# Zones and Neighbors

This section describes how to configure zones and neighbors on the Expressway (**Configuration** > **Zones**).



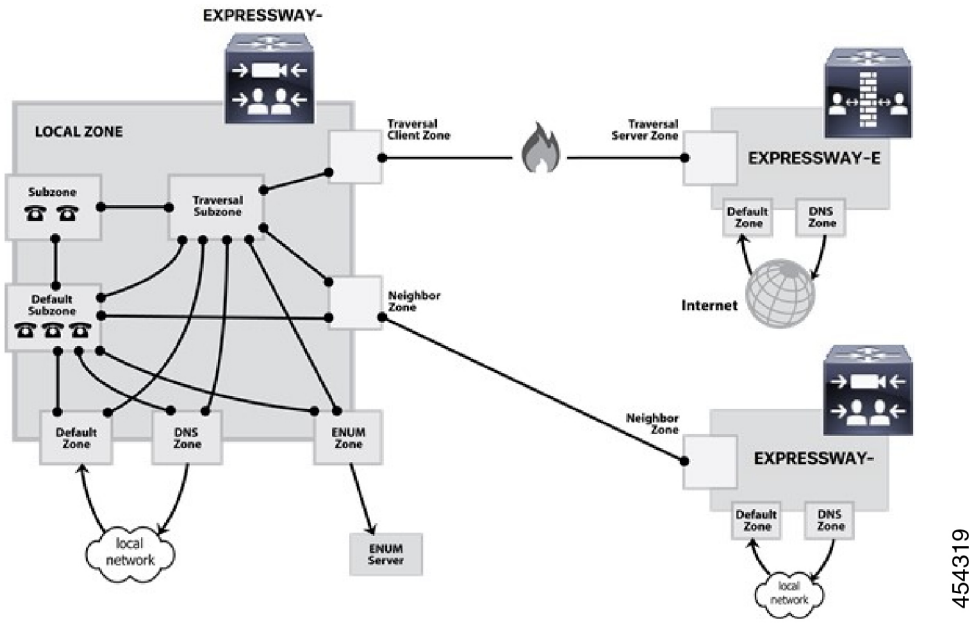
# Video Network Fundamentals

This section summarizes the different parts of a video communications network that uses Expressway, and the ways to connect them.

The most basic implementation is a single Expressway connected to the internet with one or more endpoints registered to it. Depending on the size and complexity of your enterprise the Expressway may be part of a network of endpoints, other Expressways and other network infrastructure devices, and with one or more firewalls between the Expressway and the internet. (In such situations you may want to apply restrictions to the amount of bandwidth used by and between different parts of your network.)

The diagram shows the different subzones and zones for an example Expressway deployment. It uses a Expressway-C as the example Local Zone, to show how it's made up of multiple subzones connected by links. The Local Zone is connected to external Expressways and to the internet via particular types of zones.

*Figure 1: Example network diagram*




# Structuring the Dial Plan

As you start deploying more than one Expressway, it is useful to neighbor the systems together so that they can query each other about their registered endpoints. Before you start, you should consider how you will structure your dial plan. This will determine the aliases assigned to the endpoints, and the way in which the Expressways are neighbored together. The solution you choose will depend on the complexity of your system. Some possible options are described in the following sections.

## Flat Dial Plan

The simplest approach is to assign each endpoint a unique alias and divide the endpoint registrations between the Expressways. Each Expressway is then configured with all the other Expressway as neighbor zones. When one Expressway receives a call for an endpoint which is not registered with it, it will send out a Location Request to all the other neighbor Expressways.

While conceptually simple, this sort of flat dial plan does not scale very well. Adding or moving an Expressway requires changing the configuration of every Expressway, and one call attempt can result in a large number of location requests. This option is therefore most suitable for a deployment with just one or two Expressways plus its peers.

## Structured Dial Plan

An alternative deployment would use a structured dial plan where endpoints are assigned an alias based on the system they are registering with.

If you are using E.164 aliases, each Expressway would be assigned an area code. When the Expressways are neighbored together, each neighbor zone would have an associated search rule configured with its corresponding area code as a prefix (a **Mode** of *Alias pattern match* and a **Pattern type** of *Prefix*). That neighbor would then only be queried for calls to numbers which begin with its prefix.

In a URI based dial plan, similar behavior may be obtained by configuring search rules for each neighbor with a suffix to match the desired domain name.

It may be desirable to have endpoints register with just the subscriber number — the last part of the E.164 number. In that case, the search rule could be configured to strip prefixes before sending the query to that zone.

A structured dial plan minimizes the number of queries issued when a call is attempted. However, it still requires a fully connected mesh of all Expressways in your deployment. A hierarchical dial plan can simplify this.

# Hierarchical Dial Plan

In this type of structure one Expressway is nominated as the central directory Expressway for the deployment, and all other Expressways are neighbored with it alone.

- The directory Expressway is configured with each Expressway as a neighbor zone, and search rules for each zone that have a **Mode** of *Alias pattern match* and the target Expressway's prefix (as with the structured dial plan) as the **Pattern string**.
- Each Expressway is configured with the directory Expressway as a neighbor zone, and a search rule with a **Mode** of *Any alias* and a **Target** of the directory Expressway.

Unless your deployment uses device authentication, there's no need to neighbor every Expressway with each other. Adding a new Expressway now only requires changing configuration on the new Expressway and the directory Expressway. It may be necessary to neighbor the Expressways to each other if you use device authentication (see below).

Failure of the directory Expressway in this situation could cause significant disruption to communications. Consideration should be given to the use of clustering for increased resilience.

### Hierarchical dial plan (directory Expressway) deployments and device authentication

See Hierarchical dial plans and authentication policy for important information about how to configure your authentication policy within a hierarchical dial plan.

# About Zones

A zone is a collection of endpoints, either all registered to a single system or located in a certain way such as through an ENUM or DNS lookup. Zones have many functions, including:

- Control through links whether calls can be made between these zones.
- Manage the bandwidth of calls between your local subzones and endpoints in other zones.
- Search for aliases that are not registered locally.
- Control the services available to endpoints within that zone by setting up its authentication policy.

- Control the Configuring Media Encryption Policy and Configuring ICE Messaging Support capabilities for SIP calls to and from a zone.

You can configure up to 1000 zones. Each zone is configured as one of the following zone types:

- Configuring Neighbor Zones: A connection to a neighbor system of the local Expressway.
- Configuring Traversal Client Zones: The local Expressway is a traversal client of the system being connected to, and there is a firewall between the two.
- Configuring Traversal Server Zones: The local Expressway is a traversal server for the system being connected to, and there is a firewall between the two.
- Configuring ENUM Zones: The zone contains endpoints discoverable by ENUM lookup.
- Configuring DNS Zones: The zone contains endpoints discoverable by DNS lookup.
- Unified Communications traversal: A traversal client or traversal server zone used for Unified Communications features such as mobile and remote access or Jabber Guest.

The Expressway also has a pre-configured Configuring the Default Zone.

- See the Configuring Zones (Non-Default Zones) section for information about the configuration options available for all zone types.
- See the Configuring search and zone transform rules section for information about including zones as targets for search rules.

### Automatically generated neighbor zones

The Expressway may automatically generate some non-configurable neighbor zones:

- An Expressway-C automatically generates neighbor zones between itself and each discovered Unified CM node when the system is configured for mobile and remote access.
- An Expressway automatically generates a neighbor zone named “To Microsoft destination via B2BUA” when the Microsoft interoperability service is enabled.
- Expressway automatically generates a neighbor zone named “CEOAuth <Unified CM name>” between itself and each discovered Unified CM node when SIP OAuth Mode is enabled on Unified CM.

# Configuring ICE Messaging Support

The **ICE support** option is a per-zone configuration setting that controls how the Expressway supports ICE messages to and from SIP devices within that zone.

The behavior depends on the **ICE support** setting configuration on the incoming (ingress) and outgoing (egress) zone. When there is a mismatch of settings (*On* on one side and *Off* on the other side) the Expressway invokes its back-to-back user agent (B2BUA) to perform ICE negotiation with the relevant host.

All zones have **ICE support** set to *Off* by default.

When the B2BUA performs ICE negotiation with a host, it can offer TURN relay candidate addresses. To do this, the B2BUA must be configured with the addresses of the TURN servers to offer (via **Applications** > **B2BUA** > **B2BUA TURN servers**).

The following matrix shows the Expressway behavior for the different possible combinations of the **ICE support** setting when handling a call between, for example, zone A and zone B:

| **ICE support setting** | | **Zone A** | |
|---|---|---|---|
| | | **Off** | **On** |
| **Zone B** | **Off** | Standard Expressway proxying behavior.<br>B2BUA is not normally invoked (however, see the note below regarding media encryption policy). | B2BUA is invoked.<br>B2BUA includes ICE candidates in messages to hosts in Zone A. |
| | **On** | B2BUA is invoked.<br>B2BUA includes ICE candidates in messages to hosts in Zone B. | Standard Expressway proxying behavior.<br>B2BUA is not normally invoked (however, see the note below regarding media encryption policy). |

### Effect of media encryption policy when combined with ICE support

The Expressway also invokes the B2BUA if it has to apply a Configuring Media Encryption Policy, on page 6 (any encryption setting other than *Auto*). This table shows the effect on ICE negotiation behavior depending on the ICE support and media encryption modes of the ingress and egress zones:

| ICE support | Media encryption mode | B2BUA invoked | Effect on ICE negotiation |
|---|---|---|---|
| Both zones = *Off* | At least one zone is **not** *Auto* | Yes | The B2BUA will not perform any ICE negotiation with either host. |
| Both zones = *On* | At least one zone is **not** *Auto* | Yes | The B2BUA will perform ICE negotiation with both hosts. |
| Both zones = *On* | Both zones = *Auto* | No | The Expressway will not offer any TURN relay candidate addresses to either of the ICE capable hosts.<br>**Note** Each host device may have already been provisioned with TURN relay candidate addresses. |

**Note**

- B2BUA routed calls are identified in the call history by a component type of *B2BUA*.
- An RMS call license is used when a call goes via the encryption B2BUA except when calling to/from a registered endpoint.
- There is a limit of 100 concurrent calls (500 calls on Large systems) that can be routed via B2BUA.

# Configuring Media Encryption Policy

The media encryption policy settings allow you to selectively add or remove media encryption capabilities for SIP calls flowing through the Expressway. This allows you to configure your system so that, for example, all traffic arriving or leaving an Expressway-E from the public internet is encrypted, but is unencrypted when in your private network.

- The policy is configured on a per zone/subzone basis and applies only to that leg of the call in/out of that zone/subzone.
- Encryption is applied to the SIP leg of the call, even if other legs are H.323.

Media encryption policy is configured through the **Media encryption mode** setting on each zone and subzone, however the resulting encryption status of the call is also dependent on the encryption policy settings of the target system (such as an endpoint or another Expressway).

The encryption mode options are:

- *Force encrypted*: All media to and from the zone/subzone must be encrypted. If the target system/endpoint is configured to not use encryption, then the call will be dropped.
- *Force unencrypted*: All media must be unencrypted. If the target system/endpoint is configured to use encryption, then the call may be dropped; if it is configured to use *Best effort* then the call will fall back to unencrypted media.
- *Best effort*: Use encryption if available, otherwise fall back to unencrypted media.
- *Auto*: No specific media encryption policy is applied by the Expressway. Media encryption is purely dependent on the target system/endpoint requests. This is the default behavior and is equivalent to how the Expressway operated before this feature was introduced.

Encryption policy (any encryption setting other than *Auto*) is applied to a call by routing it through a back-to-back user agent (B2BUA) hosted on the Expressway.

**Note** Remember that when configuring your system to use media encryption:

- Any zone with an encryption mode of *Force encrypted* or *Force unencrypted* must be configured as a SIP-only zone (H.323 must be disabled on that zone).
- TLS transport must be enabled if an encryption mode of *Force encrypted* or *Best effort* is required.
- The call component routed through the B2BUA can be identified in the call history details as having a component type of B2BUA.
- As the B2BUA must take the media, each call is classified as a traversal call and thus uses a Rich Media Session (RMS) license except when both the endpoints are registered to Cisco infrastructure.
- There is a limit per Expressway of 100 simultaneous video calls (500 video calls on Large systems) that can have a media encryption policy applied.
- The B2BUA can also be invoked when Configuring ICE Messaging Support is enabled.

## Configuring the B2BUA for Media Encryption

The B2BUA used for encryption (and ICE support) is a different instance to the B2BUA used for Microsoft interoperability. The Microsoft interoperability service B2BUA has to be manually configured and enabled, the B2BUA used for encryption is automatically enabled whenever an encryption policy is applied.

# About the Local Zone and Subzones

The collection of all devices registered with the Expressway makes up its **Local Zone**.

The Local Zone is divided into **subzones**. These include an automatically created **Default Subzone** and up to 1000 manually configurable subzones.

When an endpoint registers with the Expressway, it's allocated to an appropriate subzone based on subzone membership rules. These rules specify the range of IP addresses or alias pattern matches for each subzone. If an endpoint's IP address or alias does not match any of the membership rules, it is assigned to the Default Subzone.

The Local Zone may be independent of network topology, and may comprise multiple network segments. The Expressway also has two special types of subzones:

- Traversal Subzone, which is always present
- Cluster Subzone, which is always present but only used when the Expressway is part of a cluster

### Bandwidth management

The Local Zone's subzones are used for bandwidth management. After you have set up your subzones you can apply bandwidth limits to:

- Individual calls between two endpoints within the subzone.
- Individual calls between an endpoint within the subzone and another endpoint outside of the subzone.
- The total of calls to or from endpoints within the subzone.

For full details of how to create and configure subzones, and apply bandwidth limitations to subzones including the Default Subzone and Traversal Subzone, see the Bandwidth control section.

### Registration, authentication and media encryption policies

In addition to bandwidth management, subzones are also used to control the Expressway's registration, authentication and media encryption policies.

See Configuring Subzones for more information about how to configure these settings.

### Local Zone searches

One of the functions of the Expressway is to route a call received from a locally registered endpoint or external zone to its appropriate destination. Calls are routed based on the address or alias of the destination endpoint.

The Expressway searches for a destination endpoint in its Local Zone and its configured external zones. You can prioritize the order in which these zones are searched, and filter the search requests sent to each zone, based on the address or alias being searched for. This allows you to reduce the potential number of search requests sent to the Local Zone and out to external zones, and speed up the search process.

For further information about how to configure search rules for the Local Zone, see the Configuring search and zone transform rules section.

# Configuring the Default Zone

The Default Zone represents any incoming calls from endpoints or other devices that are unregistered or not recognized as belonging to the Local Zone or any of the existing configured zones.

The Expressway comes preconfigured with the Default Zone and default links between it and the Traversal Subzone. The Default Zone cannot be deleted.

## Default Zone Settings

By configuring the Default Zone you can control how the Expressway handles calls from unrecognized systems and endpoints. Go to **Configuration** > **Zones** > **Zones** and click **DefaultZone**. The configurable options are:

| Field | Description | Usage tips |
|---|---|---|
| **Authentication policy** | The **Authentication policy** setting controls how the Expressway challenges incoming messages to the Default Zone. | See Authentication policy for more information. |
| **Media encryption mode** | The **Media encryption mode** setting controls the media encryption capabilities for SIP calls flowing through the Default Zone. | See Configuring Media Encryption Policy for more information. |
| **ICE support** | Controls whether ICE messages are supported by the devices in this zone. | See Configuring ICE Messaging Support for more information. |
| **Enable Mutual TLS on Default Zone** | *On* enforces MTLS (Mutual Transport Layer Security) on incoming connections through the Default Zone.<br><br>*Off* means that MTLS is not enforced on connections to the TLS port. MTLS will still be enforced if the connections are made to the dedicated MTLS port - if that port is enabled on **Configuration** > **Protocols** > **SIP**.<br><br>Default: *Off* | This setting does not affect other connections to the Default Zone (H.323, SIP UDP, or SIP TCP).<br><br>**Note** The B2BUA is not capable of client certificate checks. Calls will fail if you engage the B2BUA when MTLS is configured on TLS port 5061. We recommend that you enable TLS and MTLS on different ports (on **Protocols** > **SIP** page).<br><br>If you must use port 5061 for MTLS, then you should avoid engaging the B2BUA - by switching **Media encryption mode** to *Auto* on all zones in the call path. |

# Using Links and Pipes to Manage Access and Bandwidth

You can also manage calls from unrecognized systems and endpoints by configuring the “links” and “pipes” associated with the Default Zone. For example, you can delete the default links to prevent any incoming calls from unrecognized endpoints, or apply pipes to the default links to control the bandwidth consumed by incoming calls from unrecognized endpoints.

# Configuring Default Zone Access Rules

Create Default Zone access rules (**Configuration** > **Zones** > **Default Zone access rules**) to control which external systems are allowed to connect over SIP TLS to the Expressway via the Default Zone.

For each rule, you specify a pattern to compare against the CN (and any SANs) in the certificates received from external systems. You can then choose whether to allow or deny access to systems that present matching certificates. Up to 10,000 rules can be configured.

***Table 1: Default Zone Access Rule Parameters***

| Field | Description | Usagge tips |
|---|---|---|
| **Name** | The name assigned to the rule. | |
| **Description** | An optional free-form description of the rule. | |
| **Priority** | Determines the order in which the rules are applied if the certificate names match multiple rules. The rules with the highest priority (1, then 2, then 3 and so on) are applied first. Multiple rules with the same priority are applied in configuration order. | |
| **Pattern type** | The way in which the **Pattern string** must match the Subject Common Name or any Subject Alternative Names contained within the certificate.<br>*Exact*: The entire string must exactly match the name, character for character.<br>*Prefix*: The string must appear at the beginning of the name.<br>*Suffix*: The string must appear at the end of the name.<br>*Regex*: Treats the string as a regular expression. | You can test whether a pattern matches a particular name by using the Check pattern tool (**Maintenance** > **Tools** > **Check pattern**). |
| **Pattern string** | The pattern against which the name is compared. | |

| Field | Description | Usagge tips |
|---|---|---|
| **Action** | The action to take if the certificate matches this access rule.<br>*Allow*: Allows the external system to connect via the Default Zone.<br>*Deny*: Rejects any connection requests received from the external system. | |
| **State** | Indicates if the rule is enabled or not. | Use this setting to test configuration changes, or to temporarily disable certain rules. Any disabled rules still appear in the rules list but are ignored. |

# Configuring Zones (Non-Default Zones)

The **Zones** page (**Configuration** > **Zones** > **Zones**) lists all the zones that have been configured on the Expressway, and lets you create, edit and delete zones. Information is displayed for each listed zone about the number of calls, bandwidth used, number of proxied registrations, protocol status, and search rule status.

The H.323 or SIP status options are:

- *Off*: The protocol is disabled at either the zone or system level.
- *Active*: The protocol is enabled for the zone and it has at least one active connection; if multiple connections are configured and some of those connections have failed, the display indicates how many of the connections are *Active*.
- *On*: Indicates that the protocol is enabled for the zone (for zone types that do not have active connections, eg. DNS and ENUM zones).
- *Failed*: The protocol is enabled for the zone but its connection has failed.
- *Checking*: The protocol is enabled for the zone and the system is currently trying to establish a connection.

You configure a zone on the local Expressway to neighbor with another system (such as another Expressway or gatekeeper), to create a connection over a firewall to a traversal server or traversal client, or to discover endpoints via an ENUM or DNS lookup. The available zone types are:

- Configuring Neighbor Zones: Connects the local Expressway to a neighbor system.
- Configuring Traversal Client Zones: Connects the local Expressway to a traversal server.
- Configuring Traversal Server Zones: Connects the local Expressway-E to a traversal client.
- Configuring ENUM Zones: Enables ENUM dialing via the local Expressway.
- Configuring DNS Zones: Enables the local Expressway to locate endpoints and other systems by using DNS lookups.
- Unified Communications traversal: A traversal client or traversal server zone used for Unified Communications features such as mobile and remote access or Jabber Guest.

- Configuring the Webex Zone: Enables a specifically configured DNS zone for use with Cisco Collaboration Cloud.

The zone type indicates the nature of the connection and determines which configuration options are available. For traversal server zones, traversal client zones, and neighbor zones this includes providing information about the neighbor system such as its IP address and ports. See About Zones for more information about zones and the different zone types.

The Expressway also has a preconfigured Configuring the Default Zone. The Default Zone represents any incoming calls from endpoints or other devices that are unregistered or not recognized as belonging to the Local Zone or any of the existing configured zones.

Connections between the Expressway and neighbor systems must be configured to use the same SIP transport type, that is they must both be configured to use TLS or both be configured to use TCP. Any connection failures due to transport type mismatches are recorded in the Event Log.

After creating a zone you would normally make it a target of at least one of your zone policy search rules (**Configuration** > **Dial plan** > **Search rules**) otherwise search requests will not be sent to that zone.

# Configuring Neighbor Zones

A neighbor zone could be a collection of endpoints registered to another system (such as a VCS or Expressway), or it could be a SIP device (for example Cisco Unified Communications Manager). The other system or SIP device is referred to as a neighbor. Neighbors can be part of your own enterprise network, part of a separate network, or even standalone systems.

You create a neighbor relationship with the other system by adding it as a neighbor zone on your local Expressway. Then you can do the following operations with the neighbor zone:

- Query the neighbor about its endpoints.
- Apply transforms to any requests before they are sent to the neighbor.
- Control the bandwidth used for calls between your local Expressway and the neighbor zone.

**Note**

- Neighbor zone relationship definitions are one-way; adding a system as a neighbor to your Expressway does not automatically make your Expressway a neighbor of that system.
- Inbound calls from any configured neighbor are identified as coming from that neighbor.
- Systems that are configured as cluster peers (formerly known as Alternates) must not be configured as neighbors to each other.

The configurable options for a neighbor zone are described in the table.

***Table 2: Neighbor zone settings***

| Field | Description | Usage tips |
|---|---|---|
| **Configuration** section: | | |

| Field | Description | Usage tips |
|---|---|---|
| **Name** | The name acts as a unique identifier, allowing you to distinguish between zones of the same type. | |
| **Type** | The nature of the specified zone, in relation to the local Expressway. Select *Neighbor*. | Once a zone is created, you cannot change the **Type**. |
| **Hop count** | The hop count is the number of times a request will be forwarded to a neighbor gatekeeper or proxy (see the Hop counts section for more information). This field specifies the hop count to use when sending a search request to this particular zone. | If the search request was received from another zone and already has a hop count assigned, the lower of the two values is used. |
| **H.323** section: | | |
| **Mode** | Determines whether H.323 calls are allowed to and from the neighbor system. | |
| **Port** | The port on the neighbor system used for H.323 searches initiated from the local Expressway. | Must be the same port number as that configured on the neighbor system as its H.323 UDP port.<br>If the neighbor is a Expressway acting as a gatekeeper, this corresponds to the **Registration UDP Port** on **Configuration** > **Protocols** > **H.323** page. |
| **SIP** section: | | |
| **Mode** | Determines whether SIP calls are allowed to and from the neighbor system. | |
| **Port** | The port on the neighbor system used for outgoing SIP messages initiated from the local Expressway. | Must be the same port number as that configured on the neighbor system as its SIP TCP, SIP TLS or SIP UDP listening port (depending on which SIP **Transport** mode is in use). |
| **Transport** | Determines which transport type is used for SIP calls to and from the neighbor system. The default is *TLS*. | |
| **TLS verify mode** | Controls whether the Expressway performs X.509 certificate checking against the neighbor system when communicating over TLS. | If the neighbor system is another Expressway, both systems can verify each other's certificate (known as mutual authentication). See TLS Certificate Verification of Neighbor Systems for more information. |

| Field | Description | Usage tips |
|---|---|---|
| **Accept proxied registrations** | Controls whether proxied SIP registrations routed through this zone are accepted. | This setting only applies to registration requests for a domain for which the Expressway is acting as a Registrar. For requests for other domains the **SIP registration proxy mode** setting applies. See Proxying registration requests for more information. |
| **Media encryption mode** | Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. | See Configuring Media Encryption Policy for more information. |
| **ICE support** | Controls whether ICE messages are supported by the devices in this zone. | See Configuring ICE Messaging Support for more information. |
| **ICE Passthrough support** | Controls how the Expressway supports ICE Passthrough in this zone. | ICE Passthrough support takes precedence over ICE support. Best practice is to turn on ICE Passthrough support and turn off ICE support.<br>Configuration details and required versions for ICE passthrough are in the *Mobile and Remote Access Through Cisco Expressway guide* on the Expressway Configuration Guides page. |
| **Multistream mode** | Controls whether the Expressway B2BUA allows multistream calls to be negotiated between calling parties.<br>*On*: Expressway allows the calling parties to negotiate and set up a multistream call through this zone<br>*Off*: Expressway rejects multistream negotiation through this zone. The calling parties should fall back on negotiating a standard call. | This toggle has no effect on the call when the call does not traverse the B2BUA.<br>The default is *On* because we expect calling parties to respond correctly to each other if they do not both have multistream capability. However, if you are having trouble with configuring multistream between the calling parties, you may wish to disable multistream mode to check if the calling parties can negotiate a standard call.<br>In the case of a TelePresence Server, a standard call means that the TelePresence Server composes the streams from multiple participants into one "conference stream" to send to the endpoint, instead of sending multiple streams to the endpoint to process in its own way. |

| Field | Description | Usage tips |
|---|---|---|
| **Preloaded SIP routes support** | 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. | |
| **AES GCM support** | Enables AES GCM algorithms to encrypt/decrypt media passing through this zone. | This is disabled by default. You should enable it if the calling parties are trying to negotiate AES GCM. |
| **SIP UPDATE for session refresh** | Determines whether this zone supports the SIP UPDATE method to send and receive session refresh requests. | *On*: This zone sends and receives SIP UPDATE for session refresh requests.<br>*Off*: This zone does not allow SIP UPDATE for session refresh requests.<br>Default: *Off* |
| **Authentication** section: | | |
| **Authentication policy** | 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. See Authentication policy for more information. |
| **SIP authentication trust mode** | Controls whether authenticated SIP messages (ones containing a P-Asserted-Identity header) from this zone are trusted without further challenge. | See SIP Authentication Trust for more information. |
| **Location** section: | | |

| Field | Description | Usage tips |
|---|---|---|
| **Look up peers by** | Determines whether you look up peers by address, or by service (SRV) record lookup.<br>• *Address* (default) allows you to add up to six peers. When you click **Save**, the Expressway does the lookup for the addresses.<br>• *Service record* produces a field to enter the Service Domain. When you click **Save**, the Expressway queries its DNS server for service records based on the domain you entered and the protocols and transports that are enabled on the zone.<br>When you next visit the zone page, the status is reported where the peer addresses are shown. It shows the protocol (SIP, SIPS, H323), whether the peer is reachable, and the peer address followed by the port. | **Notes about SRV record lookup:**<br>These four service lookups are possible:<br>• _sip._udp.example.com. SIP over UDP (this is disabled on Expressway and its zones by default)<br>• _sip._tcp.example.com. SIP over TCP<br>• _sips._tcp.example.com. SIP over TLS (secure SIP)<br>• _h323._udp.example.com. H.323 over UDP (other transports have never been supported for H.323)<br>For any given neighbor zone configured with an SRV record lookup, by default the maximum number of peers the Expressway can register against is 15.<br>If you use look up by DNS server be aware that your zones communicate over the SRV record-specified port and not the zone port. Keep the DNS-specified port open on your firewall. |
| **Peer 1 to Peer 6 address** | The IP address or FQDN of the neighbor system.<br>Enter the addresses of additional peers if:<br>• The neighbor is an Expressway cluster, in which case you must specify all of the peers in the cluster<br>• The neighbor is a resilient non-Expressway system, in which case you must enter the addresses of all of the resilient elements in that system | Calls to an Expressway cluster are routed to whichever peer in that neighboring cluster has the lowest resource usage. See Neighboring Between Expressway Clusters for more information.<br>For connections to non-Expressway systems, the Expressway uses a round-robin selection process to decide which peer to contact if no resource usage information is available. |
| **Advanced** section: | | |

| Field | Description | Usage tips |
|---|---|---|
| **Zone profile** | Determines how the zone's advanced settings are configured.<br>*Default*: Uses the factory default profile.<br>*Custom*: Allows you to configure each setting individually.<br>Alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system. The options include:<br>• *Default*<br>• *Custom*<br>• *Cisco Unified Communications Manager (8.6 and below)*<br>• *Cisco Unified Communications Manager (8.6.1 or 8.6.2)*<br>• *Cisco Unified Communications Manager (9.x or later)*<br>• *Nortel Communication Server 1000*<br>• *Infrastructure device* (typically used for non-gatekeeper devices such as an MCU) | See Zone Configuration: Advanced Settings for details on the advanced settings.<br>Only use the *Custom* profile to configure the individual advanced settings on the advice of Cisco customer support.<br>See Cisco Unified Communications Manager with Expressway Deployment Guide for more information about *Cisco Unified Communications Manager* profiles. |

# Configuring Traversal Client Zones

To traverse a firewall, the Expressway must be connected with a traversal server (typically, an Expressway-E). In this situation your local Expressway is a traversal client, so you create a connection with the traversal server by creating a traversal client zone on your local Expressway. You then configure the client zone with details of the corresponding zone on the traversal server. (The traversal server must also be configured with details of the Expressway client zone.)

After you have neighbored with the traversal server you can do the following:

- Use the neighbor as a traversal server.
- Query the traversal server about its endpoints.
- Apply transforms to any queries before they are sent to the traversal server.
- Control the bandwidth used for calls between your local Expressway and the traversal server.

**Note** An NTP server must be configured for traversal zones to work.

### More information

Details about how traversal client zones and traversal server zones work together for firewall traversal are in About Firewall Traversal.

### Traversal client zone settings

The configurable options for a traversal client zone are described in the table.

***Table 3: Traversal client zone settings***

| Field | Description | Usage tips |
|---|---|---|
| **Configuration** section: | | |
| **Name** | The name acts as a unique identifier, allowing you to distinguish between zones of the same type. | |
| **Type** | The nature of the specified zone, in relation to the local Expressway. Select *Traversal client*. | After a zone has been created, the **Type** cannot be changed. |
| **Hop count** | The hop count is the number of times a request will be forwarded to a neighbor gatekeeper or proxy (see the Hop counts section for more information). This field specifies the hop count to use when sending a search request to this particular zone. | If the search request was received from another zone and already has a hop count assigned, the lower of the two values is used. |
| **Connection credentials** section: | | |
| **Username** and **Password** | Traversal clients must always authenticate with traversal servers by providing their authentication credentials. Each traversal client zone must specify a **Username** and **Password** to be used for authentication with the traversal server. | Multiple traversal client zones can be configured, each with distinct credentials, to connect to one or more service providers. |
| **H.323** section: | | |
| **Mode** | Determines whether H.323 calls are allowed to and from the traversal server. | |
| **Protocol** | Determines which of the two firewall traversal protocols (*Assent* or *H.460*.18) to use for calls to the traversal server. | See Configuring Ports for Firewall Traversal for more information. |
| **Port** | The port on the traversal server to use for H.323 calls to and from the local Expressway. | For firewall traversal to work via H.323, the traversal server must have a traversal server zone configured on it to represent this Expressway, using this same port number. |
| **SIP** section: | | |

| Field | Description | Usage tips |
|---|---|---|
| **Mode** | Determines whether SIP calls are allowed to and from the traversal server. | |
| **Port** | The port on the traversal server to use for SIP calls to and from the Expressway.<br>This must be different from the listening ports used for incoming SIP calls. | For firewall traversal to work via SIP, the traversal server must have a traversal server zone configured on it to represent this Expressway, using this same transport type and port number. |
| **Transport** | Determines which transport type is used for SIP calls to and from the traversal server. The default is *TLS*. | |
| **TLS verify mode** | Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal server when communicating over TLS. | See TLS Certificate Verification of Neighbor Systems for more information. |
| **Accept proxied registrations** | Controls whether proxied SIP registrations routed through this zone are accepted. | This setting only applies to registration requests for a domain for which the Expressway is acting as a Registrar. For requests for other domains the **SIP registration proxy mode** setting applies. See Proxying registration requests for more information. |
| **Media encryption mode** | Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. | See Configuring Media Encryption Policy for more information. |
| **ICE support** | Controls whether ICE messages are supported by the devices in this zone. | See Configuring ICE Messaging Support for more information. |
| **ICE Passthrough support** | Controls how the Expressway supports ICE Passthrough in this zone. | ICE Passthrough support takes precedence over ICE support. Best practice is to turn on ICE Passthrough support and turn off ICE support.<br>Configuration details and required versions for ICE passthrough are in the *Mobile and Remote Access Through Cisco Expressway Guide* on the Expressway Configuration Guides page. |

| Field | Description | Usage tips |
|---|---|---|
| **Multistream mode** | Controls whether the Expressway B2BUA allows multistream calls to be negotiated between calling parties.<br>*On*: Expressway allows the calling parties to negotiate and set up a multistream call through this zone<br>*Off*: Expressway rejects multistream negotiation through this zone. The calling parties should fall back on negotiating a standard call. | This toggle has no effect on the call when the call does not traverse the B2BUA.<br>The default is *On* because we expect calling parties to respond correctly to each other if they do not both have multistream capability. However, if you are having trouble with configuring multistream between the calling parties, you may wish to disable multistream mode to check if the calling parties can negotiate a standard call.<br>In the case of a TelePresence Server, a standard call means that the TelePresence Server composes the streams from multiple participants into one "conference stream" to send to the endpoint, instead of sending multiple streams to the endpoint to process in its own way. |
| **SIP poison mode** | Determines if SIP requests sent to systems located via this zone are "poisoned" such that if they are received by this Expressway again they will be rejected. | |
| **Preloaded SIP routes support** | 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. | |
| **SIP parameter preservation** | Determines whether the Expressway's B2BUA preserves or rewrites the parameters in SIP requests routed via this zone. | *On* preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA.<br>*Off* allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary.<br>Default: *Off* |
| **AES GCM support** | Enables AES GCM algorithms to encrypt/decrypt media passing through this zone. | This is disabled by default. You should enable it if the calling parties are trying to negotiate AES GCM. |

| Field | Description | Usage tips |
|---|---|---|
| **SIP UPDATE for session refresh** | Determines whether this zone supports the SIP UPDATE method to send and receive session refresh requests. | *On*: This zone sends and receives SIP UPDATE for session refresh requests.<br>*Off*: This zone does not allow SIP UPDATE for session refresh requests.<br>Default: *Off* |
| **Authentication** section: | | |
| **Authentication policy** | 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. | See Authentication policy for more information. |
| **Client settings** section: | | |
| **Retry interval** | The interval in seconds with which a failed attempt to establish a connection to the traversal server should be retried. | |
| **Location** section: | | |
| **Peer 1 to Peer 6 address** | The IP address or FQDN of the traversal server.<br>If the traversal server is an Expressway-E cluster, this should include all of its peers. | See Neighboring Between Expressway Clusters for more information. |

# Configuring Traversal Server Zones

An Expressway-E can act as a traversal server, providing firewall traversal on behalf of traversal clients (an Expressway-C).

For firewall traversal to work, the traversal server (Expressway-E) must have a special type of two-way relationship with each traversal client. To create this connection between a Expressway-E and a Expressway-C, see Configuring a Traversal Client and Server. For full details on how traversal client zones and traversal server zones work together to achieve firewall traversal, see About Firewall Traversal.

**Note** You must synchronize with an NTP server to make sure that traversal zones to work.

After you have neighbored with the traversal client you can:

- Provide firewall traversal services to the traversal client
- Query the traversal client about its endpoints

- Apply transforms to any queries before they are sent to the traversal client
- Control the bandwidth used for calls between your local Expressway and the traversal client
- View zone status information, including the connection addresses

**Note** Connection addresses listed in the status information may have been translated by a NAT element between the traversal server zone and the originating device.

*Table 4: Traversal server zone configuration reference*

| Field | Description | Usage tips |
|---|---|---|
| **Configuration** section: | | |
| **Name** | The name acts as a unique identifier, allowing you to distinguish between zones of the same type. | |
| **Type** | The nature of the specified zone, in relation to the local Expressway. Select *Traversal server*. | After a zone has been created, the **Type** cannot be changed. |
| **Hop count** | The hop count is the number of times a request will be forwarded to a neighbor gatekeeper or proxy (see the Hop counts section for more information). This field specifies the hop count to use when sending a search request to this particular zone. | If the search request was received from another zone and already has a hop count assigned, the lower of the two values is used. |
| **Connection credentials** section: | | |
| **Username** | Traversal clients must always authenticate with traversal servers by providing their authentication credentials.<br>The authentication username is the name that the traversal client must provide to the Expressway-E. (It is configured as the connection credentials **Username** in its traversal client zone.) | There must also be an entry in the Expressway-E's local authentication database for the client's authentication username and password. To check the list of entries and add it if necessary, go to the **Local authentication database** page. Either:<br>• Click on the **Add/Edit local authentication database** link<br>• Go to **Configuration** > **Authentication** > **Local database** |
| **H.323** section: | | |
| **Mode** | Determines whether H.323 calls are allowed to and from the traversal client. | |
| **Protocol** | Determines the protocol (*Assent* or *H.460.18*) to use to traverse the firewall/NAT. | See Configuring Ports for Firewall Traversal for more information. |

| Field | Description | Usage tips |
|---|---|---|
| **Port** | The port on the local Expressway-E to use for H.323 calls to and from the traversal client. | |
| **H.460.19 demultiplexing mode** | Determines whether or not the same two ports are used for media by two or more calls.<br>*On*: All calls from the traversal client use the same two ports for media.<br>*Off*: Each call from the traversal client uses a separate pair of ports for media. | |
| **SIP** section: | | |
| **Mode** | Determines whether SIP calls are allowed to and from the traversal client. | |
| **Port** | The port on the local Expressway-E to use for SIP calls to and from the traversal client. | This must be different from the listening ports used for incoming TCP, TLS and UDP SIP calls (typically 5060 and 5061). |
| **Transport** | Determines which transport type is used for SIP calls to and from the traversal client. The default is *TLS*. | |
| **Unified Communications services** | Controls whether this traversal zone provides Unified Communications services, such as mobile and remote access. | If enabled, this zone must also be configured to use TLS with **TLS verify mode** enabled.<br>This setting only applies when Unified Communications mode is set to *Mobile and remote access*. |
| **TLS verify mode and subject name** | Controls X.509 certificate checking and mutual authentication between this Expressway and the traversal client.<br>If **TLS verify mode** is enabled, a **TLS verify subject name** must be specified. This is the certificate holder's name to look for in the traversal client's X.509 certificate. | If the traversal client is clustered, the **TLS verify subject name** must be the FQDN of the cluster.<br>See TLS Certificate Verification of Neighbor Systems for more information. |
| **Accept proxied registrations** | Controls whether proxied SIP registrations routed through this zone are accepted. | This setting only applies to registration requests for a domain for which the Expressway is acting as a Registrar. For requests for other domains the **SIP Registration Proxy Mode** setting applies. See Proxying registration requests for more information. |
| **Media encryption mode** | Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to and from this zone. | See Configuring Media Encryption Policy for more information. |

| Field | Description | Usage tips |
|---|---|---|
| **ICE support** | Controls whether ICE messages are supported by the devices in this zone. | See Configuring ICE Messaging Support for more information. |
| **ICE Passthrough support** | Controls how the Expressway supports ICE Passthrough in this zone. | ICE Passthrough support takes precedence over ICE support. Best practice is to turn on ICE Passthrough support and turn off ICE support.<br>Configuration details and required versions for ICE passthrough are in the *Mobile and Remote Access Through Cisco Expressway Guide* on the Expressway Configuration Guides page. |
| **Multistream mode** | Controls whether the Expressway B2BUA allows multistream calls to be negotiated between calling parties.<br>*On*: Expressway allows the calling parties to negotiate and set up a multistream call through this zone<br>*Off*: Expressway rejects multistream negotiation through this zone. The calling parties should fall back on negotiating a standard call. | This toggle has no effect on the call when the call does not traverse the B2BUA.<br>The default is *On* because we expect calling parties to respond correctly to each other if they do not both have multistream capability. However, if you are having trouble with configuring multistream between the calling parties, you may wish to disable multistream mode to check if the calling parties can negotiate a standard call.<br>In the case of a TelePresence Server, a standard call means that the TelePresence Server composes the streams from multiple participants into one "conference stream" to send to the endpoint, instead of sending multiple streams to the endpoint to process in its own way. |
| **Poison mode** | Determines if SIP requests sent to systems located via this zone are "poisoned" such that if they are received by this Expressway again they will be rejected. | |
| **Preloaded SIP routes support** | 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. | |

| Field | Description | Usage tips |
|---|---|---|
| **SIP parameter preservation** | Determines whether the Expressway's B2BUA preserves or rewrites the parameters in SIP requests routed via this zone. | *On* preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA.<br>*Off* allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary.<br>Default: *Off* |
| **AES GCM support** | Enables AES GCM algorithms to encrypt/decrypt media passing through this zone. | This is disabled by default. You should enable it if the calling parties are trying to negotiate AES GCM. |
| **SIP UPDATE for session refresh** | Determines whether this zone supports the SIP UPDATE method to send and receive session refresh requests. | *On*: This zone sends and receives SIP UPDATE for session refresh requests.<br>*Off*: This zone does not allow SIP UPDATE for session refresh requests.<br>Default: *Off* |
| **Authentication** section: | | |
| **Authentication policy** | 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. | See Authentication policy for more information. |
| **UDP / TCP probes** section: | | |
| **UDP retry interval** | The frequency (in seconds) with which the client sends a UDP probe to the Expressway-E if a keep alive confirmation has not been received. | The default UDP and TCP probe retry intervals are suitable for most situations. However, if you experience problems with NAT bindings timing out, they may need to be changed. |
| **UDP retry count** | The number of times the client attempts to send a UDP probe to the Expressway-E during call setup. | |
| **UDP keep alive interval** | The interval (in seconds) with which the client sends a UDP probe to the Expressway-E after a call is established, in order to keep the firewall's NAT bindings open. | |

| Field | Description | Usage tips |
|---|---|---|
| **TCP retry interval** | The interval (in seconds) with which the traversal client sends a TCP probe to the Expressway-E if a keep alive confirmation has not been received. | |
| **TCP retry count** | The number of times the client attempts to send a TCP probe to the Expressway-E during call setup. | |
| **TCP keep alive interval** | The interval (in seconds) with which the traversal client sends a TCP probe to the Expressway-E when a call is in place, in order to maintain the firewall's NAT bindings. | |

# Configuring ENUM Zones

ENUM zones allow you to locate endpoints via an ENUM lookup. You can create one or more search rules for ENUM zones based on the ENUM DNS suffix used and/or by pattern matching of the endpoints' aliases.

After you have configured one or more ENUM zones, you can

- Apply transforms to alias search requests directed to that group of endpoints.
- Control the bandwidth used for calls between your local Expressway and each group of ENUM endpoints.

Full details of how to use and configure ENUM zones are given in the About ENUM Dialing section.

The configurable options for an ENUM zone are described in the table.

***Table 5: ENUM zone settings***

| Field | Description | Usage tips |
|---|---|---|
| **Name** | The name acts as a unique identifier, allowing you to distinguish between zones of the same type. | |
| **Type** | The nature of the specified zone, in relation to the local Expressway. Select *ENUM*. | After a zone has been created, the **Type** cannot be changed. |
| **Hop count** | The hop count is the number of times a request will be forwarded to a neighbor gatekeeper or proxy (see the Hop counts section for more information). This field specifies the hop count to use when sending a search request to this particular zone. | If the search request was received from another zone and already has a hop count assigned, the lower of the two values is used. |
| **DNS suffix** | The domain to be appended to the transformed E.164 number to create an ENUM domain for which this zone is queried. | |

| Field | Description | Usage tips |
|---|---|---|
| **H.323 mode** | Determines whether H.323 records are looked up for this zone. | |
| **SIP mode** | Determines whether SIP records are looked up for this zone. | |

# Configuring DNS Zones

DNS zones allow you to locate endpoints via a DNS lookup. You can create one or more search rules for DNS zones based on pattern matching of the endpoint aliases.

After you configure one or more DNS zones, you can apply transforms to alias search requests directed to that group of endpoints. You can also control the bandwidth used for calls between your local Expressway and each group of DNS endpoints. See About URI Dialing for more information on configuring and using DNS zones.

The configurable options for a DNS zone are described in the table.

***Table 6: DNS zone settings***

| Field | Description | Usage tips |
|---|---|---|
| **Name** | The name acts as a unique identifier, allowing you to distinguish between zones of the same type. | |
| **Type** | The nature of the specified zone, in relation to the local Expressway. Select *DNS*. | After a zone has been created, the **Type** cannot be changed. |
| **Hop count** | The hop count is the number of times a request will be forwarded to a neighbor gatekeeper or proxy (see the Hop counts section for more information). This field specifies the hop count to use when sending a search request to this particular zone. | If the search request was received from another zone and already has a hop count assigned, the lower of the two values is used. |
| **H.323** section | | |
| **H.323 mode** | Determines whether H.323 calls are allowed to systems and endpoints located using DNS lookups via this zone. | |
| **SIP** section | | |
| **SIP mode** | Determines whether SIP calls are allowed to systems and endpoints located using DNS lookups via this zone. | |

| Field | Description | Usage tips |
|---|---|---|
| **TLS verify mode and subject name** | Controls whether the Expressway performs X.509 certificate checking against the destination system server returned by the DNS lookup.<br>If **TLS verify mode** is enabled, a **TLS verify subject name** must be specified. This is the certificate holder's name to look for in the destination system server's X.509 certificate. | This setting only applies if the DNS lookup specifies TLS as the required protocol. If TLS is not required then the setting is ignored. See TLS Certificate Verification of Neighbor Systems for more information. |
| **TLS verify subject name** | The certificate holder's name to look for in the destination system server's X.509 certificate (must be in the SAN - Subject Alternative Name - attribute). | |
| **TLS verify inbound mapping** | Switch Inbound TLS mapping On to map inbound TLS connections to this zone if the peer certificate contains the TLS verify subject name. If the received certificate does not contain the TLS verify subject name (as Common Name or Subject Alternative Name) then the connection is not mapped to this zone. | Switch Inbound TLS mapping *Off* to prevent the Expressway from attempting to map inbound TLS connections to this zone. |
| **Fallback transport protocol** | The transport type to use for SIP calls from the DNS zone, when DNS NAPTR records and SIP URI parameters do not provide the preferred transport information.<br>The default is *UDP* (if enabled). | |
| **Media encryption mode** | Controls the media encryption policy applied by the Expressway for SIP calls (including interworked calls) to the internet. | See Configuring Media Encryption Policy for more information. |
| **ICE support** | Controls whether ICE messages are supported by the devices in this zone. | See Configuring ICE Messaging Support for more information. |
| **Preloaded SIP routes support** | 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. | |
| **Modify DNS request** | Routes outbound SIP calls from this zone to a manually specified SIP domain instead of the domain in the dialed destination. | This option is primarily intended for use with Call Service Connect. See www.cisco.com/go/hybrid-services. |
| **Domain to search for** | Enter a fully qualified domain name to find in DNS instead of searching for the domain on the outbound SIP URI. The original SIP URI is not affected. | |

| Field | Description | Usage tips |
|---|---|---|
| **AES GCM support** | Enables AES GCM algorithms to encrypt/decrypt media passing through this zone. | This is disabled by default. You should enable it if the calling parties are trying to negotiate AES GCM. |
| **SIP UPDATE for session refresh** | Determines whether this zone supports SIP UPDATE method to send and receive session refresh requests. | *On*: This zone sends and receives SIP UPDATE for session refresh requests.<br>*Off*: This zone does not allow SIP UPDATE for session refresh requests.<br>Default: *Off* |
| **Authentication** section | | |
| **SIP authentication trust mode** | Used in conjunction with the **Authentication Policy** to control whether pre-authenticated SIP messages (ones containing a P-Asserted-Identity header) received from this zone are trusted and are subsequently treated as authenticated or unauthenticated within the Expressway.<br>*On*: Pre-authenticated messages are trusted without further challenge and subsequently treated as authenticated within the Expressway. Unauthenticated messages are challenged if the **Authentication Policy** is set to *Check credentials*.<br>*Off*: Any existing authenticated indicators (the P-Asserted-Identity header) are removed from the message. Messages from a local domain are challenged if the **Authentication Policy** is set to *Check credentials*. | For a DNS zone, you should always set **Authentication policy** to treated as authenticated. |
| **Advanced** section | | |

| Field | Description | Usage tips |
|---|---|---|
| **Include address record** | 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 before moving on to query lower priority zones. If A and AAAA records exist at the same domain for systems other than those that support SIP or H.323, this may result in the Expressway believing the search was successful and forwarding calls to this zone, and the call will fail.<br>*On*: The Expressway queries for A or AAAA records. If any are found, the Expressway will not then query any lower priority zones.<br>*Off*: (Default) The Expressway will not query for A and AAAA records and instead will continue with the search, querying the remaining lower priority zones. | |
| **Zone profile** | Determines how the zone's advanced settings are configured.<br>*Default*: Uses the factory default profile.<br>*Custom*: Allows you to configure each setting individually. | See Zone Configuration: Advanced Settings for details on the advanced settings.<br>Only use the *Custom* profile to configure the individual advanced settings on the advice of Cisco customer support. |

# Configuring the Webex Zone

The Webex zone is a pre-configured DNS zone for connecting the Expressway-E to Cisco Webex. You can use this zone to enable Cisco Webex Hybrid Call Service or Webex Meetings, or both.

Expressway-E connects to Cisco Unified Communications Manager without Expressway-C. No traversal or firewall is required for this scenario, and Expressway E connects the Webex Cloud directly to Cisco Unified Communications Manager. The tested configuration uses standard Webex Edge Audio over the internet, with a Neighbor zone between Cisco Unified Communications Manager and Expressway -E.

This scenario requires inbound connections to be opened on the internal firewall. So it is **not** supported for standard Expressway deployments with the usual dual firewall configuration.

### To enable the Webex zone:

1. Go to **Configuration** > **Zones** > **Zones**.
2. Click **New**.
3. Select *Webex* from the **Type** dropdown.

Expressway creates the new zone, with a pre-configured name and pre-configured parameters that ensure the correct connections to Cisco Webex.

**Note** You cannot create more than one zone of this type, and you cannot modify the single instance of this zone after you have enabled it.

See Hybrid Call Service documentation for detailed configuration information.

### How to change the default settings

The media encryption mode for the Webex zone is "Auto". Because a Webex zone is a pre-configured DNS zone, if some scenarios require it to be "On", we recommend creating a DNS zone instead. Then change the DNS zone through the Expressway web interface (**Configuration** > **Zones** > **Zones** and set **Media encryption mode** to *On*). The same workaround can be used to change the **SIP authentication trust mode** to *On*.

# Zone Configuration: Advanced Settings

The table below describes the advanced zone configuration options for the Custom zone profile. Some of these settings only apply to specific zone types.

| Setting | Description | Default | Zone types |
|---|---|---|---|
| **Include address record** | 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 before moving on to query lower priority zones. If A and AAAA records exist at the same domain for systems other than those that support SIP or H.323, this may result in the Expressway believing the search was successful and forwarding calls to this zone, and the call will fail.<br>*On*: The Expressway queries for A or AAAA records. If any are found, the Expressway will not then query any lower priority zones.<br>*Off*: The Expressway will not query for A and AAAA records and instead will continue with the search, querying the remaining lower priority zones. | Off | DNS |
| **Monitor peer status** | Specifies whether the Expressway monitors the status of the zone's peers. If enabled, H.323 LRQs and/or SIP OPTIONS are periodically sent to the peers. If a peer fails to respond, that peer is marked as inactive. If all peers fail to respond the zone is marked as inactive. | Yes | Neighbor |

| Setting | Description | Default | Zone types |
|---|---|---|---|
| **Call signaling routed mode** | Specifies how the Expressway handles the signaling for calls to and from this neighbor.<br>*Auto*: Signaling is taken as determined by the **Call signaling optimization** (**Configuration** > **Call routing**) configuration.<br>*Always*: Signaling is always taken for calls to or from this neighbor, regardless of the **Call signaling optimization** configuration.<br>Calls via traversal zones or the B2BUA always take the signaling. | Auto | Neighbor |
| **Automatically respond to H.323 searches** | Determines what happens when the Expressway receives an H.323 search, destined for this zone.<br>*Off*: An LRQ message is sent to the zone.<br>*On*: Searches are responded to automatically, without being forwarded to the zone. | Off | Neighbor |
| **Automatically respond to SIP searches** | Determines what happens when the Expressway receives a SIP search that originated as an H.323 search.<br>*Off*: A SIP OPTIONS or SIP INFO message is sent.<br>*On*: Searches are responded to automatically, without being forwarded.<br>This should normally be left as the default *Off*. However, some systems do not accept SIP OPTIONS messages, so for these zones it must be set to On. If you change this to *On*, you must also configure pattern matches to ensure that only those searches that actually match endpoints in this zone are responded to. If you do not, the search will not continue to other lower-priority zones, and the call will be forwarded to this zone even if it cannot support it. | Off | Neighbor DNS |

| Setting | Description | Default | Zone types |
|---|---|---|---|
| **Send empty INVITE for interworked calls** | Determines whether the Expressway generates a SIP INVITE message with no SDP to send via 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.<br>*On*: SIP INVITEs with no SDP are generated.<br>*Off*: SIP INVITEs are generated and a pre-configured SDP is inserted before the INVITEs are sent.<br>In most cases this option should normally be left as the default *On*. However, some devices do not accept invites with no SDP, so for these zones this should be set to *Off*.<br>**Note** The settings for the pre-configured SDP are configurable via the CLI using the `xConfiguration Zones Zone [1..1000] [Neighbor/DNS] Interworking SIP` commands. They should only be changed on the advice of Cisco customer support. | | |
| **SIP parameter preservation** | Determines whether the Expressway's B2BUA preserves or rewrites the parameters in SIP requests routed via this zone.<br>*On* preserves the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA.<br>*Off* allows the B2BUA to rewrite the SIP Request URI and Contact parameters of requests routing between this zone and the B2BUA, if necessary.<br>Default: *Off* | Off | Neighbor<br>DNS<br>UC Traversal<br>Traversal Server<br>Traversal Client |
| **SIP poison mode** | *On*: SIP requests sent to systems located via this zone are "poisoned" such that if they are received by this Expressway again they will be rejected.<br>*Off*: SIP requests sent out via this zone that are received by this Expressway again will not be rejected; they will be processed as normal. | Off | Neighbor Traversal clientTraversal serverDNS |
| **SIP encryption mode** | Determines whether or not the Expressway allows encrypted SIP calls on this zone.<br>*Auto*: SIP calls are encrypted if a secure SIP transport (TLS) is used.<br>*Microsoft*: SIP calls are encrypted using MS-SRTP.<br>*Off*: SIP calls are never encrypted.<br>This option should normally be left as the default *Auto*. | Auto | Neighbor |

| Setting | Description | Default | Zone types |
|---|---|---|---|
| **SIP REFER mode** | Determines how SIP REFER requests are handled.<br>*Forward*: SIP REFER requests are forwarded to the target.<br>*Terminate*: SIP REFER requests are terminated by the Expressway. | Forward | Neighbor |
| **Meeting Server load balancing** | From X8.11, Cisco Expressway Series supports the mechanism that is used to load balance calls between Meeting Servers that are in call bridge groups.<br>When Cisco Meeting Servers are in a call bridge group, and a participant tries to join a space on a server that has no capacity, the call is rerouted to another server. That other server then sends a SIP INVITE to the call control layer, using the original call details. The participant is now in the correct space, on a different Meeting Server. In cases where there is capacity in the "second" server, but another Meeting Server has more capacity, it asks that Meeting Server in the group to send the SIP INVITE.<br>*On*: Expressway B2BUA processes the INVITEs from the Meeting Server. Required to enable load balancing for endpoints that are registered to Unified CM or this Expressway, or to a neighboring VCS or Expressway.<br>*Off*: Expressway B2BUA does not p | Off | Neighbor |
| **SIP multipart MIME strip mode** | Controls whether or not multipart MIME stripping is performed on requests from this zone.<br>This option should normally be left as the default *Off*. | Off | Neighbor |
| **SIP UPDATE strip mode** | Controls whether or not the Expressway strips the UPDATE method from the Allow header of all requests and responses received from, and sent to, this zone.<br>This option should normally be left as the default *Off*. However, some systems do not support the UPDATE method in the Allow header, so for these zones this should be set to *On*. | Off | Neighbor |
| **Interworking SIP search strategy** | Determines how the Expressway searches for SIP endpoints when interworking an H.323 call.<br>*Options*: The Expressway sends an OPTIONS request.<br>*Info*: The Expressway sends an INFO request.<br>This option should normally be left as the default *Options*. However, some endpoints cannot respond to OPTIONS requests, so this must be set to *Info* for such endpoints. | Options | Neighbor |

| Setting | Description | Default | Zone types |
|---|---|---|---|
| **SIP UDP/BFCP filter mode** | 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.<br>*On*: Any media line referring to the UDP/BFCP protocol is replaced with TCP/BFCP and disabled.<br>*Off*: INVITE requests are not modified. | Off | Neighbor<br>DNS |
| **SIP UDP/IX filter mode** | 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.<br>*On*: Any media line referring to the UDP/UDT/IX or UDP/DTLS/UDT/IX protocol is replaced with RTP/AVP and disabled.<br>*Off*: INVITE requests are not modified.<br>We recommend that **SIP UDP/IX filter mode** is set to *On* for:<br>• Business-to-business calls routed through neighbor zones that connect to external networks / non-Cisco infrastructure<br>• Calls that connect internally to Unified CM 8.x or earlier (use *Off* for 9.x or later) | *Off* in Cisco Unified Communications Manager preconfigured zone profile.<br>*On* otherwise. | Neighbor<br>DNS |
| **SIP record route address type** | 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.<br>*IP*: Uses the Expressway's IP address.<br>*Hostname*: Uses the Expressway's **System host name** (if it is blank the IP address is used instead). | IP | Neighbor<br>DNS |
| **SIP Proxy-Require header strip list** | A comma-separated list of option tags to search for and remove from Proxy-Require headers in SIP requests received from this zone. | None | Neighbor |

# Zone Configuration: Pre-Configured Profile Settings

The table below shows the advanced zone configuration option settings that are automatically applied for each of the pre-configured profiles.

| Setting | Cisco Unified CM, (9.x or later) | Cisco Unified CM, (8.6.1 or 8.6.2) | Cisco Unified CM (8.6 and below) | Nortel Communication Server 1000 | Infrastructure device | Default |
|---|---|---|---|---|---|---|
| Monitor peer status | Yes | Yes | Yes | Yes | No | Yes |
| Call signaling routed mode | Always | Always | Always | Auto | Always | Auto |
| Automatically respond to H.323 searches | Off | Off | Off | Off | On | Off |
| Automatically respond to SIP searches | Off | Off | Off | Off | On | Off |
| Send empty INVITE for interworked calls | On | On | On | On | On | On |
| SIP parameter preservation | Off | Off | Off | Off | Off | Off |
| SIP poison mode | Off | Off | Off | Off | Off | Off |
| SIP encryption mode | Auto | Auto | Auto | Auto | Auto | Auto |
| SIP REFER mode | Forward | Forward | Forward | Forward | Forward | Forward |
| Meeting Server load balancing | Off | Off | Off | Off | Off | On |
| SIP multipart MIME strip mode | Off | Off | Off | Off | Off | Off |
| SIP UPDATE strip mode | Off | Off | Off | On | Off | Off |
| Interworking SIP search strategy | Options | Options | Options | Options | Options | Options |

| Setting | Cisco Unified CM, (9.x or later) | Cisco Unified CM, (8.6.1 or 8.6.2) | Cisco Unified CM (8.6 and below) | Nortel Communication Server 1000 | Infrastructure device | Default |
|---|---|---|---|---|---|---|
| SIP UDP/BFCP filter mode | Off | Off | On | Off | Off | Off |
| SIP UDP/IX filter mode | Off | On | On | On | On | Off |
| SIP record route address type | IP | IP | IP | IP | IP | IP |
| SIP Proxy-Require header strip list | <blank> | <blank> | <blank> | [illegible] | <blank> | <blank> |

**More information about configuring a SIP trunk between Expressway and Unified CM:**

See *Cisco Expressway and CUCM via SIP Trunk Deployment Guide* on the Expressway Configuration Guides page.

# TLS Certificate Verification of Neighbor Systems

When a SIP TLS connection is established between an Expressway and a neighbor system, the Expressway can be configured to check the X.509 certificate of the neighbor system to verify its identity. You do this by configuring the zone's **TLS verify mode** setting.

If **TLS verify mode** is enabled, the neighbor system's FQDN or IP address, as specified in the **Peer address** field of the zone's configuration, is used to verify against the certificate holder's name contained within the X.509 certificate presented by that system. (The name has to be contained in the Subject Alternative Name attributes of the certificate.) The certificate itself must also be valid and signed by a trusted certificate authority.

**Note** For traversal server and DNS zones, the FQDN or IP address of the connecting traversal client is not configured, so the required certificate holder's name is specified separately.

If the neighbor system is another Expressway, or it is a traversal client / traversal server relationship, the two systems can be configured to authenticate each other's certificates. This is known as mutual authentication and in this case each Expressway acts both as a client and as a server and therefore you must ensure that each Expressway's certificate is valid both as a client and as a server.

See Security Basics for more information about certificate verification and for instructions on uploading the Expressway's server certificate and uploading a list of trusted certificate authorities.

# Configuring a Zone for Incoming Calls Only

To configure a zone so that it is never sent an alias search request (for example if you only want to receive incoming calls from this zone), do not define any search rules that have that zone as its target.

In this scenario, when viewing the zone, you can ignore the warning indicating that search rules have not been configured.