Reference Material

About Event Log Levels

All events have an associated level in the range 1-4, with Level 1 Events considered the most important. The table below gives an overview of the levels assigned to different events.

Level	Assigned events
1	High-level events such as registration requests and call attempts. Easily human readable. For example: • call attempt/connected/disconnected • registration attempt accepted/rejected
2	All Level 1 events, plus: logs of protocol messages sent and received (SIP, H.323, LDAP and so on) excluding noisy messages such as H.460.18 keepalives and H.245 video fast-updates
3	All Level 1 and Level 2 events, plus: • protocol keepalives • call-related SIP signaling messages
4	The most verbose level: all Level 1, Level 2 and Level 3 events, plus: • network level SIP messages

See the Events and Levels section for a complete list of all events that are logged by the Expressway, and the level at which they are logged.

Event Log Format

The Event Log is displayed in an extension of the UNIX syslog format:

```
date time process_name: message_details
```

where:

Field	Description
date	The local date on which the message was logged.
time	The local time at which the message was logged.
process_name	The name of the program generating the log message. This could include: • **tvcs** for all messages originating from Expressway processes • **web** for all web login and configuration events • **licensemanager** for messages originating from the call license manager • **b2bua** for B2BUA events • **portforwarding** for internal communications between the Expressway-C and the Expressway-E • **ssh** for ssh tunnels between the Expressway-C and the Expressway-E but will differ for messages from other applications running on the Expressway.

Field	Description
message_details	The body of the message (see the Message Details Field section for further information).

Administrator Events

Administrator session related events are:

- Admin Session Start
- Admin Session Finish
- Admin Session Login Failure

The Message Details Field includes:

- the name of the administrator user to whom the session relates, and their IP address
- the date and time that the login was attempted, started, or ended

Message Details Field

For all messages logged from the tvcs process, the `message_details` field, which contains the body of the message, consists of a number of human-readable `name=value` pairs, separated by a space.

The first name element within the `message_details` field is always `Event` and the last name element is always `Level`.

The table below shows all the possible name elements within the `message_details` field, in the order that they would normally appear, along with a description of each.

Note In addition to the events described below, a `syslog.info` event containing the string `MARK` is logged after each hour of inactivity to provide confirmation that logging is still active.

Name	Description
Event	The event which caused the log message to be generated. See Events and Levels for a list of all events that are logged by the Expressway, and the level at which they are logged.
User	The username that was entered when a login attempt was made.
ipaddr	The source IP address of the user who has logged in.

Name	Description
Protocol	Specifies which protocol was used for the communication. Valid values are: • TCP • UDP • TLS
Reason	Textual string containing any reason information associated with the event.
Service	Specifies which protocol was used for the communication. Will be one of: • H.323 • SIP • H.225 • H.245 • LDAP • Q.931 • NeighbourGatekeeper • Clustering • ConferenceFactory
Message Type	Specifies the type of the message.
Response-code	SIP response code or, for H.323 and interworked calls, a SIP equivalent response code.
Src-ip	Source IP address (the IP address of the device attempting to establish communications). This can be an IPv4 address or an IPv6 address.
Dst-ip	Destination IP address (the IP address of the destination for a communication attempt). The destination IP is recorded in the same format as Src-ip.
Src-port	Source port: the IP port of the device attempting to establish communications.
Dst-port	Destination port: the IP port of the destination for a communication attempt.

Name	Description
Src-alias	If present, the first H.323 alias associated with the originator of the message. If present, the first E.164 alias associated with the originator of the message.
Dst-alias	If present, the first H.323 alias associated with the recipient of the message. If present, the first E.164 alias associated with the recipient of the message.
Detail	Descriptive detail of the Event.
Auth	Whether the call attempt has been authenticated successfully.
Method	SIP method (INVITE, BYE, UPDATE, REGISTER, SUBSCRIBE, etc).
Contact	Contact: header from REGISTER.
AOR	Address of record.
Call-id	The Call-ID header field uniquely identifies a particular invitation or all registrations of a particular client.
Call-serial-number	The local Call Serial Number that is common to all protocol messages for a particular call.
Tag	The Tag is common to all searches and protocol messages across an Expressway network for all forks of a call.
Call-routed	Indicates if the Expressway took the signaling for the call.
To	• for REGISTER requests: the AOR for the REGISTER request • for INVITEs: the original alias that was dialed • for all other SIP messages: the AOR of the destination.
Request-URI	The SIP or SIPS URI indicating the user or service to which this request is being addressed.
Num-bytes	The number of bytes sent/received in the message.
Protocol-buffer	Shows the data contained in the buffer when a message could not be decoded.
Duration	Request/granted registration expiry duration.
Time	A full UTC timestamp in YYYY/MM/DD-HH:MM:SS format. Using this format permits simple ASCII text sorting/ordering to naturally sort by time. This is included due to the limitations of standard syslog timestamps.

Name	Description
Level	The level of the event as defined in the About Event Log Levels section.
UTC Time	Time the event occurred, shown in UTC format.

Events and Levels

The following table lists the events that can appear in the Event Log:

Event	Description	Level
Alarm acknowledged	An administrator has acknowledged an alarm. The **Detail** event parameter provides information about the nature of the issue.	1
Alarm lowered	The issue that caused an alarm to be raised has been resolved. The **Detail** event parameter provides information about the nature of the issue.	1
Alarm raised	The Expressway has detected an issue and raised an alarm. The **Detail** event parameter provides information about the nature of the issue.	1
Admin Session CBA Authorization Failure	An unsuccessful attempt has been made to log in when the Expressway is configured to use certificate-based authentication.	1
Admin Session Finish	An administrator has logged off the system.	1
Admin Session Login Failure	An unsuccessful attempt has been made to log in as an administrator. This could be because an incorrect username or password (or both) was entered.	1
Admin Session Start	An administrator has logged onto the system.	1
Application Exit	The Expressway application has been exited. Further information may be provided in the **Detail** event parameter.	1
Application Failed	The Expressway application is out of service due to an unexpected failure.	1
Application Start	The Expressway has started. Further detail may be provided in the **Detail** event parameter.	1
Application Warning	The Expressway application is still running but has experienced a recoverable problem. Further detail may be provided in the **Detail** event parameter.	1

Event	Description	Level
Authorization Failure	The user has either entered invalid credentials, does not belong to an access group, or belongs to a group that has an access level of "None". Applies when remote authentication is enabled.	1
Beginning System Backup	A system backup has started.	1
Beginning System Restore	A system restore has started.	1
Call Answer Attempted	An attempt to answer a call has been made.	1
Call Attempted	A call has been attempted.	1
Call Bandwidth Changed	The endpoints in a call have renegotiated call bandwidth.	1
Call Connected	A call has been connected.	1
Call Diverted	A call has been diverted.	1
Call Disconnected	A call has been disconnected.	1
Call Inactivity Timer	A call has been disconnected due to inactivity.	1
Call Rejected	A call has been rejected. The **Reason** event parameter contains a textual representation of the H.225 additional cause code.	1
Call Rerouted	The Expressway has **Call signaling optimization** set to *On* and has removed itself from the call signaling path.	1
CBA Authorization Failure	An attempt to log in using certificate-based authentication has been rejected due to authorization failure.	1
Certificate Management	Indicates that security certificates have been uploaded. See the **Detail** event parameter for more information.	1
Completed System Backup	A system backup has completed.	1
Completed System restore	A system restore has completed.	1
Configlog Cleared	An operator cleared the Configuration Log.	1
Decode Error	A syntax error was encountered when decoding a SIP or H.323 message.	1
Diagnostic Logging	Indicates that diagnostic logging is in progress. The **Detail** event parameter provides additional details.	1

Event	Description	Level
Error Response Sent	The TURN server has sent an error message to a client (using STUN protocol).	3
Eventlog Cleared	An operator cleared the Event Log.	
External Server Communication Failure	Communication with an external server failed unexpectedly. The **Detail** event parameter should differentiate between “no response” and “request rejected”. Servers concerned are: • DNS • LDAP Servers • Neighbor Gatekeeper • NTP servers • Peers	
Hardware Failure	There is an issue with the Expressway hardware. If the problem persists, contact your Cisco support representative.	
License Limit Reached	Licensing limits for a given feature have been reached. The **Detail** event parameter specifies the facility/limits concerned. If this occurs frequently, you may want to contact your Cisco representative to purchase more licenses.	
Message Received	An incoming RAS message has been received.	2
Message Received	An incoming RAS NSM Keepalive, H.225, H.245 or a RAS message between peers has been received.	3
Message Received	(SIP) An incoming message has been received.	4

Event	Description	Level
Message Rejected	This could be for one of two reasons: • If authentication is enabled and an endpoint has unsuccessfully attempted to send a message (such as a registration request) to the Expressway. This could be either because the endpoint has not supplied any authentication credentials, or because its credentials do not match those expected by the Expressway. • Clustering is enabled but bandwidth across the cluster has not been configured identically, and the Expressway has received a message relating to an unknown peer, link, pipe, subzone or zone.	
Message Sent	An outgoing RAS message has been sent.	2
Message Sent	An outgoing RAS NSM Keepalive, H.225, H.245 or a RAS message between peers has been sent.	3
Message Sent	(SIP) An outgoing message has been sent.	4
Operator Call Disconnect	An administrator has disconnected a call.	1
Outbound TLS Negotiation Error	The Expressway is unable to communicate with another system over TLS. The event parameters provide more information.	1
Package Install	A package, for example a language pack, has been installed or removed.	2
Policy Change	A policy file has been updated.	1
POST request failed	A HTTP POST request was submitted from an unauthorized session.	1
Provisioning	Diagnostic messages from the provisioning server. The **Detail** event parameter provides additional information.	1
Reboot Requested	A system reboot has been requested. The **Reason** event parameter provides specific information.	1
Registration Accepted	A registration request has been accepted.	1
Registration Refresh Accepted	A request to refresh or keep a registration alive has been accepted.	3
Registration Refresh Rejected	A request to refresh a registration has been rejected.	1

Event	Description	Level
Registration Refresh Requested	A request to refresh or keep a registration alive has been received.	3
Registration Rejected	A registration request has been rejected. The **Reason** and **Detail** event parameters provide more information about the nature of the rejection.	1
Registration Removed	A registration has been removed by the Expressway. The **Reason** event parameter specifies the reason why the registration was removed. This is one of: • Authentication change • Conflicting zones • Operator forced removal • Operator forced removal (all registrations removed) • Registration superseded	1
Registration Requested	A registration has been requested.	1
Relay Allocated	A TURN server relay has been allocated.	2
Relay Deleted	A TURN server relay has been deleted.	2
Relay Expired	A TURN server relay has expired.	2
Request Failed	A request sent to the Conference Factory has failed.	1
Request Received	A call-related SIP request has been received.	2
Request Received	A non-call-related SIP request has been received.	3
Request Sent	A call-related SIP request has been sent.	2
Request Sent	A non-call-related SIP request has been sent.	3
Request Successful	A successful request was sent to the Conference Factory.	1
Response Received	A call-related SIP response has been received.	2
Response Received	A non-call-related SIP response has been received.	3
Response Sent	A call-related SIP response has been sent.	2
Response Sent	A non-call-related SIP response has been sent.	3
Restart Requested	A system restart has been requested. The **Reason** event parameter provides specific information.	1

Event	Description	Level
Search Attempted	A search has been attempted.	1
Search Cancelled	A search has been cancelled.	1
Search Completed	A search has been completed.	1
Search Loop detected	The Expressway is in **Call loop detection** mode and has identified and terminated a looped branch of a search.	2
Secure mode disabled	The Expressway has successfully exited **Advanced account security** mode.	1
Secure mode enabled	The Expressway has successfully entered **Advanced account security** mode.	1
Security Alert	A potential security-related attack on the Expressway has been detected.	1
Success Response Sent	The TURN server has sent a success message to a client (using STUN protocol).	3
System backup completed	The system backup process has completed.	1
System Backup error	An error occurred while attempting a system backup.	1
System backup started	The system backup process has started.	1
System Configuration Changed	An item of configuration on the system has changed. The **Detail** event parameter contains the name of the changed configuration item and its new value.	1
System restore completed	The system restore process has completed.	1
System restore backing up current config	System restore process has started backing up the current configuration	1
System restore backup of current config completed	System restore process has completed backing up the current configuration	1
System restore error	An error occurred while attempting a system restore.	1
System restore started	The system restore process has started.	1
System Shutdown	The operating system was shutdown.	1
System snapshot started	A system snapshot has been initiated.	1
System snapshot completed	A system snapshot has completed.	1

Event	Description	Level
System Start	The operating system has started. The **Detail** event parameter may contain additional information if there are startup problems.	1
TLS Negotiation Error	Transport Layer Security (TLS) connection failed to negotiate.	1
Unregistration Accepted	An unregistration request has been accepted.	1
Unregistration Rejected	An unregistration request has been rejected.	1
Unregistration Requested	An unregistration request has been received.	1
Upgrade	Messages related to the software upgrade process. The **Detail** event parameter provides specific information.	1

CPL Reference

Call Processing Language (CPL) is an XML-based language for defining call handling. This section gives details of the Expressway's implementation of the CPL language and should be read in conjunction with the CPL standard RFC 3880.

The Expressway has many powerful inbuilt transform features so CPL should be required only if advanced call handling rules are required.

The Expressway supports most of the CPL standard along with some TANDBERG-defined extensions. It does not support the top level actions `<incoming>` and `<outgoing>` as described in *RFC 3880*. Instead it supports a single section of CPL within a `<taa:routed>` section.

When Call Policy is implemented by uploading a CPL script to the Expressway, the script is checked against an XML schema to verify the syntax. There are two schemas - one for the basic CPL specification and one for the TANDBERG extensions. Both of these schemas can be downloaded from the web interface and used to validate your script before uploading to the Expressway.

The following example shows the correct use of namespaces to make the syntax acceptable:

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
 xmlns:taa="http://www.tandberg.net/cpl-extensions"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <address-switch field="destination">
   <address is="reception@example.com">
    <proxy/>
   </address>
  </address-switch>
 </taa:routed>
</cpl>
```

Source and destination address formats

When the descriptions in this section refer to the source or destination aliases of a call, this means all supported address formats (URIs, IP addresses, E.164 aliases and so on).

CPL Address-Switch Node

The `address-switch` node allows the script to run different actions based on the source or destination aliases of the call. It specifies which fields to match, and then a list of address nodes contains the possible matches and their associated actions.

The address-switch has two node parameters: `field` and `subfield`.

Address

The `address` construct is used within an `address-switch` to specify addresses to match. It supports the use of Regular Expressions.

Valid values are:

`is=string`	Selected field and subfield exactly match the given string.
`contains=string`	Selected field and subfield contain the given string. Note that the CPL standard only allows for this matching on the display subfield; however the Expressway allows it on any type of field.
`subdomain-of=string`	If the selected field is numeric (for example, the tel subfield) then this matches as a prefix; so `address subdomain-of="555"` matches `5556734` and so on. If the field is not numeric then normal domain name matching is applied; so `address subdomain-of="company.com"` matches `nodeA.company.com` and so on.
`regex="regular expression"`	Selected field and subfield match the given regular expression.

All address comparisons ignore upper/lower case differences so `address is="Fred"` will also match `fred`, `freD` and so on.

Field

Within the `address-switch` node, the mandatory `field` parameter specifies which address is to be considered. The supported attributes and their interpretation are shown below:

Field parameter attributes	SIP	H.323
`unauthenticated-origin`	The “From” and “ReplyTo” fields of the incoming message.	The source aliases from the original LRQ or ARQ that started the call. If a SETUP is received without a preceding RAS message then the origin is taken from the SETUP.

Field parameter attributes	SIP	H.323
`authenticated-origin` and `origin`	The "From" and "ReplyTo" fields of the message, if it authenticates correctly (or where the relevant **Authentication Policy** is *Treat as authenticated*), otherwise `not-present`.	The source aliases from the original LRQ or ARQ that started the call if it authenticated correctly (or where the relevant **Authentication Policy** is *Treat as authenticated*) otherwise `not-present`. Because SETUP messages are not authenticated, if the Expressway receives a SETUP without a preceding RAS message the origin will always be `not-present`.
`originating-zone`	The name of the zone or subzone for the originating leg of the call. If the call originates from a neighbor, traversal server or traversal client zone then this will equate to the zone name. If it comes from an endpoint within one of the local subzones this will be the name of the subzone. If the call originates from any other locally registered endpoint this will be "DefaultSubZone". In all other cases this will be "DefaultZone".	
`originating-user`	If the relevant **Authentication Policy** is *Check credentials* or *Treat as authenticated* this is the username used for authentication, otherwise `not-present`.	
`registered-origin`	If the call originates from a registered endpoint this is the list of all aliases it has registered, otherwise `not-present`.	
`destination`	The destination aliases.	
`original-destination`	The destination aliases.	

Note that any Authentication Policy settings that apply are those configured for the relevant zone according to the source of the incoming message.

If the selected field contains multiple aliases then the Expressway will attempt to match each address node with all of the aliases before proceeding to the next address node, that is, an address node matches if it matches any alias.

Subfield

Within the address-switch node, the optional subfield parameter specifies which part of the address is to be considered. The following table gives the definition of subfields for each alias type.

If a subfield is not specified for the alias type being matched then the `not-present` action is taken.

`address-type`	Either `h323` or `sip`, based on the type of endpoint that originated the call.
`user`	For URI aliases this selects the username part. For H.323 IDs it is the entire ID and for E.164 numbers it is the entire number.

`host`	For URI aliases this selects the domain name part. If the alias is an IP address then this subfield is the complete address in dotted decimal form.
`tel`	For E.164 numbers this selects the entire string of digits.
`alias-type`	Gives a string representation of the type of alias. The type is inferred from the format of the alias. Possible types are: • Address Type • Result • URI • url-ID • H.323 ID • h323-ID • Dialed Digits • dialedDigits

Otherwise

The `otherwise` node is executed if the address specified in the `address-switch` was found but none of the preceding address nodes matched.

Not-Present

The `not-present` node is executed when the address specified in the `address-switch` was not present in the call setup message. This form is most useful when authentication is being used. With authentication enabled the Expressway will only use authenticated aliases when running policy so the not-present action can be used to take appropriate action when a call is received from an unauthenticated user (see the example *Call screening of authenticated users*).

Location

As the CPL script is evaluated it maintains a list of addresses (H.323 IDs, URLs and E.164 numbers) which are used as the destination of the call if a `proxy` node is executed. The `taa:location` node allows the location set to be modified so that calls can be redirected to different destinations.

At the start of script execution the location set is initialized to the original destination.

The following attributes are supported on `taa:location` nodes. It supports the use of Regular Expressions.

`Clear = "yes" | "no"`	Specifies whether to clear the current location set before adding the new location. The default is to append this location to the end of the set.

`url=string`	The new location to be added to the location set. The given string can specify a URL (for example, `user@domain.com`), H.323 ID or an E.164 number.
`priority=<0.0..1.0> | "random"`	Specified either as a floating point number in the range 0.0 to 1.0, or `random`, which assigns a random number within the same range. 1.0 is the highest priority. Locations with the same priority are searched in parallel.
`regex="<regular expression>"` `replace="<string>"`	Specifies the way in which a location matching the regular expression is to be changed.
`source-url-for-message="<string>"`	Replaces the From header (source alias) with the specified string.
`source-url-for-message-regex="<regular expression>"` together with `source-url-for-message-replace="<string>"`	Replaces any From header (source alias) that matches the regular expression with the specified replacement string. If there are multiple From headers (applies to H.323 only) then any From headers that do not match are left unchanged.

If the source URL of a From header is modified, any corresponding display name is also modified to match the username part of the modified source URL.

Rule-Switch

This extension to CPL is provided to simplify Call Policy scripts that need to make decisions based on both the source and destination of the call. A `taa:rule-switch` can contain any number of rules that are tested in sequence; as soon as a match is found the CPL within that rule element is executed.

Each rule must take one of the following forms:

```
<taa:rule-switch>
 <taa:rule origin="<regular expression>" destination="<regular expression>"
message-regex="<regular expression>">
 <taa:rule authenticated-origin="<regular expression>" destination="<regular expression>"
message-regex="<regular expression>">
 <taa:rule unauthenticated-origin="<regular expression>" destination="<regular expression>"
 message-regex="<regular expression>">
 <taa:rule registered-origin="<regular expression>" destination="<regular expression>"
message-regex="<regular expression>">
 <taa:rule originating-user="<regular expression>" destination="<regular expression>"
message-regex="<regular expression>">
 <taa:rule originating-zone="<regular expression>" destination="<regular expression>"
message-regex="<regular expression>">
</taa:rule-switch>
```

The meaning of the various origin selectors is as described in the CPL Address-Switch Node section.

The `message-regex` parameter allows a regular expression to be matched against the entire incoming SIP message.

Note Any rule containing a message-regex parameter will never match an H.323 call.

Proxy

On executing a proxy node the Expressway attempts to forward the call to the locations specified in the current location set. If multiple entries are in the location set then this results in a forked call. If the current location set is empty the call is forwarded to its original destination.

The proxy node supports the following optional parameters:

`timeout=<1..86400>`	Timeout duration, specified in seconds
`stop-on-busy = "yes" | "no"`	Whether to stop searching if a busy response is received

The proxy action can lead to the results shown in the table below:

`failure`	The proxy failed to route the call
busy	Destination is found but is busy
`noanswer`	Destination is found but does not answer
`redirection`	Expressway is asked to redirect the call
`default`	CPL to run if the other results do not apply

The CPL can perform further actions based on these results. Any results nodes must be contained within the `proxy` node. For example:

```
<proxy timeout="10">
 <busy>
  <!--If busy route to recording service-->
  <location clear="yes" url="recorder">
   <proxy/>
  </location>
 </busy>
</proxy>
```

Reject

If a `reject` node is executed the Expressway stops any further script processing and rejects the current call.

The custom reject strings `status=string` and `reason=string` options are supported here and should be used together to ensure consistency of the strings.

Unsupported CPL Elements

The Expressway does not currently support some elements that are described in the CPL RFC. If an attempt is made to upload a script containing any of the following elements an error message will be generated and the Expressway will continue to use its existing policy.

The following elements are not currently supported:

- time-switch
- string-switch

- language-switch
- priority-switch
- redirect
- mail
- log
- subaction
- lookup
- remove-location

CPL Examples

This section provides a selection of CPL examples:

- Call screening of authenticated users
- Call screening based on domain
- Allow calls from locally registered endpoints only
- Block calls from Default Zone and Default Subzone
- Restricting access to a local gateway

CPL Example: Call Screening of Authenticated Users

Note You can configure this behavior using Call Policy Rules, so you don't need to do it using a CPL script. However, you cannot use a combination of UI configured rules and uploaded CPL script, so if you have any CPL requirements that you cannot implement using the UI rules, you must use a script for all of your rules. See About Call Policy.

In this example, only calls from users with authenticated source addresses are allowed. See About Device Authentication, for details on how to enable authentication.

If calls are coming in through Expressway-E, then we recommend screening on the Expressway-E to prevent unwelcome calls from progressing into the network.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
 xmlns:taa="http://www.tandberg.net/cpl-extensions"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <address-switch field="authenticated-origin">
   <not-present>
    <!-- Reject call with a status code of 403 (Forbidden) -->
    <reject status="403" reason="Denied by policy"/>
   </not-present>
  </address-switch>
```

```
 </taa:routed>
</cpl>
```

CPL Example: Call Screening Based on Alias

Note You can configure this behavior using Call Policy Rules, so you don't need to do it using a CPL script. However, you cannot use a combination of UI configured rules and uploaded CPL script, so if you have any CPL requirements that you cannot implement using the UI rules, you must use a script for all of your rules. See About Call Policy.

In this example, user ceo will only accept calls from users `vpsales`, `vpmarketing` or `vpengineering`.

If calls are coming in through Expressway-E, then we recommend screening on the Expressway-E to prevent unwelcome calls from progressing into the network.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
 xmlns:taa="http://www.tandberg.net/cpl-extensions"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <address-switch field="destination">
   <address is="ceo">
    <address-switch field="authenticated-origin">
     <address regex="vpsales|vpmarketing|vpengineering">
      <!-- Allow the call -->
      <proxy/>
     </address>
     <not-present>
      <!-- Unauthenticated user -->
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="Denied by policy"/>
     </not-present>
     <otherwise>
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="Denied by policy"/>
     </otherwise>
    </address-switch>
   </address>
  </address-switch>
 </taa:routed>
</cpl>
```

CPL Example: Call Screening Based on Domain

Note You can configure this behavior using Call Policy Rules, so you don't need to do it using a CPL script. However, you cannot use a combination of UI configured rules and uploaded CPL script, so if you have any CPL requirements that you cannot implement using the UI rules, you must use a script for all of your rules. See About Call Policy.

In this example, user fred will not accept calls from anyone at `annoying.com`, or from any unauthenticated users. All other users will allow any calls.

If calls are coming in through Expressway-E, then we recommend screening on the Expressway-E to prevent unwelcome calls from progressing into the network.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
 xmlns:taa="http://www.tandberg.net/cpl-extensions"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <address-switch field="destination">
   <address is="fred">
    <address-switch field="authenticated-origin" subfield="host">
     <address subdomain-of="annoying.com">
      <!-- Don't accept calls from this source -->
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="Denied by policy"/>
     </address>
     <not-present>
      <!-- Don't accept calls from unauthenticated sources -->
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="Denied by policy"/>
     </not-present>
     <otherwise>
      <!-- All other calls allowed -->
      <proxy/>
     </otherwise>
    </address-switch>
   </address>
  </address-switch>
 </taa:routed>
</cpl>
```

CPL Example: Allow Calls From Locally Registered Endpoints Only

Note In this example, the administrator only wants to allow calls that originate from locally registered endpoints.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
 xmlns:taa="http://www.tandberg.net/cpl-extensions"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <address-switch field="registered-origin">
   <not-present>
    <reject status="403" reason="Only local endpoints can use this Expressway"/>
   </not-present>
  </address-switch>
 </taa:routed>
</cpl>
```

CPL Example: Block Calls From Default Zone and Default Subzone

Note You can configure this behavior using Call Policy Rules, so you don't need to do it using a CPL script. However, you cannot use a combination of UI configured rules and uploaded CPL script, so if you have any CPL requirements that you cannot implement using the UI rules, you must use a script for all of your rules. See About Call Policy.

The script to *allow calls from locally registered endpoints* only can be extended to also allow calls from configured zones but not from the Default Zone or Default Subzone.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
 xmlns:taa="http://www.tandberg.net/cpl-extensions"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <address-switch field="registered-origin">
   <not-present>
    <address-switch field="originating-zone">
     <address is="DefaultZone">
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="Denied by policy"/>
     </address>
     <address is="DefaultSubZone">
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="Denied by policy"/>
     </address>
     <otherwise>
      <proxy/>
     </otherwise>
    </address-switch>
   </not-present>
  </address-switch>
 </taa:routed>
</cpl>
```

CPL Example: Restricting Access to a Local Gateway

Note You can configure this behavior using Call Policy Rules, so you don't need to do it using a CPL script. However, you cannot use a combination of UI configured rules and uploaded CPL script, so if you have any CPL requirements that you cannot implement using the UI rules, you must use a script for all of your rules. See About Call Policy.

In these examples, a gateway is registered to the Expressway with a prefix of 9 and the administrator wants to stop calls from outside the organization being routed through it.

This can be done in two ways: using the `address-switch` node or the `taa:rule-switch` node. Examples of each are shown below.

Note You can achieve the same result with Call Routing on Cisco Unified Communications Manager. This example is here because you may want to prevent these types of calls from getting any deeper into the network.

Using the Address-Switch Node:

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
 xmlns:taa="http://www.tandberg.net/cpl-extensions"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <address-switch field="destination">
   <address regex="9(.*)">
    <address-switch field="originating-zone">
```

```
    <!-- Calls coming from the traversal zone are not allowed to use this gateway -->
    <address is="TraversalZone">
     <!-- Reject call with a status code of 403 (Forbidden) -->
     <reject status="403" reason="Denied by policy"/>
    </address>
   </address-switch>
  </address>
 </address-switch>
</taa:routed>
</cpl>
```

Using the Taa:Rule-Switch Node

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
 xmlns:taa="http://www.tandberg.net/cpl-extensions"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
 <taa:routed>
  <taa:rule-switch>
   <taa:rule originating-zone="TraversalZone" destination="9(.*)">
    <!-- Calls coming from the traversal zone are not allowed to use this gateway -->
    <!-- Reject call with a status code of 403 (Forbidden) -->
    <reject status="403" reason="Denied by policy"/>
   </taa:rule>
   <taa:rule origin="(.*)" destination="(.*)">
    <!-- All other calls allowed -->
    <proxy/>
   </taa:rule>
  </taa:rule-switch>
 </taa:routed>
</cpl>
```

LDAP Server Configuration for Device Authentication

The Expressway can be configured to authenticate devices against an H.350 directory service on an LDAP server.

This section describes how to:

- Downloading the H.350 Schemas that must be installed on the LDAP server
- Install and configure two common types of LDAP servers for use with the Expressway:
  - Configuring a Microsoft Active Directory LDAP Server
  - Configuring an OpenLDAP Server

Downloading the H.350 Schemas

The following ITU specifications describe the schemas which are required to be installed on the LDAP server:

H.350	Directory services architecture for multimedia conferencing - an LDAP schema to represent endpoints on the network.
H.350.1	Directory services architecture for H.323 - an LDAP schema to represent H.323 endpoints.

H.350.2	Directory services architecture for H.235 - an LDAP schema to represent H.235 elements.
H.350.4	Directory services architecture for SIP - an LDAP schema to represent SIP endpoints.

The schemas can be downloaded from the web interface on the Expressway. To do this:

1. Go to **Configuration** > **Authentication** > **Devices** > **H.350 directory schemas**. You are presented with a list of downloadable schemas.
2. Click on the **Download** button next to each file to open it.
3. Use your browser's **Save As** command to store it on your file system.

Configuring a Microsoft Active Directory LDAP Server

Prerequisites

These instructions assume that Active Directory has already been installed. For details on installing Active Directory please consult your Windows documentation.

The following instructions are for Windows Server 2003 Enterprise Edition. If you are not using this version of Windows, your instructions may vary.

Installing the H.350 Schemas

After you have Downloading the H.350 Schemas, install them as follows:

Open an elevated command prompt by right-clicking Command Prompt and selecting 'Run as administrator'. For each file execute the following command:

```
ldifde -i -c DC=X <ldap_base> -f filename.ldf
```

where:

`<ldap_base>` is the base DN for your Active Directory server.

Adding H.350 Objects

Create the organizational hierarchy:

1. Open up the Active Directory **Users and Computers** MMC snap-in.
2. Under your BaseDN right-click and select **New Organizational Unit**.
3. Create an Organizational unit called *h350*.

It is good practice to keep the H.350 directory in its own organizational unit to separate out H.350 objects from other types of objects. This allows access controls to be setup which only allow the Expressway read access to the BaseDN and therefore limit access to other sections of the directory.

Add the H.350 objects:

1. Create an ldif file with the following contents:

```
# MeetingRoom1 endpoint
dn: commUniqueId=comm1,ou=h350,DC=X
objectClass: commObject
objectClass: h323Identity
objectClass: h235Identity
objectClass: SIPIdentity
commUniqueId: comm1
h323Identityh323-ID: MeetingRoom1
h323IdentitydialedDigits: 626262
h235IdentityEndpointID: meetingroom1
h235IdentityPassword: mypassword
SIPIdentityUserName: meetingroom1
SIPIdentityPassword: mypassword
SIPIdentitySIPURI: sip:MeetingRoom@X
```

2. Add the ldif file to the server using the command:

   ```
   ldifde -i -c DC=X <ldap_base> -f filename.ldf
   ```

   where:

   `<ldap_base>` is the base DN of your Active Directory Server.

The example above will add a single endpoint with an H.323 ID alias of `MeetingRoom1`, an E.164 alias of `626262` and a SIP URI of `MeetingRoom@X`. The entry also has H.235 and SIP credentials of ID `meetingroom1` and password `mypassword` which are used during authentication.

H.323 registrations will look for the H.323 and H.235 attributes; SIP will look for the SIP attributes. Therefore if your endpoint is registering with just one protocol you do not need to include elements relating to the other.

Note The SIP URI in the `ldif` file must be prefixed by `sip:`.

For information about what happens when an alias is not in the LDAP database, see *Source of aliases for registration* in the Device authentication using LDAP section.

Securing with TLS

To enable Active Directory to use TLS, you must request and install a certificate on the Active Directory server. The certificate must meet the following requirements:

- Be located in the Local Computer's Personal certificate store. This can be seen using the Certificates MMC snap-in.
- Have the private details on how to obtain a key associated for use with it stored locally. When viewing the certificate you should see a message saying "You have a private key that corresponds to this certificate".
- Have a private key that does not have strong private key protection enabled. This is an attribute that can be added to a key request.
- The Enhanced Key Usage extension includes the Server Authentication object identifier, again this forms part of the key request.
- Issued by a CA that both the domain controller and the client trust.
- Include the Active Directory fully qualified domain name of the domain controller in the common name in the subject field and/or the DNS entry in the subject alternative name extension.

To configure the Expressway to use TLS on the connection to the LDAP server you must upload the CA's certificate as a trusted CA certificate. This can be done on the Expressway by going to: **Maintenance** > **Security** > **Trusted CA certificate**.

Configuring an OpenLDAP Server

Prerequisites

These instructions assume that an OpenLDAP server has already been installed. For details on installing OpenLDAP see the documentation at http://www.openldap.org.

The following examples use a standard OpenLDAP installation on the Linux platform. For installations on other platforms the location of the OpenLDAP configuration files may be different. See the OpenLDAP installation documentation for details.

Installing the H.350 Schemas

1. Download all the schema files from the Expressway (**Configuration** > **Authentication** > **Devices** > **LDAP schemas**). Ensure that all characters in the filename are in lowercase and name each file with a .schema extension. Hence:

   commobject.schema

   h323identity.schema

   h235identity.schema

   sipidentity.schema

2. Determine the index of each schema file via slapcat. For example, for **commobject.schema**:

   ```
   sudo slapcat -f schema_convert.conf -F ldif_output -n 0 | grep commobject,cn=schema
   ```

   will return something similar to: `dn: cn={14}commobject,cn=schema,cn=config`

   The index value inside the curly brackets {} will vary.

3. Convert each schema file into ldif format via `slapcat`. Use the index value returned by the previous command. For example, for **commobject.schema**:

   ```
   slapcat -f schema_convert.conf -F ldif_output -n0 -H
   ldap:///cn={14}commobject,cn=schema,cn=config -l cn=commobject.ldif
   ```

4. Use a text editor to edit the newly created file (**cn=commobject.ldif** in the case of the commobject file) and remove the following lines:

   ```
   structuralObjectClass:
   entryUUID:
   creatorsName:
   createTimestamp:
   entryCSN:
   modifiersName:
   modifyTimestamp:
   ```

5. Add each schema to the ldap database via `ldapadd`. For example, for **cn=commobject.ldif**:

   ```
   sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f cn\=commobject.ldif
   ```

   (the backslash after `cn` is an escape character)

6. Repeat these steps for every schema file.

More information is available at https://help.ubuntu.com/13.04/serverguide/openldap-server.html.

Adding H.350 Objects

Create the organizational hierarchy:

1. Create an `ldif` file with the following contents:

```
# This example creates a single organizational unit to contain the H.350 objects
dn: ou=h350,dc=my-domain,dc=com
objectClass: organizationalUnit
ou: h350
```

2. Add the ldif file to the server via `slapadd` using the format:

```
slapadd -l <ldif_file>
```

This organizational unit will form the BaseDN to which the Expressway will issue searches. In this example the BaseDN will be: `ou=h350,dc=my-domain,dc=com`.

It is good practice to keep the H.350 directory in its own organizational unit to separate out H.350 objects from other types of objects. This allows access controls to be setup which only allow the Expressway read access to the BaseDN and therefore limit access to other sections of the directory.

Note The SIP URI in the `ldif` file must be prefixed by `sip:`

Add the H.350 objects:

1. Create an ldif file with the following contents:

```
# MeetingRoom1 endpoint
dn: commUniqueId=comm1,ou=h350,dc=mydomain,dc=com
objectClass: commObject
objectClass: h323Identity
objectClass: h235Identity
objectClass: SIPIdentity
commUniqueId: comm1
h323Identityh323-ID: MeetingRoom1
h323IdentitydialedDigits: 626262
h235IdentityEndpointID: meetingroom1
h235IdentityPassword: mypassword
SIPIdentityUserName: meetingroom1
SIPIdentityPassword: mypassword
SIPIdentitySIPURI: sip:MeetingRoom@domain.com
```

2. Add the ldif file to the server via `slapadd` using the format:

```
slapadd -l <ldif_file>
```

The example above will add a single endpoint with an H.323 ID alias of `MeetingRoom1`, an E.164 alias of `626262` and a SIP URI of `MeetingRoom@domain.com`. The entry also has H.235 and SIP credentials of ID `meetingroom1` and password `mypassword` which are used during authentication.

H.323 registrations will look for the H.323 and H.235 attributes; SIP will look for the SIP attributes. Therefore if your endpoint is registering with just one protocol you do not need to include elements relating to the other.

For information about what happens when an alias is not in the LDAP database see *Source of aliases for registration* in the Device authentication using LDAP section.

Securing with TLS

The connection to the LDAP server can be encrypted by enabling Transport Level Security (TLS) on the connection. To do this you must create an X.509 certificate for the LDAP server to allow the Expressway to verify the server's identity. After the certificate has been created you will need to install the following three files associated with the certificate onto the LDAP server:

- The certificate for the LDAP server
- The private key for the LDAP server
- The certificate of the Certificate Authority (CA) that was used to sign the LDAP server's certificate

All three files should be in PEM file format.

The LDAP server must be configured to use the certificate. To do this:

- Edit /etc/openldap/slapd.conf and add the following three lines:

```
TLSCACertificateFile <path to CA certificate>
TLSCertificateFile <path to LDAP server certificate>
TLSCertificateKeyFile <path to LDAP private key>
```

The OpenLDAP daemon (`slapd`) must be restarted for the TLS settings to take effect.

To configure the Expressway to use TLS on the connection to the LDAP server you must upload the CA's certificate as a trusted CA certificate. This can be done on the Expressway by going to: **Maintenance** > **Security** > **Trusted CA certificate**.

Using the Collaboration Solutions Analyzer Tool

The *Collaboration Solutions Analyzer* is created by Cisco Technical Assistance Center (TAC) to help you with validating your deployment, and to assist with troubleshooting by analyzing Expressway log files. For example, you can use the Business to Business Call Tester to validate and test calls, including Microsoft interworked calls.

You need a customer or partner account to use the Collaboration Solutions Analyzer.

Getting started

1. If you plan to use the log analysis tool, first collect the Expressway logs.
2. Sign in to https://cway.cisco.com/tools/CollaborationSolutionsAnalyzer/

   From X12.6 you can use the **Analyze log** button on the **Diagnostic logging** page (**Maintenance** > **Diagnostics**) to open a link to the Collaboration Solutions Analyzer troubleshooting tool.
3. Click the tool you want to use. For example, to work with logs:
   a. Click **Log analysis**.
   b. Upload the log file(s).
   c. Select the files you want to analyze.

d. Click **Run analysis**.

The tool analyzes the log files and displays the information in a format which is much easier to understand than the raw logs. For example, you can generate ladder diagrams to show SIP calls.

Changing the Default SSH Key

Using the default key means that SSH sessions established to the Expressway may be vulnerable to "man-in-the-middle" attacks, so we recommend that you generate new SSH keys that are unique to your Expressway.

An alarm message "Security alert: the SSH service is using the default key" is displayed if your Expressway is still configured with its factory default SSH key.

To generate a new SSH key for the Expressway:

1. Log into the CLI as *root*.
2. Type `regeneratesshkey`.
3. Type `exit` to log out of the root account.
4. Log in to the web interface.
5. Go to **Maintenance** > **Restart**. You are taken to the **Restart** page.
6. Check the number of calls and registrations currently in place.
7. Click **Restart system** and then confirm the restart when asked.

If you have a clustered Expressway system you must generate new SSH keys for every cluster peer. Log into each peer in turn and follow the instructions above. You do not have to decluster or disable replication.

When you next log in to the Expressway over SSH you may receive a warning that the key identity of the Expressway has changed. Please follow the appropriate process for your SSH client to suppress this warning.

If your Expressway is subsequently downgraded to an earlier version of Expressway firmware, the default SSH keys will be restored.

Restoring the Default Configuration (Factory Reset)

Rarely, it may be necessary to run the "factory-reset" script on your system. This reinstalls the software image and resets the configuration to the default, functional minimum.

Before You Begin

If you've upgraded since the system was first set up, be aware that the reset reinstalls your latest software version.

The factory reset procedure is intended for system recovery after a serious failure. **It is NOT designed as a security mechanism to erase information from physical storage.** Do not rely on a reset to return the system

to a “clean” or “blank” secure state. The reset is intended just to return the system to a minimum configuration state.

The system uses the default configuration values that currently apply in the software version installed by the reset. These may differ from your previously configured values, especially if the system has been upgraded from an older version. In particular this may affect port settings, such as multiplexed media ports. After restoring the default configuration you may want to reset those port settings to match the expected behavior of your firewall. (As described below, optionally it's possible to retain a few configuration values like option keys, SSH keys, and FIPS140 mode, but we recommend that you reset all these values.)

Prerequisites

- As the virtual machine console is required to complete this process, **you need appropriate VMware access in order to open the VM console**.
- The factory reset procedure described below rebuilds the system based on the most recent successfully installed software image. The following two files stored in the **/mnt/harddisk/factory-reset/** system folder, are used for the reinstallation. In some cases these files are not present on the system (most commonly with a fresh VM installation that has not been upgraded). If so, you must first put the files in place using SCP as root.
  - A text file containing just the 16-character Release Key, named *rk*
  - A file containing the software image in tar.gz format, named *tandberg-image.tar.gz*. You need to manually rename the downloaded version-specific tar file to *tandberg-image.tar.gz*.

Process to Reset to the Default Configuration

You must do this procedure from the console (or for hardware-based CE appliances you can optionally use a direct connection to the appliance with a keyboard and monitor). Because the network settings are rewritten, all calls and any SSH session used to initiate the reset will be dropped and you won't be able to see the procedure output.

The process takes approximately 20 minutes.

1. Log in to the system as **root**.
2. Type `factory-reset`.
3. Answer the questions as required. The recommended responses will reset the system completely to a factory default state:

Prompt	Recommended response
Keep option keys [YES/NO]?	NO
Keep FIPS140 configuration [YES/NO]?	NO
Keep IP configuration [YES/NO]?	NO
Keep ssh keys [YES/NO]?	NO

Prompt	Recommended response
Keep server certificate, associated key and CA trust store [YES/NO]? This option does *not* preserve SNI / domain certificates, which are always deleted regardless of what you respond. Only the server certificate and associated key and CA trust store are saved (if you respond YES).	NO
Keep root and admin passwords [YES/NO]?	NO
Save log files [YES/NO]?	NO

4. Confirm that you want to proceed.
5. After the VM boots, you are taken to the Install Wizard. You must complete the wizard through the VM console. Some of the questions in the wizard may be skipped depending on your responses in step 3, but even if you preserved the IP configuration and password, you still need to complete the Install Wizard through the VM console.

Note If you were using FIPS140 and you want to enable it again, see the section in this guide about configuring FIPS140-2 cryptographic mode.

Resetting via USB Stick - CE Hardware Appliances

This section does not apply to virtualized, VM-based Expressways.

Cisco TAC may suggest an alternative reset method, to download the software image onto a USB stick and then reboot the system with the USB stick plugged in.

If you use this method you must clear down and rebuild the USB stick after use. Do not reset one system and then take the USB stick and re-use it on another system.

Note Reset functionality comes built in with the CE hardware appliances, through the Internal Recovery Partition (IRP). See the *CEnnnn Appliance Installation Guide* on the Install and Upgrade Guides page for more information.

Pattern Matching Variables

The Expressway makes use of pattern matching in a number of its features, namely Allow Lists and Deny Lists, pre-search transforms and when configuring search rules and zone transforms.

For each of these pattern matches, the Expressway allows you to use a variable that it will replace with the current configuration values before the pattern is checked.

These variables can be used as either or both of:

- all or part of the pattern that is being searched for
- all or part of the string that is replacing the pattern that was found

The variables can be used in all types of patterns (*Prefix*, *Suffix*, *Regex*, and *Exact*).

The table below shows the strings that are valid as variables, and the values they represent.

String	Represents value returned by...	When used in a Pattern field	When used in a Replace field
%ip%	xConfiguration Ethernet 1 IP V4 Address xConfiguration Ethernet 1 IP V6 Address xConfiguration Ethernet 2 IP V4 Address xConfiguration Ethernet 2 IP V6 Address	Matches all IPv4 and IPv6 addresses. Applies to all peer addresses if the Expressway is part of a cluster.	not applicable
%ipv4%	xConfiguration Ethernet 1 IP V4 Address xConfiguration Ethernet 2 IP V4 Address	Matches the IPv4 addresses currently configured for LAN 1 and LAN 2. Applies to all peer addresses if the Expressway is part of a cluster.	not applicable
%ipv4_1%	xConfiguration Ethernet 1 IP V4 Address	Matches the IPv4 address currently configured for LAN 1. Applies to all peer addresses if the Expressway is part of a cluster.	Replaces the string with the LAN 1 IPv4 address. If the Expressway is part of a cluster, the address of the local peer is always used.
%ipv4_2%	xConfiguration Ethernet 2 IP V4 Address	Matches the IPv4 address currently configured for LAN 2. Applies to all peer addresses if the Expressway is part of a cluster.	Replaces the string with the LAN 2 IPv4 address. If the Expressway is part of a cluster, the address of the local peer is always used.

String	Represents value returned by...	When used in a Pattern field	When used in a Replace field
%ipv6%	xConfiguration Ethernet 1 IP V6 Address xConfiguration Ethernet 2 IP V6 Address	Matches the IPv6 addresses currently configured for LAN 1 and LAN 2. Applies to all peer addresses if the Expressway is part of a cluster.	not applicable
%ipv6_1%	xConfiguration Ethernet 1 IP V6 Address	Matches the IPv6 address currently configured for LAN 1. Applies to all peer addresses if the Expressway is part of a cluster.	Replaces the string with the LAN 1 IPv6 address. If the Expressway is part of a cluster, the address of the local peer is always used.
%ipv6_2%	xConfiguration Ethernet 2 IP V6 Address	Matches the IPv6 address currently configured for LAN 2. Applies to all peer addresses if the Expressway is part of a cluster.	Replaces the string with the LAN 2 IPv6 address. If the Expressway is part of a cluster, the address of the local peer is always used.
%systemname%	xConfiguration SystemUnit Name	Matches the Expressway's System Name.	Replaces the string with the Expressway's System Name.

You can test whether a pattern matches a particular alias and is transformed in the expected way by using the Check pattern tool (**Maintenance** > **Tools** > **Check pattern**).

Port Reference

See the *Cisco Expressway IP Port Usage Configuration Guide*, for your version, on the Cisco Expressway Series configuration guides page.

Regular Expressions

Regular expressions can be used in conjunction with a number of Expressway features such as alias transformations, zone transformations, CPL policy and ENUM. The Expressway uses POSIX format regular expression syntax. The table below provides a list of commonly used special characters in regular expression syntax. This is only a subset of the full range of expressions available. For a detailed description of regular expression syntax see the publication *Regular Expression Pocket Reference*.

Character	Description	Example
.	Matches any single character.	
\d	Matches any decimal digit, i.e. 0-9.	
*	Matches 0 or more repetitions of the previous character or expression.	.* matches against any sequence of characters
+	Matches 1 or more repetitions of the previous character or expression.	
?	Matches 0 or 1 repetitions of the previous character or expression.	`9?123` matches against 9123 and 123
{n}	Matches n repetitions of the previous character or expression	`\d{3}` matches 3 digits
{n,m}	Matches n to m repetitions of the previous character or expression	`\d{3,5}` matches 3, 4 or 5 digits
[...]	Matches a set of specified characters. Each character in the set can be specified individually, or a range can be specified by giving the first character in the range followed by the - character and then the last character in the range. You cannot use special characters within the [] - they will be taken literally.	`[a-z]` matches any alphabetical character `[0-9#*]` matches against any single E.164 character - the E.164 character set is made up of the digits 0-9 plus the hash key (#) and the asterisk key (*)
[^...]	Matches anything except the set of specified characters. Each character in the set can be specified individually, or a range can be specified by giving the first character in the range followed by the - character and then the last character in the range. You cannot use special characters within the [] - they will be taken literally.	`[^a-z]` matches any non-alphabetical character `[^0-9#*]` matches anything other than the digits 0-9, the hash key (#) and the asterisk key (*)

Character	Description	Example
(...)	Groups a set of matching characters together. Groups can then be referenced in order using the characters \1, \2, etc. as part of a replace string.	A regular expression can be constructed to transform a URI containing a user's full name to a URI based on their initials. The regular expression `(.).*_(.).*(@example.com)` would match against the user `john_smith@example.com` and with a replace string of `\1\2\3` would transform it to `js@example.com`
|	Matches against one expression or an alternate expression.	`.*@example.(net|com)` matches against any URI for the domain `example.com` or the domain `example.net`
\	Escapes a regular expression special character.	
^	Signifies the start of a line. When used immediately after an opening brace, negates the character set inside the brace.	`[^abc]` matches any single character that is NOT one of a, b or c
$	Signifies the end of a line.	`^\d\d\d$` matches any string that is exactly 3 digits long
(?!...)	Negative lookahead. Defines a subexpression that must not be present.	`(?!.*@example.com$).*` matches any string that does not end with `@example.com` `(?!alice).*` matches any string that does not start with `alice`
(?<!...)	Negative lookbehind. Defines a subexpression that must not be present.	`.*(?<!net)` matches any string that does not end with `net`

Note that regex comparisons are not case sensitive.

For an example of regular expression usage, see the CPL Examples section.

Supported Characters

The Expressway supports the following characters when entering text in the CLI and web interface:

- the letters A-Z and a-z
- decimal digits (0-9)
- underscore (_)

- minus sign / hyphen (-)
- equals sign (=)
- plus sign (+)
- at sign (@)
- comma (,)
- period/full stop (.)
- exclamation mark (!)
- spaces

The following characters are specifically not allowed:

- tabs
- angle brackets (< and >)
- ampersand (&)
- caret (^)

Note that some specific text fields (including Administrator groups) have different restrictions and these are noted in the relevant sections of this guide.

Case sensitivity

Text items entered through the CLI and web interface are case insensitive. The only exceptions are passwords and local administrator account names which are case sensitive.

Product Identifiers and Corresponding Keys

Cisco PIDs (Product Identifiers) are also sometimes known as a product name, model name, or product number. These are examples of PIDs that can apply to Expressway, depending on the software version. Many have been phased out in later software versions - for example, a Release Key is no longer used from X12.5.4 for Cisco Expressway products.

Feature or License Option	PID (Product Identifier)	Key Pattern	Valid On	Required For
Release Key	`LIC-SW-VMVCS-K9`	16 digit number	VCS Control VCS Expressway	Enabling the system. The key is unique to a serial number and a particular base version of software. Most features will not work permanently without this key.

Feature or License Option	PID (Product Identifier)	Key Pattern	Valid On	Required For
Release Key	LIC-SW-EXP-K9	16 digit number	Expressway-C Expressway-E	Enabling the system. The key is unique to a serial number and a particular base version of software. Most features will not work permanently without this key.
Expressway Series	LIC-EXP-SERIES	116341E00-m-########	Expressway-C Expressway-E	Enabling an Expressway Series system (for anything except Cisco Webex Hybrid Services)

Feature or License Option	PID (Product Identifier)	Key Pattern	Valid On	Required For
Rich Media Session licenses	LIC-EXP-RMS	116341Yn-m-#########	Expressway-C Expressway-E	Calls enabled by Expressway where the Expressway must process the media streams (also known as 'traverse' or 'handle' the media). RMS licenses are used by calls that require: • IPv4-IPv6 interworking • H.323-SIP interworking • Media encryption on behalf of another entity • Microsoft SIP to standards-based SIP interworking **Note:** If both endpoints are registered to the Cisco infrastructure RMS license is not required. RMS licenses are not used by CMR Cloud calls

Feature or License Option	PID (Product Identifier)	Key Pattern	Valid On	Required For
Traversal call licenses	LIC-VCSE-n	116341Wn-m-########	VCS Control VCS Expressway	Calls enabled by VCS where the VCS must process the media streams (also known as 'traverse' or 'handle' the media). Traversal call licenses are used by calls that require: • IPv4-IPv6 interworking • H.323-SIP interworking • Media encryption on behalf of another entity • Microsoft SIP to standards-based SIP interworking Traversal call licenses are not used by CMR Cloud calls
Non-traversal call licenses	LIC-VCS-n	116341Vn-m-########	VCS Control VCS Expressway	Calls enabled by VCS that don't require media traversal (signaling only)
Registration licenses	LIC-VCS-nREG	116341Rn-m-########	VCS Control VCS Expressway	Registering callers to VCS
Room system registration licenses	LIC-EXP-ROOM	116341An-m-########	Expressway-C Expressway-E	Registering TelePresence rooms to Expressway-C.
Desktop system registration licenses	LIC-EXP-DSK	116341Bn-m-########	Expressway-C Expressway-E	Registering desktop endpoints to Expressway-C.

Feature or License Option	PID (Product Identifier)	Key Pattern	Valid On	Required For
TURN relay licenses	LIC-EXP-TURN	116341In-m-########	VCS Expressway Expressway-E	Jabber Guest, Microsoft Interoperability (offsite MS clients)
Traversal Server feature (not used in X12.6 and later)	LIC-EXP-E	116341T00-m-########	VCS Expressway Expressway-E	Firewall traversal: MRA, B2B, CMR Cloud, CMR Hybrid, Proxy registrations, Jabber Guest, MS interop (offsite MS clients)
FindMe feature	LIC-VCS-FINDME	116341U00-m-########	VCS Control Expressway-C	Multiple aliases managed by Cisco TMS. This key is not explicitly required, but does not interfere with operation if loaded.
Interworking H.323 to SIP feature	LIC-EXP-GW	116341G00-m-########	VCS Control VCS Expressway Expressway-C Expressway-E	This key is not explicitly required, but does not interfere with operation if loaded.
Device Provisioning feature	LIC-VCS-DEVPROV	116341P00-m-########	VCS Control Expressway-C	Provisioning endpoints with configuration and phonebook data from Cisco TMS. This key is not explicitly required, but does not interfere with operation if loaded.
Advanced Networking feature	LIC-EXP-AN	116341L00-m-########	VCS Expressway Expressway-E	Enabling second NIC and static NAT. This key is not explicitly required, but does not interfere with operation if loaded.

Feature or License Option	PID (Product Identifier)	Key Pattern	Valid On	Required For
Advanced Account Security feature	LIC-VCS-JITC	116341J00-m-#########	VCS Control VCS Expressway	Enabling FIPS140-2 cryptographic mode (in highly secure environments) Enabling Advanced Account Security mode
Advanced Account Security feature	LIC-EXP-JITC=	116341J00-m-#########	Expressway-C Expressway-E	Enabling FIPS140-2 cryptographic mode (in highly secure environments) Enabling Advanced Account Security mode
Microsoft Interoperability	LIC-EXP-MSFT	116341C00-m-#########	VCS Control Expressway-C	All integration between Expressway and Microsoft infrastructure, including: A/V call interworking, desktop sharing from Microsoft clients, chat and presence federation with IM&P.

n - the number of licenses supplied with this key. If this position contains `00`, it means the key is for a feature, rather than a number of licenses.

m - the index of the key, usually 1.

- a hex digit.

Allow List Rules File Reference

You can define rules using a CSV file. This topic provides a reference to acceptable data for each rule argument, and demonstrates the format of the CSV rules.

Table 1: Allow List Rule Arguments

Argument index	Parameter name	Required/Optional	Sample value
0	Url	Required	`protocol://host[:port][/path]` Where: • protocol is `http` or `https` • host may be a DNS name or IP address • :port is optional, and may only be : followed by one number in the range 0-65535, eg. `:8443` If the port is not specified, then the Expressway uses the default port for the supplied protocol (80 or 443) • /path is optional and must conform to HTTP specification
1	Deployment	Optional	Name of the deployment that uses this rule. Required when you have more than one deployment, otherwise supply an empty argument.
2	HttpMethods	Optional	Comma-delimited list of HTTP methods, optionally in double-quotes, eg. `"GET,PUT"`
3	MatchType	Optional	`exact` or `prefix` . Default is `prefix`
4	Description	Optional	Text description of the rule. Enclose with double quotes if there are spaces.

Example CSV file

```
Url,Deployment,HttpMethods,MatchType,Description
https://myServer1:8443/myPath1,myDomain1,GET,,"First Rule"
```

```
http://myServer2:8000/myPath2,myDomain200,"GET,PUT",exact,
https://myServer3:8080/myPath3,myDomain1,,prefix,"Third Rule"
https://myServer4/myPath4,myDomain1,,prefix,"Fourth Rule"
http://myServer5/myPath5,myDomain1,,prefix,"Fifth Rule"
```

- List the parameter names (as shown) in the first line of the file
- One rule per line, one line per rule
- Separate arguments with commas
- Correctly order the rule values as shown in the table above
- Enclose values that have spaces in them with double quotes

Allow List Tests File Reference

You can define tests using a CSV file. This topic provides a reference to acceptable data for each test argument, and demonstrates the format of the CSV tests.

Table 2: Allow List Test Arguments

Argument index	Parameter name	Required/Optional	Sample value
0	Url	Required	`protocol://host[:port][/path]` Where: • protocol is `http` or `https` • host may be a DNS name or IP address • :port is optional, and may only be : followed by one number in the range 0-65535 • /path is optional and must conform to HTTP specification
1	ExpectedResult	Required	`allow` or `block`. Specifies whether the test expects that the rules should allow or block the specified URL.
2	Deployment	Optional	Name of the deployment to test with this URL. If you omit this argument, the test will use the default deployment.

Argument index	Parameter name	Required/Optional	Sample value
3	Description	Optional	Text description of the rule. Enclose with double quotes if there are spaces.
4	HttpMethod	Optional	Specify one HTTP method to test eg. `PUT`. Defaults to `GET` if not supplied.

Example CSV file

```
Url,ExpectedResult,Deployment,Description,HttpMethod
https://myServer1:8443/myPath1,block,"my deployment","a block test",GET
http://myServer2:8000/myPath2,allow,"my deployment","an allow test",PUT
https://myServer4/myPath4,allow,,,GET
http://myServer4/myPath4,block,,,POST
```

- List the parameter names (as shown) in the first line
- One test per line, one line per test
- Separate arguments with commas
- Correctly order the test values as shown in the table above
- Enclose values that have spaces in them with double quotes

Expressway Multitenancy Overview

The Expressway product line is used in Cisco Hosted Collaboration Solution to provide various edge access features including the following:

- Mobile and Remote Access (MRA) allows endpoints such as Cisco Jabber to have their registration, call control, provisioning, messaging, and presence services provided by Cisco Unified Communications Manager for endpoints outside the enterprise network. The Expressway provides secure firewall traversal and line-side support for Unified CM registrations.
- Business to Business (B2B) enables secure connectivity options that allow dialing to and from non-Cisco Hosted Collaboration Solution enterprises reachable through the Internet.
- Cisco Webex Hybrid Services links on-premises equipment with the Cisco Collaboration cloud for an integrated Cisco Webex experience.

Deploying these services requires a Cisco Expressway-E cluster and Expressway-C cluster to be set up and managed for each customer. For small customers, this can lead to inefficient utilization of resources and an extra management burden.

To help alleviate this overhead, a multitenant configuration can be deployed. This allows the partner to share the Expressway-E cluster across up to 50 customers while a dedicated Expressway-C cluster is deployed per customer.

This dedicated Expressway-C cluster can be used for all three services: MRA, B2B, and Hybrid. This configuration is intended to support small customers, up to around 500 users per customer.

For larger customers, we recommend using a single-tenant (dedicated) Expressway-E cluster to meet the customer's scale and performance requirements.

Multitenant Expressway Restrictions

Multitenant Expressway has some restrictions relative to the standard Expressway product. The following features are not supported in multi-tenant mode:

- Jabber Guest
- H323 in its various modes, including:
  - H323/SIP Interworking
  - Business-to-Business H323
  - H323 Gatekeeper
- Lync interop
- Skype for Business interop
- IPv6
- Cisco Meeting Server (CMS)

More Information

For detailed information about multitenancy, please refer to the following documents on the Cisco Hosted Collaboration Solution documentation page:

- Cisco Hosted Collaboration Solution Reference Network Design Guide
- Cisco Hosted Collaboration Customer Onboarding Guide
- Cisco Hosted Collaboration Solution Capacity Planning Guide
- Cisco Hosted Collaboration Solution Troubleshooting Guide

Multitenant Expressway Sizing

In previous Expressway releases, Expressway-E and Expressway-C cluster deployments are restricted to matching cluster and OVA sizes. The number of nodes in the Expressway-E cluster must match the number of nodes in the Expressway-C cluster. Each node must be the same OVA size in both clusters.

With the multitenant deployment option, that restriction is relaxed. The recommended deployment is a shared 6-node large OVA Expressway-E cluster, and dedicated 2-node medium OVA Expressway-C cluster per customer.

For customers who need more capacity than a 2-node medium OVA cluster affords, we recommend deploying a dedicated Expressway-E cluster to meet their requirements.

For overall sizing recommendations, refer to the Collaboration Solution Sizing Guidance chapter of the *Cisco Hosted Collaboration Solution Reference Network Design Guide*. In particular, the Expressway section of this chapter discusses the sizing and capacity of Expressway clusters.

In a multitenant deployment, the Expressway-E's capacity is shared across all of the customers, whereas the Expressway-C cluster's capacity is dedicated to the customer. The following tables provide the recommended capacity per customer. Note that the figures for video and audio-only calls are for either one or the other call type; not both.

Shared Expressway-E cluster sizing

Cluster size	Proxied MRA registrations	Video calls	Audio-only calls
6 nodes, large OVA N+2 arrangement so capacity is for 4 nodes, allowing 2 nodes to fail without loss of capacity	10,000	2,000	4,000
Per-customer maximum (for 50 customers)	200	40	80

Dedicated Expressway-C cluster sizing

Cluster size	Proxied MRA registrations	Video calls	Audio-only calls
2 nodes, medium OVA N+1 arrangement so capacity is a single node, allowing 1 node to fail without loss of capacity	2,500	100	200

In the above tables, the video calls and audio-only calls account for the total of MRA calls, B2B calls, and Hybrid calls. With the recommended 50-customer maximum per shared Expressway-E cluster, the maximum average concurrent MRA registrations per customer is 200, well below the Expressway-C cluster's capacity.

Likewise, the maximum average concurrent video calls per customer is 40, again below the capacity of the Expressway-C cluster. This spare capacity in the Expressway-C cluster is used by the co-resident Hybrid connectors without impacting the proxied registration or call capacity.

There are two use cases to consider when planning the size of customers that are sharing the Expressway-E. In both of these use cases, the Expressway-E cluster is the limiting factor; there is plenty of capacity in the Expressway-C.

Use Case 1

Most customers are using MPLS for in-office connectivity and only using MRA at home or when mobile. In this case, only a small percentage (10-20%) of users are registered with MRA at any given time. Maximum users per customer should be around 500.

Use Case 2

Most customers are not using MPLS and are using MRA for all connectivity. In this case, 100% of users are registered with MRA. Maximum users per customer must not exceed 200.

The following table summarizes these deployment options.

Table 3: Deployment scenarios

Use case	Average maximum users per customer	Percentage of users that can register via MRA at once	Notes
1	500	40%	Use this when most customers are using MPLS for in-office connectivity.
2	200	100%	Use this when most customers are using MRA for in-office connectivity.

See *Multitenancy with Cisco Expressway* on the Cisco Hosted Collaboration Solution page.

Alarms Reference

These tables list the alarms that can be raised on the Expressway:

- Table 4: Hardware Alarms
- Table 5: Software Alarms
- Table 6: Cluster Alarms
- Table 7: Network Alarms
- Table 8: License Alarms
- Table 9: External Applications / Services Alarms
- Table 10: Security Alarms
- Table 11: Misconfiguration Alarms
- Table 12: Back to Back User Agent Alarms
- Table 13: Management Connector Alarms
- Table 14: Calendar Connector Alarms
- Table 15: Call Connector Alarms
- Table 16: Significant Event Alarms
- Table 17: Telemetry Alarms

Table 4: Hardware Alarms

ID	Title	Description	Solution	Severity
10001	Hardware failure	Raised when the following hardware issues occur: • Fan speed below the threshold. • System temperature higher than the threshold. • System input voltage below the threshold. • System input voltage higher than the threshold.	Follow your Cisco RMA process to obtain replacement parts. For information about how to replace server components, see *Cisco UCS C220 M4 Server Installation and Service Guide* on the Cisco UCS C220 M4 Rack Server page.	Critical
10002	RAID degraded	<problem description>	Follow your Cisco RMA process to obtain replacement parts. For information about how to replace server components, see *Cisco UCS C220 M4 Server Installation and Service Guide* on the Cisco UCS C220 M4 Rack Server page.	Critical

ID	Title	Description	Solution	Severity
10003	PSU redundancy lost	<problem description>	Follow your Cisco RMA process to obtain replacement parts. For information about how to replace server components, see *Cisco UCS C220 M4 Server Installation and Service Guide* on the Cisco UCS C220 M4 Rack Server page.	Critical
10004	RAID rebuilding	<problem description>	Wait for the rebuild to complete. On successful completion, all RAID-related alarms will be automatically lowered.	Critical
10005	Unsuitable hardware warning	Your current hardware does not meet supported VM configuration requirements for this version of Expressway.	Contact your Cisco representative for an upgrade to a supported hardware version. For information on supported versions, refer to *Cisco Expressway on Virtual Machine Installation Guide* on Expressway Install Guides page.	Warning

Table 5: Software Alarms

ID	Title	Description	Solution	Severity
15004	Application failed	An unexpected software error was detected in <module>	View the incident reporting page	Error

ID	Title	Description	Solution	Severity
15005	Database failure	Please remove database and restore from backup, then reboot the system	Reboot the system	Warning
15006	Restart required	A language pack has been installed, however a restart is required for this to take effect	Restart the system	Warning
15007	The system is busy	The system is shutting down, or starting		Alert
15008	Failed to load database	The database failed to load; some configuration data has been lost	Restore system data from backup	Warning
15009	Factory reset started	Factory reset started		Alert
15010	Application failed	An unexpected software error was detected in <module>	View the incident reporting page	Error
15011	Application failed	An unexpected software error was detected in <module>	View the incident reporting page	Error
15012	Language pack mismatch	Some text labels may not be translated	Contact your Cisco representative to see if an up-to-date language pack is available	Warning
15013	Factory reset failed	Factory reset failed		Alert
15014	Restart required	Core dump mode has been changed however, a restart is required for this to take effect	Restart the system	Warning
15015	Maintenance mode	The Expressway is in maintenance mode and will no longer accept calls and registrations		Warning

ID	Title	Description	Solution	Severity
15016	Directory service database failure	The directory service database is not running	Restart the system	Warning
15017	Application failed	The OpenDS service has stopped unexpectedly and has been restarted	If the problem persists, contact your Cisco representative	Warning
15018	Boot selection mismatch	Booted system does not match expected configuration; this may be caused by user input or spurious characters on the serial console during the boot	Reboot the system	Critical
15019	Application failed	An unexpected software error was detected in <details>	Restart the system; if the problem persists, contact your Cisco support representative	Critical
15021	Delayed Cisco XCP Router restart	The Cisco XCP Router service is currently not running on the latest configuration as the delayed Cisco XCP Router restart feature is enabled.	Restart the router on the Delayed Cisco XCP Router restart page or set it to restart at a scheduled time	Warning
15022	Restart required	Domain certificate configuration has been changed, however a restart is required for this to take effect.	Restart the system	Warning
15023	Restore failed	Backup was not restored. The system is restored onto the previous configuration.	Check the error log for more information and retry the operation; if the problem persists, contact your Cisco support representative	Error

ID	Title	Description	Solution	Severity
15024	Crypto device failure	A failure was detected while testing encrypt/decrypt cycle with the configured crypto device.	Please refer to the HSM configuration page for details	Critical
15025	HSM disenrollment failure	Disenrollment of peer to HSM failed.	Please refer to the HSM configuration page for details	Error
15026	HSM enrollment failure	Enrollment of peer to HSM failed.	Please refer to the HSM configuration page for details	Error
15027	HSM failure	An HSM failure needs administrator attention.	Please refer to the HSM configuration page for details	Critical
15028	Restart required	Server certificate and private key have been changed, however a restart is required for this to take effect.	Restart the Expressway to make this change effective	Warning
15029	Failed to send Crash Report	Failed to send Crash Report to the Server.	Check the network connectivity between Expressway and the Crash Reporting Server. Make sure the Crash Reporting Server certificate is not expired or revoked and the certificates in the CA chain were updated in the trust store.	

ID	Title	Description	Solution	Severity
15030	Unified CM data crosscheck failure	Unified CM configuration data on Expressway is inconsistent.	Please delete all Unified CM servers and then add them again. For details see the Mobile and Remote Access Through Cisco Expressway Deployment Guide, section “ Discover Unified CM Servers”	Error
15031	HSM TLP not installed	An HSM failure needs administrator attention.	Please refer to the Upgrade page for details.	Error
15032	Unified CM server unavailable	Unified CM configuration for publisher includes unavailable servers	See event log for further details. Correct the issue and refresh. For details see the Mobile and Remote Access Through Cisco Expressway Deployment Guide, section Discover Unified CM Servers.	Warning

Table 6: Cluster Alarms

ID	Title	Description	Solution	Severity
20020	Restart required	TLS verification configuration does not match active status.	Restart the system.	Warning
20021	Cluster communication failure	Unable to establish a TCP connection with <peers> on ports <ports>	Check the port reference guide.	Warning
20003	Invalid cluster configuration	The cluster configuration is invalid	Check the Clustering page and ensure that this system's IP address is included and there are no duplicate IP addresses	Warning

ID	Title	Description	Solution	Severity
20004	Cluster communication failure	The system is unable to communicate with one or more of the cluster peers	Check the clustering configuration	Warning
20005	Invalid peer address	One or more peer addresses are invalid	Check the Clustering page and ensure that all Peer fields use a valid IP address	Warning
20006	Cluster database communication failure	The database is unable to replicate with one or more of the cluster peers	Check the clustering configuration and restart	Warning
20007	Restart required	Cluster configuration has been changed, however a restart is required for this to take effect	Restart the system	Warning
20008	Cluster replication error	Automatic replication of configuration has been temporarily disabled because an upgrade is in progress	Please wait until the upgrade has completed	Warning
20009	Cluster replication error	There was an error during automatic replication of configuration	View cluster replication instructions	Warning
20011	Cluster replication error	This peer's configuration conflicts with the primary's configuration, manual synchronization of configuration is required	View cluster replication instructions	Warning

ID	Title	Description	Solution	Severity
20012	Cluster replication error	This peer's cluster configuration settings do not match the configuration primary peer's settings	Configure this peer's cluster settings	Warning
20014	Cluster replication error	Cannot find primary or this peer's configuration file, manual synchronization of configuration is required	View cluster replication instructions	Warning
20014	Cluster replication error	Cannot find primary or this subordinate's peer configuration file	Restart the node	Warning
20015	Cluster replication error	The local Expressway does not appear in the list of peers	Check the list of peers for this cluster	Warning
20016	Cluster replication error	The primary peer is unreachable	Check the list of peers for this cluster	Warning
20017	Cluster replication error	Configuration primary ID is inconsistent, manual synchronization of configuration is required	View cluster replication instructions	Warning
20018	Invalid clustering configuration	H.323 mode must be turned On - clustering uses H.323 communications between peers	Configure H.323 mode	Warning
20019	Cluster name not configured	If FindMe or clustering are in use a cluster name must be defined.	Configure the cluster name	Warning

ID	Title	Description	Solution	Severity
20024	Cluster configuration error	Cluster is in inconsistent state	View Cisco Expressway Cluster Creation and Maintenance Deployment Guide to recreate the cluster	Warning
20025	Failed to synchronize database	Database synchronization failed on node <nodename>, reboot node <nodename> from CLI Here, <nodename> is either the IP address or Fully Qualified Domain Name (FQDN)	Reboot the affected node from Command Line Interface (CLI)	Critical
20026	Failed to recover ClusterDB log server	ClusterDB log server is frozen and CDB log messages are not processed.	If the problem persists, contact your Cisco representative.	Critical

Table 7: Network Alarms

ID	Title	Description	Solution	Severity
25001	Restart required	Network configuration has been changed, however a restart is required for this to take effect	Restart the system	Warning
25002	Date and time not validated	The system is unable to obtain the correct time and date from an NTP server	Check the time configuration	Warning
25003	IP configuration mismatch	IP protocol is set to both IPv4 and IPv6, but the system does not have any IPv4 addresses defined	Configure IP settings	Warning

ID	Title	Description	Solution	Severity
25004	IP configuration mismatch	IP protocol is set to both IPv4 and IPv6, but the system does not have an IPv4 gateway defined	Configure IP settings	Warning
25006	Restart required	Advanced Networking option key has been changed, however a restart is required for this to take effect	Configure your required LAN and static NAT settings on the IP page and then restart the system.	Warning
25007	Restart required	QoS settings have been changed, however a restart is required for this to take effect	Restart the system	Warning
25008	Restart required	Port configuration has been changed, however a restart is required for this to take effect	Restart the system	Warning
25009	Restart required	Ethernet configuration has been changed, however a restart is required for this to take effect	Restart the system	Warning
25010	Restart required	IP configuration has been changed, however a restart is required for this to take effect	Restart the system	Warning
25011	Restart required	HTTPS service has been changed, however a restart is required for this to take effect	Restart the system	Warning
25013	IP configuration mismatch	IP protocol is set to both IPv4 and IPv6, but the system does not have an IPv6 gateway defined	Configure IP settings	Warning

ID	Title	Description	Solution	Severity
25014	Configuration warning	IP protocol is set to both IPv4 and IPv6, but the Expressway does not have any IPv6 addresses defined	Configure IP settings	Warning
25015	Restart required	SSH service has been changed, however a restart is required for this to take effect	Restart the system	Warning
25016	Ethernet speed not recommended	An Ethernet interface speed setting has been negotiated to a value other than 1000Mb/s full duplex or 100Mb/s full duplex; this may result in packet loss over your network	Configure Ethernet parameters	Warning
25017	Restart required	HTTP service has been changed, however a restart is required for this to take effect	Restart the system	Warning
25018	Port conflict	There is a port conflict between <function> <port> and <function> <port>	Review the port configuration on the Local inbound ports and Local outbound ports pages	Warning
25019	Verbose log levels configured	One or more modules of the Network Log or Support Log are set to a level of Debug or Trace	Network Log and Support Log modules should be set to a level of Info, unless advised otherwise by your Cisco support representative. If diagnostic logging is in progress they will be reset automatically when diagnostic logging is stopped	Warning

ID	Title	Description	Solution	Severity
25020	NTP client failure	The system is unable to run the NTP client	Check NTP status information, including any key configuration and expiry dates	Warning
25021	NTP server not available	The system is unable to contact an NTP server	Check Time configuration and status; check DNS configuration	Warning
25022	Time not synchronized over traversal zone	The system time of this server is different from that on a server on the other side of a SIP traversal zone	Ensure that your systems have consistent Time configuration; note that any changes may take some time to become effective	Warning
25023	XMPP Federation configuration warning	Failed to configure Unified CM IM and Presence Service servers with Expressway address for XMPP federation	Check that the IM and Presence Service servers are running, and that the AXL service is running on them, then refresh the servers.	Warning
25024	XMPP configuration error	Invalid configuration of XMPP network address	Check that the IPv4 addresses are correct. You may not use 127.0.0.1 (loopback address)	Error
25026	Restart required	Web administration port has been changed, however, a restart is required for this to take effect	Restart the system	Warning
25027	SSLH failure	The protocol multiplexing service cannot start because the configuration file was not written. The Expressway-E is not able to listen on TCP 443 for TURN and WebRTC requests.	Reconfigure the TURN service	Critical

ID	Title	Description	Solution	Severity
25028	HSM box connectivity issue	There is an issue with HSM modules	Please refer to the HSM configuration page for details	Alert
25029	Restart required	TURN Protocol Mode changed to UDP. Due to this, the TCP 443 TURN service has been turned OFF, however a restart is required for this to take effect	Restart the system	
25030	Reverse DNS Lookup failed	Failed to do reverse DNS Lookup for address <*IP Address of E server*>. This can cause MRA login to fail.	Ensure your DNS server is configured with valid PTR record for that address <*IP Address of E server*>.	Error
25031	Certificate verification failed	FQDN in PTR record for address <*IP Address of E server*> does not match with SAN entries presented in certificate of that Server with IP <*IP Address of E server*>.	Ensure a valid PTR record (only one) is created for address <*IP Address of E server*> with an FQDN which is present as a SAN entry in the Expressway-E's server certificate.	Error

Table 8: License Alarms

ID	Title	Description	Solution	Severity
30001	Capacity warning	The number of concurrent traversal calls has approached the licensed limit	Contact your Cisco representative	Warning
30002	Capacity warning	The number of concurrent traversal calls has approached the unit's physical limit	Contact your Cisco representative	Warning

ID	Title	Description	Solution	Severity
30003	Capacity warning	The number of concurrent non-traversal calls has approached the unit's physical limit	Contact your Cisco representative	Warning
30004	Capacity warning	The number of concurrent non-traversal calls has approached the licensed limit	Contact your Cisco representative	Warning
30005	Capacity warning	TURN relays usage has approached the unit's physical limit	Contact your Cisco representative	Warning
30007	Capacity warning	TURN relays usage has approached the licensed limit	Contact your Cisco representative	Warning
30009	TURN relays installed	TURN services are only available on Expressway-E; TURN option key ignored	Add/Remove opton keys	Warning
30010	Capacity warning	The number of concurrent registrations has approached the licensed limit	Contact your Cisco representative	Warning
30011	TURN relay licenses required	TURN services are enabled but no TURN relay license option keys are installed	Add option keys or disable TURN services	Warning
30012	License usage of lost cluster peer	Cluster peer <n> has been unavailable for more than <n> hours. Its licenses will be removed from the total available for use across the cluster on <date>.	Resolve the issue with this peer, or remove it from the cluster configuration	Warning

ID	Title	Description	Solution	Severity
30013	License usage of lost cluster peer	Several cluster peers have been unavailable for more than <n> hours. Their licenses will be removed from the total available for use across the cluster as follows: <details>.	Resolve the issue with this peer, or remove it from the cluster configuration	Warning
30014	License usage of lost cluster peer	Cluster peer <n> has been unavailable for more than <n> days. Its licenses will be removed from the total available for use across the cluster on <date>.	Resolve the issue with this peer, or remove it from the cluster configuration	Warning
30015	License usage of lost cluster peer	Several cluster peers have been unavailable for more than <n> days. Their licenses will be removed from the total available for use across the cluster as follows: <details>.	Resolve the issue with this peer, or remove it from the cluster configuration	Warning
30016	Licenses of lost cluster peer have been taken off the license pool	Cluster peer <n> has been unavailable for more than <n> days. Its licenses have been removed from the total available for use across the cluster on <date>.	Resolve the issue with this peer, or remove it from the cluster configuration	Warning
30017	Licenses of lost cluster peer have been taken off the license pool	Several cluster peers have been unavailable for more than <n> days. Their licenses have been removed from the total available for use across the cluster as follows: <details>.	Resolve the issue with this peer, or remove it from the cluster configuration	Warning

ID	Title	Description	Solution	Severity
30018	Provisioning licenses limit reached	The number of concurrently provisioned devices has reached the licensed limit	Provisioning limits are set by Cisco TMS; contact your Cisco representative if you require more licenses	Warning
30019	Call license limit reached	You have reached your license limit of <n> concurrent non-traversal call licenses	If the problem persists, contact your Cisco representative to buy more call licenses	Warning
30020	Call license limit reached	You have reached your license limit of <n> concurrent traversal call licenses	If the problem persists, contact your Cisco representative to buy more call licenses	Warning
30021	TURN relay license limit reached	You have reached your license limit of <n> concurrent TURN relay licenses	If the problem persists, contact your Cisco representative to buy more TURN relay licenses	Warning
30022	Call capacity limit reached	The number of concurrent non-traversal calls has reached the unit's physical limit	Add more capacity to your system; contact your Cisco representative	Warning
30023	Call capacity limit reached	The number of concurrent traversal calls has reached the unit's physical limit	Add more capacity to your system; contact your Cisco representative	Warning
30024	TURN relay capacity limit reached	The number of concurrent TURN relay calls has reached the unit's physical limit	Add more capacity to your system; contact your Cisco representative	Warning
30025	Restart required	An option key or the type has been changed, however a restart is required for this to take effect	Restart the system	Warning

ID	Title	Description	Solution	Severity
30026	Approaching room system license limit	The number of concurrent registered TelePresence room systems is approaching the license limit	Contact your Cisco representative if you require more licenses	Warning
30027	Capacity warning	The number of concurrent registered TelePresence room systems and registered desktop systems has reached the physical limit in one or more peer(s)	Ensure that your registrations are distributed evenly across all peers. Add more capacity to your system; contact your Cisco representative	Warning
30028	Room system registrations limit reached	The number of registered TelePresence room systems has reached the license limit	Contact your Cisco representative to buy more room system licenses	Warning
30029	Approaching desktop system license limit	The number of concurrent registered desktop systems is approaching the license limit	Contact your Cisco representative if you require more licenses	Warning
30030	Capacity warning	The number of registered TelePresence room systems and registered desktop systems has reached the unit's physical limit	Add more capacity to your system; contact your Cisco representative	Warning
30031	Desktop system license limit reached	The number of registered desktop systems has reached the license limit	Contact your Cisco representative to buy more desktop system licenses	Warning
30035	Smart license in Eval	The system is operating in Evaluation Mode that will expire in 30, 7, 3 , 2, 1 days	Register the system with Cisco Smart Software Manager or satellite	Warning

ID	Title	Description	Solution	Severity
30036	Smart license in overage out of compliance	The system is operating with an insufficient number of licenses	Configure additional licenses in Cisco Smart Software Manager	Alert
30037	Smart license no provision out of compliance	The system is operating with an insufficient number of licenses	Configure additional licenses in Cisco Smart Software Manager in order to restore the ability to provision users and devices	Critical
30038	Smart license no provision Eval expired	The license evaluation period has expired and the product is in enforced mode	Please check the network connection and renew the license authorization in order to restore the ability to provision users and devices	Critical
30039	Smart license in overage authorization expired	The license authorization has expired	Please check the network connection and renew the license authorization to avoid losing the ability to provision users and devices	Alert
30040	Smart license no provision authorization expired	The license authorization has expired and the product is in enforced mode	Please check the network connection and renew the license authorization in order to restore the ability to provision users and devices	Critical

ID	Title	Description	Solution	Severity
30041	Smart license registration expired	The license registration has expired and the system is unregistered with Cisco Smart Software Manager or satellite	Please check the network connectivity to Cisco Smart Software manager or satellite. Also verify your system clock is correct and then register the system with Cisco Smart Software Manager or satellite. If the issue still persists, please raise a TAC case	Error
30042	Smart license communication error	The system failed to communicate with cloud-based Cisco Smart Software Manager or On-Prem	Please check the network connectivity to cloud-based Cisco Smart Software manager or On-Prem	Error
30043	Smart license authorization expiring soon	The license authorization period will expire soon	Please initiate an authorization renewal	Warning
30044	Smart license renew auth failed	The license authorization renewal failed	Please retry an authorization renewal. If the problem persists please raise a TAC case	Error
30045	Smart license renew registration failed	The license registration renewal failed	Please retry a registration renewal. If the problem persists please raise a TAC case	Error
30046	Smart license registration expiring soon	The registration with Cisco Smart Software Manager or satellite will expire soon	Please initiate a registration renewal to avoid losing ability to provision users or devices	Warning

ID	Title	Description	Solution	Severity
30047	Capacity warning	The system has reached the licensed limit to support the number of devices for encrypted signaling sessions due to the Export Control Classification	Contact your Cisco representative	Warning
30048	Approaching Capacity warning	The system is reaching the licensed limit to support the number of devices for encrypted signaling sessions due to Export Control Classification	Contact your Cisco representative	Warning

Table 9: External Applications / Services Alarms

ID	Title	Description	Solution	Severity
35001	Configuration warning	Active Directory mode has been enabled but the DNS hostname has not been configured	Configure DNS hostname	Warning
35002	Configuration warning	Active Directory mode has been enabled but the NTP server has not been configured	Configure NTP server	Warning
35003	Configuration warning	Active Directory mode has been enabled but no DNS servers have been configured	Configure a DNS server	Warning

ID	Title	Description	Solution	Severity
35004	LDAP configuration required	Remote login authentication is in use for administrator accounts but a valid LDAP Server address, Port, Bind_DN and Base_DN have not been configured	Configure LDAP parameters	Warning
35005	Configuration warning	Active Directory mode has been enabled but a domain has not been configured	Configure domain on Active Directory Service page	Warning
35007	Configuration warning	Active Directory SPNEGO disabled; you are recommended to enable the SPNEGO setting	Enable SPNEGO	Warning
35008	Configuration warning	Active Directory mode has been enabled but a workgroup has not been configured	Configure workgroup on Active Directory Service page	Warning
35009	TMS Provisioning Extension services communication failure	The Expressway is unable to communicate with the TMS Provisioning Extension services. Phone book service failures can also occur if TMS does not have any users provisioned against this cluster.	Go to the TMS Provisioning Extension service status page and select the failed service to view details about the problem	Warning

ID	Title	Description	Solution	Severity
35010	TMS Provisioning Extension services data import failure	An import from the TMS Provisioning Extension services has been canceled as it would cause the Expressway to exceed internal table limits	See the Expressway Event Log for details, then check the corresponding data within TMS; you must perform a full synchronization after the data has been corrected in TMS	Warning
35011	TMS Provisioning Extension services data import failure	One or more records imported from the TMS Provisioning Extension services have been dropped due to unrecognized data format	See the Expressway Event Log for details, then check the corresponding data within TMS; you must perform a full synchronization after the data has been corrected in TMS	Warning
35012	Failed to connect to LDAP server	Failed to connect to the LDAP server for H.350 device authentication	Ensure that your H.350 directory service is correctly configured	Warning
35013	Unified Communications SSH tunnel failure	This system cannot communicate with one or more remote hosts: <*Host 1*, *Host 2*, ...> Note that the list of hosts is truncated to 200 characters.	Review the Event Log and check that the traversal zone between the Expressway-C and the Expressway-E is active	Warning
35014	Unified Communications SSH tunnel notification failure	This system cannot communicate with one or more remote hosts	Ensure that your firewall allows traffic from the Expressway-C ephemeral ports to 2222 TCP on the Expressway-E	Warning

ID	Title	Description	Solution	Severity
35015	Unified CM port conflict	There is a port conflict on Unified CM <name> between neighbor zone <name> and Unified Communications (both are using port <number>)	The same port on Unified CM cannot be used for line side (Unified Communications) and SIP trunk traffic. Review the port configuration on Unified CM and reconfigure the <zone> if necessary	Warning
35016	SAML metadata has been modified	Configuration changes have modified the local SAML metadata, which is now different to any copies on Identity Provider(s). This metadata may have been modified by changing the server certificate or the SSO-enabled domains, or by changing the number of traversal server peers or their addresses	Export the SAML metadata so you can import it on the Identity Provider	Warning

Table 10: Security Alarms

ID	Title	Description	Solution	Severity
40001	Security alert	No CRL distribution points have been defined for automatic updates	Check CRL configuration	Warning
40002	Security alert	Automatic updating of CRL files has failed	If the problem persists, contact your Cisco representative	Warning
40003	Insecure password in use	The root user has the default password set	View instructions on changing the root password	Warning

ID	Title	Description	Solution	Severity
40004	Certificate-based authentication required	Your system is recommended to have client certificate-based security set to *Certificate-based authentication* when in advanced account security mode	Configure client certificate-based security	Warning
40005	Insecure password in use	The admin user has the default password set	Change the admin password	Error
40006	Security alert	Unable to download CRL update	Check CRL distribution points and the Event Log	Warning
40007	Security alert	Failed to find configuration file for CRL automatic updates	If the problem persists, contact your Cisco representative	Warning
40008	Security alert	The SSH service is using the default key	View instructions on Changing the Default SSH Key	Warning
40009	Restart required	HTTPS client certificates validation mode has changed, however a restart is required for this to take effect	Restart the system	Warning
40011	Per-account session limit required	A non-zero per-account session limit is required when in advanced account security mode	Configure per-account session limit	Warning
40012	External manager connection is using HTTP	You are recommended to use HTTPS connections to the external manger when in advanced account security mode	Configure external manager	Warning

ID	Title	Description	Solution	Severity
40013	HTTPS client certificate validation disabled	You are recommended to enable client side certificate validation for HTTPS connections when in advanced account security mode	Configure HTTPS client certificate validation	Warning
40014	Time out period required	A non-zero system session time out period is required when in advanced account security mode	Configure session time out period	Warning
40015	System session limit required	A non-zero system session limit is required when in advanced account security mode	Configure system session limit	Warning
40016	Encryption required	Your login account LDAP server configuration is recommended to have encryption set to *TLS* when in advanced account security mode	Configure login account LDAP server	Warning
40017	Incident reporting enabled	You are recommended to disable incident reporting when in advanced account security mode	Configure incident reporting	Warning
40018	Insecure password in use	One or more users has a non-strict password		Warning
40019	External manager has certificate checking disabled	You are recommended to enable external manager certificate checking when in advanced account security mode	Configure external manager	Warning

ID	Title	Description	Solution	Severity
40020	Security alert	The connection to the Active Directory Service is not using TLS encryption	Configure Active Directory Service connection settings	Warning
40021	Remote logging enabled	You are recommended to disable the remote syslog server when in advanced account security mode	Configure remote logging	Warning
40022	Security alert	Active Directory secure channel disabled; you are recommended to enable the secure channel setting	Enable secure channel	Warning
40024	CRL checking required	Your login account LDAP server configuration is recommended to have certificate revocation list (CRL) checking set to *All* when in advanced account security mode	Configure login account LDAP server	Warning
40025	SNMP enabled	You are recommended to disable SNMP when in advanced account security mode	Configure SNMP mode	Warning
40026	Reboot required	The advanced account security mode has changed, however a reboot is required for this to take effect	Reboot the Expressway	Warning
40027	Security alert	The connection to the TMS Provisioning Extension services is not using TLS encryption	Configure TMS Provisioning Extension services connection settings	Warning

ID	Title	Description	Solution	Severity
40028	Insecure password in use	The root user's password is hashed using MD5, which is not secure enough	View instructions on changing the root password	Warning
40029	LDAP server CA certificate is missing	A valid CA certificate for the LDAP database has not been uploaded; this is required for connections via TLS	Upload a valid CA certificate	Warning
40030	Security alert	Firewall rules activation failed; the firewall configuration contains at least one rejected rule	Check your firewall rules configuration, fix any rejected rules and re-try the activation	Warning
40031	Security alert	Unable to restore previous firewall configuration	Check your firewall rules configuration, fix any rejected rules, activate and accept the rules; if the problem persists, contact your Cisco representative	Warning
40032	Security alert	Unable to initialize firewall	Restart the system; if the problem persists, contact your Cisco representative	Warning
40033	Configuration warning	The Default Zone access rules are enabled, but leaving SIP over UDP or SIP over TCP enabled offers a way to circumvent this security feature	Either disable UDP and TCP on the SIP page to enforce certificate identity checking using TLS, or disable the access rules for the Default Zone.	Warning
40034	Security alert	Firewall rules activation failed; the firewall configuration contains rules with duplicated priorities	Check your firewall rules configuration, ensure all rules have a unique priority and re-try the activation	Warning

ID	Title	Description	Solution	Severity
40036	Delegated credential checking error	The traversal server zone associated with SIP domain <domain> cannot connect to the traversal client system	Check that the domain and its associated traversal server zone are configured correctly. You may also need to check the remote traversal client system	Warning
40037	Delegated credential checking error	There is a communication problem with the traversal client zone <zone> used to receive delegated credential checking requests	Check that the traversal client zone is configured correctly. You may also need to check the remote traversal server system	Warning
40038	Delegated credential checking configuration error	TLS verify mode is not enabled on the traversal server zone associated with SIP domain <domain>	Check the domain and ensure that TLS verify mode is enabled on the associated traversal server zone	Warning
40039	Delegated credential checking configuration error	TLS verify mode is not enabled on the traversal client zone (<zone>) that has been configured to accept delegated authentication requests	Ensure that TLS verify mode is enabled on the traversal client zone	Warning
40040	Unified Communications configuration error	TLS verify mode is not enabled on a traversal zone configured for Unified Communications services	Ensure that TLS verify mode is enabled on the traversal zone; you may also need to check the remote traversal system	Warning
40041	Security alert	Automated intrusion protection rules are not available	Disable and then re-enable the failed services	Warning

ID	Title	Description	Solution	Severity
40042	FIPS140-2 compliance restriction	Some SIP configuration is not using TLS transport; FIPS140-2 compliance requires TLS	Ensure that TLS is the only enabled system-wide SIP transport mode on the SIP page, and that all zones are using TLS. Alternatively, if you are transitioning into FIPS140-2 you may want to restore a FIPS-compliant backup of your data.	Warning
40043	Unified Communications configuration error	Media encryption is not enforced on a traversal zone configured for Unified Communications services	Ensure that media encryption is set to 'Force encrypted' on the traversal zone	Warning
40044	System reset required	FIPS140-2 mode has been enabled; a system reset is required to complete this process	Ensure that all alarms are cleared, then take a system backup before performing a system reset	Warning
40045	Restart required	FIPS140-2 mode has been disabled; a system restart is required to complete this process	Restart the system	Warning
40046	FIPS140-2 compliance restriction	Clustered systems are not FIPS140-2 compliant	Disband the cluster	Warning
40048	Unified Communications configuration error	Unified Communications services are enabled but SIP TLS is disabled	Ensure that SIP TLS mode is set to 'On' on SIP configuration page	Warning
40049	Cluster TLS permissive	Cluster TLS verification mode permits invalid certificates	Change the cluster's TLS verification mode to Enforcing	Notice

ID	Title	Description	Solution	Severity
40050	Security alert	Unable to install new firewall configuration	Check your firewall configuration and rate limits configuration, fix any rejected rules; Do not restart your system; if the problem persists, contact your Cisco representative	
40051	CMS not Identified by Server Certificate	CMS address <*address*> has been entered on the Expressway-C but is not identified by the Expressway-E server certificate	Check that the CMS address on the Expressway-C matches the SAN entry on the Expressway-E server. You may need to generate a CSR for a new server certificate that includes the CMS as a SAN, or edit (or remove) the CMS on the Expressway-C	
40052	Certificate error	Server certificate does not have a Common Name (CN) attribute. Some services do not work without the CN	Update certificate	
40053	Invalid Cipher config	The following entries have cipher values that are invalid in FIPS140-2 mode: <*List*>	Please reconfigure the affected cipher entries at ciphers	
40054	Token decryption failure	The Expressway-C failed to decrypt or decode an OAuth token issued by Unified CM. This could be caused by changes to the issuer.	Refresh the Cisco Unified Communications Manager configuration.	Warning

ID	Title	Description	Solution	Severity
40055	Failed to update key file	Failed to update system key file due to inconsistent state	Restart the system. If that doesn't clear the problem, contact your Cisco representative	Warning
40056	fail2ban banned any IP address	HTTP proxy protocol violation Access to Expressway is blocked for new IP addresses - xx.xx.xx.xx	See number of failures and banned addresses for specific jails.	Warning
40061	ACME auto-sign failure	A failure was detected while running the auto-sign command for the server certificate	Please refer to the server certificate page for details	Warning
40062	ACME auto-sign failure	A failure was detected while running the auto-sign command for SNI domains [<*domain*>]	Please refer to the domain certificates page for details	Warning
40063	ACME auto-deploy failure	A failure was detected while running the auto-deploy command for the server certificate	Please refer to the server certificate page for details	Warning
40064	ACME auto-deploy failure	A failure was detected while running the auto-deploy command for SNI domains [*domain*]	Please refer to the domain certificates page for details	Warning
40066	HSM certificate is not used	An HSM certificate is installed but not in use	Please refer to the HSM configuration page for details	Alert
40068	Server certificate validity	Server certificate expired *or* Server certificate expires today	Create and upload a new server certificate	Critical

ID	Title	Description	Solution	Severity
40069	Server certificate validity	Server certificate expires in <*n*> days	You are recommended to create and upload a new server certificate	Alert
40100	Security alert	Firewall rules are not synchronized with network interfaces	Restart the system. If that doesn't clear the problem, contact your Cisco representative	Warning
40101	Absolute Time out period required	A non-zero system absolute time out period is required when in advanced account security mode	Configure absolute time out period	Warning

Table 11: Misconfiguration Alarms

ID	Title	Description	Solution	Severity
45001	Failed to load Call Policy file	<failure details>	Configure Call Policy	Warning
45002	Configuration warning	Expected default link between the Default Subzone and the Default Zone is missing	Configure default links	Warning
45003	Configuration warning	H.323 and SIP modes are set to Off; one or both of them should be enabled	Configure H.323 and/or SIP modes	Warning
45006	Configuration warning	Expected default link between the Default Subzone and the Cluster Subzone is missing	Configure default links	Warning
45007	Configuration warning	Expected default link between the Default Subzone and the Traversal Subzone is missing	Configure default links	Warning

ID	Title	Description	Solution	Severity
45008	Configuration warning	Expected default link between the Traversal Subzone and the Default Zone is missing	Configure default links	Warning
45009	Configuration warning	For provisioning to work correctly, authentication policy must be enabled on the Default Zone and any other relevant zone that receives provisioning requests	Set authentication policy to either “Check credentials” or “Treat as authenticated” for each relevant zone	Warning
45012	Configuration warning	For Presence services to work correctly, authentication policy must be enabled on the Default Subzone and any other relevant subzone; authentication must also be enabled on the Default Zone if the endpoints are not registered	Set authentication policy to either “Check credentials” or “Treat as authenticated” for the Default Subzone and each relevant subzone and zone	Warning
45013	Configuration warning	For phone book requests to work correctly, authentication policy must be enabled on the Default Subzone and any other relevant subzone; authentication must also be enabled on the Default Zone if the endpoints are not registered	Set authentication policy to either “Check credentials” or “Treat as authenticated” for the Default Subzone and each relevant subzone and zone	Warning

ID	Title	Description	Solution	Severity
45014	Configuration warning	H.323 is enabled in a zone with a SIP media encryption mode of “Force encrypted” or “Force unencrypted”	On the relevant zone, either disable H.323 or select a different SIP media encryption mode	Warning
45016	Configuration warning	A zone has a SIP media encryption mode of “Best effort” or “Force encrypted” but the transport is not TLS. TLS is required for encryption.	On the relevant zone, either set the SIP transport to TLS or select a different SIP media encryption mode	Warning
45017	Configuration warning	A subzone has a SIP media encryption mode of “Best effort” or “Force encrypted” but TLS is not enabled. TLS is required for encryption.	Either enable TLS on the SIP configuration page or select a different SIP media encryption mode for the relevant subzone or Default Subzone	Warning
45018	Configuration warning	DNS zones (including <zone_name>) have their SIP default transport protocol set to <protocol>, but that protocol is disabled system-wide	Check that the SIP default transport protocol for the DNS zone and the system-wide SIP transport settings are consistent	Warning
45019	Insufficient media ports	There is an insufficient number of media ports to support the number of licensed calls	Increase the media port range	Warning
45021	HSM server configuration issue	There is an issue with the HSM server configuration	Please refer to the HSM configuration page for details	Alert

ID	Title	Description	Solution	Severity
45022	Restart required	DMI administration configuration has been changed; however a restart is required for this to take effect.	Restart the system	Warning
45023	Configuration error	Attempt to share host/port tuple among multiple connections.	Review zones and correct any hostname or port conflict	Error
45024	SSLH failure	As *Administration DMI only* mode is not set and Web Administration is using port 443, the protocol multiplexing service cannot start. The Expressway is unable to listen on TCP 443 for TURN and WebRTC requests.		Critical

Table 12: Back to Back User Agent Alarms

ID	Title	Description	Solution	Severity
55001	B2BUA service restart required	Some B2BUA service specific configuration has changed, however a restart is required for this to take effect	Restart the B2BUA service	Warning
55002	B2BUA misconfiguration	The port on B2BUA for Expressway communications is misconfigured	Check B2BUA configuration (advanced settings)	Warning
55003	B2BUA misconfiguration	Invalid trusted host IP address of Microsoft device	Check configured addresses of trusted hosts	Warning
55004	B2BUA misconfiguration	The port on B2BUA for Microsoft call communications is misconfigured	Check B2BUA configuration (advanced settings)	Warning

ID	Title	Description	Solution	Severity
55005	B2BUA misconfiguration	The Microsoft destination address is misconfigured	Check B2BUA configuration	Warning
55006	B2BUA misconfiguration	The Microsoft destination port is misconfigured	Check B2BUA configuration	Warning
55007	B2BUA misconfiguration	The Microsoft transport type is misconfigured	Check B2BUA configuration	Warning
55008	B2BUA misconfiguration	Missing or invalid FQDN of service	Check the Expressway's system host name and domain name	Warning
55009	B2BUA misconfiguration	Invalid IP address of service	Check the Expressway's LAN 1 IPv4 address	Warning
55010	B2BUA misconfiguration	The B2BUA media port range end value is misconfigured	Check B2BUA configuration (advanced settings)	Warning
55011	B2BUA misconfiguration	The B2BUA media port range start value is misconfigured	Check B2BUA configuration (advanced settings)	Warning
55012	B2BUA misconfiguration	Invalid Microsoft interoperability mode	Check B2BUA configuration	Warning
55013	B2BUA misconfiguration	Invalid option key	Check option keys	Warning
55014	B2BUA misconfiguration	Invalid hop count	Check B2BUA configuration (advanced settings)	Warning
55015	B2BUA misconfiguration	Invalid trusted host IP address of transcoder	Check configured addresses of trusted hosts	Warning
55016	B2BUA misconfiguration	The setting to enable transcoders for this B2BUA is misconfigured	Check B2BUA configuration (transcoder settings)	Warning

ID	Title	Description	Solution	Severity
55017	B2BUA misconfiguration	The port on B2BUA for transcoder communications is misconfigured	Check B2BUA configuration (transcoder settings)	Warning
55018	B2BUA misconfiguration	Transcoder address and/or port details are misconfigured	Check B2BUA configuration (transcoder settings) and the configured addresses of trusted hosts	Warning
55019	B2BUA misconfiguration	Invalid TURN server address	Check B2BUA configuration (TURN settings)	Warning
55021	B2BUA misconfiguration	The setting to offer TURN services for this B2BUA is misconfigured	Check B2BUA configuration (TURN settings)	Warning
55026	B2BUA misconfiguration	TURN services are enabled, but there are no valid TURN servers configured	Configure the TURN server address	Warning
55028	B2BUA misconfiguration	The start and end media port ranges are misconfigured	Check the B2BUA media port range settings	Warning
55029	B2BUA misconfiguration	The media port ranges used by the B2BUA overlap with the media port ranges used by <module>	Check the port configuration for both services	Warning
55030	B2BUA misconfiguration	The port used by the B2BUA for Expressway communications is also used by <module>	Check the port configuration for both services	Warning
55031	B2BUA misconfiguration	The port used by the B2BUA for Microsoft call communications is also used by <module>	Check the port configuration for both services	Warning

ID	Title	Description	Solution	Severity
55032	B2BUA misconfiguration	The port used by the B2BUA for transcoder communications is also used by <module>	Check the port configuration for both services	Warning
55033	B2BUA misconfiguration	No valid Microsoft trusted hosts have been configured	Configure at least one trusted host device	Warning
55034	B2BUA misconfiguration	No valid transcoder trusted hosts have been configured	Configure at least one transcoder trusted host	Warning
55035	B2BUA connectivity problem	The B2BUA cannot connect to the transcoders	Restart the B2BUA service	Warning
55036	B2BUA connectivity problem	The B2BUA cannot connect to the Expressway	Restart the B2BUA service	Warning
55037	B2BUA connectivity problem	The B2BUA cannot connect to the Microsoft environment	Check the Microsoft interoperability status page for more information about the problem; you will then need to restart the B2BUA service after making any configuration changes	Warning
55101	B2BUA misconfiguration	Invalid Expressway authorized host IP address	Restart the service; contact your Cisco representative if the problem persists	Warning
55102	B2BUA misconfiguration	Invalid URI format of Expressway contact address	Restart the service; contact your Cisco representative if the problem persists	Warning
55103	B2BUA misconfiguration	Invalid Expressway encryption mode	Restart the service; contact your Cisco representative if the problem persists	Warning

ID	Title	Description	Solution	Severity
55104	B2BUA misconfiguration	Invalid Expressway ICE mode	Restart the service; contact your Cisco representative if the problem persists	Warning
55105	B2BUA misconfiguration	Invalid Expressway next hop host configuration	Restart the service; contact your Cisco representative if the problem persists	Warning
55106	B2BUA misconfiguration	Invalid Expressway next hop liveness mode	Restart the service; contact your Cisco representative if the problem persists	Warning
55107	B2BUA misconfiguration	Invalid Expressway next hop mode	Restart the service; contact your Cisco representative if the problem persists	Warning
55108	B2BUA misconfiguration	Invalid Expressway next hop port	Restart the service; contact your Cisco representative if the problem persists	Warning
55109	B2BUA misconfiguration	Invalid Expressway transport type	Restart the service; contact your Cisco representative if the problem persists	Warning
55110	B2BUA misconfiguration	Invalid URI format of B side contact address	Restart the service; contact your Cisco representative if the problem persists	Warning
55111	B2BUA misconfiguration	Invalid B side encryption mode	Restart the service; contact your Cisco representative if the problem persists	Warning
55112	B2BUA misconfiguration	Invalid B side ICE mode	Restart the service; contact your Cisco representative if the problem persists	Warning
55113	B2BUA misconfiguration	Invalid B side next hop liveness mode	Restart the service; contact your Cisco representative if the problem persists	Warning

ID	Title	Description	Solution	Severity
55114	B2BUA misconfiguration	Invalid B side next hop mode	Restart the service; contact your Cisco representative if the problem persists	Warning
55115	B2BUA misconfiguration	Invalid command listening port	Restart the service; contact your Cisco representative if the problem persists	Warning
55116	B2BUA misconfiguration	Invalid debug status path	Restart the service; contact your Cisco representative if the problem persists	Warning
55117	B2BUA misconfiguration	Invalid service	Restart the service; contact your Cisco representative if the problem persists	Warning
55118	B2BUA misconfiguration	Invalid software string	Restart the service; contact your Cisco representative if the problem persists	Warning
55119	B2BUA misconfiguration	Invalid URI format of transcoding service contact address	Restart the service; contact your Cisco representative if the problem persists	Warning
55120	B2BUA misconfiguration	Invalid transcoding service encryption mode	Restart the service; contact your Cisco representative if the problem persists	Warning
55121	B2BUA misconfiguration	Invalid transcoding service ICE mode	Restart the service; contact your Cisco representative if the problem persists	Warning
55122	B2BUA misconfiguration	Invalid transcoding service next hop liveness mode	Restart the service; contact your Cisco representative if the problem persists	Warning
55123	B2BUA misconfiguration	The transcoding service transport type is misconfigured	Restart the service; contact your Cisco representative if the problem persists	Warning

ID	Title	Description	Solution	Severity
55124	B2BUA misconfiguration	The mandatory TURN server setting is misconfigured	Restart the service; contact your Cisco representative if the problem persists	Warning
55125	B2BUA misconfiguration	Invalid Expressway next hop host configuration	Restart the service; contact your Cisco representative if the problem persists	Warning
55126	B2BUA misconfiguration	Invalid Expressway authorized host IP address	Restart the service; contact your Cisco representative if the problem persists	Warning
55127	B2BUA misconfiguration	Cannot start B2BUA application because FQDN configuration is missing	Configure the **System host name** and **Domain name** on the DNS page, and then restart the B2BUA service	Warning
55128	B2BUA misconfiguration	Cannot start B2BUA application because IPv4 interface address configuration is missing	Configure the LAN 1 IPv4 address on the IP page, and then restart the B2BUA service	Warning
55129	B2BUA misconfiguration	Cannot start B2BUA application because cluster name configuration is missing	Configure the cluster name on the Clustering page	Warning
55130	B2BUA misconfiguration	Invalid cluster name	Check the cluster name and then restart the B2BUA service	Warning
55131	B2BUA misconfiguration	Invalid session refresh interval	Check B2BUA configuration (advanced settings), then restart the B2BUA service	Warning
55132	B2BUA misconfiguration	Invalid call resource limit	Restart the service; contact your Cisco representative if the problem persists	Warning

ID	Title	Description	Solution	Severity
55133	B2BUA misconfiguration	The B2BUA session refresh interval is smaller than the minimum session refresh interval	Check both settings on the B2BUA configuration (advanced settings) and then restart the B2BUA service	Warning
55134	B2BUA misconfiguration	Invalid minimum session refresh interval	Check B2BUA configuration (advanced settings), then restart the B2BUA service	Warning
55135	B2BUA configuration warning	A large number of Microsoft trusted host devices have been configured; this may impact performance, or extreme cases it may prevent calls from accessing enough network resources to connect	Review your network topology and try lowering the number of trusted host devices on the B2BUA trusted hosts page.	Warning
55137	B2BUA misconfiguration	Invalid VCS multistream mode	Check B2BUA configuration (advanced settings), then restart the B2BUA service	Warning
55139	B2BUA misconfiguration	Invalid VCS multistream mode	Check B2BUA configuration (advanced settings), then restart the B2BUA service	Warning
55142	Insufficient RDP TCP/UDP ports	There is an insufficient number of TCP/UDP ports to support the maximum number of RDP calls	Increase the RDP TCP/UDP port ranges on the B2BUA configuration	Warning

Table 13: Management Connector Alarms

ID	Title	Description	Solution	Severity
60050	[Hybrid services] Connectivity error	Could not reach Cisco Collaboration Cloud address: <*string*>	Check <*string*>, or <*string*>, or use network utilities <*string*>, to verify this address.	error
60051	[Hybrid services] Communication error	HTTP error code <*string*> from Cisco Collaboration Cloud (address: <*string*>)	Check Hybrid Services status. Contact your Cisco Collaboration Cloud administrator if the issue persists.	error
60052	[Hybrid services] Communication error	<*string*>	Verify your <*string*>, <*string*>, <*string*> the address. Contact your Cisco Collaboration Cloud administrator if you have ruled these out.	error
60053	[Hybrid services] Access error	<*string*>	Contact your Cisco Collaboration Cloud administrator.	error
60054	[Hybrid services] Connector install error	<*string*>	Contact your Cisco Collaboration Cloud administrator.	error
60055	[Hybrid services] Download failed because the certificate was not valid	<*string*>	Check the Expressway's trusted CA list for the CA that signed the received certificate.	error
60056	[Hybrid services] Upgrade failed because certificate was not valid	<*string*>	Check the Expressway's trusted CA list for the CA that signed the received certificate.	error
60057	[Hybrid services] Upgrade failed because certificate name did not match	<*string*>	Check that the CN or a SAN on the certificate from <*string*> matches its hostname.	error

ID	Title	Description	Solution	Severity
60058	[Hybrid services] Connection failed because the CA certificate was not found	Cannot securely connect to the Cisco Collaboration Cloud because the root CA that signed the certificate from <*string*> is not in the Expressway's trusted CA list.	Update the Expressway's trusted CA list to include the CA that signed the received certificate.	error
60059	[Hybrid services] Connection failed because the certificate name did not match	The certificate from <*string*> did not have a CN or SAN attribute that matches its hostname.	Check that the CN or a SAN on the certificate from the remote server matches its hostname.	error
60060	[Hybrid services] Connection failed because the certificate was not validated	The Expressway could not validate the certificate from <*string*>. This can happen because the Expressway does not trust the CA, or because the certificate is not currently valid.	Check that the Expressway <*string*> list contains the root certificate of the CA that signed the received certificate. Check that the CA certificate is current and was not revoked. Check that the <*string*> is configured and that the Expressway is synchronized. If you can rule out these potential causes, contact Cisco; the server certificate we sent you might be invalid.	error

ID	Title	Description	Solution	Severity
60061	[Hybrid services] Upgrade prevented by user choice	You previously rejected connector upgrades currently advertised by Cisco Collaboration Cloud. Automatic upgrades will continue when the next versions are available. The advertised versions are: <*string*>	View connector versions	alert
60062	[Hybrid services] Connector disable error	<*string*>	Contact your Cisco Collaboration Cloud administrator.	error
60063	[Hybrid services] Connector enable error	<*string*>	Contact your Cisco Collaboration Cloud administrator	error
60064	[Hybrid services] Connector unexpectedly not running	<*string*>	Restart the stopped connector. If that connector upgraded itself recently, roll it back to the previous version. If the error persists, contact your Cisco Collaboration Cloud administrator.	error
60065	[Hybrid services] Connector version mismatch	<*string*>	Contact your Cisco Collaboration Cloud administrator.	error
60066	[Hybrid services] Routine authentication refresh failed	The Expressway periodically renews its authentication through <*string*>, but did not succeed this time. The Expressway will retry in <*string*> minutes.	If this issue persists, contact your Cisco Collaboration Cloud administrator.	error

ID	Title	Description	Solution	Severity
60067	[Hybrid services] Connectivity Error	Error when trying to access <*string*>. The Expressway will try again in approximately <*string*> seconds.	Check <*string*>, and check for network issues if the error persists.	error
60068	[Hybrid services] Invalid responses from Cisco Collaboration Cloud	Invalid data was received from <*string*>.	Check that you have the expected address for Cisco Collaboration Cloud.	error
60069	[Hybrid services] No service connectors	You registered for Hybrid Services but there are no service connectors installed. The Management Connector is active and is making unnecessary connections to the Cisco Collaboration Cloud.	Go to Cisco Cloud Collaboration Management and check that your organization is entitled to use one or more Hybrid Services. If you are not using any Hybrid Services, we strongly recommend that you <*string*> this Expressway.	alert
60070	[Hybrid services] HTTP exception	Received exception: <*string*>, while processing HTTP response from <*string*>	If the issue persists, contact your Cisco Collaboration Cloud administrator.	error
60071	[Hybrid services] Key error	This system could not register properly because of a data error in a connector file. The associated services will not work as expected, even if you appear to have registered successfully.	Try to register again (you may need to deregister first). If the issue persists, contact your Cisco Collaboration Cloud administrator.	error

ID	Title	Description	Solution	Severity
60072	[Hybrid services] Unsupported Expressway version	Your version of Expressway is no longer supported for Hybrid Services. To continue using Hybrid Services, you must upgrade to a newer version.	Please upgrade to the latest Expressway version, available on cisco.com.	alert
60073	[Hybrid services] Unsupported Expressway version	A new version of Cisco Expressway was released. We advise that you upgrade to this version at your earliest convenience to use the latest features and avoid an unsupported Hybrid Services deployment when the next Expressway version is released. Your current version will be supported until the next Expressway release.	Please upgrade to the latest Expressway version, available on cisco.com.	alert
60074	[Hybrid services] Connectivity error	Unable to reach the Cisco Collaboration Cloud.	Check Network requirements for Teams Service and follow the proxy guidelines as highlighted.	error

Table 14: Calendar Connector Alarms

ID	Title	Description	Solution	Severity
60100	Microsoft Exchange Server unreachable	An error occurred accessing the Microsoft Exchange Server. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: this includes <*string*>. The last known error is: <*string*>	Check network connectivity between Microsoft Exchange Server and Calendar Connector. Check the load on Microsoft Exchange Server	critical
60101	Microsoft Exchange Server access denied	Access to the Microsoft Exchange Server was denied. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: this includes <*string*>. The last known error is: <*string*>	Verify that the service account has valid credentials and correct permissions, and is not locked out	critical
60102	Microsoft Exchange Server certificate not validated	The certificate for the Microsoft Exchange Server could not be validated. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: this includes <*string*>. The last known error is: <*string*>	Verify the Microsoft Exchange Server certificate is valid	critical
60103	Microsoft Exchange Server version unsupported	The version of the configured Microsoft Exchange Server is not supported. Detailed info: <*string*>	Microsoft Exchange Server must be upgraded to supported version	critical

ID	Title	Description	Solution	Severity
60104	No Microsoft Exchange Server configured	The Calendar Connector stopped because no Microsoft Exchange Server settings are configured	Configure at least one Microsoft Exchange Server in the Calendar Connector and re-enable it	critical
60110	Microsoft Exchange Autodiscover unreachable	A timeout occurred accessing the Microsoft Exchange Server during user autodiscover. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: this includes <*string*>. The last known error is: <*string*>	Check network connectivity between Microsoft Exchange Autodiscover Server and Calendar Connector	critical
60111	Microsoft Exchange Autodiscover access denied	Access to the Microsoft Exchange Server during user autodiscover was denied. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: this includes <*string*>. The last known error is: <*string*>	Verify that the service account has valid credentials and correct permissions, and is not locked out	critical
60112	Microsoft Exchange Autodiscover certificate not validated	During autodiscover, the certificate for the the Microsoft Exchange Server could not be validated. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: this includes <*string*>. The last known error is: <*string*>	Verify the server certificate is valid	critical

ID	Title	Description	Solution	Severity
60113	Redirected Microsoft Exchange Autodiscovery URL not trusted	The redirected Microsoft Exchange Autodiscovery URL is changed and not trusted. Detailed info: <*string*>	Open the Exchange Service Record and save the record again. Confirm the new redirection URL is to be trusted	critical
60120	Microsoft Exchange Autodiscover LDAP unreachable	A timeout occurred during autodiscover, accessing the Microsoft LDAP server. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: this includes <*string*>. The last known error is: <*string*>	Check network connectivity between Microsoft Exchange Autodiscover LDAP Server and Calendar Connector	critical
60121	Microsoft Exchange Autodiscover LDAP access denied	Access to the Microsoft LDAP Server during autodiscover was denied. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: this includes <*string*>. The last known error is: <*string*>	Verify that the service account has valid credentials and correct permissions, and is not locked out	critical
60130	Microsoft Exchange Server user subscription failure	<*string*> users failed to subscribe to Microsoft Exchange Server(s). Detailed info: the users include <*string*>	Verify the Microsoft Exchange Server is not busy and the network connectivity between Microsoft Exchange Server and Calendar Connector	error

ID	Title	Description	Solution	Severity
60131	SMTP address has no mailbox	Multiple (<*string*>) SMTP address(es) have been detected with no associated mailbox(es). Detailed info: <*string*>	Verify the target mailbox is fully enabled and the target server is correct	error
60132	Subscription not operational	The Calendar Service has not received notifications from the Microsoft Exchange Server for one or more users. Calendar Service requests and notifications for these users will not be processed until this is addressed	Verify that the Microsoft Exchange Server(s) are functioning correctly, and that you have network connectivity. If the condition continues, consider restarting the Calendar Service	error
60140	Meeting notification incoming rate too high	The incoming meeting notification rate is too high for <*string*> Calendar Service user(s). Detailed info: the users include <*string*>	Check Microsoft Exchange Server for the mailbox(es) of the user(s)	error
60142	Meeting processing time too long	Calendar Service meeting processing time exceeds a threshold of 5 minutes for at least one user	Check Microsoft Exchange Server and Calendar Service for user notification rate	error
60150	Cisco Collaboration Cloud Monitor Service unreachable	A required cloud service currently cannot be reached. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: <*string*>	Verify connectivity to Internet	critical

ID	Title	Description	Solution	Severity
60151	Cisco Collaboration Cloud Monitor Service access denied	Access to Cisco Collaboration Cloud services was denied. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: <*string*>	Contact tech support	critical
60152	Cisco Collaboration Cloud API Service unreachable	A required cloud service currently cannot be reached. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: <*string*>	Verify connectivity to Internet	critical
60153	Cisco Collaboration Cloud API Service access denied	Access to Cisco Collaboration Cloud services was denied. Calendar Service requests and notifications will not be processed until this is resolved. Detailed info: <*string*>	Contact tech support	critical
60154	Retrieving key from encryption service failed	Calendar Connector failed to retrieve an existing key or request to generate a new key from an encryption service. Detailed info: the encryption service is <*string*>	Verify the encryption service is on	error

ID	Title	Description	Solution	Severity
60155	Cisco Collaboration Cloud Monitor message service not connected	Calendar Connector failed to connect to Cisco Collaboration Cloud Monitor message service. Detailed info: the cloud service route is <*string*>	Verify network connectivity to Cisco Collaboration Cloud Monitor message service	critical
60156	Cisco Collaboration Cloud API message service not connected	Calendar Connector failed to connect to Cisco Collaboration Cloud API message service. Detailed info: the cloud service route is <*string*>	Verify network connectivity to Cisco Collaboration Cloud API message service	critical
60160	Cisco Collaboration Meeting Rooms (CMR) service unreachable or access denied	Cisco Collaboration Meeting Rooms (CMR) service currently cannot be reached or access was denied. @webex meetings will not be processed until this is resolved. Detailed info: the CMR service site name includes <*string*>	Verify network connectivity and configured account credentials to CMR service	error
60161	WebEx user account not available	<*string*> WebEx user account(s) are not available. @webex meetings for these users will not be processed until their account problems are resolved. Detailed info: the affected users include <*string*>	Verify WebEx service account and user accounts. Make sure the user has a WebEx account, and the account is not locked out, deactivated or Personal Room disabled	warning

ID	Title	Description	Solution	Severity
60162	Cisco WebEx administrator password has expired or invalid	Cisco WebEx service cannot be accessed due to expired or invalid administrator password. @webex meetings on affected site will not be processed until this is resolved. Detailed info: the WebEx service site name includes <*string*>	Change the expired or invalid administrator password on affected WebEx server	error
60163	Cisco WebEx administrator password expiring	Cisco WebEx administrator password for <*string*> site(s) will expire soon. Detailed info: the WebEx service site with expiring administrator password includes <*string*>	Change the expiring administrator password on affected WebEx server	warning
60164	Cisco WebEx administrator account locked out	Cisco WebEx service cannot be accessed due to locked out administrator account. @webex meetings on affected site will not be processed until this is resolved. Detailed info: the WebEx service site name includes <*string*>	Unlock the administrator account on affected WebEx server	error
60170	Management Connector not running	Calendar Connector is not operational because Management Connector is not running	Go to **Applications** > **Cloud Extensions** > **Connector Management** to start the Management Connector	error

ID	Title	Description	Solution	Severity
60171	Management Connector not operational	Calendar Connector is not operational because Management Connector is not operational	Check the status of the Management Connector and restart it if necessary	error
60190	Calendar Connector not operational	Calendar Connector is not operational since one or more cloud and/or on-premises services are not operational	Check the Calendar Connector status for details	critical

Table 15: Call Connector Alarms

ID	Title	Description	Solution	Severity
60300	The user is not configured with any directory numbers.	The user is not configured with any directory numbers - user[<*string*>]: <*string*>	Add at least one line on a device associated with the user in Unified CM	warning
60301	The user has no valid devices in the control list.	The user has no valid devices in the control list - user[<*string*>]: <*string*>	Associate at least one valid device with at least one line with the user in Unified CM	warning
60302	The user is not configured with a directory URI.	The user is not configured with a directory URI - user[<*string*>]: <*string*>	Enter a directory URI value under the user's account settings in Unified CM	warning
60303	Could not find a user with this email address.	Could not find a user with this email address - user[<*string*>]: <*string*>	Enter an email address for the user in Unified CM	warning
60304	Email mismatch with directory URI	The user's email does not match the directory URI - user[<*string*>]: <*string*>	Verify that the user's email and directory URI are identical in Unified CM	warning

ID	Title	Description	Solution	Severity
60305	The user's primary directory URI does not match the directory URI configured for the primary line.	The user's primary directory URI does not match the directory URI configured for the primary line - user[<*string*>]: <*string*>	Verify that the user's directory URI and line URI on an associated device are identical in Unified CM	warning
60306	The user is not configured with a valid CTI remote device.	The user is not configured with a valid CTI remote device - user[<*string*>]: <*string*>	Configure a CTI remote device and add to the user's control list in Unified CM.	warning
60307	Webex SIP address cannot be routed to the Webex cloud.	The user's Webex SIP address cannot be routed to the Webex cloud - user[<*string*>]: <*string*>	Check the rerouting calling search space on Unified CM and the partition configured for the Webex SIP address pattern.	error
60308	Webex SIP address is already in use.	The User's Webex SIP address is assigned to another user - user[<*string*>]: <*string*>	In Cisco Unified CM administration, check whether the user's remote destination is already used by a device.	error
60309	The user's remote destination was not removed.	When the user is deactivated for Call Service Connect, the remote destination was not removed. - user[<*string*>]: <*string*>	In Cisco Unified CM administration, check whether the user's remote destination is already used by a device. Remove the remote destination from the user's CTI remote device in Unified CM.	warning

ID	Title	Description	Solution	Severity
60310	Unable to add the user's Webex SIP address in Unified CM.	Unable to add the user's Webex SIP address in Unified CM - user[<*string*>]: <*string*>	In Cisco Unified CM Administration, delete a manually created remote destination if it exists. Then call connector will recreate the remote destination automatically.	error
60311	The user is not configured with a primary directory number.	The user is not configured with a primary directory number - user[<*string*>]: <*string*>	Configure a primary directory number for the user in Unified CM.	warning
60315	Automatic Spark Remote Device created with truncated name	The Automatic Spark Remote Device name was shortened during Call Service Connect activation. - user[<*string*>]: <*string*> has device with nam <*string*>	To avoid this issue, user IDs must not exceed 15 characters.	warning
60316	Unable to delete Spark Remote Device	Call connector cannot delete the Spark remote device after Call Service Connect was deactivated - user[<*string*>]: <*string*>	Check error messages in Unified CM.	warning
60317	Call connector is unable to create a CTI Remote Device in Unified CM.	Call connector is unable to create a CTI Remote Device in Unified CM - user[<*string*>]: <*string*>	Check for any potentially conflicting device names.	warning

ID	Title	Description	Solution	Severity
60318	Users must have mobility enabled for call connector to create a CTI remote device.	Users must have mobility enabled for call connector to create a Remote Device for Webex - user[<*string*>]: <*string*>	Check whether the Unified CM user is enabled for mobility.	warning
60319	Connectivity to Unified CM AXL Service lost	Connectivity to Unified CM AXL Service lost - for Unified CM [<*string*>]	Check whether the AXL service is running on Unified CM and resolve any network issues.	error
60320	Cannot connect to Unified CM CTIManager Service.	Cannot connect to Unified CM CTIManager Service - for Unified CM [<*string*>]	Check whether the CTIManager service is running on Unified CM and resolve any networking issues.	error
60321	Certificate verification failed	Call Connector stopped as it could not verify the certificate provided by the Webex cloud.	Download the certificate as part of the Expressway registration process and reregister the Expressway-C. If the error remains, update the Webex certificate in the Expressway-C trust store.	error
60322	Fully Qualified Domain Name is not valid	Fully Qualified Domain Name is Empty - user[<*string*>]: <*string*>	Add a fully qualified domain name in the Unified CM enterprise parameter. See the documentation for guidance.	warning
60323	Fully Qualified Domain Name is not valid	Fully Qualified Domain Name contains wild card - user[<*string*>]: <*string*>	Add a new fully qualified domain name without wildcards in the Unified CM enterprise parameter.	warning

ID	Title	Description	Solution	Severity
60324	Unable to reach the Unified CM AXL server.	Unable to reach the Unified CM AXL server - server[<*string*>]	Check network connectivity between call connector and Unified CM.	error
60325	Unable to authenticate with Unified CM AXL server	Unable to authenticate with Unified CM AXL server - [<*string*>]	Check the Unified CM user credentials that you provided during call connector configuration.	error
60326	User configured for Unified CM AXL communication is not authorized	User configured for Unified CM AXL communication is not authorized - server [<*string*>]	Check the access roles for the user configured in UCM Configuration on the Call Connector.	error
60327	No Unified CM Configured	No Unified CM is configured for call connector.	Configure a Unified CM for Call Connector.	warning
60328	The user is configured for more than one Unified CM cluster.	The user is configured for more than one Unified CM cluster - user[<*string*>]: <*string*>	Check the user's home cluster setting on all Unified CMs configured on this call connector.	warning
60329	Call connector received an invalid Webex SIP Address.	Invalid Spark SIP Address - for user[<*string*>]: <*string*>	Check the user and device configuration. Follow the documentation to reconfigure these, and if needed, reconfigure to create a valid Webex SIP address.	error
60330	The user is configured with more than one CTI remote device.	The user is configured with more than one CTI remote device - user[<*string*>]: <*string*>	Remove extra devices from the user's control list in Unified CM.	warning

ID	Title	Description	Solution	Severity
60331	The CTI remote device has no configured directory numbers.	The CTI remote device has no configured directory numbers - user[<*string*>]: <*string*>	In Unified CM, add at least one line to the CTI remote device associated with the user.	warning
60332	In Unified CM CTIManager, a request timed out to update the remote destination.	In Unified CM CTIManager, a request timed out to update the remote destination - user[<*string*>]: <*string*>	Verify that the Unified CM CTIManager service is up and running.	warning
60333	Unable to connect to Unified CM CTIManager	Unable to connect to Unified CM CTIManager	Check network connectivity between Call connector and Unified CM.	error
60334	Unable to authenticate user configured for Unified CM CTIManager	Unable to authenticate user configured for Unified CM CTIManager	Check the user credentials in Unified CM configuration on the call connector.	error
60335	Conflict in Device Ownership on Unified CM.	Unified CM shows a conflict with the owner of the device - for user[<*string*>]: <*string*>	Check the configuration in Unified CM.	warning
60336	A device exists with the same name as the CTI remote device tried to create for the user.	A device exists with the same name as the CTI remote device tried to create - for user[<*string*>]: <*string*>	Check the device names and configuration in Unified CM.	warning
60337	CTI remote device successfully created for the user, but the device subscription to receive call events failed.	CTI remote device successfully created for the user, but the device subscription to receive call events failed - for user[<*string*>]: <*string*>	Check the configuration in Unified CM and retry.	warning

ID	Title	Description	Solution	Severity
60338	Invalid remote destination on Unified CM.	Invalid remote destination on Unified CM - for user[<*string*>]: <*string*>	Follow the user and remote device configuration in the documentation to create a valid Webex SIP address.	warning
60339	The user exceeds the remote destination limit.	Unable to create a Webex SIP address. The user exceeds the remote destination limit in Cisco Unified CM.	Remove any unused remote destinations or increase the limit.	error
60340	The user is not configured with a home cluster.	The user is not configured with a home cluster - user[<*string*>]: <*string*>	Configure a home cluster for this user on Unified CM.	warning
60341	Call connector invalid configuration	Invalid Configuration reason=[<*string*>]	Fix the configuration error and then restart the call connector.	error
60342	Call connector version mismatch with the Webex cloud	Invalid message received in state [<*string*>], potential version mismatch with the Webex cloud	Go to admin.webex.com > Services > Hybrid Call > View all to open the resources, and then upgrade to the latest Call Connector software.	error
60343	Webex SIP Address exceeds the 48 character limit.	Unable to add Webex SIP address for a user. Unified CM does not support remote destinations that are longer than 48 characters.	Change device names so Webex SIP addresses don't exceed the character limit.	error
60344	User's directory URI is not in the organization's verified domain list	User's directory URI is not in the organization's verified domain list - user[<*string*>]: <*string*> has domain list = <*string*>	Check the user's directory URI and list of verified domains for this user	warning

ID	Title	Description	Solution	Severity
60345	Failed to Build Unified CM Cluster Data-Cache	Failed to Build Unified CM Cluster Data-Cache - server[<*string*>]	Check if the AXL service is running on Unified CM cluster nodes and resolve any network issues.	error
60346	Authentication Failure with Cisco Collaboration Cloud Services.	Authentication credentials available on Expressway are invalid.	Go to the Expressway, and then reregister it to the cloud under **Applications** > **Hybrid Services** > **Connector Management**.	error
60347	Authorization Failure with Cisco Collaboration Cloud Services.	Invalid role or access scope for this Expressway to access Cisco Collaboration Cloud Services.	Go to the Expressway, and then reregister it to the cloud under **Applications** > **Hybrid Services** > **Connector Management**.	error
60348	Connection from the Cisco Collaboration Cloud is down.	Connection from the Cisco Collaboration Cloud is down.	Check your network DNS or proxy settings and then try again.	error
60349	Connection to the Cisco Collaboration Cloud is down.	Connection to the Cisco Collaboration Cloud is down.	Check your network DNS or proxy settings and then try again.	error
60350	Cannot enable hybrid voicemail for your organization.	Cannot enable hybrid voicemail for your organization.	If this error persists, work with your trials team or contact support by submitting feedback through the Cisco Spark app.	warning

ID	Title	Description	Solution	Severity
60351	Call connector detected an invalid hybrid voicemail configuration.	Call connector detected an invalid hybrid voicemail configuration.	Check the Hybrid Voicemail deployment steps. If this error persists, work with your trials team or contact support by submitting feedback through the Cisco Spark app.	error
60352	No Directory Number exists in UCM with this directory URI	No Directory Number exists in UCM with this directory URI	Configure a Directory Number in UCM with this directory URI	error
60353	AXL Change Notification is not started at Unified CM.	AXL Change Notification is not started at Unified CM - server[<*string*>]	Enable AXL Change Notification in Enterprise Parameters of Unified CM.	error

Table 16: Significant Event Alarms

ID	Title	Description	Solution	Severity
90001	Emergency call	Emergency call has been made by ([*user@example.com*]), from zone (*zone name*), source IP (*IP address*).	NA	emergency

Table 17: Telemetry Alarms

ID	Title	Description	Solution	Severity
60800	CollectD Service Down	Core Telemetry Service is not operational	Disable and enable the Telemetry Connector and check for network issues. If the problem persists, contact your Cisco support representative.	Critical

ID	Title	Description	Solution	Severity
60801	Cloud-Connected UC Connection Down	Connection to Cloud-Connected UC is broken	Disable and enable the Telemetry Connector and check for network issues. If the problem persists, contact your Cisco support representative.	Critical
60802	Configuration Error	Configuration Update or Configuration Fetch Failed	Disable and enable the Telemetry Connector and check for network issues. Also, check if the cluster or node is authorized, and onboarded properly. If the problem still persists, contact your Cisco support representative.	Error
60803	Authentication Error	Authentication Failed on one or all the Telemetry Connector Connections or Transactions Processing	Disable and enable the Telemetry Connector and check for network issues. Also, check if the cluster or node is authorized, onboarded properly and the necessary certificates are installed. If the problem still persists, contact your Cisco support representative.	Error

ID	Title	Description	Solution	Severity
60804	CA Certificate Read Error	Failed to Read or include CA Certificate	• Check if the cluster or node is authorized, onboarded properly and the necessary certificates are installed. • Reinstall the required certificates. • Disable and Enable Telemetry Connector and check for network issues. If the problem persists, contact your Cisco support representative.	Error
60805	Invalid Certificate Error	Invalid Certificate Loaded	• Check if the cluster or node is authorized, onboarded properly and the valid certificates are installed. • Reinstall the correct and valid certificates. • Disable and Enable Telemetry Connector and check for network issues. If the problem persists, contact your Cisco support representative.	Error

Command Reference — xConfiguration

The `xConfiguration` group of commands are used to set and change individual items of configuration. Each command is made up of a main element followed by one or more sub-elements.

To obtain information about existing configuration, type:

- `xConfiguration` to return all current configuration settings
- `xConfiguration <element>` to return configuration for that element and all its sub-elements
- `xConfiguration <element> <subelement>` to return configuration for that sub-element

To obtain information about using each of the `xConfiguration` commands, type:

- `xConfiguration ?` to return a list of all elements available under the `xConfiguration` command
- `xConfiguration ??` to return a list of all elements available under the `xConfiguration` command, along with the valuespace, description and default values for each element
- `xConfiguration <element> ?` to return all available sub-elements and their valuespace, description and default values
- `xConfiguration <element> <sub-element> ?` to return all available sub-elements and their valuespace, description and default values

To set a configuration item, type the command as shown. The valid values for each command are indicated in the angle brackets following each command, using the following notation:

Table 18: Data conventions used in the CLI reference

Format	Meaning
<0..63>	Indicates an integer value is required. The numbers indicate the minimum and maximum value. In this example the value must be in the range 0 to 63.
<S: 7,15>	An **S** indicates a string value, to be enclosed in quotation marks, is required. The numbers indicate the minimum and maximum number of characters for the string. In this example the string must be between 7 and 15 characters long.
<Off/Direct/Indirect>	Lists the set of valid values. Do not enclose the value in quotation marks.
[1..50]	Square brackets indicate that you can configure more than one of this particular item. Each item is assigned an index within the range shown. For example `IP Route [1..50] Address <S: 0,39>` means that up to 50 IP routes can be specified with each route requiring an address of up to 39 characters in length.

xConfiguration Commands

All of the available **xConfiguration** commands are listed in the table below:

Table 19: xConfiguration CLI reference

xConfiguration Administration DeviceProvisioning: <On/Off> Determines whether the **System** > **TMS Provisioning Extension services** page is accessible in the Expressway web user interface. From there you can connect to the Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE) and its provisioning services for users, devices, FindMe and phone books. Default: Off. *On*: the **System** > **TMS Provisioning Extension services** page is accessible and provisioning services can be configured for this Expressway. *Off*: the **System** > **TMS Provisioning Extension services** page is not accessible. Example: `xConfiguration Administration DeviceProvisioning: On`
xConfiguration Administration HTTP Mode: <On/Off> Determines whether HTTP calls will be redirected to the HTTPS port. You must restart the system for any changes to take effect. Default: On. *On*: calls will be redirected to HTTPS. *Off*: no HTTP access will be available. Example: `xConfiguration Administration HTTP Mode: On`
xConfiguration Administration HTTPS Mode: <On/Off> Determines whether the Expressway can be accessed via the web interface. This must be On to enable both web interface and TMS access. You must restart the system for any changes to take effect. Default: On. Example: `xConfiguration Administration HTTPS Mode: On`
xConfiguration Administration LCDPanel Mode: <On/Off> Controls whether the LCD panel on the front of the Expressway identifies the system. Default: On. *On*: the system name and first active IP address are shown. *Off*: the LCD panel reveals no identifying information about the system. Example: `xConfiguration Administration LCDPanel Mode: On`
xConfiguration Administration SSH Mode: <On/Off> Determines whether the Expressway can be accessed via SSH and SCP. You must restart the system for any changes to take effect. Default: On. Example: `xConfiguration Administration SSH Mode: On`
xConfiguration Alarm Notification Email Custom Alarm ID: <String> If one or more customized alarm notifications is configured. The alarm Id for customized or disabled notifications.

xConfiguration Alarm Notification Email Custom Disable Notify: <Off>

If one or more customized alarm notifications is configured.

xConfiguration Alarm Notification Email Custom Email: <String>

If one or more customized alarm notifications is configured. The email id to which the selected alarm notifications are to be sent (maximum length 254).

xConfiguration Alarm Notification Email Destination Alert: <S: 0, 254>

The email destination for alarms with severity attribute “Alert”.

Example: `xConfiguration Alarm Notification Email Destination Alert: "ucadmin@example.com"`

xConfiguration Alarm Notification Email Destination Critical: <S: 0, 254>

The email destination for alarms with severity attribute “Critical”.

Example: `xConfiguration Alarm Notification Email Destination Alert: "ucadmin@example.com"`

xConfiguration Alarm Notification Email Destination Debug: <S: 0, 254>

The email destination for alarms with severity attribute “Debug”.

Example: `xConfiguration Alarm Notification Email Destination Debug: "uctech@example.com"`

xConfiguration Alarm Notification Email Destination Emergency: <S: 0, 254>

The email destination for alarms with severity attribute “Emergency”.

Example: `xConfiguration Alarm Notification Email Destination Emergency: "ert@example.com"`

xConfiguration Alarm Notification Email Destination Error: <S: 0, 254>

The email destination for alarms with severity attribute “Error”.

Example: `xConfiguration Alarm Notification Email Destination Error: "ucadmin@example.com"`

xConfiguration Alarm Notification Email Destination Info: <S: 0, 254>

The email destination for alarms with severity attribute “Info”.

Example: `xConfiguration Alarm Notification Email Destination Info: "ucadmin@example.com"`

xConfiguration Alarm Notification Email Destination Notice: <S: 0, 254>

The email destination for alarms with severity attribute “Notice”.

Example: `xConfiguration Alarm Notification Email Destination Notice: "ucadmin@example.com"`

xConfiguration Alarm Notification Email Destination Warning: <S: 0, 254>

The email destination for alarms with severity attribute “Warning”.

Example: `xConfiguration Alarm Notification Email Destination Warning: "ucadmin@example.com"`

xConfiguration Alarm Notification SMTP Mode: <On/Off>

Determines whether or not alarm-based email notifications will be used. The default is Off.

Example: `xConfiguration Alarm Notification SMTP Mode: On`

xConfiguration Alarm Notification SMTP Server Email: <S: 0, 254>

The source email from which alarm-based email notifications are sent to the configured destination address.

Example: `Alarm Notification SMTP Server Email: "ucadmin@example.com"`

xConfiguration Alarm Notification SMTP Server Host: <S: 0, 128>

IP address or FQDN of the SMTP server to be used to send alarm-based email notifications.

Example: `xConfiguration Alarm Notification SMTP Server Host: "email.example.com"`

xConfiguration Alarm Notification SMTP Server Password: <Password>

Password for the SMTP server to be used to send alarm-based email notifications.

Example: `xConfiguration Alarm Notification SMTP Server Password: "{cipher}$NNxx1xxx-xxxx-xxxx-xxxn-fnxnxNNNxxxN$1$xX+xnXnnXxnnxxnnnXXXnxnXXxnxXxxx/XXxnxnxxxx="`

xConfiguration Alarm Notification SMTP Server Port:

Port number of the SMTP server to be used to send alarm-based email notifications. Default is 587.

Example: `xConfiguration Alarm Notification SMTP Server Port: 587`

xConfiguration Alternates Cluster Name: <S: 0,128>

The fully qualified domain name used in SRV records that address this Expressway cluster, for example "cluster1.example.com". The name can only contain letters, digits, hyphens and underscores.

Warning: if you change the cluster name after any user accounts have been configured on this Expressway, you may need to reconfigure your user accounts to use the new cluster name.

Example: `xConfiguration Alternates Cluster Name: "Regional"`

xConfiguration Alternates ConfigurationPrimary: <1..6>

Specifies which peer in this cluster is the primary, from which configuration will be replicated to all other peers. A cluster consists of up to 6 peers, including the local Expressway.

Example: `xConfiguration Alternates ConfigurationPrimary: 1`

xConfiguration Alternates Peer [1..6] Address: <S: 0, 128>

Specifies the address of one of the peers in the cluster to which this Expressway belongs. A cluster consists of up to 6 peers, including the local Expressway. We recommend using FQDNs, but these can be IP addresses.

Example: `xConfiguration Alternates 1 Peer Address: "cluster1peer3.example.com"`

xConfiguration ApacheModReqTimeOut

You can set all available properties for the request timeout using a single shorthand command.

Example: `xConfiguration ApacheModReqTimeout Apachehead:20 Apachebody:20 Status:On`

xConfiguration ApacheModReqTimeOut Apachebody: <0..120>

Modifes the number of seconds that the Apache web server waits for the request body. If the full request body is not received before the timeout expires, Apache returns a timeout error. Default: 20.

Example: `xConfiguration ApacheModReqTimeout Apachebody:20`

xConfiguration ApacheModReqTimeOut Apacheheader: <0..120>

Modifes the number of seconds that the Apache web server waits for the request header. If the full request header is not received before the timeout expires, Apache returns a timeout error. Default: 20.

Example: `xConfiguration ApacheModReqTimeout Apacheheader:20`

xConfiguration ApacheModReqTimeOut Status: <On/Off>

Toggles the custom Apache request timeout. Displays the status of the timeout if you omit the switch.

On: The default Apache request timeout is superseded with your settings (or the defaults) for `Apachebody` and `Apacheheader`.

Off: `Apachebody` and `Apacheheader` have no effect. The Apache request timeout defaults to 300 seconds.

Example: `xConfiguration ApacheModReqTimeout Status:On`

xConfiguration Applications ConferenceFactory Alias: <S:0,60>

The alias that will be dialed by the endpoints when the Multiway feature is activated. This must be pre-configured on all endpoints that may be used to initiate the Multiway feature.

Example: `xConfiguration Applications ConferenceFactory Alias: "multiway@example.com"`

xConfiguration Applications ConferenceFactory Mode: <On/Off>

The Mode option allows you to enable or disable the Conference Factory application. Default: Off.

Example: `xConfiguration Applications ConferenceFactory Mode: Off`

xConfiguration Applications ConferenceFactory Range End: <1..65535>

The last number of the range that replaces %% in the template used to generate a conference alias. Default: 65535.

Example: `xConfiguration Applications ConferenceFactory Range End: 30000`

xConfiguration Applications ConferenceFactory Range Start: <1..65535>

The first number of the range that replaces %% in the template used to generate a conference alias. Default: 65535.

Example: `xConfiguration Applications ConferenceFactory Range Start: 10000`

xConfiguration Applications ConferenceFactory Template: <S:0,60>

The alias that the Expressway will tell the endpoint to dial in order to create a Multiway conference on the MCU. This alias must route to the MCU as a fully-qualified SIP alias

Example: `xConfiguration Applications ConferenceFactory Template: "563%%@example.com"`

xConfiguration Applications External Status [1..10] Filename: <S:0,255>

XML file containing status that is to be attached for an external application.

Example: `xConfiguration Applications External Status 1 Filename: "foo.xml"`

xConfiguration Applications External Status [1..10] Name: <S:0,64>

Descriptive name for the external application whose status is being referenced.

Example: `xConfiguration Applications External Status 1 Name: "foo"`

xConfiguration Authentication ADS ADDomain: <S: 0,255>

The Kerberos realm used when the Expressway joins the AD domain. Note: this field is case sensitive.

Example: `xConfiguration Authentication ADS ADDomain: "CORPORATION.INT"`

xConfiguration Authentication ADS Clockskew: <1..65535>

Maximum allowed clockskew between the Expressway and the KDC before the Kerberos message is assumed to be invalid (in seconds). Default: 300.

Example: `xConfiguration Authentication ADS Clockskew: 300`

xConfiguration Authentication ADS CipherSuite: <S:1,2048>

Specifies the cipher suite to use when the Expressway makes a TLS-encrypted LDAP connection to join the AD domain. The command accepts a string in the 'OpenSSL ciphers' format (See https://www.openssl.org/docs/man1.0.2/apps/ciphers.html#CIPHER-LIST-FORMAT).

Example: `xConfiguration Authentication ADS CipherSuite: "HIGH:MEDIUM:!ADH:!aNULL:!eNULL:-AES128-SHA256:@STRENGTH"`

xConfiguration Authentication ADS DC [1..5] Address: <S: 0,39>

The address of a domain controller that can be used when the Expressway joins the AD domain. Not specifying a specific AD will result the use of DNS SRV queries to find an AD.

Example: `xConfiguration Authentication ADS DC 1 Address: "192.168.0.0"`

xConfiguration Authentication ADS Encryption: <Off/TLS>

Sets the encryption to use for the LDAP connection to the ADS server.

Note Removed the weak ciphers, but retained one cipher (eTYPE-ARCFOUR-HMAC-MD5) to allow for backward compatibility.

Default: TLS.

Off: no encryption is used.

TLS: TLS encryption is used.

Example: `xConfiguration Authentication ADS Encryption: TLS`

xConfiguration Authentication ADS KDC [1..5] Address: <S: 0,39>

The address of a Kerberos Distribution Center (KDC) to be used when connected to the AD domain. Not specifying a specific KDC will result in the use of DNS SRV queries to find a KDC.

Example: `xConfiguration Authentication ADS KDC 1 Address: "192.168.0.0"`

xConfiguration Authentication ADS KDC [1..5] Port: <1..65534>

Specifies the port of a KDC that can be used when the Expressway joins the AD domain. Default: 88.

Example: `xConfiguration Authentication ADS KDC 1 Port: 88`

xConfiguration Authentication ADS MachineName: <S: 0..15>

This overides the default NETBIOS machine name used when the Expressway joins the AD domain.

Example: `xConfiguration Authentication ADS MachineName: "short_name"`

xConfiguration Authentication ADS MachinePassword Refresh: <On/Off>

Determines if this samba client should refresh its machine password every 7 days, when joined to the AD domain. Default: On.

Example: `xConfiguration Authentication ADS MachinePassword Refresh: On`

xConfiguration Authentication ADS Mode: <On/Off>

Indicates if the Expressway should attempt to form a relationship with the AD. Default: Off.

Example: `xConfiguration Authentication ADS Mode: On`

xConfiguration Authentication ADS SPNEGO: <Enabled/Disabled>

Indicates if SPNEGO (Simple and Protected GSSAPI Negotiation Mechanism) is used when the client (the Expressway) authenticates with the server (the AD domain controller). Default: Enabled.

Example: `xConfiguration Authentication ADS SPNEGO: Enabled`

xConfiguration Authentication ADS SecureChannel: <Auto/Enabled/Disabled>

Indicates if data transmitted from the Expressway to an AD domain controller is sent over a secure channel. Default: Auto.

Example: `xConfiguration Authentication ADS SecureChannel: Auto`

xConfiguration Authentication ADS Workgroup: <S: 0,15>

The workgroup used when the Expressway joins the AD domain.

Example: `xConfiguration Authentication ADS Workgroup: "corporation"`

xConfiguration Authentication Account Admin Account [1..n] AccessAPI: <On/Off>

Determines whether this account is allowed to access the system's status and configuration via the Application Programming Interface (API). Default: On.

Example: `xConfiguration Authentication Account Admin Account 1 AccessAPI: On`

xConfiguration Authentication Account Admin Account [1..n] AccessWeb: <On/Off>

Determines whether this account is allowed to log in to the system using the web interface. Default: On.

Example: `xConfiguration Authentication Account Admin Account 1 AccessWeb: On`

xConfiguration Authentication Account Admin Account [1..n] Enabled: <On/Off>

Indicates if the account is enabled or disabled. Access will be denied to disabled accounts. Default: On.

Example: `xConfiguration Authentication Account Admin Account 1 Enabled: On`

xConfiguration Authentication Account Admin Account [1..n] Name: <S: 0, 128>

The username for the administrator account.

Example: `xConfiguration Authentication Account Admin Account 1 Name: "bob_smith"`

xConfiguration Authentication Account Admin Account [1..n] Password: <Password>

The password that this administrator will use to log in to the Expressway.

Example: `xConfiguration Authentication Account Admin Account 1 Password: "abcXYZ_123"`

xConfiguration Authentication Account Admin Group [1..n] AccessAPI: <On/Off>

Determines whether members of this group are allowed to access the system's status and configuration using the Application Programming Interface (API). Default: On.

Example: `xConfiguration Authentication Account Admin Group 1 AccessAPI: On`

xConfiguration Authentication Account Admin Group [1..n] AccessWeb: <On/Off>

Determines whether members of this group are allowed to log in to the system using the web interface. Default: On.

Example: `xConfiguration Authentication Account Admin Group 1 AccessWeb: On`

xConfiguration Authentication Account Admin Group [1..n] Enabled: <On/Off>

Indicates if the group is enabled or disabled. Access will be denied to members of disabled groups. Default: On.

Example: `xConfiguration Authentication Account Admin Group 1 Enabled: On`

xConfiguration Authentication Account Admin Group [1..n] Name: <S: 0, 128>

The name of the administrator group.

Example: `xConfiguration Authentication Account Admin Group 1 Name: "administrators"`

xConfiguration Authentication Certificate Crlcheck: <None/Peer/All>

Specifies whether HTTPS client certificates are checked against certificate revocation lists (CRLs). CRL data is uploaded to the Expressway via the CRL management page. Default: All.

None: no CRL checking is performed.

Peer: only the CRL associated with the CA that issued the client's certificate is checked.

All: all CRLs in the trusted certificate chain of the CA that issued the client's certificate are checked.

Example: `xConfiguration Authentication Certificate Crlcheck: All`

xConfiguration Authentication Certificate Crlinaccessible: <Ignore/Fail>

Controls the revocation list checking behavior if the revocation status cannot be established, for example if the revocation source cannot be contacted or no appropriate revocation list is present. Default: Ignore.

Ignore: treat the certificate as not revoked.

Fail: treat the certificate as revoked (and thus do not allow the TLS connection).

Example: `xConfiguration Authentication Certificate Crlinaccessible: Ignore`

xConfiguration Authentication Certificate Mode: <NotRequired/Validation/Authentication>

Controls the level of security required to allow client systems (typically web browsers) to communicate with the Expressway over HTTPS. Default: NotRequired.

NotRequired: the client system does not have to present any form of certificate.

Validation: the client system must present a valid certificate that has been signed by a trusted certificate authority (CA). Note that a restart is required if you are changing from Not required to Certificate validation.

Authentication: the client system must present a valid certificate that has been signed by a trusted CA and contains the client's authentication credentials. When this mode is enabled, the standard login mechanism is no longer available.

Example: `xConfiguration Authentication Certificate Mode: NotRequired`

xConfiguration Authentication Certificate UsernameRegex: <String>

The regular expression to apply to the client certificate presented to the Expressway. Use the (? regex) syntax to supply names for capture groups so that matching sub-patterns can be substituted in the associated template. Default: /Subject:.*CN= (? ([^,\]|(\,))*)/m

Example: `xConfiguration Authentication Certificate UsernameRegex: "/Subject:.*CN= (? ([^,\]|(\,))*)/m"`

xConfiguration Authentication Certificate UsernameTemplate: <String>

A template containing a mixture of fixed text and the capture group names used in the Regex. Delimit each capture group name with # , for example, prefix#Group1#suffix. Each capture group name will be replaced with the text obtained from the regular expression processing. The resulting string is used as the user's authentication credentials (username). Default: #captureCommonName#

Example: `xConfiguration Authentication Certificate UsernameTemplate: "#captureCommonName#"`

xConfiguration Authentication H350 BindPassword: <S: 0, 60>

Sets the password to use when binding to the LDAP server.

Example: `xConfiguration Authentication H350 BindPassword: "abcXYZ_123"`

xConfiguration Authentication H350 BindSaslMode: <None/DIGEST-MD5>

The SASL (Simple Authentication and Security Layer) mechanism to use when binding to the LDAP server. Default: DIGEST-MD5.

None: no mechanism is used.

DIGEST-MD5: the DIGEST-MD5 mechanism is used.

Example: `xConfiguration Authentication H350 BindSaslMode: DIGEST-MD5`

xConfiguration Authentication H350 BindUserDn: <S: 0, 500>

Sets the user distinguished name to use when binding to the LDAP server.

Example: `xConfiguration Authentication H350 BindUserDn: "manager"`

xConfiguration Authentication H350 BindUserName: <S: 0, 500>

Sets the username to use when binding to the LDAP server. Only applies if using SASL.

Example: `xConfiguration Authentication H350 BindUserName: "manager"`

xConfiguration Authentication H350 DirectoryBaseDn: <S: 0, 500>

Sets the Distinguished Name to use when connecting to an LDAP server.

Example: `xConfiguration Authentication H350 DirectoryBaseDn: "dc=example,dc=company,dc=com"`

xConfiguration Authentication H350 LdapEncryption: <Off/TLS>

Sets the encryption to use for the connection to the LDAP server. Default : TLS.

Off: no encryption is used.

TLS: TLS encryption is used.

Example: `xConfiguration Authentication H350 LdapEncryption: TLS`

xConfiguration Authentication H350 LdapServerAddress: <S: 0, 256>

The IP address or Fully Qualified Domain Name of the LDAP server to use when making LDAP queries for device authentication.

Example: `xConfiguration Authentication H350 LdapServerAddress: "ldap_server.example.com"`

xConfiguration Authentication H350 LdapServerAddressResolution: <AddressRecord/ServiceRecord>

Sets how the LDAP server address is resolved if specified as an FQDN. Default: AddressRecord.

Address record: DNS A or AAAA record lookup.

SRV record: DNS SRV record lookup.

Example: `xConfiguration Authentication H350 LdapServerAddressResolution: AddressRecord`

xConfiguration Authentication H350 LdapServerPort: <1..65535>

Sets the IP port of the LDAP server to use when making LDAP queries for device authentication. Typically, non-secure connections use 389. Default : 389

Example: `xConfiguration Authentication H350 LdapServerPort: 389`

xConfiguration Authentication H350 Mode: <On/Off>

Enables or disables the use of an H.350 directory for device authentication. Default: Off.

Example: `xConfiguration Authentication H350 Mode: Off`

xConfiguration Authentication LDAP AliasOrigin: <LDAP/Endpoint/Combined>

Determines how aliases are checked and registered. Default: LDAP.

LDAP: the aliases presented by the endpoint are checked against those listed in the LDAP database.

Endpoint: the aliases presented by the endpoint are used; any in the LDAP database are ignored.

Combined: the aliases presented by the endpoint are used in addition to any listed in the LDAP database.

Example: `xConfiguration Authentication LDAP AliasOrigin: LDAP`

xConfiguration Authentication Password: <S: 0, 215>

The password used by the Expressway when authenticating with another system. The maximum plaintext length is 128 characters, which is then encrypted. Note: this does not apply to traversal client zones.

Example: `xConfiguration Authentication Password: "password123"`

xConfiguration Authentication Remote Digest Cache ExpireCheckInterval: <0..65535>

The interval between digest authentication cache expiration checks in seconds. Default: 600

Example: `xConfiguration Authentication Remote Digest Cache ExpireCheckInterval: 600`

xConfiguration Authentication Remote Digest Cache Lifetime: <0..43200>

The lifetime of digest authentication interim hashes in seconds. Default: 600

Example: `xConfiguration Authentication Remote Digest Cache Lifetime: 600`

xConfiguration Authentication Remote Digest Cache Limit: <0..65535>

The interval between digest authentication cache expiration checks in seconds. Default: 10000

Example: `xConfiguration Authentication Remote Digest Cache Limit: 10000`

xConfiguration Authentication Remote Digest Cache Mode: <On/Off>

Controls whether the digest authentication cache is enabled. Default: On

Example: `xConfiguration Authentication Remote Digest Cache Mode: On`

xConfiguration Authentication StrictPassword Enabled: <On/Off>

Determines whether local administrator account passwords must meet a minimum level of complexity before they are accepted. In addition, passwords must not: be based on a dictionary word contain too many consecutive characters such as “abc” or “123”, contain too few different characters or be palindromes. Default: Off.

On: local administrator account passwords must meet the complexity requirements.

Off: passwords are not checked for complexity.

Example: `xConfiguration Authentication StrictPassword Enabled: Off`

xConfiguration Authentication StrictPassword MaximumConsecutiveRepeated: <0..255>

The maximum number of times the same character can be repeated consecutively. A value of 0 disables this check. Default: 0

Example: `xConfiguration Authentication StrictPassword MaximumConsecutiveRepeated: 0`

xConfiguration Authentication StrictPassword MinimumClasses: <0..4>

The minimum number of character classes that must be present. There are four character classes: digit, upper case, lower case and special. Use this setting if you want to mandate the use of 2-3 different character classes without requiring all of them to be present. A value of 0 disables this check. Default: 0.

Example: `xConfiguration Authentication StrictPassword MinimumClasses: 0`

xConfiguration Authentication StrictPassword MinimumDigits: <0..255>

The minimum number of digits that must be present. A value of 0 disables this check. Default: 2.

Example: `xConfiguration Authentication StrictPassword MinimumDigits: 2`

xConfiguration Authentication StrictPassword MinimumLength: <6..255>

The minimum length of the password. Default: 15.

Example: `xConfiguration Authentication StrictPassword MinimumLength: 15`

xConfiguration Authentication StrictPassword MinimumLowerCase: <0..255>

The minimum number of lower case characters that must be present. A value of 0 disables this check. Default: 2.

Example: `xConfiguration Authentication StrictPassword MinimumLowerCase: 2`

xConfiguration Authentication StrictPassword MinimumOther: <0..255>

The minimum number of special characters that must be present. A special character is anything that is not a letter or a digit. A value of 0 disables this check. Default: 2

Example: `xConfiguration Authentication StrictPassword MinimumOther: 2`

xConfiguration Authentication StrictPassword MinimumUpperCase: <0..255>

The minimum number of upper case characters that must be present. A value of 0 disables this check. Default : 2

Example: `xConfiguration Authentication StrictPassword MinimumUpperCase: 2`

xConfiguration Authentication UserName: <S: 0, 128>

The username used by the Expressway when authenticating with another system. Note: this does not apply to traversal client zones.

Example: `xConfiguration Authentication UserName: "user123"`

xConfiguration Bandwidth Default: <64..65535>

The bandwidth (in kbps) to use on calls managed by the Expressway where no bandwidth has been specified by the endpoint. Default: 384.

Example: `xConfiguration Bandwidth Default: 384`

xConfiguration Bandwidth Downspeed PerCall Mode: <On/Off>

Determines whether the Expressway attempts to downspeed a call if there is insufficient per-call bandwidth available to fulfill the request. Default: On.

On: the Expressway will attempt to place the call at a lower bandwidth.

Off: the call will be rejected.

Example: `xConfiguration Bandwidth Downspeed PerCall Mode: On`

xConfiguration Bandwidth Downspeed Total Mode: <On/Off>

Determines whether the Expressway attempts to downspeed a call if there is insufficient total bandwidth available to fulfill the request. Default: On.

On: the Expressway will attempt to place the call at a lower bandwidth.

Off: the call will be rejected.

Example: `xConfiguration Bandwidth Downspeed Total Mode: On`

xConfiguration Bandwidth Link [1..3000] Name: <S: 1, 50>

Assigns a name to this link.

Example: `xConfiguration Bandwidth Link 1 Name: "HQ to BranchOffice"`

xConfiguration Bandwidth Link [1..3000] Node1 Name: <S: 0, 50>

Specifies the first zone or subzone to which this link will be applied.

Example: `xConfiguration Bandwidth Link 1 Node1 Name: "HQ"`

xConfiguration Bandwidth Link [1..3000] Node2 Name: <S: 0, 50>

Specifies the second zone or subzone to which this link will be applied.

Example: `xConfiguration Bandwidth Link 1 Node2 Name: "BranchOffice"`

xConfiguration Bandwidth Link [1..3000] Pipe1 Name: <S: 0, 50>

Specifies the first pipe to be associated with this link.

Example: `xConfiguration Bandwidth Link 1 Pipe1 Name: "512Kb ASDL"`

xConfiguration Bandwidth Link [1..3000] Pipe2 Name: <S: 0, 50>

Specifies the second pipe to be associated with this link.

Example: `xConfiguration Bandwidth Link 1 Pipe2 Name: "2Gb Broadband"`

xConfiguration Bandwidth Pipe [1..1000] Bandwidth PerCall Limit: <1..100000000>

If this pipe has limited per-call bandwidth, sets the maximum amount of bandwidth (in kbps) available for any one call. Default: 1920.

Example: `xConfiguration Bandwidth Pipe 1 Bandwidth PerCall Limit: 256`

xConfiguration Bandwidth Pipe [1..1000] Bandwidth PerCall Mode: <Limited/Unlimited/NoBandwidth>

Determines whether or not this pipe is limiting the bandwidth of individual calls. Default: Unlimited.

NoBandwidth: no bandwidth available. No calls can be made on this pipe.

Example: `xConfiguration Bandwidth Pipe 1 Bandwidth PerCall Mode: Limited`

xConfiguration Bandwidth Pipe [1..1000] Bandwidth Total Limit: <1..100000000>

If this pipe has limited bandwidth, sets the maximum bandwidth (in kbps) available at any one time on the pipe. Default: 500000.

Example: `xConfiguration Bandwidth Pipe 1 Bandwidth Total Limit: 1024`

xConfiguration Bandwidth Pipe [1..1000] Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>

Determines whether or not this pipe is enforcing total bandwidth restrictions. Default: Unlimited.

NoBandwidth: no bandwidth available. No calls can be made on this pipe.

Example: `xConfiguration Bandwidth Pipe 1 Bandwidth Total Mode: Limited`

xConfiguration Bandwidth Pipe [1..1000] Name: <S: 1, 50>

Assigns a name to this pipe.

Example: `xConfiguration Bandwidth Pipe 1 Name: "512Kb ASDL"`

xConfiguration Call Loop Detection Mode: <On/Off>

Specifies whether the Expressway will check for call loops. Default: On.

Example: `xConfiguration Call Loop Detection Mode: On`

xConfiguration Call Routed Mode: <Always/Optimal>

Specifies whether the Expressway routes the signaling for calls. Default: Always.

Always: the Expressway will always route the call signaling.

Optimal: if possible, the Expressway will remove itself from the call signaling path, which may mean the call does not consume a call license.

Example: `xConfiguration Call Routed Mode: Always`

xConfiguration Call Services CallsToUnknownIPAddresses: <Off/Direct/Indirect>

The way in which the Expressway attempts to call systems that are not registered with it or one of its neighbors. Default: Indirect.

Direct: allows an endpoint to make a call to an unknown IP address without the Expressway querying any neighbors. The call setup would occur just as it would if the far end were registered directly to the local system.

Indirect: upon receiving a call to an unknown IP address, the Expressway will query its neighbors for the remote address and if permitted will route the call through the neighbor.

Off: endpoints registered directly to the Expressway may only call an IP address of a system also registered directly to that Expressway.

Example: `xConfiguration Call Services CallsToUnknownIPAddresses: Indirect`

xConfiguration Call Services Fallback Alias: <S: 0, 60>

Specifies the alias to which incoming calls are placed for calls where the IP address or domain name of the Expressway has been given but no callee alias has been specified.

Example: `xConfiguration Call Services Fallback Alias: "reception@example.com"`

xConfiguration CollaborationEdge AllowEmbeddedSafari: <Yes/No>

This only applies to Cisco Jabber 11.8 or later, on iPads or iPhones using iOS 9 or later, when they authorize using OAuth tokens.

Select *Yes* to allow Jabber on iOS devices to display the authentication page in the native Safari browser.

Select *No* to have Jabber on iOS devices display the authentication page in the WebView browser, rather than in the Safari browser.

Note If you toggle this option, also make the corresponding selection for **SSO Login Behavior for iOS** in Cisco Unified Communications Manager.

Example: `xConfiguration CollaborationEdge AllowEmbeddedSafari: No`

xConfiguration CollaborationEdge AllowList DefaultMethods: <String>

Configure one or more default HTTP methods for the HTTP allow list.

Configuration Parameters:

Methods: <OPTIONS/GET/HEAD/POST/PUT/DELETE> - A comma-delimiting set of one or more http methods

Example: `xConfiguration CollaborationEdge AllowList DefaultMethods: PUT,GET,POST`

xConfiguration CollaborationEdge AllowOnboardingOverMra: <On/Off>

Enables or disables activation code onboarding for MRA devices. If enabled/disabled, mTLS is automatically enabled/disabled on the MRA port. The necessary CA certificates for mTLS are auto-generated.

Example: `xConfiguration CollaborationEdge AllowOnboardingOverMra: On`

xConfiguration CollaborationEdge AllowRedirectUri: <On/Off>

Enables or disables Redirect URI. Allows the client to use Embedded browser for (and MRA) OAuth flow. Default value is *No*. Set the value to *Yes* to enable this option.

Example: `xConfiguration CollaborationEdge AllowRedirectUri: Off`

xConfiguration CollaborationEdge Enabled: <On/Off>

Enables or disables Mobile and Remote Access on this Expressway.

Example: `xConfiguration CollaborationEdge Enabled: On`

xConfiguration CollaborationEdge InternalCheck: <No/Yes>

This switch determines whether the Expressway-C will check the user's home node for available authentication modes. If you select *No* , the Expressway tells the client that the authentication modes enabled on the Expressway-C are available, without actually checking the home node. You should see less traffic on the internal network as a result, but you should only select this option if you know that all nodes have the same authentication modes available.

Select *Yes* to allow the Expressway-C to check on the user's home node before the Expressway-E responds to the client.

Example: `xConfiguration CollaborationEdge InternalCheck: No`

xConfiguration CollaborationEdge JabbercEnabled: <On/Off>

Enables or disables Jabber Guest services on this Expressway.

Example: `xConfiguration JabbercEnabled: Off`

xConfiguration CollaborationEdge JabbercProxyProtocol: <http/https>

Selects the protocol used to proxy Jabber Guest services requests through the Expressway.

Example: `xConfiguration JabbercProxyProtocol: https`

xConfiguration CollaborationEdge LegacyCred: <On/Off>

Select On if Unified Communications services authorize MRA clients based on the username and password they supply to the Expressway.

Example: `xConfiguration CollaborationEdge LegacyCred: Off`

xConfiguration CollaborationEdge LegacySso: <On/Off/Exclusive>

Select On if Unified Communications services authorize MRA clients based on the OAuth token they supply to the Expressway. This is not the self-describing OAuth token type.

Example: `xConfiguration CollaborationEdge LegacySso: Off`

xConfiguration CollaborationEdge OauthLocal: <On/Off>

Enables or disables OAuth local authentication for mobile and remote access to Unified Communications services.

Example: `xConfiguration CollaborationEdge OauthLocal: Off`

xConfiguration CollaborationEdge OauthSso: <On/Off>

Enables or disables OAuth Single Sign-On for mobile and remote access to Unified Communications services.

Example: `xConfiguration CollaborationEdge OauthSso: Off`

xConfiguration CollaborationEdge RFC3327Enabled: <On/Off>

Changes Path header support for registrations going through automatically generated neighbor zones to Unified CM nodes.

On: The Expressway-C inserts its address into the Path header of the REGISTER message, and into the response to that message.

Off: The Expressway-C overwrites the address in the Contact header of the REGISTER message.

Example: `xConfiguration CollaborationEdge rfc3327Enabled: On`

xConfiguration CollaborationEdge SSO Scope: <PEER/CLUSTER>

Use PEER if you wish to use a SAML agreement, with your chosen IdP, for each Expressway peer. Use CLUSTER if you wish to use a single SAML agreement for the cl uster.

Example: `xConfiguration CollaborationEdge SSO Scope: CLUSTER`

xConfiguration CollaborationEdge SSO IdP <index> Digest: <sha1/sha256>

Changes the hash algorithm that the Expressway uses when signing SAML authentication requests given to the client.

<*index*> is an integer distinguishing a particular IdP from the list that is configured on the Expressway.

Example: `xConfiguration CollaborationEdge SSO IdP 1 Digest: sha256`

xConfiguration CollaborationEdge SsoAlwaysAvailable: <On/Off>

Determines whether the Expressway-C will check if the user's home node has SSO available.

On: The Expressway-E always tells the client that SSO is available, without actually checking the home node.

Off: Allow the Expressway-C to check if SSO is available on the user's home node before the Expressway-E responds to the client.

Example: `xConfiguration CollaborationEdge SsoAlwaysAvailable: Off`

Note The default value *Off* corresponds to the following default on the web UI: **Check for internal SSO availability**: *Yes*

xConfiguration CollaborationEdge SsoEnabled: <On/Off>

Toggles Single Sign-On for mobile and remote access to UC services.

Example: `xConfiguration CollaborationEdge SsoEnabled: Off`

xConfiguration CollaborationEdge SsoSipTokenExtraTtl: <0..172800>

Extends the lifetime of the SIP authorization token by the supplied number of seconds.

Important The extended time-to-live means that external users can still use SIP over the edge after their on-premises UC credentials have expired. This gives users a short window in which they can still accept calls (if they haven't noticed that they need to re-authenticate), but you should balance this convenience against the increased security exposure.

Example: `xConfiguration CollaborationEdge SsoSipTokenExtraTtl: 0`

xConfiguration CollaborationEdgeDeployments <index> DeploymentId: <1..65535>

Changes the deployment ID of a particular deployment.

<*index*> is an integer distinguishing a particular IdP from the list that is configured on the Expressway.

Example: `xConfiguration CollaborationEdgeDeployments 1 DeploymentId: 5`

xConfiguration CollaborationEdgeDeployments <index> UserReadableName: <String>

Enter a name for this deployment. You can use multiple deployments to partition the Unified Communications services provided via this Expressway. See Using deployments to partition Unified Communications services.

<*index*> is an integer distinguishing a particular IdP from the list that is configured on the Expressway.

Example: `xConfiguration CollaborationEdgeDeployments 1 UserReadableName: StagingDeployment`

xConfiguration Ciphers SIPTLSCiphers Value: <S:0,2048>

Specifies the SIP TLS cipher suite to use in 'OpenSSL ciphers' format (See https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT). Note that a restart is required for this to take effect. Also note that aNULL ciphers are not supported for inbound connections.

Default: `EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:+ADH`

Example: `xConfiguration Ciphers SIPTLSCiphers Value: "EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:+ADH"`

To change SIP TLS protocol value, see: *SIP Advanced SipTlsVersions*.

xConfiguration Ciphers HTTPSCiphers Value: <S:0,2048>

Specifies the HTTPS cipher suite to use in 'OpenSSL ciphers' format (See https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT).

Default: `EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL`

Example: `xConfiguration Ciphers HTTPSCiphers Value: "EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL"`

xConfiguration Ciphers HTTPSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2>

Specifies the HTTPS TLS protocol minimum version.

Default: `minTLSv1.2`

Example: `xConfiguration Ciphers HTTPSProtocol Value: "minTLSv1.2"`

xConfiguration Ciphers SMTPTLSCiphers Value: <S:0,2048>

Specifies the SMTP TLS cipher suite to use in 'OpenSSL ciphers' format (see https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT

Default: `EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL`

Example: `xConfiguration Ciphers SMTPTLSCiphers Value: "EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL"`

xConfiguration Ciphers SMTPTLSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2>

Specifies the SMTP TLS protocol minimum version.

Default: `minTLSv1.2`

Example: `xConfiguration Ciphers SMTPTLSProtocol Value: "minTLSv1.2"`

xConfiguration Ciphers ReverseProxyTLSCiphers Value: <S:0,2048>

Specifies the Reverse Proxy TLS cipher suite to use in 'OpenSSL ciphers' format (See https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT).

Default: `EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL`

Example: `xConfiguration Ciphers ReverseProxyTLSCiphers Value: "EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL"`

xConfiguration Ciphers ReverseProxyTLSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2>

Specifies the Reverse Proxy TLS protocol minimum version.

Default: `minTLSv1.2`

Example: `xConfiguration Ciphers ReverseProxyTLSProtocol Value: "minTLSv1.2"`

xConfiguration Ciphers UcClientTLSCiphers Value: <S:0,2048>

Specifies the UC Client TLS cipher suite to use in 'OpenSSL ciphers' format (See https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT).

Default: `EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL`

Example: `xConfiguration CiphersUcClientTLSCiphers Value: "EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL"`

xConfiguration Ciphers UcClientTLSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2>

Specifies the UC Client TLS protocol minimum version.

Default: `minTLSv1.2`

Example: `xConfiguration Ciphers UcClientTLSProtocol Value: "minTLSv1.2"`

xConfiguration Ciphers XCPTLSCiphers Value: <S:0,2048>

Specifies the XCP TLS cipher suite to use in 'OpenSSL ciphers' format (See https://www.openssl.org/docs/manmaster/man1/ciphers.html#CIPHER-LIST-FORMAT). Note that a restart is required for this to take effect.

Default: `EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL`

Example: `xConfiguration Ciphers XCPTLSCiphers Value: "EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL"`

xConfiguration Ciphers XCPTLSProtocol Value: <S:minTLSv1.0, minTLSv1.1, minTLSv1.2>

Specifies the XCP TLS protocol minimum version.

Default: `minTLSv1.2`

Example: `xConfiguration Ciphers XCPTLSProtocol Value: minTLSv1.2`

xConfiguration Ciphers sshd_ciphers Value: <S:0,2048>

Configures the available ciphers for admin/root SSH connections (TCP/22 or 5022) in "openssh" format.

Note Port 22 is configured as the Administrator SSH port on Expressway Appliances. The Expressway Virtual Machine can be deployed on port 22 or 5022 when the VM is deployed.

Default: `aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr`

Example: `xConfiguration Ciphers sshd_ciphers Value: "aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr"`

xConfiguration Ciphers sshd_kex Value: <S:0,2048>

Configures key exchange algorithms for admin/root SSH connections (TCP/22 or 5022) in "openssh" format.

Note Port 22 is configured as the Administrator SSH port on Expressway Appliances. The Expressway Virtual Machine can be deployed on port 22 or 5022 when the VM is deployed.

Default: `ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1`

Example: `xConfiguration Ciphers sshd_kex Value: "ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1"`

xConfiguration Ciphers sshd_macs Value: <S:0,2048>

Configures the message authentication code digests for admin/root SSH connections (TCP/22 or 5022) in "openssh" format.

Note Port 22 is configured as the Administrator SSH port on Expressway Appliances. The Expressway Virtual Machine can be deployed on port 22 or 5022 when the VM is deployed.

Default: `hmac-sha2-512,hmac-sha2-256,hmac-sha1`

Example: `xConfiguration Ciphers sshd_macs Value: "hmac-sha2-512,hmac-sha2-256,hmac-sha1"`

xConfiguration Ciphers sshd_pfwd_ciphers Value: <S:0,2048>

The ciphers available for the SSH tunnels used for the forward and reverse HTTP proxies (i.e. APNS and MRA HTTP traffic).

Default: `aes256-ctr`

Example: `xConfiguration Ciphers sshd_pfwd_ciphers Value: "aes256-ctr"`

xconfiguration Ciphers sshd_pfwd_pubkeyalgorithms

Configure the available public key algorithms.

Default values:
`"x509v3-rsa2048-sha256,x509v3-ecdsa-sha2-nistp256,x509v3-ecdsa-sha2-nistp384,x509v3-ecdsa-sha2-nistp521"`

Only following values are allowed:
`x509v3-rsa2048-sha256,x509v3-ecdsa-sha2-nistp256,x509v3-ecdsa-sha2-nistp384,x509v3-ecdsa-sha2-nistp521`

Example: `xconfiguration Ciphers sshd_pfwd_pubkeyalgorithms Value: "x509v3-rsa2048-sha256,x509v3-ecdsa-sha2-nistp256"`

Note You must use the default value for the **sshd_pfwd_pubkeyalgorithms** configuration (All four types of public key configured).

Configure all public key types that the server certificate of this node uses in case you plan to customize this configuration. Similarly, configure all other nodes that are connecting to this node using ssh tunnel.

For example, One node Expressway-C has a server certificate created using ECDSA with 256 size and this is connecting to another node Expressway-E over ssh tunnel which has a server certificate created using ECDSA with 384 size. Configure **sshd_pfwd_pubkeyalgorithms** to values `"x509v3-ecdsa-sha2-nistp256,x509v3-ecdsa-sha2-nistp384"` for both the nodes.

xConfiguration DNS PerDomainServer [1..5] Address: <S: 0, 39>

The IP address of the DNS server to use only when resolving hostnames for the associated domain names.

Example: `xConfiguration DNS PerDomainServer 1 Address: "192.168.12.1"`

xConfiguration DNS PerDomainServer [1..5] Domain1: <S: 0, 39>

The first domain name to be resolved by this particular DNS server.

Example: `xConfiguration DNS PerDomainServer 1 Domain1: "dept.example.com"`

xConfiguration DNS PerDomainServer [1..5] Domain2: <S: 0, 39>

The second domain name to be resolved by this particular DNS server.

Example: `xConfiguration DNS PerDomainServer 1 Domain2: "other.example.com"`

xConfiguration DNS Server [1..5] Address: <S: 0, 39>

The IP address of a default DNS server to use when resolving domain names. You can specify up to 5 servers. These default DNS servers are used if there is no per-domain DNS server defined for the domain being looked up.

Example: `xConfiguration DNS Server 1 Address: "192.168.12.0"`

xConfiguration EdgeConfigServer CredentialTtl: <0..604800>

Does not apply to SSO authentications.

Specifies the lifetime of the authentication token issued by the Expressway to a successfully authenticated client. A client that successfully authenticates should request a refresh before this token expires, or it will need to re-authenticate.

Example: `xConfiguration EdgeConfigServer CredentialTtl: 28800`

xConfiguration EdgeConfigServer PurgeInterval: <0..604800>

Does not apply to SSO authentications.

Specifies how long the Expressway waits between cache clearing operations. Only expired tokens are removed when the cache is cleared, so this setting is the longest possible time that an expired token can remain in the cache.

Example: `xConfiguration EdgeConfigServer PurgeInterval: 43200`

xConfiguration EdgeConfigServer RateLimitLogins: <0..100>

Limits the number of times that any user's credentials can authorize via VCS per rate control period. Any device using the same user credentials contributes to the number.

After the limit is reached, any further attempts to use these credentials are rejected until the current rate control period expires.

Enter 0 to disable the rate control feature.

Example: `xConfiguration EdgeConfigServer RateLimitLogins: 3`

xConfiguration EdgeConfigServer RateLimitPeriod: <0..86400>

Defines the period (in seconds) over which authorizations are counted. If rate control is enabled, then a user's first authorization starts the counter and the timer. When the rate control period expires, the counter is reset and a new period will start with the user's next authorization.

Enter 0 to disable the rate control feature.

Example: `xConfiguration EdgeConfigServer RateLimitPeriod: 300`

xConfiguration ErrorReport Contact: <S: 0, 128>

An optional contact email address for follow up on incident reports if required.

Example: `xConfiguration ErrorReport Contact: "bob smith"`

xConfiguration ErrorReport CoreDump: <On/Off>

Determines whether diagnostic core dump files are created. Default: On.

Example: `xConfiguration ErrorReport CoreDump: On`

xConfiguration ErrorReport Mode: <On/Off>

Determines whether details of application failures are automatically sent to a web service. Default: Off.

Example: `xConfiguration ErrorReport Mode: Off`

xConfiguration ErrorReport Proxy: <S: 0, 128>

An optional proxy server to use for the HTTP/HTTPS connections to the incident reporting server.

Example: `xConfiguration ErrorReport Proxy: https://proxy_address/submiterror/`

xConfiguration ErrorReport Url: <S: 0, 128>

The URL of the web service to which details of application failures are sent. Default: https://cc-reports.cisco.com/submitapplicationerror/

Example: `xConfiguration ErrorReport Url: https://cc-reports.cisco.com/submitapplicationerror/`

xConfiguration Ethernet [1..2] IP V4 Address: <S: 7,15>

Specifies the IPv4 address of the specified LAN port. Note: you must restart the system for any changes to take effect.

Example: `xConfiguration Ethernet 1 IP V4 Address: "192.168.10.10"`

xConfiguration Ethernet [1..2] IP V4 StaticNAT Address: <S:7,15>

If the Expressway is operating in static NAT mode, this specifies the external public IPv4 address of that static NAT. You must restart the system for any changes to take effect.

Example: `xConfiguration Ethernet 1 IP V4 StaticNAT Address: "64.22.64.85"`

xConfiguration Ethernet [1..2] IP V4 StaticNAT Mode: <On/Off>

Specifies whether the Expressway is located behind a static NAT. You must restart the system for any changes to take effect. Default: Off.

Example: `xConfiguration Ethernet 1 IP V4 StaticNAT Mode: On`

xConfiguration Ethernet [1..2] IP V4 SubnetMask: <S: 7,15>

Specifies the IPv4 subnet mask of the specified LAN port. You must restart the system for any changes to take effect.

Example: `xConfiguration Ethernet 1 IP V4 SubnetMask: "255.255.255.0"`

xConfiguration Ethernet [1..2] IP V6 Address: <S: 0, 39>

Specifies the IPv6 address of the specified LAN port. You must restart the system for any changes to take effect.

Example: `xConfiguration Ethernet 1 IP V6 Address: "2001:db8::1428:57ab"`

xConfiguration Ethernet [1..2] Speed: <Auto/10half/10full/100half/100full/1000full

Sets the speed of the Ethernet link from the specified LAN port. Use Auto to automatically configure the speed. You must restart the system for any changes to take effect. Default: Auto.

Example: `xConfiguration Ethernet 1 Speed: Auto`

xConfiguration ExternalManager Address: <S: 0, 128>

Sets the IP address or Fully Qualified Domain Name (FQDN) of the external manager.

Example: `xConfiguration ExternalManager Address: "192.168.0.0"`

xConfiguration ExternalManager Path: <S: 0, 255>

Sets the URL of the external manager. Default: tms/public/external/management/SystemManagementService.asmx

Example: `xConfiguration ExternalManager Path: "tms/public/external/management/SystemManagementService.asmx"`

xConfiguration ExternalManager Protocol: <HTTP/HTTPS>

The protocol used to connect to the external manager. Default: HTTPS.

Example: `xConfiguration ExternalManager Protocol: HTTPS`

xConfiguration ExternalManager Server Certificate Verification Mode: <On/Off>

Controls whether the certificate presented by the external manager is verified. Default: On.

Example: `xConfiguration ExternalManager Server Certificate Verification Mode: On`

xConfiguration H323 Gatekeeper AutoDiscovery Mode: <On/Off>

Determines whether or not the Expressway responds to gatekeeper discovery requests from endpoints. Default: On.

Example: `xConfiguration H323 Gatekeeper AutoDiscovery Mode: On`

xConfiguration H323 Gatekeeper CallSignaling PortRange End: <1024..65534>

Specifies the upper port in the range to be used by calls once they are established. Default: 19999.

Example: `xConfiguration H323 Gatekeeper CallSignaling PortRange End: 19999`

xConfiguration H323 Gatekeeper CallSignaling PortRange Start: <1024..65534>

Specifies the lower port in the range to be used by calls once they are established. Default: 15000.

Example: `xConfiguration H323 Gatekeeper CallSignaling PortRange Start: 15000`

xConfiguration H323 Gatekeeper CallSignaling TCP Port: <1024..65534>

Specifies the port that listens for H.323 call signaling. Default: 1720.

Example: `xConfiguration H323 Gatekeeper CallSignaling TCP Port: 1720`

xConfiguration H323 Gatekeeper CallTimeToLive: <60..65534>

Specifies the interval (in seconds) at which the Expressway polls the endpoints in a call to verify that they are still in the call. Default: 120.

Example: `xConfiguration H323 Gatekeeper CallTimeToLive: 120`

xConfiguration H323 Gatekeeper Registration RIPAllRequests: <On/Off>

Determines whether the Expressway will respond to H.323 registration request with a Request In Progress message.

Enable this setting if you are experiencing registration timeouts when authenticating registration requests with a remote LDAP directory service. Default: Off

Example: `xConfiguration H323 Gatekeeper Registration RIPAllRequests: Off`

xConfiguration H323 Gatekeeper Registration ConflictMode: <Reject/Overwrite>

How the system behaves if an endpoint attempts to register an alias currently registered from another IP address. Default: Reject.

Reject: denies the registration.

Overwrite: deletes the original registration and replaces it with the new registration.

Example: `xConfiguration H323 Gatekeeper Registration ConflictMode: Reject`

xConfiguration H323 Gatekeeper Registration UDP Port: <1024..65534>

Specifies the port to be used for H.323 UDP registrations. Default: 1719.

Example: `xConfiguration H323 Gatekeeper Registration UDP Port: 1719`

xConfiguration H323 Gatekeeper TimeToLive: <60..65534>

The interval (in seconds) at which an H.323 endpoint must re-register with the Expressway to confirm that it is still functioning. Default: 1800.

Example: `xConfiguration H323 Gatekeeper TimeToLive: 1800`

xConfiguration H323 Gateway CallerId: <IncludePrefix/ExcludePrefix>

Specifies whether the prefix of the ISDN gateway is inserted into the caller's E.164 number presented on the destination endpoint. Including the prefix allows the recipient to directly return the call. Default: ExcludePrefix.

IncludePrefix: inserts the ISDN gateway's prefix into the source E.164 number.

ExcludePrefix: only displays the source E.164 number.

Example: `xConfiguration H323 Gateway CallerId: ExcludePrefix`

xConfiguration H323 Mode: <On/Off>

Determines whether or not the Expressway will provide H.323 gatekeeper functionality. Default: Off.

Example: `xConfiguration H323 Mode: On`

xConfiguration Interworking BFCP Compatibility Mode: <Auto/TAA/Draft>

Controls the compatibility settings of the SIP to H.323 interworking BFCP component. Default: Auto.

Example: `xConfiguration Interworking BFCP Compatibility Mode: Auto`

xConfiguration Interworking Encryption KeySize2048: <On/Off>

Determines whether or not the Expressway includes 2048-bit Diffie-Hellman keys for encryption of H.323-SIP interworking. Default: On.

On: Expressway will offer both 1024-bit and 2048-bit encryption key lengths.

Off: Expressway will not offer 2048-bit encryption key length.

Example: `xConfiguration Interworking Encryption KeySize2048: On`

xConfiguration Interworking Encryption Mode: <Auto/Off>

Determines whether or not the Expressway will allow encrypted calls between SIP and H.323 endpoints. Default: Auto.

Off: interworked calls will never be encrypted.

Auto: interworked calls will be encrypted if the endpoints request it.

Example: `xConfiguration Interworking Encryption Mode: Auto`

xConfiguration Interworking Encryption Replay Protection Mode: <On/Off>

Controls whether the Expressway will perform replay protection for incoming SRTP packets when interworking a call. Default: Off.

On: replayed SRTP packets will be dropped by the Expressway.

Off: the Expressway will not check for replayed SRTP packets.

Example: `xConfiguration Interworking Encryption Replay Protection Mode: Off`

xConfiguration Interworking Mode: <On/Off/RegisteredOnly>

Determines whether or not the Expressway will act as a gateway between SIP and H.323 calls. Default: RegisteredOnly.

Off: the Expressway will not act as a SIP-H.323 gateway.

On: the Expressway will act as SIP-H.323 gateway regardless of whether the endpoints are locally registered.

RegisteredOnly: the Expressway will act as a SIP-H.323 gateway but only if at least one of the endpoints is locally registered.

Example: `xConfiguration Interworking Mode: On`

xConfiguration Interworking Require Invite Header Mode: <On/Off>

Controls whether the SIP to H.323 interworking function sends com.tandberg.sdp.duo.enable and com.tandberg.sdp.bfcp.udp in the require header for dialog forming INVITEs. Default: Off.

Example: `xConfiguration Interworking Require Invite Header Mode: Off`

xConfiguration IP DNS Domain Name: <S: 0, 128>

The name to be appended to an unqualified host name before querying the DNS server. Used when attempting to resolve unqualified domain names for NTP, LDAP, external manager and remote syslog servers. May also be used along with the **System host name** to identify references to this Expressway in SIP messaging.

Example: `xConfiguration IP DNS Domain Name: "example.com"`

xConfiguration IP DNS Hostname : <S: 0, 63>

The DNS host name that this system is known by. This is not the fully-qualified domain name, just the host label portion. The name can only contain letters, digits, hyphens and underscores. The first character must be a letter and the last character must be a letter or a digit.

Example: `xConfiguration IP DNS Hostname: "localsystem"`

xConfiguration IP DNS MaxPort: <1024..65535>

The upper source port in the range used for sending DNS queries. Requests choose a random port from this range. Warning: setting a small source port range increases your vulnerability to DNS spoofing attacks. Default: 65535.

Example: `xConfiguration IP DNS MaxPort: 65535`

xConfiguration IP DNS MinPort: <1024..65535>

The lower source port in the range used for sending DNS queries. Requests choose a random port from this range. Warning: setting a small source port range increases your vulnerability to DNS spoofing attacks. Default: 1024.

Example: `xConfiguration IP DNS MinPort: 1024`

xConfiguration IP DNS SearchDomains: <S: 0, 1024>

Space separated list of extra domain names to be searched when querying the DNS server. Used when attempting to resolve unqualified domain names for NTP, LDAP, external manager and remote syslog servers. May also be used along with the local System host name to identify references to this system in SIP messaging. (Peer-specific)

Example: `xConfiguration IP DNS SearchDomains: "example1.int" "example2.int" "example3.int"`

xConfiguration IP DNS UseEphemeralPortRange: <On/Off>

Determines whether outgoing DNS queries use the system's normal ephemeral port range, or a custom port range that you can configure. Default: On.

Example: `xConfiguration IP DNS UseEphemeralPortRange: On`

xConfiguration IP Ephemeral PortRange End: <1024..65534>

The highest port in the range used for ephemeral outbound connections not otherwise constrained by Expressway call processing. Default: 35999.

Example: `xConfiguration IP Ephemeral PortRange End: 35999`

xConfiguration IP Ephemeral PortRange Start: <1024..65534>

The lowest port in the range used for ephemeral outbound connections not otherwise constrained by Expressway call processing. Default: 30000.

Example: `xConfiguration IP Ephemeral PortRange Start: 30000`

xConfiguration IP External Interface: <LAN1/LAN2>

Defines which LAN interface is externally facing. Default: LAN1.

Example: `xConfiguration IP External Interface: LAN1`

xConfiguration IP Gateway: <S: 7,15>

Specifies the IPv4 gateway of the Expressway. Note: you must restart the system for any changes to take effect. Default: 127.0.0.1

Example: `xConfiguration IP Gateway: "192.168.127.0"`

xConfiguration IP QoS Mode: <None/DiffServ>

The type of QoS (Quality of Service) tags to apply to all signaling and media packets. You must restart the system for any changes to take effect. Default: None.

None: no specific QoS tagging is applied.

DiffServ: puts the specified Tag value in the TOS (Type Of Service) field of the IPv4 header or TC (Traffic Class) field of the IPv6 header.

Example: `xConfiguration IP QoS Mode: DiffServ`

Important This command is discontinued from Version X8.9 and replaced by commands `QoS Audio`, `QoS Video`, `QoS XMPP`, and `QoS Signaling`.

xConfiguration IP QoS Value: <0..63>

The value to stamp onto all signaling and media traffic routed through the system. You must restart the system for any changes to take effect. Default: 0.

Example: `xConfiguration IP QoS Value: 16`

Important This command is discontinued from Version X8.9 and replaced by commands `QoS Audio`, `QoS Video`, `QoS XMPP`, and `QoS Signaling`.

xConfiguration IP RFC4821 Mode: <Auto/Enabled/Disabled>

Determines when RFC4821 Packetization Layer Path MTU Discovery is used by the Expressway network interface. You must restart the system for any changes to take effect. Default: Disabled.

Enabled: Packetization layer MTU probing is always performed.

Auto: Disabled by default, enabled when an ICMP black hole is detected.

Disabled: Packetization layer MTU probing is not performed.

Example: `xConfiguration IP RFC4821 Mode: Disabled`

xConfiguration IP Route [1..50] Address: <S: 0, 39>

Specifies an IP address used in conjunction with the Prefix Length to determine the network to which this route applies.

Example: `xConfiguration IP Route 1 Address: "128.168.0.0"`

xConfiguration IP Route [1..50] Gateway: <S: 0, 39>

Specifies the IP address of the Gateway for this route.

Example: `xConfiguration IP Route 1 Gateway: "192.168.0.0"`

xConfiguration IP Route [1..50] Interface: <Auto/LAN1/LAN2>

Specifies the LAN interface to use for this route. Auto: The Expressway will select the most appropriate interface to use. Default: Auto.

Example: `xConfiguration IP Route 1 Interface: Auto`

xConfiguration IP Route [1..50] PrefixLength: <0..128>

The number of bits of the IP address which must match when determining the network to which this route applies. Default: 32.

Example: `xConfiguration IP Route 1 PrefixLength: 16`

xConfiguration IP V6 Gateway: <S: 0, 39>

Specifies the IPv6 gateway of the Expressway. You must restart the system for any changes to take effect.

Example: `xConfiguration IP V6 Gateway: "3dda:80bb:6::9:144"`

xConfiguration IPProtocol: <Both/IPv4/IPv6>

Selects whether the Expressway is operating in IPv4, IPv6 or dual stack mode. You must restart the system for any changes to take effect. Default: IPv4.

Example: `xConfiguration IPProtocol: IPv4`

xConfiguration Language Default: <S: 0, 128>

The default language used on the web interface. Default: "en_US".

Example: `xConfiguration Language Default: "en_US"`

xConfiguration Log CDR Service: <off/serviceonly/serviceandlogging>

Select how to log Call Detail Records produced by this Expressway.

Off: Call Detail Records are not logged.

serviceonly: Call Detail Records are stored locally for 7 days and then deleted. The logged records are not accessible via the user interface.

serviceandlogging: As for serviceonly, except the CDRs are accessible via the local Event log. If you have added syslog server addresses, the records are sent to those as Info messages.

Default: *off*

Example: `xConfiguration Log CDR Service: serviceonly`

xConfiguration Log Level: <1..4>

Controls the granularity of Event Logging. 1 is the least verbose, 4 the most. Note: this setting is not retrospective; it determines which events are written to the Event Log from now onwards. Default: 1

Example: `xConfiguration Log Level: 1`

xConfiguration Log MediaStats Logging: <On/Off>

Toggles media statistics logging. Default: Off

Example: `xConfiguration Log MediaStats Logging: On`

xConfiguration Log SystemMetrics Interval: <30..600>

Sets the number of seconds to wait between metrics collection events.

Important A shorter interval has more impact on system performance, while a longer interval yields coarser metrics. We recommend using the longest interval unless you need very fine metrics.

Default: 60

Example: `xConfiguration Log SystemMetrics Interval: 60`

xConfiguration Log SystemMetrics Mode: <On/Off>

Toggles the System Metrics Collection service. Enter On to start collecting metrics for this system.

Default: *Off*

Example: `xConfiguration Log SystemMetrics Mode: On`

xConfiguration Log SystemMetrics Network Address: <S: 0,1024>

Enter the address of the listening server. You may use IP address, hostname, or FQDN.

Default: *Empty*

Example: `xConfiguration log SystemMetrics Network Address: "192.168.0.5"`

xConfiguration Log SystemMetrics Network Port: <1..65535>

Enter the port on which the listening server is expecting System Metrics traffic.

Default: *25826*

Example: `xConfiguration log SystemMetrics Network Port: 25826`

xConfiguration Logger Network [1..n] Level: <FATAL/ERROR/WARN/INFO/DEBUG/TRACE>

The logging level for the nominated module. Default : INFO.

Example: `xConfiguration Logger Developer 1 Level: INFO`

xConfiguration Login Remote LDAP BaseDN Accounts: <S: 0,255>

Sets the Distinguished Name to use as the base when searching for administrator and user accounts.

Example: `xConfiguration Login Remote LDAP BaseDN Accounts: "ou=useraccounts,dc=corporation,dc=int"`

xConfiguration Login Remote LDAP BaseDN Groups: <S: 0,255>

Sets the Distinguished Name to use as the base when searching for administrator and user groups.

Example: `xConfiguration Login Remote LDAP BaseDN Groups: "ou=groups,dc=corporation,dc=int"`

xConfiguration Login Remote LDAP CRLCheck: <None/Peer/All>

Specifies whether certificate revocation lists (CRLs) are checked when forming a TLS connection with the LDAP server. CRL data is uploaded to the Expressway via the trusted CA certificate PEM file. Default: None.

None: no CRL checking is performed.

Peer: only the CRL associated with the CA that issued the LDAP server's certificate is checked.

All: all CRLs in the trusted certificate chain of the CA that issued the LDAP server's certificate are checked.

Example: `xConfiguration Login Remote LDAP CRLCheck: Peer`

xConfiguration Login Remote LDAP DirectoryType: <ActiveDirectory>

Defines the type of LDAP directory that is being accessed. Default: ActiveDirectory.

ActiveDirectory: directory is Windows Active Directory.

Example: `xConfiguration Login Remote LDAP DirectoryType: ActiveDirectory`

xConfiguration Login Remote LDAP Encryption: <Off/TLS>

Sets the encryption to use for the connection to the LDAP server. Default: TLS.

Off: no encryption is used.

TLS: TLS encryption is used.

Example: `xConfiguration Login Remote LDAP Encryption: Off`

xConfiguration Login Remote LDAP SASL: <None/DIGEST-MD5>

The SASL (Simple Authentication and Security Layer) mechanism to use when binding to the LDAP server. Default: DIGEST-MD5.

None: no mechanism is used.

DIGEST-MD5: The DIGEST-MD5 mechanism is used.

Example: `xConfiguration Login Remote LDAP SASL: DIGEST-MD5`

xConfiguration Login Remote LDAP SearchOptimize NestedDepth: <1..16>

Sets the subgroup search depth level for LDAP authentication. Default: 16

Example: `xConfiguration Login Remote LDAP SearchOptimize NestedDepth: "1"`

xConfiguration Login Remote LDAP SearchOptimize SkipMembers: <Yes/No>

Defines whether to skip group member lookup when searching groups for LDAP authentication. Default: Yes

Example: `xConfiguration Login Remote LDAP SearchOptimize SkipMembers: "No"`

xConfiguration Login Remote LDAP Server Address: <S: 0,128>

Sets the IP address or Fully Qualified Domain Name (FQDN) of the LDAP server to use when making LDAP queries.

Example: `xConfiguration Login Remote LDAP Server Address: "server.example.com"`

xConfiguration Login Remote LDAP Server FQDNResolution: <AddressRecord/SRVRecord>

Sets how the LDAP server address is resolved if specified as an FQDN. Default: AddressRecord.

AddressRecord: DNS A or AAAA record lookup.

SRVRecord: DNS SRV record lookup.

Example: `xConfiguration Login Remote LDAP Server FQDNResolution: AddressRecord`

xConfiguration Login Remote LDAP Server Port: <1..65534>

Sets the IP port of the LDAP server to use when making LDAP queries. Non-secure connections use 389 and secure connections use 636. Other ports are not supported. Default: 389.

Example: `xConfiguration Login Remote LDAP Server Port: 389`

xConfiguration Login Remote LDAP VCS BindDN: <S: 0,255>

Sets the user distinguished name to use when binding to the LDAP server.

Example: `xConfiguration Login Remote LDAP VCS BindDN: "systemmanager"`

xConfiguration Login Remote LDAP VCS BindPassword: <S: 0,122>

Sets the password to use when binding to the LDAP server. The maximum plaintext length is 60 characters, which is then encrypted.

Example: `xConfiguration Login Remote LDAP VCS BindPassword: "password123"`

xConfiguration Login Remote LDAP VCS BindUsername: <S: 0,255>

Sets the username to use when binding to the LDAP server. Only applies if using SASL.

Example: `xConfiguration Login Remote LDAP VCS BindUsername: "systemmanager"`

xConfiguration Login Remote Protocol: <LDAP>

The protocol used to connect to the external directory. Default: LDAP.

Example: `xConfiguration Login Remote Protocol: LDAP`

xConfiguration Login Source Admin: <LocalOnly/RemoteOnly/Both>

Defines where administrator login credentials are authenticated before access is allowed. Default: LocalOnly.

LocalOnly: credentials are verified against a local database stored on the Expressway.

RemoteOnly: credentials are verified against an external credentials directory, for example Windows Active Directory. Note that this disables login access via the default admin account.

Both: credentials are verified first against a local database stored on the Expressway, and then if no matching account is found the external credentials directory is used instead.

Example: `xConfiguration Login Source Admin: LocalOnly`

xConfiguration Login User [1..n] Name: <S: 0,60>

Defines the name for this entry in the local authentication database.

Example: `xConfiguration Login User 1 Name: "alice"`

xConfiguration Login User [1..n] Password: <S: 0,128>

Defines the password for this entry in the local authentication database.

Example: `xConfiguration Login User 1 Password: "abcXYZ_123"`

xConfiguration Management Interface HstsMode: <On/Off>

Determines whether web browsers are instructed to only ever use a secure connection to access this server. Enabling this feature gives added protection against man-in-the-middle (MITM) attacks. Default: On.

On: the Strict-Transport-Security header is sent with all responses from the web server, with a 1 year expiry time.

Off: the Strict-Transport-Security header is not sent, and browsers work as normal. Note: you must restart the system for any changes to take effect.

Example: `xConfiguration Management Interface HstsMode: On`

xConfiguration Management Interface Port: <1..65535>

Sets the https listening port for administrators to access the Expressway web interface. Default: 443.

Example: `xConfiguration Management Interface Port: 7443`

Warning Check if you can access the Expressway Web Interface port using your Browser. If the Browser is unresponsive, it means that you cannot administer using the Web Interface. Ensure that the Firewall or any other security equipment in your network do not block the specified port. The ports offered in the Web Interface (443, 445, 7443, 9000) are likely to work in most networks.

xConfiguration Management Session InactivityTimeout: <0..65535>

Sets the number of minutes that an administration session (serial port, HTTPS or SSH) may be inactive before the session is timed out. A value of 0 turns session time outs off. Default: 30.

Example: `xConfiguration Management Session InactivityTimeout: 30`

xConfiguration Management Session MaxConcurrentSessionsTotal: <0..65535>

The maximum number of concurrent administrator sessions allowed on the system. This includes web, SSH and serial sessions. A value of 0 turns session limits off. Default: 0.

Example: `xConfiguration Management Session MaxConcurrentSessionsTotal: 0`

xConfiguration Management Session MaxConcurrentSessionsUser: <0..65535>

The number of concurrent sessions that each individual administrator account is allowed on the system. This includes web, SSH and serial sessions. A value of 0 turns session limits off. Default: 0.

Example: `xConfiguration Management Session MaxConcurrentSessionsUser: 0`

xConfiguration NetworkLimits

Configures the experimental rate limiting feature. Enter `xconfig networklimits ?` to read the help.

Example: `xConfiguration NetworkLimits Configuration GarbageCollectSecs: 5`

xConfiguration NTP Server [1..5] Address: <S: 0, 128>

Sets the IP address or Fully Qualified Domain Name (FQDN) of up to 5 NTP servers to be used when synchronizing system time.

Example: `xConfiguration NTP Server 1 Address: "ntp.server.example.com"`

xConfiguration Option [1..64] Key: <S: 0, 90>

Specifies the option key of your software option. These are added to the system in order to add extra functionality, such as increasing the system's capacity. Contact your Cisco support representative for further information.

Example: `xConfiguration Option 1 Key: "1X4757T5-1-60BAD5CD"`

xConfiguration Policy AdministratorPolicy Mode: <Off/LocalCPL/LocalService/PolicyService>

Enables and disables use of Call Policy. Default: Off.

Off: Disables call policy.

LocalCPL: uses policy from an uploaded CPL file.

LocalService: uses group policy information and a local file.

PolicyService: uses an external policy server.

Example: `xConfiguration Policy AdministratorPolicy Mode: Off`

xConfiguration Policy AdministratorPolicy Service DefaultCPL: <S: 0,255>

The CPL used by the Expressway when the remote service is unavailable. Default: <reject status='403' reason='Service Unavailable'/>

Example: `xConfiguration Policy AdministratorPolicy Service DefaultCPL: "<reject status='403' reason='Service Unavailable'/>"`

xConfiguration Policy AdministratorPolicy Service Password: <S: 0,82>

Specifies the password used by the Expressway to log in and query the remote service. The maximum plaintext length is 30 characters, which will then be encrypted.

Example: `xConfiguration Policy AdministratorPolicy Service Password: "password123"`

xConfiguration Policy AdministratorPolicy Service Path: <S: 0,255>

Specifies the URL of the remote service.

Example: `xConfiguration Policy AdministratorPolicy Service Path: "service"`

xConfiguration Policy AdministratorPolicy Service Protocol: <HTTP/HTTPS>

Specifies the protocol used to connect to the remote service. Default: HTTPS.

Example: `xConfiguration Policy AdministratorPolicy Service Protocol: HTTPS`

xConfiguration Policy AdministratorPolicy Service Server [1..3] Address: <S: 0,128>

Specifies the IP address or Fully Qualified Domain Name (FQDN) of the remote service.

Example: `xConfiguration Policy AdministratorPolicy Service Server 1 Address: "service.server.example.com"`

xConfiguration Policy AdministratorPolicy Service Status Path: <S: 0..255>

Specifies the path for obtaining the remote service status. Default: status

Example: `xConfiguration Policy AdministratorPolicy Service Status Path: status`

xConfiguration Policy AdministratorPolicy Service TLS CRLCheck Mode: <On/Off>

Controls certificate revocation list checking of the certificate supplied by the policy service. When enabled, the server's X.509 certificate will be checked against the revocation list of the certificate authority of the certificate. Default: Off.

Example: `xConfiguration Policy AdministratorPolicy Service TLS CRLCheck Mode: Off`

xConfiguration Policy AdministratorPolicy Service TLS Verify Mode: <On/Off>

Controls X.509 certificate checking and mutual authentication between this Expressway and the policy service. When enabled, the server's FQDN or IP address, as specified in the address field, must be contained within the server's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes). Default: On.

Example: `xConfiguration Policy AdministratorPolicy Service TLS Verify Mode: On`

xConfiguration Policy AdministratorPolicy Service UserName: <S: 0,30>

Specifies the user name used by the Expressway to log in and query the remote policy service.

Example: `xConfiguration Policy AdministratorPolicy Service UserName: "user123"`

xConfiguration Policy FindMe CallerID: <FindMeID/IncomingID>

Determines how the source of an incoming call is presented to the callee. Default: IncomingID.

IncomingID: displays the address of the endpoint from which the call was placed.

FindMeID: displays the FindMe ID associated with the originating endpoint's address.

Example: `xConfiguration Policy FindMe CallerId: FindMeID`

xConfiguration Policy FindMe Mode: <Off/On/ThirdPartyManager>

Configures how the FindMe application operates. Default: Off.

Off: disables FindMe.

On: enables FindMe.

ThirdPartyManager: uses an off-box, third-party FindMe manager.

Example: `xConfiguration Policy FindMe Mode: On`

xConfiguration Policy FindMe Server Address: <S: 0, 128>

Specifies the IP address or Fully Qualified Domain Name (FQDN) of the remote FindMe Manager.

Example: `xConfiguration Policy FindMe Server Address: "userpolicy.server.example.com"`

xConfiguration Policy FindMe Server Password: <S: 0, 82>

Specifies the password used by the Expressway to log in and query the remote FindMe Manager. The maximum plaintext length is 30 characters, which will then be encrypted.

Example: `xConfiguration Policy FindMe Server Password: "password123"`

xConfiguration Policy FindMe Server Path: <S: 0, 255>

Specifies the URL of the remote FindMe Manager.

Example: `xConfiguration Policy FindMe Server Path: "service"`

xConfiguration Policy Services Service [1..20] DefaultCPL: <S: 0,255>

The CPL used by the Expressway when the remote service is unavailable. Default: <reject status='504' reason='Policy Service Unavailable'/>

Example: `xConfiguration Policy Services Service 1 DefaultCPL: "<reject status='403' reason='Service Unavailable'/>"`

xConfiguration Policy Services Service [1..20] Description: <S: 0,64>

A free-form description of the Policy Service.

Example: `xConfiguration Policy Services Service 1 Description: "Conference management service"`

xConfiguration Policy Services Service [1..20] HTTPMethod: <POST/GET>

Specifies the HTTP method type to use for the remote service. Default: POST.

Example: `xConfiguration Policy Services Service 1 HTTPMethod: POST`

xConfiguration Policy Services Service [1..20] Name: <S: 0,50>

Assigns a name to this Policy Service.

Example: `xConfiguration Policy Services Service 1 Name: "Conference handler"`

xConfiguration Policy Services Service [1..20] Password: <S: 0,82>

Specifies the password used by the Expressway to log in and query the remote service. The maximum plaintext length is 30 characters, which will then be encrypted.

Example: `xConfiguration Policy Services Service 1 Password: "password123"`

xConfiguration Policy Services Service [1..20] Path: <S: 0,255>

Specifies the URL of the remote service.

Example: `xConfiguration Policy Services Service 1 Path: "service"`

xConfiguration Policy Services Service [1..20] Protocol: <HTTP/HTTPS>

Specifies the protocol used to connect to the remote service. Default: HTTPS.

Example: `xConfiguration Policy Services Service 1 Protocol: HTTPS`

xConfiguration Policy Services Service [1..20] Server [1..3] Address: <S: 0,128>

Specifies the IP address or Fully Qualified Domain Name (FQDN) of the remote service.

Example: `xConfiguration Policy Services Service 1 Server 1 Address: "192.168.0.0"`

xConfiguration Policy Services Service [1..20] Status Path: <S: 0..255>

Specifies the path for obtaining the remote service status. Default: status

Example: `xConfiguration Policy Services Service 1 Status Path: status`

xConfiguration Policy Services Service [1..20] TLS CRLCheck Mode: <On/Off>

Controls certificate revocation list checking of the certificate supplied by the policy service. When enabled, the server's X.509 certificate will be checked against the revocation list of the certificate authority of the certificate. Default: Off.

Example: `xConfiguration Policy Services Service 1 TLS CRLCheck Mode: Off`

xConfiguration Policy Services Service [1..20] TLS Verify Mode: <On/Off>

Controls X.509 certificate checking and mutual authentication between this Expressway and the policy service. When enabled, the server's FQDN or IP address, as specified in the address field, must be contained within the server's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes). Default: On.

Example: `xConfiguration Policy Services Service 1 TLS Verify Mode: On`

xConfiguration Policy Services Service [1..20] UserName: <S: 0,30>

Specifies the user name used by the Expressway to log in and query the remote service.

Example: `xConfiguration Policy Services Service 1 UserName: "user123"`

xConfiguration QoS Audio <0..63>

Defines a DSCP (Differentiated Service Code Point) value for Quality of Service marking of audio traffic. The DSCP value is stamped (marked) onto SIP and H.323 audio media traffic routed through the Expressway, by writing it to the IP packet headers. To the ToS field for IPv4 or to the TC field for IPv6. A value of "0" specifies standard best effort service. Default: 46.

You must restart the system for any changes to take effect.

Example: `xConfiguration QoS Audio: 30`

xConfiguration QoS Video <0..63>

Defines a DSCP value for Quality of Service marking of video traffic. The DSCP value is stamped (marked) onto SIP and H.323 video media traffic routed through the Expressway, by writing it to the IP packet headers. To the ToS field for IPv4 or to the TC field for IPv6. A value of "0" specifies standard best effort service. Default: 34.

You must restart the system for any changes to take effect.

Example: `xConfiguration QoS Video: 43`

xConfiguration QoS XMPP <0..63>

Defines a DSCP value for Quality of Service marking of IM & Presence traffic. The DSCP value is stamped (marked) onto XMPP traffic routed through the Expressway, by writing it to the IP packet headers. To the ToS field for IPv4 or to the TC field for IPv6. A value of "0" specifies standard best effort service. Default: 24.

You must restart the system for any changes to take effect.

Example: `xConfiguration QoS XMPP: 34`

xConfiguration QoS Signaling <0..63>

Defines a DSCP value for Quality of Service marking of signaling traffic. The DSCP value is stamped (marked) onto SIP and H.323 signaling traffic routed through the Expressway, by writing it to the IP packet headers. To the ToS field for IPv4 or to the TC field for IPv6. A value of "0" specifies standard best effort service. Default: 24.

You must restart the system for any changes to take effect.

Example: `xConfiguration QoS Signaling: 34`

xConfiguration Registration AllowList [1..2500] Description: <S: 0,64>

A free-form description of the Allow List rule.

Example: `xConfiguration Registration AllowList 1 Description: "Everybody at @example.com"`

xConfiguration Registration AllowList [1..2500] Pattern String: <S: 0, 60>

Specifies an entry to be added to the Allow List. If one of an endpoint's aliases matches one of the patterns in the Allow List, the registration will be permitted.

Example: `xConfiguration Registration AllowList 1 Pattern String: "john.smith@example.com"`

xConfiguration Registration AllowList [1..2500] Pattern Type: <Exact/Prefix/Suffix/Regex>

Specifies whether the entry in the Allow List is a prefix, suffix, regular expression, or must be matched exactly. Default: Exact.

Exact: the string must match the alias character for character.

Prefix: the string must appear at the beginning of the alias.

Suffix: the string must appear at the end of the alias.

Regex: the string will be treated as a regular expression.

Example: `xConfiguration Registration AllowList 1 Pattern Type: Exact`

xConfiguration Registration AllowList [1..2500] Pattern Type: <Exact/Prefix/Suffix/Regex>

Specifies whether the entry in the Allow List is a prefix, suffix, regular expression, or must be matched exactly. Default: Exact.

Exact: the string must match the alias character for character.

Prefix: the string must appear at the beginning of the alias.

Suffix: the string must appear at the end of the alias.

Regex: the string will be treated as a regular expression.

Example: `xConfiguration Registration AllowList 1 Pattern Type: Exact`

xConfiguration Registration DenyList [1..2500] Description: <S: 0,64>

A free-form description of the Deny List rule.

Example: `xConfiguration Registration DenyList 1 Description: "Anybody at @nuisance.com"`

xConfiguration Registration DenyList [1..2500] Pattern String: <S: 0, 60>

Specifies an entry to be added to the Deny List. If one of an endpoint's aliases matches one of the patterns in the Deny List, the registration will not be permitted.

Example: `xConfiguration Registration DenyList 1 Pattern String: "john.jones@example.com"`

xConfiguration Registration DenyList [1..2500] Pattern Type: <Exact/Prefix/Suffix/Regex>

Specifies whether the entry in the Deny List is a prefix, suffix, regular expression, or must be matched exactly. Default: Exact.

Exact: the string must match the alias character for character.

Prefix: the string must appear at the beginning of the alias.

Suffix: the string must appear at the end of the alias.

Regex: the string will be treated as a regular expression.

Example: `xConfiguration Registration DenyList 1 Pattern Type: Exact`

xConfiguration Registration RestrictionPolicy Mode: <None/AllowList/DenyList/Directory/PolicyService>

Specifies the policy to be used when determining which endpoints may register with the system. Default: None.

None: no restriction.

AllowList: only endpoints attempting to register with an alias listed on the Allow List may register.

DenyList: all endpoints, except those attempting to register with an alias listed on the Deny List, may register.

Directory: only endpoints who register an alias listed in the local Directory, may register.

PolicyService: only endpoints who register with details allowed by the Policy Service, may register.

Example: `xConfiguration Registration RestrictionPolicy Mode: None`

xConfiguration Registration RestrictionPolicy Service DefaultCPL: <S: 0,255>

The CPL used by the Expressway when the remote service is unavailable. Default: <reject status='504' reason='Policy Service Unavailable'/>

Example: `xConfiguration Registration RestrictionPolicy Service DefaultCPL: "<reject status='403' reason='Service Unavailable'/>"`

xConfiguration Registration RestrictionPolicy Service Password: <S: 0,82>

Specifies the password used by the Expressway to log in and query the remote service. The maximum plaintext length is 30 characters, which will then be encrypted.

Example: `xConfiguration Registration RestrictionPolicy Service Password: "password123"`

xConfiguration Registration RestrictionPolicy Service Path: <S: 0,255>

Specifies the URL of the remote service.

Example: `xConfiguration Registration RestrictionPolicy Service Path: "service"`

xConfiguration Registration RestrictionPolicy Service Protocol: <HTTP/HTTPS>

Specifies the protocol used to connect to the remote service. Default: HTTPS.

Example: `xConfiguration Registration RestrictionPolicy Service Protocol: HTTPS`

xConfiguration Registration RestrictionPolicy Service Server [1..3] Address: <S: 0,128>

Specifies the IP address or Fully Qualified Domain Name (FQDN) of the remote service.

Example: `xConfiguration Registration RestrictionPolicy Service Server 1 Address: "192.168.0.0"`

xConfiguration Registration RestrictionPolicy Service Status Path: <S: 0..255>

Specifies the path for obtaining the remote service status. Default: status

Example: `xConfiguration Registration RestrictionPolicy Service Status Path: status`

xConfiguration Registration RestrictionPolicy Service TLS CRLCheck Mode: <On/Off>

Controls certificate revocation list checking of the certificate supplied by the policy service. When enabled, the server's X.509 certificate will be checked against the revocation list of the certificate authority of the certificate. Default: Off.

Example: `xConfiguration Registration RestrictionPolicy Service TLS CRLCheck Mode: Off`

xConfiguration Registration RestrictionPolicy Service TLS Verify Mode: <On/Off>

Controls X.509 certificate checking and mutual authentication between this Expressway and the policy service. When enabled, the server's FQDN or IP address, as specified in the address field, must be contained within the server's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes). Default: On.

Example: `xConfiguration Registration RestrictionPolicy Service TLS Verify Mode: On`

xConfiguration Registration RestrictionPolicy Service UserName: <S: 0,30>

Specifies the user name used by the Expressway to log in and query the remote service.

Example: `xConfiguration Registration RestrictionPolicy Service UserName: "user123"`

xConfiguration Remote Syslog [1..4] Address: <S: 0..128>

The IP address or Fully Qualified Domain Name (FQDN) of up to 4 remote syslog servers to which the log is written. These servers must support the BSD or IETF syslog protocols.

Example: `xConfiguration Remote Syslog 1 Address: "remote_server.example.com"`

xConfiguration Remote Syslog [1..4] Crlcheck: <On/Off>

Controls whether the certificate supplied by the syslog server is checked against the certificate revocation list (CRL). Default: Off.

Example: `xConfiguration Remote Syslog 1 Crlcheck: Off`

xConfiguration Remote Syslog [1..4] Format: <bsd/ietf>

The format in which remote syslog messages are written. Default: bsd.

Example: `xConfiguration Remote Syslog 1 Format: bsd`

xConfiguration Remote Syslog [1..4] Loglevel: <emergency/alert/critical/error/warning/notice/informational/debug>

Select the minimum severity of log messages to send to this syslog server. Default: informational.

Example: `xConfiguration Remote Syslog 1 Loglevel: informational`

xConfiguration Remote Syslog [1..4] Mode: <bsd/ietf/ietf_secure/user_defined>

Select the syslog protocol to use when sending messages to the syslog server, or choose user_defined to configure individually the transport type, port and format. Default: bsd.

Example: `xConfiguration Remote Syslog 1 Mode: bsd`

xConfiguration Remote Syslog [1..4] Port: <1..65535>

The UDP/TCP destination port to use. Suggested ports: UDP=514 TCP/TLS=6514. Default : 514.

Example: `xConfiguration Remote Syslog 1 Port: 514`

xConfiguration Remote Syslog [1..4] Transport: <udp/tcp/tls>

The transport protocol to use when communicating with the syslog server. If you use TLS encryption, you must upload a suitable CA certificate file. Default: UDP.

Example: `xConfiguration Remote Syslog 1 Transport: udp`

xConfiguration ResourceUsage Warning Activation Level: <0..100>

Controls if and when the Expressway will warn that it is approaching its maximum licensed capacity for calls or registrations. The number represents the percentage of the maximum that, when reached, will trigger a warning. 0: Warnings will never appear. Default: 90.

Example: `xConfiguration ResourceUsage Warning Activation Level: 90`

xConfiguration Security CSRFProtection Status: "Disabled"

Use this command to disable (if enabled) CSRF Protection, that is, disable the usage of the header 'X-CSRF-Header' for CDB Rest, XMLPut, and SOAP API.

Default: Disabled

xConfiguration Security CSRFProtection Status: "Enabled"

Use this command to enable CSRF Protection, which enables the usage of header 'X-CSRF-Header' for CDB Rest, XMLPut, and SOAP API.

xConfiguration SIP Advanced BibInviteDelay: <1..5000>

Specifies the maximum delay of a SIP BIB invite message that the server must handle (in milliseconds).

Default: 0

Example: `xConfiguration SIP Advanced BibInviteDelay: 1000`

xConfiguration SIP Advanced BusytoneReferDelay: <0..2000>

Specifies the maximum delay of a SIP REFER message . It contains DtLineBusyTone during initial call dialog (ensure SIP messages proceeds in a sequence) that the server can handle (in milliseconds).

Expressway processes and sends SIP messages (REFER contain DtLineBusyTone parameter and 183 Session Progress), which causes Jabber Over MRA to intermittently play Ringing Tone instead of Busy Tone

Default: 0

Recommend adjust delay between 100-200 milliseconds.

Example: `xConfiguration SIP Advanced BusytoneReferDelay: <0..2000>`

xConfiguration SIP Advanced SipMaxSize: <1..1048576>

Specifies the maximum size of a SIP message that can be handled by the server (in bytes). Default: `32768`

Example: `xConfiguration SIP Advanced SipMaxSize: 32768`

xConfiguration SIP Advanced SipTcpConnectTimeout: <1..150>

Enter the maximum number of seconds to wait for an outgoing SIP TCP connection to be established. Default: 10.

Example: `xConfiguration SIP Advanced SipTcpConnectTimeout: 10`

xConfiguration SIP Advanced SipTlsDhKeySize: <1024/2048/3072>

Specifies the default key size for inbound connections that use Diffie-Hellman key exchange (in bits).

Default: 1024.

Note You must restart the system for any changes to take effect.

Example: `xConfiguration SIP Advanced SipTlsDhKeySize: 1024`

xConfiguration SIP Advanced SipTlsVersions: <TLSv1/TLSv1.1/TLSv1.2/TLSv1:TLSv1.1/TLSv1:TLSv1.2/TLSv1.1:TLSv1.2/TLSv1:TLSv1.1:TLSv1.2>

Specifies the supported SIP TLS protocol versions. Default: TLSv1:TLSv1.1:TLSv1.2

Example: `xConfiguration SIP Advanced SipTlsVersions: TLSv1.1:TLSv1.2`

xConfiguration SIP Authentication Digest Nonce ExpireDelta: <30..3600>

Specifies the maximum time (in seconds) that a nonce may be re-used for. Default: 300.

Example: `xConfiguration SIP Authentication Digest Nonce ExpireDelta: 300`

xConfiguration SIP Authentication Digest Nonce Length: <32..512>

Length of nonce or cnonce to generate for use in SIP Digest authentication. Default: 60.

Example: `xConfiguration SIP Authentication Digest Nonce Length: 60`

xConfiguration SIP Authentication Digest Nonce Limit: <1..65535>

Maximum limit on the number of nonces to store. Default: 10000.

Example: `xConfiguration SIP Authentication Digest Nonce Limit: 10000`

xConfiguration SIP Authentication Digest Nonce Maximum Use Count: <1..1024>

Maximum number of times that a nonce generated by the Expressway may be used by a client. Default: 128.

Example: `xConfiguration SIP Authentication Digest Nonce Maximum Use Count: 128`

xConfiguration SIP Authentication NTLM Mode: <On/Off/Auto>

Controls when the Expressway will challenge endpoints using the NTLM protocol. Default: Auto.

Off: the Expressway will never send a challenge containing the NTLM protocol.

On: the Expressway will always include NTLM in its challenges.

Auto: the Expressway will decide based on endpoint type whether to challenge with NTLM.

Example: `xConfiguration SIP Authentication NTLM Mode: Auto`

xConfiguration SIP Authentication NTLM SA Lifetime: <30..43200>

Specifies the lifetime of NTLM security associations in seconds. Default: 28800.

Example: `xConfiguration SIP Authentication NTLM SA Lifetime: 28800`

xConfiguration SIP Authentication NTLM SA Limit: <1..65535>

Maximum number of NTLM security associations to store. Default: 10000.

Example: `xConfiguration SIP Authentication NTLM SA Limit: 10000`

xConfiguration SIP Authentication Retry Limit: <1..16>

The number of times a SIP UA will be challenged due to authentication failure before receiving a 403 Forbidden response. Note that this applies only to SIP Digest challenges (not NTLM challenges). Default: 3.

Example: `xConfiguration SIP Authentication Retry Limit: 3`

xConfiguration SIP Domain [1..200] Authzone: <S: 0,128>

The traversal zone to use when delegating credential checks for SIP messages for this domain.

Example: `xConfiguration SIP Domain 1 Authzone: "traversalzone"`

xConfiguration SIP Domain [1..200] Edge: <On/Off>

Whether remote and mobile collaboration features are enabled. Default Off.

Example: `xConfiguration SIP Domain 1 Edge: On`

xConfiguration SIP Domain [1..200] Name: <S: 0,128>

Specifies a domain for which this Expressway is authoritative. The domain name can comprise multiple levels. Each level's name can only contain letters, digits and hyphens, with each level separated by a period (dot). A level name cannot start or end with a hyphen, and the final level name must start with a letter. An example valid domain name is “100.example-name.com”.

Example: `xConfiguration SIP Domain 1 Name: "100.example-name.com"`

xConfiguration SIP Domain [1..200] Sip: <On/Off>

Specifies whether the Expressway will act as a SIP registrar for this domain, and will accept registration requests for any SIP endpoints attempting to register with an alias that includes this domain. Default On.

Example: `xConfiguration SIP Domain 1 Sip: On`

xConfiguration SIP GRUU Mode: <On/Off>

Controls whether GRUU (RFC5627) support is active. Default: On.

Example: `xConfiguration SIP GRUU Mode: On`

xConfiguration SIP MediaRouting ICE Mode: <On/Off>

Controls whether the Expressway takes the media for an ICE to non-ICE call where the ICE participant is thought to be behind a NAT device. Default: Off.

Example: `xConfiguration SIP MediaRouting ICE Mode: Off`

xConfiguration SIP Mode: <On/Off>

Determines whether or not the Expressway will provide SIP registrar and SIP proxy functionality. Default: Off.

Example: `xConfiguration SIP Mode: On`

xConfiguration SIP PreRoutedRouteHeader: <S:0,128>

Controls which Request Messages are allowed to go through the new pre-routed route header path.

As at X12.5, this flag is available only for the SIP REGISTER message.

Example: `xConfiguration SIP PreRoutedRouteHeader: "REGISTER"`

xConfiguration SIP Registration Call Remove: <Yes/No>

Specifies whether associated calls are dropped when a SIP registration expires or is removed. Default: No.

Example: `xConfiguration SIP Registration Call Remove: No`

xConfiguration SIP Registration Mode: <Off/On>

Determines whether or not the Expressway provides SIP registration. Default: On

Example: `xConfiguration SIP Registration Mode: Off`

xConfiguration SIP Registration Outbound Flow Timer: <0..600>

Specifies the value for the Flow-Timer header in Outbound registration responses. It defines the number of seconds after which the server will consider the registration flow to be dead if no keep-alive is sent by the user agent. Default: 0 (no header is added).

Example: `xConfiguration SIP Registration Outbound Flow Timer: 0`

xConfiguration SIP Registration Outbound Refresh Maximum: <30..7200>

The maximum allowed value for a SIP registration refresh period for Outbound registrations. Requests for a value greater than this will result in a lower value (calculated according to the Outbound registration refresh strategy) being returned. Default: 3600 seconds.

Example: `xConfiguration SIP Registration Outbound Refresh Maximum: 3600`

xConfiguration SIP Registration Outbound Refresh Minimum: <30..7200>

The minimum allowed value for a SIP registration refresh period for Outbound registrations. Requests for a value lower than this value will result in the registration being rejected with a 423 Interval Too Brief response. Default: 300 seconds.

Example: `xConfiguration SIP Registration Outbound Refresh Minimum: 300`

xConfiguration SIP Registration Outbound Refresh Strategy: <Maximum/Variable>

The method used to generate the SIP registration expiry period for Outbound registrations. Default: Variable.

Maximum: uses the lesser of the configured maximum refresh value and the value requested in the registration.

Variable: generates a random value between the configured minimum refresh value and the lesser of the configured maximum refresh value and the value requested in the registration.

Example: `xConfiguration SIP Registration Outbound Refresh Strategy: Variable`

xConfiguration SIP Registration Proxy Mode: <Off/ProxyToKnownOnly/ProxyToAny>

Specifies how proxied registrations should be handled. Default: Off.

Off: registration requests will not be proxied.

ProxyToKnownOnly: registration requests will be proxied to neighbors only.

ProxyToAny: registration requests will be proxied in accordance with the Expressway's existing call processing rules.

Example: `xConfiguration SIP Registration Proxy Mode: Off`

xConfiguration SIP Registration Standard Refresh Maximum: <30..7200>

The maximum allowed value for a SIP registration refresh period for standard registrations. Requests for a value greater than this will result in a lower value being returned. That value is calculated according to the standard registration refresh strategy. Default: 60 seconds.

Example: `xConfiguration SIP Registration Standard Refresh Maximum: 60`

xConfiguration SIP Registration Standard Refresh Minimum: <30..3600>

The minimum allowed value for a SIP registration refresh period for standard registrations. Requests for a value lower than this value will result in the registration being rejected with a 423 Interval Too Brief response. Default: 45 seconds.

Example: `xConfiguration SIP Registration Standard Refresh Minimum: 45`

xConfiguration SIP Registration Standard Refresh Strategy: <Maximum/Variable>

The method used to generate the SIP registration expiry period for standard registrations. Default: Maximum.

Maximum: uses the lesser of the configured maximum refresh value and the value requested in the registration.

Variable: generates a random value between the configured minimum refresh value and the lesser of the configured maximum refresh value and the value requested in the registration.

Example: `xConfiguration SIP Registration Standard Refresh Strategy: Maximum`

xConfiguration SIP Require Duo Video Mode: <On/Off>

Controls whether the Expressway requires the use of the com.tandberg.sdp.duo.enable extension for endpoints that support it. Default: On.

Example: `xConfiguration SIP Require Duo Video Mode: On`

xConfiguration SIP Require UDP BFCP Mode: <On/Off>

Controls whether the Expressway will require the use of the com.tandberg.udp.bfcp extension for endpoints that support it. Default: On.

Example: `xConfiguration SIP Require UDP BFCP Mode: On`

xConfiguration SIP Routes Route [1..20] Address: <S:0,39>

Specifies the IP address of the next hop for this route, where matching SIP requests will be forwarded. Note: this command is intended for developer use only.

Example: `xConfiguration SIP Routes Route 1 Address: "127.0.0.1"`

xConfiguration SIP Routes Route [1..20] Authenticated: <On/Off>

Whether to forward authenticated requests. Default: Off. Note: this command is intended for developer use only.

On: only forward requests along route if incoming message has been authenticated.

Off: always forward messages that match this route.

Example: `xConfiguration SIP Routes Route 1 Authenticated: On`

xConfiguration SIP Routes Route [1..20] Header Name: <S:0,64>

Name of SIP header field to match (e.g. Event). Note: this command is intended for developer use only.

Example: `xConfiguration SIP Routes Route 1 Header Name: "Event"`

xConfiguration SIP Routes Route [1..20] Header Pattern: <S:0,128>

Regular expression to match against the specified SIP header field. Note: this command is intended for developer use only.

Example: `xConfiguration SIP Routes Route 1 Header Pattern: "(my-event-package)(.*)"`

xConfiguration SIP Routes Route [1..20] Method: <S:0,64>

SIP method to match to select this route (e.g. INVITE, SUBSCRIBE). Note: this command is intended for developer use only.

Example: `xConfiguration SIP Routes Route 1 Method: "SUBSCRIBE"`

xConfiguration SIP Routes Route [1..20] Port: <1..65534>

Specifies the port on the next hop for this route to which matching SIP requests will be routed. Default: 5060. Note: this command is intended for developer use only.

Example: `xConfiguration SIP Routes Route 1 Port: 22400`

xConfiguration SIP Routes Route [1..20] Request Line Pattern: <S:0,128>

Regular expression to match against the SIP request line. Note: this command is intended for developer use only.

Example: `xConfiguration SIP Routes Route 1 Request Line Pattern: ".*@(%localdomains%|%ip%)"`

xConfiguration SIP Routes Route [1..20] Tag: <S:0,64>

Tag value specified by external applications to identify routes that they create. Note: this command is intended for developer use only.

Example: `xConfiguration SIP Routes Route 1 Tag: "Tag1"`

xConfiguration SIP Routes Route [1..20] Transport: <UDP/TCP/TLS>

Determines which transport type will be used for SIP messages forwarded along this route. Default: TCP. Note: this command is intended for developer use only.

Example: `xConfiguration SIP Routes Route 1 Transport: TCP`

xConfiguration SIP Service SipRegistrationMode: <Off/On>

Determines whether or not the Expressway provides SIP Service registration. Default: On

Example: `xConfiguration SIP Service SipRegistrationMode: Off`

Important The following command is discontinued from Version X14.0.1.

`xConfiguration SIP Registration Mode: <Off/On>`

xConfiguration SIP Session Refresh Minimum: <90..7200>

The minimum value the Expressway will negotiate for the session refresh interval for SIP calls. For more information see the definition of Min-SE header in RFC 4028. Default: 500.

Example: `xConfiguration SIP Session Refresh Minimum: 500`

xConfiguration SIP Session Refresh Value: <90..86400>

The maximum time allowed between session refresh requests for SIP calls. For more information see the definition of Session-Expires in RFC 4028. Default: 1800.

Example: `xConfiguration SIP Session Refresh Value: 1800`

xConfiguration SIP TCP Mode: <On/Off>

Determines whether incoming and outgoing SIP calls using the TCP protocol will be allowed. Default: Off.

Example: `xConfiguration SIP TCP Mode: On`

xConfiguration SIP TCP Outbound Port End: <1024..65534>

Specifies the upper port in the range to be used by outbound TCP/TLS SIP connections. Default: 29999.

Example: `xConfiguration SIP TCP Outbound Port End: 29999`

xConfiguration SIP TCP Outbound Port Start: <1024..65534>

Specifies the lower port in the range to be used by outbound TCP/TLS SIP connections. Default: 25000.

Example: `xConfiguration SIP TCP Outbound Port Start: 25000`

xConfiguration SIP TCP Port: <1024..65534>

Specifies the listening port for incoming SIP TCP calls. Default: 5060.

Example: `xConfiguration SIP TCP Port: 5060`

xConfiguration SIP TLS Certificate Revocation Checking CRL Mode: <On/Off>

Controls whether Certificate Revocation Lists (CRLs) are used to perform certificate revocation checking. CRLs can be loaded manually onto the Expressway, downloaded automatically from pre-configured URIs, or downloaded automatically from a CRL distribution point (CDP) URI contained in the X.509 certificate. Default: On.

Example: `xConfiguration SIP TLS Certificate Revocation Checking CRL Mode: On`

xConfiguration SIP TLS Certificate Revocation Checking CRL Network Fetch Mode: <On/Off>

Controls whether the download of CRLs from the CDP URIs contained in X.509 certificates is allowed. Default: On.

Example: `xConfiguration SIP TLS Certificate Revocation Checking CRL Network Fetch Mode: On`

xConfiguration SIP TLS Certificate Revocation Checking Mode: <On/Off>

Controls whether revocation checking is performed for certificates exchanged during SIP TLS connection establishment. Default: Off.

Example: `xConfiguration SIP TLS Certificate Revocation Checking Mode: Off`

xConfiguration SIP TLS Certificate Revocation Checking OCSP Mode: <On/Off>

Controls whether the Online Certificate Status Protocol (OCSP) may be used to perform certificate revocation checking. To use OCSP, the X.509 certificate to be checked must contain an OCSP responder URI. Default: On.

Example: `xConfiguration SIP TLS Certificate Revocation Checking OCSP Mode: On`

xConfiguration SIP TLS Certificate Revocation Checking Source Inaccessibility Behavior: <Ignore/Fail>

Controls the revocation checking behavior if the revocation source cannot be contacted. Default: Fail.

Fail: treat the certificate as revoked (and thus do not allow the TLS connection).

Ignore: treat the certificate as not revoked.

Example: `xConfiguration SIP TLS Certificate Revocation Checking Source Inaccessibility Behavior: Fail`

xConfiguration SIP TLS Mode: <On/Off>

Determines whether incoming and outgoing SIP calls using the TLS protocol will be allowed. Default: On.

Example: `xConfiguration SIP TLS Mode: On`

xConfiguration SIP TLS Port: <1024..65534>

Specifies the listening port for incoming SIP TLS calls. Default: 5061.

Example: `xConfiguration SIP TLS Port: 5061`

xConfiguration SIP UDP Mode: <On/Off>

Determines whether incoming and outgoing SIP calls using the UDP protocol will be allowed. Default: Off.

Example: `xConfiguration SIP UDP Mode: On`

xConfiguration SIP UDP Port: <1024..65534>

Specifies the listening port for incoming SIP UDP calls. Default: 5060.

Example: `xConfiguration SIP UDP Port: 5060`

xConfiguration SNMP CommunityName: <S: 0, 16>

The Expressway's SNMP community name. Default: public

Example: `xConfiguration SNMP CommunityName: "public"`

xConfiguration SNMP SystemContact: <S: 0, 70>

The name of the person who can be contacted regarding issues with the Expressway. Default: Administrator.

Example: `xConfiguration SNMP SystemContact: Administrator`

xConfiguration SNMP SystemLocation: <S: 0, 70>

The physical location of the system.

Example: `xConfiguration SNMP SystemLocation: "Server Room 128"`

xConfiguration SNMP V1Mode: <On/Off>

Enables or disables SNMP Version 1 support. Default: Off.

Example: `xConfiguration SNMP V1Mode: Off`

xConfiguration SNMP V2cMode: <On/Off>

Enables or disables SNMP Version 2c support. Default: On.

Example: `xConfiguration SNMP V2cMode: On`

xConfiguration SNMP V3AuthenticationMode: <On/Off>

Enables or disables SNMP Version 3 authentication. Default: On.

Example: `xConfiguration SNMP V3AuthenticationMode: On`

xConfiguration SNMP V3AuthenticationPassword: <S: 0,215>

Sets SNMP Version 3 authentication password. It must be at least 8 characters.

Example: `xConfiguration SNMP V3AuthenticationPassword: "password123"`

xConfiguration SNMP V3Mode: <On/Off>

Enables or disables SNMP Version 3 support. Default: On.

Example: `xConfiguration SNMPV3 Mode: On`

xConfiguration SNMP V3PrivacyMode: <On/Off>

Enables or disables SNMP Version 3 privacy. Default: On.

Example: `xConfiguration SNMP V3PrivacyMode: On`

xConfiguration SNMP V3PrivacyPassword: <S: 0,215>

Sets SNMP Version 3 privacy password. It must be at least 8 characters.

Example: `xConfiguration SNMP V3PrivacyPassword: "password123"`

xConfiguration SNMP V3PrivacyType: <AES>

Sets SNMP Version 3 privacy type. Default: AES.

Example: `xConfiguration SNMP V3PrivacyType: AES`

xConfiguration SNMP V3UserName: <S: 0,70>

Sets the username to use when using SNMP V3.

Example: `xConfiguration SNMP V3UserName: "user123"`

xConfiguration SystemUnit Maintenance Mode: <On/Off>

Sets the Expressway into maintenance mode. New calls and registrations are disallowed and existing calls and registrations are allowed to expire. Default: Off.

Example: `xConfiguration SystemUnit Maintenance Mode: Off`

xConfiguration SystemUnit Name: <S:, 0, 50>

Defines the name of the Expressway. The system name appears in various places in the web interface and on the front panel of the unit. Choose a name that uniquely identifies the system.

Example: `xConfiguration SystemUnit Name: "MainHQ"`

xConfiguration TimeZone Name: <S: 0, 64>

Sets the local time zone of the Expressway. Time zone names follow the POSIX naming convention e.g. Europe/London or America/New_York. Default: GMT.

Example: `xConfiguration TimeZone Name: "GMT"`

xConfiguration Transform [1..100] Description: <S: 0,64>

A free-form description of the transform.

Example: `xConfiguration Transform [1..100] Description: "Change example.net to example.com"`

xConfiguration Transform [1..100] Pattern Behavior: <Strip/Replace>

How the alias is modified. Default: Strip.

Strip: removes the matching prefix or suffix from the alias.

Replace: substitutes the matching part of the alias with the text in replace string.

AddPrefix: prepends the replace string to the alias.

AddSuffix: appends the replace string to the alias.

Example: `xConfiguration Transform 1 Pattern Behavior: Replace`

xConfiguration Transform [1..100] Pattern Replace: <S: 0, 60>

The text string to use in conjunction with the selected Pattern behavior.

Example: `xConfiguration Transform 1 Pattern Replace: "example.com"`

xConfiguration Transform [1..100] Pattern String: <S: 0, 60>

The pattern against which the alias is compared.

Example: `xConfiguration Transform 1 Pattern String: "example.net"`

xConfiguration Transform [1..100] Pattern Type: <Exact/Prefix/Suffix/Regex>

How the pattern string must match the alias for the transform to be applied. Default: Prefix.

Exact: the entire string must exactly match the alias character for character.

Prefix: the string must appear at the beginning of the alias.

Suffix: the string must appear at the end of the alias.

Regex: the string is treated as a regular expression.

Example: `xConfiguration Transform 1 Pattern Type: Suffix`

xConfiguration Transform [1..100] Priority: <1..65534>

Assigns a priority to the specified transform. Transforms are compared with incoming aliases in order of priority, and the priority must be unique for each transform. Default: 1 .

Example: `xConfiguration Transform 1 Priority: 10`

xConfiguration Transform [1..100] State: <Enabled/Disabled>

Indicates if the transform is enabled or disabled. Disabled transforms are ignored.

Example: `xConfiguration Transform 1 State: Enabled`

xConfiguration Traversal Media Port End: <1025..65533>

For traversal calls (where the Expressway takes the media as well as the signaling), specifies the upper port in the range to use for the media. Ports are allocated from this range in pairs, the first of each being even. Thus the range must end with an odd number. Default: 59999 .

Example: `xConfiguration Traversal Media Port End: 59999`

xConfiguration Traversal Media Port Start: <1024..65532>

For traversal calls (where the Expressway takes the media as well as the signaling), specifies the lower port in the range to use for the media. Ports are allocated from this range in pairs, the first of each being even. Thus the range must start with an even number. Default: 36000 .

Example: `xConfiguration Traversal Media Port Start: 36000`

xConfiguration Traversal Server H323 Assent CallSignaling Port: <1024..65534>

The port on the Expressway to use for Assent signaling. Default: 2776 .

Example: `xConfiguration Traversal Server H323 Assent CallSignaling Port: 2777`

xConfiguration Traversal Server H323 H46018 CallSignaling Port: <1024..65534>

The port on the Expressway to use for H460.18 signaling. Default: 2777 .

Example: `xConfiguration Traversal Server H323 H46018 CallSignaling Port: 2777`

xConfiguration Traversal Server TURN Authentication Realm: <S: 1,128>

The realm sent by the server in its authentication challenges. Default: TANDBERG .

Example: `xConfiguration Traversal Server TURN Authentication Realm: "TANDBERG"`

xConfiguration Traversal Server TURN Authentication Remote Mode: <On/Off>

Determines whether the server requires requests to be authenticated. When enabled the server will also authenticate its responses. Default: On.

Example: `xConfiguration Traversal Server TURN Authentication Remote Mode: On`

xConfiguration Traversal Server TURN Media Port End: <1024..65534>

The upper port in the range used for TURN relays. Default: 61799.

Example: `xConfiguration Traversal Server TURN Media Port End: 61799`

xConfiguration Traversal Server TURN Media Port Start: <1024..65534>

The lower port in the range used for TURN relays. Default: 60000.

Example: `xConfiguration Traversal Server TURN Media Port Start: 60000`

xConfiguration Traversal Server TURN Mode: <On/Off>

Determines whether the Expressway offers TURN services to traversal clients. Default: Off .

Example: `xConfiguration Traversal Server TURN Mode: Off`

xConfiguration Traversal Server TURN Port: <1024..65534>

The listening port for TURN requests. Default: 3478.

Example: `xConfiguration Traversal Server TURN Port: 3478`

xConfiguration Traversal Server TURN PortRangeEnd: <1024..65534>

The upper port in the range used for TURN requests. Default: 3483

Example: `xConfiguration Traversal Server TURN PortRangeEnd: 3483`

xConfiguration Traversal Server TURN PortRangeStart: <1024..65534>

The lower port in the range used for TURN requests. Default: 3478.

Example: `xConfiguration Traversal Server TURN PortRangeStart: 3478`

xConfiguration Traversal Server TURN ProtocolMode: <TCP/UDP/Both>

The permitted protocols for TURN requests. Default: Both.

Example: `xConfiguration Traversal Server TURN ProtocolMode: Both`

xConfiguration xConfiguration Traversal Server TURN Authentication Mode: <On/Off>>

Determines whether the server will require requests to be authenticated. When enabled the server will also authenticate its responses. Default: On

Example: `xConfiguration Traversal Server TURN Authentication Mode: On`

xConfiguration XCP Config FcmService: <On/Off>

Controls whether FCM Push Notifications for Jabber Android Devices over MRA are enabled. Default: Off.

Example: `xConfiguration XCP Config FcmService: On`

xConfiguration XCP DelayedRestart EnableDelayedRestart: <On/Off>

Controls whether the Delayed Cisco XCP Router restart feature is enabled. Default: Off.

Example: `xConfiguration DelayedRestart EnableDelayedRestart: On`

xConfiguration XCP DelayedRestart EnableScheduledRestart: <On/Off>

Controls whether a scheduled restart of the Cisco XCP Router is enabled. Default: Off.

Example: `xConfiguration XCP DelayedRestart EnableScheduledRestart: On`

xConfiguration XCP DelayedRestart MultitenancyEnabled: <On/Off>

Turn on multitenancy to configure the delayed Cisco XCP Router restart. Default: Off.

Example: `xConfiguration XCP DelayedRestart MultitenancyEnabled: On`

xConfiguration XCP DelayedRestart ScheduledTime:

The time each day that the scheduled restart takes place.

Example: `xConfiguration XCP DelayedRestart ScheduledTime: 01.00`

xConfiguration XCP DelayedRestartNotify RestartTime:

Set the notification for the restart time.

Example: `xConfiguration DelayedRestartNotify RestartTime: 01.00`

xConfiguration XCP TLS Certificate CVS CertificateRevocationCheck: <On/Off>

Controls whether Certificate Revocation Lists (CRLs) are used to perform certificate revocation checking for XCP TLS connection. CRLs can be loaded manually onto the Expressway, downloaded automatically from pre-configured URIs, or downloaded automatically from a CRL distribution point (CDP) URI contained in the X.509 certificate as well as using OCSP. Default: Off.

Example: `xConfiguration XCP TLS Certificate CVS CertificateRevocationCheck: Off`

xConfiguration XCP TLS Certificate CVS ConvertIpToHostname: <On/Off>

Controls whether Expressway automatically converts XCP peer's IP address to FQDN for certificate verification. Default: On.

Example: `xConfiguration XCP TLS Certificate CVS ConvertIpToHostname: On`

xConfiguration XCP TLS Certificate CVS CrlNetworkFetchEnabled: <On/Off>

Controls whether the Expressway is allowed to download CRLs from the CDP URIs contained in its X.509 certificate. Default: On.

Example: `xConfiguration XCP TLS Certificate CVS CrlNetworkFetchEnabled: On`

xConfiguration XCP TLS Certificate CVS EnableCvs: <On/Off>

Controls whether or not to verify XCP peers' certificates during XCP TLS connection. When *Off*, all other XCP TLS Certificate CVS configuration options will have no effect. Default: On.

Example: `xConfiguration XCP TLS Certificate CVS EnableCvs: On`

xConfiguration XCP TLS Certificate CVS FailOnInaccessibleSource: <On/Off>

Controls the certificate verification behavior if the revocation source cannot be contacted.

On: treat the certificate as revoked (and thus do not allow the TLS connection).

Off: treat the certificate as not revoked.

Default: On.

Example: `xConfiguration XCP TLS Certificate CVS FailOnInaccessibleSource: On`

xConfiguration XCP TLS Certificate CVS UseCrl: <On/Off>

Controls whether Expressway checks its own CRL for revocation of certificates exchanged during establishment of XCP TLS connections. Default: On.

Example: `xConfiguration XCP TLS Certificate CVS UseCrl: On`

xConfiguration XCP TLS Certificate CVS UseOcsp: <On/Off>

Controls whether the Expressway can use OCSP to check if the certificate is revoked. to perform certificate revocation checking. To use OCSP, the X.509 certificate to be checked must contain an OCSP responder URI. Default: On.

Example: `xConfiguration XCP TLS Certificate CVS UseOcsp: On`

xConfiguration XCP TLS Certificate CVS VerifyHostname: <On/Off>

Controls whether the Expressway verifies the hostname from the XCP host's certificate against its own peer configuration. Default: On.

Example: `xConfiguration XCP TLS Certificate CVS VerifyHostname: On`

xConfiguration Zones DefaultZone Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. Default: DoNotCheckCredentials.

Example: `xConfiguration Zones DefaultZone Authentication Mode: DoNotCheckCredentials`

xConfiguration Zones DefaultZone SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

The media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Default: Auto.

On: All media must be encrypted.

Off: All media must be unencrypted.

BestEffort: Use encryption if available otherwise fallback to unencrypted media.

Auto: No media encryption policy is applied.

Example: `xConfiguration Zones DefaultZone SIP Media Encryption Mode: Auto`

xConfiguration Zones DefaultZone SIP Media ICE Support: <On/Off>

Controls whether ICE is supported by the devices in the zone. Default: Off

On: This zone supports ICE.

Off: This zone does not support ICE.

Example: `xConfiguration Zones DefaultZone SIP Media ICE Support: On`

xConfiguration Zones DefaultZone SIP Multistream Mode: <Off/On>

Controls if the Expressway allows Multistream to and from devices in this zone. Default: On

On: allow Multistream

Off: disallow Multistream.

Example: `xConfiguration Zones DefaultZone SIP Multistream Mode: Off`

xConfiguration Zones DefaultZone SIP Record Route Address Type: <IP/Hostname>

Controls whether the Expressway uses its IP address or host name in the Record-Route or Path headers of outgoing SIP requests to this zone. Note: setting this value to hostname also requires a valid DNS system host name to be configured on the Expressway. Default: IP.

Example: `xConfiguration Zones DefaultZone SIP Record Route Address Type: IP`

xConfiguration Zones DefaultZone SIP SipUpdateRefresh Support: <On/Off>

Determines whether session refresh by SIP UPDATE message is supported in this zone.

On: This zone sends SIP UPDATE messages for SIP session refresh.

Off: This zone does not send SIP UPDATE messages for SIP session refresh.

Default: Off.

Example: `xConfiguration Zones DefaultZone SIP SipUpdateRefresh Support: Off`

xConfiguration Zones DefaultZone SIP TLS Verify Mode: <On/Off>

Controls whether the hostname contained within the certificate presented by the external system is verified by the Expressway. If enabled, the certificate hostname (also known as the Common Name) is checked against the patterns specified in the Default Zone access rules. Default: Off.

Example: `xConfiguration Zones DefaultZone SIP TLS Verify Mode: Off`

xConfiguration Zones LocalZone DefaultSubZone Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Controls how the Expressway authenticates incoming messages from this subzone and whether they are subsequently treated as authenticated, unauthenticated or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. Default: DoNotCheckCredentials.

Example: `xConfiguration Zones LocalZone DefaultSubZone Authentication Mode: DoNotCheckCredentials`

xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Limit: <1..100000000>

The bandwidth limit (in kbps) for any one call to or from an endpoint in the Default Subzone (applies only if the mode is set to Limited). Default: 1920.

Example: `xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Limit: 1920`

xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Mode: <Limited/Unlimited/NoBandwidth>

Controls if there is a limit on the bandwidth for any one call to or from an endpoint in the Default Subzone.

NoBandwidth: no bandwidth available. No calls can be made to or from the Default Subzone.

Default: Unlimited.

Example: `xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Mode: Limited`

xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Limit: <1..100000000>

The bandwidth limit (in kbps) for any one call between two endpoints within the Default Subzone (applies only if the mode is set to Limited). Default: 1920.

Example: `xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Limit: 1920`

xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Mode: <Limited/Unlimited/NoBandwidth>

Controls if there is a limit on the bandwidth for any one call between two endpoints within the Default Subzone.

NoBandwidth: no bandwidth available. No calls can be made within the Default Subzone.

Default: Unlimited.

Example: `xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Mode: Limited`

xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Limit: <1..100000000>

Sets the total bandwidth limit (in kbps) of the Default Subzone (applies only if Mode is set to Limited). Default: 500000 .

Example: `xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Limit: 500000`

xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>

Controls if the Default Subzone has a limit on the total bandwidth being used by its endpoints at any one time.

NoBandwidth: no bandwidth available. No calls can be made to, from, or within the Default Subzone.

Default: Unlimited.

Example: `xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Mode: Limited`

xConfiguration Zones LocalZone DefaultSubZone Registrations: <Allow/Deny>

Controls whether registrations assigned to the Default Subzone are accepted. Default: Allow.

Example: `xConfiguration Zones LocalZone DefaultSubZone Registrations: Allow`

xConfiguration Zones LocalZone DefaultSubZone SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

The media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this subzone. Default: Auto

On: All media must be encrypted.

Off: All media must be unencrypted.

BestEffort: Use encryption if available otherwise fallback to unencrypted media.

Auto: No media encryption policy is applied.

Example: `xConfiguration Zones LocalZone DefaultSubZone SIP Media Encryption Mode: Auto`

xConfiguration Zones LocalZone DefaultSubZone SIP Media ICE Support: <On/Off>

Controls whether ICE is supported by the devices in the zone. Default: Off

On: This zone supports ICE.

Off: This zone does not support ICE.

Example: `xConfiguration Zones LocalZone DefaultSubZone SIP Media ICE Support: On`

xConfiguration Zones LocalZone DefaultSubZone SIP Multistream Mode: <Off/On>

Controls if the Expressway allows Multistream to and from devices in this zone. Default: On

On: allow Multistream

Off: disallow Multistream.

Example: `xConfiguration Zones LocalZone DefaultSubZone SIP Multistream Mode: Off`

xConfiguration Zones LocalZone DefaultSubZone SIP SipUpdateRefresh Support: <On/Off>

Determines whether session refresh by SIP UPDATE message is supported in this zone.

On: This zone sends SIP UPDATE messages for SIP session refresh.

Off: This zone does not send SIP UPDATE messages for SIP session refresh.

Default: Off.

Example: `xConfiguration Zones LocalZone DefaultSubZone SIP SipUpdateRefresh Support: On`

xConfiguration Zones LocalZone SIP Record Route Address Type: <IP/Hostname>

Controls whether the Expressway uses its IP address or host name in the Record-Route or Path headers of outgoing SIP requests to this zone. Note: setting this value to hostname also requires a valid DNS system host name to be configured on the Expressway. Default: IP.

Example: `xConfiguration Zones LocalZone SIP Record Route Address Type: IP`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Description: <S: 0,64>

A free-form description of the membership rule.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Description: "Office-based staff"`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Name: <S: 0,50>

Assigns a name to this membership rule.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Name: "Office Workers"`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Pattern String: <S: 0,60>

Specifies the pattern against which the alias is compared.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Pattern String: "@example.com"`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Pattern Type: <Exact/Prefix/Suffix/Regex>

The way in which the pattern must match the alias.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Pattern Type: Suffix`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Priority: <1..65534>

Determines the order in which the rules are applied (and thus to which subzone the endpoint is assigned) if an endpoint's address satisfies multiple rules. The rules with the highest priority (1, then 2, then 3 and so on) are applied first. If multiple Subnet rules have the same priority the rule with the largest prefix length is applied first. Alias Pattern Match rules at the same priority are searched in configuration order. Default: 100.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Priority: 100`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] State: <Enabled/Disabled>

Indicates if the membership rule is enabled or disabled. Disabled membership rules are ignored. Default: Enabled.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 State: Enabled`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] SubZoneName: <S: 0,50>

The subzone to which an endpoint is assigned if its address satisfies this rule.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 SubZoneName: "Branch Office"`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Subnet Address: <S: 0,39>

Specifies an IP address used (in conjunction with the prefix length) to identify this subnet.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Subnet Address: "192.168.0.0"`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Subnet PrefixLength: <1..128>

The number of bits of the subnet address which must match for an IP address to belong in this subnet. Default: 32.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Subnet PrefixLength: 32`

xConfiguration Zones LocalZone SubZones MembershipRules Rule [1..3000] Type: <Subnet/AliasPatternMatch>

The type of address that applies to this rule.

Subnet: assigns the device if its IP address falls within the configured IP address subnet.

AliasPatternMatch: assigns the device if its alias matches the configured pattern.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Type: Subnet`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Controls how the Expressway authenticates incoming messages from this subzone and whether they are subsequently treated as authenticated, unauthenticated or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. See the Administrator Guide for further information. Default: DoNotCheckCredentials.

Example: `xConfiguration Zones LocalZone SubZones SubZone 1 Authentication Mode: DoNotCheckCredentials`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Bandwidth PerCall Inter Limit: <1..100000000>

The bandwidth limit (in kbps) on any one call to or from an endpoint in this subzone (applies only if Mode is set to Limited). Default: 1920.

Example: `xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Inter Limit: 1920`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Bandwidth PerCall Inter Mode: <Limited/Unlimited/NoBandwidth>

Determines whether there is a limit on the bandwidth for any one call to or from an endpoint in this subzone. Default: Unlimited.

NoBandwidth: no bandwidth available. No calls can be made to or from this subzone.

Example: `xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Inter Mode: Limited`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Bandwidth PerCall Intra Limit: <1..100000000>

The bandwidth limit (in kbps) for any one call between two endpoints within this subzone (applies only if the mode is set to Limited). Default: 1920.

Example: `xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Intra Limit: 1920`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Bandwidth PerCall Intra Mode: <Limited/Unlimited/NoBandwidth>

Determines whether there is a limit on the bandwidth for any one call between two endpoints within this subzone. Default: Unlimited.

NoBandwidth: no bandwidth available. No calls can be made within this subzone.

Example: `xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Intra Mode: Limited`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Bandwidth Total Limit: <1..100000000>

Sets the total bandwidth limit (in kbps) of this subzone (applies only if the mode is set to Limited). Default: 500000.

Example: `xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth Total Limit: 500000`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>

Controls if this subzone has a limit on the total bandwidth of calls being used by its endpoints at any one time. Default: Unlimited.

NoBandwidth: no bandwidth available. No calls can be made to, from, or within this subzone.

Example: `xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth Total Mode: Limited`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Name: <S: 0, 50>

Assigns a name to this subzone.

Example: `xConfiguration Zones LocalZone SubZones SubZone 1 Name: "BranchOffice"`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] Registrations: <Allow/Deny>

Controls whether registrations assigned to this subzone are accepted. Default: Allow.

Example: `xConfiguration Zones LocalZone SubZones SubZone 1 Registrations: Allow`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

The media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this subzone. Default: Auto

On: All media must be encrypted.

Off: All media must be unencrypted.

BestEffort: Use encryption if available otherwise fallback to unencrypted media.

Auto: No media encryption policy is applied.

Example: `xConfiguration Zones LocalZone SubZones SubZone 1 SIP Media Encryption Mode: Auto`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] SIP Media ICE Support: <On/Off>

Controls whether ICE is supported by the devices in the zone. Default: Off

On: This zone supports ICE.

Off: This zone does not support ICE.

Example: `xConfiguration Zones LocalZone SubZones Subzone 1 SIP Media ICE Support: On`

xConfiguration Zones LocalZone SubZones SubZone [1..1000] SIP Multistream Mode: <Off/On>

Controls if the Expressway allows Multistream to and from devices in this zone. Default: On

On: allow Multistream

Off: disallow Multistream.

Example: `xConfiguration Zones LocalZone SubZones Subzone 1 SIP Multistream Mode: Off`

xConfiguration Zones LocalZone Traversal H323 Assent Mode: <On/Off>

Determines whether or not H.323 calls using Assent mode for firewall traversal will be allowed. Applies to traversal-enabled endpoints registered directly with the Expressway. Default: On .

Example: `xConfiguration Zones LocalZone Traversal H323 Assent Mode: On`

xConfiguration Zones LocalZone Traversal H323 H46018 Mode: <On/Off>

Controls whether H.323 calls using H460.18 mode for firewall traversal are allowed. Applies to traversal-enabled endpoints registered directly with the Expressway. Default: On .

Example: `xConfiguration Zones LocalZone Traversal H323 H46018 Mode: On`

xConfiguration Zones LocalZone Traversal H323 H46019 Demultiplexing Mode: <On/Off>

Controls whether the Expressway operates in Demultiplexing mode for calls from traversal-enabled endpoints registered directly with it. Default: Off .

On: allows use of the same two ports for all calls.

Off: each call will use a separate pair of ports for media.

Example: `xConfiguration Zones LocalZone Traversal H323 H46019 Demultiplexing Mode: Off`

xConfiguration Zones LocalZone Traversal H323 Preference: <Assent/H46018>

If an endpoint that is registered directly with the Expressway supports both Assent and H460.18 protocols, this setting determines which the Expressway uses. Default: Assent.

Example: `xConfiguration Zones LocalZone Traversal H323 Preference: Assent`

xConfiguration Zones LocalZone Traversal H323 TCPProbe KeepAliveInterval: <1..65534>

Sets the interval (in seconds) with which a traversal-enabled endpoint registered directly with the Expressway will send a TCP probe to the Expressway once a call is established, in order to keep the firewall's NAT bindings open. Default: 20 .

Example: `xConfiguration Zones LocalZone Traversal H323 TCPProbe KeepAliveInterval: 20`

xConfiguration Zones LocalZone Traversal H323 TCPProbe RetryCount: <1..65534>

Sets the number of times traversal-enabled endpoints registered directly with the Expressway will attempt to send a TCP probe. Default: 5 .

Example: `xConfiguration Zones LocalZone Traversal H323 TCPProbe RetryCount: 5`

xConfiguration Zones LocalZone Traversal H323 TCPProbe RetryInterval: <1..65534>

Sets the frequency (in seconds) with which traversal-enabled endpoints registered directly with the Expressway will send a TCP probe. Default: 2 .

Example: `xConfiguration Zones LocalZone Traversal H323 TCPProbe RetryInterval: 2`

xConfiguration Zones LocalZone Traversal H323 UDPProbe KeepAliveInterval: <1..65534>

Sets the interval (in seconds) with which a traversal-enabled endpoint registered directly with the Expressway will send a UDP probe to the Expressway once a call is established, in order to keep the firewall's NAT bindings open. Default: 20 .

Example: `xConfiguration Zones LocalZone Traversal H323 UDPProbe KeepAliveInterval: 20`

xConfiguration Zones LocalZone Traversal H323 UDPProbe RetryCount: <1..65534>

Sets the number of times traversal-enabled endpoints registered directly with the Expressway will attempt to send a UDP probe. Default: 5 .

Example: `xConfiguration Zones LocalZone Traversal H323 UDPProbe RetryCount: 5`

xConfiguration Zones LocalZone Traversal H323 UDPProbe RetryInterval: <1..65534>

Sets the frequency (in seconds) with which traversal-enabled endpoints registered directly with the Expressway will send a UDP probe. Default: 2 .

Example: `xConfiguration Zones LocalZone Traversal H323 UDPProbe RetryInterval: 2`

xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Limit: <1..100000000>

The bandwidth limit (in kbps) applied to any one traversal call being handled by the Expressway (applies only if the mode is set to Limited). Default: 1920 .

Example: `xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Limit: 1920`

xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Mode: <Limited/Unlimited/NoBandwidth>

Determines whether there is a limit on the bandwidth of any one traversal call being handled by the Expressway. Default: Unlimited.

NoBandwidth: no bandwidth available. No traversal calls can be made.

Example: `xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Mode: Limited`

xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Limit: <1..100000000>

The total bandwidth (in kbps) allowed for all traversal calls being handled by the Expressway (applies only if the mode is set to Limited). Default: 500000 .

Example: `xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Limit: 500000`

xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>

Determines whether or not there is a limit to the total bandwidth of all traversal calls being handled by the Expressway. Default: Unlimited.

NoBandwidth: no bandwidth available. No traversal calls can be made.

Example: `xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Mode: Limited`

xConfiguration Zones Policy Mode: <SearchRules/Directory>

The mode used when attempting to locate a destination. Default: SearchRules.

SearchRules: use the configured search rules to determine which zones are queried and in what order.

Directory: use the facilities of a directory service to direct the request to the correct zones.

Example: `xConfiguration Zones Policy Mode: SearchRules`

xConfiguration Zones Policy SearchRules Rule [1..2000] Authentication: <Yes/No>

Specifies whether this search rule applies only to authenticated search requests. Default: No.

Example: `xConfiguration Zones Policy SearchRules Rule 1 Authentication: No`

xConfiguration Zones Policy SearchRules Rule [1..2000] Description: <S: 0,64>

A free-form description of the search rule.

Example: `xConfiguration Zones Policy SearchRules Rule 1 Description: "Send query to the DNS zone"`

xConfiguration Zones Policy SearchRules Rule [1..2000] Mode: <AliasPatternMatch/AnyAlias/AnyIPAddress>

Determines whether a query is sent to the target zone. Default: AnyAlias.

AliasPatternMatch: queries the zone only if the alias matches the corresponding pattern type and string.

AnyAlias: queries the zone for any alias (but not IP address).

AnyIPAddress: queries the zone for any given IP address (but not alias).

Example: `xConfiguration Zones Policy SearchRules Rule 1 Mode: AnyAlias`

xConfiguration Zones Policy SearchRules Rule [1..2000] Name: <S: 0,50>

Descriptive name for the search rule.

Example: `xConfiguration Zones Policy SearchRules Rule 1 Name: "DNS lookup"`

xConfiguration Zones Policy SearchRules Rule [1..2000] Pattern Behavior: <Strip/Leave/Replace>

Determines whether the matched part of the alias is modified before being sent to the target zone. (Applies to Alias Pattern Match mode only.) Default: Strip.

Leave: the alias is not modified.

Strip: the matching prefix or suffix is removed from the alias.

Replace: the matching part of the alias is substituted with the text in the replace string.

Example: `xConfiguration Zones Policy SearchRules Rule 1 Pattern Behavior: Strip`

xConfiguration Zones Policy SearchRules Rule [1..2000] Pattern Replace: <S: 0,60>

The string to substitute for the part of the alias that matches the pattern. (Applies to Replace pattern behavior only.)

Example: `xConfiguration Zones Policy SearchRules Rule 1 Pattern Replace: "@example.net"`

xConfiguration Zones Policy SearchRules Rule [1..2000] Pattern String: <S: 0,60>

The pattern against which the alias is compared. (Applies to Alias Pattern Match mode only.)

Example: `xConfiguration Zones Policy SearchRules Rule 1 Pattern String: "@example.com"`

xConfiguration Zones Policy SearchRules Rule [1..2000] Pattern Type: <Exact/Prefix/Suffix/Regex>

How the pattern string must match the alias for the rule to be applied. (Applies to Alias Pattern Match mode only.) Default: Prefix.

Exact: the entire string must exactly match the alias character for character.

Prefix: the string must appear at the beginning of the alias.

Suffix: the string must appear at the end of the alias.

Regex: the string is treated as a regular expression.

Example: `xConfiguration Zones Policy SearchRules Rule 1 Pattern Type: Suffix`

xConfiguration Zones Policy SearchRules Rule [1..2000] Priority: <1..65534>

The order in the search process that this rule is applied, when compared to the priority of the other search rules. All Priority 1 search rules are applied first, followed by all Priority 2 search rules, and so on. Default: 100.

Example: `xConfiguration Zones Policy SearchRules Rule 1 Priority: 100`

xConfiguration Zones Policy SearchRules Rule [1..2000] Progress: <Continue/Stop>

Specifies the ongoing search behavior if the alias matches this search rule. If 'stop' is selected, any rules with the same priority level as this rule are still applied. Default: Continue.

Continue: continue applying the remaining search rules (in priority order) until the endpoint identified by the alias is found.

Stop: do not apply any more search rules, even if the endpoint identified by the alias is not found in the target zone.

Example: `xConfiguration Zones Policy SearchRules Rule 1 Progress: Continue`

xConfiguration Zones Policy SearchRules Rule [1..2000] Protocol: <Any/H323/SIP>

The source protocol required for the rule to match.

Example: `xConfiguration Zones Policy SearchRules Rule 1 Protocol: Any`

xConfiguration Zones Policy SearchRules Rule [1..2000] Source Mode: <Any/AllZones/LocalZone/Named>

The sources of the requests for which this rule applies. Default: Any.

Any: locally registered devices, neighbor or traversal zones, and any non-registered devices.

All zones: locally registered devices plus neighbor or traversal zones.

Local Zone: locally registered devices only.

Named: A specific Zone or SubZone.

Example: `xConfiguration Zones Policy SearchRules Rule 1 Source Mode: Any`

xConfiguration Zones Policy SearchRules Rule [1..2000] Source Name: <S: 0..50>

The name of the source (Sub)Zone for which this rule applies.

Example: `xConfiguration Zones Policy SearchRules Rule 1 Source Name: “Local Office”`

xConfiguration Zones Policy SearchRules Rule [1..2000] State: <Enabled/Disabled>

Indicates if the search rule is enabled or disabled. Disabled search rules are ignored. Default: Enabled .

Example: `xConfiguration Zones Policy SearchRules Rule 1 State: Enabled`

xConfiguration Zones Policy SearchRules Rule [1..2000] Target Name: <S: 0,50>

The zone or policy service to query if the alias matches the search rule.

Example: `xConfiguration Zones Policy SearchRules Rule 1 Target Name: “Sales Office”`

xConfiguration Zones Policy SearchRules Rule [1..2000] Target Type: <Zone/PolicyService>

The type of target this search rule applies to.

Example: `xConfiguration Zones Policy SearchRules Rule 1 Target Type: Zone`

xConfiguration Zones Zone [1..1000] DNS IncludeAddressRecord: <On/Off>

Determines whether, if no NAPTR (SIP) or SRV (SIP and H.323) records have been found for the dialed alias via this zone, the Expressway will then query for A and AAAA DNS Records. Default: Off .

Example: `xConfiguration Zones Zone 1 DNS IncludeAddressRecord: Off`

xConfiguration Zones Zone [1..1000] DNS Interworking SIP Audio DefaultCodec:

`<G711u/G711a/G722_48/G722_56/G722_64/G722_1_16/G722_1_24/G722_1_32/G722_1_48/G723_1/G728/G729/AACLD_48/AACLD_56/AACLD_64/AMR>`

Specifies which audio codec to use when empty INVITEs are not allowed. Default: G711u .

Example: `xConfiguration Zones Zone 1 DNS Interworking SIP Audio DefaultCodec: G711u`

xConfiguration Zones Zone [1..1000] DNS Interworking SIP EmptyInviteAllowed: <On/Off>

Controls if the Expressway will generate a SIP INVITE message with no SDP to send to this zone. INVITEs with no SDP mean that the destination device is asked to initiate the codec selection, and are used when the call has been interworked locally from H.323. Default: On.

On: SIP INVITEs with no SDP will be generated and sent to this neighbor.

Off: SIP INVITEs will be generated and a pre-configured SDP will be inserted before the INVITEs are sent to this neighbor.

Example: `xConfiguration Zones Zone 1 DNS Interworking SIP EmptyInviteAllowed: On`

xConfiguration Zones Zone [1..1000] DNS Interworking SIP Video DefaultBitrate: <64..65535>

Specifies which video bit rate to use when empty INVITEs are not allowed. Default: 384 .

Example: `xConfiguration Zones Zone 1 DNS Interworking SIP Video DefaultBitrate: 384`

xConfiguration Zones Zone [1..1000] DNS Interworking SIP Video DefaultCodec: <None/H261/H263/H263p/H263pp/H264>

Specifies which video codec to use when empty INVITEs are not allowed. Default: H263 .

Example: `xConfiguration Zones Zone 1 DNS Interworking SIP Video DefaultCodec: H263`

xConfiguration Zones Zone [1..1000] DNS Interworking SIP Video DefaultResolution: <None/QCIF/CIF/4CIF/SIF/4SIF/VGA/SVGA/XGA>

Specifies which video resolution to use when empty INVITEs are not allowed. Default: CIF .

Example: `xConfiguration Zones Zone 1 DNS Interworking SIP Video DefaultResolution: CIF`

xConfiguration Zones Zone [1..1000] DNS SIP Default Transport: <UDP/TCP/TLS>

Determines which transport type is used for SIP calls from the DNS zone, when DNS NAPTR records and SIP URI parameters do not provide the preferred transport information. RFC 3263 suggests that UDP should be used. Default: UDP.

Example: `xConfiguration Zones Zone [1..1000] DNS SIP Default Transport: UDP`

xConfiguration Zones Zone [1..1000] DNS SIP Media AesGcm Support: <Off/On>

Enables AES GCM algorithms to encrypt/decrypt media passing through this zone. Default: Off.

Example: `xConfiguration Zones Zone 1 DNS SIP Media AesGcm Support: On`

xConfiguration Zones Zone [1..1000] DNS SIP SipUpdateRefresh Support: <Off/On>

Determines whether session refresh by SIP UPDATE message is supported in this zone.

On: This zone sends SIP UPDATE messages for SIP session refresh.

Off: This zone does not send SIP UPDATE messages for SIP session refresh.

Default: Off.

Example: `xConfiguration Zones Zone 1 DNS SIP SipUpdateRefresh Support: On`

xConfiguration Zones Zone [1..1000] DNS SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

The media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Default: Auto.

On: All media must be encrypted.

Off: All media must be unencrypted.

BestEffort: Use encryption if available otherwise fallback to unencrypted media.

Auto: No media encryption policy is applied.

Example: `xConfiguration Zones Zone 1 DNS SIP Media Encryption Mode: Auto`

xConfiguration Zones Zone [1..1000] DNS SIP Media ICE Support: <On/Off>

Controls whether ICE is supported by the devices in the zone. Default: Off.

On: This zone supports ICE.

Off: This zone does not support ICE.

Example: `xConfiguration Zones Zone 1 DNS SIP Media ICE Support: Off`

xConfiguration Zones Zone [1..1000] DNS SIP Media ICEPassThrough Support: <On/Off>

Controls whether ICE Pass Through is supported by the devices in the zone. Default: Off

On: This zone supports ICE Pass Through.

Off: This zone does not support ICE Pass Through.

Example: `xConfiguration Zones Zone 1 DNS SIP Media ICEPassThrough Support: On`

xConfiguration Zones Zone [1..1000] DNS SIP Poison Mode: <On/Off>

Determines whether SIP requests sent out to this zone will be "poisoned" such that if they are received by the local Expressway again they will be rejected. Default: Off .

On: SIP requests sent out via this zone that are received again by this Expressway will be rejected.

Off: SIP requests sent out via this zone that are received by this Expressway again will be processed as normal.

Example: `xConfiguration Zones Zone 1 DNS SIP Poison Mode: Off`

xConfiguration Zones Zone [1..1000] DNS SIP PreloadedSipRoutes Accept: <Off/On>

Switch Preloaded SIP routes support On to enable this zone to process SIP INVITE requests that contain the Route header. Switch Preloaded SIP routes support Off if you want the zone to reject SIP INVITE requests containing this header.

Example: `xConfiguration Zones Zone 3 Neighbor SIP PreloadedSipRoutes Accept: On`

xConfiguration Zones Zone [1..1000] DNS SIP Record Route Address Type: <IP/Hostname>

Controls whether the Expressway uses its IP address or host name in the Record-Route or Path headers of outgoing SIP requests to this zone. Note: setting this value to Hostname also requires a valid DNS system host name to be configured on the Expressway. Default: IP.

Example: `xConfiguration Zones Zone 1 DNS SIP Record Route Address Type: IP`

xConfiguration Zones Zone [1..1000] DNS SIP SearchAutoResponse: <On/Off>

Controls what happens when the Expressway receives a SIP search that originated as an H.323 search, destined for this zone. Default: Off .

Off: a SIP OPTION message will be sent to the zone.

On: searches will be responded to automatically, without being forwarded to the zone.

Example: `xConfiguration Zones Zone 1 DNS SIP SearchAutoResponse: Off`

xConfiguration Zones Zone [1..1000] DNS SIP TLS Verify Mode: <On/Off>

Controls X.509 certificate checking between this Expressway and the destination system server returned by the DNS lookup. When enabled, the domain name submitted to the DNS lookup must be contained within the server's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes).

Default: Off.

Example: `xConfiguration Zones Zone 1 DNS SIP TLS Verify Mode: On`

xConfiguration Zones Zone [1..1000] DNS SIP TLS Verify Subject Name: <S: 0..128>

The certificate holder's name to look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes). If empty then the domain portion of the resolved URI is used.

Example: `xConfiguration Zones Zone 1 DNS SIP TLS Verify Subject Name: "example.com"`

xConfiguration Zones Zone [1..1000] DNS SIP UDP BFCP Filter Mode: <On/Off>

Determines whether INVITE requests sent to this zone filter out UDP/BFCP. This option may be required to enable interoperability with SIP devices that do not support the UDP/BFCP protocol. Default: Off .

On: any media line referring to the UDP/BFCP protocol is replaced with TCP/BFCP and disabled.

Off: INVITE requests are not modified.

Example: `xConfiguration Zones Zone 1 DNS SIP UDP BFCP Filter Mode: Off`

xConfiguration Zones Zone [1..1000] DNS ZoneProfile:

`<Default/Custom/CiscoUnifiedCommunicationsManager/CiscoUnifiedCommunicationsManagerBFCP/NortelCS1000/NonRegisteringDevice/LocalB2BUAService>`

Determines how the zone's advanced settings are configured.

Default: uses the factory defaults.

Custom: allows you to configure each setting individually.

Preconfigured profiles: alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system.

Example: `xConfiguration Zones Zone 1 DNS ZoneProfile: Default`

xConfiguration Zones Zone [1..1000] ENUM DNSSuffix: <S: 0, 128>

The DNS zone to append to the transformed E.164 number to create an ENUM host name which this zone is then queried for.

Example: `xConfiguration Zones Zone 2 ENUM DNSSuffix: "e164.arpa"`

xConfiguration Zones Zone [1..1000] H323 Mode: <On/Off>

Determines whether H.323 calls will be allowed to and from this zone. Default: On .

Example: `xConfiguration Zones Zone 2 H323 Mode: On`

xConfiguration Zones Zone [1..1000] HopCount: <1..255>

Specifies the hop count to be used when sending an alias search request to this zone. Note: if the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used. Default: 15 .

Example: `xConfiguration Zones Zone 2 HopCount: 15`

xConfiguration Zones Zone [1..1000] Name: <S: 1, 50>

Assigns a name to this zone.

Example: `xConfiguration Zones Zone 3 Name: "UK Sales Office"`

xConfiguration Zones Zone [1..1000] Neighbor Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. Default: DoNotCheckCredentials.

Example: `xConfiguration Zones Zone 3 Neighbor Authentication Mode: DoNotCheckCredentials`

xConfiguration Zones Zone [1..1000] Neighbor H323 CallSignaling Port: <1024..65534>

The port on the neighbor to use for H.323 calls to and from this Expressway. Default: 1720 .

Example: `xConfiguration Zones Zone 3 Neighbor H323 CallSignaling Port: 1720`

xConfiguration Zones Zone [1..1000] Neighbor H323 Port: <1024..65534>

The port on the neighbor to use for H.323 searches to and from this Expressway. Default: 1719 .

Example: `xConfiguration Zones Zone 3 Neighbor H323 Port: 1719`

xConfiguration Zones Zone [1..1000] Neighbor H323 SearchAutoResponse: <On/Off>

Determines what happens when the Expressway receives a H323 search, destined for this zone. Default: Off.

Off: an LRQ message will be sent to the zone.

On: searches will be responded to automatically, without being forwarded to the zone.

Example: `xConfiguration Zones Zone 3 Neighbor H323 SearchAutoResponse: Off`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP Audio DefaultCodec:

`<G711u/G711a/G722_48/G722_56/G722_64/G722_1_16/G722_1_24/G722_1_32/G722_1_48/G723_1/G728/G729/AACLD_48/AACLD_56/AACLD_64/AMR>`

Specifies which audio codec to use when empty INVITEs are not allowed. Default: G711u .

Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Audio DefaultCodec: G711u`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP EmptyInviteAllowed: <On/Off>

Determines whether the Expressway will generate a SIP INVITE message with no SDP to send to this zone. INVITEs with no SDP mean that the destination device is asked to initiate the codec selection, and are used when the call has been interworked locally from H.323. Default: On .

On: SIP INVITEs with no SDP will be generated and sent to this neighbor.

Off: SIP INVITEs will be generated and a pre-configured SDP will be inserted before the INVITEs are sent to this neighbor.

Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP EmptyInviteAllowed: On`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP Encryption EncryptSRTCP: <Yes/No>

Controls if the Expressway offers encrypted SRTCP in calls to this zone. The Expressway will send an INFO request. Default: No.

Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Encryption EncryptSRTCP: No`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP Search Strategy: <Options/Info>

Determines how the Expressway will search for SIP endpoints when interworking an H.323 call. Default: Options .

Options: the Expressway will send an OPTIONS request.

Info: the Expressway will send an INFO request.

Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Search Strategy: Options`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP Video DefaultBitrate: <64..65535>

Specifies which video bit rate to use when empty INVITEs are not allowed. Default: 384 .

Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Video DefaultBitrate: 384`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP Video DefaultCodec: <None/H261/H263/H263p/H263pp/H264>

Specifies which video codec to use when empty INVITEs are not allowed. Default: H263 .

Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Video DefaultCodec: H263`

xConfiguration Zones Zone [1..1000] Neighbor Interworking SIP Video DefaultResolution: <None/QCIF/CIF/4CIF/SIF/4SIF/VGA/SVGA/XGA>

Specifies which video resolution to use when empty INVITEs are not allowed. Default: CIF .

Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Video DefaultResolution: CIF`

xConfiguration Zones Zone [1..1000] Neighbor Monitor: <Yes/No>

Specifies whether the zone monitors the aliveness of its neighbor peers. H323 LRQs and/or SIP OPTIONS will be periodically sent to the peers. If any peer fails to respond, that peer will be marked as inactive. If no peer manages to respond the zone will be marked as inactive. Default: Yes.

Example: `xConfiguration Zones Zone 3 Neighbor Monitor: Yes`

xConfiguration Zones Zone [1..1000] Neighbor Peer [1..6] Address: <S:0,128>

Specifies the IP address or Fully Qualified Domain Name (FQDN) of the neighbor. If the neighbor zone is an Expressway cluster, this will be one of the peers in that cluster.

Example: `xConfiguration Zones Zone 3 Neighbor Peer 1 Address: "192.44.0.18"`

xConfiguration Zones Zone [1..1000] Neighbor Registrations: <Allow/Deny>

Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow .

Example: `xConfiguration Zones Zone 3 Neighbor Registrations: Allow`

xConfiguration Zones Zone [1..1000] Neighbor RetainConnectionOnParseErrorMode: <mode>

Controls how tolerant the system is of malformed or corrupt SIP messages.

DropAll: The system closes the SIP connection when it receives a malformed or corrupt SIP message.

RetainSome: The system maintains the SIP connection when it receives a SIP message with malformed, non-mandatory headers. It closes the connection if any mandatory headers are malformed.

RetainAll: The system maintains the SIP connection when it receives a SIP message with any malformed headers (including mandatory headers).

Default: DropAll.

Note

- The *Content-Length* header is an exception. If this header is missing or malformed, the connection is always closed, regardless of the mode.
- The connection is also always closed, regardless of the mode, if the Expressway receives more than 10 consecutive malformed messages.
- For CMR Cloud deployments, we recommend configuring RetainAll mode.

Example: `xConfiguration Zones Zone 3 RetainConnectionOnParseErrorMode: RetainSome`

xConfiguration Zones Zone [1..1000] Neighbor SIP Authentication Trust Mode: <On/Off>

Controls if authenticated SIP messages (ones containing a P-Asserted-Identity header) from this zone are trusted. Default: Off .

On: messages are trusted without further challenge.

Off: messages are challenged for authentication.

Example: `xConfiguration Zones Zone 3 Neighbor SIP Authentication Trust Mode: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP B2BUA Refer Mode: <Forward/Terminate>

Determines how SIP REFER requests are handled.

Forward: SIP REFER requests are forwarded to the target.

Terminate: SIP REFER requests are terminated by the Expressway.

Default: Forward

Example: `xConfiguration Zones Zone 3 Neighbor SIP B2BUA Refer Mode: Terminate`

xConfiguration Zones Zone [1..1000] Neighbor SIP B2BUA Replaces Mode: <Forward/Terminate>

Enables the Expressway to process load balancing INVITE messages from Meeting Server call bridge groups. Default: Forward

Terminate: Expressway B2BUA processes the INVITEs from the Meeting Server. Required to enable load balancing for endpoints that are registered to this Expressway, or to a neighboring VCS or Expressway.

Forward: Expressway proxies the INVITEs from the Meeting Server. This is an option if your endpoints are registered to Unified CM, because Unified CM could process those INVITEs instead.

Example: `xConfiguration Zones Zone 3 Neighbor SIP B2BUA Replaces Mode: Terminate`

xConfiguration Zones Zone [1..1000] Neighbor SIP B2BUA Service Identifier: <0..64>

The identifier that represents an instance of a local SIP Back-to-Back User Agent service.

Example: `xConfiguration Zones Zone 3 Neighbor SIP B2BUA Service Identifier: 1`

xConfiguration Zones Zone [1..1000] Neighbor SIP ClassFiveResponseLiveness: <Yes/No>

Specifies whether Class 5 SIP responses from neighbor peers result in the zone being considered alive for use. Default: Yes.

Example: `xConfiguration Zones Zone 3 Neighbor SIP ClassFiveResponseLiveness: Yes`

xConfiguration Zones Zone [1..1000] Neighbor SIP Encryption Mode: <Auto/Microsoft/Off>

Determines how the Expressway handles encrypted SIP calls on this zone. Default: Auto.

Auto: SIP calls are encrypted if a secure SIP transport (TLS) is used.

Microsoft: SIP calls are encrypted using MS-SRTP.

Off: SIP calls are never encrypted.

Example: `xConfiguration Zones Zone 3 Neighbor SIP Encryption Mode: Auto`

xConfiguration Zones Zone [1..1000] Neighbor SIP MIME Strip Mode: <On/Off>

Controls whether multipart MIME stripping is performed on requests from this zone. This must be set to On for connections to a Microsoft Office Communications Server 2007. Default: Off.

Example: `xConfiguration Zones Zone 3 Neighbor SIP MIME Strip Mode: Off`

xConfiguration Zones Zone [1..1000] Neighbor SIP Media AesGcm Support: <Off/On>

Enables AES GCM algorithms to encrypt/decrypt media passing through this zone. Default: Off.

Example: `xConfiguration Zones Zone 1 Neighbor SIP Media AesGcm Support: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

The media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Default: Auto

On: All media must be encrypted.

Off: All media must be unencrypted.

BestEffort: Use encryption if available otherwise fallback to unencrypted media.

Auto: No media encryption policy is applied.

Example: `xConfiguration Zones Zone 3 Neighbor SIP Media Encryption Mode: Auto`

xConfiguration Zones Zone [1..1000] Neighbor SIP Media ICE Support: <On/Off>

Controls whether ICE is supported by the devices in the zone. Default: Off

On: This zone supports ICE.

Off: This zone does not support ICE.

Example: `xConfiguration Zones Zone 3 Neighbor SIP Media ICE Support: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP Media ICEPassThrough Support: <On/Off>

Controls whether ICE Pass Through is supported by the devices in the zone. Default: Off

On: This zone supports ICE Pass Through.

Off: This zone does not support ICE Pass Through.

Example: `xConfiguration Zones Zone 3 Neighbor SIP Media ICEPassThrough Support: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP MediaRouting Mode: <Auto/Signaled/Latching>

How the Expressway handles media for calls to and from this neighbor, and where it will forward the media destined for this neighbor. Default: Auto. .

Signaled: media is always taken for calls to and from this neighbor. It will be forwarded as signaled in the SDP received from this neighbor.

Latching: media is always taken for calls to and from this neighbor. It will be forwarded to the IP address and port from which media from this neighbor is received.

Auto: media is only taken if the call is a traversal call. If this neighbor is behind a NAT the Expressway will forward the media to the IP address and port from which media from this zone is received (latching). Otherwise it will forward the media to the IP address and port signaled in the SDP (signaled).

Example: `xConfiguration Zones Zone 3 Neighbor SIP MediaRouting Mode: Auto`

xConfiguration Zones Zone [1..1000] Neighbor SIP Multistream Mode: <Off/On>

Controls if the Expressway allows Multistream to and from devices in this zone. Default: On

On: allow Multistream

Off: disallow Multistream.

Example: `xConfiguration Zones Zone 1 Neighbor SIP Multistream Mode: Off`

xConfiguration Zones Zone [1..1000] Neighbor SIP Poison Mode: <On/Off>

Controls whether SIP requests sent out to this zone will be "poisoned" such that if they are received by the local Expressway again they will be rejected. Default: Off .

On: SIP requests sent out via this zone that are received again by this Expressway will be rejected.

Off: SIP requests sent out via this zone that are received by this Expressway again will be processed as normal.

Example: `xConfiguration Zones Zone 3 Neighbor SIP Poison Mode: Off`

xConfiguration Zones Zone [1..1000] Neighbor SIP Port: <1024..65534>

Specifies the port on the neighbor to be used for SIP calls to and from this Expressway. Default: 5061 .

Example: `xConfiguration Zones Zone 3 Neighbor SIP Port: 5061`

xConfiguration Zones Zone [1..1000] Neighbor SIP PreloadedSipRoutes Accept: <Off/On>

Switch Preloaded SIP routes support On to enable this zone to process SIP INVITE requests that contain the Route header. Switch Preloaded SIP routes support Off if you want the zone to reject SIP INVITE requests containing this header.

Example: `xConfiguration Zones Zone 3 Neighbor SIP PreloadedSipRoutes Accept: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP ProxyRequire Strip List: <S: 0,255>

A comma separated list of option tags to search for and remove from Proxy-Require headers in SIP requests received from this zone. By default, no option tags are specified.

Example: `xConfiguration Zones Zone 3 Neighbor SIP ProxyRequire Strip List: "com.example.something,com.example.somethingelse"`

xConfiguration Zones Zone [1..1000] Neighbor SIP RFC3327 Enabled: <Yes/No>

Controls whether the Expressway will insert RFC3327 Path headers when proxying REGISTER messages toward this zone. If disabled the Expressway will instead rewrite the contact header to allow interworking with SIP registrars that do not support RFC3327. Default: Yes.

Example: `xConfiguration Zones Zone [1..1000] Neighbor SIP RFC3327 Enabled: Yes`

Note In version X8.9 we introduced a toggle that controls this feature for the automatically created neighbor zones used for MRA. In that version, on those zones, the default is No. See `xConfiguration CollaborationEdge RFC3327Enabled`.

xConfiguration Zones Zone [1..1000] Neighbor SIP Record Route Address Type: <IP/Hostname>

Controls whether the Expressway uses its IP address or host name in the Record-Route or Path headers of outgoing SIP requests to this zone. Note: setting this value to Hostname also requires a valid DNS system host name to be configured on the Expressway. Default: IP.

Example: `xConfiguration Zones Zone 3 Neighbor SIP Record Route Address Type: IP`

xConfiguration Zones Zone [1..1000] Neighbor SIP SearchAutoResponse: <On/Off>

Controls what happens when the Expressway receives a SIP search that originated as an H.323 search, destined for this zone. Default: Off .

Off: a SIP OPTION message will be sent to the zone.

On: searches will be responded to automatically, without being forwarded to the zone.

Example: `xConfiguration Zones Zone 3 Neighbor SIP SearchAutoResponse: Off`

xConfiguration Zones Zone [1..1000] Neighbor SIP SipUpdateRefresh Support: <On/Off>

Determines whether session refresh by SIP UPDATE message is supported in this zone.

On: This zone sends SIP UPDATE messages for SIP session refresh.

Off: This zone does not send SIP UPDATE messages for SIP session refresh.

Default: Off

Example: `xConfiguration Zones Zone 3 Neighbor SIP SipUpdateRefresh Support: Off`

xConfiguration Zones Zone [1..1000] Neighbor SIP TLS Verify Mode: <On/Off>

Controls X.509 certificate checking and mutual authentication for inbound and outbound connections between this Expressway and the neighbor system. When enabled, the neighbor system's FQDN or IP address, as specified in the Peer address field, must be contained within the neighbor's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes). Default: Off .

Example: `xConfiguration Zones Zone 3 Neighbor SIP TLS Verify Mode: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP Transport: <UDP/TCP/TLS>

Determines which transport type will be used for SIP calls to and from this neighbor. Default: TLS .

Example: `xConfiguration Zones Zone 3 Neighbor SIP Transport: TLS`

xConfiguration Zones Zone [1..1000] Neighbor SIP UDP BFCP Filter Mode: <On/Off>

Determines whether INVITE requests sent to this zone filter out UDP/BFCP. This option may be required to enable interoperability with SIP devices that do not support the UDP/BFCP protocol. Default: Off .

On: any media line referring to the UDP/BFCP protocol is replaced with TCP/BFCP and disabled.

Off: INVITE requests are not modified.

Example: `xConfiguration Zones Zone 3 Neighbor SIP UDP BFCP Filter Mode: Off`

xConfiguration Zones Zone 1 Neighbor SIP UDP IX Filter Mode: <On/Off>

Determines whether INVITE requests sent to this zone filter out UDP/UDT/IX or UDP/DTLS/UDT/IX.

This option may be required to enable interoperability with SIP devices that do not support the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol. Default: Off.

On: any media line referring to the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol is replaced with RTP/AVP and disabled.

Off: INVITE requests are not modified.

Example: `xConfiguration Zones Zone 1 neighbor SIP UDP IX Filter Mode: On`

xConfiguration Zones Zone [1..1000] Neighbor SIP UPDATE Strip Mode: <On/Off>

Determines whether the Expressway strips the UPDATE method from the Allow header of all requests and responses going to and from this zone. Default: Off .

Example: `xConfiguration Zones Zone 3 Neighbor SIP UPDATE Strip Mode: Off`

xConfiguration Zones Zone [1..1000] Neighbor SignalingRouting Mode: <Auto/Always>

Specifies how the Expressway handles the signaling for calls to and from this neighbor. Default: Auto.

Auto: Signaling will be taken as determined by the Call Routed Mode configuration.

Always: Signaling will always be taken for calls to or from this neighbor, regardless of the Call Routed Mode configuration.

Example: `xConfiguration Zones Zone 3 Neighbor SignalingRouting Mode: Auto`

xConfiguration Zones Zone [1..1000] Neighbor SRV MaxPeers: <1..30>

Specifies the maximum number of peers the Expressway can register with when the given neighbor zone is configured with an SRV record lookup.

Examples: `xConfiguration Zones Zone 1 Neighbor SRV MaxPeers: 30`

xConfiguration Zones Zone [1..1000] Neighbor ZoneProfile:

`<Default/Custom/CiscoUnifiedCommunicationsManager/CiscoUnifiedCommunicationsManagerBFCP/NortelCS1000/NonRegisteringDevice/LocalB2BUAService>`

Determines how the zone's advanced settings are configured.

Default: uses the factory defaults.

Custom: allows you to configure each setting individually.

Preconfigured profiles: alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system.

Example: `xConfiguration Zones Zone 3 Neighbor ZoneProfile: Default`

xConfiguration Zones Zone [1..1000] SIP Mode: <On/Off>

Determines whether SIP calls will be allowed to and from this zone. Default: On.

Example: `xConfiguration Zones Zone 3 SIP Mode: On`

xConfiguration Zones Zone [1..1000] TraversalClient Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. Default: DoNotCheckCredentials.

Example: `xConfiguration Zones Zone 4 TraversalClient Authentication Mode: DoNotCheckCredentials`

xConfiguration Zones Zone [1..1000] TraversalClient Authentication Password: <S: 0,215>

The password used by the Expressway when connecting to the traversal server. The maximum plaintext length is 128 characters, which is then encrypted.

Example: `xConfiguration Zones Zone 4 TraversalClient Authentication Password: "password123"`

xConfiguration Zones Zone [1..1000] TraversalClient Authentication UserName: <S: 0,128>

The user name used by the Expressway when connecting to the traversal server.

Example: `xConfiguration Zones Zone 4 TraversalClient Authentication UserName: "clientname"`

xConfiguration Zones Zone [1..1000] TraversalClient DisconnectOnFailInterval: <10>

When a peer fails to respond to an OPTIONS ping, the Traversal Client zone enters an error state. If the DISCONNECT_ON_FAIL_INTERVAL is configured, then, while in the error state the expressway node disconnects the connection before sending the OPTIONS ping to ensure connectivity robustness. The disconnect occurs at intervals according to the DISCONNECT_ON_FAIL_INTERVAL.

By default, this flag is disabled. To enable, set the value range from 0 to 3600 seconds

Min Value = 0.

Max Value = 3600.

Default: 0 (Disabled)

Example: `xConfiguration Zones Zone 1 TraversalClient DisconnectOnFailInterval: "10"`

xConfiguration Zones Zone [1..1000] TraversalClient H323 Port: <1024..65534>

The port on the traversal server to use for H.323 firewall traversal calls from this Expressway. If the traversal server is an Expressway-E, this must be the port number that is configured on the Expressway-E's traversal server zone associated with this Expressway.

Example: `xConfiguration Zones Zone 4 TraversalClient H323 Port: 2777`

xConfiguration Zones Zone [1..1000] TraversalClient H323 Protocol: <Assent/H46018>

Determines which of the two firewall traversal protocols will be used for calls to and from the traversal server. Note: the same protocol must be set on the server for calls to and from this traversal client. Default: Assent.

Example: `xConfiguration Zones Zone 4 TraversalClient H323 Protocol: Assent`

xConfiguration Zones Zone [1..1000] TraversalClient Peer [1..6] Address: <S:0,128>

Specifies the IP address or Fully Qualified Domain Name (FQDN) of the traversal server. If the traversal server is an Expressway-E cluster, this will be one of the peers in that cluster.

Example: `xConfiguration Zones Zone 4 TraversalClient Peer 1 Address: "10.192.168.1"`

xConfiguration Zones Zone [1..1000] TraversalClient Registrations: <Allow/Deny>

Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow.

Example: `xConfiguration Zones Zone 4 TraversalClient Registrations: Allow`

xConfiguration Zones Zone [1..1000] TraversalClient RetryInterval: <1..65534>

The interval (in seconds) with which a failed attempt to establish a connection to the traversal server should be retried. Default: 120.

Example: `xConfiguration Zones Zone 4 TraversalClient RetryInterval: 120`

xConfiguration Zones Zone [1..1000] TraversalClient SIP SipUpdateRefresh Support: <Off/On>

Determines whether session refresh by SIP UPDATE message is supported in this zone.

On: This zone sends SIP UPDATE messages for SIP session refresh.

Off: This zone does not send SIP UPDATE messages for SIP session refresh.

Default: Off

Example: `xConfiguration Zones Zone 1 TraversalClient SIP SipUpdateRefresh Support: On`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Media AesGcm Support: <Off/On>

Enables AES GCM algorithms to encrypt/decrypt media passing through this zone. Default: Off.

Example: `xConfiguration Zones Zone 1 TraversalClient SIP Media AesGcm Support: On`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

The media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Default: Auto.

On: All media must be encrypted.

Off: All media must be unencrypted.

BestEffort: Use encryption if available otherwise fallback to unencrypted media.

Auto: No media encryption policy is applied.

Example: `xConfiguration Zones Zone 4 TraversalClient SIP Media Encryption Mode: Auto`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Media ICE Support: <On/Off>

Controls whether ICE is supported by the devices in the zone. Default: Off

On: This zone supports ICE.

Off: This zone does not support ICE.

Example: `xConfiguration Zones Zone 4 TraversalClient SIP Media ICE Support: On`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Media ICEPassThrough Support: <On/Off>

Controls whether ICE Pass Through is supported by the devices in the zone. Default: Off

On: This zone supports ICE Pass Through.

Off: This zone does not support ICE Pass Through.

Example: `xConfiguration Zones Zone 4 TraversalClient SIP Media ICEPassThrough Support: On`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Multistream Mode: <Off/On>

Controls if the Expressway allows Multistream to and from devices in this zone. Default: On

On: allow Multistream

Off: disallow Multistream.

Example: `xConfiguration Zones Zone 1 TraversalClient SIP Multistream Mode: Off`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Poison Mode: <On/Off>

Controls whether SIP requests sent out to this zone are "poisoned" such that if they are received by the local Expressway again they will be rejected. Default: Off .

On: SIP requests sent out via this zone that are received again by this Expressway will be rejected.

Off: SIP requests sent out via this zone that are received by this Expressway again will be processed as normal.

Example: `xConfiguration Zones Zone 4 TraversalClient SIP Poison Mode: Off`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Port: <1024..65534>

Specifies the port on the traversal server to be used for SIP calls from this Expressway. If your traversal server is an Expressway-E, this must be the port number that has been configured in the traversal server zone for this Expressway.

Example: `xConfiguration Zones Zone 4 TraversalClient SIP Port: 5061`

xConfiguration Zones Zone [1..1000] TraversalClient SIP PreloadedSipRoutes Accept: <Off/On>

Switch Preloaded SIP routes support On to enable this zone to process SIP INVITE requests that contain the Route header. Switch Preloaded SIP routes support Off if you want the zone to reject SIP INVITE requests containing this header.

Example: `xConfiguration Zones Zone 3 Neighbor SIP PreloadedSipRoutes Accept: On`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Protocol: <Assent/TURN/ICE>

Determines which firewall traversal protocol will be used for SIP calls to and from the traversal server. Note: the same protocol must be set on the server for calls to and from this traversal client. Default: Assent.

Example: `xConfiguration Zones Zone 4 TraversalClient SIP Protocol: Assent`

xConfiguration Zones Zone [1..1000] TraversalClient SIP TLS Verify Mode: <On/Off>

Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal server. When enabled, the server's FQDN or IP address, as specified in the Peer address field, must be contained within the server's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes). Default: Off.

Example: `xConfiguration Zones Zone 4 TraversalClient SIP TLS Verify Mode: On`

xConfiguration Zones Zone [1..1000] TraversalClient SIP Transport: <TCP/TLS>

Determines which transport type will be used for SIP calls to and from the traversal server. Default: TLS .

Example: `xConfiguration Zones Zone 4 TraversalClient SIP Transport: TLS`

xConfiguration Zones Zone [1..1000] TraversalServer Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Controls how the Expressway authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. Default: DoNotCheckCredentials.

Example: `xConfiguration Zones Zone 5 TraversalServer Authentication Mode: DoNotCheckCredentials`

xConfiguration Zones Zone [1..1000] TraversalServer Authentication UserName: <S: 0,128>

The name used by the traversal client when authenticating with the traversal server. If the traversal client is an Expressway, this must be the Expressway's authentication user name. If the traversal client is a gatekeeper, this must be the gatekeeper's System Name.

Example: `xConfiguration Zones Zone 5 TraversalServer Authentication UserName: "User123"`

xConfiguration Zones Zone [1..1000] TraversalServer H323 H46019 Demultiplexing Mode: <On/Off>

Determines whether the Expressway will operate in demultiplexing mode for calls from the traversal client. Default: Off .

On: allows use of the same two ports for all calls.

Off: each call will use a separate pair of ports for media.

Example: `xConfiguration Zones Zone 5 TraversalServer H323 H46019 Demultiplexing Mode: Off`

xConfiguration Zones Zone [1..1000] TraversalServer H323 Port: <1024..65534>

Specifies the port on the Expressway being used for H.323 firewall traversal from this traversal client. Default: 6001, incrementing by 1 for each new zone.

Example: `xConfiguration Zones Zone 5 TraversalServer H323 Port: 2777`

xConfiguration Zones Zone [1..1000] TraversalServer H323 Protocol: <Assent/H46018>

Determines which of the two firewall traversal protocols will be used for calls to and from the traversal client. Note: the same protocol must be set on the client for calls to and from this traversal server. Default: Assent .

Example: `xConfiguration Zones Zone 5 TraversalServer H323 Protocol: Assent`

xConfiguration Zones Zone [1..1000] TraversalServer Registrations: <Allow/Deny>

Controls whether proxied SIP registrations routed through this zone are accepted. Default: Allow .

Example: `xConfiguration Zones Zone 5 TraversalServer Registrations: Allow`

xConfiguration Zones Zone [1..1000] TraversalServer SIP SipUpdateRefresh Support: <Off/On>

Determines whether session refresh by SIP UPDATE message is supported in this zone.

On: This zone sends SIP UPDATE messages for SIP session refresh.

Off: This zone does not send SIP UPDATE messages for SIP session refresh.

Default: Off.

Example: `xConfiguration Zones Zone 1 TraversalServer SIP SipUpdateRefresh Support: On`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Media AesGcm Support: <Off/On>

Enables AES GCM algorithms to encrypt/decrypt media passing through this zone. Default: Off.

Example: `xConfiguration Zones Zone 1 TraversalServer SIP Media AesGcm Support: On`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Media Encryption Mode: <Off/On/BestEffort/Auto>

The media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. Default: Auto

On: All media must be encrypted.

Off: All media must be unencrypted.

BestEffort: Use encryption if available otherwise fallback to unencrypted media.

Auto: No media encryption policy is applied.

Example: `xConfiguration Zones Zone 5 TraversalServer SIP Media Encryption Mode: Auto`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Media ICE Support: <On/Off>

Controls whether ICE is supported by the devices in the zone. Default: Off

On: This zone supports ICE.

Off: This zone does not supports ICE.

Example: `xConfiguration Zones Zone 5 TraversalServer SIP Media ICE Support: On`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Media ICEPassThrough Support: <On/Off>

Controls whether ICE Pass Through is supported by the devices in the zone. Default: Off

On: This zone supports ICE Pass Through.

Off: This zone does not supports ICE Pass Through.

Example: `xConfiguration Zones Zone 5 TraversalServer SIP Media ICEPassThrough Support: On`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Multistream Mode: <Off/On>

Controls if the Expressway allows Multistream to and from devices in this zone. Default: On

On: allow Multistream

Off: disallow Multistream.

Example: `xConfiguration Zones Zone 1 TraversalServer SIP Multistream Mode: Off`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Poison Mode: <On/Off>

Controls whether SIP requests sent out to this zone are "poisoned" such that if they are received by the local Expressway again they will be rejected. Default: Off .

On: SIP requests sent out via this zone that are received again by this Expressway will be rejected.

Off: SIP requests sent out via this zone that are received by this Expressway again will be processed as normal.

Example: `xConfiguration Zones Zone 5 TraversalServer SIP Poison Mode: Off`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Port: <1024..65534>

The port on the Expressway being used for SIP firewall traversal from this traversal client. Default: 7001, incrementing by 1 for each new zone.

Example: `xConfiguration Zones Zone 5 TraversalServer SIP Port: 5061`

xConfiguration Zones Zone [1..1000] TraversalServer SIP PreloadedSipRoutes Accept: <Off/On>

Switch Preloaded SIP routes support On to enable this zone to process SIP INVITE requests that contain the Route header. Switch Preloaded SIP routes support Off if you want the zone to reject SIP INVITE requests containing this header.

Example: `xConfiguration Zones Zone 3 Neighbor SIP PreloadedSipRoutes Accept: On`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Protocol: <Assent/TURN/ICE>

Determines which firewall traversal protocol will be used for SIP calls to and from the traversal client. Note: the same protocol must be set on the client for calls to and from this traversal server. Default: Assent.

Example: `xConfiguration Zones Zone 5 TraversalServer SIP Protocol: Assent`

xConfiguration Zones Zone [1..1000] TraversalServer SIP TLS Verify Mode: <On/Off>

Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal client. If enabled, a TLS verify subject name must be specified. Default: Off.

Example: `xConfiguration Zones Zone 5 TraversalServer SIP TLS Verify Mode: On`

xConfiguration Zones Zone [1..1000] TraversalServer SIP TLS Verify Subject Name: <S: 0,128>

The certificate holder's name to look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes).

Example: `xConfiguration Zones Zone 5 TraversalServer SIP TLS Verify Subject Name: "myclientname"`

xConfiguration Zones Zone [1..1000] TraversalServer SIP Transport: <TCP/TLS>

Determines which of the two transport types will be used for SIP calls between the traversal client and Expressway. Default: TLS .

Example: `xConfiguration Zones Zone 5 TraversalServer SIP Transport: TLS`

xConfiguration Zones Zone [1..1000] TraversalServer TCPProbe KeepAliveInterval: <1..65534>

Sets the interval (in seconds) with which the traversal client will send a TCP probe to the Expressway once a call is established, in order to keep the firewall's NAT bindings open. Default: 20.

Example: `xConfiguration Zones Zone 5 TraversalServer TCPProbe KeepAliveInterval: 20`

xConfiguration Zones Zone [1..1000] TraversalServer TCPProbe RetryCount: <1..65534>

Sets the number of times the traversal client will attempt to send a TCP probe to the Expressway. Default: 5 .

Example: `xConfiguration Zones Zone 5 TraversalServer TCPProbe RetryCount: 5`

xConfiguration Zones Zone [1..1000] TraversalServer TCPProbe RetryInterval: <1..65534>

Sets the frequency (in seconds) with which the traversal client will send a TCP probe to the Expressway. Default: 2 .

Example: `xConfiguration Zones Zone 5 TraversalServer TCPProbe RetryInterval: 2`

xConfiguration Zones Zone [1..1000] TraversalServer UDPProbe KeepAliveInterval: <1..65534>

Sets the interval (in seconds) with which the traversal client will send a UDP probe to the Expressway once a call is established, in order to keep the firewall's NAT bindings open. Default: 20.

Example: `xConfiguration Zones Zone 5 TraversalServer UDPProbe KeepAliveInterval: 20`

xConfiguration Zones Zone [1..1000] TraversalServer UDPProbe RetryCount: <1..65534>

Sets the number of times the traversal client will attempt to send a UDP probe to the Expressway. Default: 5.

Example: `xConfiguration Zones Zone 5 TraversalServer UDPProbe RetryCount: 5`

xConfiguration Zones Zone [1..1000] TraversalServer UDPProbe RetryInterval: <1..65534>

Sets the frequency (in seconds) with which the traversal client will send a UDP probe to the Expressway. Default: 2.

Example: `xConfiguration Zones Zone 5 TraversalServer UDPProbe RetryInterval: 2`

xConfiguration Zones Zone [1..1000] Type: <Neighbor/TraversalClient/TraversalServer/ENUM/DNS>

Determines the nature of the specified zone, in relation to the local Expressway.

Neighbor: the new zone will be a neighbor of the local Expressway.

TraversalClient: there is a firewall between the zones, and the local Expressway is a traversal client of the new zone.

TraversalServer: there is a firewall between the zones and the local Expressway is a traversal server for the new zone.

ENUM: the new zone contains endpoints discoverable by ENUM lookup.

DNS: the new zone contains endpoints discoverable by DNS lookup.

Example: `xConfiguration Zones Zone 3 Type: Neighbor`

xConfiguration license smart debug: <error/trace/debug/all>

Enables debugging for Smart Licensing. Default: Error.

Error: Logs errors encountered in Smart Licensing.

Trace: Logs trace messages during normal Smart Licensing operations.

Debug: Logs debug messages.

All: Enables all three levels. (Peer-specific)

Example: `xConfiguration license smart debug: all`

xConfiguration license smart deregister: <On/Off>

The product reverts to evaluation mode providing the evaluation period has not expired. All license entitlements used for the product are released immediately to the virtual account and are available for other product instances to use it. (Peer-specific)

Example: `xConfiguration license smart deregister: On`

xConfiguration license smart privacy: <none/all/hostname/version>

Use if hostname and IP address of this product instance must not be exchanged with the Cisco Smart Software Manager or Cisco Smart Software Manager Satellite. (Peer-specific)

Example: `xConfiguration license smart privacy: all`

xConfiguration license smart register idtoken: <String>

Use the Product Instance Registration token that you generated from Smart Software Manager or your Smart Software Manager satellite to register the product. (Peer-specific)

Example: `xConfiguration license smart register idtoken: <Token>`

xConfiguration license smart renew ID: <On/Off>

Perform this operation if automatic registration renewal fails due to network connectivity issues with Cisco Smart Software Manager. (Peer-specific)

Example: `xConfiguration license smart renew ID: On`

xConfiguration license smart renew auth: <On/Off>

Perform this operation if automatic authorization status renewal failed due to network connectivity issues with Cisco Smart Software Manager. (Peer-specific)

Example: `xConfiguration license smart renew auth: On`

xConfiguration license smart transport: <direct/satellite>

Determines how this product instance communicate with Cisco Smart Software Manager to send and receive usage information.

Direct: Communicates directly over the internet to the Cisco Smart Software Manager.

Satellite: Communicates through a Smart Software Manager satellite deployed on your premises.

Example: `xConfiguration license smart transport: direct`

xConfiguration license smart reregister: <String>

Perform this operation to reregister the product instance in the following cases: Previous registration attempt of this product instance failed due to network connectivity issue and you want to reregister after resolving this issue. To reregister the product instance, already registered with a virtual account, to a different virtual account. (Peer-specific)

Example: `xConfiguration license smart reregister: <Token>`

xConfiguration license smart url: <String>

Enter the URL of the Cisco Smart Software Manager satellite server. (Peer-specific)

Example: `xConfiguration license smart url: http://www.alpha.crate.cisco.com/Transport gateway`

Command Reference — xCommand

The **xCommand** group of commands are used to add and delete items and issue system commands.

The following section lists all the currently available **xCommand** commands.

To issue a command, type the command as shown, followed by one or more of the given parameters and values. The valid values for each parameter are indicated in the angle brackets following each parameter, using the following notation:

Format	Meaning
<0..63>	Indicates an integer value is required. The numbers indicate the minimum and maximum value. In this example the value must be in the range 0 to 63.
<S: 7,15>	An **S** indicates a string value, to be enclosed in quotation marks, is required. The numbers indicate the minimum and maximum number of characters for the string. In this example the string must be between 7 and 15 characters long.
<Off/Direct/Indirect>	Lists the set of valid values for the command. Do not enclose the value in quotation marks
(r)	Indicates that this is a required parameter. Note that the (r) is not part of the command itself.

To obtain information about using each of the **xCommand** commands from within the CLI, type:

- **xCommand** or **xCommand ?** to return a list of all available **xCommand** commands.
- **xCommand ??** to return all current **xCommand** commands, along with a description of each command, a list of its parameters, and for each parameter its valuespaces and description.
- **xCommand <command> ?** to return a description of the command, a list of its parameters, and for each parameter its valuespaces and description.

About the set-access command (experimental)

The set-access command enables access to Expressway internal system commands. **These commands exist for the use of Cisco support and development teams only.** Do not access the commands unless it is under the advice and supervision of your Cisco support representative.

Caution Incorrect usage of these commands could cause the system operation to become unstable, cause performance problems, and cause persistent corruption of system configuration.

To use set-access:

1. Log into the CLI as administrator.
2. Type `set-access qwertsys`

   This enables the system commands (“sys-”) that are associated with set-access.

3. Enter ? to list the available commands.

xCommand Commands

All the available **xCommand** commands are listed in the table below:

Table 20: xCommand CLI reference

xCommand ACME Delete Pending Cert Deletes a pending certificate. *Domain: <String>* A pending certificate is one that has been signed by an ACME provider and which may have/not have been deployed to the Expressway. If passed no arguments or empty string, the command deletes the pending server certificate, otherwise it will delete pending certificate for the specified domain. Examples: `xCommand ACME Delete Pending Cert` `xCommand ACME Delete Pending Cert Domain:"example.com"`
xCommand ACME Deploy Deploys a pending certificate. *Domain: <String>* *ReloadCerts: <On/Off>* If passed no arguments, the command deploys the pending server certificate and reloads the certificate for the required processes. Otherwise it deploys the certificate for the specified domain and reloads the certificate if specified by ReloadCerts parameter. Examples: `xCommand ACME Deploy` `xCommand ACME Deploy Domain:"example.com" ReloadCerts:"On"`
xCommand ACME Get Pending Cert Fetches a pending certificate. *Domain: <String>* A pending certificate is one that has been signed by an ACME provider and which may have/not have been deployed to the Expressway. If passed no arguments the command fetches the server certificate, otherwise it fetches the certificate for the specified domain. Examples: `xCommand ACME Get Pending Cert` `xCommand ACME Get Pending Cert Domain:"example.com"`

xCommand ACME Providers Read

Reads information about the ACME provider.

ProviderUuid: <"Default"/String>

If passed no arguments the command will return information about all providers in the database. The string "Default" returns information about the default provider. Provide a UUID to return information about that specific provider.

Examples: `xCommand ACME Providers Read`

```
xCommand ACME Providers Read ProviderUuid: "Default"
```

```
xCommand ACME Providers Read ProviderUuid: "Provider-UUID"
```

xCommand ACME Providers Write

Updates information about the provider.

Default: <On/Off>

Email(r): <String>

Name: <String>

ProviderUuid(r): <"Default"/String>

TermsOfService(r): <Accepted>

Url: <String>

You must supply ProviderUuid, Email, and TermsOfService arguments. The command only allows you to update the Email address and Terms Of Service for a particular provider. It ignores all other arguments that you supply.

Example: `xCommand ACME Providers Write ProviderUuid: "Default" Email: "new-email@example.com" TermsOfService: "Accepted"`

xCommand ACME Reset

Resets the ACME service on the Expressway-E, removing all configuration issued through CLI, Rest API, or web interface.

Action: <execute>

The command can only be invoked on Expressway-E. It cannot run if SIGN, DISCARD, or DEPLOY commands are in progress. Acmereset cannot run unless ACME service is disabled for all domain certificates and the server certificate.

Example: `xCommand ACME Reset execute`

```
xCommand ACME Reset Action: "execute"
```

xCommand ACME Revoke

Revokes an ACME certificate.

CertPath: <String>

Provider: <String>

Before you can revoke an ACME certificate, you must prove to the provider that you control the domain name/SAN entries in that certificate.

To validate this control, you must use the normal submit and sign process to generate a new certificate containing the same domain name/SAN entries as the original certificate.

After you receive the new certificate, revoke the old one using `acmerevoke` with the path to the certificate

Example, using the default ACME provider: `xCommand ACME Revoke "/path_to_cert_to_be_revoked"`

Example, using a specific ACME provider: `xCommand ACME Revoke CertPath:"/path_to_cert_to_be_revoked" Provider:"ACME_Provider_Name"`

xCommand ACME Settings Read

Reads ACME settings.

Domain: <String>

Enter this command without parameters to read the ACME settings for the server certificate. Otherwise, supply the domain to read ACME settings for a specified domain.

Examples: `xCommand ACME Settings Read`

`xCommand ACME Settings Read "example.com"`

xCommand ACME Settings Write

Writes ACME settings.

AcmeManaged(r): <Disabled/Manual/Automated>

Domain: <String>

ProviderUuid: <String>

RenewKey: <Retain/Rotate>

RenewalSchedule: <String>

If you do not specify a domain, the command writes the settings for the ACME service managing the server certificate. Otherwise it writes settings for the specified domain.

If the specified domain does not yet have ACME settings, the command writes the settings for that domain using the default provider's UUID.

If the specified domain already has ACME settings, the command updates the settings that you supply, and does not change any settings you did not specify.

You must supply the AcmeManaged parameter. If you set AcmeManaged to Automated, then you must also supply RenewalSchedule and RenewKey.

Examples: `xCommand ACME Settings Write AcmeManaged: "Manual"`

`xCommand ACME Settings Write AcmeManaged: "Automated" Domain: "example.com" RenewalSchedule: "{"DaysOfWeek":["Mon"],"TimeOfDay":"04:00"}" RenewKey: "Rotate"`

xCommand ACME Sign

Signs a CSR.

Domain: <String>

NumSanEntries: <-2147483648..2147483647>

Enter the command with no parameters to submit the CSR for the server certificate to its ACME provider. Supply a domain to submit the CSR for a domain certificate to its ACME provider.

Do not supply the `NumSanEntries` parameter. It has no user-modifiable purpose.

Example: `xCommand Acme Sign`

```
xCommand ACME Sign Domain: "example.com"
```

xCommand Admin Account Add

Adds a local administrator account.

Name(r): <S: 0, 128>

The username for this account.

Password(r): <Password>

The password for this account.

AccessAPI: <On/Off>

Whether this account is allowed to access the system's status and configuration via the API. Default: On.

AccessWeb: <On/Off>

Whether this account is allowed to log in to the system using the web interface. Default: On.

Enabled: <On/Off>

Indicates if the account is enabled or disabled. Access is denied to disabled accounts. Default: On.

Example: `xCommand Admin Account Add Name: "bob_smith" Password: "abcXYZ_123" AccessAPI: On AccessWeb: On Enabled: On`

xCommand Admin Account Delete

Deletes a local administrator account.

Name(r): <S: 0, 128>

The username of the account to delete.

Example: `xCommand Admin Account Delete: "bob_smith"`

xCommand Admin Group Add

Name(r): <S: 0, 128>

The name of the administrator group.

AccessAPI: <On/Off>

Whether members of this group are allowed to access the system's status and configuration using the API. Default: On.

AccessWeb: <On/Off>

Whether members of this group are allowed to log in to the system using the web interface. Default: On.

Enabled: <On/Off>

Indicates if the group is enabled or disabled. Access is denied to members of disabled groups. Default: On.

Example: `xCommand Admin Group Add Name: "administrators" AccessAPI: On AccessWeb: On Enabled: On`

xCommand Admin Group Delete

Deletes an administrator group.

Name(r): <S: 0, 128>

The name of the group to delete.

Example: `xCommand Admin Group Delete: "administrators"`

xCommand Allow List Add

Adds an entry to the Allow List.

PatternString(r): <S: 1, 60>

Specifies an entry to be added to the Allow List. If one of an endpoint's aliases matches one of the patterns in the Allow List, the registration will be permitted.

PatternType: <Exact/Prefix/Suffix/Regex>

Specifies whether the entry in the Allow List is a prefix, suffix, regular expression, or must be matched exactly.

Exact: the string must match the alias character for character.

Prefix: the string must appear at the beginning of the alias.

Suffix: the string must appear at the end of the alias.

Regex: the string will be treated as a regular expression.

Default: Exact.

Description: <S: 0,64>

A free-form description of the Allow List rule.

Example: `xCommand Allow List Add PatternString: "John.Smith@example.com" PatternType: Exact Description: "Allow John Smith"`

xCommand Allow List Delete

Deletes an entry from the Allow List.

AllowListId(r): <1..2500>

The index of the entry to be deleted.

Example: `xCommand Allow List Delete AllowListId: 2`

xCommand Boot

Reboots the Expressway.

This command has no parameters.

Example: `xCommand Boot`

xcommand Certs Command for Server CSR

Allows to generate Server Certificate Signing Request (CSR)

Default value of Publickeyalgorithm parameter is “RSA”

The following are the Supported Keysize(s) for

- ECDSA: 256, 384, 521
- RSA: 2048, 4096

Example: `xcommand Certs Command csr_create subjectfields: '{"CN": "www.cisco.com", "C": "US", "OU": "expressway" }' Keysize: 256 Publickeyalgorithm: ECDSA`

xcommand Certs Command for Domain CSR

Allows to generate Domain Certificate Signing Request (CSR)

Deafult value of Publickeyalgorithm parameter is “RSA”

The following are the Supported Keysize(s) for

- ECDSA: 256, 384, 521
- RSA: 2048, 4096

Example: `xcommand Certs Command: csr_create subjectfields: '{"CN": "www.cisco.com", "C": "US", "OU": "expressway" }' Keysize: 256 Publickeyalgorithm: ECDSA Domain: cisco.com`

xCommand Check Bandwidth

A diagnostic tool that returns the status and route (as a list of nodes and links) that a call of the specified type and bandwidth would take between two nodes. Note that this command does not change any existing system configuration.

Node1(r): <S: 1, 50>

The subzone or zone from which the call originates.

Node2(r): <S: 1, 50>

The subzone or zone at which the call terminates.

Bandwidth(r): <1..100000000>

The requested bandwidth of the call (in kbps).

CallType(r): <Traversal/NonTraversal>

Whether the call type is Traversal or Non-traversal.

Example: `xCommand Check Bandwidth Node1: "DefaultSubzone" Node2: "UK Sales Office" Bandwidth: 512 CallType: nontraversal`

xCommand Check Pattern

A diagnostic tool that allows you to check the result of an alias transform (local or zone) before you configure it on the system.

Target(r): <S: 1, 60>

The alias you want to use to test the pattern match or transform.

Pattern(r): <S: 1, 60>

The pattern against which the alias is compared.

Type(r): <Exact/Prefix/Suffix/Regex>

How the pattern string must match the alias for the pattern behavior to be applied.

Behavior(r): <Strip/Leave/Replace/AddPrefix/AddSuffix>

How the alias is modified.

Replace: <S: 0, 60>

The text string to use in conjunction with the selected Pattern behavior.

Example: `xCommand Check Pattern Target: "bob@a.net" Pattern: "@a.net" Type: "suffix" Behavior: replace Replace: "@a.com"`

xCommand Clear All Status

Clears all status and history on the system.

Example: `xCommand Clear All Status`

xCommand Cluster Address Mapping Add

Fqdn(r): <Value>

IpAddress(r): <Value>

Adds an FQDN/IP mapping entry to the cluster address mapping table.

xCommand Cluster Address Mapping Delete

Fqdn(r): <Value>

IpAddress(r): <Value>

Deletes an FQDN/IP mapping entry from the cluster address mapping table.

xCommand CMS Add

Manage Cisco Meeting Server web bridges. Add a Guest account client URI

Name: <Value>

Example: `xCommand CMS Add name: "join.example.com"`

xCommand CMS Delete

Manage Cisco Meeting Server web bridges. Delete a Guest account client URI

Name: <Value>

Example: `xCommand CMS Delete name: "join.example.com"`

xCommand Credential Add

Adds an entry to the local authentication database.

Name(r): <String>

Defines the name for this entry in the local authentication database.

Password(r): <Password>

Defines the password for this entry in the local authentication database.

The maximum plaintext length is 128 characters, which will then be encrypted.

Example: `xCommand Credential Add Name: "alice" Password: "abcXYZ_123"`

xCommand Credential Delete

Deletes an entry from the local authentication database.

Name(r): <String>

The name of the entry to delete.

Example: `xCommand Credential Delete Name: "alice"`

xCommand CUCM Config Add

Performs a lookup on a Unified CM publisher.

Address(r): <Value>

The FQDN or IP address of the Unified CM publisher.

Axlpassword(r): <Value>

The password used by the Expressway to access the Unified CM publisher.

Axlusername(r): <Value>

The user name used by the Expressway to access the Unified CM publisher.

CertValidationDisabled: <On/Off>

Controls X.509 certificate checking against the certificate presented by the Unified CM publisher. Default: On

Example: `xCommand CUCM Config Add Address: "cucm.example.com" Axlpassword: "xyz" Axlusername: "abc"`

xCommand CUCM Config Delete

Deletes the details of a Unified CM publisher.

Address(r): <Value>

The FQDN or IP address of the Unified CM publisher.

Example: `xCommand CUCM Config delete Address: "cucm.example.com"`

xCommand CUCM Mixed Mode Check

Address(r): <Value>

The FQDN or IP address of the Unified CM publisher.

Axlpassword(r): <Value>

The password used by the Expressway to access the Unified CM publisher.

Axlusername(r): <Value>

The user name used by the Expressway to access the Unified CM publisher.

xCommand Custom Notification Add

Adds a customized entry for alarm-based email notifications. Per alarm id, either to disable notifications for the alarm ID or to direct them to a specified email address.

alarm_id: <String> Enter the alarm Id for which you want to customize or disable notifications.

custom_email: <S: 0, 254> If the Notification is “Custom”, enter the email id to which the selected alarm notifications are to be sent.

disable_notify: <on/off> Choose the action you want for the selected alarm:

- On : No notification regarding the selected alarm will be sent.
- Off : Notification regarding the selected alarm will be sent to the email id entered in the Email field.

Default: On

To add a custom notification, specify disable_notify as “Off”.

After a custom notification is added, it will be listed in the xconfiguration command “Alarm Notification Email”.

xCommand Custom Notification Delete

Removes a customized entry for alarm-based email notifications.

alarm_id(r): <String> Enter the alarm Id for which you want to customize or disable notifications.

xCommand Default Links Add

Restores links between the Default Subzone, Traversal Subzone and the Default Zone.

This command has no parameters.

Example: `xCommand Default Links Add`

xCommand Default Values Set

Resets system parameters to default values. Level 1 resets most configuration items to their default value, with the exception of the Level 2 and Level 3 items. Level 2 resets configuration items related to remote authentication, plus Level 1 items to their default value. Level 3 resets all critical configuration items, plus Level 1 and Level 2 items to their default value.

Level(r): <1..3>

The level of system parameters to be reset.

Example: `xCommand Default Values Set Level: 1`

xCommand Deny List Add

Adds an entry to the Deny List.

PatternString(r): <S: 1, 60>

Specifies an entry to be added to the Deny List. If one of an endpoint's aliases matches one of the patterns in the Deny List, the registration will not be permitted.

PatternType: <Exact/Prefix/Suffix/Regex>

Specifies whether the entry in the Deny List is a prefix, suffix, regular expression, or must be matched exactly.

Exact: the string must match the alias character for character.

Prefix: the string must appear at the beginning of the alias.

Suffix: the string must appear at the end of the alias.

Regex: the string will be treated as a regular expression.

Default: Exact.

Description: <S: 0, 64>

A free-form description of the Deny List rule.

Example: `xCommand Deny List Add PatternString: "sally.jones@example.com" PatternType: exact Description: "Deny Sally Jones"`

xCommand Deny List Delete

Deletes an entry from the Deny List.

DenyListId(r): <1..2500>

The index of the entry to be deleted.

Example: `xCommand Deny List Delete DenyListId: 2`

xCommand Disconnect Call

Disconnects a call.

Call: <1..1000>

The index of the call to be disconnected.

CallSerialNumber: <S: 1, 255>

The serial number of the call to be disconnected. You must specify either a call index or a call serial number.

Example: `xCommand Disconnect Call CallSerialNumber: "6d843434-211c-11b2-b35d-0010f30f521c"`

xCommand DNS Lookup

Queries DNS for a supplied hostname.

Hostname: <Value>

The name of the host you want to query.

RecordType: <all/a/aaaa/srv/naptr>

The type of record you want to search for. If not specified, all record types are returned.

Example: `xCommand DNS Lookup Hostname: "example.com" RecordType: all`

xCommand DNS Per Domain Server Add

Adds a DNS server to use only for resolving hostnames for specific domains.

Address(r): <Value>

The IP address of the DNS server to use when resolving hostnames for the associated domain names.

Domain1(r): <Value>

The domain to associate with the specific DNS server.

Domain2(r): <Value>

An optional second domain to associate with the specific DNS server.

Index: <0..5>

The index of the server to add.

Example: `xCommand DNS Server Add Address: "192.168.12.0" Index: 1`

xCommand DNS Per Domain Server Delete

Deletes a DNS server used for resolving hostnames for a specific domain.

Address: <Value>

The IP address of the DNS server to delete.

Example: `xCommand DNS Per Domain Server Delete Address: "192.168.12.0"`

xCommand DNS Server Add

Adds a default DNS server. Default servers are used if there is no per-domain DNS server defined for the domain being looked up.

Address(r): <Value>

The IP address of a default DNS server to use when resolving domain names.

Index: <0..5>

The index of the server to add.

Example: `xCommand DNS Server Add Address: "192.168.12.0" Index: 1`

xCommand DNS Server Delete

Deletes a DNS server

Address: <Value>

The IP address of the DNS server to delete.

Example: `xCommand DNS Server Delete Address: "192.168.12.0"`

xCommand Domain Add

Adds a domain for which this Expressway is authoritative.

Name(r): <S: 1, 128>

The domain name. It can comprise multiple levels. Each level's name can only contain letters, digits and hyphens, with each level separated by a period (dot). A level name cannot start or end with a hyphen, and the final level name must start with a letter.

Edgesip: <On/Off>

Endpoint registration, call control and provisioning services are provided by Unified CM. Default: Off.

Edgexmpp: <On/Off>

Instant messaging and presence services for this SIP domain are provided by the Unified CM IM&P service. Default: Off.

Sip: <On/Off>

Controls whether the Expressway is authoritative for this domain. The Expressway acts as a SIP registrar and Presence Serverfor the domain, and will accept registration requests for any SIP endpoints attempting to register with an alias that includes this domain. Default: On.

Xmppfederation: <On/Off>

Controls whether the domain is available for XMPP federation. Default: Off.

Example: `xCommand Domain Add Name: "100.example-name.com" Authzone: "Traversal zone" Edge: Off Sip: On`

xCommand Domain Delete

Deletes a domain.

DomainId(r): <1..200>

The index of the domain to be deleted.

Example: `xCommand Domain Delete DomainId: 2`

xCommand Domain Certs

Manage multidomain certificates for Server Name Indication (SNI).

Each Domain Certs xCommand requires a 'command' parameter specifying an operation to be performed, followed by any additional parameters required for the specific command.

Domain Certs commands and associated parameters:

domain_list: Lists domains for which certificates are managed for SNI.

parameters: (none)

Example: `xCommand Domain Certs command: domain_list`

domain_create: Creates a new domain for managing certificates for SNI.

parameters: domain

Example: `xCommand Domain Certs command: domain_create domain: a.com`

domain_delete: Deletes the specified certificate domain.

parameters: domain

Example: `xCommand Domain Certs command: domain_delete domain: a.com`

is_csr_pending: Returns true if a certificate signing request is pending for the domain.

parameters: domain

Example: `xCommand Domain Certs command: is_csr_pending domain: a.com`

csr_create: Creates a certificate signing request for a domain.

parameters: domain, subjectfields, sans, digestalgorithm, keysize

Example: `xCommand Domain Certs command: csr_create domain: a.com keysize: 4096 digestalgorithm: sha256 sans: 'DNS:host1.a.com, DNS:host2.a.com' subjectfields: '{ "CN": "www.a.com", "C": "US", "ST": "North Carolina", "L": "RTP", "O": "a", "OU": "example org unit", "emailAddress": "admin@a.com" }'`

Note

- xCommand parameter values can be contained in single quotes so that space can be included.
- sans is an optional, comma-separated list of hostnames, each hostname prefixed by 'DNS:', see RFC5280.
- subjectfields is a JSON object containing a list of name: value pairs for each Subject Name field, see RFC5280.
- JSON names and values must be contained in double quotes as shown.
- keysize is the length in bits of the private key generated for the CSR.
- digestalgorithm is the name of the message digest algorithm used to sign the CSR, see 'openssl dgst'.

csr_get: Returns a pending certificate signing request in PEM format.

parameters: domain

Example: `xCommand Domain Certs command: csr_get domain: a.com`

csr_delete: Deletes a pending certificate signing request.

parameters: domain

Example: `xCommand Domain Certs command: csr_delete domain: a.com`

is_cert_set: Returns true if a certificate has been set for the domain.

parameters: domain

Example: `xCommand Domain Certs command: is_cert_set domain: a.com`

cert_put: Uploads a certificate and private key.

parameters: domain, certpath, keypath

Example: `xCommand Domain Certs command: cert_put domain: a.com certpath: /tmp/cert.pem keypath: /tmp/key.pem`

Note
- When a certificate and key have not been uploaded yet, both must be specified.
- When a certificate signing request is in progress, only a certificate can be uploaded.

cert_get: Returns a domain's certificate in PEM format.

parameters: domain

Example: `xCommand Domain Certs command: cert_get domain: a.com`

cert_delete: Deletes a domain's certificate and private key.

parameters: domain

Example: `xCommand Domain Certs command: cert_delete domain: a.com`

default command help:"

Certpath: <String>

Command:
<domain_list/domain_create/domain_delete/csr_create/csr_get/csr_delete/cert_put/cert_get/cert_delete/is_csr_pending/is_cert_set>

Digestalgorithm: </sha256/sha384/sha512>

Domain: <String>

Keypath: <String>

Keysize: <Value>

Sans: <String>

Subjectfields: <String>

xCommand Edge SSO Delete Tokens

Deletes all tokens issued to a particular user.

Username(r): <String>

Specifes which user's tokens will be deleted.

Example: `xCommand Edge SSO Delete Tokens Username: "APerson"`

xCommand Edge SSO Purge Tokens

Deletes all tokens issued to all users.

Example: `xCommand Edge SSO Purge Tokens`

xCommand Edge SSO Status Clear

Resets the SSO request/response counters to 0.

Example: `xCommand Edge SSO Status Clear`

xCommand Feedback Deregister

Deactivates a particular feedback request.

ID: <1..3>

The index of the feedback request to be deactivated.

Example: `xCommand Feedback Deregister ID: 1`

xCommand Feedback Register

Activates notifications on the event or status changes described by the expressions. Notifications are sent in XML format to the specified URL. Up to 15 expressions may be registered for each of 3 feedback IDs.

ID: <1..3>

The ID of this particular feedback request.

URL(r): <S: 1, 256>

The URL to which notifications are to be sent.

Expression.1..15: <S: 1, 256>

The events or status change to be notified. Valid Expressions are:

```
Status/Ethernet   Event/RegistrationFailure  Event/AuthenticationFailure
Event/    Status/Calls    Event/CallDisconnected
Event/CallFailure   Status/NTP    Status/LDAP
Status/Zones   Event/Bandwidth    Event/Locate
Status/Feedback   Event/CallAttempt   Event/CallConnected
Event/ResourceUsage   Status/ExternalManager
```

Example: `xCommand Feedback Register ID: 1 URL: "http://192.168.0.1/feedback/" Expression.1: "Status/Calls" Expression.2: "Event/CallAttempt"`

xCommand Find Registration

Returns information about the registration associated with the specified alias. The alias must be registered on the Expressway on which the command is issued.

Alias(r): <S: 1, 60>

The alias that you want to find out about.

Example: `xCommand Find Registration Alias: "john.smith@example.com"`

Important FIPS140-2 mode is **only available** on Cisoc Video Communication Server (VCS) with the *Advanced Security option key* and *Expressway Select*, **not** *Expressway* (Export Control Restricted version).

xCommand Fips

Sets FIPS140-2 cryptographic mode.

Command: <leave/enter/status>

Either enters, leaves or provides the current status of the system's FIPS140-2 cryptographic mode.

Example: `xCommand Fips Command: enter`

xCommand Force Config Update

Forces the relevant configuration on this peer to be updated to match that of the cluster primary.

This command has no parameters.

Example: `xCommand Force Config Update`

Important HSM functionality may be a Preview feature only, depending on the Expressway software version. For example, it is a Preview feature in version X12.6.

Please check the release notes for your Expressway version before you use HSM and if its status is Preview for your software version, **only enable HSM and use these HSM-related commands if you are willing to implement it as a Preview feature, and subject to the Preview disclaimer contained in the Expressway Release Notes**.

xCommand HSM Mode Read

Returns the current HSM mode set on the Expressway.

Example: `xCommand HSM Mode Read`

xCommand HSM Mode Write

Changes the HSM mode on Expressway. Can only be used if HSM settings and at least one HSM module is already configured on the Expressway.

Mode: <enabled, disabled>

Example: `xCommand HSM Mode Write Mode: enabled`

xCommand HSM Module Add

Adds a new HSM module to the Expressway configuration. HSM provider settings must be configured before using this command.

Ip(r): <S: 0, 1024>

The IP address of the HSM device to be added.

Port: <1..65535>

The port being used to communicate with an nShield HSM. Optional. Default is 9004.

Esn: <S: 0, 1024>

The serial number of an nShield HSM. Required.

Kneti: <S: 0, 1024>

The security hash used to verify an nShield HSM. Required.

Example: `xCommand HSM Module Add Ip: 1.1.1.1 Port: 9004 Esn: abcd-abcd-abcd Kneti: abcd1234abcd1234a`

xCommand HSM Module Remove

Removes an HSM module from the list of modules used by the Expressway.

Ip(r): <S: 0, 1024>

This command requires an IP address of an already configured HSM module.

Example: `xCommand HSM Module Remove Ip: 1.1.1.1`

xCommand HSM Modules

Returns a list of the HSM modules to be used by the Expressway.

Example: `xCommand HSM Modules`

xCommand HSM Settings Read

Returns the currently configured HSM settings.

Example: `xCommand HSM settings Read`

xCommand HSM Settings Write

Configures the HSM provider to be used (see the *Expressway Release Notes* for details of which providers are supported; support may be on a Preview basis only).

Provider(r): <nShield>

The HSM provider to be configured.

Rfsip: <S: 0, 1024>

The IP address of the Thales RFS (Remote File System). Required when nShield HSMs are used.

Rfsport: <1..65535>

The port being used to communicate with the RFS. Required when nShield HSMs are used. Default 9004

Example: `xCommand HSM Settings Write Provider: "nShield" Rfsip: "1.1.1.1" Rfsport: "9004"`

xCommand HTTP Allow List Export

Export the HTTP allow list rules in CSV format from the database.

File: <S>

Specifies the path to a file where the rules will get exported in CSV format. The file path should start with '/tmp/'.

Deployment: <S>

Use with URL to specify which of your deployments uses this rule. Not required unless you have multiple deployments. If you have multiple deployments, the rule will use the default deployment if you don't specify the deployment.

xCommand HTTP Allow List Export Test

Export the HTTP allow list tests in CSV format from the database.

File: <S>

Specifies the path to a file where the tests will get exported in CSV format. The file path should start with '/tmp/'.

Deployment: <S>

Use with URL to specify which of your deployments uses this test. Not required unless you have multiple deployments. If you have multiple deployments, the rule will use the default deployment if you don't specify the deployment.

xCommand HTTP Allow List Rule Add

Adds one or more rules to the HTTP allow list. You must specify at least URL or URLFile.

URL(r): <S>

Specifies the URL of a resource that HTTP clients will be allowed to access. IPv6 addresses must use RFC 2732 format.

For example: `https://[2001:DB8::1]:8443/path` or `https://www.example.com:8443/resource`

Do not supply URL if you are supplying URLFile.

URL must contain the protocol, either `http://` or `https://`, and the hostname. It should also contain domain, port, and path to make the URL more specific. If you omit some portions of the URL, Expressway will supply its defaults. eg. `http://hostname` allows clients to access to everything included by `http://hostname.SystemDNSDomain:80`. The default ports are 80 for http and 443 for https.

URLFile(r): <S>

Specifies the path to a CSV file that contains multiple rules. See Allow List Rules File Reference.

Do not supply URLFile if you are supplying URL.

MatchType: <exact/starts-with/startswith/prefix>

Use with URL to specify whether the rule matches exactly what is in URL, or uses it as a base for a prefix match. Defaults to `exact` if not supplied. The other options are all equivalent.

Deployment: <S: "Your Deployment 1"/"Your Deployment 2">

Use with URL to specify which of your deployments uses this rule. Not required unless you have multiple deployments. If you have multiple deployments, the rule will use the default deployment if you don't specify the deployment.

Description: <S:128>

A text description of the rule.

HttpMethods: <OPTIONS/GET/HEAD/POST/PUT/DELETE>

A comma-delimited set of methods to allow with this rule. If you do not specify the methods, the rule will use the default methods configured on **Configuration** > **Unified Communications** > **HTTP allow list** > **Editable inbound rules**.

Example 1: `xCommand HTTP Allow List Rule Add URLfile: "/tmp/rules.csv"`

Example 2: `xCommand HTTP Allow List Rule Add URL: "https://cucm2.example.com:8443/partial/path" MatchType: starts-with Description: "https access to read everything below partial/path/ on cucm2.example.com" HttpMethods: "OPTIONS,GET"`

xCommand HTTP Allow List Rule Delete

Deletes one or more rules from the HTTP allow list. You must specify at least URL or URLFile. You may need to specify other parameters if you have multiple rules for a single host.

URL(r): <S>

Specifies the URL of the rule you are deleting.

Do not supply URL if you are supplying URLFile.

URL must contain the protocol, either `http://` or `https://`, and the hostname. It should also contain domain, port, and path to make the URL more specific. If you omit some portions of the URL, Expressway will supply its defaults. eg. `http://hostname` will delete the rule `http://hostname.SystemDNSDomain:80`. The default ports are 80 for http and 443 for https.

URLFile(r): <S>

Specifies the path to a CSV file that contains multiple rules that you want to delete.

Do not supply URLFile if you are supplying URL.

MatchType: <exact/starts-with/startswith/prefix>

Use with URL to specify whether the rule matches exactly what is in URL, or uses it as a base for a prefix match. Defaults to `exact` if not supplied. The other options are all equivalent.

Deployment: <S>

Use with URL to specify which of your deployments uses this rule. Not required unless you have multiple deployments. If you have multiple deployments, the rule will use the default deployment if you don't specify the deployment.

Description: <S:128>

A text description of the rule.

HttpMethods: <OPTIONS/GET/HEAD/POST/PUT/DELETE>

A comma-delimited set of methods to allow with this rule. If you do not specify the methods, the rule will use the default methods configured on **Configuration** > **Unified Communications** > **HTTP allow list** > **Editable inbound rules**.

Example 1: `xCommand HTTP Allow List Rule Delete URLfile: "/tmp/rules.csv"`

Example 2: `xCommand HTTP Allow List Rule Delete URL: "https://cucm2.example.com:8443/partial/path" MatchType: starts-with Description: "https access to read everything below partial/path/ on cucm2.example.com" HttpMethods: "OPTIONS,GET"`

xCommand HTTP Allow List Rules Test

(Experimental)

Tests a collection of URLs (defined in a CSV file) against a list of rules (defined in a CSV file). This enables you to test rules before you apply them, or to test that existing rules are working as expected.

You can provide either the tests, or the rules, or both, as CSV files. If you provide both, the tests in the Tests CSV file are run against the rules in the Rules CSV file. If you omit one or both parameters, this command uses the rules or tests (or both) that are already on the Expressway. (Use `xstatus collaborationedge httpallowlist` to see the current rules).

Tests: <S>

Specifies the path to a CSV file that contains multiple tests, eg. `/tmp/tests.csv`. See Allow List Tests File Reference.

Rules: <S>

Specifies the path to a CSV file that contains multiple rules you want to test, eg. `/tmp/rules.csv`. See Allow List Rules File Reference.

Example: `xCommand HTTP Allow List Rules Test Tests: "/tmp/tests.csv" Rules: "/tmp/rules.csv"`

xCommand HTTP Allow List Test Add

(Experimental)

Adds one or more URLs to test against the HTTP allow list. You must specify at least URL or URLFile; if you specify URL, you must specify ExpectedResult.

URL(r): <S>

Specifies the test URL. IPv6 addresses must use RFC 2732 format.

For example: `https://[2001:DB8::1]:8443/path` or `https://www.example.com:8443/resource`

Do not supply URL if you are supplying URLFile.

URL must contain the protocol, either `http://` or `https://`, and the hostname. It should also contain domain, port, and path to make the URL more specific. If you omit some portions of the URL, Expressway will supply its defaults. eg. `http://hostname` tests the URL `http://hostname.SystemDNSDomain:80`. The default ports are 80 for http and 443 for https.

URLFile(r): <S>

Specifies the path to a CSV file that contains multiple tests. See Allow List Tests File Reference.

Do not supply URLFile if you are supplying URL.

ExpectedResult(r): <allow/block>

Required with URL to specify whether the URL should be allowed or blocked by the allow list.

Deployment: <S>

Use with URL to specify which of your deployments uses this test. Not required unless you have multiple deployments. If you have multiple deployments, the test will use the default deployment unless you specify the deployment.

Description: <S:128>

A text description of the test.

HttpMethod: <OPTIONS/GET/HEAD/POST/PUT/DELETE>

Specify one method to test. If you do not specify the method, the test will use GET.

Example 1: `xCommand HTTP Allow List Test Add URLfile: "/tmp/tests.csv"`

Example 2: `xCommand MRA Allow List Test Add URL: "https://cucm2.example.com:8443/partial/path" ExpectedResult: block Description: "https access to write to partial/path/ on cucm2.example.com" HttpMethod: "POST"`

xCommand HTTP Allow List Test Delete

(Experimental)

Deletes one or more test URLs from the HTTP allow list. You must specify at least URL or URLFile; if you specify URL, you must specify ExpectedResult.

URL(r): <S>

Specifies the test URL you are deleting.

Do not supply URL if you are supplying URLFile.

URLFile(r): <S>

Specifies the path to a CSV file that contains multiple tests you want to delete.

Do not supply URLFile if you are supplying URL.

ExpectedResult(r): <allow/block>

Specify the result expected by the test you are deleting. Required for deleting the test.

Deployment: <S>

Specify which deployment use the test you are deleting. Not required unless you have multiple deployments.

Description: <S:128>

A text description of the test. Not required for deleting the test unless you have multiple tests that cannot otherwise be distinguished from each other.

HttpMethod: <OPTIONS/GET/HEAD/POST/PUT/DELETE>

Specify which method is used in the test you are deleting. If you omit the methods, the Expressway uses the current default methods with this command. This means the delete could fail unless the test was created with the corresponding methods.

Example 1: `xCommand HTTP Allow List Test Delete URLfile: "/tmp/tests.csv"`

Example 2: `xCommand HTTP Allow List Test Delete URL: "https://cucm2.example.com:8443/partial/path" ExpectedResult: allow HttpMethod: "get"`

xCommand HTTP Proxy Jabber CTargets Add

Configures a Jabber Guest Server and associates it with a Jabber Guest domain.

DomainIndex(r): <0..200>

Index of the domain with which this Jabber Guest Server is associated

Host(r): <S:1,1024>

The FQDN of a Jabber Guest Server to use for the selected domain. This must be an FQDN, not an unqualified hostname or an IP address.

Note that you can specify alternative addresses for the same domain, each with different priorities.

Priority: <0..9>

The order in which connections to this hostname are attempted for this domain. All priority 1 hostnames for the domain are attempted first, followed by all priority 2 hostnames, and so on.

Example: `xCommand HTTP Proxy Jabber CTargets Add DomainIndex: 2 Host: jabberguest.example.com`

xCommand HTTP Proxy Jabber CTargets Delete

Deletes the configured Jabber Guest Server from the Expressway.

Host(r): <S:1,1024> The FQDN of the Jabber Guest Server to delete.

xCommand IMP Server Add

Adds an external messaging server to which to route Microsoft SIP Simple messages.

IMP(r): <Value> configuration/b2bua/imp/imp

xCommand IMP Server Delete

Deletes an external messaging server.

IMP(r): <Value> configuration/b2bua/imp/imp

xCommand License Smart Deregister

The product reverts to evaluation mode providing the evaluation period has not expired. License entitlements used for the product are released immediately to the virtual account and are available for other product instances to use it.

xCommand License Smart Register Idtoken: <String>

Use the Product Instance Registration token that you generated from Smart Software Manager or your Smart Software Manager satellite to register the product.

xCommand License Smart Renew Auth

Perform this operation if automatic authorization status renewal failed due to network connectivity issues with Cisco Smart Software Manager.

xCommand License Smart Renew ID

Perform this operation if automatic registration renewal failed due to network connectivity issues with Cisco Smart Software Manager.

xCommand License Smart Reregister: <String>

Perform this operation to reregister the product instance in the following cases:

- Previous registration attempt of this product instance failed due to network connectivity issue and you want to reregister after resolving this issue.
- To reregister the product instance, already registered with a virtual account, to a different virtual account.

xCommand Link Add

Adds and configures a new link.

LinkName(r): <S: 1, 50>

Assigns a name to this link.

Node1: <S: 1, 50>

Specifies the first zone or subzone to which this link will be applied.

Node2: <S: 1, 50>

Specifies the second zone or subzone to which this link will be applied.

Pipe1: <S: 1, 50>

Specifies the first pipe to be associated with this link.

Pipe2: <S: 1, 50>

Specifies the second pipe to be associated with this link.

Example: `xCommand Link Add LinkName: "Subzone1 to UK" Node1: "Subzone1" Node2: "UK Sales Office" Pipe1: "512Kb ASDL"`

xCommand Link Delete

Deletes a link.

LinkId(r): <1..3000>

The index of the link to be deleted.

Example: `xCommand Link Delete LinkId: 2`

xCommand Locate

Runs the Expressway's location algorithm to locate the endpoint identified by the given alias, searching locally, on neighbors, and on systems discovered through the DNS system, within the specified number of 'hops'. Results are reported back through the xFeedback mechanism, which must therefore be activated before issuing this command (e.g. xFeedback register event/locate).

Alias(r): <S: 1, 60>

The alias associated with the endpoint you wish to locate.

HopCount(r): <0..255>

The hop count to be used in the search.

Protocol(r): <H323/SIP>

The protocol used to initiate the search.

SourceZone: <S: 1, 50>

The zone from which to simulate the search request. Choose from the Default Zone (an unknown remote system), the Local Zone (a locally registered endpoint) or any other configured neighbor, traversal client or traversal server zone.

Authenticated: <Yes/No>

Whether the search request should be treated as authenticated or not.

SourceAlias: <S: 0, 60>

The source alias to be used for the search request. Default: xcom-locate

Example: `xCommand Locate Alias: "john.smith@example.com" HopCount: 15 Protocol: SIP SourceZone: LocalZone Authenticated: Yes SourceAlias: alice@example.com`

xCommand Network Interface

Controls whether the LAN 2 port is enabled for management and call signaling.

DualInterfaces(r): <enable/disable/status>

Sets or reports on the current status of the LAN 2 port.

Example: `xCommand Networkinterface DualInterfaces: enable`

DedicatedManagementInterface: <enable/disable/status>

If enabled, the Dedicated Management Interface (DMI) uses the LAN3 port for management traffic. (If you try to disable the DMI and a management service is using it as its only interface, the command will fail.)

Example: `xCommand Network Interface DedicatedManagementInterface: enable`

xCommand Network Limits

Controls the experimental rate limiting feature.

Enter `xCommand Network Limits ?` to read the help.

xCommand NTP Server Add

Adds an NTP server to be used when synchronizing system time.

Address(r): <Value>

The IP address or Fully Qualified Domain Name (FQDN) of the NTP server to add.

Example: `xCommand NTP Server Add Address: ntp.server.example.com`

xCommand NTP Server Delete

Address(r): <Value>

The IP address or Fully Qualified Domain Name (FQDN) of the NTP server to delete.

Example: `xCommand NTP Server Delete Address: "ntp.server.example.com"`

xCommand Option Key Add

Adds a new option key to the Expressway. These are added to the Expressway in order to add extra functionality, such as increasing the Expressway's capacity. Contact your Cisco representative for further information.

Key(r): <S: 0, 90>

Specifies the option key of your software option.

Example: `xCommand Option Key Add Key: "1X4757T5-1-60BAD5CD"`

xCommand Option Key Delete

Deletes a software option key from the Expressway.

OptionKeyId(r): <1..64>

Specifies the ID of the software option to be deleted.

Example: `xCommand Option Key Delete OptionKeyId: 2`

xCommand Ping

Checks that a particular host system is contactable.

Hostname: <Value>

The IP address or hostname of the host system you want to try to contact.

Example: `xCommand Ping Hostname: "example.com"`

xCommand Pipe Add

Adds and configures a new pipe.

PipeName(r): <S: 1, 50>

Assigns a name to this pipe.

TotalMode: <Unlimited/Limited/NoBandwidth>

Controls total bandwidth restrictions for the pipe.

NoBandwidth: no calls can be made using this pipe. Default: Unlimited.

Total: <1..100000000>

If this pipe has limited bandwidth, sets the maximum bandwidth (in kbps) available at any one time on the pipe. Default: 500000.

PerCallMode: <Unlimited/Limited/NoBandwidth>

Controls bandwidth restrictions of individual calls.

NoBandwidth: no calls can be made using this pipe. Default: Unlimited.

PerCall: <1..100000000> For limited per-call mode, sets the maximum bandwidth (in kbps) available per call. Default: 1920.

Example: `xCommand Pipe Add PipeName: "512k ADSL" TotalMode: Limited Total: 512 PerCallMode: Limited PerCall: 128`

xCommand Pipe Delete

Deletes a pipe.

PipeId(r): <1..1000>

The index of the pipe to be deleted.

Example: `xCommand Pipe Delete PipeId: 2`

xCommand Policy Service Add

Adds a policy service.

Name(r): <S: 0, 50>

Assigns a name to this Policy Service.

Description: <S: 0, 64>

A free-form description of the Policy Service.

Protocol: <HTTP/HTTPS>

Specifies the protocol used to connect to the remote service. Default: HTTPS

Verify: <On/Off>

Controls X.509 certificate checking and mutual authentication between this Expressway and the policy service. When enabled, the server's FQDN or IP address, as specified in the address field, must be contained within the server's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes). Default: On

CRLCheck: <On/Off>

Controls certificate revocation list checking of the certificate supplied by the policy service. When enabled, the server's X.509 certificate will be checked against the revocation list of the certificate authority of the certificate. Default: Off

Address: <S: 0, 128>

Specifies the IP address or Fully Qualified Domain Name (FQDN) of the remote service.

Path: <S: 0, 255>

Specifies the URL of the remote service.

StatusPath: <S: 0..255>

Specifies the path for obtaining the remote service status. Default: status

UserName: <S: 0, 30>

Specifies the user name used by the Expressway to log in and query the remote service.

Password: <S: 0, 82>

The password used by the Expressway to log in and query the remote service. The maximum plaintext length is 30 characters.

DefaultCPL: <S: 0, 255>

The CPL used when the remote service is unavailable. Default: <reject status='403' reason='Service Unavailable'/>

Example: `xCommand Policy Service Add Name: “Conference” Description: “Conference service” Protocol: HTTPS Verify: On CRLCheck: On Address: “service.example.com” Path: “service” StatusPath: “status” UserName: “user123” Password: “password123” DefaultCPL: “<reject status='403' reason='Service Unavailable'/>”`

xCommand Policy Service Delete

Deletes a policy service.

PolicyServiceId(r): <1..20>

The index of the policy service to be deleted.

Example: `xCommand Policy Service Delete PolicyServiceId: 1`

xCommand Remote Syslog Add

Adds the address of a remote syslog server.

Address(r): <Value>

The IP address or FQDN of the remote syslog server.

Crlcheck: <On/Off>

Controls whether the certificate supplied by the syslog server is checked against the certificate revocation list (CRL). Default : Off

Format: <bsd/ietf>

The format in which remote syslog messages are written. Default : bsd

Loglevel: <emergency/alert/critical/error/warning/notice/informational/debug>

The minimum severity of log messages to send to this syslog server. Default: informational.

Mode: <bsd/ietf/ietf_secure/user_defined>

The syslog protocol to use when sending messages to the syslog server. Default: bsd.

Port: <1..65535>

The UDP/TCP destination port to use. Suggested ports: UDP=514 TCP/TLS=6514 Default : 514

Transport: <udp/tcp/tls>

The transport protocol to use when communicating with the syslog server. Default: udp

Example: `xCommand Remote Syslog Add Address: "remote_server.example.com" Crlcheck: Off Format: bsd Loglevel: warning Mode: bsd Port: 514 Transport: udp`

xCommand Remote Syslog Delete

Address(r): <Value>

The IP address or Fully Qualified Domain Name (FQDN) of the remote syslog server to delete.

Port(r): <1..65535>

The port used by the remote syslog server to be deleted.

Transport(r): <udp/tcp/tls>

The transport protocol used by the remote syslog server to be deleted.

Example: `xCommand Remote Syslog Delete Address: "remote_server.example.com" Port: 514 Transport: udp`

xCommand Remove Registration

Removes a registration from the Expressway.

Registration: <1..3750>

The index of the registration to be removed.

RegistrationSerialNumber: <S: 1, 255>

The serial number of the registration to be removed.

Example: `xCommand Remove Registration RegistrationSerialNumber: "a761c4bc-25c9-11b2-a37f-0010f30f521c"`

xCommand Restart

Restarts the Expressway without a full system reboot.

This command has no parameters.

Example: `xCommand Restart`

xCommand Route Add

Adds and configures a new IP route (also known as a static route).

Address(r): <S: 1, 39>

Specifies an IP address used in conjunction with the prefix length to determine the network to which this route applies. Default: 32

PrefixLength(r): <1..128>

Specifies the number of bits of the IP address which must match when determining the network to which this route applies.

Gateway(r): <S: 1, 39>

Specifies the IP address of the gateway for this route.

Interface: <Auto/LAN1/LAN2>

The LAN interface to use for this route. *Auto*: the Expressway selects the most appropriate interface to use. Default: Auto

Example: `xCommand Route Add Address: "10.13.8.0" PrefixLength: 32 Gateway: "192.44.0.1"`

xCommand Route Delete

Deletes a route.

RouteId(r): <1..50>

The index of the route to be deleted.

Example: `xCommand Route Delete RouteId: 1`

Important This command is applicable **only** to Cisco TelePresence Video Communication Server (VCS) Series.

xCommand Secure Mode

Controls Advanced Account Security options.

Command(r): <on/off/status>

The index of the route to be deleted.

Example: `xCommand Secure Mode Command: off`

xCommand Search Rule Add

Adds a new search rule to route searches and calls toward a zone or policy service.

Name(r): <S: 0, 50>

Descriptive name for the search rule.

ZoneName: <S: 0, 50>

The zone or policy service to query if the alias matches the search rule.

Description: <S: 0, 64>

A free-form description of the search rule.

Example: `xCommand Search Rule Add Name: "DNS lookup" ZoneName: "Sales Office Description": "Send query to the DNS zone"`

xCommand Search Rule Delete

Deletes a search rule.

SearchRuleId(r): <1..2000>

The index of the search rule to be deleted.

Example: `xCommand Search Rule Delete SearchRuleId: 1`

xCommand Trace Path

Discover the path taken by a network packet sent to a particular destination host system.

Hostname: <Value>

The IP address or hostname of the host system to which you want to trace the path.

Example: `xCommand Trace Path Hostname: "example.com"`

xCommand Trace Route

Discover the route taken by a network packet sent to a particular destination host system. It reports the details of each router along the path, and the time taken for each router to respond to the request.

Hostname: <Value>

The IP address or hostname of the host system to which you want to trace the route.

Example: `xCommand Trace Route Hostname: "example.com"`

xCommand Transform Add

Adds and configures a new transform.

Pattern(r): <S: 1, 60>

Specifies the pattern against which the alias is compared.

Type: <Exact/Prefix/Suffix/Regex>

How the pattern string must match the alias for the transform to be applied.

Exact: the entire string must exactly match the alias character for character.

Prefix: the string must appear at the beginning of the alias.

Suffix: the string must appear at the end of the alias.

Regex: the string is treated as a regular expression. Default: Prefix

Behavior: <Strip/Replace/AddPrefix/AddSuffix>

How the alias is modified.

Strip: removes the matching prefix or suffix from the alias.

Replace: substitutes the matching part of the alias with the text in the replace string.

AddPrefix: prepends the replace string to the alias.

AddSuffix: appends the replace string to the alias. Default: Strip

Replace: <S: 0, 60>

The text string to use in conjunction with the selected Pattern behavior.

Priority: <1..65534>

Assigns a priority to the specified transform. Transforms are compared with incoming aliases in order of priority, and the priority must be unique for each transform. Default: 1

Description: <S: 0, 64>

A free-form description of the transform.

State: <Enabled/Disabled>

Indicates if the transform is enabled or disabled. Disabled transforms are ignored. Default: Enabled

Example: `xCommand Transform Add Pattern: "example.net" Type: suffix Behavior: replace Replace: "example.com" Priority: 3 Description: "Change example.net to example.com" State: Enabled`

xCommand Transform Delete

Deletes a transform.

TransformId(r): <1..100>

The index of the transform to be deleted.

Example: `xCommand Transform Delete TransformId: 2`

xCommand Ucxn Config Add

Configures a link to a Cisco Unity Connection server, for use with Mobile and Remote Access.

Address(r): <S:0,1024>

The FQDN or IP address of a Unity Connection publisher.

CertValidationDisabled: <On/Off>

If CertValidationDisabled is Off, the Cisco Unity Connection system's FQDN or IP address must be contained within the X.509 certificate presented by that system (in either the Subject Common Name or the Subject Alternative Name attributes of the certificate). The certificate itself must also be valid and signed by a trusted certificate authority.

DeploymentId: <1..65535>

This Unity Connection publisher is associated with the selected deployment and can only communicate with other members of the selected deployment. It cannot communicate with members of other deployments.

Password(r): <S:1,1024>

The password used by the Expressway-C to access the Cisco Unity Connection publisher.

Username(r): <S:1,1024>

The username used by the Expressway to access the Unity Connection publisher. For example, System Administrator role in UC publisher.

xCommand Ucxn Config Delete

Removes a link to a Cisco Unity Connection server from the VCS.

Address(r): <S:0,1024>

The FQDN or IP address of a Unity Connection publisher.

xCommand XMPP Delete

Deletes the details of IM and Presence servers.

Address(r): <Value>

The IP address or Fully Qualified Domain Name (FQDN) of the IM and Presence server to delete.

Example: `xCommand XMPP Delete Address: "imp_server.example.com"`

xCommand XMPP Discovery

Discovers the details of IM and Presence servers.

Address(r): <Value>

The IP address or Fully Qualified Domain Name (FQDN) of the IM and Presence server to discover.

Axlpassword(r): <Password>

The password used to access the IM and Presence publisher.

Axlusername(r): <String>

The username used to access the IM and Presence publisher.

CertValidationDisabled: <On/Off>

Controls X.509 certificate checking against the certificate presented by the IM and Presence publisher. Default: On

Example: `xCommand XMPP Discovery Address: "imp.example.com" Axlpassword: "xyz" Axlusername: "abc"`

xCommand Zone Add

Adds and configures a new zone.

ZoneName(r): <S: 1, 50>

Assigns a name to this zone.

Type(r): <Neighbor/TraversalClient/TraversalServer/ENUM/DNS>

Determines the nature of the specified zone, in relation to the local Expressway.

Neighbor: the new zone will be a neighbor of the local Expressway.

TraversalClient: a firewall exists between the zones, and the local Expressway is a traversal client of the new zone.

TraversalServer: a firewall exists between the zones and the local Expressway is a traversal server for the new zone.

ENUM: the new zone contains endpoints discoverable by ENUM lookup.

DNS: the new zone contains endpoints discoverable by DNS lookup.

Example: `xCommand Zone Add ZoneName: "UK Sales Office" Type: Neighbor`

xCommand Zone Delete

Deletes a zone.

ZoneId(r): <1..1000>

The index of the zone to be deleted.

Example: `xCommand Zone Delete ZoneId: 2`

xCommand Zone List

A diagnostic tool that returns the list of zones (grouped by priority) that would be queried, and any transforms that would be applied, in a search for a given alias.

Note that this command does not change any existing system configuration.

Alias(r): <S: 1, 60>

The alias to be searched for.

Example: `xCommand Zone List Alias: "john.smith@example.com"`

Command Reference — xStatus

The **xStatus** group of commands are used to return information about the current status of the system. Each **xStatus** element returns information about one or more sub-elements.

The following section lists all the currently available **xStatus** commands, and the information that is returned by each command.

To obtain information about the existing status, type:

- **xStatus** to return the current status of all status elements
- **xStatus <element>** to return the current status for that particular element and all its sub-elements
- **xStatus <element> <sub-element>** to return the current status of that group of sub-elements

To obtain information about the **xStatus** commands, type:

- **xStatus ?** to return a list of all elements available under the **xStatus** command

xStatus elements

The current xStatus elements are:

- Alarm
- Alternates
- Applications
- Authentication
- Authzkeys
- B2BUACalls
- B2buapresencerelayservice
- B2buapresencerelayuser
- CDR
- Cafe

- Calls
- Cloud
- Cluster
- CollaborationEdge
- Edgeauth
- Edgecmsserver
- EdgeConfigProvisioning
- Edgeconfigprovisioning
- Edgedomain
- Edgeexternalfqdn
- Edgeauthcodecache
- Edgesso
- ExternalManager
- Fail2ban
- Feedback
- Fips
- Firewall
- Gwtunnels
- H323
- HTTPProxy
- Hardware
- IntrusionProtection
- Iptablesacceptedrule
- Iptablesrule
- License
- Links
- Mediastatistics
- MicrosoftContent
- MicrosoftIMP
- NetworkInterface
- NetworkLimits (experimental)
- Ntpcertificates

- Options
- PhonebookServer
- Pipes
- Policy
- PortUsage
- Registrations
- ResourceUsage
- Resourceusage
- SIP
- SipServiceDomains
- SipServiceZones
- SystemMetrics
- SystemUnit
- TURN
- Teststatus
- Time
- Traversalserverresourceusage
- Tunnels
- Warnings
- XMPP
- Xcps2s
- Zones

External Policy Overview

The Cisco Expressway (Expressway) has built in support for Registration Policy and Call Policy configuration. It also supports CPL (Call Processing Language) for implementing more complex policy decisions. CPL is designed as a machine-generated language and is not immediately intuitive; while the Expressway can be loaded with CPL to implement advanced call policy decisions, complex CPL is difficult to write and maintain.

The Expressway's external policy feature allows policy decisions to be taken by an external system which can then instruct the Expressway on the course of action to take (such as whether to accept a registration, fork a call and so on). Call policy can now be managed independently of the Expressway, and can implement features that are unavailable on the Expressway. The external policy server can make routing decisions based on data available from any source that the policy server has access to, allowing companies to make routing decisions based on their specific requirements.

When the Expressway is configured to use an external policy server the Expressway sends the external policy server a service request (over HTTP or HTTPS), the service will send a response back containing a CPL snippet which the Expressway will then execute.

Using an External Policy Server

The main areas where the Expressway can be configured to use an external policy server are:

- Registration Policy – to allow or reject registrations.
- Call Policy (also known as Admin Policy) – to control the allowing, rejecting, routing (with fallback if calls fail) and forking of calls.
- Search rules (policy can be applied for specific dial plan search rules).

Each of these areas can be configured independently of each other as to whether or not to use a policy service. If a policy service is used, the decisions made by the policy service replace (rather than supplement) those made by the Expressway.

When configuring policy services:

- Up to 3 external policy servers may be specified to provide resiliency (and not load balancing).
- Default CPL can be configured, to be processed by the Expressway as a fallback, if the service is not available.
- The status and reachability of the service can be queried via a status path.

More information about policy services, including example CPL, can be found in the *External Policy on Expressway Deployment Guide*.

External Policy Request Parameters

When the Expressway uses a policy service it sends information about the call or registration request to the service in a POST message using a set of name-value pair parameters. The service can then make decisions based upon these parameters combined with its own policy decision logic and supporting data (for example lists of aliases that are allowed to register or make and receive calls, via external data lookups such as an LDAP database or other information sources).

The service response must be a 200 OK message with CPL contained in the body.

The following table lists the possible parameters contained within a request and indicates with a √ in which request types that parameter is included. It also indicates, where relevant, the range of accepted values.

Parameter name	Values	Registration policy	Search rules	Call policy
ALIAS		√		
ALLOW_INTERWORKING	TRUE / FALSE		√	√
AUTHENTICATED	TRUE / FALSE		√	√
AUTHENTICATED_SOURCE_ALIAS			√	√

Parameter name	Values	Registration policy	Search rules	Call policy
AUTHENTICATION_USER_NAME			√	√
CLUSTER_NAME		√	√	√
DESTINATION_ALIAS			√	√
DESTINATION_ALIAS_PARAMS			√	√
GLOBAL_CALL-SERIAL_NUMBER	GUID		√	√
LOCAL_CALL_SERIAL_NUMBER	GUID		√	√
METHOD	INVITE / ARQ / LRQ / OPTIONS / SETUP / REGISTER	√	√	√
NETWORK_TYPE	IPV4 / IPV6		√	√
POLICY_TYPE	REGISTRATION / SEARCH / ADMIN	√	√	√
PROTOCOL	SIP / H323	√	√	√
REGISTERED_ALIAS			√	√
SOURCE_ADDRESS		√	√	√
SOURCE_IP		√	√	√
SOURCE_PORT		√	√	√
TRAVERSAL_TYPE	TYPE_[UNDEF / ASSENTSERVER / ASSENTCLIENT / H460SERVER / H460CLIENT / TURNSERVER / TURNCLIENT / ICE]		√	√
UNAUTHENTICATED_SOURCE_ALIAS			√	√
UTCTIME		√	√	√

Parameter name	Values	Registration policy	Search rules	Call policy
ZONE_NAME			√	√

Cryptography support

External policy servers should support TLS and AES-256/AES-128/3DES-168.

SHA-1 is required for MAC and Diffie-Hellman / Elliptic Curve Diffie-Hellman key exchange; the Expressway does not support MD5.

Default CPL for Policy Services

When configuring a policy service, you can specify the **Default CPL** that is used by the Expressway if the service is not available.

The **Default CPL** for registrations and Call Policy defaults to:

<reject status='403' reason='Service Unavailable'/>

and this will reject the request.

The **Default CPL** for policy services used by search rules defaults to:

<reject status='504' reason='Policy Service Unavailable'/>

and this will stop the search via that particular search rule.

This default CPL mean that in the event of a loss of connectivity to the policy server, all call and registration requests will be rejected. If this is not your required behavior then you are recommended to specify alternative default CPL.

We recommend that you use unique reason values for each type of service, so that if calls or registrations are rejected it is clear why and which service is rejecting the request.

Flash Status Word Reference Table

The flash status word is used in diagnosing NTP server synchronization issues.

It is displayed by the *ntpq* program *rv* command. It comprises a number of bits, coded in hexadecimal as follows:

Code	Tag	Message	Description
0001	TEST1	pkt_dup	duplicate packet
0002	TEST2	pkt_bogus	bogus packet
0004	TEST3	pkt_unsync	server not synchronized
0008	TEST4	pkt_denied	access denied
0010	TEST5	pkt_auth	authentication failure

Code	Tag	Message	Description
0020	TEST6	pkt_stratum	invalid leap or stratum
0040	TEST7	pkt_header	header distance exceeded
0080	TEST8	pkt_autokey	Autokey sequence error
0100	TEST9	pkt_crypto	Autokey protocol error
0200	TEST10	peer_stratum	invalid header or stratum
0400	TEST11	peer_dist	distance threshold exceeded
0800	TEST12	peer_loop	synchronization loop
1000	TEST13	peer_unreach	unreachable or nonselect

Supported RFCs

Expressway supports the following RFCs:

Table 21: Supported RFCs

RFC	Description
791	Internet Protocol
1213	Management Information Base for Network Management of TCP/IP-based internets
1305	Network Time Protocol (Version 3) Specification, Implementation and Analysis
2327	SDP: Session Description Protocol
2460	Internet Protocol, Version 6 (IPv6) Specification (partial, static global addresses only)
2464	Transmission of IPv6 Packets over Ethernet Networks
2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
2782	A DNS RR for specifying the location of services (DNS SRV)
2833	RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
2915	The Naming Authority Pointer (NAPTR) DNS Resource Record

RFC	Description
2976	SIP INFO method
3164	The BSD syslog Protocol
3261	Session Initiation Protocol
3263	Locating SIP Servers
3264	An Offer/Answer Model with the Session Description Protocol (SDP)
3325	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
3326	The Reason Header Field for the Session initiation Protocol (SIP)
3265	Session Initiation Protocol (SIP) – Specific Event Notification
3327	Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts
3489	STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
3515	The Session Initiation Protocol (SIP) Refer Method
3550	RTP: A Transport Protocol for Real-Time Applications
3581	An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing
3596	DNS Extensions to Support IP Version 6
3761	The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)
3880	Call Processing Language (CPL): A Language for User Control of Internet Telephony Services
3891	Replaces header
3892	Referred-by header
3903	Session Initiation Protocol (SIP) Extension for Event State Publication
3944	H.350 Directory Services
3986	Uniform Resource Identifier (URI): Generic Syntax

RFC	Description
4028	Session Timers in the Session Initiation Protocol
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers
4291	IP Version 6 Addressing Architecture
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
4480	RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)
4787	Network Address Translation (NAT) Behavioral Requirements for Unicast UDP
4861	Neighbor Discovery for IP version 6 (IPv6)
5095	Deprecation of Type 0 Routing Headers in IPv6
5104	Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF): Temporary Maximum Media Stream Bit Rate Request (TMMBR)
5245	Interactive Connectivity Establishment (ICE)
5389	Session Traversal Utilities for NAT (STUN)
5424	The Syslog Protocol
5626	Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)
5627	Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP). Note that this RFC is only partially supported: Public GRUU is supported; Temporary GRUU is not supported.
5766	Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)
5806	Diversion Indication in SIP
6156	Traversal Using Relays around NAT (TURN) Extension for IPv6

Software Version History

This section summarizes feature updates in earlier software releases, starting from version X8.7. For information about a particular feature, see Release Notes for the relevant software version.

New features from software version X12.5 and later are not supported for the Cisco VCS product, and apply only to the Cisco Expressway product. For VCS systems, this version is provided for maintenance and bug fixing purposes only.

X12.6 Features

Table 22: Feature History by Release Number - Cisco Expressway Series

Feature/ change	Status
Whisper Coaching / Whisper Announcements over MRA	Supported from X12.6.2
Customizable Alarm-based Email Notifications	Supported from X12.6.2
Agent Greeting over MRA	Supported from X12.6.2
Display Active MRA Registrations Count	Supported from X12.6.1
Silent Monitoring Over MRA	Supported from X12.6.1
Security Enhancements	Supported from X12.6
Smart Licensing	Supported from X12.6
Type and Series Configuration by UI Setting not by Option Key	Supported from X12.6
Alarm-based Email Notifications	Supported from X12.6
Hardware Security Module (HSM) Support	Preview
Android Push Notifications for IM&P	Preview (disabled by default from X12.6.2)
Headset Capabilities for Cisco Contact Center	Preview
Multiple Presence Domains over MRA	Preview
Expressway Forward Proxy	Removed from X12.6.2
Smart Call Home	Removed from X12.6.2
Advanced Media Gateway	Removed from X12.6

X12.5 Features

Table 23: Feature History by Release Number - Cisco Expressway Series

Feature/ change	X12.5	X12.5.1	X12.5.2, X12.5.3	X12.5.4, X12.5.5, X12.5.6, X12.5.9 (X12.5.7 & X12.5.8 withdrawn)
Direct 9-1-1 Calls for “Kari's Law” (for Applicable B2B Deployments)	NA	NA	NA	Supported from X12.5.7 onwards
Virtualized Systems - ESXi Qualification and version support	Please see the *Cisco Expressway on Virtual Machine Installation Guide* for details			
ACME (Automated Certificate Management Environment) support on Expressway-E	Supported	Supported	Supported	Supported
Single SAML for Clusters	Supported	Supported	Supported	Supported
SIP Proxy to Multiple Meeting Server Conference Bridges - Support for Cisco Meeting Server Load Balancing (Not new in X12.5. Included for information due to its preview status)	Preview	Supported	Supported	Supported
MRA: Media Path Optimization for ICE	Supported	Supported	Supported	Supported
MRA: Improved Handling of Dual Network Domains with no Split DNS	Supported	Supported	Supported	Supported

Feature/ change	X12.5	X12.5.1	X12.5.2, X12.5.3	X12.5.4, X12.5.5, X12.5.6, X12.5.9 (X12.5.7 & X12.5.8 withdrawn)
MRA: OAuth with Refresh (Self-Describing) on Unified CM SIP Lines	Preview	Supported	Supported	Supported
MRA: Device Onboarding with Activation Codes	Preview	Preview	Preview	Supported
MRA: Support for Encrypted iX	Preview	Preview	Preview	Supported
MRA: Support for Headset Management	Preview	Preview	Preview	Supported
Features which are not new in X12.5 but included for information due to their former preview status:				
Cisco Meeting App can use the Expressway-E TURN Server	Preview	Supported	Supported	Supported
Multiple Presence Domains over MRA	Preview	Preview	Preview	Preview
Smart Call Home	Deprecated and Preview	Deprecated and Preview	Deprecated and Preview	Deprecated and Preview

X8.11 Features

Table 24: Feature History by Release Number

Feature/ change	X8.11 (withdrawn)	X8.11.1 (withdrawn)	X8.11.2 (withdrawn)	X8.11.3 (withdrawn)	X8.11.4
System Size Selection for Appliances	—	—	—	Supported	Supported

Feature/ change	X8.11 (withdrawn)	X8.11.1 (withdrawn)	X8.11.2 (withdrawn)	X8.11.3 (withdrawn)	X8.11.4
Finesse Agent Support over MRA	—	—	Supported	Supported	Supported
First Software Release for the CE1200 Appliance	—	Supported	Supported	Supported	Supported
Device Registration to Expressway-E (SIP and H.323)	Supported	Supported	Supported	Supported	Supported
Changes to Cisco TMS Provisioning Access	Supported	Supported	Supported	Supported	Supported
Multiway Conferencing on Cisco Expressway Series	Supported	Supported	Supported	Supported	Supported
SIP Proxy to Multiple Meeting Server Conference Bridges (Support for Cisco Meeting Server Load Balancing)	Preview	Preview	Preview	Preview	Preview
Web Proxy to Multiple Meeting Server Web Bridges	Supported	Supported	Supported	Supported	Supported
Cisco Meeting App can use Expressway-E TURN Server	Preview	Preview	Preview	Preview	Preview
TURN on TCP 443	Supported	Supported	Supported	Supported	Supported

Feature/ change	X8.11 (withdrawn)	X8.11.1 (withdrawn)	X8.11.2 (withdrawn)	X8.11.3 (withdrawn)	X8.11.4
TURN Port Multiplexing on Large Expressway-E	Supported	Supported	Supported	Supported	Supported
Improved Security of Data at Rest	Supported	Supported	Supported	Supported	Supported
Common Criteria Preparation	Supported	Supported	Supported	Supported	Supported
Mandatory Password on Backups	Supported	Supported	Supported	Supported	Supported
Custom Domain Search	Supported	Supported	Supported	Supported	Supported
Built-in-Bridge Recording over MRA (Not new in X8.11. Included for information due to its former preview status) Information about BiB over MRA is now available in the *Mobile and Remote Access Through Cisco Expressway* guide	Supported (formerly preview)	Supported	Supported	Supported	Supported
Access Policy Support over MRA (Not new in X8.11. Included for information due to its former preview status)	Supported (formerly preview) Requires Cisco Jabber 12.0	As for X8.11	As for X8.11	As for X8.11	As for X8.11

Feature/ change	X8.11 (withdrawn)	X8.11.1 (withdrawn)	X8.11.2 (withdrawn)	X8.11.3 (withdrawn)	X8.11.4
Multiple Presence Domains over MRA (Not new in X8.11. Included for information due to its preview status)	Preview	Preview	Preview	Preview	Preview
License Key Consolidation	Supported	Supported	Supported	Supported	Supported
Factory Reset of Peer Leaving Cluster	Supported	Supported	Supported	Supported	Supported
Smart Call Home (Not new in X8.11. Included for information due to its preview status)	Preview	Preview	Preview	Preview	Preview
SRV Connectivity Tester Tool	Supported	Supported	Supported	Supported	Supported
REST API Expansion	Supported	Supported	Supported	Supported	Supported

X8.10 Features

Table 25: Feature History by Release Number

Feature / change	X8.10	X8.10.1	X8.10.2	X8.10.3 (no change)	X8.10.4 (no change)
Built-in-Bridge Recording over MRA	Not supported	Not supported	Preview	Preview	Preview
Improved Push Notification Support for MRA	Preview	Supported	Supported	Supported	Supported

Feature / change	X8.10	X8.10.1	X8.10.2	X8.10.3 (no change)	X8.10.4 (no change)
Self-Describing Tokens Support for MRA (OAuth tokens with refresh)	Preview	Supported	Supported	Supported	Supported
Access Control Configuration Changes for MRA	Supported	Supported	Supported	Supported	Supported
Access Policy Support for MRA	Preview	Preview	Preview	Preview	Preview
Changes to TLS and Cipher Suite Defaults	Supported	Supported	Supported	Supported	Supported
AES-GCM Cipher Mode for Media Encryption	Supported	Supported	Supported	Supported	Supported
Delayed Cisco XCP Router Restart for Multitenancy	Supported	Supported	Supported	Supported	Supported
Server Name Indication for Multitenancy	Supported	Supported	Supported	Supported	Supported
Session Identifier Support	Supported	Supported	Supported	Supported	Supported
REST API Expansion	Supported	Supported	Supported	Supported	Supported
Smart Call Home (Not new in X8.10. Included for information due to its preview status)	Preview	Preview	Preview	Preview	Preview

X8.9 Features

Table 26: Feature History by Release Number

Feature / change	X8.9	X8.9.1	X8.9.2
Apple Push Notifications Service Pass Through to Cisco Jabber for iPhone and iPad	Not supported	Supported	Supported
Edge Traversal of Microsoft SIP Traffic for Cisco Meeting Server	Supported	Supported	Supported
Web Proxy for Meeting Server	Not supported	Not supported	Supported
IM and Presence Service Federation With Skype for Business or Office 365 Organizations	Preview	Supported	Supported
Cisco Expressway as H.323 Gatekeeper	Supported	Supported	Supported
REST API Expansion	Supported	Supported	Supported
Allow Jabber for iPhone and iPad to Use Safari for SSO Over MRA	Supported	Supported	Supported
Shared Line / Multiple Line Support for MRA Endpoints	Preview	Supported	Supported
Smart Call Home	Preview	Preview	Preview
Secure Install Wizard	Supported	Supported	Supported
DiffServ Code Point Marking	Supported	Supported	Supported
Maintenance Mode For MRA	Supported	Supported	Supported

X8.8 Features

Table 27: Feature History by Release Number

Feature / change	X8.8
Registrations On Expressway	Supported
Skype for Business 2016 and Skype for Business Mobile Support	Supported
Broker for Microsoft SIP Traffic	Supported
Multistream Support	Supported
Service Setup Wizard	Supported
MRA Allow List Improvement	Supported
API for Remote Configuration of MRA	Supported
Large VM CPU Reservation Reduced	Supported
High Security Environment	Supported
Software Package Signing	Supported
SSL/TLS Support Restricted	Supported

X8.7 Features

Table 28: Feature History by Release Number

Feature / change	X8.7
Dial via Office-Reverse (DVO-R)	Supported
Lync Screen Sharing Through a Gateway Cluster	Supported
Mobile and Remote Access with Supported Cisco IP Phones	Supported
Hybrid Services and Expressway/VCS Rebranding	Supported
Hosting on VMWare vSphere® 6.0	Supported
Keyword Filter for Syslog Output	Supported

Legal Notices

Intellectual Property Rights

This Administrator Guide and the product to which it relates contain information that is proprietary to TANDBERG and its licensors. Information regarding the product is found below in the **Copyright notice** and **Patent information** sections.

TANDBERG® is a registered trademark belonging to Tandberg ASA. Other trademarks used in this document are the property of their respective holders. This Guide may be reproduced in its entirety, including all copyright and intellectual property notices, in limited quantities in connection with the use of this product. Except for the limited exception set forth in the previous sentence, no part of this Guide may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, electronically, mechanically, by photocopying, or otherwise, without the prior written permission of TANDBERG.

COPYRIGHT © TANDBERG

Copyright Notice

The product that is covered by this Administrator Guide is protected under copyright, patent, and other intellectual property rights of various jurisdictions.

This product is Copyright © 2014, Tandberg Telecom UK Limited. All rights reserved.

TANDBERG is now part of Cisco. Tandberg Telecom UK Limited is a wholly owned subsidiary of Cisco Systems, Inc.

This product includes copyrighted software licensed from others. A list of the licenses and notices for open source software used in this product can be found at: http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-licensing-information-listing.html

This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing).

This product includes software developed by the University of California, Berkeley and its contributors.

IMPORTANT: USE OF THIS PRODUCT IS SUBJECT IN ALL CASES TO THE COPYRIGHT RIGHTS AND THE TERMS AND CONDITIONS OF USE REFERRED TO ABOVE. USE OF THIS PRODUCT CONSTITUTES AGREEMENT TO SUCH TERMS AND CONDITIONS.

AVC Video License

With respect to each AVC/H.264 product, we are obligated to provide the following notice:

This product is licensed under the AVC patent portfolio license for the personal use of a consumer or other uses in which it does not receive remuneration to (i) encode video in compliance with the AVC standard (“AVC video”) and/or (ii) decode AVC video that was encoded by a consumer engaged in a personal activity and/or was obtained from a video provider licensed to provide AVC video. No license is granted or shall be implied for any other use. Additional information may be obtained from MPEG LA, L.L.C.

See .http://www.mpegla.com

Accordingly, please be advised that service providers, content providers, and broadcasters are required to obtain a separate use license from MPEG LA prior to any use of AVC/H.264 encoders and/or decoders.

Patent Information

This product is covered by one or more of the following patents:

- US7,512,708
- EP1305927
- EP1338127