses that are already in the penalty box. In other words, the **PenaltyBoxTime** parameter only affects new entries in the penalty box.

The penalty box feature is applied only when the 'non-responding' destination timeout a non-persistent connection. A similar penalty box feature for the TLS persistent connections is available via the **SipEp.TransportFailbackInterval** parameter.

This value is expressed in seconds (s).

Also see the **PenaltyBoxEnable** parameter.

ErrorMappingSipToCause (Table: user-defined, 40 lines max.)

This table allow the user to override the default mapping for SIP code to ISDN cause.
The default mapping is defined in RFC 3398

SipCode (Index) | Table: ErrorMappingSipToCause

Type	UInt32
Range	400..699
Script/CLI	SipEp.ErrorMappingSipToCause[].SipCode
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1100.100.1.100

SIP code to map to a cause. It's also the unique identifier of the row.
SIP code:

- 400: Bad Request
- 401: Unauthorized
- 402: Payment required
- 403: Forbidden
- 404: Not found
- 405: Method not allowed
- 406: Not acceptable
- 407: Proxy authentication required
- 408: Request timeout
- 410: Gone
- 413: Request Entity too long
- 414: Request-URI too long
- 415: Unsupported media type
- 416: Unsupported URI Scheme
- 420: Bad extension
- 421: Extension Required

- 423: Interval Too Brief
- 480: Temporarily unavailable
- 481: Call/Transaction Does not Exist
- 482: Loop Detected
- 483: Too many hops
- 484: Address incomplete
- 485: Ambiguous
- 486: Busy here
- 500: Server internal error
- 501: Not implemented
- 502: Bad gateway
- 503: Service unavailable
- 504: Server time-out
- 504: Version Not Supported
- 513: Message Too Large
- 600: Busy everywhere
- 603: Decline
- 604: Does not exist anywhere

Cause (Config Parameter) | Table: ErrorMappingSipToCause

Type	UInt32
Range	1..127
Default	127
Script/CLI	SipEp.ErrorMappingSipToCause[].Cause
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1100.100.1.200

Cause to map the the SIP code.
The cause specified in Q.931 are:

Normal event:

- 1: Unassigned (unallocated) number.
- 2: No route to specified transit network.
- 3: No route to destination.
- 6: Channel unacceptable.
- 7: Call awarded and being delivered in an established channel.

- 17: User busy.
- 18: No user responding.
- 19: User alerting, no answer.
- 20: Subscriber absent.
- 21: Call rejected.
- 22: Number changed.
- 23: Redirection to new destination.
- 26: Non-selected user clearing.
- 27: Destination out of order.
- 28: Invalid number format (incomplete number).
- 29: Facility rejected.
- 30: Response to STATUS ENQUIRY.
- 31: Normal, unspecified.

Resource unavailable:

- 34: No circuit/channel available.
- 38: Network out of order.
- 41: Temporary failure.
- 42: Switching equipment congestion.
- 43: Access information discarded.
- 44: Requested circuit/channel not available.
- 47: Resource unavailable, unspecified.

Service or option not available:

- 55: Incoming calls barred within CUG.
- 57: Bearer capability not authorized.
- 58: Bearer capability not presently available.
- 63: Service or option not available, unspecified.

Service or option not implemented:

- 65: Bearer capability not implemented.
- 66: Channel type not implemented.
- 69: Requested facility not implemented.
- 70: Only restricted digital information bearer capability is available.
- 79: Service or option not implemented, unspecified.

Invalid message:

- 81: Invalid call reference value.

- 82: Identified channel does not exist.
- 83: A suspended call exists, but this call identity does not.
- 84: Call identity in use.
- 85: No call suspended.
- 86: Call having the requested call identity has been cleared.
- 87: user not member of CUG.
- 88: Incompatible destination.
- 91: Invalid transit network selection.
- 95: Invalid message, unspecified.

Protocol error:

- 96: Mandatory information element is missing
- 97: Message type non-existent or not implemented
- 98: Message not compatible with call state or message type non-existent or not implemented
- 99: Information element non-existent or not implemented
- 100: Invalid information element contents
- 101: Message not compatible with call state
- 102: Recovery on time expiry
- 111: Protocol error, unspecified

Interworking:

- 127: Interworking, unspecified

Delete (Row Command) | Table: ErrorMappingSipToCause

Script/CLI:	SipEp.ErrorMappingSipToCause[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1100.100.1.300

Delete this row.

ErrorMappingCauseToSip (Table: user-defined, 40 lines max.)

This table allow the user to override the default mapping for ISDN cause to SIP.
The default mapping is defined in RFC 3398

Cause (Index) | Table: ErrorMappingCauseToSip

Type	UInt32
Range	1..127
Script/CLI	SipEp.ErrorMappingCauseToSip[].Cause
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1100.300.1.100

Cause to map the the SIP code. It's also the unique identificator of the row.
The cause specified in Q.931 are:

Normal event:

- 1: Unassigned (unallocated) number.
- 2: No route to specified transit network.
- 3: No route to destination.
- 6: Channel unacceptable.
- 7: Call awarded and being delivered in an established channel.
- 17: User busy.
- 18: No user responding.
- 19: User alerting, no answer.
- 20: Subscriber absent.
- 21: Call rejected.
- 22: Number changed.
- 23: Redirection to new destination.
- 26: Non-selected user clearing.
- 27: Destination out of order.
- 28: Invalid number format (incomplete number).
- 29: Facility rejected.
- 30: Response to STATUS ENQUIRY.
- 31: Normal, unspecified.

Resource unavailable:

- 34: No circuit/channel available.
- 38: Network out of order.
- 41: Temporary failure.
- 42: Switching equipment congestion.
- 43: Access information discarded.

- 44: Requested circuit/channel not available.
- 47: Resource unavailable, unspecified.

Service or option not available:

- 55: Incoming calls barred within CUG.
- 57: Bearer capability not authorized.
- 58: Bearer capability not presently available.
- 63: Service or option not available, unspecified.

Service or option not implemented:

- 65: Bearer capability not implemented.
- 66: Channel type not implemented.
- 69: Requested facility not implemented.
- 70: Only restricted digital information bearer capability is available.
- 79: Service or option not implemented, unspecified.

Invalid message:

- 81: Invalid call reference value.
- 82: Identified channel does not exist.
- 83: A suspended call exists, but this call identity does not.
- 84: Call identity in use.
- 85: No call suspended.
- 86: Call having the requested call identity has been cleared.
- 87: user not member of CUG.
- 88: Incompatible destination.
- 91: Invalid transit network selection.
- 95: Invalid message, unspecified.

Protocol error:

- 96: Mandatory information element is missing
- 97: Message type non-existent or not implemented
- 98: Message not compatible with call state or message type non-existent or not implemented
- 99: Information element non-existent or not implemented
- 100: Invalid information element contents
- 101: Message not compatible with call state
- 102: Recovery on time expiry
- 111: Protocol error, unspecified

Interworking:

- 127: Interworking, unspecified

SipCode (Config Parameter) | Table: ErrorMappingCauseToSip

Type	UInt32
Range	400..699
Default	500
Script/CLI	SipEp.ErrorMappingCauseToSip[].SipCode
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1100.300.1.200

SIP code to map to a cause.
SIP code:

- 400: Bad Request
- 401: Unauthorized
- 402: Payment required
- 403: Forbidden
- 404: Not found
- 405: Method not allowed
- 406: Not acceptable
- 407: Proxy authentication required
- 408: Request timeout
- 410: Gone
- 413: Request Entity too long
- 414: Request-URI too long
- 415: Unsupported media type
- 416: Unsupported URI Scheme
- 420: Bad extension
- 421: Extension Required
- 423: Interval Too Brief
- 480: Temporarily unavailable
- 481: Call/Transaction Does not Exist
- 482: Loop Detected
- 483: Too many hops
- 484: Address incomplete
- 485: Ambiguous
- 486: Busy here

- 500: Server internal error
- 501: Not implemented
- 502: Bad gateway
- 503: Service unavailable
- 504: Server time-out
- 504: Version Not Supported
- 513: Message Too Large
- 600: Busy everywhere
- 603: Decline
- 604: Does not exist anywhere

Delete (Row Command) | Table: ErrorMappingCauseToSip

Script/CLI:	SipEp.ErrorMappingCauseToSip[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1100.300.1.300

Delete this row.

ReasonHeaderSupport (Config Parameter)

Type	Enum
Range	None(100) | SendQ850(200) | ReceiveQ850(300) | SendReceiveQ850(400)
Default	None
Script/CLI	SipEp.ReasonHeaderSupport
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1100.500

Configures how the unit handles the SIP Reason header.

- None: Silently ignore any incoming SIP Reason headers. Do not send the SIP Reason header.
- SendQ850: Silently ignore incoming SIP Reason headers. Send the SIP Reason header with a Q.850 code. When the original Q.850 code is available from an ISDN interface, this code is used. When no original Q.850 code is available, a Q.850 code is used to represent the actual cause. The Reason code sent is not affected by the entries in the **ErrorMappingSipToCause** table. These SIP Reason headers are sent in the following SIP messages:
  - In all 4xx, 5xx, and 6xx responses to an original INVITE.
  - In all CANCEL requests.
  - In all BYE requests.

- ReceiveQ850: Relay the Q.850 code in the incoming SIP Reason headers to the telephony interface if it is an ISDN interface. When received, the Q.850 Reason code supersedes any entries in the **ErrorMappingSipToCause** table. Do not send the SIP Reason header.
- SendReceiveQ850: Send the SIP Reason headers as when set to SendQ850. Relay the Q.850 code in the incoming SIP Reason headers as when set to ReceiveQ850.

SipKeepAliveMethod (Config Parameter)

Type	Enum
Range	None(100) | SipOptions(200) | Ping(300) | TcpKeepAlive(400)
Default	None
Script/CLI	SipEp.SipKeepAliveMethod
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1300.100

Method used to perform the SIP Keep-Alive. The Keep-Alive mechanism generates an activity between the SIP gateway and the remote end. If the mechanism is unable to reach the remote end, the SIP gateway is disconnected.

- None: No Keep-Alive is performed.
- SipOptions: SIP OPTIONS are sent periodically for each gateway to the corresponding server. Any response received from the server means that it is reachable. No additional processing is performed on the response. If no response is received after the retransmission timer expires (configurable via the **InteropTransmissionTimeout** parameter), the gateway considers the server as unreachable. In this case, any call attempt through the gateway is refused. SIP OPTIONS are still sent when the server is unreachable and as soon as it becomes reachable again, new calls are allowed.
- Ping: A Ping is sent periodically for each gateway to the corresponding server. The response received from the server means that it is reachable. If no response is received after the retransmission timer expires (sipTransmissionTimeout), the gateway considers the server as unreachable. In this case, any call attempt through the gateway is refused. The Pings are still sent when the server is unreachable and as soon as it becomes reachable again, new calls are allowed.
- TcpKeepAlive: For TCP and TLS connections, a small Keep-Alive packet is periodically sent to probe an idle connection. The connection is terminated if the remote end failed to reply after a few retries, configurable through the **SipEp.SipKeepAliveRetry** parameter. The delay between two Keep-Alive transmissions is configurable with the **SipEp.SipKeepAliveInterval** parameter.

Note: The SipOptions and Ping methods are only available for Trunk gateways, See the **Gateway.Type** parameter.

SipKeepAliveInterval (Config Parameter)

Type	UInt32
Range	1..3600
Default	30
Script/CLI	SipEp.SipKeepAliveInterval
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1300.200

Interval at which Sip Keep-Alive requests using *SipOptions*, *Ping* or *TcpKeepAlive* are sent to verify the server status.
This value is expressed in seconds (s).

SipKeepAliveRetry (Config Parameter)

Type	UInt32
Range	0..10
Default	3
Script/CLI	SipEp.SipKeepAliveRetry
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1300.210

Specifies the number of retransmissions to be carried out before considering the remote end as unavailable and closing the connection.
Note: Only available when the **SipKeepAliveMethod** parameter is configured to *TcpKeepAlive*.

SipKeepAliveDestination (Config Parameter)

Type	Enum
Range	FirstSipDestination(100) | AlternateDestination(200)
Default	FirstSipDestination
Script/CLI	SipEp.SipKeepAliveDestination
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1300.300

Determines the behaviour of the device when performing the Keep-Alive action.

- FirstSipDestination: Perform the Keep-Alive action through the first SIP destination. This corresponds to the outbound proxy host when specified, otherwise it is the proxy host.

- AlternateDestination: Perform the Keep-Alive action through the alternate destination target (refer to the **GwKeepAliveAlternateDestination** parameter).

Note: Only available when the **SipKeepAliveMethod** parameter is configured to *SipOptions* or *Ping*.

GwKeepAliveAlternateDestination (Table)

A table of Keep-Alive destination alternate target indexed by the SIP gateway name. It is used to override the default value when the **SipKeepAliveDestination** parameter is set to "AlternateDestination". If the **TlsEnable** parameter is set to "Enable", the persistent connection maintains the Keep-Alive action as well as with the default proxy in addition to the alternate destination.

GatewayName (Index) | Table: GwKeepAliveAlternateDestination

Type	Text
Range	
Script/CLI	SipEp.GwKeepAliveAlternateDestination[].GatewayName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1300.400.1.100

String that identifies a SIP gateway in other tables.

AlternateDestination (Config Parameter) | Table: GwKeepAliveAlternateDestination

Type	IpHostNamePort
Range	
Default	192.168.0.10:0
Script/CLI	SipEp.GwKeepAliveAlternateDestination[].AlternateDestination
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1300.400.1.200

Alternate destination target server FQDN and port for a specific SIP gateway.

UasPrackSupport (Config Parameter)

Type	Enum
Range	Unsupported(200) | Supported(300)
Default	Unsupported
Script/CLI	SipEp.UasPrackSupport
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1400.100

Determines the support of RFC 3262 (PRACK) when acting as a user agent server.

- Unsupported: The option tag "100rel" is ignored if present in the Supported or Required headers of received initial INVITEs and provisional responses are not sent reliably as per RFC 3261.
- Supported: If the option tag "100rel" is present in the Supported or Required header of initial received INVITEs, provisional responses are sent reliably as per RFC 3262 by adding the option tag "100rel" to the Require header.

Receiving an UPDATE request to negotiate "early media" is supported only if the **UasPrackSupport** parameter is set to 'Supported'.

UacPrackSupport (Config Parameter)

Type	Enum
Range	Unsupported(200) | Supported(300) | Required(400)
Default	Unsupported
Script/CLI	SipEp.UacPrackSupport
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1400.200

Determines the support of RFC 3262 (PRACK) when acting as a user agent client.

- Unsupported: The option tag "100rel" is not added in the Supported or Required headers of sent INVITEs as per RFC 3261. If the provisional response contains a "Require" header field with the option tag "100rel", the indication is ignored and no PRACK are sent.
- Supported: The option tag "100rel" is added to the Supported header of sent initial INVITEs as per RFC 3262. If the received provisional response contains a Require header field with the option tag "100rel", the response is to be sent reliably using the PRACK method.
- Required: The option tag "100rel" is added to the Require header of sent initial INVITEs as per RFC 3262. If the received provisional response contains a Require header field with the option tag "100rel", the response is to be sent reliably using the PRACK method.

AnswerCodecNegotiation (Config Parameter)

Type	Enum
Range	AllCommonLocalPriority(100) | FirstCommonLocalPriority(200) | AllCommonPeerPriority(300) | FirstCommonPeerPriority(400)
Default	AllCommonLocalPriority
Script/CLI	SipEp.AnswerCodecNegotiation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1500.100

Defines the codec negotiation rule when generating a SDP answer.

- AllCommonLocalPriority : When generating an answer to an offered session, all common codecs are listed in the local order of priority. The local priority is defined for each codec in the Mipt service.
- FirstCommonLocalPriority : When generating an answer to an offered session, only the first common codec with the higher local priority is listed. The local priority is defined for each codec in the Mipt service.
- AllCommonPeerPriority : When generating an answer to an offered session, all common codecs are listed. The codecs order is the same as in the peer offer.
- FirstCommonPeerPriority : When generating an answer to an offered session, only the first common codec is listed. The codecs order is the same as in the peer offer.

DiversionConfig (Table)

A table of the call diversion configuration indexed by the SIP gateway name.

GatewayName (Index) | Table: DiversionConfig

Type	Text
Range	
Script/CLI	SipEp.DiversionConfig[].GatewayName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1600.100.1.100

String that identifies a SIP gateway in other tables.

Method (Config Parameter) | Table: DiversionConfig

Type	Enum
Range	None(100) | DiversionHeader(200)
Default	None
Script/CLI	SipEp.DiversionConfig[].Method
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1600.100.1.200

Selects the SIP method used to receive/send call diversion information in an INVITE.

- None: No diversion information is sent in SIP messages.
- DiversionHeader: The SIP gateway supports the SIP header 'Diversion' (RFC 5806) in received and sent INVITEs, as well as in 302 messages.

SupportedDnsQueries (Config Parameter)

Type	Enum
Range	Address(100) | Srv(200) | Naptr(300)
Default	Naptr
Script/CLI	SipEp.SupportedDnsQueries
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1700.100

Specify the type of DNS queries that the SipEp service supports and uses.

- Address: Sends only Address requests (type A or AAAA, based on the value of the **DnsIpVersion** parameter).
- Srv: Sends a Service request (type SRV) first and then Address requests (type A) if needed.
- Naptr: Sends a Naming Authority Pointer request (type NAPTR) first and then Service requests (type SRV) or Address requests (type A) as needed.

DnsFailureConcealment (Config Parameter)

Type	Enum
Range	None(100) | OnNoResolution(300)
Default	None
Script/CLI	SipEp.DnsFailureConcealment
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1700.200

Configures the way failed DNS queries are handled.

- None: When a DNS query times-out or returns an error, the SIP transaction fails.
- OnNoResolution: When a DNS query times-out or returns an error, the result from the last succesful query for the same FQDN is used.

Note: This parameter applies only to the 'Endpoint' type Gateways.

DnsIpVersion (Config Parameter)

Type	Enum
Range	IpV4Only(100) | IpV4Preferred(200)
Default	IpV4Preferred
Script/CLI	SipEp.DnsIpVersion
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1700.300

Configures which versions of IP are supported or enabled for DNS queries made for SIP requests.

- Ipv4Only: The DNS queries for SIP requests only support IPv4.
- Ipv4Preferred: The DNS queries for SIP requests support both IPv4 and IPv6: If both are resolved successfully, IPv4 will be used.

DefaultStaticMessagingHost (Config Parameter)

Type	IpHostNamePort
Range	
Default	192.168.10.10:0
Script/CLI	SipEp.DefaultStaticMessagingHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1800.100

Messaging server FQDN and port.
A Messaging system host is a server that accepts MWI SUBSCRIBE requests and places the information it receives in those requests into the location service for the domain it handles.

Note: If the host corresponds to a domain name that is bound to a SRV record, the port must be set to 0 for the unit to perform DNS SRV queries; otherwise only type A record lookups will be used.

When the Sbc service is available, the special macro '%sbc%' can be entered to use the SBC as the destination host. This macro resolves to the IP address and port of the 'loop_s' signaling interface in the Sbc service.

If the special macro %sbc% is used in the home domain proxy, then the registration and messaging hosts must be either set to %sbc% or left empty.

If a specific configuration is set in the **GwSpecificMwi.MessagingHost** parameter and the **GwSpecificMwi.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultUsernameInRequestUriEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.DefaultUsernameInRequestUriEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1800.110

Indicates whether or not the unit adds the username in the request URI of MWI SUBSCRIBE requests.

- enable: The unit adds the username in the Request-URI of sent MWI SUBSCRIBE requests.
- disable: No username in Request-URI of MWI SUBSCRIBE requests sent by the unit.

If a specific configuration is set in the **GwSpecificMwi.UsernameInRequestUriEnable** parameter and the **GwSpecificMwi.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

GwSpecificMwi (Table)

A table of the MWI subscription configuration indexed by the SIP gateway name. It is used to override the default value.

GatewayName (Index) | Table: GwSpecificMwi

Type	Text
Range	
Script/CLI	SipEp.GwSpecificMwi[].GatewayName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1800.200.1.100

String that identifies a SIP gateway in other tables.

EnableConfig (Config Parameter) | Table: GwSpecificMwi

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.GwSpecificMwi[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1800.200.1.200

Defines the configuration to use for a specific SIP gateway.

- Disable: The SIP gateway uses the default configuration as defined in the **DefaultStaticMessagingHost** and **DefaultUsernameInRequestUriEnable** parameters.
- Enable: The endpoint uses the specific configuration as defined in the **GwSpecificMwi.MessagingHost** and **GwSpecificMwi.UsernameInRequestUriEnable** parameters.

MessagingHost (Config Parameter) | Table: GwSpecificMwi

Type	IpHostNamePort
Range	
Default	192.168.10.10:0
Script/CLI	SipEp.GwSpecificMwi[].MessagingHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1800.200.1.300

Messaging server FQDN and port.
When the Sbc service is available, the special macro '%sbc%' can be entered to use the SBC as the destination host. This macro resolves to the IP address and port of the 'loop_s' signaling interface in the Sbc service.

If the special macro %sbc% is used in the home domain proxy, then the registration and messaging hosts must be either set to %sbc% or left empty.

UsernameInRequestUriEnable (Config Parameter) | Table: GwSpecificMwi

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.GwSpecificMwi[].UsernameInRequestUriEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1800.200.1.400

Indicates whether or not the unit adds the username in the request URI of MWI SUBSCRIBE requests.

- enable: The unit adds the username in the Request-URI of sent MWI SUBSCRIBE requests.
- disable: No username in Request-URI of MWI SUBSCRIBE requests sent by the unit.

MwiStatus (Table)

Index (Index) | Table: MwiStatus

Type	UInt32
Range	
Script/CLI	SipEp.MwiStatus[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1800.300.1.100

Unique identifier of the row.

GatewayName (Status Parameter) | Table: MwiStatus

Type	Text
Range	
Script/CLI	SipEp.MwiStatus[].GatewayName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1800.300.1.200

The SIP gateway used for this subscription.

SubscriptionState (Status Parameter) | Table: MwiStatus

Type	Enum
Range	Unsubscribed(100) | Subscribing(200) | Subscribed(300) | Refreshing(400) | Unsubscribing(500) | Unreachable(600) | AuthFailed(700) | Rejected(800) | ConfigError(900) | InvalidResponse (1000) | Error (1100)
Script/CLI	SipEp.MwiStatus[].SubscriptionState
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1800.300.1.300

The current state of the subscription.

- Unsubscribed: The unit/endpoint is not subscribed and never tries to subscribe. This case occurs if the network interface used by the SIP gateway is not up or the unit/ endpoint is locked.
- Subscribing: The subscription is currently trying to subscribe.
- Subscribed: The subscription is successfully subscribed.
- Refreshing: The subscription is trying to refresh.
- Unreachable: The last subscription attempt failed because the messaging server is unreachable.

- AuthFailed: The last subscription attempt failed because authentication was not successful.
- Rejected: The last subscription attempt failed because the messaging server rejects the subscription.
- ConfigError: The last subscription attempt failed because it was badly configured. Check if the username and the messaging host are not empty.
- InvalidResponse: The received 200 OK response contact does not match the contact of the messaging server, or the 200 OK response for an un-subscribe contains a contact.
- Error: The last subscription attempt failed for unspecified reason. This may occur on an 'Endpoint' gateway preventing a subscription until registration is completed

Endpoint (Status Parameter) | Table: MwiStatus

Type	Text
Range	
Script/CLI	SipEp.MwiStatus[].Endpoint
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1800.300.1.400

The endpoint related to this subscription.

MessagingHost (Status Parameter) | Table: MwiStatus

Type	Text
Range	
Script/CLI	SipEp.MwiStatus[].MessagingHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1800.300.1.500

Messaging server FQDN and port used to subscribe the event state.

Username (Status Parameter) | Table: MwiStatus

Type	Text
Range	
Script/CLI	SipEp.MwiStatus[].Username
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1800.300.1.600

The username currently used by the subscription.

DefaultStaticConferenceServerUri (Config Parameter)

Type	Text
Range	SIZE(0..255)
Default	
Script/CLI	SipEp.DefaultStaticConferenceServerUri
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1900.100

URI used in the Request-URI of the INVITE sent to the conference server as defined in RFC 4579. This parameter only has an effect when the conference type is 'ConferenceServer'. See the **EpServ.DefaultConferenceType** parameter.

Please refer to the documentation shipped with your device for more details regarding this parameter's semantics.

If a specific configuration is set in the **GwSpecificConference.ServerUri** parameter and the **GwSpecificConference.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

Rfc4579ConferenceErrorRecovery (Config Parameter)

Type	Enum
Range	Rfc4579WithoutErrorRecovery(100) | Rfc4579WithErrorRecovery(200)
Default	Rfc4579WithErrorRecovery
Script/CLI	SipEp.Rfc4579ConferenceErrorRecovery
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1900.200

This parameter determines the mechanism used to establish a conference and how the participants are connected to the conference server.

- Rfc4579WithoutErrorRecovery: The connection with the conference server is made as defined in RFC 4579. The participants are connected to the conference server by sending the REFERs simultaneously, without waiting for a REFER to be completed before issuing the next REFER. The connection with the participant is terminated if the participant fails to complete the REFER.
- Rfc4579WithErrorRecovery: The connection with the conference server is made as defined in RFC 4579. The participants are connected to the conference server by sending the REFERs sequentially. A REFER must complete before issuing the next REFER. The REFER is not sent to the second participant and the call stays in the same state if the first participant fails to complete the REFER.

GwSpecificConference (Table)

A table of the conference configuration indexed by the SIP gateway name. It is used to override the default value.

GatewayName (Index) | Table: GwSpecificConference

Type	Text
Range	
Script/CLI	SipEp.GwSpecificConference[].GatewayName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1900.1000.1.100

String that identifies a SIP gateway in other tables.

EnableConfig (Config Parameter) | Table: GwSpecificConference

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.GwSpecificConference[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1900.1000.1.200

Defines the configuration to use for a specific SIP gateway.

- Disable: The SIP gateway uses the default configuration as defined in the **DefaultStaticConferenceServerUri** parameter.
- Enable: The endpoint uses the specific configuration as defined in the **GwSpecificConference.ServerUri** parameter.

ServerUri (Config Parameter) | Table: GwSpecificConference

Type	Text
Range	SIZE(0..255)
Default	
Script/CLI	SipEp.GwSpecificConference[].ServerUri
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.1900.1000.1.300

URI used in the Request-URI of the INVITE sent to the conference server as defined in RFC 4579. This parameter only has an effect when the conference type is 'ConferenceServer'. See the **EpServ.DefaultConferenceType** parameter.

Please refer to the documentation shipped with your device for more details regarding this parameter's semantics.

DefaultOutboundPriorityCallRouting (Config Parameter)

Type	Enum
Range	Normal(100) | SkipOutboundProxy(200)
Default	SkipOutboundProxy
Script/CLI	SipEp.DefaultOutboundPriorityCallRouting
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.2000.100

Describes how to route priority calls including emergency calls.

- Normal: Send call using normal SIP call routing to the outbound proxy (if defined) and to the target host (usually the SIP server).
- SkipOutboundProxy: Send call directly to the configured server skipping the outbound proxy.

GwEventHandling (Table)

A table of event handling configuration indexed by SIP gateway.

GatewayName (Index) | Table: GwEventHandling

Type	Text
Range	
Script/CLI	SipEp.GwEventHandling[].GatewayName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.2100.100.1.100

String that identifies a SIP gateway in other tables.

Reboot (Config Parameter) | Table: GwEventHandling

Type	Enum
Range	Rejected(100) | Restart(200)
Default	Rejected
Script/CLI	SipEp.GwEventHandling[].Reboot
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.2100.100.1.200

Specifies how this Sip gateway handles the reception of a 'reboot' SIP NOTIFY message.

- Rejected: The 'reboot' notification is rejected on reception.
- Restart: When receiving a 'Reboot' notification, a restart of the unit is done.

CheckSync (Config Parameter) | Table: GwEventHandling

Type	Enum
Range	Rejected(100) | TransferScript(200) | CwmpInform(300)
Default	Rejected
Script/CLI	SipEp.GwEventHandling[].CheckSync
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.2100.100.1.300

Specifies how this SIP gateway handles the reception of a 'check-sync' SIP NOTIFY message.

- Rejected: The 'check-sync' notification is rejected on reception.
- TransferScript: When receiving a 'check-sync' notification, the `Conf.ConfiguredScriptsTransferAndRun` command is executed and a provisioning request is sent to Virtuo if EMS provisioning is enabled.

- CwmpInform: When receiving a 'check-sync' notification, the Cwmp service sends a TR-069 INFORM message to its configured ACS.

SipMessageSupport (Config Parameter)

Type	Enum
Range	Disabled(100) | AcceptPlainText(200)
Default	Disabled
Script/CLI	SipEp.SipMessageSupport
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.2100.200

Specifies the support of incoming SIP MESSAGE for notifications.

- Disabled: SIP MESSAGEs are rejected with a 405 Method Not Allowed.
- AcceptPlainText: SIP MESSAGEs are accepted if the payload type is text/plain, otherwise the MESSAGE is rejected with a 405 Method Not Allowed.

Accepted MESSAGE are sent to the corresponding FXS endpoint, which will trigger an alert if the **Pots.FxsSipMessageAlertingEnable** parameter is enabled.

This feature is usually used for call forwarding notifications.

ReferredByHeader (Config Parameter)

Type	Enum
Range	None(100) | HeaderOnly(200)
Default	None
Script/CLI	SipEp.ReferredByHeader
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.2200.100

Indicates how the Referred-By header is used when participating in a transfer.

- None: When acting as the transferor (sending the REFER), the REFER does not contain a Referred-By header. When acting as the transferee (receiving the REFER and sending the INVITE to the target), the Referred-By header is not copied from the REFER to the INVITE.
- HeaderOnly: When acting as the transferor (sending the REFER), the Referred-By header contains the SIP URI and the parameters of the transferor. When acting as the transferee (receiving the REFER and sending the INVITE to the target), the Referred-By header is copied from the REFER to the INVITE.

BlindTransferMethod (Config Parameter)

Type	Enum
Range	SemiAttended(100) | SemiAttendedConfirmed(200) | SemiAttendedCancelled(300)
Default	SemiAttended
Script/CLI	SipEp.BlindTransferMethod
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.2200.200

Indicates how the blind transfer is achieved when participating in a transfer as the transferor.

- SemiAttended: When blind transfer is invoked by the transferor, the device does not wait for the 200 OK response before sending the REFER request, causing the call transfer to be executed before the transfer-target answers. The transferee and the target are connected together early and the transferee can hear the ringback from the target until the target answers.
- SemiAttendedConfirmed: When blind transfer is invoked by the transferor, the device waits for receiving the 200 OK from the transfer-target before sending a REFER to the transferee. This is as per RFC 5589 section 7.6, figure 11.
- SemiAttendedCancelled: Similar to SemiAttended but the INVITE to the transfer-target is cancelled when the blind transfer is invoked before receiving a 200 OK. This is as per RFC 5589 section 7.6, Figure 12.

ReferToHeaderUriSource (Config Parameter)

Type	Enum
Range	Aor(100) | ContactUri(200)
Default	Aor
Script/CLI	SipEp.ReferToHeaderUriSource
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.2200.300

Source of the URI inserted in the Refer-To header when acting as a transferor.

- Aor: The URI of the Refer-To header is based on the Address of Record of the transfer target.
- ContactUri: The URI of the Refer-To header is based on the Contact URI of the transfer target.

AocConfig (Table)

A table of the Aoc configuration indexed by the SIP gateway name.

GatewayName (Index) | Table: AocConfig

Type	Text
Range	
Script/CLI	SipEp.AocConfig[].GatewayName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.2300.100.1.100

String that identifies a SIP gateway in other tables.

AocDSupport (Config Parameter) | Table: AocConfig

Type	Enum
Range	Disabled(100) | Transparent(200)
Default	Disabled
Script/CLI	SipEp.AocConfig[].AocDSupport
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.2300.100.1.200

Send/Receive the current charge (D)uring the call in AOC-D messages.

- Disabled: No AOC information is sent. Received AOC information is discarded.
- Transparent: AOC information is forwarded to the peer interface if AOC messages are received from the network.

AocESupport (Config Parameter) | Table: AocConfig

Type	Enum
Range	Disabled(100) | Transparent(200)
Default	Transparent
Script/CLI	SipEp.AocConfig[].AocESupport
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.2300.100.1.300

Send/Receive the total charge at the (E)nd of the call in AOC-E messages.

- Disabled: No AOC information is sent. Received AOC information is discarded.
- Transparent: AOC information is forwarded to the peer interface if AOC messages are received from the network.

UasKpmlSupport (Config Parameter)

Type	Enum
Range	Unsupported(100) | SupportedInDialog(200)
Default	Unsupported
Script/CLI	SipEp.UasKpmlSupport
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.2400.100

Determines the support of RFC 4730 (KPML) when the SIP gateway is acting as a user agent server.

- Unsupported: The KPML SUBSCRIBEs are rejected.
- SupportedInDialog: The KPML SUBSCRIBEs are accepted only when received inside a call dialog.

MediaSecurityAgreementEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.MediaSecurityAgreementEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.2500.100

Determines if the mediasec parameter is supported or not, as defined in the draft-dawes-sipcore-mediasec-parameter IETF draft.

- Disable: The media security agreement mechanism is not supported.
- Enable: The media security agreement mechanism is supported and used accordingly to section 6.1, 6.2, and 6.5 of the mediasec parameter IETF draft.

Once enabled, this parameter adds security headers to the SIP signalling to agree upon the security mechanism to be used for the media, i.e. SRTP with SDES.

Some environments require this parameter to be enabled to support SRTP calls, in which case:

- the **Mipt.DefaultSecurityRtpMode** parameter should be configured to "Secure" or "SecureWithFallback"; and
- the **Mipt.DefaultSecurityKeyManagement** parameter to "Sdes".

PrivacyHeadersInResponse (Config Parameter)

Type	Enum
Range	Unsupported(100) | SupportedPAssertedIdentity(200)
Default	Unsupported
Script/CLI	SipEp.PrivacyHeadersInResponse
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.2600.100

Determines if the usage of privacy and identity headers in responses is supported.

- Unsupported: No privacy or identity headers are added in SIP responses. Privacy and identity headers received in response are ignored.
- SupportedPAssertedIdentity: The P-Asserted-Identity header is added in SIP responses. For received SIP responses, the content of the P-Asserted-Identity header is relayed to the telephony interfaces. Mostly useful with the CONP/COLP supplementary services in ISDN. The supported SIP responses are 180, 183, and 200.

DefaultStaticRtcpXrCollectorUri (Config Parameter)

Type	Text
Range	SIZE(0..255)
Default	
Script/CLI	SipEp.DefaultStaticRtcpXrCollectorUri
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.2700.100

Define the URI for the Request-URI of the collector server that will receive RTCP XR voice quality reports.
The reports are sent through a SIP PUBLISH with an 'vq-rtcpxr' event, as defined in RFC 6035.

A report is usually sent at the end of a call, and may also be sent periodically if the **DefaultRtcpXrPeriodicReportsInterval** parameter is defined.

When empty, the publication of RTCP XR reports is disabled.

Valid SIP URI examples:

- sip:alice@example.com:5070
- sip:alice@example.com
- sip:example.com

If a specific configuration is set in the **GwSpecificRtcpXr.CollectorUri** parameter and the **GwSpecificRtcpXr.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultRtcpXrPeriodicReportsInterval (Config Parameter)

Type	UInt32
Range	0..60
Default	0
Script/CLI	SipEp.DefaultRtcpXrPeriodicReportsInterval
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.2700.200

Configures the interval on which the periodic RTCP XR report are sent.
A value of 0 disables the periodic interval report.

This value is expressed in minutes (min).

If a specific configuration is set in the **GwSpecificRtcpXr.PeriodicReportsInterval** parameter and the **GwSpecificRtcpXr.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

LocalGroup (Config Parameter)

Type	Text
Range	SIZE(0..255)
Default	
Script/CLI	SipEp.LocalGroup
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.2700.300

Defines the LocalGroup sent in the RTCP XR report.
An empty value removes the LocalGroup from the RTCP XR report.

RemoteGroup (Config Parameter)

Type	Text
Range	SIZE(0..255)
Default	
Script/CLI	SipEp.RemoteGroup
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.2700.400

Defines the RemoteGroup sent in the RTCP XR report.
An empty value removes the RemoteGroup from the RTCP XR report.

GwSpecificRtcpXr (Table)

A table of the RTCP XR configuration indexed by the SIP gateway name. It is used to override the default value.

GatewayName (Index) | Table: GwSpecificRtcpXr

Type	Text
Range	
Script/CLI	SipEp.GwSpecificRtcpXr[].GatewayName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.2700.1000.1.100

String that identifies a SIP gateway in other tables.

EnableConfig (Config Parameter) | Table: GwSpecificRtcpXr

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.GwSpecificRtcpXr[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.2700.1000.1.200

Defines the configuration to use for a specific SIP gateway.

- Disable: The SIP gateway uses the default configuration as defined in the **DefaultStaticRtcpXrCollectorUri** parameter.
- Enable: The endpoint uses the specific configuration as defined in the **GwSpecificRtcpXr.CollectorUri** parameter.

CollectorUri (Config Parameter) | Table: GwSpecificRtcpXr

Type	Text
Range	SIZE(0..255)
Default	
Script/CLI	SipEp.GwSpecificRtcpXr[].CollectorUri
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.2700.1000.1.300

Define the URI for the Request-URI of the collector server that will receive RTCP XR voice quality reports.
The reports are sent through a SIP PUBLISH with an 'vq-rtcpxr' event, as defined in RFC 6035.

A report is usually sent at the end of a call, and may also be sent periodically if the **PeriodicReportsInterval** parameter is defined.

When empty, the publication of RTCP XR reports is disabled.

Valid SIP URI examples:

- sip:alice@example.com:5070
- sip:alice@example.com
- sip:example.com

PeriodicReportsInterval (Config Parameter) | Table: GwSpecificRtcpXr

Type	UInt32
Range	0..60
Default	0
Script/CLI	SipEp.GwSpecificRtcpXr[].PeriodicReportsInterval
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.2700.1000.1.400

Configures the interval on which the periodic RTCP XR report are sent.
A value of 0 disables the periodic interval report.

This value is expressed in minutes (min).

UserToUserHeaderInInvite (Config Parameter)

Type	Enum
Range	Unsupported(100) | Supported(200)
Default	Unsupported
Script/CLI	SipEp.UserToUserHeaderInInvite
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.2800.100

Enables the SIP INVITE User-to-User header support.

- Unsupported: No User-to-User header is added to the SIP INVITE. Received SIP INVITE User-to-User headers are ignored.
- Supported: The User-to-User header is supported in the original INVITEs as defined in RFC7433/RFC7434. For received SIP INVITEs, the User-to-User header content is relayed to the ISDN telephony interfaces. The User-to-User header will be added to the original INVITE on reception of the User-to-User information element contained in the ISDN SETUP. The user-to-User header will also be added to the generated SIP INVITE on reception of a SIP REFER containing a User-to-User header.

InteropTransmissionTimeout (Config Parameter)

Type	UInt32
Range	1..32
Default	32
Script/CLI	SipEp.InteropTransmissionTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.400

Changes the time to wait for a response or an ACK before considering a transaction timed out. This corresponds to timers B, F and H for all transport protocols and timer J for UDP. These timers are defined in section A of RFC 3261.
This timeout affects the number of retransmissions. Retransmissions continue to follow the timing guidelines described in RFC 3261.

For example, if using DNS SRV and multiple entries are present, this value is the time spent waiting for answers from each entry.

This value is expressed in seconds (s).

InteropTcpConnectTimeout (Config Parameter)

Type	UInt32
Range	1..127
Default	127
Script/CLI	SipEp.InteropTcpConnectTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.450

Defines the maximum time, in seconds, the unit should try to establish a TCP connection to SIP hosts. This timeout value is useful to have a faster detection of unreachable remote hosts. This timer can also affects the TLS connection establishment time.

InteropSymmetricUdpSourcePortEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	SipEp.InteropSymmetricUdpSourcePortEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.600

Indicates whether the unit always uses the same local port when sending SIP traffic over UDP. Symmetric UDP ports are sometimes needed to traverse NAT/Firewall devices.

Note that when changing this setting, all destinations are automatically thrown out of the penalty box, when applicable.

- enable: SIP signaling sent over UDP originates from the same port as the port on which the user agent is listening. This is configured in the **PortConfig** parameter. When enabled, ICMP messages are not processed, which means that unreachable targets will take longer to detect.
- disable: SIP signaling over UDP uses a randomly-generated originating port. ICMP errors are processed correctly.

Note: This parameter applies only to Trunk gateways. For Endpoint gateways, only symmetric ports are used.

InteropMaxForwardsValue (Config Parameter)

Type	Int32
Range	0..200
Default	70
Script/CLI	SipEp.InteropMaxForwardsValue
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.700

Sets the value used in the Max-Forwards header, in conformance with RFC 3261.

InteropSendUaHeaderEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	SipEp.InteropSendUaHeaderEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.800

Enables/Disables sending of the SIP User-Agent header.

InteropSdpDirectionAttributeEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	SipEp.InteropSdpDirectionAttributeEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.900

Indicates if the SDP direction attribute is supported by the unit.
This parameter is used only when the negotiated media uses an IPv4 address. The application always behaves as if this parameter is set to 'Enable' for media using an IPv6 address.

When disabled, the application uses the RFC 2543 method to put a session on hold:

- No direction attribute is present in the SDP sent by the unit.
- Any direction attribute found in the SDP received from the peer is ignored by the unit.

When enabled, the application uses the RFC 3264 method to put a session on hold:

- The unit always sends the direction attribute in the SDP of an initiated call. For all other SDP messages sent by the unit, refer to the **InteropSdpDetectPeerDirectionAttributeSupportEnable** parameter.
- If present in the SDP, the direction attribute is preferred over the connection address to transmit session modification information.

InteropSdpDetectPeerDirectionAttributeSupportEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	SipEp.InteropSdpDetectPeerDirectionAttributeSupportEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.950

Indicates if the SDP direction attribute support should be autodetected in the SDP received from the peer.
This parameter is used only when the negotiated media uses an IPv4 address and when the **InteropSdpDirectionAttributeEnable** parameter is enabled. The application always behaves as if this parameter is set to 'Disable' for media using an IPv6 address.

When disabled, the unit always sends the direction attribute in the SDP without autodetection of peer support.

When enabled: the initial handshake determines if the peer supports the direction attribute. The direction attribute will be present when the peer supports it.

InteropOnHoldSdpConnectionAddress (Config Parameter)

Type	Enum
Range	HoldAddress(100) | MediaAddress(200)
Default	HoldAddress
Script/CLI	SipEp.InteropOnHoldSdpConnectionAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.975

Indicates the value of the connection address sent in the SDP when an endpoint is on hold and no longer listening to media packets.
This parameter is used only when the negotiated media uses an IPv4 address. The application always behaves as if this parameter is set to 'MediaAddress' for media using an IPv6 address.

- HoldAddress: The connection address sent in the SDP is '0.0.0.0' if the media uses an IPv4 address. This method is described by RFC 2543.
- MediaAddress: The connection address sent in the SDP is the listening address.

InteropOnHoldSdpStreamDirection (Config Parameter)

Type	Enum
Range	Inactive(100) | Sendonly(200)
Default	Inactive
Script/CLI	SipEp.InteropOnHoldSdpStreamDirection
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.1000

Indicates the direction attribute sent in the SDP when putting an endpoint on hold.

- Inactive: The stream is put on hold by marking it as inactive.
- Sendonly: The stream is put on hold by marking it as sendonly. This method is in conformance with RFC 3264.

This configuration has no effect if the **InteropSdpDirectionAttributeEnable** parameter is set to 'Disable'.

InteropOnHoldAnswerSdpStreamDirection (Config Parameter)

Type	Enum
Range	Inactive(100) | Recvonly(200)
Default	Recvonly
Script/CLI	SipEp.InteropOnHoldAnswerSdpStreamDirection
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.1025

Indicates how to set the direction attribute in the SDP when answering a hold offer with the direction attribute 'sendonly'.

- Inactive: The stream is marked as inactive. If the stream uses an IPv4 address, the connection address is set according to the **InteropOnHoldSdpConnectionAddress** parameter.
- Recvonly: If the stream is currently active or receive only, the stream is marked as recvonly and the connection address is set to the IP address of the unit. If the stream is currently send only or inactive, the stream is marked as inactive and the connection address is set according to the **InteropOnHoldSdpConnectionAddress** parameter.

In both cases, no direction attribute is present in the SDP if the **InteropSdpDirectionAttributeEnable** parameter is set to 'Disable'.

InteropSdpDirectionAttributeLevel (Config Parameter)

Type	Enum
Range	MediaOrSessionLevel(100) | MediaAndSessionLevel(200)
Default	MediaOrSessionLevel
Script/CLI	SipEp.InteropSdpDirectionAttributeLevel
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.1050

Preferred location where the stream direction attribute is set.

- MediaOrSessionLevel: If every media have the same direction, the stream direction attribute is only present at session level. Otherwise, the stream direction attribute is only present at media level.
- MediaAndSessionLevel: If every media have the same direction, the stream direction attribute is present both at session level and media level. Otherwise, the stream direction attribute is only present at media level.

InteropLocalRingOnProvisionalResponse (Config Parameter)

Type	Enum
Range	Disable(0) | LocalRingWhenNoEstablishedMediaStream(1) | LocalRingAlways(2)
Default	Disable
Script/CLI	SipEp.InteropLocalRingOnProvisionalResponse
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.1100

Specifies if the local ring should be started upon receiving a '18x Provisional' response without SDP.

- Disable: The local ring is not started on a '18x Provisional' response without SDP, with one exception: the '180 Ringing' without SDP will start the local ring if the media stream is not already established.
- LocalRingWhenNoEstablishedMediaStream: The local ring is started on any '18x Provisional' response without SDP if the media stream is not already established.
- LocalRingAlways: The local ring is always started on any '18x Provisional' response without SDP.

InteropSdpOriginLineSessionIdAndVersionMaxLength (Config Parameter)

Type	Enum
Range	Max32bits(100) | Max64bits(200)
Default	Max64bits
Script/CLI	SipEp.InteropSdpOriginLineSessionIdAndVersionMaxLength
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.1200

The maximum length of the session ID and the session version number in the origin line (o=) of the SDP.

- Max-32bits: The session ID and the session version number are represented with a 32 bit integer. They have a maximum length of 10 digits.
- Max-64bits: The session ID and the session version number are represented with a 64 bit integer. They have a maximum length of 20 digits.

InteropLockDnsSrvRecordPerCallEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.InteropLockDnsSrvRecordPerCallEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.1400

Configures the behaviour of the DNS SRV feature.

- Disable: The behaviour follows RFC 3263.
- Enable: All messages during a call or registration use the same SRV record.

InteropLockDnsSrvRecordForRegister (Config Parameter)

Type	Enum
Range	AlwaysLock(100) | UnlockOnRefresh(200)
Default	AlwaysLock
Script/CLI	SipEp.InteropLockDnsSrvRecordForRegister
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.1420

Defines the behavior of REGISTER requests when the **SipEp.InteropLockDnsSrvRecordPerCallEnable** parameter is enabled.

- AlwaysLock: The registration lock to a DNS record is maintained for periodic refresh requests, unless there is a registration error with the current locked DNS record.
- UnlockOnRefresh: The registration lock to a DNS record is released after a successfull registration. This means that any following registration refresh will try to be sent to the DNS record with the highest priority.

InteropLockDnsSrvRecordWithInviteBoundToRegisterEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.InteropLockDnsSrvRecordWithInviteBoundToRegisterEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.1430

Configures if INVITEs should be sent to the same DNS record target where they registered to.

- Disable: The INVITE requests are independent of the REGISTER.
- Enable: The INVITE requests are sent first to the destination of their last successful REGISTER, bound by their user endpoint registration, if defined. Otherwise, the INVITEs are bound to the unit registration.

It is recommended to enable this parameter if the targets are not synchronized between themselves, or would reject INVITEs registered to another target.

Note: This parameter is ignored if the **SipEp.InteropLockDnsSrvRecordPerCallEnable** parameter is disabled.

InteropRejectCodeForUnsupportedSdpOffer (Config Parameter)

Type	Enum
Range	UnsupportedMediaType(415) | NotAcceptableHere(488)
Default	UnsupportedMediaType
Script/CLI	SipEp.InteropRejectCodeForUnsupportedSdpOffer
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.1750

Configures the rejection code used when an offer is received with invalid or unsupported SDP Offer.

- UnsupportedMediaType: The SIP error code 415 'Unsupported Media Type' is returned if the Content-Type is invalid; the payload is missing or the SDP content is invalid.
- NotAcceptableHere: The SIP error code 488 'Not Acceptable Here' is returned if the SDP content is invalid.

RFC 3261 recommends using the error code 488 'Not Acceptable Here'.

InteropUseDtmfPayloadTypeFoundInAnswer (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.InteropUseDtmfPayloadTypeFoundInAnswer
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.2200

The default behaviour when sending an initial offer that contains an RFC 2833 payload type is to keep using that payload type even if the response comes back with a different one. When this parameter is enabled, the unit rather uses the payload type found in the answer. The parameter does not affect the behaviour when receiving an offer.

- Disable: Keep using the initial payload type.
- Enable: Use the RFC 2833 payload type found in the received answer.

This parameter only has an effect when the **DefaultDtmfTransportMethod** parameter is set to 'OutOfBandUsingRtp'.

InteropRegisterHomeDomainOverride (Config Parameter)

Type	Text
Range	SIZE(0..255)
Default	
Script/CLI	SipEp.InteropRegisterHomeDomainOverride
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.2400

Home domain override configuration. If not empty, the address of record in the register uses this string instead of the home domain proxy (refer to the **DefaultStaticProxyHomeDomainHost** parameter).

InteropEnforceOfferAnswerModel (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	SipEp.InteropEnforceOfferAnswerModel
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.2600

Determines whether or not the unit requires strict adherence to RFC 3264 when receiving an answer from the peer when negotiating capabilities for the establishment of a media session.
When enabled, the following guidelines from the Offer-Answer Model must be strictly followed. An answer must:

- Include at least one codec from the list that the unit sent in the offer;
- Contain the same number of media lines that the unit put in its offer.

Otherwise, the answer is rejected and the unit ends the call.

When disabled, then the peer can freely:

- Send back a brand new list of codecs;
- Add new media lines.

As long as at least one codec sent back was present in the initial offer, the call can go on. Any media line added by the peer is simply ignored.

The **InteropAllowLessMediaInResponse** parameter allows other deviations from the Offer/Answer model.

InteropMapPlusToTonInternational (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	SipEp.InteropMapPlusToTonInternational
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.2700

When enabled, the service has the following behaviour:

- For a call to SIP, prefixes the username with '+' if the call has the call property 'type of number' set to 'international'. Also adds the 'user' parameter with value 'phone' to the SIP URI. e.g.: 'sip:1234@domain.com;user=phone'
- For a call from SIP, sets the call property 'type of number' to 'international' if the username has the prefix '+'.

InteropAllowLessMediaInResponse (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.InteropAllowLessMediaInResponse
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.2800

Determines the behaviour of the device when receiving less medias announcement in the response than in the offer.

- Enable: Tries to find matching media when the response contains less media announcement than in the offer.
- Disable: Rejects the response with less media announcement than in the offer.

The **InteropEnforceOfferAnswerModel** parameter enable other deviations from the Offer/Answer model.

InteropDefaultUsernameValue (Config Parameter)

Type	Enum
Range	Anonymous(100) | Host(200)
Default	Anonymous
Script/CLI	SipEp.InteropDefaultUsernameValue
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.3000

Determines the username to use when the username is empty or undefined.

- Anonymous: Set the username to 'anonymous'.
- Host: Set the username to the same value as the host.

InteropCallWaitingSipInfoPrivateNumberCriteria (Config Parameter)

Type	Text
Range	SIZE(0..255)
Default	
Script/CLI	SipEp.InteropCallWaitingSipInfoPrivateNumberCriteria
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.3250

Specify the call waiting criteria, in the form of a regular expression, that defines a private number received in a SIP INFO.
For example, the value "(Anonymous|anonymous)" would define a calling number that is either "Anonymous" or "anonymous" as private. The regular expression symbols to match the beginning and end of the number are implicit and do not need to be specified.

The parameter is effective only if the **EpServ.DefaultCallHookFlashProcessing** or **EpServ.EpSpecificCall.HookFlashProcessing** parameters are set to "TransmitUsingSignalingProtocol".

InteropSdpT38ParametersEncoding (Config Parameter)

Type	Enum
Range	ItuT38AnnexD(100) | SippingRealTimeFax00InternetDraft(200)
Default	SippingRealTimeFax00InternetDraft
Script/CLI	SipEp.InteropSdpT38ParametersEncoding
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.3300

Determines the format in which the unit's T.38 capabilities are advertised. This format is used in the SDP portion of SIP packets.

- SippingRealTimeFax00InternetDraft : Support for the boolean T.38 **T38FaxFillBitRemoval**, **T38FaxTranscodingMMR** and **T38FaxTranscodingJBIG** parameters is advertised by associating a value of 0 (unsupported) or 1 (supported) with the parameter in the following manner: 'a=T38FaxFillBitRemoval:0', 'a=T38FaxTranscodingMMR:0' and 'a=T38FaxTranscodingJBIG:0'. This is compliant with the draft-ietf-sipping-realtimefax-00.txt internet draft.
- ItuT38AnnexD : Support for the above T.38 parameters is advertised in conformance with ITU-T Recommendation T.38, section D.2.3. The presence of the parameter in the SDP indicates support for it (without the need for an associated value), while its absence means that it is not supported.

InteropReInviteForVoiceOn606NotAcceptable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.InteropReInviteForVoiceOn606NotAcceptable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.3400

Determines the behaviour of the device when receiving a 606 Not Acceptable in response to an INVITE for T.38 fax.

- Enable: Fallback to voice is done by sending an INVITE for voice codec negotiation. Also, fax detection is disabled for the remainder of the call.
- Disable: The call is released.

InteropAllowMultipleActiveMediaInAnswer (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	SipEp.InteropAllowMultipleActiveMediaInAnswer
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.3500

Determines the behaviour of the device when answering a request offering more than one active media.

- Enable: Each matching active media in the offer is specified as active in the answer. Other medias are set to inactive.
- Disable: The answer contains only one active media. The media specified as active in the answer is the top-most matching one in the offer. Other medias are set to inactive.

InteropIgnoreSipOptionsOnNoUsuableEndpoints (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.InteropIgnoreSipOptionsOnNoUsuableEndpoints
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.3550

Determines whether or not the SIP OPTIONS requests should be ignored when all endpoints are unusable.
Enable: The unit ignores SIP OPTIONS request when all endpoints are unusable. When at least one endpoint is usable, then the SIP OPTIONS requests are answered as configured in the **InteropSipOptionsMethodSupport** parameter.

Disable: The SIP OPTIONS requests are answered as configured in the **InteropSipOptionsMethodSupport** parameter regardless of the state of the endpoints.

InteropSipOptionsMethodSupport (Config Parameter)

Type	Enum
Range	None(100) | AlwaysOk(200)
Default	None
Script/CLI	SipEp.InteropSipOptionsMethodSupport
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.3600

Determines the behaviour of the device when answering a SIP OPTIONS request.

- None: The unit responds with an error 405 Method not allowed.
- AlwaysOk: The unit responds with a 200 OK regardless of the content of the OPTIONS request.

InteropAllowMediaReactivationInAnswer (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.InteropAllowMediaReactivationInAnswer
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.3700

Determines the unit behaviour when receiving a SDP answer activating a media that had been previously deactivated in the offer.

- Enable: A media reactivated in an incoming answer is ignored. This behaviour goes against the SDP Offer/Answer model described by IETF RFC 3264.
- Disable: A media reactivated in an incoming answer ends the current media negotiation and the call. This behaviour follows the SDP Offer/Answer model described by IETF RFC 3264.

The **InteropEnforceOfferAnswerModel**, **InteropAllowLessMediaInResponse** and **InteropAllowMultipleActiveMediaInAnswer** parameters allow to enable or disable other deviations from the Offer/Answer model.

InteropAllowAudioAndImageNegotiation (Config Parameter)

Type	Enum
Range	Enable(100) | DisableOffer(200) | DisableAll(300)
Default	DisableOffer
Script/CLI	SipEp.InteropAllowAudioAndImageNegotiation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.3800

Determines the unit behaviour when offering media or answering to a media offer with audio and image negotiation.

- Enable: The unit offers audio and image media simultaneously in outgoing SDP offers and transits to T.38 mode upon reception of a T.38 packet. Also, when the unit answers positively to a SDP offer with audio and image, it transits to T.38 mode upon reception of a T.38 packet.
- DisableOffer: Outgoing offers never include image and audio simultaneously. Incoming offers with audio and image media with a non-zero port are answered with audio and image media, but considered as offering only audio.
- DisableAll: Outgoing offers never include image and audio simultaneously. Incoming offers with audio and image media with a non-zero port are answered with audio and image media but the image media will be disabled. If it has the T.38 codec enabled and wishes to send or receive fax, a new re-INVITE will be sent to negotiate image port.

InteropEscapePoundInSipUriUsername (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	SipEp.InteropEscapePoundInSipUriUsername
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.4000

Determines whether or not the pound character (#) must be escaped in the username part of a SIP URI.

- Enable: Pound character (#) is escaped in the username part of a SIP URI.
- Disable: Pound character (#) is not escaped in the username part of a SIP URI.

Note: RFC 3261 specifies that the pound character (#) needs to be escaped in the username part of a SIP URI.

InteropSiemensTransportHeaderEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.InteropSiemensTransportHeaderEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.4100

Triggers the addition of the 'x-Siemens-Call-Type' header to the SIP packets sent by the unit. When enabled, the header is added, and assigned the value 'ST-secure', as soon as secure transport and secure payload are being used. If secure transport or secure payload are not used, the header is not added.

InteropTlsClientAuthenticationEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.InteropTlsClientAuthenticationEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.4200

Specifies whether mutual authentication is enforced when the gateway is acting as a TLS server.

- Enable: The TLS clients have to provide their host certificate in order for the connection to be allowed. In this case, the level of security used to validate the host certificate is TrustedCertificate, whatever the value set in the **SipEp.InteropTlsCertificateValidation** parameter.
- Disable: The unit does not require to TLS client to provide their host certificate in order for the connection to be allowed.

InteropTlsCertificateValidation (Config Parameter)

Type	Enum
Range	NoValidation(100) | TrustedCertificate(200) | DnsSrvResponse(300) | HostName(400)
Default	HostName
Script/CLI	SipEp.InteropTlsCertificateValidation
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.4250

When the unit is acting as a TLS client, this parameter specifies which level of security is used to validate a TLS server certificate.
NOTE: This parameter has no effect on the TLS client authentication when the unit is acting as a TLS server (See the **InteropTlsClientAuthenticationEnable** parameter).

- NoValidation: No validation of the peer certificate is performed. All TLS connections are accepted without any verification. Note that at least one certificate must be returned by the peer even if no validation is made. This option provides no security and should be restricted to a lab use only.
- TrustedCertificate: Allow a TLS connection only if the peer certificate is trusted. A certificate is considered trusted when the certificate authority (CA) that signed the peer certificate is present in the certMIB/othersCertificatesInfoTable. This option provides a minimum level of security and should be restricted to a lab use only.
- DnsSrvResponse: Allow a TLS connection if the peer certificate is trusted and contains a known host name. A known host name can be the FQDN or IP address configured as the SIP server, or can also be returned by a DNS SRV request. In this case, the match is performed against the DNS response name. If it matches either one of the Subject Alternate Name (SAN) or Common Name (CN) in the peer certificate, the connection is allowed. This option provides an acceptable level of security, but not as good as HostName.
- HostName: Allow a TLS connection if the peer certificate is trusted and contains a known host name. A known host name can only be the FQDN or IP address configured as the SIP server. If it matches either one of the Subject Alternate Name (SAN) or Common Name (CN) in the peer certificate, the connection is allowed. This option provides the highest level of security.

InteropIgnorePlusInUsername (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.InteropIgnorePlusInUsername
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.4300

Determines whether or not the plus character (+) is ignored when attempting to match a challenge username with usernames in the **Authentication** table.

- Enable: Plus character (+) is ignored when attempting to match a username in the **Authentication** table.
- Disable: Plus character (+) is not ignored when attempting to match a username in the **Authentication** table.

Note that the plus character is ignored in both the challenge username and the **Authentication** table username.

BehaviorOnT38InviteNotAccepted (Table)

This table defines the device behaviour after receiving an error to a SIP INVITE for T.38 fax.

SipErrorCode (Index) | Table: BehaviorOnT38InviteNotAccepted

Type	UInt32
Range	406..406 | 415..415 | 488..488 | 606..606
Script/CLI	SipEp.BehaviorOnT38InviteNotAccepted[].SipErrorCode
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.4600.1.100

SIP code in the error response to an INVITE for T.38 fax.

Behavior (Config Parameter) | Table: BehaviorOnT38InviteNotAccepted

Type	Enum
Range	DropCall(100) | ReInviteForClearChannelOnly(200) | ReEstablishAudio(300) | UsePreviousMediaNegotiation(400)
Default	ReInviteForClearChannelOnly
Script/CLI	SipEp.BehaviorOnT38InviteNotAccepted[].Behavior
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.4600.1.200

Behaviour of the device when receiving a SIP error response to an INVITE for T.38 fax.

- DropCall: The call is dropped by sending a BYE.
- ReInviteForClearChannelOnly: A re-INVITE is sent with enabled clear channel codecs only.
- ReEstablishAudio: A re-INVITE is sent to re-establish the audio path. Also, fax detection is disabled for the remainder of the call.
- UsePreviousMediaNegotiation: No re-INVITE is sent and the audio codec from the last successful negotiation is used. For the remainder of the call, T.38 is disabled and fax detection may trigger a switch to a clear channel codec that was available in the last successful negotiation.

InteropBehaviorOnMachineDetection (Config Parameter)

Type	Enum
Range	ReInviteOnFaxT38Only(100) | ReInviteOnNoNegotiatedDataCodec(200) | ReInviteUnconditional(300)
Default	ReInviteOnFaxT38Only
Script/CLI	SipEp.InteropBehaviorOnMachineDetection
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.4650

Specifies the SIP device behaviour when a machine is detected during a call.

- ReInviteOnFaxT38Only: A SIP re-INVITE is sent only on a fax detection and T.38 is enabled.
- ReInviteOnNoNegotiatedDataCodec: A SIP re-INVITE is sent on a fax or modem detection if no data codec was previously negotiated in the original SDP negotiation. In the case where at least one data codec was previously negotiated in the SDP negotiation, the device switches silently to a data codec without sending a SIP re-INVITE. Note that if there is no data codec enabled on the device, no SIP re-INVITE is sent and the call is dropped by sending a BYE.

- ReInviteUnconditional : A SIP re-INVITE is sent with data codecs upon detection of a fax or modem even if a data codec was negotiated in the initial offer-answer. The T.38 codec is offered if it is enabled and a fax is detected.

InteropCodecVsBearerCapabilitiesMappingPreferredCodecChoice (Config Parameter)

Type	Enum
Range	FirstCodec(100) | PrioritizeClearChannel(200)
Default	FirstCodec
Script/CLI	SipEp.InteropCodecVsBearerCapabilitiesMappingPreferredCodecChoice
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.4700

Configures the behaviour of the **CodecVsBearerCapabilitiesMapping** table by modifying the selection of the preferred codec in the incoming SDP.

- FirstCodec: The first valid codec in the incoming SDP is considered the preferred one and is used when looking up the **CodecVsBearerCapabilitiesMapping** table.
- PrioritizeClearChannel: When a clear channel codec is in the incoming SDP, it is always considered as the preferred one, no matter where it stands in the codec list, and is used when looking up the **CodecVsBearerCapabilitiesMapping** table.

InteropSipUriUserParameterValue (Config Parameter)

Type	Text
Range	SIZE(0..255)
Default	
Script/CLI	SipEp.InteropSipUriUserParameterValue
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.4800

Determines the value of the user parameter in SIP URIs sent by the unit. If empty, the parameter is not added.
ex: 'sip:1234@domain.com;user=InteropSipUriUserParameterValue'

Note that when the **InteropMapPlusToTonInternational** parameter is enabled, the parameter's value might be overwritten.

InteropListenForEarlyRtpEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.InteropListenForEarlyRtpEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.4900

Listen for RTP even before the reception of a response with SDP.

- Enable: The RTP port is opened after the initial INVITE has been sent, without waiting for a provisional or final response with SDP to be received. No local ring is generated. This conforms to section 5.1 of RFC 3264.
- Disable: The RTP port is opened only after a response with SDP is received.

This parameter only applies to calls initiated from analog endpoints (FXS/FXO) with non-secure RTP.

InteropRegistrationContactMatching (Config Parameter)

Type	Enum
Range	Strict(100) | IgnoreUriParams(200) | IgnoreUriAndPortParams(300)
Default	Strict
Script/CLI	SipEp.InteropRegistrationContactMatching
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.5000

Configures the matching behaviour for the contact header received in positive responses to REGISTER requests sent by the unit.

- Strict: Validate the complete contact's SIP URI including any URI parameters, if any, as per RFC 3261 sections '10.2.4 Refreshing Bindings' and '19.1.4 URI Comparison'. The contact's SIP URI of a 2XX positive response MUST match the contact's SIP URI of the REGISTER request.
- IgnoreUriParams: Validate the username and the host port part of the contact's SIP URI. All URI parameters are ignored.
- IgnoreUriAndPortParams: Validate the username part of the contact's SIP URI. All URI and host port parameters are ignored.

InteropResolveRouteHeaderEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.InteropResolveRouteHeaderEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.5100

Allows the resolution of the FQDN in the top-most route header of outgoing packets.

- Enable: The FQDN in the top-most route header is replaced by the IP address of the packet's destination if the FQDN matches the gateway's configured outbound proxy.
- Disable: The route header is not modified.

InteropForceDnsNaptrInTls (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.InteropForceDnsNaptrInTls
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.5200

Force DNS NAPTR request when SIP transport is TLS.

- Enable: A DNS NAPTR request is sent to obtain the DNS record associated with SIP over TLS. An SRV request is performed afterward. If no SIP over TLS entry is returned, the call fails.
- Disable: The DNS SRV request is sent directly with the SIP transport in SIP URI as recommended in RFC 3263, section 4.1.

This parameter only applies to calls over TLS when the **SupportedDnsQueries** parameter is set to Naptr.

InteropAckBranchMatching (Config Parameter)

Type	Enum
Range	Rfc3261(100) | Rfc3261WithoutAck(200)
Default	Rfc3261
Script/CLI	SipEp.InteropAckBranchMatching
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.5300

Configures the method used to match incoming ACK SIP packets.

- Rfc3261: Follow the method described in RFC 3261 (section 8.1.1.7). The branch value in the topmost via of the ACK request to a 2XX response MUST be different than the one of the INVITE.
- Rfc3261WithoutAck: Follow the method described in RFC 3261 (section 8.1.1.7) but enable the handling of ACK requests (for 2XX responses) that have the same branch value in the topmost via as the INVITE.

InteropIgnoreRequireHeaderEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	SipEp.InteropIgnoreRequireHeaderEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.5400

Indicates if the Require Header must be ignored when processing the incoming SIP Client requests (Invite, re-Invite, Bye, etc.).

- Enable: The Require Header is ignored and no validation about these options-tags is performed.
- Disable: The Require Header options-tags are validated and, when an option-tag is not supported, a 420 (Bad Extension) response is sent.
  The supported options-tags are:
  - * 100rel
  - * replaces
  - * timer

InteropUaHeaderFormat (Config Parameter)

Type	Text
Range	
Default	%product%/v%version% %profile%
Script/CLI	SipEp.InteropUaHeaderFormat
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.5500

The text to display in the User-Agent Header. Macros can be used to include information specific to the unit.
The supported macros are:

- %version% - Application version.
- %mac% - MAC address.
- %product% - Product name.
- %profile% - Profile.
- %serial% - Serial number.
- %% - Insert % character.

InteropSipInfoWithoutContentAnswer (Config Parameter)

Type	Enum
Range	Ok(200) | UnsupportedMediaType(415)
Default	UnsupportedMediaType
Script/CLI	SipEp.InteropSipInfoWithoutContentAnswer
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.5600

Determines the response of the device to a received SIP INFO with no message body for an existing call.

- UnsupportedMediaType: The unit responds with the SIP error code 415 'Unsupported Media Type'.
- Ok: The unit responds with a 200 OK.

RFC 2976 recommends that a 200 OK response MUST be sent for an INFO request with no message body if the INFO request was successfully received for an existing call.

InteropRegistrationDelayValue (Config Parameter)

Type	UInt32
Range	0..600
Default	0
Script/CLI	SipEp.InteropRegistrationDelayValue
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.5700

The maximum number of seconds that the system uses to apply a random algorithm, which is used to determine a delay before requesting a user registration or an endpoint registration. When the value is 0, the request registration is done immediately.
Note: The random algorithm applies individually to all registrations meaning registrations order may not follow their corresponding index.

This value is expressed in second(s).

InteropUnsupportedContentType (Config Parameter)

Type	Enum
Range	Reject(100) | Allow(200) | Ignore(300)
Default	Reject
Script/CLI	SipEp.InteropUnsupportedContentType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.5800

Determines the behaviour of the device upon reception of a SIP packet containing multiple unsupported Content-Type in the payload.

- Reject: Unsupported Content-Type are rejected.
- Allow: Unsupported Content-Type are allowed and ignored if at least one Content-Type is supported.
- Ignore: Unsupported Content-Type are ignored.

Note: When ignored, unsupported Content-Type are treated as if they were not present in the packet.

InteropWaitConfirmedDialogForBlindTransfer (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.InteropWaitConfirmedDialogForBlindTransfer
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.5900

This parameter is obsolete and has been replaced by the **TransferGroup.BlindTransferMethod** parameter.

InteropPendingBlindTransferTimeout (Config Parameter)

Type	UInt32
Range	5..600
Default	30
Script/CLI	SipEp.InteropPendingBlindTransferTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.6000

The maximum number of seconds that the system keeps a blind transfer pending (waiting for a 200 OK response) when the **TransferGroup.BlindTransferMethod** parameter is set to SemiAttendedConfirmed. If the timeout expires, the call transfer is cancelled.

InteropForkedProvisionalResponsesBehavior (Config Parameter)

Type	Enum
Range	InterpretFirst(100) | InterpretAll(200)
Default	InterpretFirst
Script/CLI	SipEp.InteropForkedProvisionalResponsesBehavior
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.6100

Configure the unit's behaviour when receiving forked provisional answers.

- InterpretFirst: Only the first provisional answer is interpreted. Following responses do not change the state of the call and the SDP is ignored if present.

- InterpretAll: Each forked provisional response received by the unit is interpreted replacing the previous one. If the response contains SDP, it replaces previous answers if any.

This configuration has no effect if the **UACPrackSupport** parameter is set to a value other than 'Unsupported'. Otherwise, see the **InteropReliableForkedProvisionalResponsesBehavior** parameter.

InteropReliableForkedProvisionalResponsesBehavior (Config Parameter)

Type	Enum
Range	InterpretFirst(100) | InterpretFirstRemoteMedia(200)
Default	InterpretFirst
Script/CLI	SipEp.InteropReliableForkedProvisionalResponsesBehavior
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.6110

Configure the unit's behaviour when receiving reliable forked provisional answers.

- InterpretFirst: Only the first provisional answer is interpreted. Following forked responses, do not change the state of the call and the SDP is ignored if present.
- InterpretFirstRemoteMedia: The first forked provisional response received by the unit is interpreted. If a following forked response contains SDP and the media is not already negociated, it replaces the previous answer. Once media is negociated, following provisional responses are ignored.

This configuration has effect only if the **UACPrackSupport** parameter is set to a value other than 'Unsupported'. Otherwise, see the **InteropForkedProvisionalResponsesBehavior** parameter.

InteropSipContactDisplayNamePresence (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	SipEp.InteropSipContactDisplayNamePresence
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.6200

Determines if the display name appears in the SIP Contact header sent by the unit.

- Enable : The display name parameter appears in the SIP Contact header of sent SIP request.
- Disable : The display name does not appear.

InteropEscapeFormat (Config Parameter)

Type	Enum
Range	LowercaseHex(100) | UppercaseHex(200)
Default	LowercaseHex
Script/CLI	SipEp.InteropEscapeFormat
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.6300

Configures the format of the escaped characters in all SIP header.

- LowercaseHex: Escaped characters are displayed in a lowercase hexadecimals format.
- UppercaseHex: Escaped characters are displayed in a uppercase hexadecimals format.

InteropKeepAliveOptionFormat (Config Parameter)

Type	Enum
Range	ShortFrom(100) | FullFrom(200)
Default	ShortFrom
Script/CLI	SipEp.InteropKeepAliveOptionFormat
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.6400

Configures the Keep-Alive OPTION requests format.

- ShortFrom : The unit sends the OPTION request with the standard format with only the unit's IP address in the from header.
- FullFrom : The unit sends the OPTION request with the standard format with the first registered username and IP address in the from header.

The SipEp service must be restarted to apply a new username to the Keep-Alive.

InteropInfoDtmfRelayFlashEvent (Config Parameter)

Type	Enum
Range	Disable(100) | EvR(200) | Ev16(300)
Default	Disable
Script/CLI	SipEp.InteropInfoDtmfRelayFlashEvent
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.6500

This parameter specifies which SIP INFO event triggers a hook flash on the PSTN interface when the DTMF transport method is set to InfoDtmfRelay. The event is the value of the Signal parameter in the SIP INFO message.

- Disable: No event is defined.
- EvR: The event is the string "R" (case insensitive).
- Ev16: The event is the string "16".

The string must contain no other character.

This parameter only has an effect when the **InteropDtmfTransportMethod** parameter is set to 'InfoDtmfRelay'.

InteropSdpPTimeAttribute (Config Parameter)

Type	Enum
Range	Disabled(100) | DeclarativePreferredCodec(200) | DeclarativeConfigured(300)
Default	Disabled
Script/CLI	SipEp.InteropSdpPTimeAttribute
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.6600

This parameter specifies what value must be put in the ptime attribute of the SDP offers.

- Disabled: No ptime attribute is inserted.
- DeclarativePreferredCodec: The ptime attribute is set to the packetization time of the preferred codec.
- DeclarativeConfigured: The ptime attribute is set to the value configured in the **InteropSdpPTimeAttributeValue** parameter.

The preferred codec is the highest priority codec that would be advertised in the SDP offer of an INVITE. The preferred codec and its packetization time depend on configuration parameters in the Mipt service.

InteropSdpPTimeAttributeValue (Config Parameter)

Type	UInt32
Range	10..80
Default	20
Script/CLI	SipEp.InteropSdpPTimeAttributeValue
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.6700

This parameter specifies the configurable value to be put in the ptime attribute of the SDP offers when the **InteropSdpPTimeAttribute** parameter is set to 'DeclarativeConfigured'.

Note that this value is not checked for validity.

InteropIncrementSdpVersionWhenModified (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	SipEp.InteropIncrementSdpVersionWhenModified
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.6800

This parameter specifies if the SDP must be checked for differences before updating its version.

- Disable: The version will be incremented on all new generation of the SDP.
- Enable: The version will be updated on new generation if there is a difference with the last one sent.

InteropActivateEarlyMediaOnProvisionalResponseAck (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.InteropActivateEarlyMediaOnProvisionalResponseAck
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.7000

This parameter specifies if the system must wait for a provisional response acknowledgement before sending the early media stream.

- Disable: The activation of the early media stream is triggered by the transmission of a provisional response (i.e. SIP 18X).
- Enable: The activation of the early media stream is triggered by the transmission of the final positive response of a provisional response acknowledgement (i.e. 200 OK of PRACK).

In any case, the SIP SDP negotiation is not altered by this interop parameter.

This parameter has an effect only when:

- the **UasPrackSupport** parameter is set to 'supported',
- the received SIP INVITE contains SDP and a '100rel' option-tag header (i.e. PRACK), and
- early media negotiation is completed and ready to be played towards the remote SIP peer.

InteropSend183WithSdpBefore180WithoutSdp (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.InteropSend183WithSdpBefore180WithoutSdp
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.7100

This parameter specifies if the system must send a 183 with SDP before sending a 180 without SDP.

- Disable: Do not send a 183 with SDP before a 180 without SDP.
- Enable: Send a 183 with SDP before sending a 180 without SDP. Even if the 183 with SDP completes the media negotiation, the system will start sending media only after sending the 200 OK.

Enabling this parameter may improve interoperability with VoLTE endpoints.

This parameter has an effect only when:

- the **UasPrackSupport** parameter is set to 'supported',
- the received SIP INVITE contains SDP and a '100rel' option-tag header (i.e. PRACK), and
- the call destination is an FXS endpoint.

InteropCollectCallProprietaryHeader (Config Parameter)

Type	Enum
Range	Ignore(100) | Relay(200) | Block(300)
Default	Ignore
Script/CLI	SipEp.InteropCollectCallProprietaryHeader
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.7200

Defines how the reception of a collect call, also known as "reverse charging" call, is handled:

- Ignore: Ignore the "Collect Call" header and relay the call as a normal call.
- Relay: Relay the call as a collect call to the ISDN or R2 telephony lines.
- Block: Upon reception, reject with a 603 Decline all incoming calls with the collect call header.

This is supported only if the incoming SIP INVITE has this proprietary header:

- P-Asserted-Service-Info: service-code=Collect Call

InteropDtmfTransportMethod (Config Parameter)

Type	Enum
Range	DraftChoudhuriSipInfoDigit00(100) | InfoDtmfRelay(200)
Default	DraftChoudhuriSipInfoDigit00
Script/CLI	SipEp.InteropDtmfTransportMethod
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.50000.100

Configures the signaling method used to transmit DTMFs over the SIP protocol.
This parameter is effective only if the endpoint DTMF transport is configured with the *OutOfBandUsingSignalingProtocol* or *SignalingProtocolDependent* method (refer to the **Mipt.DefaultDtmfTransportMethod** and **Mipt.EpSpecificDtmfTransport.Method** parameters).

- DraftChoudhuriSipInfoDigit00: The unit negotiates the 'rtpmap:111 X-nt-inforeq' through the SDP and if the peer supports it, it sends the DTMFs using a SIP INFO method with a 'application/vnd.nortelnetworks.digits' content type. Otherwise the unit falls back to Inband.
- InfoDtmfRelay: The unit does not advertise any method. The DTMFs are transmitted by using a custom SIP INFO method. This custom method does not require SDP negotiation and assumes that the other peer uses the same method. When sending DTMF, it mutes the audio and sends a SIP INFO message with a 'application/dtmf-relay' content type.

When both *SignalingProtocolDependent* and *DraftChoudhuriSipInfoDigit00* methods are selected, the unit advertises both RFC-2833 (RTP telephony events) and 'application/vnd.nortelnetworks.digits', and may use one or both of these methods if the peer supports them. Otherwise the unit falls back to Inband.

When the *InfoDtmfRelay* method is selected,

- the payload of the SIP INFO message contains the transmitted DTMF and its duration (in ms) with these attributes:
  - Signal= 1
  - Duration= 160
- On sending, the duration is the one set in the **InteropDtmfTransportduration** parameter.
- On reception, the duration of the received DTMF will be ignored, the DTMF will be played accordingly to the selected country dialing settings (refer to the **TelIf.CountrySelection** parameter). The DTMF duration can be overridden by the **TelIf.DefaultCountryCustomizationDialingDtmfDuration** parameter.
- The DTMFs are transmitted only one at a time.
- Available digits are '0123456789ABCD*#'. The Mediatrix unit also supports the ',;p' characters when receiving DTMFs.

InteropDtmfTransportDuration (Config Parameter)

Type	Int32
Range	50..2000
Default	100
Script/CLI	SipEp.InteropDtmfTransportDuration
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50000.50000.200

Configures the DTMF duration sent in the INFO message when using the *InfoDtmfRelay* method (refer to the **InteropDtmfTransportMethod** parameter).

This value is expressed in milliseconds (ms).

SipNotificationsGateway (Config Parameter)

Type	Text
Range	
Default	default
Script/CLI	SipEp.SipNotificationsGateway
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50500.100

Defines the SIP gateway used to send SIP NOTIFY containing the notification events. Notification events are configured in the **Nlm.Events** table.

MaxNotificationsPerNotify (Config Parameter)

Type	UInt32
Range	1..25
Default	5
Script/CLI	SipEp.MaxNotificationsPerNotify
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.50500.200

Defines the maximal number of notification events the device may have to send in one SIP NOTIFY request. Notifications are sent in XML elements through the SIP NOTIFY's body request.

DebugSignalingLogEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	SipEp.DebugSignalingLogEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.51000.100

Enables the logging client debugging tool for IP telephony signaling.

DebugSignalingLogHost (Config Parameter)

Type	IpHostNamePort
Range	
Default	192.168.10.10:0
Script/CLI	SipEp.DebugSignalingLogHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.51000.200

Logging client FQDN and port.
The default port is 6000.

DebugContextSnapshotTime (Config Parameter)

Type	UInt32
Range	0..10080
Default	0
Script/CLI	SipEp.DebugContextSnapshotTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.51000.300

Sets the time between snapshots.
The list of contexts currently in use in the sipFramework and sipApplication are periodically output as debug-level syslog messages.

Note that for this feature to work, the system log severity level must be set to 'debug', and the syslog feature must be properly configured.

Note that enabling this feature also triggers an instant snapshot.

To disable this feature, set this parameter to zero (0).

This value is expressed in minutes (min).

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	SipEp.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	SipEp.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1400.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

ErrorMappingInsertCauseToSip (Command)

Insert a new row at the end of the **ErrorMappingCauseToSip** table

Cause (Argument) | Command: ErrorMappingInsertCauseToSip

Type	UInt32
Range	1..127
Default	

Cause to map the the SIP code.
The cause specified in Q.931 are:

Normal event:

- 1: Unassigned (unallocated) number.
- 2: No route to specified transit network.
- 3: No route to destination.
- 6: Channel unacceptable.
- 7: Call awarded and being delivered in an established channel.
- 17: User busy.
- 18: No user responding.
- 19: User alerting, no answer.
- 20: Subscriber absent.
- 21: Call rejected.
- 22: Number changed.
- 23: Redirection to new destination.
- 26: Non-selected user clearing.
- 27: Destination out of order.
- 28: Invalid number format (incomplete number).
- 29: Facility rejected.
- 30: Response to STATUS ENQUIRY.
- 31: Normal, unspecified.

Resource unavailable:

- 34: No circuit/channel available.
- 38: Network out of order.
- 41: Temporary failure.
- 42: Switching equipment congestion.
- 43: Access information discarded.
- 44: Requested circuit/channel not available.
- 47: Resource unavailable, unspecified.

Service or option not available:

- 55: Incoming calls barred within CUG.
- 57: Bearer capability not authorized.
- 58: Bearer capability not presently available.
- 63: Service or option not available, unspecified.

Service or option not implemented:

- 65: Bearer capability not implemented.
- 66: Channel type not implemented.
- 69: Requested facility not implemented.
- 70: Only restricted digital information bearer capability is available.
- 79: Service or option not implemented, unspecified.

Invalid message:

- 81: Invalid call reference value.
- 82: Identified channel does not exist.
- 83: A suspended call exists, but this call identity does not.
- 84: Call identity in use.
- 85: No call suspended.
- 86: Call having the requested call identity has been cleared.
- 87: user not member of CUG.
- 88: Incompatible destination.
- 91: Invalid transit network selection.
- 95: Invalid message, unspecified.

Protocol error:

- 96: Mandatory information element is missing
- 97: Message type non-existent or not implemented
- 98: Message not compatible with call state or message type non-existent or not implemented
- 99: Information element non-existent or not implemented

- 100: Invalid information element contents
- 101: Message not compatible with call state
- 102: Recovery on time expiry
- 111: Protocol error, unspecified

Interworking:

- 127: Interworking, unspecified

SipCode (Argument) | Command: ErrorMappingInsertCauseToSip

Type	UInt32
Range	400..699
Default	

SIP code to map to a cause. It's also the unique identifier of the row.
SIP code:

- 400: Bad Request
- 401: Unauthorized
- 402: Payment required
- 403: Forbidden
- 404: Not found
- 405: Method not allowed
- 406: Not acceptable
- 407: Proxy authentication required
- 408: Request timeout
- 410: Gone
- 413: Request Entity too long
- 414: Request-URI too long
- 415: Unsupported media type
- 416: Unsupported URI Scheme
- 420: Bad extension
- 421: Extension Required
- 423: Interval Too Brief
- 480: Temporarily unavailable
- 481: Call/Transaction Does not Exist
- 482: Loop Detected

- 483: Too many hops
- 484: Address incomplete
- 485: Ambiguous
- 486: Busy here
- 500: Server internal error
- 501: Not implemented
- 502: Bad gateway
- 503: Service unavailable
- 504: Server time-out
- 504: Version Not Supported
- 513: Message Too Large
- 600: Busy everywhere
- 603: Decline
- 604: Does not exist anywhere

ErrorMappingInsertSipToCause (Command)

Insert a new row at the end of the **ErrorMappingSipToCause** table.

SipCode (Argument) | Command: ErrorMappingInsertSipToCause

Type	UInt32
Range	400..699
Default	

SIP code to map to a cause. It's also the unique identifier of the row.
SIP code:

- 400: Bad Request
- 401: Unauthorized
- 402: Payment required
- 403: Forbidden
- 404: Not found
- 405: Method not allowed
- 406: Not acceptable
- 407: Proxy authentication required
- 408: Request timeout

- 410: Gone
- 413: Request Entity too long
- 414: Request-URI too long
- 415: Unsupported media type
- 416: Unsupported URI Scheme
- 420: Bad extension
- 421: Extension Required
- 423: Interval Too Brief
- 480: Temporarily unavailable
- 481: Call/Transaction Does not Exist
- 482: Loop Detected
- 483: Too many hops
- 484: Address incomplete
- 485: Ambiguous
- 486: Busy here
- 500: Server internal error
- 501: Not implemented
- 502: Bad gateway
- 503: Service unavailable
- 504: Server time-out
- 504: Version Not Supported
- 513: Message Too Large
- 600: Busy everywhere
- 603: Decline
- 604: Does not exist anywhere

Cause (Argument) | Command: ErrorMappingInsertSipToCause

Type	UInt32
Range	1..127
Default	

Cause to map the the SIP code.
The cause specified in Q.931 are:

Normal event:

- 1: Unassigned (unallocated) number.

- 2: No route to specified transit network.
- 3: No route to destination.
- 6: Channel unacceptable.
- 7: Call awarded and being delivered in an established channel.
- 17: User busy.
- 18: No user responding.
- 19: User alerting, no answer.
- 20: Subscriber absent.
- 21: Call rejected.
- 22: Number changed.
- 23: Redirection to new destination.
- 26: Non-selected user clearing.
- 27: Destination out of order.
- 28: Invalid number format (incomplete number).
- 29: Facility rejected.
- 30: Response to STATUS ENQUIRY.
- 31: Normal, unspecified.

Resource unavailable:

- 34: No circuit/channel available.
- 38: Network out of order.
- 41: Temporary failure.
- 42: Switching equipment congestion.
- 43: Access information discarded.
- 44: Requested circuit/channel not available.
- 47: Resource unavailable, unspecified.

Service or option not available:

- 55: Incoming calls barred within CUG.
- 57: Bearer capability not authorized.
- 58: Bearer capability not presently available.
- 63: Service or option not available, unspecified.

Service or option not implemented:

- 65: Bearer capability not implemented.
- 66: Channel type not implemented.
- 69: Requested facility not implemented.
- 70: Only restricted digital information bearer capability is available.

- 79: Service or option not implemented, unspecified.

Invalid message:

- 81: Invalid call reference value.
- 82: Identified channel does not exist.
- 83: A suspended call exists, but this call identity does not.
- 84: Call identity in use.
- 85: No call suspended.
- 86: Call having the requested call identity has been cleared.
- 87: user not member of CUG.
- 88: Incompatible destination.
- 91: Invalid transit network selection.
- 95: Invalid message, unspecified.

Protocol error:

- 96: Mandatory information element is missing
- 97: Message type non-existent or not implemented
- 98: Message not compatible with call state or message type non-existent or not implemented
- 99: Information element non-existent or not implemented
- 100: Invalid information element contents
- 101: Message not compatible with call state
- 102: Recovery on time expiry
- 111: Protocol error, unspecified

Interworking:

- 127: Interworking, unspecified

InsertAuthentication (Command)

Inserts a new row at the end of the authentication table.

Number (Argument) | Command: InsertAuthentication

Type	UInt32
Range	1..100
Default	1

Number of rows to add.

InsertGateway (Command)

Inserts a new row in the **Gateway** table.

Name (Argument) | Command: InsertGateway

Type	Text
Range	SIZE(1..16)
Default	

Name of the SIP Gateway to insert.
Only alphanumeric characters, '-', and '_' are accepted.

InsertUnitRegistration (Command)

Inserts a new row at the end of the **UnitRegistrations** table.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

MwiSubscriptionRefresh (Command)

Command to refresh the MWI subscription.
All enabled endpoints unsubscribe themselves from the previous Messaging system and send a new subscription to the current Messaging system with the current parameters.

RegistrationRefresh (Command)

Command to refresh the registrations.
All enabled endpoints unregister themselves from the previous registrar and send a new registration to the current registrar with the current parameters.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the SipEp service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.1400.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	The endpoint %1$s cannot register because the authentication failed.	Error	The endpoint cannot register because it was not properly configured to respond to the registrar challenge.
15	The user %1$s cannot register because the authentication failed.	Error	The user cannot register because it was not properly configured to respond to the registrar challenge.
20	The endpoint %1$s cannot register because the registrar is unreachable.	Error	The registration failed because the registrar does not respond to the endpoint registration request.
25	The user %1$s cannot register because the registrar is unreachable.	Error	The registration failed because the registrar does not respond to the user registration request.
30	The endpoint %1$s cannot register because of invalid configuration.	Error	The endpoint cannot register because it does not have a valid configuration. Check if the home domain proxy and the user name are properly set.
35	The user %1$s cannot register because of invalid configuration.	Error	The user cannot register because it does not have a valid configuration. Check if the home domain proxy and the user name are properly set.
40	The call %1$d from %2$s to %3$s on endpoint %4$s cannot be established because the destination is unreachable.	Warning	The destination of the call cannot be reached. This case can occur when: • The destination is not known by the registrar. • The destination uses unsuported SIP transport. In that case, enabling either the UDP/TCP or TLS transports can fix the problem. • The destination does not respond to the request.
50	The call %1$d from %2$s to %3$s on endpoint %4$s cannot be established because the authentication failed.	Warning	The endpoint is not properly configured to authenticate to the destination.

NumKey	Message	Severity	Description
55	The call %1$d from %2$s to %3$s on endpoint %4$s cannot be established because no media network is available.	Warning	The call cannot be established because all configured interfaces for media are down or disabled.
60	The incoming call %1$d from %2$s to %3$s is rejected because the destination is unknown.	Warning	The incoming call is rejected because the destination does not match any endpoint user name or internal routing rule.
70	Incoming call %1$d from %2$s to %3$s is established on endpoint %4$s.	Debug	The incoming call is properly established.
80	Outgoing call %1$d from %2$s to %3$s is established on endpoint %4$s.	Debug	The outgoing call is properly established.
90	The endpoint %1$s is registered.	Info	The endpoint is properly registered to the registrar.
95	The user %1$s is registered.	Info	The user is properly registered to the registrar.
100	New outgoing call %1$d from %2$s to %3$s on endpoint %4$s.	Debug	The device initiated a new call. The call is not established yet.
110	New incoming call %1$d from %2$s to %3$s.	Debug	The device received a new call. The call is not established yet.
120	The endpoint %1$s registration is refreshed.	Debug	The endpoint properly refreshed its registration with the registrar.
125	The user %1$s registration is refreshed.	Debug	The user properly refreshed its registration with the registrar.
130	The call %1$d from %2$s to %3$s is rejected because the resource is busy.	Debug	The endpoint rejected the incoming call because it does not have enough available resource to handle the call.
135	The call %1$d from %2$s to %3$s was rejected: the target interface could not find any available resource.	Warning	The unit rejected the incoming call: the target interface could not allocate the required resources to process the call.

NumKey	Message	Severity	Description
140	The endpoint %1$s rejected the incoming call because it is unavailable.	Debug	The endpoint rejected the incoming call because it was not available. An endpoint is not available when: • it is locked. • it is not registered.
145	The incoming call %1$d from %2$s to %3$s is rejected because no media network is available.	Warning	The endpoint rejected the incoming call because all configured interfaces for media are down or disabled.
150	The session timer configuration is incoherent.	Warning	The unit has detected an incoherent configuration of the session timer feature. The maximal session timer value is lower than the minimal session timer value. The unit will use the minimal session timer value for the maximum session timer.
210	SIP gateways with network interface named %1$s are invalid. Automatically updated network interface name to %2$s.	Warning	This message is issued when a network interface with an invalid name is encountered at service startup. An invalid name starts with a character that is not a letter or contains a character other than a letter, number or underscore.
220	The endpoint %1$s cannot register/ unregister because the response is invalid.	Error	The endpoint cannot register because the received 200 OK contact does not match the REGISTER contact. This error also occurs if the 200 OK response for an unregister contains contact. In that case, the registration is considered unregistered.
230	The user %1$s cannot register/unregister because the response is invalid.	Error	The user cannot register because the received 200 OK contact does not match the REGISTER contact. This error also occurs if the 200 OK response for an unregister contains contact. In that case, the registration is considered unregistered.
240	Secure media transport enabled (SRTP) without secure signaling transport (TLS).	Warning	Secure RTP (SRTP) has been enabled on at least one line while secure SIP transport is disabled (TLS). This is acceptable for testing purposes, but must never be used in a production environment, since an attacker could easily break it. Enabling TLS for SIP Transport is strongly recommended.

NumKey	Message	Severity	Description
250	TLS connection with remote host %1$s failed because it is either unreachable or not listening for TLS on the specified port.	Error	This message is issued when a TLS connection cannot be established with a remote host because it is either unreachable or it is not listening for TLS on the specified port. This notification is only issued for Trunk gateways.
260	TLS connection with remote host %1$s failed because the received certificate is not trusted.	Error	This message is issued when a TLS persistent connection cannot be established with a remote host because the received certificate is not trusted. This notification is only issued for Trunk gateways.
265	OCSP verification on the certificate of %1$s with responder URL %2$s completed with status %3$s.	Info	This message is issued every time an OCSP request is completed (successful or not).
266	Certificate revocation status cannot be verified for TLS connection with remote host %1$s because the OCSP responder %2$s is unreachable.	Warning	This message is issued when certificate revocation status cannot be verified because the received peer certificate does not include the Authority Information Access extension providing the URI for the OCSP responder or the OCSP responder cannot be reached.
267	Certificate revocation status cannot be verified for TLS connection with remote host %1$s because the response from OCSP responder %2$s could not be accepted.	Warning	This message is issued when the response obtained from the OCSP responder cannot be accepted. Possible causes include: failure to match the response with the request, response delay too large, response cannot be parsed, response fails verification.
268	Certificate revocation status cannot be verified on the certificate of %1$s because the responder URL %2$s is not valid.	Warning	This message is issued when the responder URL does not follow the supported syntax.

NumKey	Message	Severity	Description
270	TLS connection using local port %1$d failed because another entity is already listening on this port.	Error	This message is issued when a TLS persistent connection cannot be established with a remote host because the local port used to establish the connection is already used by another entity. Verify that there is no other entities that are listening on the specified port. This notification is only issued for Trunk gateways.
290	TLS connection with remote host %1$s, using the local address %2$s:%3$d on the %4$s signalling network interface, failed.	Error	This message is issued when a TLS persistent connection cannot be established with a remote host. Validate that the SIP local configuration (Gateway, Transport, Servers, Addresses, Port) is properly set. This notification is only issued for Trunk gateways.
300	TLS connection with remote host %1$s failed because of an unspecified error.	Error	This message is issued when a TLS connection cannot be established with a remote host and the reason is not available. This notification is only issued for Trunk gateways.
302	TLS connection with remote host %1$s is now established for SIP gateway %2$s.	Info	This message is issued when a TLS connection is established. This notification is only issued for Trunk gateways.
303	TLS connection with remote host %1$s is now ready to be used for SIP gateway %2$s.	Info	This message is issued when a TLS connection is established and ready to be used. This notification is only issued for Trunk gateways.
305	Gracefully terminating TLS connection with remote host %1$s for SIP gateway %2$s.	Info	This message is issued when a TLS connection initiate a graceful terminate. This occurs when a higher priority TLS connection is established. This notification is only issued for Trunk gateways.
307	TLS connection with remote host %1$s is now terminated for SIP gateway %2$s.	Info	This message is issued when a TLS connection is terminated. This notification is only issued for Trunk gateways.
310	Server %1$s is now reachable for SIP gateway %2$s.	Info	This message is issued when the server was unreachable but now answers the Keep-Alive request.

NumKey	Message	Severity	Description
315	Cannot start Keep-Alive mechanism for SIP gateway %1$s because the specified destination %2$s is in the wrong IP address version.	Error	This message is issued when the specified destination of the Keep-Alive mechanism has an IP address version different than the SIP gateway.
320	Server %1$s is unreachable for SIP gateway %2$s.	Error	This message is issued when the server doesn't answer the Keep-Alive request.
325	Cannot start Keep-Alive mechanism for SIP gateway %1$s because no destination is specified.	Error	This message is issued when the Keep-Alive mechanism is configured to use a destination and none is specified for the SIP gateway.
330	The total number of registrations exceeds the limit of %1$d.	Error	This message is issued when the total number of registrations currently configured exceeds the defined limit. Registrations are enabled gateway by gateway until the limit is reached. The rest is ignored.
340	Invalid SIP blind NOTIFY received or cannot be matched with a valid endpoint.	Warning	This message is issued when a blind notify for a MWI uses is received and cannot be parsed correctly or cannot be matched with a valid endpoint.
350	Invalid SIP MWI NOTIFY received or cannot be matched with a valid endpoint.	Warning	This message is issued when a notify for a MWI uses is received and cannot be parsed correctly or cannot be matched with a valid endpoint.
360	The endpoint %1$s MWI subscription is refreshed.	Debug	The endpoint properly refreshed its MWI subscription with the messaging server.
370	The endpoint %1$s is subscribed.	Info	The endpoint is properly subscribed to the messaging server.
380	The endpoint %1$s cannot subscribe/ unsubscribe to messaging server because the response is invalid.	Error	The endpoint cannot subscribe to messaging server because the received 200 OK contact does not match the SUBSCRIBE contact. In that case, the MWI subscription is considered unsubscribed.
390	The endpoint %1$s cannot subscribe because of invalid configuration.	Error	The endpoint cannot subscribe to messaging server because of an invalid configuration. Check if the messaging server host and the user name are properly set.

NumKey	Message	Severity	Description
400	The endpoint %1$s cannot subscribe to the messaging server because it is unreachable.	Error	The subscription failed because the messaging server does not respond to the endpoint subscription request.
410	The endpoint %1$s cannot subscribe to the messaging server because the authentication failed.	Error	The endpoint cannot subscribe because it was not properly configured to respond to the messaging server challenge.
420	Received a Method Not Allowed response for UPDATE method on call %1$d from %2$s to %3$s on endpoint %4$s.	Warning	The peer UAS doesn't support the UPDATE method and issued a Method Not Allowed response. The UPDATE method was likely issued because the unit is configured to use it for sending Session Refresh Requests. If this is the case, change configuration to use the INVITE method instead.
430	A configuration script execution is requested by a SIP blind NOTIFY.	Info	This message is issued to inform that a configuration script execution is requested by a incoming SIP blind NOTIFY containing a 'check-sync' event.
440	A reboot of the unit is requested by a SIP blind NOTIFY.	Info	This message is issued to inform that a reboot is requested by an incoming SIP blind NOTIFY containing a 'reboot' event.
450	Gateway %1$s rejected SIP message from unexpected peer %2$s: %3$d	Info	This message is issued to inform that a SIP message from an unexpected peer was rejected.
460	DNS Server didn't respond or responded with an error on gateway %1$s.	Error	The DNS server didn't respond or responded with an error.
470	DNS failure concealement is not allowed on Trunk gateways.	Warning	This message is issued if a gateway is set to type 'Trunk' and DNS failure concealment is active. DNS failure concealment is not supported for Trunk gateways. In this case the DNS concealment feature is considered to be set to 'None'. See the **Gateway.Type** and **DnsFailureConcealment** parameters for details.

NumKey	Message	Severity	Description
480	Listening SIP ports are not allowed for Endpoint gateway %1$s.	Warning	This message is issued when the port or secure port is set to non-zero value on an Endpoint gateway. Listening ports are not allowed on Endpoint gateways. See the **Gateway.Port**, **Gateway.SecurePort** and **Gateway.Type** parameters for details.
490	Next hop must be a single target for Endpoint gateway %1$s.	Error	This message is issued when an Endpoint gateway have no outbound proxy set and registrar is not the same as the domain proxy. That configuration is not a valid configuration for an Endpoint gateway.
500	Keep-Alive is not allowed on an Endpoint gateways.	Warning	This message is issued if an unsupported SIP Keep-Alive method is enabled on an Endpoint gateway. SIP Keep-Alive is not fully supported for Endpoint gateways. In this case the SIP Keep-Alive feature is completely disabled. See the **Gateway.Type** and **SipKeepAliveMethod** parameters for details.
510	Unit Registration %1$s is not allowed for gateway %2$s.	Warning	This message is issued if a unit registration entry is associated with an Endpoint gateway. Unit registrations are not supported for Endpoint gateways but remain active for gateways of other types. See the **Gateway.Type** and **UnitRegistrations.GatewayName** parameters for details.
520	Penalty Box is not allowed on Endpoint gateways.	Warning	This message is issued if the **PenaltyBoxEnable** parameter is set to 'Enable' and a gateway is set to type 'Endpoint'. Penalty Box is not allowed on Endpoint gateways. In this case the PenaltyBox feature is completely disabled.
530	Symmetric UDP source port not disabled for Endpoint gateways.	Warning	This message is issued if the **InteropSymmetricUdpSourceportEnable** parameter is set to 'disable' and an Endpoint gateway is configured. This parameter have no effect on Endpoint gateways. Endpoint gateways always use symmetric local ports.
540	SIP monitoring notifications are not allowed on Endpoint gateways.	Warning	This message is issued if the **SipNotificationsGateway** parameter is set to an Endpoint gateway. In this case the SIP monitoring notifications are disabled.

NumKey	Message	Severity	Description
550	User %1$s has several different friendly names on gateway %2$s.	Warning	This message is issued when a user does not have a unique friendly name on all the endpoints on which it is registered for a given gateway. The friendly name used in the SIP messages will be parameter.
570	Invalid configuration of SIP Failover Conditions %1$s for gateway %2$s. Using %3$s instead.	Warning	This message is issued when the configuration of the SIP Failover Conditions is not supported on this type of gateway. The gateway uses the indicated configuration instead.
580	User %1$s has several different contact domains on gateway %2$s.	Warning	This message is issued when a user does not have a unique contact domain name on all the endpoints on which it is registered for a given gateway. The contact domain used in the SIP messages will be parameter.
590	The call %1$d from %2$s to %3$s received an AOC amount with a decimal value. The amount %4$s is replaced by its next integer value.	Warning	This message is issued when the received AOC currency-amount tag has a decimal value instead of an unit value.
600	User %1$s has several different accept language on gateway %2$s.	Warning	This message is issued when a user does not have a unique accept language on all the endpoints on which it is registered for a given gateway. The accept language used in the SIP messages will be parameter.
610	The gateway %1$s is configured for SBC binding but not its signaling interface.	Warning	When a gateway is configured for SBC binding, it is mandatory to have its **Gateway.NetworkInterface** parameter configured to 'Loop' for SBC binding. **Note:** This notification is platform-specific.
620	The gateway %1$s cannot have multiple media interfaces because it is bound to the SBC.	Warning	When a gateway is configured for SBC binding, the **Gateway.MediaNetworks** parameter cannot contain multiple media interfaces. **Note:** This notification is platform-specific.

NumKey	Message	Severity	Description
630	The gateway %1$s servers configuration does not allow correct SBC binding.	Warning	The %sbc% macro was found in at least one of the servers used by the gateway, but the servers configuration is not consistent. The allowed configurations are: • The outbound proxy is set to %sbc%. • The outbound proxy is not set, the home domain proxy is set to %sbc% and the registrar and messaging servers are either configured to %sbc% or not configured. **Note:** This notification is platform-specific.
640	KPML SUBSCRIBE from %1$s to %2$s was rejected because it is out-of-dialog.	Warning	A KPML SUBSCRIBE was rejected because it was not in a call dialog. This notification is not sent if the SUBSCRIBE is rejected because the KPML is disabled in the **UasKpmlSupport** parameter.
650	KPML SUBSCRIBE from %1$s to %2$s was rejected because a subscribe is already active.	Warning	A KPML SUBSCRIBE was rejected because a subscription is already active in the call dialog.
660	KPML SUBSCRIBE from %1$s to %2$s was rejected because of an invalid content.	Warning	A KPML SUBSCRIBE was rejected because it contains unsupported content. This notification is not sent if the SUBSCRIBE is rejected because the KPML is disabled in the **UasKpmlSupport** parameter.
670	Gateway %1$s has a new connection available to %2$s.	Info	A new connection is ready for an eventual registration attempt by an Endpoint gateway. This notification is issued only for Endpoint gateways.
680	Gateway %1$s is registering to %2$s.	Info	The Endpoint gateway is starting a registration attempt to one of its target. This notification is issued only for Endpoint gateways.
690	Gateway %1$s has an active connection to %2$s.	Info	The Endpoint gateway is now using the specified target as the active connection. This notification is issued only for Endpoint gateways.

NumKey	Message	Severity	Description
700	Gateway %1$s failed registration: %2$s.	Error	The Endpoint gateway could not register successfully. This notification is issued only for Endpoint gateways.
710	Gateway %1$s received a connection error with %2$s.	Error	A connection error occured on an Endpoint gateway. This notification is issued only for Endpoint gateways.
720	Gateway %1$s detected a SIP connection error with %2$s.	Error	A SIP connection error occurred on an Endpoint gateway. The error can be because the connection does not exist, an ICMP error was received, a SIP timeout occurred, etc. This notification is issued only for Endpoint gateways.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.

NumKey	Message	Severity	Description
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.

NumKey	Message	Severity	Description
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to SipEp.

Message	Severity	Description
The limit of %1$d registrations is reached with the current gateways and registrations configuration.	Warning	This message is issued when the total number of registrations currently configured reached the defined limit. Verify that the Gateway Names are properly configured for each registrations and that the total number of registrations is below the limit.
The TLS certificate validation is disabled.	Warning	This message is issued when the TLS certificate validation is disabled. The unit is vulnerable to attacks. Ensure that the TLS certificate validation is set to a stronger level.
Keep-Alive not allowed for Endpoint gateways.	Warning	This message is issued if an incompatible SIP Keep-Alive method is enabled on an Endpoint gateway. SIP Keep-Alive is not supported for Endpoint gateways. In this case the SIP Keep-Alive feature is completely disabled. See the **Gateway.Type** and **SipKeepAliveMethod** parameters for details.
DNS failure concealement is not allowed on Trunk gateways.	Warning	This message is issued if a gateway is set to type 'Trunk' and DNS failure concealment is active. DNS failure concealment is not supported for Trunk gateways. In this case the DNS concealment feature is considered to be set to 'None'. See the **Gateway.Type** and **DnsFailureConcealment** parameters for details.
Listening SIP ports are not allowed for Endpoint gateways.	Warning	This message is issued when the port or secure port is set to non-zero value on an Endpoint gateway. Listening ports are not allowed on Endpoint gateways. See **Gateway.Port**, **Gateway.SecurePort** and **Gateway.Type** parameters for details.
Symmetric UDP source port not disabled for Endpoint gateways.	Warning	This message is issued if the **InteropSymmetricUdpSourceportEnable** parameter is set to 'disable' and an Endpoint gateway is configured. This parameter have no effect on Endpoint gateways. Endpoint gateways always use symmetric local ports.

Message	Severity	Description
SIP monitoring notifications are not allowed on Endpoint gateways.	Warning	This message is issued if the **SipNotificationsGateway** parameter set to an Endpoint gateway. In this case the SIP monitoring notifications are disabled..
Penalty Box is not allowed on Endpoint gateways.	Warning	This message is issued if the **PenaltyBoxEnable** parameter is set to 'Enable' and a gateway is set to type 'Endpoint'. Penalty Box is not allowed on Endpoint gateways. In this case the PenaltyBox feature is completely disabled.
Unit Registrations are not allowed for Endpoint gateway.	Warning	This message is issued if a unit registration entry is associated with an Endpoint gateway. Unit registrations are not supported for Endpoint gateways but remain active for gateways of other types. See the **Gateway.Type** and Unit**Registrations.GatewayName** parameters for details.
Invalid configuration of SIP Failover Conditions %1$s for gateway %2$s. Using %3$s instead.	Warning	This message is issued when the configuration of the SIP Failover Conditions is not supported on this type of gateway. The gateway uses the indicated configuration instead.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.

Message	Severity	Description
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

SIP Proxy (SipProxy)

The SIP Proxy (SipProxy) service is used to add local survivability for local endpoints and SIP phones.

Parameters

MonitoringState (Status Parameter)

Type	Enum
Range	DestinationIsUp(100) | DestinationIsDown(200) | Inactive(300) | Unknown(400)
Script/CLI	SipProxy.MonitoringState
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.100.100

Indicates the current monitoring status. A SIP server is monitored to determine if it is usable. Monitoring is performed through the SIP OPTIONS method.

- DestinationIsUp: The destination SIP server correctly responds and is considered to be alive.
- DestinationIsDown: The destination SIP server fails to correctly respond. The destination SIP server is considered to be down.
- Inactive: The monitoring is not in use.
- Unknown: The initial response to monitoring has not yet been received. This is the initial state when monitoring is used.

ProxyStatus (Status Parameter)

Type	Enum
Range	Starting(100) | Running(200) | RunningInSurvivability(300) | Stopping(400) | ErrorPortAlreadyInUse(500) | ErrorWaitingForTimeSynchronization(600) | ErrorInternal(700)
Script/CLI	SipProxy.ProxyStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.100.200

The SipProxy service current status.

- Starting: The SIP proxy is starting: it cannot listen for incoming SIP traffic or send SIP traffic.
- Running: The SIP proxy acts in transparent mode: it does not respond to REGISTER requests and it transparently forwards SIP messages to their normal routes. Registration Throttling can be activated in that state.
- RunningInSurvivability: The SIP proxy acts in survivability mode: it responds to REGISTER requests and it routes SIP messages.
- Stopping: The SIP proxy is stopping: it cannot listen for incoming SIP traffic or send SIP traffic.

- ErrorPortAlreadyInUse: The SIP proxy cannot open its IP port because the port is already used by a SIP gateway.
- ErrorWaitingForTimeSynchronization: The SIP proxy is started but it cannot open the SIP TLS port because the real-time clock is not synchronised. This generally occurs when the SNTP server is not set or is unreachable.
- ErrorInternal: The SIP proxy cannot start because of an internal error. Refer to the release notes or contact a technical support specialist.

NbActiveCalls (Status Parameter)

Type	UInt32
Range	
Script/CLI	SipProxy.NbActiveCalls
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.100.250

The number of active calls currently handled by the SIP proxy.
The maximum number of active calls is platform-dependent.

PersistentConnectionStatus (Table)

This table holds the status of the persistent connections.

Id (Index) | Table: PersistentConnectionStatus

Type	UInt32
Range	
Script/CLI	SipProxy.PersistentConnectionStatus[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.100.300.1.100

Unique identifier of the row.

LocalPort (Status Parameter) | Table: PersistentConnectionStatus

Type	ExtIpPort
Range	
Script/CLI	SipProxy.PersistentConnectionStatus[].LocalPort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.100.300.1.300

Local port used by the persistent connection.

RemoteHost (Status Parameter) | Table: PersistentConnectionStatus

Type	Text
Range	
Script/CLI	SipProxy.PersistentConnectionStatus[].RemoteHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.100.300.1.400

The remote host used to establish the persistent connection. The remote host can be a host name or an IP address of the proxy, outbound proxy, or registrar.

RemoteHostIpAddr (Status Parameter) | Table: PersistentConnectionStatus

Type	Text
Range	
Script/CLI	SipProxy.PersistentConnectionStatus[].RemoteHostIpAddr
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.100.300.1.450

The resolved IP address of the remote host used to establish the persistent connection.

State (Status Parameter) | Table: PersistentConnectionStatus

Type	Enum
Range	Up(100) | Down(200) | WaitingShutdown(300) | WaitingUp(400)
Script/CLI	SipProxy.PersistentConnectionStatus[].State
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.100.300.1.500

The current state of the persistent connection.

- Up: The connection is established and ready to be used.
- Down: The connection is not established.
- WaitingShutdown: The connection is established but in a graceful shutdown.
- WaitingUp: The connection is established but not yet ready to be used.

Transport (Status Parameter) | Table: PersistentConnectionStatus

Type	Enum
Range	Udp(100) | Tcp(200) | Tls(300)
Script/CLI	SipProxy.PersistentConnectionStatus[].Transport
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.100.300.1.600

The current Transport of the persistent connection.

- Udp: Transport for the connection is UDP.
- Tcp: Transport for the connection is TCP.
- Tls: Transport for the connection is TLS.

SurvivabilityMode (Config Parameter)

Type	Enum
Range	Automatic(100) | AlwaysOn(200) | Disabled(300)
Default	Automatic
Script/CLI	SipProxy.SurvivabilityMode
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.200.100

Survivability mode executed by the SIP proxy.

- Automatic: The SIP proxy applies the normal survivability strategy, i.e. it uses monitoring to determine if the SIP server is up or down.
- AlwaysOn: The SIP proxy always acts as if the SIP server is down. Useful for debugging.
- Disabled: The SIP proxy always acts as if the SIP server is up. Useful for debugging.

Note that this parameter does not affect whether monitoring is performed or not.

OutboundProxyHost (Config Parameter)

Type	IpHostNamePort
Range	
Default	
Script/CLI	SipProxy.OutboundProxyHost
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.200.200

Outbound proxy server FQDN and port.
To disable the outbound proxy, leave the **OutboundProxyHost** parameter empty.

When the parameter is enabled, each time an incoming requests arrives from an endpoint, the SipProxy will insert a Route header pointing to its configured outbound proxy as the first route. The Request-URI still contains the home domain proxy address.

The monitoring requests are also sent through this outbound proxy. The SIP proxy uses persistent connections, or a virtual persistent connections for UDP, to create a path towards the outbound proxy.

ConfigModifiedStatus (Status Parameter)

Type	Enum
Range	Yes(100) | No(200)
Script/CLI	SipProxy.ConfigModifiedStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.200.300

Indicates that some configuration changes need the `ApplyConfiguration` command to be executed in order to take effect or to be validated. Restarting the service will also apply these changes.

- Yes: The configuration has been modified but has not been applied.
- No: The configuration has not been modified.

Use the `ApplyConfiguration` command to apply the configuration.

ConfigAppliedStatus (Status Parameter)

Type	Enum
Range	Yes(100) | No(200)
Script/CLI	SipProxy.ConfigAppliedStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.200.400

Indicates that the configuration changes were applied or not.

- Yes: Configuration changes were applied successfully.
- No: Configuration changes not applied because of errors.

NetworkInterface (Config Parameter)

Type	Text
Range	Size(1..50)
Default	Uplink
Script/CLI	SipProxy.NetworkInterface
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.300.100

The network on which the SIP proxy listens for incoming SIP traffic and sends SIP traffic.

Port (Config Parameter)

Type	ExtIpPort
Range	
Default	0
Script/CLI	SipProxy.Port
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.300.200

Port on which the SIP proxy listens for incoming unsecure SIP traffic.
This is used only when UDP and/or TCP transports are enabled.

If set to 0, the unit uses the default SIP port.

SecurePort (Config Parameter)

Type	ExtIpPort
Range	
Default	0
Script/CLI	SipProxy.SecurePort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.300.300

Port on which the SIP proxy listens for incoming secure SIP traffic.
This is used only when the TLS transport is enabled.

If set to 0, the unit uses the default SIP secure port.

ContactOverrideEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	SipProxy.ContactOverrideEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.400.50

Defines if the SIP proxy should modify the Contact header of REGISTER requests.

- Disabled: Act as a transparent proxy. Generally not recommended in TLS.
- Enabled: Modify the Contact header of REGISTER requests with the IP address and port of the proxy, so inbound requests are routed back to the proxy. Also adds an alias in the Contact URI for tracking purposes.

EndpointSurvivabilityExpiration (Config Parameter)

Type	UInt32
Range	10..86400
Default	90
Script/CLI	SipProxy.EndpointSurvivabilityExpiration
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.400.100

Configures the maximum registration expiration delay, i.e. the EXPIRES value returned by the SIP proxy registrar in the 200 OK responses.
This value is expressed in seconds (s).

This parameter applies only when the survivability mode is active, when the SIP proxy's internal registrar replies to the REGISTER requests.

- If the value included in the REGISTER is lower or equal to the value of this parameter, the value included in the REGISTER is used.
- Otherwise, the value defined by the **EndpointSurvivabilityExpiration** parameter is used.

Note: Using expiration values smaller than 32 seconds may cause conflicts with the SIP retransmission timeouts. It is not recommended to use expiration values smaller than 32 seconds unless the network environment requires very few retransmissions or the retransmission timeouts of the devices are set to short values.

RelayedThrottlingExpiration (Config Parameter)

Type	UInt32
Range	0..0 | 10..86400
Default	0
Script/CLI	SipProxy.RelayedThrottlingExpiration
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.400.200

Configures the expiration value in the REGISTERs relayed to the external registrar when Registration Throttling is used.
This value is expressed in seconds (s).

A value of 0 has the effect proposing no expiration value to the registrar during Registration Throttling. Any expiration value present in the REGISTER is removed before relaying it to the registrar.

The value of the **RelayedThrottlingExpiration** should be at least twice the value of the **EndpointThrottlingExpiration** parameter otherwise Registration Throttling is ineffective.

The expiration value returned by the registrar in the 200 OK response always has precedence over the expiration value that we propose in the REGISTER requests sent to the registrar

Note: Using expiration values smaller than 32 seconds may cause conflicts with the SIP retransmission timeouts. It is not recommended to use expiration values smaller than 32 seconds unless the network environment requires very few retransmissions or the retransmission timeouts of the devices are set to short values.

EndpointThrottlingExpiration (Config Parameter)

Type	UInt32
Range	0..0 | 10..3600
Default	120
Script/CLI	SipProxy.EndpointThrottlingExpiration
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.400.300

Configures the maximum registration expiration on the endpoint side when Registration Throttling is used.
This value is expressed in seconds (s).

A value of 0 disables Registration Throttling.

The value of the **RelayedThrottlingExpiration** should be at least twice the value of the **EndpointThrottlingExpiration** parameter otherwise Registration Throttling is ineffective.

This parameter applies only when the Registration Throttling replies to REGISTER requests.

- If the expiration value included in the REGISTER is lower or equal to the value of this parameter, the value included in the REGISTER is used.
- Otherwise, the value defined by the **EndpointThrottlingExpiration** parameter is used.
- The expiration value returned by the registrar in the 200 OK has no impact on the expiration used on the endpoint side.

Note: Using expiration values smaller than 32 seconds may cause conflicts with the SIP retransmission timeouts. It is not recommended to use expiration values smaller than 32 seconds unless the network environment requires very few retransmissions or the retransmission timeouts of the devices are set to short values.

RegistrationCacheSearchName (Status Parameter)

Type	Text
Range	
Script/CLI	SipProxy.RegistrationCacheSearchName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.400.400.100

The name pattern to search in **Aor** and **Contact** from the registration database used to populate the **RegistrationCacheSearchResult** table when using the **SearchRegistration** command.

RegistrationCacheSearchSort (Status Parameter)

Type	Enum
Range	Aor(100) | Contact(200) | ReceivedTime(300) | EndpointExpiration(400) | RegistrarExpiration(500) | Unsorted(1000)
Script/CLI	SipProxy.RegistrationCacheSearchSort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.400.400.200

The sort order applied to **RegistrationCacheSearchResult** table when using the **SearchRegistration** command.

- Aor: Address of record in the REGISTER.
- Contact: Contact in the REGISTER.
- ReceivedTime: Time at which the registration was received.
- EndpointExpiration: Time at which the endpoint-side registration expires.
- RegistrarExpiration: Time at which the registrar-side registration expires.
- Unsorted: Internal cache order.

RegistrationCacheSearchResult (Table)

This table contains the registration cache entries filtered by the **SearchRegistrationCache** command.

Id (Index) | Table: RegistrationCacheSearchResult

Type	UInt32
Range	
Script/CLI	SipProxy.RegistrationCacheSearchResult[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.400.400.300.1.100

Unique numerical identifier for a registration search result.

Aor (Status Parameter) | Table: RegistrationCacheSearchResult

Type	Text
Range	
Script/CLI	SipProxy.RegistrationCacheSearchResult[].Aor
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.400.400.300.1.200

The Address of Record, in URI format, present in the REGISTER.
For example: sip:alice@example.com

This value is taken from the REGISTER.

Contact (Status Parameter) | Table: RegistrationCacheSearchResult

Type	Text
Range	
Script/CLI	SipProxy.RegistrationCacheSearchResult[].Contact
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.400.400.300.1.300

The Contact, in URI format, present in the REGISTER.
For example: sip:5551212@192.168.11.23:5060

This value is taken from the REGISTER.

ReceivedTime (Status Parameter) | Table: RegistrationCacheSearchResult

Type	Text
Range	
Script/CLI	SipProxy.RegistrationCacheSearchResult[].ReceivedTime
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.400.400.300.1.400

Time at which the registration was received. Expressed as the local time computed from the Time Zone defined in the **Hoc.StaticTimeZone** parameter.
Format is DD/MM/YYYY hh:mm:ss

EndpointExpiration (Status Parameter) | Table: RegistrationCacheSearchResult

Type	Text
Range	
Script/CLI	SipProxy.RegistrationCacheSearchResult[].EndpointExpiration
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.400.400.300.1.500

Time at which the registration expires on the endpoint side. Expressed as a local time computed from the Time Zone defined in the **Hoc.StaticTimeZone** parameter.
Format is DD/MM/YYYY hh:mm:ss

The expiration time of the endpoint side can differ from the expiration time of the registrar side. This happens:

- if Registration Throttling is enabled and the expiration delay is shorter on the endpoint side, or
- if the system is in survivability.

RegistrarExpiration (Status Parameter) | Table: RegistrationCacheSearchResult

Type	Text
Range	
Script/CLI	SipProxy.RegistrationCacheSearchResult[].RegistrarExpiration
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.400.400.300.1.550

Time at which the registration expires on the registrar side. Expressed as a local time computed from the Time Zone defined in the **Hoc.StaticTimeZone** parameter.
Format is DD/MM/YYYY hh:mm:ss

The expiration time of the endpoint side can differ from the expiration time of the registrar side. This happens:

- if Registration Throttling is enabled, where the expiration delay is shorter on the endpoint side, or
- if the system is in survivability.

When the SipProxy service state switches to RunningInSurvivability, all the registrations on the registrar side are overridden at the time the switch occurred. This ensures that endpoint registrations are quickly refreshed on the registrar side after the system exits from survivability mode.

RegisteredTo (Status Parameter) | Table: RegistrationCacheSearchResult

Type	Enum
Range	Normal(100) | Local(200)
Script/CLI	SipProxy.RegistrationCacheSearchResult[].RegisteredTo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.400.400.300.1.600

Registrar that handled the registration.

- Normal: The registration was forwarded to the normal registrar.
- Local: The registration was handled by the local registrar.

TotalRegistrationCacheCount (Status Parameter)

Type	UInt32
Range	
Script/CLI	SipProxy.TotalRegistrationCacheCount
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.400.400.400

The total number of registrations cached by the SipProxy service. This number also includes the registrations in progress but not yet completed.

MonitoringInterval (Config Parameter)

Type	UInt32
Range	0..3600
Default	30
Script/CLI	SipProxy.MonitoringInterval
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.500.100

Interval at which monitoring requests are sent to verify the SIP server status.
This value is expressed in seconds (s).

SIP OPTIONS are sent periodically to the monitored SIP server.

The SIP server is considered unreachable if one of these conditions occurs:

- No response is received after the retransmission timer expires (configurable via the **InteropRequestTransactionTimeout** parameter).
- The response code received is listed in the **KeepAliveOptionErrorCodes** parameter.

When the SIP server is considered unreachable, the survivability mode enters its active state. Monitoring is still performed when the SIP server is unreachable and as soon as it becomes reachable again, the survivability mode becomes inactive.

Setting this parameter to 0 disables the monitoring.

MonitoringToggleDelay (Config Parameter)

Type	UInt32
Range	0..3600
Default	0
Script/CLI	SipProxy.MonitoringToggleDelay
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.500.200

Delay before reporting a status change of the monitored destination.
This value is expressed in seconds (s).

Monitoring must succeed or fail for at least this duration to conclude that the state of monitoring has changed (toggled).

Delay measurement is reset each time the result of a monitoring attempt is obtained that reconfirms the current state of monitoring.

MonitoringDestination (Config Parameter)

Type	IpHostNamePort
Range	
Default	
Script/CLI	SipProxy.MonitoringDestination
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.500.300

Destination target. FQDN and port for a specific SIP proxy.

KeepAliveOptionErrorCodes (Config Parameter)

Type	Text
Range	Size(0..255)
Default	
Script/CLI	SipProxy.KeepAliveOptionErrorCodes
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.500.400

Comma-separated list of response codes indicating that the SIP server is down, when monitoring is performed through SIP OPTIONS.

SipOptionsMethodSupport (Config Parameter)

Type	Enum
Range	Default(100) | AcceptAll(200) | RejectAll(300)
Default	Default
Script/CLI	SipProxy.SipOptionsMethodSupport
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.600.100

Determines the behaviour of the SIP proxy when answering a SIP OPTIONS request.

- Default: The SIP proxy responds with a 200 OK only if the SIP proxy is the destination of the OPTIONS request regardless of the other content. If the SIP proxy is not the destination, the OPTIONS request is forwarded.
- AcceptAll: The SIP proxy accepts all OPTIONS requests and responds with a 200 OK, regardless of the content and destination.
- RejectAll: The SIP proxy rejects all OPTIONS requests and responds with an error 405 Method Not Allowed.

Route (Table: user-defined, 25 lines max.)

This table contains the routes that can be applied by the SIP proxy. Each table entry is a route. When a SIP request must be routed, the table is searched in decreasing priority order to find the first matching route. A route is selected when the criteria defined by **CriteriaType** and **CriteriaExpression** parameters matches.

Id (Index) | Table: Route

Type	UInt32
Range	
Script/CLI	SipProxy.Route[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.700.100.1.100

Unique numerical identifier for a routing rule.

Priority (Config Parameter) | Table: Route

Type	UInt32
Range	
Default	1
Script/CLI	SipProxy.Route[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.700.100.1.200

Priority used to determine search order in the table when routing is executed.

CriteriaType (Config Parameter) | Table: Route

Type	Enum
Range	ToUri(100) | ToUser(200) | ToHost(300) | ContactUri(400) | ContactUser(500) | ContactHost(600)
Default	ToUser
Script/CLI	SipProxy.Route[].CriteriaType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.700.100.1.300

Type of criteria used to match the routing rule against the SIP message.

- ToUri: The full URI of the TO header.
- ToUser: The user part of the URI in the TO header.
- ToHost: The host part of the URI in the TO header.
- ContactUri: The full URI of the CONTACT header.
- ContactUser: The user part of the URI in the CONTACT header.
- ContactHost: The host part of the URI in the CONTACT header.

CriteriaExpression (Config Parameter) | Table: Route

Type	Text
Range	Size(0..255)
Default	
Script/CLI	SipProxy.Route[].CriteriaExpression
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.700.100.1.400

Regular expression compared with the value of the Criteria Type found in the SIP message. If it matches, the route defined by this table entry is used.
The regular expression is implicitly searched from the beginning of the searched string. The regular expression must not contain the begin string character (^).

The special syntax %gateway=gw_name% can be used to refer to an internal gateway. The gw_name refers to the gateway name as it appears in the **SipEp.Gateway.Name** parameter.

TargetType (Config Parameter) | Table: Route

Type	Enum
Range	RegisteredAor(100) | RegisteredAorUser(200) | HardcodedHost(300)
Default	RegisteredAorUser
Script/CLI	SipProxy.Route[].TargetType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.700.100.1.500

Type of target used by the route.

- RegisteredAor: Routing is based on the registration database. Entries with an AOR matching the Request-URI (R-URI) of the SIP request are looked up in the database. Matching is based on the full AOR.
- RegisteredAorUser: Routing is based on the registration database. Entries with an AOR matching the R-URI of the SIP request are looked up in the database. Matching is based on the user portion of the AOR.
- HardcodedHost: The SIP request is routed to the host defined by the **HardcodedHostPort** parameter. The use of a specific phone number can also be forced by using the transformation specified by the **Route.TargetUserTransformationName** parameter. When this option is selected, the **Route.RegisteredUserTransformationName** parameter is not used.

TargetUserTransformationName (Config Parameter) | Table: Route

Type	Text
Range	Size(0..255)
Default	
Script/CLI	SipProxy.Route[].TargetUserTransformationName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.700.100.1.600

Name of the transformation in the **UserTransformations** table. This transformation is applied to the user part of the target Request-URI (R-URI) in the SIP request. This transformation allows modifying the user part of the R-URI in a SIP request forwarded by the router. This parameter can be used to modify a phone number: add/remove a regional code, add a prefix, add a suffix, ...

RegisteredUserTransformationName (Config Parameter) | Table: Route

Type	Text
Range	Size(0..255)
Default	
Script/CLI	SipProxy.Route[].RegisteredUserTransformationName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.700.100.1.700

Name of a transformation in the **UserTransformations** table. This transformation is used during the registration database lookup, to normalise the database entries before checking for matches. The transformation is applied to the user part of the **RegistrationStatus.Aor** parameter. Only a copy of the parameter is modified: this transformation does not modify the content of the **RegistrationStatus** table.

This parameter is ignored when the **Route.TargetType** parameter is set to 'HardcodedHost'.

HardcodedHostPort (Config Parameter) | Table: Route

Type	IpHostNamePort
Range	
Default	
Script/CLI	SipProxy.Route[].HardcodedHostPort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.700.100.1.800

Hardcoded host that can be used as a target in routes. The host can be expressed as an IP address or a domain name. The port is optional. A port value of 0 is interpreted as the default port.
The special %gateway=gw_name% syntax can be used to refer to an internal gateway. The gw_name refers to the gateway name as it appears in the **SipEp.Gateway.Name** parameter.

ConfigStatus (Status Parameter) | Table: Route

Type	Enum
Range	Valid(100) | PriorityDuplicate(200) | MissingHardcodedHostport(300) | InexistentTargetUserTransformation(400) | InexistentRegisteredUserTransformation(500) | Invalid(600)
Script/CLI	SipProxy.Route[].ConfigStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.700.100.1.2000

Indicates if the configuration of this row is valid.

- Valid: The current content of the row is valid.
- PriorityDuplicate: Two or more entries have the same priority.
- MissingHardcodedHostport: The **TargetType** parameter is set to 'HardcodedHost' but the **HardcodedHostPort** parameter is not configured.
- InexistentTargetUserTransformation: The **TargetUserTransformationName** parameter refers to an inexistent transformation.
- InexistentRegisteredUserTransformation: The **RegisteredUserTransformationName** parameter refers to an inexistent transformation.
- Invalid: The current content of the row is invalid.

Delete (Row Command) | Table: Route

Script/CLI:	SipProxy.Route[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.700.100.1.2100

Deletes this row.

UserTransformations (Table: user-defined, 100 lines max.)

This table contains the transformations to be applied to a user portion of a URI. The name and the criteria must match to have the transformation applied. There can be multiple entries with the same name. The entries are checked in decreasing priority order and the first entry with matching name and criteria is applied. If no matching entry is found, no transformation is applied and the user stays unmodified.

Id (Index) | Table: UserTransformations

Type	UInt32
Range	
Script/CLI	SipProxy.UserTransformations[].Id
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.700.300.1.100

Unique numerical identifier.

Priority (Config Parameter) | Table: UserTransformations

Type	UInt32
Range	
Default	1
Script/CLI	SipProxy.UserTransformations[].Priority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.700.300.1.200

Priority used to determine search order in the table when routing is executed. Search order is from lower to higher priority values.
Entries with the same name must have different prioriry values.

Name (Config Parameter) | Table: UserTransformations

Type	Text
Range	Size(0..50)
Default	
Script/CLI	SipProxy.UserTransformations[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.700.300.1.300

The name of the transformation. There can be several transformations of the same name. Must match values of **RegisteredUserTransformationName** or **UserTransformationName** parameters.

Criteria (Config Parameter) | Table: UserTransformations

Type	Text
Range	Size(0..250)
Default	
Script/CLI	SipProxy.UserTransformations[].Criteria
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.700.300.1.400

The criteria to be used in the transformation. If the criteria does not match, the search in the table continues. The criteria is a regular expression used for two things:

- Matching: If the expression matches, this transformation is used. If it does not, the search continues for entries with the same name in the table.
- Creating groups to be used as backreferences in the pattern expression.

The regular expression is implicitly searched from the beginning of the searched string: the begin string character (^) must not be used in the regular expression.

Pattern (Config Parameter) | Table: UserTransformations

Type	Text
Range	Size(0..250)
Default	
Script/CLI	SipProxy.UserTransformations[].Pattern
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.700.300.1.500

Pattern expression that creates the transformed value. Can use backreferences to the groups created in the criteria.

ConfigStatus (Status Parameter) | Table: UserTransformations

Type	Enum
Range	Valid(100) | PriorityDuplicate(200) | MissingName(300) | Invalid(400)
Script/CLI	SipProxy.UserTransformations[].ConfigStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.700.300.1.2000

Indicates if the configuration of this row is valid.

- Valid: The current content of the row is valid.
- PriorityDuplicate: Two or more entries with the same name have the same priority.
- MissingName: The entry must have a name.
- Invalid: The current content of the row is invalid.

Delete (Row Command) | Table: UserTransformations

Script/CLI:	SipProxy.UserTransformations[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.700.300.1.2100

Deletes this row.

InteropRequestTransactionTimeout (Config Parameter)

Type	UInt32
Range	1..32
Default	32
Script/CLI	SipProxy.InteropRequestTransactionTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.800.100

The transaction timeout for SIP requests. Corresponds to timers B and F in RFC 3261.
This value applies to:

- all requests (INVITE as well as non-INVITE) relayed by the SipProxy service, and
- the monitoring requests initiated by the SipProxy itself.

Setting this parameter to a relatively small value is useful in cases where the SipProxy handles a request with an FQDN that resolves to several targets. It gives time to try several targets when the first target(s) do not respond.

Example: if this parameter is set to 5 seconds and the SIP client that sent a request through the SipProxy has a transaction timeout of 32 seconds, the SipProxy is able to try about 6 targets before the transaction timer of the SIP client expires.

This parameter is ignored if it has a value larger than the value of the **SipEp.InteropTransmissionTimeout** parameter.

This value is expressed in seconds (s).

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	SipProxy.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	SipProxy.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4600.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

ApplyConfiguration (Command)

Apply the SipProxy configuration changes that do not take effect immediately during edition.

The **ConfigModifiedStatus** parameter indicates if some changes are pending.

The execution of this command is refused when the **NeedRestartInfo** parameter is set.

See also the `CancelEdits` command.

CancelEdits (Command)

Cancel the configuration changes that are not currently applied.
The **ConfigModifiedStatus** parameter indicates if some changes are currently not applied.

InsertRoute (Command)

Inserts a new row in the **Route** table.

Id (Argument) | Command: InsertRoute

Type	UInt32
Range	0..2147483647
Default	0

Unique numerical identifier for a **Route** table entry.

The special value '0' (default value) inserts the route at the end of the table and generates an ID equal to the largest current ID value + 1.

InsertUserTransformation (Command)

Inserts a new row in the **UserTransformation** table.

Id (Argument) | Command: InsertUserTransformation

Type	UInt32
Range	0..2147483647
Default	0

Unique numerical identifier for a Route table entry.
The special value '0' (default value) inserts the route at the end of the table and generates an ID equal to the largest current ID value + 1.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

SearchRegistrationCache (Command)

Search through the registration cache of the proxy, and filter by the **Name** parameter.
The results are returned in the **RegistrationCacheSearchResult** table.

Name (Argument) | Command: SearchRegistrationCache

Type	Text
Range	Size(0..256)
Default	

The name pattern to search in the **Address of Record** and **Contact** fields from the registration cache.

Sort (Argument) | Command: SearchRegistrationCache

Type	Enum
Range	Aor(100) | Contact(200) | ReceivedTime(300) | EndpointExpiration(400) | RegistrarExpiration(500) | Unsorted(1000)
Default	ReceivedTime

The sort order applied to **RegistrationCacheSearchResult** table.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the SipProxy service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.4600.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	The SIP proxy is entering in survivability mode.	Warning	The unit enters in survivability mode when the SIP server fails to respond to monitoring. The reason why the SIP server failed to respond should be investigated.
20	The SIP proxy is exiting survivability mode.	Warning	The unit exits the survivability mode when the SIP server restarts responding to monitoring.
30	SIP registration was rejected by the SIP proxy. Maximum allowed number of licences exceeded.	Warning	This message is issued when the SIP proxy rejects a SIP registration because the maximum number of licences is exceeded.
40	SIP invite was rejected by the SIP proxy. Maximum number of simultaneous calls exceeded.	Warning	This message is issued when the SIP proxy rejects a SIP invite because the maximum number of simultaneous calls supported in survivability mode is exceeded.
50	SIP request was rejected by the SIP proxy. Method=%1$s Cause= %2$s.	Debug	This message is issued when the SIP proxy rejects a SIP request. The cause is stated in the message.
60	The licence activation parameters of the SipProxy service have changed. Please restart the service.	Warning	This message is sent when a new licence key has been activated on the device and the licence parameters have changed. The SipProxy service needs to be restarted for the new parameters to take effect.
70	The server (%1$s) is now reachable by the SIP proxy.	Warning	This message is issued when the server was unreachable but now answers the keep alive request.
80	Cannot start the keep alive mechanism for SIP proxy because the specified destination (%1$s) is in the wrong IP address version.	Error	This message is issued when the specified destination of the keep alive mechanism has an IP address version different than the SIP proxy.
90	The server (%1$s) cannot be reached by the SIP proxy.	Error	This message is issued when the server does not answer the keep alive request.
100	Cannot start the keep alive mechanism for SIP proxy because no destination is specified.	Error	This message is issued when the keep alive mechanism is configured to use a destination and none is specified for the SIP proxy.

NumKey	Message	Severity	Description
110	The configuration cannot be applied because of errors. Check the SipProxy service configuration.	Error	This message is sent when the configuration cannot be applied because of configuration errors.
140	%1$s connection with remote host (%2$s) failed because it is either unreachable or not listening for %3$s on the specified port.	Error	This message is issued when a persistent connection cannot be established with a remote host because it is either unreachable or it is not listening on the specified port.
150	TLS connection with remote host (%1$s) failed because the received certificate is not trusted.	Error	This message is issued when a TLS persistent connection cannot be established with a remote host because the received certificate is not trusted.
160	%1$s connection using local port %2$d failed because another entity is already listening on this port.	Error	This message is issued when a persistent connection cannot be established with a remote host because the local port used to establish the connection is already used by another entity. Verify that there is no other entities that are listening on the specified port.
170	%1$s connection with remote host (%2$s), using the local address %3$s:%4$d on the %5$s signalling network interface, failed.	Error	This message is issued when a persistent connection cannot be established with a remote host. Validate that the SIP local configuration (gateway, transport, servers, addresses and port) is properly set.
180	%1$s connection with the remote host (%2$s) failed because of an unspecified error.	Error	This message is issued when a persistent connection cannot be established with a remote host and the reason is not available.
190	%1$s connection with the remote host (%2$s) is now established for SIP proxy.	Info	This message is issued when a persistent connection is established.
200	%1$s connection with the remote host (%2$s) is now ready to be used for SIP proxy.	Info	This message is issued when a persistent connection is established and ready to be used.

NumKey	Message	Severity	Description
210	Gracefully terminating %1$s connection with the remote host (%2$s) for SIP proxy.	Info	This message is issued when a persistent connection initiate a graceful terminate. This occurs when a higher priority persistent connection is established.
220	%1$s connection with the remote host (%2$s) is now terminated for SIP proxy.	Info	This message is issued when a persistent connection is terminated.
230	SipProxy: New call from %1$s to %2$s.	Debug	This message is issued when the SIP proxy starts handling a call.
240	SipProxy: Call from %1$s to %2$s is terminated.	Debug	This message is issued when the SIP proxy has finished handling the call.
250	SipProxy: New public IP/port (%1$s:%2$d) detected.	Info	This message is issued when a new public IP address is detected from the received SIP REGISTER or monitoring OPTIONS responses. A value of ":-1" means "rport" is missing, in which case the SipEp.TransportAddRPortEnable parameter should be enabled to prevent NAT issues.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.

NumKey	Message	Severity	Description
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.

NumKey	Message	Severity	Description
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to SipProxy.

Message	Severity	Description
The configuration cannot be applied because of errors. Check the SipProxy service configuration.	Error	This message is sent when the configuration cannot be applied because of configuration errors.
The value of the RelayedThrottlingExpiration parameter should be at least twice the value of the EndpointThrottlingExpiration parameter.	Warning	The value of the **RelayedThrottlingExpiration** parameter should be at least twice the value of the **EndpointThrottlingExpiration** parameter, otherwise Registration Throttling is ineffective. Set these parameters correctly.
More than %1$d results (please refine the search)	Warning	This message is sent when the number of search results obtained from the **SearchRegistration** command exceeds the maximum number allowed.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.

Message	Severity	Description
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Simple Network Management Protocol (Snmp)

The Simple Network Management Protocol (SNMP) service allows the administrator to manage the unit using the SNMP protocol.

Parameters

EnableSnmpV1 (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Snmp.EnableSnmpV1
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.900.1.200.200

Specifies if a user can connect to the system by using SNMPv1. Please note that a "public" user might be granted (unsecure) access by using v1 while an "admin" user should rather be granted a v3 access.

EnableSnmpV2 (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Snmp.EnableSnmpV2
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.900.1.200.300

Specifies if a user can connect to the system by using SNMPv2. Please note that a "public" user might be granted (unsecure) access by using v2 while an "admin" user should rather be granted a v3 access.

EnableSnmpV3 (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Snmp.EnableSnmpV3
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.900.1.200.400

Specifies if a user can connect to the system by using SNMPv3. Please note that a "public" user might be granted (unsecure) access by using v1 while an "admin" user should rather be granted a v3 access.

AuthProtocol (Config Parameter)

Type	Enum
Range	Md5(100) | Sha1(200)
Default	Md5
Script/CLI	Snmp.AuthProtocol
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.900.1.200.500

Protocol to use with SNMPv3.

- Md5: MD5 encoding is used.
- Sha1: SHA1 encoding is used.

PrivProtocol (Config Parameter)

Type	Enum
Range	None(0) | Des(100)
Default	None
Script/CLI	Snmp.PrivProtocol
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.900.1.200.600

Protocol to use with SNMPv3.

- None: No encryption is used. The **PrivPassword** parameter is ignored.
- DES: DES encryption is used.

PrivPassword (Config Parameter)

Type	Text
Range	Size(0..255)
Default	PrivPassword
Script/CLI	Snmp.PrivPassword
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.900.1.200.700

Password to use with SNMPv3 when using DES privacy. If "None" is used, the **PrivPassword** parameter is ignored.

Password encryption is supported via the **Dcm.PasswordEncryption** table.

When **Dcm.PasswordEncryption** is enabled clear text passwords will be automatically encrypted.

Unencrypted password maximal length is 63.

Encrypted password maximal length is 113.

Community (Config Parameter)

Type	Text
Range	Size(1..32)
Default	public
Script/CLI	Snmp.Community
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.900.1.200.800

String to use for the community field of SNMPv1 and SNMPv2 read-write commands and traps. It must not be empty.
The use of a community name provides context for agents receiving requests and initiating traps. An SNMP agent won't respond to a request from a management system outside its configured community.

SnmpUser (Config Parameter)

Type	Text
Range	Size(0..50)
Default	admin
Script/CLI	Snmp.SnmpUser
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.900.1.200.900

For SNMP v1/v2, this user name is used to access the configuration. For SNMP v3, this user name is also used to authenticate, in which case the **Snmp.SnmpV3Password** should be defined.

If this parameter is empty, the **Snmp.Community** parameter is used as the user name.

Note: In any case, if the provided user name does not exist in the **AAA.UsersStatus** table, the SNMP access will fail.

SnmpV3Password (Config Parameter)

Type	Text
Range	Size(0..512)
Default	administrator
Script/CLI	Snmp.SnmpV3Password
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.900.1.200.1000

Password used to authenticate with SNMPv3.

For increased security, it is recommended to use a different password than the one from the user account in the Aaa service.

Password encryption is supported via the **Dcm.PasswordEncryption** table.

When **Dcm.PasswordEncryption** is enabled clear text passwords will be automatically encrypted.

Unencrypted password maximal length is 255.

Encrypted password maximal length is 369.

TrapDest (Config Parameter)

Type	Text
Range	Size(0..255)
Default	192.168.10.10:162
Script/CLI	Snmp.TrapDest
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.900.1.300.100

Addresses/FQDNs and ports where to send traps.
Up to 5 comma-separated destinations can be specified. The port numbers are optional.

Note that the traps are sent simultaneously to all resolved destinations. If an FQDN cannot be resolved, this destination will be skipped and will not receive the traps.

EnableTrap (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Snmp.EnableTrap
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.900.1.300.200

Specifies if traps can be sent.

Port (Config Parameter)

Type	IpPort
Range	
Default	161
Script/CLI	Snmp.Port
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.900.1.400

Port on which the SNMP service should listen for incoming SNMP requests.

StatsGetRequest (Status Parameter)

Type	UInt32
Range	
Script/CLI	Snmp.StatsGetRequest
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.900.1.10000.100

Number of GET Requests handled by the service.

StatsGetNextRequest (Status Parameter)

Type	UInt32
Range	
Script/CLI	Snmp.StatsGetNextRequest
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.900.1.10000.200

Number of GET-NEXT requests handled by the service.

StatsSetRequest (Status Parameter)

Type	UInt32
Range	
Script/CLI	Snmp.StatsSetRequest
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.900.1.10000.300

Number of SET requests handled by the service.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Snmp.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.900.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Snmp.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.900.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Snmp service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.900.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	Service is listening on address %1$s and port %2$d.	Info	This message is issued when the SNMP service is launched.
20	SNMP service is changing its configuration due to a parameter change.	Debug	This message is issued when a configuration parameter is changed, requiring the SNMP service to update its configuration.
30	%1$s request with %2$s(%3$d) result.	Debug	This message is issued when an SNMP request is received. The type of request is shown together with the result.
40	Service is listening on port %1$d of all network interfaces.	Info	This message is issued when the SNMP service is launched and that it listens on all network interfaces.
50	The FQDN '%1$s' cannot be resolved. The SNMP traps could not be sent to this destination.	Warning	This message is issued when the SNMP service cannot resolve the FQDN of a trap destinations. Verify that the FQDN is properly spelled and that the DNS servers are reachable.
60	SNMPv3 authentication failed for user %1$s.	Warning	This message is issued when the specified Snmp user cannot be authenticated.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.

NumKey	Message	Severity	Description
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.

NumKey	Message	Severity	Description
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Snmp.

Message	Severity	Description
Evaluation of expression %2$s in service %1$s failed, reason is: '%3$s'.	Error	This message is issued when the parameters evaluation or run command fails.
Assignment of value %3$s to expression %2$s in service %1$s failed, reason is: '%4$s'.	Error	This message is issued when the value assignment to a parameter failed.
Evaluation of expression %2$s in service %1$s issued the following warning: '%3$s'.	Warning	This message is issued when the parameter evaluation or running a command detects a warning condition.
Assignment of value %3$s to expression %2$s in service %1$s issued the following warning: '%4$s'.	Warning	This message is issued when the value assignment to a parameter detects a warning condition.
Unknown %1$s service, or it is not started.	Error	This message is issued when the service fails to change the context to an unknown or not started service.
Cannot add %1$s alias to entity %2$s, reason is: '%3$s'.	Error	This message is issued when the Snmp Service fails to add an alias to a entity.
Cannot remove %1$s alias : No such alias name.	Error	This message is issued when the Snmp Service fails to remove an alias.
Alias name is already used.	Error	This message is issued when the Snmp Service fails to add an alias .
No such entity name.	Error	This message is issued when the Snmp Service fails to add an alias when the entity name is failed.
%1$s is a reserved word.	Error	This message is issued when SNMP fails to add an alias when the alias name is a reserved word used by a module, a MIB parameter in current context or a Macro.
Warning: Does not match an existing user account.	Warning	This message is issued when the **SnmpUser** does not match an existing user in the **AAA.UsersStatus** table.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.

Message	Severity	Description
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Basic Telephony Interface (TelIf)

The Telephony Interface (TelIf) service manages tone generation and detection on the telephony interfaces.

Parameters

CountrySelection (Config Parameter)

Type	Enum
Range	Argentina1(900) | Australia1(1000) | Australia2(1100) | Australia3(1200) | Austria1(2000) | Brazil1(3000) | China1(4000) | CzechRepublic1(4500) | Denmark1(5000) | France1(6000) | Germany1(7000) | Germany2(7100) | Israel2(10100) | Italy1(11000) | Japan2(12100) | Mexico1(14000) | Netherlands1(15000) | NewZealand1(16000) | NorthAmerica1(17000) | Russia1(18000) | Spain1(19000) | Sweden1(20000) | Switzerland1(21000) | Uae2(23100) | Uae3(23200) | Uae4(23300) | Uk1(24000)
Default	NorthAmerica1
Script/CLI	TelIf.CountrySelection
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.100

The country selection allows to select predefined country settings for the tone profiles, ring patterns, and other parameters such as input and output gains.

DefaultCountryCustomizationUserGainInputOffset (Config Parameter)

Type	Int32
Range	-12..12
Default	0
Script/CLI	TelIf.DefaultCountryCustomizationUserGainInputOffset
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.200.100.100

The user input gain offset is added to the base input gain to compute the total input gain on all telephony interfaces. The user input gain is in dB.
Ex.: On a call involving a SIP terminal and an FXS terminal, raising the input offset will raise the volume perceived on the SIP terminal.

If a specific configuration is set in the **SpecificCountryCustomizationUserGain.InputOffset** parameter and the **SpecificCountryCustomizationUserGain.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultCountryCustomizationUserGainOutputOffset (Config Parameter)

Type	Int32
Range	-12..12
Default	0
Script/CLI	TelIf.DefaultCountryCustomizationUserGainOutputOffset
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.200.100.200

The user output gain offset is added to the base output gain to compute the total output gain on all telephony interfaces. The user output gain is in dB.
Ex.: On a call involving a SIP terminal and an FXS terminal, raising the output offset will raise the volume perceived on the FXS terminal.

If a specific configuration is set in the **SpecificCountryCustomizationUserGain.OutputOffset** parameter and the **SpecificCountryCustomizationUserGain.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

SpecificCountryCustomizationUserGain (Table)

This table allows to configure the user gain for a specific interface. All interfaces have the default configuration unless the **EnableConfig** parameter is enabled.

InterfaceId (Index) | Table: SpecificCountryCustomizationUserGain

Type	Text
Range	
Script/CLI	TelIf.SpecificCountryCustomizationUserGain[].InterfaceId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.200.100.300.1.100

String that identifies a interface in other tables.

EnableConfig (Config Parameter) | Table: SpecificCountryCustomizationUserGain

Type	EnableDisable
Range	
Default	Disable
Script/CLI	TelIf.SpecificCountryCustomizationUserGain[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.200.100.300.1.200

Defines the configuration to use for a specific interface.

- Disable: The interface uses the default configuration as defined in the **DefaultCountryCustomizationUserGainInputOffset** and **DefaultCountryCustomizationUserGainOutputOffset** parameters.
- Enable: The interface uses the specific configuration as defined in the **SpecificCountryCustomizationUserGain.InputOffset** and **SpecificCountryCustomizationUserGain.OutputOffset** parameters.

InputOffset (Config Parameter) | Table: SpecificCountryCustomizationUserGain

Type	Int32
Range	-12..12
Default	0
Script/CLI	TelIf.SpecificCountryCustomizationUserGain[].InputOffset
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.200.100.300.1.300

The user input gain offset is added to the base input gain to compute the total input gain on this specific telephony interface. The user input gain is in dB.
Ex.: On a call involving a SIP terminal and an FXS terminal, raising the input offset will raise the volume perceived on the SIP terminal.

This configuration overrides the default configuration set in the **DefaultCountryCustomizationUserGainInputOffset** parameter if the **SpecificCountryCustomizationUserGain.EnableConfig** parameter is set to 'Enable'.

OutputOffset (Config Parameter) | Table: SpecificCountryCustomizationUserGain

Type	Int32
Range	-12..12
Default	0
Script/CLI	TelIf.SpecificCountryCustomizationUserGain[].OutputOffset
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.200.100.300.1.400

The user output gain offset is added to the base output gain to compute the total output gain on this specific telephony interface. The user output gain is in dB.
Ex.: On a call involving a SIP terminal and an FXS terminal, raising the output offset will raise the volume perceived on the FXS terminal.

This configuration overrides the default configuration set in the **DefaultCountryCustomizationUserGainOutputOffset** parameter if the **SpecificCountryCustomizationUserGain.EnableConfig** parameter is set to 'Enable'.

DefaultCountryCustomizationDialingOverride (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	TelIf.DefaultCountryCustomizationDialingOverride
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.200.400.100

Allows to override the default country dialing setting.

- Disable: The interface uses the default country dialing setting.
- Enable: The interface uses the dialing country setting as defined in the **DefaultCountryCustomizationDialingInterMfR1DialDelay**, **DefaultCountryCustomizationDialingMfR1Duration**, **DefaultCountryCustomizationDialingInterDtmfDialDelay** and **DefaultCountryCustomizationDialingDtmfDuration** parameters.

If a specific configuration is set in the **SpecificCountryCustomizationDialing.Override** parameter and the **SpecificCountryCustomizationDialing.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultCountryCustomizationDialingInterDtmfDialDelay (Config Parameter)

Type	UInt32
Range	50..600
Default	100
Script/CLI	TelIf.DefaultCountryCustomizationDialingInterDtmfDialDelay
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.200.400.200

The delay between two DTMFs when dialing on the interface.
This value is expressed in milliseconds (ms).

This configuration is used only if the **DefaultCountryCustomizationDialingOverride** parameter is set to 'Enable'.

If a specific configuration is set in the **SpecificCountryCustomizationDialing.InterDtmfDialDelay** parameter and the **SpecificCountryCustomizationDialing.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultCountryCustomizationDialingDtmfDuration (Config Parameter)

Type	UInt32
Range	50..600
Default	100
Script/CLI	TelIf.DefaultCountryCustomizationDialingDtmfDuration
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.200.400.300

The duration of a DTMF when dialing on the interface.
This value is expressed in milliseconds (ms).

This configuration is used only if the **DefaultCountryCustomizationDialingOverride** parameter is set to 'Enable'.

If a specific configuration is set in the **SpecificCountryCustomizationDialing.DtmfDuration** parameter and the **SpecificCountryCustomizationDialing.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultCountryCustomizationDialingInterMfR1DialDelay (Config Parameter)

Type	UInt32
Range	50..600
Default	68
Script/CLI	TelIf.DefaultCountryCustomizationDialingInterMfR1DialDelay
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.200.400.340

The delay between two MFR1s when dialing on the interface.
This value is expressed in milliseconds (ms).

This configuration is used only if the **DefaultCountryCustomizationDialingOverride** parameter is set to 'Enable'.

If a specific configuration is set in the **SpecificCountryCustomizationDialing.InterMfR1DialDelay** parameter and the **SpecificCountryCustomizationDialing.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultCountryCustomizationDialingMfR1Duration (Config Parameter)

Type	UInt32
Range	50..600
Default	68
Script/CLI	TelIf.DefaultCountryCustomizationDialingMfR1Duration
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.200.400.370

The duration of a MFR1 when dialing on the interface.
This value is expressed in milliseconds (ms).

This configuration is used only if the **DefaultCountryCustomizationDialingOverride** parameter is set to 'Enable'.

If a specific configuration is set in the **SpecificCountryCustomizationDialing.MfR1Duration** parameter and the **SpecificCountryCustomizationDialing.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

SpecificCountryCustomizationDialing (Table)

This table allows to override the default country dialing configuration for a specific interface. All interfaces have the default configuration unless the **EnableConfig** parameter is enabled.

InterfaceId (Index) | Table: SpecificCountryCustomizationDialing

Type	Text
Range	
Script/CLI	TelIf.SpecificCountryCustomizationDialing[].InterfaceId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.200.400.400.1.100

String that identifies a Interface in other tables.

EnableConfig (Config Parameter) | Table: SpecificCountryCustomizationDialing

Type	EnableDisable
Range	
Default	Disable
Script/CLI	TelIf.SpecificCountryCustomizationDialing[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.200.400.400.1.200

Defines the configuration to use for a specific interface.

- Disable: The interface uses the default configuration as defined in the **DefaultCountryCustomizationDialingOverride**, **DefaultCountryCustomizationDialingInterMfR1DialDelay**, **DefaultCountryCustomizationDialingMfR1Duration**, **DefaultCountryCustomizationDialingInterDtmfDialDelay** and **DefaultCountryCustomizationDialingDtmfDuration** parameters.
- Enable: The interface uses the specific configuration as defined in the **SpecificCountryCustomizationDialing.Override**, **SpecificCountryCustomizationDialing.InterMfR1DialDelay**, **SpecificCountryCustomizationDialing.MfR1Duration**, **SpecificCountryCustomizationDialing.InterDtmfDialDelay** and **SpecificCountryCustomizationDialing.DtmfDuration** parameters.

Override (Config Parameter) | Table: SpecificCountryCustomizationDialing

Type	EnableDisable
Range	
Default	Disable
Script/CLI	TelIf.SpecificCountryCustomizationDialing[].Override
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.200.400.400.1.300

Allows to override the default country dialing setting.

- Disable: The interface uses the default country dialing setting.
- Enable: The interface uses the specific dialing configuration as defined in the **InterDtmfDialDelay**, **DtmfDuration**, **InterMfR1DialDelay** and **MfR1Duration** parameters.

This configuration overrides the default configuration set in the **DefaultCountryCustomizationDialingOverride** parameter if the **SpecificCountryCustomizationDialing.EnableConfig** parameter is set to 'Enable'.

InterDtmfDialDelay (Config Parameter) | Table: SpecificCountryCustomizationDialing

Type	UInt32
Range	50..600
Default	100
Script/CLI	TelIf.SpecificCountryCustomizationDialing[].InterDtmfDialDelay
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.200.400.400.1.400

The delay between two DTMFs when dialing on the interface.
This value is expressed in milliseconds (ms).

This configuration is used only if the **Override** parameter is set to 'Enable'.

This configuration overrides the default configuration set in the **DefaultCountryCustomizationDialingInterDtmfDialDelay** parameter if the **SpecificCountryCustomizationDialing.EnableConfig** parameter is set to 'Enable'.

DtmfDuration (Config Parameter) | Table: SpecificCountryCustomizationDialing

Type	UInt32
Range	50..600
Default	100
Script/CLI	TelIf.SpecificCountryCustomizationDialing[].DtmfDuration
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.200.400.400.1.500

The duration of a DTMF when dialing on the interface.
This value is expressed in milliseconds (ms).

This configuration is used only if the **Override** parameter is set to 'Enable'.

This configuration overrides the default configuration set in the **DefaultCountryCustomizationDialingDtmfDuration** parameter if the **SpecificCountryCustomizationDialing.EnableConfig** parameter is set to 'Enable'.

InterMfR1DialDelay (Config Parameter) | Table: SpecificCountryCustomizationDialing

Type	UInt32
Range	50..600
Default	68
Script/CLI	TelIf.SpecificCountryCustomizationDialing[].InterMfR1DialDelay
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.200.400.400.1.600

The delay between two MFR1s when dialing on the interface.
This value is expressed in milliseconds (ms).

This configuration is used only if the **Override** parameter is set to 'Enable'.

This configuration overrides the default configuration set in the **DefaultCountryCustomizationDialingInterMfR1DialDelay** parameter if the **SpecificCountryCustomizationDialing.EnableConfig** parameter is set to 'Enable'.

MfR1Duration (Config Parameter) | Table: SpecificCountryCustomizationDialing

Type	UInt32
Range	50..600
Default	68
Script/CLI	TelIf.SpecificCountryCustomizationDialing[].MfR1Duration
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.200.400.400.1.700

The duration of a MFR1 when dialing on the interface.
This value is expressed in milliseconds (ms).

This configuration is used only if the **Override** parameter is set to 'Enable'.

This configuration overrides the default configuration set in the **DefaultCountryCustomizationDialingMfR1Duration** parameter if the **SpecificCountryCustomizationDialing.EnableConfig** parameter is set to 'Enable'.

CountryToneStatus (Table)

This table displays the current tone pattern used (depends on the **CountrySelection** parameter and the **CountryCustomizationTone** table). The configuration applies to all interfaces.

Tone (Index) | Table: CountryToneStatus

Type	Enum
Range	Busy (100) | CallWaiting(150) | Confirmation (200) | Congestion(300) | Dial(400) | Hold(500) | Intercept(600) | MessageWaiting (700) | Preemption(800) | Reorder(900) | Ringback (1000) | Roh(1100) | Sit(1200) | Stutter(1300)
Script/CLI	TelIf.CountryToneStatus[].Tone
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.200.500.100.1.100

Tone.

Pattern (Status Parameter) | Table: CountryToneStatus

Type	Text
Range	Size(0..512)
Script/CLI	TelIf.CountryToneStatus[].Pattern
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.200.500.100.1.300

Pattern description of the currently used tone.
See the **CountryCustomizationTone.Pattern** parameter for a description of the syntax.

CountryCustomizationTone (Table)

This table allows to override the default country tone configuration. The configuration applies to all interfaces.

Tone (Index) | Table: CountryCustomizationTone

Type	Enum
Range	Busy (100) | CallWaiting(150) | Confirmation (200) | Congestion(300) | Dial(400) | Hold(500) | Intercept(600) | MessageWaiting (700) | Preemption(800) | Reorder(900) | Ringback (1000) | Roh(1100) | Sit(1200) | Stutter(1300)
Script/CLI	TelIf.CountryCustomizationTone[].Tone
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.200.500.200.1.100

Tone to customise.

Override (Config Parameter) | Table: CountryCustomizationTone

Type	EnableDisable
Range	
Default	Disable
Script/CLI	TelIf.CountryCustomizationTone[].Override
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.200.500.200.1.200

Allows to override the default country tone setting.

- Disable: The unit uses the default country dialing setting.
- Enable: The unit uses the tone configuration as defined in the **Pattern** parameter.

Pattern (Config Parameter) | Table: CountryCustomizationTone

Type	Text
Range	Size(0..512)
Default	
Script/CLI	TelIf.CountryCustomizationTone[].Pattern
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.200.500.200.1.300

Describes a tone pattern.
A tone description contains frequencies, states and loops. Up to 4 frequencies (f1 to f4) each with a power level can be defined. At least one frequency/power pair must be defined. Frequency range is from 10 to 4000 Hz and Power level range is from -99 to 3 dbm.

The syntax is: f1=<frequency>:<power>

Up to 8 states (s1 to s8) can be defined, each with an action, a set of frequencies, a duration and a next state. At least one state must be described if the tone-pattern is not empty. The action can be 'on', 'off' or 'CID' (for call waiting tones). The duration of the state is from 10 to 56000 ms. The tone is continuous if no time is specified.

The syntax is: s1=<action>:<frequency>:...:<frequency>:<duration>:<end-of-loop-indicator>:<next state>

Additionally, a set of states can be enclosed in a loop. The starting state of a loop is marked with a loop counter (l=), the range is from 2 to 128. The ending state of a loop is marked with an end-of-loop indicator (l).

The syntax is: l=<loop count>,<state definition>,...,<state definition (with end-of-loop-indicator)>,<state definition>...

Examples:

- Germany dialtone (continuous): 'f1=350:-17,f2=440:-17,s1=on:f1:f2'
- North America Recall dialtone (3 quick tones followed by a continuous tone): 'f1=350:-17,f2=440:-17,l=3,s1=on:f1:f2:100:s2,s2=off:100:l:s1,s3=on:f1:f2'
- Australia ring back tone (on 400ms, off 200 ms, on 400 ms and off 2000 ms and replay): 'f1=425:-17,f2=400:-5,f3=450:-5,s1=on:f1:f2:f3:400:s2,s2=off:200:s3,s3=on:f1:f2:f3:400:s4,s4=off:2000:s1'

Only two frequencies can be used by the Call Waiting tone.

DefaultMachineDetectionCngToneDetection (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	TelIf.DefaultMachineDetectionCngToneDetection
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.300.100

Enables fax calling tone (CNG tone) detection.

- Enable: Upon recognition of the CNG tone, the unit switches the communication from voice mode to fax mode and the CNG is transferred by using the preferred fax codec. NOTE: This option allows for quicker fax detection, but it also increases the risk of falsedetection.
- Disable: The CNG tone does not trigger a transition from voice to data and the CNG is transferred in the voice channel. NOTE: With this option, faxes are detected later, but the risk of false detection is reduced.

If a specific configuration is set in the **SpecificMachineDetection.CngToneDetection** parameter and the **SpecificMachineDetection.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultMachineDetectionCedToneDetection (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	TelIf.DefaultMachineDetectionCedToneDetection
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.300.101

Enables CED tone detection.

- Enable: Upon recognition of the CED tone, the unit behaves as defined in **DefaultMachineDetectionBehaviorOnCedToneDetection**.
- Disable: The CED tone does not trigger a transition to fax or voiceband data mode. The CED is transferred in the voice channel.

If a specific configuration is set in the **SpecificMachineDetection.CedToneDetection** parameter and the **SpecificMachineDetection.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultMachineDetectionV21ModulationDetection (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	TelIf.DefaultMachineDetectionV21ModulationDetection
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.300.102

Enables fax V.21 modulation detection.

- Enable: Upon recognition of the V.21 modulation tone, the unit switches the communication from voice mode to fax mode and the signal is transferred by using the preferred fax codec.
- Disable: The V.21 modulation does not trigger a transition from voice to data and the signal is transferred in the voice channel.

If a specific configuration is set in the **SpecificMachineDetection.CedToneDetection** parameter and the **SpecificMachineDetection.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

DefaultMachineDetectionBehaviorOnCedToneDetection (Config Parameter)

Type	Enum
Range	Passthrough (100) | Faxmode (200)
Default	Passthrough
Script/CLI	TelIf.DefaultMachineDetectionBehaviorOnCedToneDetection
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.300.110

Defines the behavior of the unit upon detection of a CED tone.

- Passthrough: In passthrough mode the CED tone triggers a transition from voice to voice band data and is transferred in the voice channel. Use this setting when any kind of analog device (i.e.: telephone, fax or modem) can be connected to this port.
- Faxmode: In 'fax mode', upon detection of a CED tone the unit switches the communication from voice mode to fax mode and the CED is transferred by using the preferred fax codec. Only a fax can then be connected to this port.

If a specific configuration is set in the **SpecificMachineDetection.BehaviorOnCedToneDetection** parameter and the **SpecificMachineDetection.EnableConfig** parameter is set to 'Enable', then it overrides the current default configuration.

Note that this parameter has no effect if the CED tone detection is disabled.

SpecificMachineDetection (Table)

specific configuration.

InterfaceId (Index) | Table: SpecificMachineDetection

Type	Text
Range	
Script/CLI	TelIf.SpecificMachineDetection[].InterfaceId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.300.200.1.100

String that identifies a interface in other tables.

EnableConfig (Config Parameter) | Table: SpecificMachineDetection

Type	EnableDisable
Range	
Default	Disable
Script/CLI	TelIf.SpecificMachineDetection[].EnableConfig
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.300.200.1.200

Defines the configuration to use for a specific interface.

- Disable: The interface uses the default configuration as defined in the **DefaultMachineDetectionCngToneDetection** and **DefaultMachineDetectionBehaviorOnCedToneDetection** parameters.
- Enable: The interface uses the specific configuration as defined in the **SpecificMachineDetection.CngToneDetection** and **SpecificMachineDetection.BehaviorOnCedToneDetection** parameters.

CngToneDetection (Config Parameter) | Table: SpecificMachineDetection

Type	EnableDisable
Range	
Default	Enable
Script/CLI	TelIf.SpecificMachineDetection[].CngToneDetection
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.300.200.1.300

Enables fax calling tone (CNG tone) detection.

- Enable: Upon recognition of the CNG tone, the unit switches the communication from voice mode to fax mode and the CNG is transferred by using the preferred fax codec. NOTE: This option allows for quicker fax detection, but it also increases the risk of false detection.
- Disable: The CNG tone does not trigger a transition from voice to data and the CNG is transferred in the voice channel. NOTE: With this option, faxes are detected later, but the risk of false detection is reduced.

This configuration overrides the default configuration set in the **DefaultMachineDetectionCngToneDetection** parameter if the **SpecificMachineDetection.EnableConfig** parameter is set to 'Enable'.

CedToneDetection (Config Parameter) | Table: SpecificMachineDetection

Type	EnableDisable
Range	
Default	Enable
Script/CLI	TelIf.SpecificMachineDetection[].CedToneDetection
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.300.200.1.310

Enables CED tone detection.

- Enable: Upon recognition of the CED tone, the unit behaves as defined in **DefaultMachineDetectionBehaviorOnCedToneDetection**.
- Disable: The CED tone does not trigger a transition to fax or voiceband data mode. The CED is transferred in the voice channel.

This configuration overrides the default configuration set in the **DefaultMachineDetectionCedToneDetection** parameter if the **SpecificMachineDetection.EnableConfig** parameter is set to 'Enable'.

V21ModulationDetection (Config Parameter) | Table: SpecificMachineDetection

Type	EnableDisable
Range	
Default	Enable
Script/CLI	TelIf.SpecificMachineDetection[].V21ModulationDetection
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.300.200.1.320

Enables fax V.21 modulation detection.

- Enable: Upon recognition of the V.21 modulation tone, the unit switches the communication from voice mode to fax mode and the signal is transferred by using the preferred fax codec.
- Disable: The V.21 modulation does not trigger a transition from voice to data and the signal is transferred in the voice channel.

This configuration overrides the default configuration set in the **DefaultMachineDetectionV21ModulationDetection** parameter if the **SpecificMachineDetection.EnableConfig** parameter is set to 'Enable'.

BehaviorOnCedToneDetection (Config Parameter) | Table: SpecificMachineDetection

Type	Enum
Range	Passthrough (100) | Faxmode (200)
Default	Passthrough
Script/CLI	TelIf.SpecificMachineDetection[].BehaviorOnCedToneDetection
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.300.200.1.400

Defines the behavior of the unit upon detection of a CED tone.

- Passthrough: In passthrough mode the CED tone does not trigger a transition from voice to data and is transferred in the voice channel. Use this setting when any kind of analog device (i.e.: telephone, fax or modem) can be connected to this port.
- Faxmode: In 'fax mode', upon detection of a CED tone the unit switches the communication from voice mode to fax mode and the CED is transferred by using the preferred fax codec. Only a fax can then be connected to this port.

This configuration overrides the default configuration set in the **DefaultMachineDetectionBehaviorOnCedToneDetection** parameter if the **SpecificMachineDetection.EnableConfig** parameter is set to 'Enable'.

Note that this parameter has no effect if the CED tone detection is disabled.

MusicOnHoldStreamingEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	TelIf.MusicOnHoldStreamingEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.400.100

Indicates whether or not the unit should play music when being put on hold.

- Disable: No music is played.
- Enable: Music is played toward the telephony side when being put on hold from the network side.

DistinctiveCallWaitingTone (Table)

This table allows to override the default country call waiting tone configuration. The configuration applies to all interfaces.

Index (Index) | Table: DistinctiveCallWaitingTone

Type	UInt32
Range	1..4
Script/CLI	TelIf.DistinctiveCallWaitingTone[].Index
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.500.100.1.100

Unique identifier of the row in the table.

ToneId (Config Parameter) | Table: DistinctiveCallWaitingTone

Type	Text
Range	Size(0..512)
Default	
Script/CLI	TelIf.DistinctiveCallWaitingTone[].ToneId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.500.100.1.200

Identification of the distinctive call waiting tone. When the **ToneId** parameter is defined and the incoming call property 'distinctive-ring' matches with it, the corresponding tone pattern is used. Otherwise, the country call waiting tone is used.

Example:

- A distinctive ring call-property of "//127.0.0.1/Bellcore-dr2" matches with the following ToneId: "//127.0.0.1/Bellcore-dr2"

Pattern (Config Parameter) | Table: DistinctiveCallWaitingTone

Type	Text
Range	Size(0..512)
Default	
Script/CLI	TelIf.DistinctiveCallWaitingTone[].Pattern
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.500.100.1.300

Pattern description of the custom tone.
See the **CountryCustomizationTone.Pattern** parameter for syntax description.

Note that only two frequencies can be used by the Call Waiting tone.

InteropDtmfDetection (Table)

DTMF Detection Configuration

InterfaceId (Index) | Table: InteropDtmfDetection

Type	Text
Range	
Script/CLI	TelIf.InteropDtmfDetection[].InterfaceId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.50000.100.1.100

String that identifies an interface in other tables.

RiseTimeCriteria (Config Parameter) | Table: InteropDtmfDetection

Type	Enum
Range	CheckSr (100) | ConfirmSnr (200)
Default	ConfirmSnr
Script/CLI	TelIf.InteropDtmfDetection[].RiseTimeCriteria
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.50000.100.1.200

Defines how the Rise Time criteria should be configured for DTMF detection.

- CheckSr: Enable the Step Rise criteria and disable the Confirm DTMF SNR criteria.
- ConfirmSnr: Enable the Confirm DTMF SNR criteria and disable the Step Rise criteria.

The Step Rise criteria compares the current frame energy to the high frequency power of the previous frame. If the current frame energy is high enough, then it passes the test, further validating the DTMF.

Disabling the Step Rise criteria may result in deteriorated talk-off performance, but increases the detection of malformed DTMF.

The Confirm DTMF SNR criteria is an additional Signal-to-noise ratio test performed before a confirmed DTMF report is sent to finally validate the DTMF.

PositiveTwist (Config Parameter) | Table: InteropDtmfDetection

Type	UInt32
Range	1..14
Default	6
Script/CLI	TelIf.InteropDtmfDetection[].PositiveTwist
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.50000.100.1.300

Defines the value for the Positive Twist DTMF detection parameter.
When the high-group frequency of a DTMF is more powerful than the low-group frequency, the difference between the high-group frequency absolute power and the low-group frequency absolute power must be smaller than or equal to the value set in this parameter. Otherwise, the DTMF is not detected.

Raising this value increases the sensitivity of DTMF detection. Raising this value too high may also cause false detections of DTMFs.

NegativeTwist (Config Parameter) | Table: InteropDtmfDetection

Type	UInt32
Range	1..14
Default	9
Script/CLI	TelIf.InteropDtmfDetection[].NegativeTwist
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.50000.100.1.350

Defines the value for the Negative Twist DTMF detection parameter.
When the low-group frequency of a DTMF is more powerful than the high-group frequency, the difference between the low-group frequency absolute power and the high-group frequency absolute power must be smaller than or equal to the value set in this parameter. Otherwise, the DTMF is not detected.

Raising this value increases the sensitivity of DTMF detection. Raising this value too high may also cause false detections of DTMFs.

MaxPowerThreshold (Config Parameter) | Table: InteropDtmfDetection

Type	Int32
Range	-20..1
Default	1
Script/CLI	TelIf.InteropDtmfDetection[].MaxPowerThreshold
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.50000.100.1.400

The average power of a DTMF must be below the value set in this parameter to be no longer detected. Raising this value increases the sensitivity of the DTMF detection. Raising this value too high may also cause false detections of DTMFs.
The value is expressed in dBm (relative to 1mW of power).

MinPowerThreshold (Config Parameter) | Table: InteropDtmfDetection

Type	Int32
Range	-45..-10
Default	-30
Script/CLI	TelIf.InteropDtmfDetection[].MinPowerThreshold
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.50000.100.1.450

The average power of a DTMF must be above the value set in this parameter for at least 30ms to be detected. Raising this value reduces the sensitivity to DTMF detection.
The value is expressed in dBm (relative to 1mW of power).

BreakPowerThreshold (Config Parameter) | Table: InteropDtmfDetection

Type	Int32
Range	-45..-12
Default	-32
Script/CLI	TelIf.InteropDtmfDetection[].BreakPowerThreshold
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.50000.100.1.500

When the average power of a DTMF falls below the value set in this parameter for at least 20ms, it is considered that the DTMF ended.
The value is expressed in dBm (relative to 1mW of power).

InteropStartCallInVbd (Table)

Start Call In VBD

InterfaceId (Index) | Table: InteropStartCallInVbd

Type	Text
Range	
Script/CLI	TelIf.InteropStartCallInVbd[].InterfaceId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.50000.200.1.100

String that identifies an interface in other tables.

Enable (Config Parameter) | Table: InteropStartCallInVbd

Type	EnableDisable
Range	
Default	Disable
Script/CLI	TelIf.InteropStartCallInVbd[].Enable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.50000.200.1.200

Indicates whether or not a call should be started in voiceband data mode.

- Disable: Call is started in voice mode. A fax/modem tone detection triggers a transition from voice to voiceband data according to the configuration in **MachineDetectionGroup**.
- Enable: Call is started in voiceband data mode.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	TelIf.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	TelIf.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1775.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the TelIf service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.1775.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.

NumKey	Message	Severity	Description
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to TelIf.

Message	Severity	Description
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.

Message	Severity	Description
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Virtual Machine (Vm)

The Virtual Machine (VM) service allows the administrator to manage virtual machines.

Parameters

Vm (Table: user-defined, 10 lines max.)

This table contains the parameters used to configure the VMs.
The changes to this table are applied on execution of the `VM.StartVm` command or when the Vm service is restarted.

Idx (Index) | Table: Vm

Type	UInt32
Range	
Script/CLI	Vm.Vm[].Idx
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.100.100.1.100

Unique numerical identifier for a VM.

Name (Dynamic Parameter) | Table: Vm

Type	Text
Range	Size(0..48)
Script/CLI	Vm.Vm[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.100.100.1.200

VM Name.
The name is set when adding a new virtual machine with the `CreateVm` command. The user cannot modify the name after the VM has been created.

VncDisplayId (Dynamic Parameter) | Table: Vm

Type	Int32
Range	-1..99
Script/CLI	Vm.Vm[].VncDisplayId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.100.100.1.300

Display Id for Vnc connections.
UnitAddress:DisplayId is the syntax to use in VNC clients. The VNC server of a VM listens to the default port 5900 + the DisplayId.

Configuring "-1" disables the VNC server for a VM.

UsbPort (Dynamic Parameter) | Table: Vm

Type	Enum
Range	None(100) | All(200)
Script/CLI	Vm.Vm[].UsbPort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.100.100.1.400

USB ports associated with this VM.

- None: No USB will be associated with this virtual machine.
- All: All USB ports will be associated with this virtual machine.

When the USB port is associated with a VM, the other VMs cannot use it.

IsoName (Dynamic Parameter) | Table: Vm

Type	Text
Range	SIZE(0..510)
Script/CLI	Vm.Vm[].IsoName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.100.100.1.500

Name of ISO file with this VM.
The ISO file must be uploaded in the VM/Drives.

This file can be used to start the virtual machine or used as a drive during a normal start.

MacAddress (Dynamic Parameter) | Table: Vm

Type	Text
Range	
Script/CLI	Vm.Vm[].MacAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.100.100.1.550

MAC address of the Vm.
Only this format is accepted: xx:xx:xx:xx:xx:xx or XX:XX:XX:XX:XX:XX.

NetworkAdapter (Dynamic Parameter) | Table: Vm

Type	Enum
Range	E1000(100) | Virtio(200)
Script/CLI	Vm.Vm[].NetworkAdapter
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.100.100.1.560

Configures the virtualised network adapter for this VM.

- E1000: Intel 82545EM emulated network interface card. Highest compatibility, slower performance.
- Virtio: Paravirtualised network adapter. Best performance, a specific guest OS VM driver is required.

This parameter is effective only if the **Eth.Link.VirtualSwitch** parameter or the **InternalVirtualSwitchEnable** parameter is enabled.

StartupType (Dynamic Parameter) | Table: Vm

Type	Enum
Range	Manual(100) | Auto(200)
Script/CLI	Vm.Vm[].StartupType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.100.100.1.600

Startup Type of the VM.

- Auto: The virtual machine is automatically started when the Vm service starts. If there are multiple virtual machines, they are launched in decreasing order of their index, meaning the one with the highest index will launch first and so forth.
- Manual: The administrator manually starts the virtual machine.

ShutdownTimeout (Dynamic Parameter) | Table: Vm

Type	UInt32
Range	0..240
Script/CLI	Vm.Vm[].ShutdownTimeout
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.100.100.1.650

Maximum delay, in seconds, allowed for the VM to stop after an ACPI powerdown command. If this delay expires before the VM has stopped completely by itself, the VM is forced to stop.
The Operating System in the VM must support ACPI to properly shutdown, otherwise the VM is forced to stop after this timeout expires.

ConfigStatus (Status Parameter) | Table: Vm

Type	Enum
Range	Valid(100) | USBNotAvailable(200) | MissingVMConfig(300) | NeedRestartToApplyConfig(400)
Script/CLI	Vm.Vm[].ConfigStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.100.100.1.700

Configuration status of the row.
Indicates if the configuration of this VM is valid and ready to be applied.

- Valid: The current content of the row is valid.
- USBNotAvailable: The VM is started witout using USB, because the configured USB is used by another VM.
- MissingVMConfig: The config file of VM is missing and the VM cannot be started. This config status is set when the Vm service tries to start a virtual machine but its image and config file are missing in vm/images.
- NeedRestartToApplyConfig: The configuration has changed but not applied, Stop and restart the VM to apply new config.

Start (Row Command) | Table: Vm

Script/CLI:	Vm.Vm[].Start
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.100.100.1.10000

Start this virtual machine.

Stop (Row Command) | Table: Vm

Script/CLI:	Vm.Vm[].Stop
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.100.100.1.10010

Stop this virtual machine.

Reboot (Row Command) | Table: Vm

Script/CLI:	Vm.Vm[].Reboot
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.100.100.1.10020

Reboot this virtual machine.
This abruptly resets the power of the VM.

IMPORTANT: Doing so may cause corruption or data lost if the VM was writing on the virtual disk.

StartFromIsoImage (Row Command) | Table: Vm

Script/CLI:	Vm.Vm[].StartFromIsoImage
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.100.100.1.10030

Start this virtual machine from an ISO Image.

Delete (Row Command) | Table: Vm

Script/CLI:	Vm.Vm[].Delete
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.100.100.1.10040

Delete this virtual machine, along with its VM image and configuration files.

InternalVirtualSwitchEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Vm.InternalVirtualSwitchEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.100.200

Specifies if an internal virtual network interface – also known as a host-only virtual switch - should be created between the VM(s) and the host.

- Disable: No internal virtual network interface.
- Enable: An internal virtual network interface is created with the address and subnet mask specified in the InternalVirtualLinkIpAddr parameter.

When enabled, the internal virtual switch is listed after the "external" virtual switches in the VM(s).

This internal virtual switch only enables internal communications on a known subnet, and does not depend on the state of the physical network ports. To allow external communications in the VM(s), see the Eth.LinksTable.LinksVirtualSwitch parameters.

InternalVirtualSwitchIpAddr (Config Parameter)

Type	IpAddrMask
Range	
Default	169.254.10.1/24
Script/CLI	Vm.InternalVirtualSwitchIpAddr
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.100.300

Specifies the IP address and subnet mask to use on the host when the InternalVirtualSwitchEnable parameter is set to enable.

AutomaticVncShutdownEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Vm.AutomaticVncShutdownEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.100.400

Configures whether a virtual machine's VNC server should be automatically disabled upon **AutomaticVncShutdownTimer** parameter timer expiration.

- Enable: VNC will be automatically disabled after the timer expiration.
- Disable: VNC won't be disabled automatically.

AutomaticVncShutdownTimer (Config Parameter)

Type	UInt32
Range	0..1440
Default	1440
Script/CLI	Vm.AutomaticVncShutdownTimer
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.100.500

When the **AutomaticVncShutdownEnable** parameter is enabled, the VNC server will be automatically disabled upon expiration of the configured time after the VM startup, by setting the Vnc Id to -1. This setting has no effect when **AutomaticVncShutdownEnable** parameter is disabled. Each virtual machine's timer starts separately, the timer's duration is applied globally. When set to 0, the VNC server is disabled as soon as the VM starts.

This value is expressed in minutes (min).

VmStatus (Table)

This table displays the status of the VMs.

Idx (Index) | Table: VmStatus

Type	UInt32
Range	
Script/CLI	Vm.VmStatus[].Idx
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.200.200.1.100

Unique numerical identifier for a VM.

Name (Status Parameter) | Table: VmStatus

Type	Text
Range	
Script/CLI	Vm.VmStatus[].Name
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.200.200.1.200

VM name.
The name is set when adding a new virtual machine with command the `AddVM` command.

The user cannot modify the name after the VM has been created.

VncDisplayId (Status Parameter) | Table: VmStatus

Type	Int32
Range	
Script/CLI	Vm.VmStatus[].VncDisplayId
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.200.200.1.300

Display Id for Vnc connection with this VM.
UnitAddress:DisplayId is the syntax to use in VNC clients. The VNC server of a VM listens to the default port 5900 + the DisplayId.

Configuring "-1" disables the VNC server for a VM.

UsbPort (Status Parameter) | Table: VmStatus

Type	Enum
Range	None(100) | All(200)
Script/CLI	Vm.VmStatus[].UsbPort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.200.200.1.400

USB ports associated with this VM.

IsoName (Status Parameter) | Table: VmStatus

Type	Text
Range	
Script/CLI	Vm.VmStatus[].IsoName
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.200.200.1.500

Name of the ISO file with this VM.
The ISO file must be uploaded in the VM/Drives.

This file can be used to start the virtual machine or used as a drive during a normal start.

MacAddress (Status Parameter) | Table: VmStatus

Type	Text
Range	
Script/CLI	Vm.VmStatus[].MacAddress
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.200.200.1.550

MAC address of the Vm.

NetworkAdapter (Status Parameter) | Table: VmStatus

Type	Enum
Range	E1000(100) | Virtio(200)
Script/CLI	Vm.VmStatus[].NetworkAdapter
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.200.200.1.560

Virtualised network adapter for this VM.

AllocatedRamMb (Status Parameter) | Table: VmStatus

Type	UInt32
Range	
Script/CLI	Vm.VmStatus[].AllocatedRamMb
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.200.200.1.600

Allocated Memory by the VM in MBytes.

AllocatedStorageGb (Status Parameter) | Table: VmStatus

Type	UInt32
Range	
Script/CLI	Vm.VmStatus[].AllocatedStorageGb
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.200.200.1.700

Allocated Storage by the VM in GBytes.

ImageFormat (Status Parameter) | Table: VmStatus

Type	Enum
Range	Qcow2(100) | Raw(200)| Unknown(300)
Script/CLI	Vm.VmStatus[].ImageFormat
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.200.200.1.710

VM image format.

AllocatedNbCores (Status Parameter) | Table: VmStatus

Type	UInt32
Range	
Script/CLI	Vm.VmStatus[].AllocatedNbCores
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.200.200.1.800

Number of Virtual CPU (vCPU) allocated to the VM.

State (Status Parameter) | Table: VmStatus

Type	Enum
Range	Stopped(100) | Started(200)| Starting(300) | Stopping(400) | InvalidConfig(500)
Script/CLI	Vm.VmStatus[].State
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.200.200.1.900

State of the VM.

- Stopped: The VM is stopped.
- Started: The VM is running.
- Starting: The VM is being started.
- Stopping: The VM is being stopped.
- InvalidConfig: The VM configuration is invalid.

ConvertVmImageResult (Status Parameter)

Type	Enum
Range	None(100) | Running(200) | Success(300) | ErrorNotEnoughSpace(400)
Script/CLI	Vm.ConvertVmImageResult
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.200.300

Conversion result returned by the executed **ConvertVmImage** command. The possible results are:

- None
- Running

- Success
- Error, not enough space

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Vm.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Vm.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.4500.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

ConvertVmImage (Command)

Convert a VM image file or a VM snapshot image file into a new VM image file. The supported output VM file formats are:

- QCOW2: QEMU copy-on-write format. The file extension is '.img'.
- RAW: Plain binary image of the VM disk image, and is very portable. The file extension is '.raw'.

The result of the conversion is returned through the **Vm.ConvertVmImageResult** parameter.

The source VM image must not be used by a running virtual machine.

InputFilename (Argument) | Command: ConvertVmImage

Type	Text
Range	Size(0..48)
Default	

Filename of the source VM image to convert, with or without extension. The filename must match an unique entry in the **File.VmImagesFiles** table.
In case the file extension is not provided, the VM image with matching filename is used.

This argument is mandatory.

OutputFilename (Argument) | Command: ConvertVmImage

Type	Text
Range	Size(0..48)
Default	

Filename of the targeted VM image, with or without extension. The filename must not match an existing entry in the **File.VmImagesFiles** table.
In case the file extension does not match the **OutputFormat** argument or is not provided, the proper extension is added at the end of the given filename.

If the output filename already exists, it will be overwritten.

This argument is mandatory.

OutputFormat (Argument) | Command: ConvertVmImage

Type	Enum
Range	Qcow2(100) | Raw(200)
Default	

VM file format of the target VM image.
This argument is mandatory.

CompressOutputImage (Argument) | Command: ConvertVmImage

Type	Enum
Range	False(100) | True(200)
Default	False

During the conversion into the QCOW2 format, the output image file is compressed. If the **OutputFormat** argument value is not QCOW2, this argument is ignored.
When a VM is running with a compressed QCOW2 image, only the initial data is compressed; all new data written inside the image will be stored uncompressed.

This argument is optional.

RemoveSourceImage (Argument) | Command: ConvertVmImage

Type	Enum
Range	False(100) | True(200)
Default	False

After a successful conversion, the source image file is deleted from the **File.VmImagesFiles** table, and cannot be recovered.
This argument is optional.

CreateVm (Command)

Insert a row in the **VMConfig** table.

A new VM config file is created with the same name if the file does not already exist. The Vm service uses the VM config file parameters, if the VM config file exists, to create the new VM.

A new image is created with the same name if it's not exist.

RamMb, **Storage** and **NbCores** are optionnel if a config file exists, otherwise they are mandatory.

When the VM config file exists and the parameters passed conflicts with this config file, the command fails.

If a VM is configured to use resources that exceed the unit's available resources, the `CreateVm` command fails.

If a VM is configured to use all available system resources, the VM will be created but it will not be possible to simultaneously start the VM with another VM.

Idx (Argument) | Command: CreateVm

Type	UInt32
Range	0..2147483647
Default	0

Unique numerical identifier for a VM.
When the command is called without a **Name** the index is used to generate a name such as 'VM_Index'.

The special value '0' (default value) generates an ID equal to the largest current ID value + 1.

Name (Argument) | Command: CreateVm

Type	Text
Range	Size(0..48)
Default	

Name of the VM.
This name must be unique among all VMs.

When the command is called without a **Name** the index is used to generate a name such as 'VM_Index'.

Alpha-numerics as well as '-' and '_' are valid characters.

RamMb (Argument) | Command: CreateVm

Type	UInt32
Range	0..131072
Default	0

Allocated memory by the VM in MB.
Depending on the total amount of volatile memory in the system, the amount of space reserved for the DGW application varies:

- If the total volatile memory is at least 8 GB, 12.5% of the total memory is reserved for the DGW application.
- If the total volatile memory is less than 8 GB, 512 MB are reserved for the DGW application.

0 MB is default value, it is valid when a VM config file exists otherwise the minimal value is 128 MB.

StorageGb (Argument) | Command: CreateVm

Type	UInt32
Range	0..4096
Default	0

Allocated storage by the VM in GB.
Note that 2 GB are reserved for the DGW application.

0 GB is the default value, it is valid when a VM config file exists otherwise the minimal value is 1 GB.

ImageFormat (Argument) | Command: CreateVm

Type	Enum
Range	Qcow2(100) | Raw(200)
Default	Raw

VM image format.

- QCOW2: QEMU copy-on-write format. The file extension is '.img'.
- RAW: Plain binary image of the VM disk image, and is very portable. The file extension is '.raw'.

'Raw' is the default value.

NbCores (Argument) | Command: CreateVm

Type	UInt32
Range	0..7
Default	0

Number of Virtual CPU (vCPU) allocated to the VM.

Note that 1 vCPU is reserved for the DGW application.

0 is default value, it is valid when a VM config file exists otherwise the minimal value is 1.

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Vm service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.4500.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10	The '%1$s' VM (%2$d) was started successfully.	Info	This message is issued when the VM has started successfully.
20	The '%1$s' VM (%2$d) was rebooted successfully	Info	This message is issued when the VM has rebooted successfully.
30	The '%1$s' VM (%2$d) was stopped successfully.	Info	This message is issued when the VM has stopped successfully.
35	The '%1$s' VM(%2$d) is stopping.	Info	This message is issued when the VM is requested to stop.
40	The '%1$s' VM (%2$d) failed to start.	Error	This message is issued when the VM has failed starting.
50	The '%1$s' VM (%2$d) failed to reboot.	Error	This message is issued when the VM has failed rebooting.
60	The '%1$s' VM (%2$d) failed to stop.	Error	This message is issued when the VM has failed stopping.
65	The '%1$s' VM(%2$d) failed to stop in time.	Error	This message means the VM was forced to stop because it did not complete its shutdown process within the allowed time.
70	No Network Interfaces is available for the '%1$s' VM (%2$d).	Warning	This message is issued when a VM has added and no network interfaces is available for this VM.
80	Insufficient system resources to start the '%1$s' VM (%2$d), reason: %3$s.	Error	This message is issued when the Vm service tries to start a VM and the System resources are insufficient for one of the following reasons: • Out Of Memory • Out Of vCPU
90	The '%1$s' VM (%2$d) apparently stopped by itself.	Warning	This message is issued when the VM has stopped without being requested to by the Vm service.
100	The '%1$s' VM (%2$d) cannot start because the VNC DisplayId %3$d is already in use.	Error	This message is issued when the Vm service tries to start a VM and its VNC display Id is used by another VM already started.

NumKey	Message	Severity	Description
110	The internal virtual switch IP address and/or subnet mask are in conflict with another network interface.	Warning	This message is issued when the internal virtual switch IP address and/or subnet mask are in conflict with another address and/or subnet mask of the Bni service.
120	The conversion of the '%1$s' VM image is started.	Info	This message is issued when the VM conversion command is started and running.
130	The conversion of the '%1$s' VM image ended with the following result: %2$s.	Info	This message is issued when the VM conversion command ended.
140	The '%1$s' VM name matches more than one VM image. The preferred VM image to run is '%2$s'.	Warning	This message is issued when more than one VM image share the same VM name.
150	The '%1$s' (%2$d) VM's VNC server has been automatically disabled after a %3$d minutes timer.	Info	This message is issued when a VM's VNC server is disabled by the AutomaticVncShutdown feature'.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.

NumKey	Message	Severity	Description
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.

NumKey	Message	Severity	Description
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Vm.

Message	Severity	Description
The parameter values are in conflict with the parameters of the existing VM configuration file.	Error	This message is issued when trying to add a virtual machine using parameters that are in conflict with an existing configuration file.
Not enough storage.	Error	This message is issued when trying to add a virtual machine with a storage size that exceeds the space available on the disk.
Not enough RAM.	Error	This message is issued when trying to add a virtual machine with a memory size that exceeds the space available in the system.
Not enough vCPU.	Error	This message is issued when trying to add a virtual machine with a number of vCPU that exceeds the quantity available in the system.
Missing VM configuration file.	Error	This message is issued when trying to add a pre-configured virtual machine while the configuration file is missing.
Missing resources to run all VMs concurrently.	Warning	This message is issued when trying to add a virtual machine using an amount of memory or quantity of vCPU that may not be available at VM start. The VMs cannot run all at the same time.
The VM failed to start.	Error	This message is issued when the Vm service has failed to start VM.
The Vm service failed to create the VM image.	Error	This message is issued when the Vm service has failed to create the VM image.
Maximum number of VMs reached.	Error	This message is issued when the maximum number of allowed virtual machines is reached.
Image file not found.	Error	This message is issued when trying to start a virtual machine and the corresponding image file does not exist.
Invalid state.	Error	This message is issued when the Vm service tries to start/stop/reboot a virtual machine and its state does not allow the execution of this command.
Insufficient system ressources to start the VM.	Error	This message is issued when the Vm service tries to start a VM and the System resources are insufficient.

Message	Severity	Description
Bootable disc file not found	Error	This message is issued when trying to start a virtual machine with a bootable disc file and the corresponding file is not found.
Vnc Display Id in use.	Error	This message is issued when a VM failed to start because the same VNC Display Id is already used by another VM.
Mismatching disk size values for the "%1$s" VM image file. The image file allocated %2$d Gb while the VM is configured for %3$d Gb.	Error	This message is issued when disk size allocated by the VM image mismatches the disk size specified in the VM configuration file.
The subnet "%1$s" is not available.	Error	This message is issued when the specified subnet is in conflict with a subnet reserved for internal use.
The VM may loose network connectivity if virtio is not supported by the OS.	Warning	This message is issued when the virtualised network adapter is set to virtio.
The Vm service failed to convert the "%1$s" VM image: %2$s.	Error	This message is issued when the Vm service has failed to start a VM conversion command, for one of the following reasons: • Not enough space • Input image file is not found • Input image file cannot be read • Input image file is corrupted • Input image file already in use by a VM • Output image file cannot be deleted
The Vm service is already running a VM image conversion.	Error	This message is issued when the Vm service is already running a VM conversion command. Only one conversion at a time is possible.
Write Success.	Info	Configuration changes were applied successfully.

Message	Severity	Description
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.

Message	Severity	Description
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Web Service (Web)

The Web service allows the administrator to manage the unit using HTTP(S) web pages.

Parameters

HttpMode (Config Parameter)

Type	Enum
Range	Secure(100) | Unsecure(200) | Both(300)
Default	Both
Script/CLI	Web.HttpMode
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1200.1.100.50

Defines the HTTP mode(s) to which the Web server should listen.

- Secure: The Web server only accepts requests using HTTPS. Requests using HTTP are ignored.
- Unsecure: The Web server only accepts requests using HTTP. Requests using HTTPS are ignored.
- Both: The Web server accepts requests using HTTP or HTTPS.

The Web server configured in 'Secure' or 'Both' modes listens to HTTPS requests only if a server certificate with "server authentication" extended key usage is present on the unit.

ServerPort (Config Parameter)

Type	IpPort
Range	
Default	80
Script/CLI	Web.ServerPort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1200.1.100.100

Listening port of the HTTP server.

SecureServerPort (Config Parameter)

Type	IpPort
Range	
Default	443
Script/CLI	Web.SecureServerPort
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1200.1.100.200

Listening port of the HTTPS server.

HttpsCipherSuite (Config Parameter)

Type	Enum
Range	CS1(100) | CS2(200) | CS3(300)
Default	CS1
Script/CLI	Web.HttpsCipherSuite
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1200.1.100.300

Defines the allowed cipher suites for the network security settings to which the Web server should listen when using the HTTPS

- CS1:
  - TLS_DHE_DSS_WITH_AES_128_CBC_SHA
  - TLS_DHE_DSS_WITH_AES_256_CBC_SHA
  - Also includes ciphers from CS2 and CS3 below

- CS2:
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - Also includes ciphers from CS3 below
- CS3:
  - The following are TLS 1.2 ciphers:
  - TLS_RSA_WITH_AES_128_CBC_SHA256
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_CBC_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
  - The following are TLS 1.3 ciphers:
  - TLS_AES_256_GCM_SHA384
  - TLS_AES_128_GCM_SHA256
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_CCM_8_SHA256
  - TLS_AES_128_CCM_SHA256

Any connection attempts to the web server using a cipher that is not allowed by the cipher suite will result in a failure to establish the connection.

TlsVersion (Config Parameter)

Type	Enum
Range	TLSv1(200) | TLSv1_1(300) | TLSv1_2 (400) | TLSv1_3 (500)
Default	TLSv1
Script/CLI	Web.TlsVersion
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1200.1.100.400

Defines the allowed TLS versions for the network security settings when using the HTTPS.

- TLSv1: Allow TLS versions 1 and up.
- TLSv1_1: Allow TLS versions 1.1 and up.
- TLSv1_2: Allow TLS versions 1.2 and up.
- TLSv1_3: Allow TLS version 1.3 only.

Any connection attempts to the web server using a TLS version that is not allowed will result in a failure to establish the connection.

HstsHeaderEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Web.HstsHeaderEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1200.1.100.500

Determines whether or not the following HTTP Strict-Transport-Security (HSTS) header should be included in HTTPS responses, as per RFC 6797:

- Strict-Transport-Security: max-age=31556952

Note: This parameter is only used when the **Web.HttpMode** parameter is set to 'Secure'.

Important: Make sure the HTTPS connection works properly before enabling this parameter. Once enabled, the web browsers will automatically initiate HTTPS requests only, until the 1-year cache expiration.

StatsRequest (Status Parameter)

Type	UInt32
Range	
Script/CLI	Web.StatsRequest
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1200.1.10000.100

Number of Requests handled by the service.

StatsRedirect (Status Parameter)

Type	UInt32
Range	
Script/CLI	Web.StatsRedirect
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1200.1.10000.200

Number of redirections handled by the service.

StatsError (Status Parameter)

Type	UInt32
Range	
Script/CLI	Web.StatsError
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1200.1.10000.300

Number of Errors handled by the service.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Web.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1200.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Web.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.1200.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Web service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.100.1200.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
11	Web server is listening for unsecure HTTP requests on address '%1$s' and port '%2$d'.	Info	This message is issued when the WEB server is listening to HTTP requests.
12	Web server is listening for secure HTTPS requests on address '%1$s' and port '%2$d'.	Info	This message is issued when the WEB server is listening to HTTPS requests.
15	Web server is not listening to any HTTP requests.	Error	This message is issued when the WEB server failed to launch.
20	Web server configuration modified due to a parameter change.	Debug	This message is issued when a configuration parameter is changed, requiring the WEB service to update its configuration.
30	No host certificate, HTTPS server functionality not available.	Warning	This message is issued when WEB cannot find any host certificate and therefor cannot enable HTTPS server functionality.
40	Web server is listening for unsecure HTTP requests on port '%1$d' of all network interfaces.	Info	This message is issued when the WEB server is listening to HTTP requests on all network interfaces.
50	Web server is listening for secure HTTPS requests on port '%1$d' of all network interfaces.	Info	This message is issued when the WEB server is listening to HTTPS requests on all network interfaces.
60	Cancelling file upload because of timeout.	Error	This message occurs when data reception stops for too long during a file upload. Note that, when the upload is canceled the 408 HTTP Timeout is returned to the browser. **Note:** This notification is platform-specific.
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.

NumKey	Message	Severity	Description
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.

NumKey	Message	Severity	Description
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Web.

Message	Severity	Description
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.

Message	Severity	Description
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Hardware Components

Hardware (Hardware)

The Hardware component manages the mainboard and the extension cards.

Parameters

ResetButtonManagement (Config Parameter)

Type	Enum
Range	All(100) | DisablePartialReset(200)
Default	All
Script/CLI	Hardware.ResetButtonManagement
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.100

Configures the actions allowed on the reset/default button.

- All: All the actions are allowed: reset, partial reset, and factory reset.
- DisablePartialReset: All actions are allowed except the partial reset.

The reset action restarts the unit.

The partial reset action provides a way to contact the unit in a known and static state while keeping most of the configuration unchanged.

The factory reset action reverts the unit back to its default factory settings.

For more details, search for the Partial Reset documentation in the Media5 Documentation Portal (https://documentation.media5corp.com).

DspCodecBank (Config Parameter)

Type	Enum
Range	Bank1(100) | Bank2(200)
Default	Bank1
Script/CLI	Hardware.DspCodecBank
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.300

Selects the codec bank. A bank contains all the codecs currently available in the system.

- Bank1:
  1. G.711
  2. G.723.1
  3. G.726
  4. G.729
  5. T.38
  6. Clear Channel, Clear Mode and X-CCD
- Bank2:
  1. G.711
  2. G.722
  3. T.38
  4. Clear Channel, Clear Mode and X-CCD

The TelIf service must be restarted to apply the selected bank.

Note: This parameter is supported on all platforms, excluding the Mediatrix 4102S rev1.

FanCheckOnBootEnable (Config Parameter)

Type	EnableDisable
Range	
Default	Enable
Script/CLI	Hardware.FanCheckOnBootEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.400

Enables or disables fan checkup on boot. If enabled, the fans will run at 100% for a few seconds during the booting process in order to detect hardware faults.

Note: This feature is only available for the Sentinel 400 and Sentinel RS platforms manufactured after January 2019.

RingManagement (Config Parameter)

Type	Enum
Range	Cascade(100) | Simultaneous(200)
Default	Cascade
Script/CLI	Hardware.RingManagement
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.1000.100

Configures how the ring pulse is sent on FXS ports.

- Cascade: FXS ports are prevented from ringing at the same time in order to reduce the peak power usage of the device.
- Simultaneous: All ports ring at the same time.

Note: This parameter is only available for the 4102S platforms.

PortsStatus (Table)

This table displays the status of each PRI port.

Port (Index) | Table: PortsStatus

Type	Text
Range	
Script/CLI	Hardware.PortsStatus[].Port
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.2000.100.1.100

Indicates the name of the port.

LineType (Status Parameter) | Table: PortsStatus

Type	Enum
Range	E1(100) | T1(200)
Script/CLI	Hardware.PortsStatus[].LineType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.2000.100.1.300

Defines the line type.

Signaling (Status Parameter) | Table: PortsStatus

Type	Enum
Range	Isdn(100) | R2(200) | Eam(300)
Script/CLI	Hardware.PortsStatus[].Signaling
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.2000.100.1.400

Defines the signaling protocol used by this port.

Ports (Table)

The settings of each PRI port are configured in this table.

Port (Index) | Table: Ports

Type	Text
Range	
Script/CLI	Hardware.Ports[].Port
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.2000.200.1.100

Indicates the name of the port.

LineType (Config Parameter) | Table: Ports

Type	Enum
Range	E1(100) | T1(200)
Default	E1
Script/CLI	Hardware.Ports[].LineType
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.2000.200.1.300

Defines the line type.

- T1: DS1 T-Carrier Signaling
- E1: E1 E-Carrier Signaling

Note: The value T1 is not valid when the **Ports.Signaling** parameter is set to R2.

Signaling (Config Parameter) | Table: Ports

Type	Enum
Range	Isdn(100) | R2(200) | Eam(300)
Default	Isdn
Script/CLI	Hardware.Ports[].Signaling
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.2000.200.1.400

Defines the signaling protocol used by this port.

- Isdn: Integrated Services Digital Network
- R2: E1-R2 CAS signaling protocol.
- Eam: E&M CAS signaling protocol.

Note: The value R2 is not valid when the **Ports.LineType** parameter is set to T1.

StatsInfo (Table)

Statistics table of each PRI port.

Port (Index) | Table: StatsInfo

Type	Text
Range	
Script/CLI	Hardware.StatsInfo[].Port
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.2000.1000.100.1.100

The name of the port.

FramesTransmitted (Status Parameter) | Table: StatsInfo

Type	UInt32
Range	
Script/CLI	Hardware.StatsInfo[].FramesTransmitted
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.2000.1000.100.1.200

Number of HDLC frames transmitted.
Note: Frames do not refer to the structure defined in I.431.

FramesReceived (Status Parameter) | Table: StatsInfo

Type	UInt32
Range	
Script/CLI	Hardware.StatsInfo[].FramesReceived
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.2000.1000.100.1.300

Number of HDLC frames received.
Note: Frames do not refer to the structure defined in I.431.

OctetsTransmitted (Status Parameter) | Table: StatsInfo

Type	UInt32
Range	
Script/CLI	Hardware.StatsInfo[].OctetsTransmitted
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.2000.1000.100.1.400

Number of octets transmitted. This value is obtained by cumulating the octets transmitted in the HDLC frames.
Note: Frames do not refer to the structure defined in I.431.

OctetsReceived (Status Parameter) | Table: StatsInfo

Type	UInt32
Range	
Script/CLI	Hardware.StatsInfo[].OctetsReceived
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.2000.1000.100.1.500

Number of octets received. This value is obtained by cumulating the octets received in the HDLC frames.
Note: Frames do not refer to the structure defined in I.431.

FcsErrors (Status Parameter) | Table: StatsInfo

Type	UInt32
Range	
Script/CLI	Hardware.StatsInfo[].FcsErrors
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.2000.1000.100.1.600

Frame check sequence (FCS) errors indicate that frames of data are being corrupted during transmission. FCS error count is the number of frames that were received with a bad checksum (CRC value) in the HDLC frame. These frames are dropped and not propagated to the upper layers. This value is available on E1 and T1.

FramesDropped (Status Parameter) | Table: StatsInfo

Type	UInt32
Range	
Script/CLI	Hardware.StatsInfo[].FramesDropped
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.2000.1000.100.1.700

Number of frames dropped. This value is obtained by cumulating the number of frames dropped when transferring data from the framer chip to the device internal buffer.
This value is available on E1 and T1.

OctetsDropped (Status Parameter) | Table: StatsInfo

Type	UInt32
Range	
Script/CLI	Hardware.StatsInfo[].OctetsDropped
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.2000.1000.100.1.800

Number of octets dropped. This value is obtained by cumulating the number of octets dropped when transferring data from the framer chip to the device internal buffer.
This value is available on E1 and T1.

NegativeFrameSlipsTransmitted (Status Parameter) | Table: StatsInfo

Type	UInt32
Range	
Script/CLI	Hardware.StatsInfo[].NegativeFrameSlipsTransmitted
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.2000.1000.100.1.900

A frame is skipped when the frequency of the transmit clock is greater than the frequency of the transmit system interface working clock (2.048 MHz on E1 or 1.544 MHz on T1).
This value is available on E1 and T1.

NegativeFrameSlipsReceived (Status Parameter) | Table: StatsInfo

Type	UInt32
Range	
Script/CLI	Hardware.StatsInfo[].NegativeFrameSlipsReceived
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.2000.1000.100.1.1000

A frame is skipped when the frequency of the received route clock is greater than the frequency of the receive system interface working clock (2.048 MHz on E1 or 1.544 MHz on T1).
This value is available on E1 and T1.

PositiveFrameSlipsTransmitted (Status Parameter) | Table: StatsInfo

Type	UInt32
Range	
Script/CLI	Hardware.StatsInfo[].PositiveFrameSlipsTransmitted
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.2000.1000.100.1.1100

A frame is repeated when the frequency of the transmit clock is less than the frequency of the transmit system interface working clock (2.048 MHz on E1 or 1.544 MHz on T1).
This value is available on E1 and T1.

PositiveFrameSlipsReceived (Status Parameter) | Table: StatsInfo

Type	UInt32
Range	
Script/CLI	Hardware.StatsInfo[].PositiveFrameSlipsReceived
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.2000.1000.100.1.1200

A frame is repeated when the frequency of the receive route clock is less than the frequency of the receive system interface working clock (2.048 MHz on E1 or 1.544 MHz on T1).
This value is available on E1 and T1.

FramingErrors (Status Parameter) | Table: StatsInfo

Type	UInt32
Range	
Script/CLI	Hardware.StatsInfo[].FramingErrors
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.2000.1000.100.1.1300

The framing error count indicates that a FAS (Frame Alignment Signal) word has been received with an error.
The FAS-bits are present in every even frame of timeslot 0 on E1.

The FAS-bits are present in ESF format on T1.

This value is available on E1 and T1.

CodeViolations (Status Parameter) | Table: StatsInfo

Type	UInt32
Range	
Script/CLI	Hardware.StatsInfo[].CodeViolations
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.2000.1000.100.1.1400

The code violations count indicates that an encoding error on the PCM line has been detected.
This value is available on E1 and T1.

CRCErrors (Status Parameter) | Table: StatsInfo

Type	UInt32
Range	
Script/CLI	Hardware.StatsInfo[].CRCErrors
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.2000.1000.100.1.1500

The CRC errors count is incremented when a multiframe has been received with a CRC error.
On E1, this counter is only available with the CRC line framing format.

On T1, this counter is only available with the ESF line framing format.

EBitErrors (Status Parameter) | Table: StatsInfo

Type	UInt32
Range	
Script/CLI	Hardware.StatsInfo[].EBitErrors
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.2000.1000.100.1.1600

The E-Bit error count gives information about the outgoing transmit PCM line if the E-bits are used by the remote end for submultiframe error indication. Incrementing is only possible in the multiframe synchronous state.
Due to signaling requirements, the E-bits of frame 13 and frame 15 of the CRC multiframe can be used to indicate an error in a received submultiframes:

- Submultiframe I status E-bit located in frame 13
- Submultiframe II status E-bit located in frame 15
- no CRC error: E = 1
- CRC error: E = 0

This value is only available in E1.

BlockErrors (Status Parameter) | Table: StatsInfo

Type	UInt32
Range	
Script/CLI	Hardware.StatsInfo[].BlockErrors
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.2000.1000.100.1.1700

The Block Error count is incremented once per multiframe if a multiframe has been received with a CRC error or if a bad frame alignment has been detected.
This value is only available for ESF format on T1 only.

ResetStats (Row Command) | Table: StatsInfo

Script/CLI:	Hardware.StatsInfo[].ResetStats
SNMP OID:	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.2000.1000.100.1.10000

Resets all statistics for the specified interface.

BriPortsStatus (Table)

This table displays the status of each BRI port.

Port (Index) | Table: BriPortsStatus

Type	Text
Range	
Script/CLI	Hardware.BriPortsStatus[].Port
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.3000.100.1.100

Indicates the name of the port.

PowerFeeding (Status Parameter) | Table: BriPortsStatus

Type	Enum
Range	On(100) | Off(200) | Unavailable(300) | Unsupported(400)
Script/CLI	Hardware.BriPortsStatus[].PowerFeeding
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.3000.100.1.200

Indicates the state of the power feeding for the port.

- On: Power is fed to the line.
- Off: Power is not fed to the line.
- Unavailable: The power feeding feature is unavailable on TE endpoints.
- Unsupported: The power feeding feature is not physically supported on this port.

BriPorts (Table)

The settings of each BRI port are configured in this table.

Port (Index) | Table: BriPorts

Type	Text
Range	
Script/CLI	Hardware.BriPorts[].Port
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.3000.200.1.100

Indicates the name of the port.

PowerFeedingEnable (Config Parameter) | Table: BriPorts

Type	EnableDisable
Range	
Default	Disable
Script/CLI	Hardware.BriPorts[].PowerFeedingEnable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.3000.200.1.200

Enables or disables the power feeding for the port.

ClockReferenceList (Status Parameter)

Type	Text
Range	
Script/CLI	Hardware.ClockReferenceList
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.5000.100

List of available clock references.
The SYNCIN value means the internal clock is synchronised with the SYNC IN port (on platforms equipped with this port).

ClockReferenceSource (Config Parameter)

Type	Text
Range	Size(0..255)
Default	
Script/CLI	Hardware.ClockReferenceSource
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.5000.200

Indicates the preferred synchronisation source(s) to use for the internal clock. Refer to the **ClockReferenceList** parameter for a list of available clock references for the platform.

When the value is empty, the platform will automatically choose the synchronisation source.

When a source or a list of sources are specified, the internal clock is synchronised with the first source that offers a valid signal. The only exception is the SYNCIN port (not present on all platforms), which is always used when encountered in the list.

The string separators to use is the ',' (comma), it allows to list the synchronization sources, per priority for the Sentinel and the G7 platforms only.

Examples:

- For C7xx: "BRI1, BRI2"
- For Sentinel 400: "Slot1/E1T1, Slot2/BRI1, Slot2/BRI2, SYNCIN"
- For Sentinel RS: "Slot1/E1T1, Slot2/BRI1, Slot2/BRI2, SYNCIN"
- For Sentinel 100 and G7: "BRI1, BRI2, PRI1, PRI2, SYNCIN"
- Any platform: ""

ClockReferenceStatus (Status Parameter)

Type	Text
Range	
Script/CLI	Hardware.ClockReferenceStatus
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.5000.300

Indicates the synchronisation source currently in use.
Only one clock reference status is displayed.

The 'None' value means the internal clock is not synchronised.

PortsConfiguration (Config Parameter)

Type	Enum
Range	Separate(100) | Bridge(200)
Default	Separate
Script/CLI	Hardware.PortsConfiguration
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.10000.100

Configures how each port provides a link interface.

- Separate: Each Ethernet port provides an independent link interface. This is the required configuration for IP Routing.
- Bridge: Both Ethernet ports are bridged together and provide a single link interface.

Note: This feature is only available on units with a total of 2 Ethernet ports.

KernelNetworkPriority (Config Parameter)

Type	UInt32
Range	0..100
Default	10
Script/CLI	Hardware.KernelNetworkPriority
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.10000.200

Controls the network priority in the kernel. The default value is platform-dependent. This parameter should not be altered, unless advised otherwise by a technical support specialist.

MinSeverity (Config Parameter)

Type	Enum
Range	Disable(0) | Debug(100) | Info(200) | Warning(300) | Error(400) | Critical (500)
Default	Warning
Script/CLI	Hardware.MinSeverity
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.60010.100

Sets the minimal severity to issue a notification message incoming from this service.

- Disable: No notification is issued.
- Debug: All notification messages are issued.
- Info: Notification messages with a "Informational" and higher severity are issued.
- Warning: Notification messages with a "Warning" and higher severity are issued.
- Error: Notification messages with an "Error" and higher severity are issued.
- Critical: Notification messages with a "Critical" severity are issued.

NeedRestartInfo (Status Parameter)

Type	Enum
Range	No(0) | Yes(100)
Script/CLI	Hardware.NeedRestartInfo
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.500.40000.1.60020.100

Indicates if the service needs to be restarted for the configuration to fully take effect.

- Yes: Service needs to be restarted.
- No: Service does not need to be restarted.

Services can be restarted by using the `Scm.ServiceCommands.Restart` command.

Commands

LockConfig (Command)

Locks the configuration parameters for this service for exclusive write access. Use the `UnlockConfig` command to release the lock.

The lock is also released automatically when no write operations are made for 30 minutes.

UnlockConfig (Command)

Releases exclusive write access to configuration parameters for this service.

Notification Messages

This section describes all the notification messages relevant to the Hardware service. Notification messages are logged or sent to the administrator based on rules defined in the Notifications and Logging Manager Service (NLM).

The complete notification message OID for the Snmp service is:

```
.1.3.6.1.4.1.4935.1000.100.200.500.40000.200.300.NumKey
```

where the NumKey refers to the following table.

NumKey	Message	Severity	Description
10000	Parameter value: [%1$s].	Debug	
60010	The service is no longer responding. Triggering the system watchdog.	Critical	A software module has an abnormal behaviour. This kind of error usually restarts a service or the entire system. Refer to the release notes or contact a technical support specialist.
60020	An internal error was encountered. Error code: %1$s.	Critical	A software module encountered an internal error. This kind of error might alter the behaviour of the system. Refer to the release notes or contact a technical support specialist.
60030	Explicit configuration lock for %1$s expired.	Warning	The explicit lock of a user expired after 30 minutes of inactivity.
60040	Implicit configuration lock for %1$s was broken by an explicit lock from %2$s.	Info	The implicit lock of a user was superseded by an explicit lock from a different user or the system.
60050	Explicit configuration lock for %1$s was denied because of an explicit lock from %2$s.	Info	The explicit lock of a user or the system is refused because another user or the system is already locking the service.
60060	Explicit configuration lock acquired for %1$s.	Debug	An implicit lock is granted to a user or the system.
60070	Explicit configuration lock released by %1$s.	Debug	An implicit lock is released by a user or the system.
60080	Profile ignored, file not present.	Info	Profile was not applied because the profile file is missing.
60090	Error while processing the profile file.	Error	System failed to process the profile file.
60100	The %1$s parameter in the profile was out of range and has been adjusted.	Warning	The requested value is not authorised.
60110	The %1$s parameter in the profile was out of range and has been ignored.	Warning	The requested value is not authorised.

NumKey	Message	Severity	Description
60120	Service going into draining mode.	Info	The service has received a draining mode request and will enter the draining state.
60130	Service going out of draining mode.	Info	The service has received a draining mode cancel and will exit the draining state.
60140	The '%1$s' scalar has changed value. Changed from '%2$s' to '%3$s'. The request was made by '%4$s'.	Info	A scalar had its value changed.
60150	The '%1$s' columnar of the '%2$s' table with '%3$s' index has changed value. Changed from '%4$s' to '%5$s'. The request was made by '%6$s'.	Info	A columnar had its value changed.
60160	A row was inserted in the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was added.
60170	A row was deleted from the '%1$s' table at the '%2$s' index. The request was made by '%3$s'.	Info	A row was deleted.
60180	All rows were deleted from the '%1$s' table. The request was made by '%2$s'.	Info	All rows were deleted.
60200	The configuration is lost because the file is too big.	Critical	This message is sent when the configuration file of the service or hardware component cannot be loaded because it becomes too big. The configuration is lost.
60210	The configuration will be lost because the file is too big.	Critical	This message is sent after writing the configuration of the service or hardware component and the file size is too big. The service or hardware component configuration will be lost at the next service restart if the number of configuration is not reduced.

Configuration Messages

This section describes all the configuration messages relevant to Hardware.

Message	Severity	Description
Power feeding is unsupported on this port.	Error	This message is issued when trying to enable or disable the power feeding on a BRI port that does not physically support it.
Write Success.	Info	Configuration changes were applied successfully.
Command Executed.	Info	Command successfully executed.
Read Success.	Info	Configuration successfully read.
Bad Syntax.	Error	Configuration change not allowed because of a syntax error.
Out of Range.	Error	Configuration change not allowed because the value is out of range.
Locked by %1$s.	Error	Configuration lock or modification not allowed because access is currently locked by the system or another user.
Configuration Locked.	Info	Configuration successfully locked.
Configuration Unlocked.	Info	Configuration successfully unlocked.
Not Found.	Error	Parameter or command not found.
No Read Access.	Error	Parameter cannot be read.
No Write Access.	Error	Parameter cannot be written.
Index Out of Range.	Error	Configuration change not allowed because the index is out of range.
Cannot Delete Row.	Error	Row deletion not allowed in this table.
Cannot Insert Row.	Error	Row insertion not allowed in this table.
Duplicate Row.	Error	Cannot insert row because a row with the same index already exists.
Maximum Size Reached.	Error	Row insertion not allowed in this table because it has reached its maximal size.
Minimum Size Reached.	Error	Row deletion not allowed in this table because it has reached its minimal size.
Row Inserted.	Info	Row insertion was successful.
Row Deleted.	Info	Row deletion was successful.
Cannot Delete All Rows.	Error	Deletion of all rows not allowed in this table.

Message	Severity	Description
Type Mismatch.	Error	Configuration change not allowed because the value type does not match the parameter type.
Warning: Possible conflict for %1$s port number %2$s. This port is currently in use.	Warning	This message is issued when a service is assigned a port number that was in use at the time the assignation was made. This indicates a possible conflict because for a given protocol (TCP or UDP) a port number can only be opened once. The administrator must make sure the configuration introduces no conflict among UDP or TCP ports.
The '%1$s' configuration line was ignored by the system and was not executed.	Warning	This message is issued when a configuration line is ignored by the system. This indicates a missing service or an unsupported feature.

Copyright Notice

Copyright © 2026 Media5 Corporation.

This document contains information that is confidential and proprietary to Media5 Corporation.

Media5 Corporation reserves all rights to this document as well as to the Intellectual Property of the document and the technology and know-how that it includes and represents.

This publication cannot be reproduced, neither in whole nor in part, in any form whatsoever, without written prior approval by Media5 Corporation.

Media5 Corporation reserves the right to revise this publication and make changes at any time and without the obligation to notify any person and/or entity of such revisions and/or changes.

media5 corporation

media5corp.com