



Dial Plan and Call Processing

This section provides information about the pages that appear under the Calls, Dial plan, Transforms and Call Policy sub-menus of the **Configuration** menu. These pages are used to configure the way in which the Expressway receives and processes calls.

- [Call Routing Process, on page 1](#)
- [About Cisco VCS's Directory Service, on page 3](#)
- [Configuring Hop Counts, on page 3](#)
- [Configuring Dial Plan Settings, on page 4](#)
- [About Transforms and Search Rules, on page 6](#)
- [Example Searches and Transforms, on page 13](#)
- [Direct 9-1-1 Calls for Kari's Law \(with Expressway as Call Control and a PSTN Gateway\), on page 24](#)
- [Configuring Search Rules to Use an External Service, on page 29](#)
- [About Call Policy, on page 32](#)
- [Supported Address Formats, on page 39](#)
- [Dialing by IP Address, on page 40](#)
- [About URI Dialing, on page 42](#)
- [About ENUM Dialing, on page 50](#)
- [Configuring DNS Servers for ENUM and URI Dialing, on page 56](#)
- [Configuring Call Routing and Signaling, on page 57](#)
- [Identifying Calls, on page 58](#)
- [Disconnecting Calls, on page 59](#)

Call Routing Process

One of the functions of the Expressway is to route calls to their appropriate destination. It does this by processing incoming search requests in order to locate the given target alias. These search requests are received from:

- Locally registered endpoints
- Neighboring systems, including neighbors, traversal clients and traversal servers
- Endpoints on the public internet

Several steps are involved in determining the destination of a call, and some of these steps can involve transforming the alias or redirecting the call to other aliases.

It's important to understand the process before setting up your [dialing plan](#) so you can avoid circular references, where an alias is transformed from its original format to a different format, and then back to the original alias. The Expressway is able to detect circular references. If it identifies one it will terminate that branch of the search and return a “policy loop detected” error message.

How the Expressway determines the destination of a call

The process followed by the Expressway when attempting to locate a destination endpoint is described below.

1. The caller enters into their endpoint the alias or address of the destination endpoint. This alias or address can be in a number of [Supported Address Formats](#).
2. The destination address is received by the Expressway.
(The address comes to Expressway directly from a registered endpoint, or it may come indirectly as a result of other call processing infrastructure in your deployment)
3. Any [About Pre-Search Transforms](#) are applied to the alias.
4. Any [Configuring Call Policy](#) is applied to the (transformed) alias. If this results in one or more new target aliases, the process starts again with the new aliases checked against the pre-search transforms.
5. Any User Policy (if [FindMe](#) is enabled) is applied to the alias. If the alias is a FindMe ID that resolves to one or more new target aliases, the process starts again with all the resulting aliases checked against pre-search transforms and Call Policy.
6. The Expressway then searches for the alias according to its search rules:

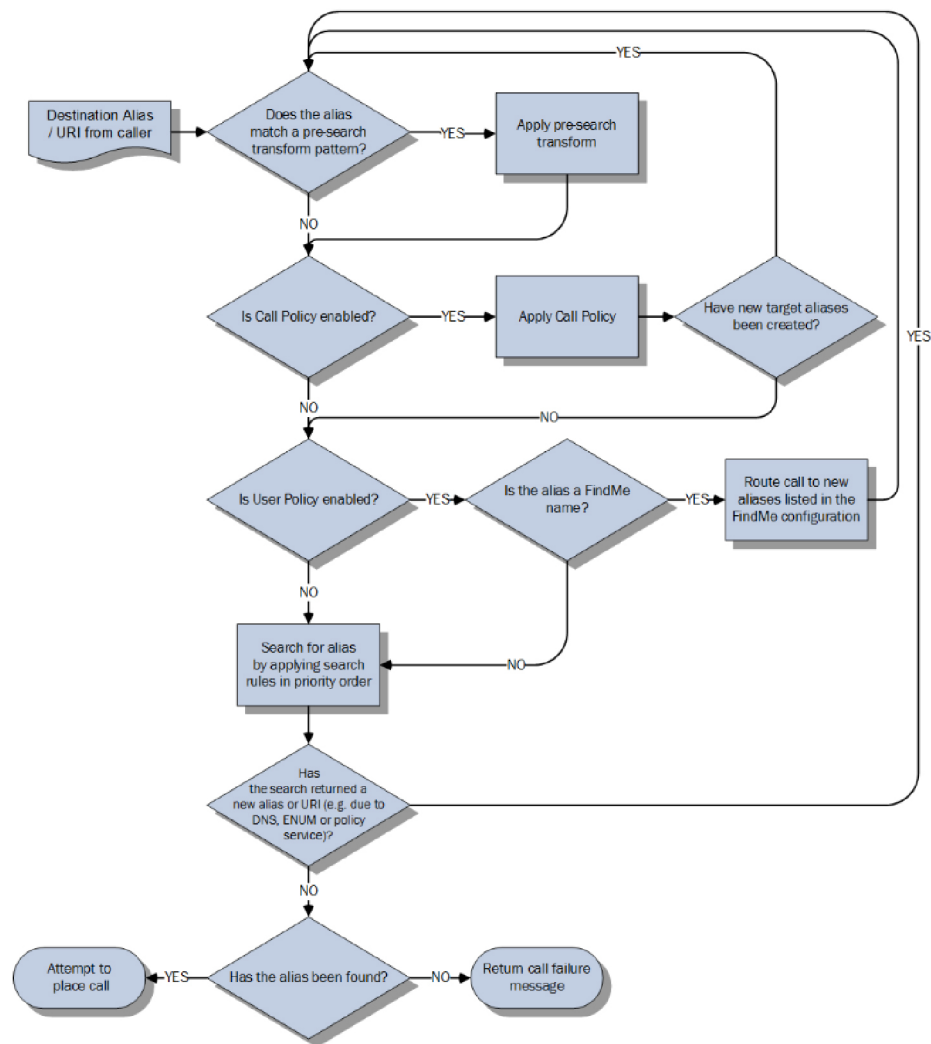


Note

The Expressway deliberately only searches for the first destination alias it reads from an H.323 Location Request. In very rare cases, this can lead to calls not being routed as expected.

- A matching rule may apply a zone transform to the alias before sending the query on to its **Target**. A **Target** can be one of the following types:
 - **Local Zone**: The endpoints and devices registered to the Expressway.
 - **Neighbor zone**: One of the Expressway's configured external neighbor zones, or a DNS or ENUM lookup zone.
 - **Policy service**: An external service or application. The service will return some CPL which could, for example, specify the zone to which the call should be routed, or it could specify a new destination alias.
- 7. If the search returns a new URI or alias (for example, due to a DNS or ENUM lookup, or the response from a policy service), the process starts again: the new URI is checked against any pre-search transforms, Call Policy and User Policy are applied and a new Expressway search is performed.
- 8. If the alias is found within the Local Zone, in one of the external zones, or a routing destination is returned by the policy service, the Expressway attempts to place the call.
- 9. If the alias is not found, it responds with a message to say that the call has failed.

Figure 1: Call Routing Flowchart



453646

About Cisco VCS's Directory Service

Configuring Hop Counts

Each search request is assigned a hop count value by the system that initiates the search. Every time the request is forwarded to another neighbor gatekeeper or proxy, the hop count value is decreased by a value of 1. When the hop count reaches 0, the request will not be forwarded on any further and the search will fail.

For search requests initiated by the local Expressway, the hop count assigned to the request is configurable on a zone-by-zone basis. The zone's hop count applies to all search requests originating from the local Expressway that are sent to that zone.

Search requests received from another zone will already have a hop count assigned. When the request is subsequently forwarded on to a neighbor zone, the lower of the two values (the original hop count or the hop count configured for that zone) is used.

For H.323, the hop count only applies to search requests. For SIP, the hop count applies to all requests sent to a zone (affecting the Max-Forwards field in the request).

The hop count value can be between 1 and 255. The default is 15.



Note If your hop counts are set higher than necessary, you may risk introducing loops into your network. In these situations a search request will be sent around the network until the hop count reaches 0, consuming resources unnecessarily. This can be prevented by setting the [Configuring Call Routing and Signaling](#) to *On*.

When dialing by URI or ENUM, the hop count used is that for the associated DNS or ENUM zone via which the destination endpoint (or intermediary SIP proxy or gatekeeper) was found.

Configuring hop counts for a zone

Hop counts are configured on a zone basis.



Important The default hop count may be too low for your environment if you have a complex network. This can cause unexpected call failures in a correctly configured deployment. Consider raising the hop count if you anticipate long call paths.

For full details on other zone options, see the [Configuring Zones \(Non-Default Zones\)](#) section.

Procedure

- Step 1** Go to the **Zones** page (**Configuration > Zones > Zones**).
- Step 2** Click on the name of the zone you want to configure. You are taken to the **Edit zone** page.
- Step 3** In the **Configuration** section, in the **Hop count** field, enter the hop count value you want to use for this zone.

Configuring Dial Plan Settings

The **Dial plan configuration** page (**Configuration > Dial plan > Configuration**) is used to configure how the Expressway routes calls in specific call scenarios.

The configurable options are:

Field	Description	Usage tips
Calls to unknown IP addresses	<p>Determines the way in which the Expressway attempts to call systems which are not registered with it or one of its neighbors.</p> <p><i>Direct:</i> 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.</p> <p><i>Indirect:</i> 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.</p> <p><i>Off:</i> Endpoints registered directly to the Expressway may only call an IP address of a system also registered directly to that Expressway.</p> <p>The default is <i>Indirect</i>.</p>	<p>This setting applies to the call's destination address prior to any zone transforms, but after any pre-search transforms, Call Policy or User Policy rules have been applied.</p> <p>In addition to controlling calls, this setting also determines the behavior of provisioning and presence messages to SIP devices, as these messages are routed to IP addresses.</p> <p>See Dialing by IP Address for more information.</p>
Fallback alias	<p>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.</p>	<p>If no fallback alias is configured, calls that do not specify an alias will be disconnected. See below for more information.</p>

About the Fallback Alias

The Expressway could receive a call that is destined for it but which does not specify an alias. This could be for one of the following reasons:

- The caller has dialed the IP address of the Expressway directly
- The caller has dialed a domain name belonging to the Expressway (either one of its configured SIP domains, or any domain that has an SRV record that points at the IP address of the Expressway), without giving an alias as a prefix

Normally such calls would be disconnected. However, such calls will be routed to the **Fallback alias** if it is specified.



Note Some endpoints do not allow users to enter an alias and an IP address to which the call should be placed.

Example usage

You may want to configure your fallback alias to be that of your receptionist, so that all calls that do not specify an alias are still answered personally and can then be redirected appropriately.

For example, Example Inc has the domain of **example.com**. The endpoint at reception has the alias **reception@example.com**. They configure their Expressway with a fallback alias of **reception@example.com**.

This means that any calls made directly to **example.com** (that is, without being prefixed by an alias), are forwarded to **reception@example.com**, where the receptionist can answer the call and direct it appropriately.

About Transforms and Search Rules

The Expressway can be configured to use transforms and search rules as a part of its call routing process.

Transforms

Transforms are used to modify the alias in a search request if it matches certain criteria. You can transform an alias by removing or replacing its prefix, suffix, or the entire string, and by the use of regular expressions.

This transformation can be applied to the alias at two points in the routing process: as a pre-search transform, and as a zone transform.

- **Pre-search transforms** are applied before any Call Policy or User Policy are applied and before the search process is performed (see [About Pre-Search Transforms](#) for more details).
- **Zone transforms** are applied during the search process by each individual search rule as required. After the search rule has matched an alias they can be used to change the target alias before the search request is sent to a target zone or policy service (see [Search and Zone Transformation Process](#) for more details).

Search rules

Search rules are used to route incoming search requests to the appropriate target zones (including the Local Zone) or policy services.

The Expressway's search rules are highly configurable. You can:

- Define alias, IP address and pattern matches to filter searches to specific zones or policy services.
- Define the priority (order) in which the rules are applied and stop applying any lower-priority search rules after a match is found; this lets you reduce the potential number of search requests sent out, and speed up the search process.
- Set up different rules according to the protocol (SIP or H.323) or the source of the query (such as the Local Zone, or a specific zone or subzone).
- Set up rules that only match specific traffic types, for example standards-based SIP or Microsoft SIP.
- Limit the range of destinations or network services available to unauthenticated devices by making specific search rules applicable to [authenticated requests](#) only.
- Use zone transforms to modify an alias before the query is sent to a target zone or policy service.



Note Multiple search rules can refer to the same target zone or policy service. This means that you can specify different sets of search criteria and zone transforms for each zone or policy service.

The Expressway uses the protocol (SIP or H.323) of the incoming call when searching a zone for a given alias. If the search is unsuccessful the Expressway may then search the same zone again using the alternative protocol, depending on where the search came from and the **Interworking mode** (**Configuration** > **Protocols** > **Interworking**).

- If the request has come from a neighboring system and **Interworking mode** is set to *Registered only*, the Expressway searches the Local Zone using both protocols, and all other zones using the native protocol only (because it will interwork the call only if one of the endpoints is locally registered).
- If **Interworking mode** is set to *On*, or the request has come from a locally registered endpoint, the Expressway searches the Local Zone and all external zones using both protocols.

About Pre-Search Transforms

The pre-search transform function allows you to modify the alias in an incoming search request. The transformation is applied by the Expressway before any Call Policy or User Policy is applied, and before any searches take place.

Each pre-search transform defines a string against which an alias is compared, and the changes to make to the alias if it matches that string. After the alias has been transformed, it remains changed and all further call processing is applied to the new alias.



Note Only one transform can be matched per search.

Clustered systems

All peers in a cluster should be configured identically, including any pre-search transforms. Each Expressway treats search requests from any of its peers as having come from its own Local Zone, and does not re-apply any pre-search transforms on receipt of the request.

When does a transform apply?

- Applied to all incoming search requests received from locally registered endpoints, neighbor, traversal client and traversal server zones, and endpoints on the public internet.
- Not applied to requests received from peers. These are configured identically and therefore will have already applied the same transform.
- Not applied to GRQ or RRQ messages received from endpoints registering with the Expressway. The endpoints will be registered with the aliases as presented in these messages.

Pre-search transform process

Up to 100 pre-search transforms can be configured. Each transform must have a unique priority number between 1 and 65534.

1. Every incoming alias is compared with each transform in order of priority, starting with that closest to 1. If and when a match is made, the transform is applied to the alias and no further pre-search checks and transformations of the new alias will take place (only one transform can be matched per search). The new alias is used for the remainder of the **call routing process**.
2. Further transforms of the alias may take place during the remainder of the search process. This may be as a result of **Call Policy** (also known as Administrator Policy) or User Policy (if **FindMe** is enabled). If this is the case, the pre-search transforms are re-applied to the new alias.

If you add a new pre-search transform that has the same priority as an existing transform, all transforms with a lower priority - those with a larger numerical value - have their priority incremented by one, and the new transform is added with the specified priority. Or an error message is issued if there are insufficient “slots” to move all the priorities down.

Configuring Presearch Transforms

The **Transforms** page (**Configuration > Dial plan > Transforms**) lists all the [About Pre-Search Transforms](#) currently configured on the Expressway. It is used to create, edit, delete, enable and disable transforms.

Aliases are compared against each transform in order of **Priority**, until a transform is found where the alias matches the **Pattern** in the manner specified by the pattern **Type**. The alias is then transformed according to the **Pattern behavior** and **Replace string** rules before the search takes place (either locally or to external zones).

After the alias has been transformed, it remains changed, and all further call processing is applied to the new alias.



Note Transforms also apply to any [Unified Communications](#) messages.

The configurable options are:

Field	Description	Usage tips
Priority	The priority of the transform. Priority can be from 1 to 65534, with 1 being the highest priority. Transforms are applied in order of priority, and the priority must be unique for each transform.	
Description	An optional free-form description of the transform.	The description appears as a tooltip if you hover your mouse pointer over a transform in the list.
Pattern type	How the Pattern string must match the alias for the rule to be applied. Options are: <i>Exact</i> : The entire string must exactly match the alias character for character. <i>Prefix</i> : The string must appear at the beginning of the alias. <i>Suffix</i> : The string must appear at the end of the alias. <i>Regex</i> : Treats the string as a regular expression .	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).
Pattern string	Specifies the pattern against which the alias is compared.	The Expressway has a set of predefined pattern matching variables that can be used to match against certain configuration elements.

Field	Description	Usage tips
Pattern behavior	Specifies how the matched part of the alias is modified. Options are: <i>Strip</i> : The matching prefix or suffix is removed. <i>Replace</i> : The matching part of the alias is substituted with the text in the Replace string. <i>Add Prefix</i> : Prepends the Additional text to the alias. <i>Add Suffix</i> : Appends the Additional text to the alias.	
Replace string	The string to substitute for the part of the alias that matches the pattern.	Only applies if the Pattern behavior is <i>Replace</i> . You can use regular expressions.
Additional text	The string to add as a prefix or suffix.	Only applies if the Pattern behavior is <i>Add Prefix</i> or <i>Add Suffix</i> .
State	Indicates if the transform 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.

Click on the transform you want to configure (or click **New** to create a new transform, or click **Delete** to remove a transform).

Search and Zone Transformation Process

The search rules and zone transform process is applied after all [About Pre-Search Transforms](#), [About Call Policy](#) and [User Policy](#) have been applied.

The process is as follows:

1. The Expressway applies the search rules in priority order (all rules with a priority of 1 are processed first, then priority 2 and so on) to see if the given alias matches the rules criteria based on the **Source** of the query and the rule **Mode**.
2. If the match is successful, any associated zone transform (where the **Mode** is *Alias pattern match* and the **Pattern behavior** is *Replace* or *Strip*) is applied to the alias.
3. The search rule's **Target** zone or policy service is queried (with the revised alias if a zone transform has been applied) using the same protocol (SIP or H.323) as the incoming call request.



Note If there are many successful matches for multiple search rules at the same priority level, every applicable **Target** is queried.

- If the alias is found, the call is forwarded to that zone. If the alias is found by more than one zone, the call is forwarded to the zone that responds first.

- If the alias is not found using the native protocol, the query is repeated using the interworked protocol, depending on the [interworking mode](#).
 - If the search returns a new URI or alias (for example, due to an ENUM lookup, or the response from a policy service), the entire [Call Routing Process](#) starts again
4. If the alias is not found, the search rules with the next highest priority are applied (go back to step 1) until:
- The alias is found, or
 - All target zones and policy services associated with search rules that meet the specified criteria have been queried, or
 - A search rule with a successful match has an **On successful match** setting of *Stop searching*.



Note The difference between a successful match (where the alias matches the search rule criteria) and an alias being found (where a query sent to a target zone is successful). The *Stop searching* option provides better control over the network's signaling infrastructure. For example, if searches for a particular domain should always be routed to a specific zone this option lets you make the search process more efficient and stop the Expressway from searching any other zones unnecessarily.

Configuring Search Rules

The **Search rules** page (**Configuration > Dial plan > Search rules**) is used to configure how the Expressway routes incoming search requests to the appropriate target zones (including the Local Zone) or policy services.

The page lists all the currently configured search rules and lets you create, edit, delete, enable and disable rules. You can click on a column heading to sort the list, for example by **Target** or **Priority**. If you hover your mouse pointer over a search rule, the rule description (if one has been defined) appears as a tooltip.

You can also copy and then edit any existing search rule by clicking **Clone** in the **Actions** column.

Up to 2000 search rules can be configured. Priority 1 search rules are applied first, followed by all priority 2 search rules, and so on.

The configurable options are:

Field	Description	Usage tips
Rule name	A descriptive name for the search rule.	
Description	An optional free-form description of the search rule.	The description appears as a tooltip if you hover your mouse pointer over a rule in the list.

Field	Description	Usage tips
Priority	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. More than one rule can be assigned the same priority, in which case any matching target zones are queried simultaneously. The default is 100.	The default configuration means that the Local Zone is searched first for all aliases. If the alias is not found locally, all neighbor, traversal client and traversal server zones are searched, and if they cannot locate the alias the request is sent to any DNS and ENUM zones.
Protocol	The source protocol for which the rule applies. The options are <i>Any</i> , <i>H.323</i> or <i>SIP</i> .	
Traffic type	The source traffic type for which this rule applies. Options are: <i>Any</i> : The rule does not inspect the traffic type. <i>Standard</i> : The rule applies if the traffic is standards-based SIP. <i>Any Microsoft</i> : The rule applies if the traffic is Microsoft SIP or Microsoft SIP-SIMPLE. <i>Microsoft SIP</i> : The rule applies if the traffic is Microsoft SIP. <i>Microsoft IM and Presence</i> : The rule applies if the traffic is Microsoft SIP-SIMPLE.	This option helps you route different types of calls to the infrastructure most suited to processing them. For example, you could use two search rules to route Standard SIP towards a Unified CM neighbor zone and route Any Microsoft towards a Cisco Meeting Server neighbor zone.
Source	The sources of the requests for which this rule applies. <i>Any</i> : Locally registered devices, neighbor or traversal zones, and any non-registered devices. <i>All zones</i> : Locally registered devices plus neighbor or traversal zones. <i>Local Zone</i> : Locally registered devices only. <i>Named</i> : A specific source zone or subzone for which the rule applies.	Named sources creates the ability for search rules to be applied as dial plan policy for specific subzones and zones.
Source name	The specific source zone or subzone for which the rule applies. Choose from the Default Zone, Default Subzone or any other configured zone or subzone.	Only applies if the Source is set to <i>Named</i> .
Request must be authenticated	Specifies whether the search rule applies only to authenticated search requests.	This can be used in conjunction with the Expressway's Authentication Policy to limit the set of services available to unauthenticated devices.

Field	Description	Usage tips
Mode	<p>The method used to test if the alias applies to the search rule.</p> <p><i>Alias pattern match:</i> The alias must match the specified Pattern type and Pattern string.</p> <p><i>Any alias:</i> Any alias (providing it is not an IP address) is allowed.</p> <p><i>Any IP Address:</i> The alias must be an IP address.</p>	
Pattern type	<p>How the Pattern string must match the alias for the rule to be applied. Options are:</p> <p><i>Exact:</i> The entire string must exactly match the alias character for character.</p> <p><i>Prefix:</i> The string must appear at the beginning of the alias.</p> <p><i>Suffix:</i> The string must appear at the end of the alias.</p> <p><i>Regex:</i> Treats the string as a regular expression.</p>	<p>Applies only if the Mode is <i>Alias Pattern Match</i>.</p> <p>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).</p>
Pattern string	The pattern against which the alias is compared.	<p>Applies only if the Mode is <i>Alias Pattern Match</i>.</p> <p>The Expressway has a set of predefined pattern matching variables that can be used to match against certain configuration elements.</p>
Pattern behavior	<p>Determines whether the matched part of the alias is modified before being sent to the target zone or policy service</p> <p><i>Leave:</i> The alias is not modified.</p> <p><i>Strip:</i> The matching prefix or suffix is removed from the alias.</p> <p><i>Replace:</i> The matching part of the alias is substituted with the text in the Replace string.</p>	<p>Applies only if the Mode is <i>Alias Pattern Match</i>.</p> <p>If you want to transform the alias before applying search rules you must use About Pre-Search Transforms.</p>
Replace string	The string to substitute for the part of the alias that matches the pattern.	<p>Only applies if the Pattern behavior is <i>Replace</i>.</p> <p>You can use regular expressions.</p>

Field	Description	Usage tips
On successful match	Controls the ongoing search behavior if the alias matches the search rule. <i>Continue:</i> Continue applying the remaining search rules (in priority order) until the endpoint identified by the alias is found. <i>Stop:</i> Do not apply any more search rules, even if the endpoint identified by the alias is not found in the target zone.	If <i>Stop</i> is selected, any rules with the same priority level as this rule are still applied.
Target	The zone or policy service to query if the alias matches the search rule.	You can configure external Configuring Search Rules to Use an External Service to use as a target of search rules. This could be used, for example, to call out to an external service or application, such as a TelePresence Conductor. The service will return some CPL which could, for example, specify a new destination alias which would start the search process over again.
State	Indicates if the search 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.

Click on the rule you want to configure (or click **New** to create a new rule, or click **Delete** to remove a rule).

Useful tools to assist in configuring search rules

- You can test whether the Expressway can find an endpoint identified by a given alias, without actually placing a call to that endpoint, by using the [Locate](#) tool (**Maintenance > Tools > Locate**).
- 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**).

Example Searches and Transforms

You can use pre-search transforms and search rules separately or together. You can also define multiple search rules that use a combination of **Any alias** and **Alias pattern match** modes, and apply the same or different priorities to each rule. This will give you a great deal of flexibility in determining if and when a target zone is queried and whether any transforms are applied.

This section gives the following examples that demonstrate how you might use pre-search transforms and search rules to solve specific use cases in your deployment.

Filter Queries to a Zone Without Transforming

You can filter the search requests sent to a zone so that it is only queried for aliases that match certain criteria. For example, assume all endpoints in your regional sales office are registered to their local Cisco VCS with a suffix of **@sales.example.com**. In this situation, it makes sense for your Head Office Expressway to query the Sales Office VCS only when it receives a search request for an alias with a suffix of **@sales.example.com**. Sending any other search requests to this particular VCS would take up resources unnecessarily. It would also be wasteful of resources to send search requests for aliases that match this pattern to any other zone (there may be other lower priority search rules defined that would also apply to these aliases). In which case setting **On successful match** to *Stop* means that the Expressway will not apply any further (lower priority) search rules.

To achieve the example described above, on your Head Office Expressway create a zone to represent the Sales Office VCS, and from the **Create search rule** page (**Configuration > Dial plan > Search rules > New**) set up an associated search rule as follows:

Field	Value
Rule name	Regional sales office
Description	Calls to aliases with a suffix of @sales.example.com
Priority	100
Source	Any
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Suffix
Pattern string	@sales.example.com
Pattern behavior	Leave
On successful match	Stop
Target	Sales office
State	Enabled

Always Query a Zone with Original Alias (No Transforms)

To configure a zone so that it is always sent search requests using the original alias, from the **Create search rule** page (**Configuration > Dial plan > Search rules > New**), set up a search rule for that zone with a **Mode** of *Any alias*:

Field	Value
Rule name	Always query with original alias
Description	Send search requests using the original alias

Field	Value
Priority	100
Source	Any
Request must be authenticated	No
Mode	Any alias
On successful match	Continue
Target	Head office
State	Enabled

Query a Zone for a Transformed Alias



Note Any *alias* mode does not support alias transforms. If you want to always query a zone using a different alias to that received, you need to use a mode of *Alias pattern match* in combination with a regular expression.

You may want to configure your dial plan so that when a user dials an alias in the format **name@example.com** the Expressway queries the zone for **name@example.co.uk** instead.

To achieve this, from the **Create search rule** page (**Configuration > Dial plan > Search rules > New**) set up a search rule as follows:

Field	Value
Rule name	Transform to example.co.uk
Description	Transform example.com to example.co.uk
Priority	100
Source	Any
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Suffix
Pattern string	example.com
Pattern behavior	Replace
Replace string	example.co.uk
On successful match	Continue

Field	Value
Target zone	Head office
State	Enabled

Query a Zone for Original and Transformed Aliases

You may want to query a zone for the original alias at the same time as you query it for a transformed alias. To do this, configure one search rule with a **Mode** of *Any alias*, and a second search rule with a **Mode** of *Alias pattern match* along with details of the transform to be applied. Both searches must be given the same **Priority** level.

For example, you may want to query a neighbor zone for both a full URI and just the name (the URI with the domain removed). To achieve this, on your local Expressway from the **Create search rule** page (**Configuration** > **Dial plan** > **Search rules** > **New**) set up two search rules as follows:

Rule #1

Field	Value
Rule name	Overseas office - original alias
Description	Query overseas office with the original alias
Priority	100
Source	Any
Request must be authenticated	No
Mode	Any alias
On successful match	Continue
Target zone	Overseas office
State	Enabled

Rule #2

Field	Value
Rule name	Overseas office - strip domain
Description	Query overseas office with domain removed
Priority	100
Source	Any

Field	Value
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Suffix
Pattern string	@example.com
Pattern behavior	Strip
On successful match	Continue
Target zone	Overseas office
State	Enabled

Query a Zone for Two or More Transformed Aliases

Zones are queried in order of priority of the search rules configured against them.

It is possible to configure multiple search rules for the same zone each with, for example, the same **Priority** and an identical **Pattern string** to be matched, but with different replacement patterns. In this situation, the Expressway queries that zone for each of the new aliases simultaneously. (Any duplicate aliases produced by the transforms are removed prior to the search requests being sent out.) If any of the new aliases are found by that zone, the call is forwarded to the zone. It is then up to the controlling system to determine the alias to which the call will be forwarded.

For example, you may want to configure your dial plan so that when a user dials an alias in the format **name@example.com**, the Expressway queries the zone simultaneously for both **name@example.co.uk** and **name@example.net**.

To achieve this, from the **Create search rule** page (**Configuration > Dial plan > Search rules > New**) set up two search rules as follows:

Rule #1

Field	Value
Rule name	Transform to example.co.uk
Description	Transform example.com to example.co.uk
Priority	100
Source	Any
Request must be authenticated	No
Mode	Alias pattern match

Field	Value
Pattern type	Suffix
Pattern string	example.com
Pattern behavior	Replace
Replace string	example.co.uk
On successful match	Continue
Target zone	Head office
State	Enabled

Rule #2

Field	Value
Rule name	Transform to example.net
Description	Transform example.com to example.net
Priority	100
Source	Any
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Suffix
Pattern string	example.com
Pattern behavior	Replace
Replace string	example.net
On successful match	Continue
Target zone	Head office
State	Enabled

Stripping @domain for Dialing to H.323 Numbers

SIP endpoints can only make calls in the form of URIs - for example **name@domain**. If the caller does not specify a domain when placing the call, the SIP endpoint automatically appends its own domain to the number that is dialed. So if you dial **123** from a SIP endpoint, the search will be placed for **123@domain**. If the H.323

endpoint being dialed is registered as **123**, the Expressway will be unable to locate the alias **123@domain** and the call will fail.

If you have a deployment that includes both SIP and H.323 endpoints that register using a number, you will need to set up the following [Pre-Search Transform](#) and [Local Zone Search Rules](#). Together these will let users place calls from both SIP and H.323 endpoints to H.323 endpoints registered using their H.323 E.164 number only.

Pre-Search Transform

On the **Create transforms** page (**Configuration > Dial plan > Transforms > New**):

Field	Value
Priority	1
Description	Take any number-only dial string and append @domain
Pattern type	Regex
Pattern string	(\d+)
Pattern behavior	Replace
Replace string	\1@domain
State	Enabled

This pre-search transform takes any number-only dial string (such as **123**) and appends the domain used in endpoint AORs and URIs in your deployment. This ensures that calls made by SIP and H.323 endpoints result in the same URI.

Local Zone Search Rules

On the **Create search rule** page (**Configuration > Dial plan > Search rules > New**), create two new search rules as follows:

Rule #1

Field	Value
Rule name	Dialing H.323 numbers
Description	Transform aliases in format number@domain to number
Priority	50
Source	Any
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex

Field	Value
Pattern string	(\d+)\@domain
Pattern behavior	Replace
Replace string	\1
On successful match	Continue
Target zone	Local Zone
State	Enabled

Rule #2

Field	Value
Rule name	Dialing H.323 numbers
Description	Place calls to number@domain with no alias transform
Priority	60
Source	Any
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string	(\d+)\@domain
Pattern behavior	Leave
On successful match	Continue
Target zone	Local Zone
State	Enabled

These search rules ensure that both the E.164 number and full URI are searched for, so that endpoints can still be reached whether they have registered with an H.323 number (**123**) or a full URI (**123@domain**).

- The first search rule takes any aliases in the format **number@domain** and transforms them into the format **number**.
- To ensure that any endpoints that have actually registered with an alias in the format **number@domain** can also still be reached, the lower-priority second search rule places calls to **number@domain** without transforming the alias.

Transforms for Alphanumeric H.323 ID Dial Strings

This example builds on the [Stripping @domain for Dialing to H.323 Numbers](#) for dialing to H.323 numbers example. That example caters for number-only dial strings, however H.323 IDs do not have to be purely numeric; they can contain alphanumeric (letters and digits) characters.

This example follows the same model as the example mentioned above — a [Pre-Search Transform](#) and two [Local Zone Search Rules](#) to ensure that endpoints can be reached whether they have registered with an H.323 ID or a full URI — but uses a different regex (regular expression) that supports alphanumeric characters.

Pre-Search Transform

On the **Create transforms** page (**Configuration > Dial plan > Transforms > New**):

Field	Value
Priority	1
Description	Append @domain to any alphanumeric dial string
Pattern type	Regex
Pattern string	([^\@]*)
Pattern behavior	Replace
Replace string	\1@domain
State	Enabled

This pre-search transform takes any alphanumeric dial string (such as **123abc**) and appends the domain used in your deployment to ensure that calls made by SIP and H.323 endpoints result in the same URI.

Local Zone Search Rules

On the **Create search rule** page (**Configuration > Dial plan > Search rules > New**), create two new search rules as follows:

Rule #1

Field	Value
Rule name	Dialing H.323 strings
Description	Transform aliases in format string@domain to string
Priority	40
Source	Any
Request must be authenticated	No
Mode	Alias pattern match

Field	Value
Pattern type	Regex
Pattern string	(.+@domain
Pattern behavior	Replace
Replace string	\1
On successful match	Continue
Target zone	Local Zone
State	Enabled

Rule #2

Field	Value
Rule name	Dialing H.323 strings with domain
Description	Place calls to string@domain with no alias transform
Priority	50
Source	Any
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string	(.+@domain
Pattern behavior	Leave
On successful match	Continue
Target zone	Local Zone
State	Enabled

These search rules ensure that both the E.164 number and full URI are searched for, so that endpoints can still be reached whether they have registered with an H.323 ID (**123abc**) or a full URI (**123abc@domain**).

- The first search rule takes any aliases in the format **string@domain** and transforms them into the format **string**.
- To ensure that any endpoints that have actually registered with an alias in the format **string@domain** can also still be reached, the lower-priority second search rule places calls to **string@domain** without transforming the alias.

Allowing Calls to IP Addresses only if They Come From Known Zones

In addition to making calls to aliases, calls can be made to specified IP addresses. To pass on such calls to the appropriate target zones you must set up search rules with a **Mode** of *Any IP address*. To provide extra security you can set the rule's **Source** option to *All zones*. This means that the query is only sent to the target zone if it originated from any configured zone or the Local Zone.

To achieve the example described above, from the **Create search rule** page (**Configuration > Dial plan > Search rules > New**) set up a search rule as follows:

Field	Value
Rule name	IP addresses from known zones
Description	Allow calls to IP addresses only from a known zone
Priority	100
Source	All zones
Request must be authenticated	No
Mode	Any IP address
On successful match	Continue
Target zone	Overseas office
State	Enabled

Forward Microsoft SIP Calls to Cisco Meeting Server

If you are using Cisco Meeting Server to enable Microsoft users to meet in spaces, you could forward any incoming calls of this type towards your Meeting Server neighbor zone with a search rule like this:

Field	Value
Rule name	Route all to Meeting Server
Description	Send all inbound MS traffic to Meeting Server
Priority	100
Protocol	SIP
Traffic type	Any Microsoft
Source	Any
Request must be authenticated	No
Mode	Any alias

Field	Value
On successful match	Stop
Target	Cisco Meeting Server
State	Enabled

Direct 9-1-1 Calls for Kari's Law (with Expressway as Call Control and a PSTN Gateway)

This section provides recommendations for configuring a dial plan to support direct 9-1-1 emergency calling through Cisco Expressway. “Kari's Law”, mandated by the Federal Communications Commission, requires multi-line telephone systems (MLTS) to support **direct** 911 calls in the United States. That is, so the person making the emergency call does not also need to dial a prefix or other additional digits.

When Does Kari's Law Apply to Expressway?

Kari's Law deals with audio calls. This law applies to Expressway deployments **in the United States** in cases where all of the following conditions apply:

- Expressway is managing the call control and the endpoint making the emergency call is directly registered to the Expressway-C.
- A gateway is configured with Expressway that enables PSTN calling.
- The PSTN calling capabilities for your deployment include 911 emergency calls.
- The endpoint involved is capable of dialing a PSTN number and making a basic audio call.

Before You Begin

- You need Cisco Expressway version X12.5.7 or later.
- You should have knowledge of the North American Numbering Plan (NANP).
- From X12.5.7, the usual requirement to have at least one RMS license installed before a call can be placed does not apply to direct 911 calls.
- To minimize toll fraud risks, avoid using the “Any” wild card for the Source setting.
- The PSTN gateway also needs to be configured to route 911 calls without a prefix.
- For deployments that are geographically spread with the gateway in a different location from the endpoints, keep in mind the practical routing requirements for 911 calls and the possibility that callers may be connected to an emergency agent in a different place from their own location.

Configuring the Search Rules

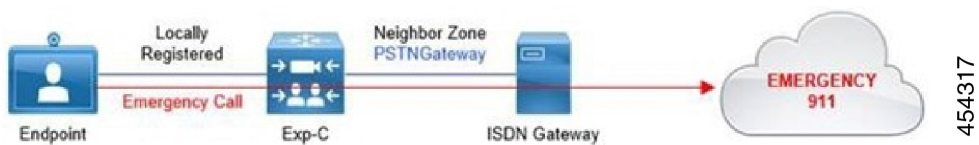
On the **Create search rule** page (**Configuration > Dial plan > Search rules > New**) create the necessary search rules. This section provides examples for these deployment types:

1. Standalone PSTN gateway (no redundancy).
2. Multiple PSTN gateways.

Example 1: Search Rules for a Standalone Gateway

These example rules assume the following:

- An ISDN gateway for PSTN calling is configured on Expressway as a neighbor zone (named “PSTNGateway”).
- 911 emergency calls are only allowed from SIP user agents or H.323 endpoints registered locally to the Expressway-C.



Example 1, Rule #1

Field	Value
Rule name	Emergency Call - 911
Description	Route the 911 emergency call via PSTNGateway
Priority	1
Protocol	Any
Source	Local Zone
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string	911 (911@%localdomains%)
Pattern behavior	Leave
On successful match	Stop

Example 2: Search Rules for Multiple Gateways

Field	Value
Target zone	PSTNGateway
State	Enable

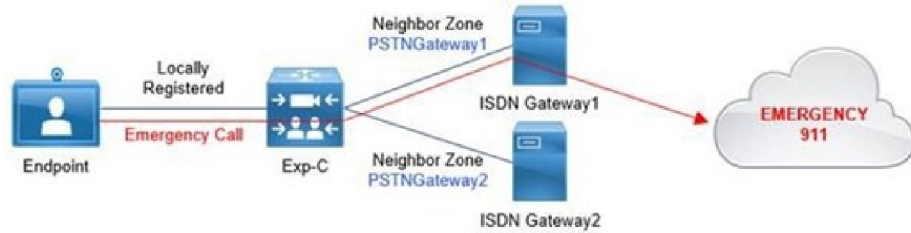
Example 1, Rule #2

Field	Value
Rule name	Emergency Call - 911 with Prefix 00
Description	Route the 911 emergency call via PSTNGateway
Priority	2
Protocol	Any
Source	Local Zone
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string	00(911 911@%localdomains%)
Pattern behavior	Replace
Replace string	\1
On successful match	Stop
Target zone	PSTNGateway
State	Enable

Example 2: Search Rules for Multiple Gateways

These example rules assume the following:

- Two ISDN gateways for PSTN calling, are available in the live network for redundancy.
- Each gateway is configured on Expressway as a neighbor zone (named “PSTNGateway1” and “PSTNGateway2”).
- 911 emergency calls are only allowed from SIP user agents or H.323 endpoints registered locally to the Expressway-C.



Here the rules specify *On successful match* = “Continue” for the primary gateway and *On successful match* = “Stop” for the .backup one.

Example 2, Rule #1

Field	Value
Rule name	Emergency Call - 911 via PSTNGateway1
Description	Route the 911 emergency call via PSTNGateway
Priority	1
Protocol	Any
Source	Local Zone
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string	911 (911@%localdomains%)
Pattern behavior	Leave
On successful match	Continue
Target zone	PSTNGateway1
State	Enable

Example 2, Rule #2

Field	Value
Rule name	Emergency Call - 911 via PSTNGateway2
Description	Route the 911 emergency call via PSTNGateway
Priority	2

Example 2: Search Rules for Multiple Gateways

Field	Value
Protocol	Any
Source	Local Zone
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string	911 (911@%localdomains%)
Pattern behavior	Leave
On successful match	Stop
Target zone	PSTNGateway2
State	Enable

Example 2, Rule #3

Field	Value
Rule name	Emergency Call - 911 with Prefix 00 via PSTNGateway1
Description	Route the 911 emergency call via PSTNGateway
Priority	3
Protocol	Any
Source	Local Zone
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string	00(911 911@%localdomains%)
Pattern behavior	Replace
Replace string	\1
On successful match	Continue
Target zone	PSTNGateway1
State	Enable

Example 2, Rule #4

Field	Value
Rule name	Emergency Call - 911 with Prefix 00 via PSTNGateway2
Description	Route the 911 emergency call via PSTNGateway
Priority	4
Protocol	Any
Source	Local Zone
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string	00(911 911@%localdomains%)
Pattern behavior	Replace
Replace string	\1
On successful match	Stop
Target zone	PSTNGateway2
State	Enable

Configuring Search Rules to Use an External Service

The configuration process to set up the Expressway to use an external policy service for search rules (dial plan) is broken down into the following steps:

- Configure the policy service to be used by search rules.
- Configure the relevant search rules to direct a search to the policy service.

Configuring a policy service to be used by search rules

Procedure

-
- Step 1** Go to **Configuration > Dial plan > Policy services**.
- Step 2** Click **New**.
- Step 3** Configure the server address and connection protocols in the same manner as for Call Policy.
- Step 4** Configure the fields on the **Create policy service** page as follows:

Field	Description	Usage tips
Name	The name of the policy service.	
Description	An optional free-form description of the policy service.	The description appears as a tooltip if you hover your mouse pointer over a policy service in the list.
Protocol	The protocol used to connect to the policy service. The default is <i>HTTPS</i> .	The Expressway automatically supports HTTP to HTTPS redirection when communicating with the policy service server.
Certificate verification mode	When connecting over HTTPS, this setting controls whether the certificate presented by the policy server is verified. If <i>On</i> , for the Expressway to connect to a policy server over HTTPS, the Expressway must have a root CA certificate loaded that authorizes that server's server certificate. Also the certificate's Subject Common Name or Subject Alternative Name must match one of the Server address fields below.	The Expressway's root CA certificates are loaded via (Maintenance > Security > Trusted CA certificate).
HTTPS certificate revocation list (CRL) checking	Enable this option if you want to protect certificate checking using CRLs and you have manually loaded CRL files, or you have enabled automatic CRL updates.	Go to Maintenance > Security > CRL management to configure how the Expressway uploads CRL files.
Server address 1 - 3	Enter the IP address or Fully Qualified Domain Name (FQDN) of the server hosting the service. You can specify a port by appending :<port> to the address.	If an FQDN is specified, ensure that the Expressway has an appropriate DNS configuration that allows the FQDN to be resolved. For resiliency, up to three server addresses can be supplied.
Path	Enter the URL of the service on the server.	
Status path	The Status path identifies the path from where the Expressway can obtain the status of the remote service. The default is <i>status</i> .	The policy server must supply return status information, see Policy Server Status and Resiliency .
Username	The username used by the Expressway to log in and query the service.	
Password	The password used by the Expressway to log in and query the service.	The maximum plaintext length is 30 characters (which is subsequently encrypted).

Field	Description	Usage tips
Default CPL	This is the fallback CPL used by the Expressway if the service is not available.	You can change it, for example, to redirect to an answer service or recorded message. For more information, see Default CPL for Policy Services .

Step 5 Click **Create policy service**.

Configuring a search rule to direct a search to the policy service

The Expressway will direct all searches that match the specified pattern to the policy service server.

Your search rules must be configured in such a way that they will result in a match for the initial alias, and then either not match or not return a reject for any aliases to which the policy server has routed the call.

Procedure

Step 1 Go to **Configuration > Dial plan > Search rules**.

Step 2 Click **New**.

Step 3 Configure the fields on the **Create search rule** page as appropriate for the searches you want to direct to the external policy server.

This example shows how to divert calls to aliases ending in .meet to the external policy server:

Field	Value
Rule name	A short name that describes the rule.
Description	A free-form description of the rule.
Priority	As required, for example 10.
Protocol	As required, for example <i>Any</i> .
Source	As required, for example <i>Any</i> .
Request must be authenticated	Configure this setting according to your authentication policy.
Mode	As required, for example <i>Alias pattern match</i> .
Pattern type	As required, for example <i>Regex</i> .
Pattern string	As required, for example <i>*\meet@example.com</i>
Pattern behavior	As required, for example <i>Leave</i> .

Field	Value
On successful match	As required. Note If Stop is selected the Expressway will not process any further search rules for the original alias, but will restart the full call processing sequence if any new aliases are returned in the CPL.
Target	Select the policy service that was created in the previous step.
State	<i>Enabled</i>

To divert all searches to the policy server you could set up 2 search rules that both target the policy service:

- The first search rule with a **Mode** of *Any alias*.
- The second search rule with a **Mode** of *Any IP address*.

Step 4 Click **Create search rule**.

About Call Policy

You can set up rules to control which calls are allowed, which calls are rejected, and which calls are to be redirected to a different destination. These rules are known as Call Policy (or Administrator Policy).

If Call Policy is enabled and has been configured, each time a call is made the Expressway will execute the policy in order to decide, based on the source and destination of the call, whether to:

- Proxy the call to its original destination.
- Redirect the call to a different destination or set of destinations.
- Reject the call.



Note When enabled, Call Policy is executed for all calls going through the Expressway.

You should:

- Use Call Policy to determine which callers can make or receive calls via the Expressway
- Use [Registration restriction policy](#) to determine which aliases can or cannot register with the Expressway

Configuring Call Policy

The **Call Policy configuration** page (**Configuration > Call Policy > Configuration**) is used to configure the Expressway's [About Call Policy](#) mode and to upload local policy files.

Call Policy Mode

The **Call Policy mode** controls from where the Expressway obtains its Call Policy configuration. The options are:

- *Local CPL*: Uses locally-defined Call Policy.
- *Policy service*: Uses an external policy service.
- *Off*: Call Policy is not in use.

Each of these options are described in more detail below:

Local CPL

The *Local CPL* option uses the Call Policy that is configured locally on the Expressway. If you choose *Local CPL* you must then either:

- [Configuring Call Policy Rules Using the Web Interface](#) through the **Call Policy rules** page (**Configuration** > **Call Policy** > **Rules**) or



Note This only lets you allow or reject specified calls.

- [Configuring Call Policy Using a CPL Script](#) that contains CPL script; however, due to the complexity of writing CPL scripts you are recommended to use an external policy service instead

Only one of these two methods can be used at any one time to specify Call Policy. If a CPL script has been uploaded, this takes precedence and you will not be able to use the **Call Policy rules** page; to use the page you must first delete the CPL script that has been uploaded.

If *Local CPL* is enabled but no policy is configured or uploaded, then a default policy is applied that allows all calls, regardless of source or destination.

The *Policy service* option is used if you want to refer all Call Policy decisions out to an external service. If you select this option an extra set of configuration fields appear so that you can specify the connection details of the external service. See [Configuring Call Policy to Use an External Service](#).

Configuring Call Policy Rules Using the Web Interface

The **Call Policy rules** page (**Configuration** > **Call Policy** > **Rules**) lists the web-configured (rather than uploaded via a CPL file) Call Policy rules currently in place and allows you to create, edit and delete rules. It provides a mechanism to set up basic Call Policy rules without having to write and upload a CPL script.

You cannot use the **Call Policy rules** page to configure Call Policy if a CPL file is already in place. If this is the case, on the **Call Policy configuration** page (**Configuration** > **Call Policy** > **Configuration**) you will have the option to **Delete uploaded file**. Doing so will delete the existing Call Policy that was put in place using a CPL script, and enable use of the **Call Policy rules** page for Call Policy configuration.



Each rule specifies the **Action** to take for calls from a particular **Source** to a particular **Destination** alias. If you have more than one rule, you can **Rearrange** the order of priority in which these rules are applied.

If you have not configured any call policy rules, the default policy is to allow all calls, regardless of source or destination.

Click on the rule you want to configure (or click **New** to create a new rule, or click **Delete** to remove a selected rule).

The configurable options for each rule are:

Field	Description	Usage tips
Source type	This field lets you choose from two types of call source: <i>Zone</i> or <i>From address</i> . Your choice affects the other fields that you use to configure the rule.	You can have a mixture of rules using different source types. Define and order them to implement your call policy or protect your conferencing resources from toll fraud.
Originating Zone	Visible for rules with Source type set to <i>Zone</i> . The dropdown shows all the zones configured on this Expressway, so you can choose the source for calls inspected by this rule. The rule inspects all calls originating from the zone that you choose.	
Rule applies to	Visible for rules with Source type set to <i>From address</i> . The field lets you choose whether the rule inspects calls from <i>Authenticated callers</i> or <i>Unauthenticated callers</i> . Authenticated callers are devices that are: <ul style="list-style-type: none"> • Locally registered and authenticated with the Expressway, or • Registered and authenticated to a neighbor which in turn has authenticated with the local Expressway 	See About Device Authentication for more information.
Source pattern	Visible for rules with Source type set to <i>From address</i> . The rule tries to match what you enter in this field to the source address that the calling endpoint uses to identify itself. If this field is blank, the policy rule applies to all incoming calls from the selected type of caller (Authenticated or Unauthenticated).	You can use a pattern for a more general rule or a single alias if you need to explicitly allow or reject a particular caller. This field supports regular expressions .
Destination pattern	Required for all rules. The rule tries to match what you enter in this field to the destination address from the incoming call.	You can use a pattern for a more general rule or a single alias if you need to explicitly allow or reject calls to a particular destination. This field supports regular expressions .

Field	Description	Usage tips
Action	<p>Defines what the rule does when a call it has inspected matches what you specified for the source and destination. You can choose <i>Allow</i> or <i>Reject</i>.</p> <p><i>Allow</i>: If the from address or originating zone matches the rule's source parameters, and if the call destination matches the rule's destination pattern, then the Expressway continues processing the call.</p> <p><i>Reject</i>: If the from address or originating zone matches the rule's source parameters, and if the call destination matches the rule's destination pattern, then the Expressway rejects the call.</p>	
Rearrange	<p>This field is only visible in the list of call policy rules (on the the Call Policy rules page).</p> <p>You can click the  and  icons to change the order of the rules, which changes their relative priority.</p>	<p>Each rule is compared with the details of the incoming call in top-down order until a rule matches the call.</p> <p>When a rule matches, the rule's action is applied to the call.</p>

Configuring Call Policy Using a CPL Script

You can use CPL scripts to configure advanced Call Policy. To do this, you must first create and save the CPL script as a text file, after which you upload it to the Expressway. However, due to the complexity of writing CPL scripts you are recommended to use an external [policy service](#) instead.

For information on the CPL syntax and commands that are supported by the Expressway, see the [CPL Reference](#) section.

Viewing existing CPL script

To view the Call Policy that is currently in place as an XML-based CPL script, go to the [Configuring Call Policy](#) page (**Configuration > Call Policy > Configuration**) and click **Show Call Policy file**.

- If Call Policy is configured to use a CPL script, this shows you the script that was uploaded.
- If Call Policy is configured by the **Call Policy rules** page, this shows you the CPL version of those call policy rules.
- If **Call Policy mode** is *On* but a policy has not been configured, this shows you a default CPL script that allows all calls.

You may want to view the file to take a backup copy of the Call Policy, or, if Call Policy has been configured using the Call Policy rules page you could take a copy of this CPL file to use as a starting point for a more advanced CPL script.

If Call Policy has been configured using the **Call Policy rules** page and you download the CPL file and then upload it back to the Expressway without editing it, the Expressway will recognize the file and automatically add each rule back into the **Call Policy rules** page.

About CPL XSD files

The CPL script must be in a format supported by the Expressway. The **Call Policy configuration** page allows you to download the XML schemas which are used to check scripts that are uploaded to the Expressway. You can use the XSD files to check in advance that your CPL script is valid. Two download options are available:

- **Show CPL XSD file:** Displays in your browser the XML schema used for the CPL script.
- **Show CPL Extensions XSD file:** Displays in your browser the XML schema used for additional CPL elements supported by the Expressway.

Uploading a CPL script

The Expressway polls for CPL script changes every 5 seconds, so the Expressway will almost immediately start using the updated CPL script. CPL scripts cannot be uploaded using the command line interface. To upload a new CPL file:

Procedure

-
- Step 1** Go to **Configuration > Call Policy > Configuration**.
 - Step 2** From the **Policy files** section, in the **Select the new Call Policy file** field, enter the file name or **Browse** to the CPL script you want upload.
 - Step 3** Click **Upload file**.
-

Deleting an existing CPL script

If a CPL script has already been uploaded, a **Delete uploaded file** button will be visible. Click it to delete the file.

Configuring Call Policy to Use an External Service

To configure Call Policy to refer all policy decisions out to an external service:

Procedure

-
- Step 1** Go to **Configuration > Call policy > Configuration**.
 - Step 2** Select a **Call Policy mode** of *Policy service*.
 - Step 3** Configure the fields that are presented as follows:

Field	Description	Usage tips
Protocol	The protocol used to connect to the policy service. The default is <i>HTTPS</i> .	The Expressway automatically supports HTTP to HTTPS redirection when communicating with the policy service server.

Field	Description	Usage tips
Certificate verification mode	When connecting over HTTPS, this setting controls whether the certificate presented by the policy server is verified. If <i>On</i> , for the Expressway to connect to a policy server over HTTPS, the Expressway must have a root CA certificate loaded that authorizes that server's server certificate. Also the certificate's Subject Common Name or Subject Alternative Name must match one of the Server address fields below.	The Expressway's root CA certificates are loaded via (Maintenance > Security > Trusted CA certificate).
HTTPS certificate revocation list (CRL) checking	Enable this option if you want to protect certificate checking using CRLs and you have manually loaded CRL files, or you have enabled automatic CRL updates.	Go to Maintenance > Security > CRL management to configure how the Expressway uploads CRL files.
Server address 1 - 3	Enter the IP address or Fully Qualified Domain Name (FQDN) of the server hosting the service. You can specify a port by appending <port> to the address.	If an FQDN is specified, ensure that the Expressway has an appropriate DNS configuration that allows the FQDN to be resolved. For resiliency, up to three server addresses can be supplied.
Path	Enter the URL of the service on the server.	
Status path	The Status path identifies the path from where the Expressway can obtain the status of the remote service. The default is <i>status</i> .	The policy server must supply return status information, see Policy Server Status and Resiliency .
Username	The username used by the Expressway to log in and query the service.	
Password	The password used by the Expressway to log in and query the service.	The maximum plaintext length is 30 characters (which is subsequently encrypted).
Default CPL	This is the fallback CPL used by the Expressway if the service is not available.	You can change it, for example, to redirect to an answer service or recorded message. For more information, see Default CPL for Policy Services .

Step 4 Configure the fields that are presented as follows:

Field	Description	Usage tips
Protocol	The protocol used to connect to the policy service. The default is <i>HTTPS</i> .	The Expressway automatically supports HTTP to HTTPS redirection when communicating with the policy service server.

Field	Description	Usage tips
Certificate verification mode	<p>When connecting over HTTPS, this setting controls whether the certificate presented by the policy server is verified.</p> <p>If <i>On</i>, for the Expressway to connect to a policy server over HTTPS, the Expressway must have a root CA certificate loaded that authorizes that server's server certificate. Also the certificate's Subject Common Name or Subject Alternative Name must match one of the Server address fields below.</p>	The Expressway's root CA certificates are loaded via (Maintenance > Security > Trusted CA certificate).
HTTPS certificate revocation list (CRL) checking	Enable this option if you want to protect certificate checking using CRLs and you have manually loaded CRL files, or you have enabled automatic CRL updates.	Go to Maintenance > Security > CRL management to configure how the Expressway uploads CRL files.
Server address 1 - 3	Enter the IP address or Fully Qualified Domain Name (FQDN) of the server hosting the service. You can specify a port by appending :<port> to the address.	<p>If an FQDN is specified, ensure that the Expressway has an appropriate DNS configuration that allows the FQDN to be resolved.</p> <p>For resiliency, up to three server addresses can be supplied.</p>
Path	Enter the URL of the service on the server.	
Status path	<p>The Status path identifies the path from where the Expressway can obtain the status of the remote service.</p> <p>The default is <i>status</i>.</p>	The policy server must supply return status information, see Policy Server Status and Resiliency .
Username	The username used by the Expressway to log in and query the service.	
Password	The password used by the Expressway to log in and query the service.	The maximum plaintext length is 30 characters (which is subsequently encrypted).
Default CPL	This is the fallback CPL used by the Expressway if the service is not available.	<p>You can change it, for example, to redirect to an answer service or recorded message.</p> <p>For more information, see Default CPL for Policy Services.</p>

Step 5 Click **Save**.

The Expressway should connect to the policy service server and start using the service for Call Policy decisions. Any connection problems will be reported on this page. Check the **Status** area at the bottom of the page and check for additional information messages against the **Server address** fields.

Supported Address Formats

The destination address that is entered using the caller's endpoint can take a number of different formats, and this affects the specific process that the Expressway follows when attempting to locate the destination endpoint. The address formats supported by the Expressway are:

- IP address, for example `10.44.10.1` or `3ffe:80ee:3706::10:35`
- H.323 ID, for example `john.smith` or `john.smith@example.com`



Note An H.323 ID can be in the form of a URI.

- E.164 alias, for example `441189876432` or `6432`
- URI, for example `john.smith@example.com`
- ENUM, for example `441189876432` or `6432`

Each of these address formats may require some configuration of the Expressway in order for them to be supported. These configuration requirements are described below.

Dialing by IP Address

Dialing by IP address is necessary when the destination endpoint is not registered with any system. See the [Dialing by IP Address](#) section for more information.

Dialing by H.323 ID or E.164 Alias

No special configuration is required to place a call using an H.323 ID or E.164 alias.

The Expressway follows the usual [Call Routing Process](#), applying any transforms and then searching the Local Zone and external zones for the alias, according to the search rules.



Note SIP endpoints always register using an AOR in the form of a URI. You are recommended to ensure that H.323 endpoints also register with an H.323 ID in the form of a URI to facilitate interworking.

Dialing by H.323 or SIP URI

When a user places a call using URI dialing, they will typically dial **name@example.com**.

If the destination endpoint is locally registered or registered to a neighbor system, no special configuration is required for the call to be placed. The Expressway follows the usual [Call Routing Process](#), applying any transforms and then searching the Local Zone and external zones for the alias, according to the search rules.

If the destination endpoint is not locally registered, URI dialing may make use of DNS to locate the destination endpoint. To support URI dialing via DNS, you must configure the Expressway with at least one DNS server and at least one DNS zone.

Full instructions on how to configure the Expressway to support URI dialing via DNS (both outbound and inbound) are given in the [About URI Dialing](#) section.

Dialing by ENUM

ENUM dialing allows an endpoint to be contacted by a caller dialing an E.164 number - a telephone number - even if that endpoint has registered using a different format of alias. The E.164 number is converted into a URI by the DNS system, and the rules for URI dialing are then followed to place the call.

The ENUM dialing facility allows you to retain the flexibility of URI dialing while having the simplicity of being called using just a number - particularly important if any of your callers are restricted to dialing using a numeric keypad.

To support ENUM dialing on the Expressway you must configure it with at least one DNS server and the appropriate ENUM zones.

Full instructions on how to configure the Expressway to support ENUM dialing (both outbound and inbound) are given in the [About ENUM Dialing](#) section.

Dialing by IP Address

Dialing by IP address is necessary when the destination endpoint is not registered with any system.

If the destination endpoint is registered, it may be possible to call it using its IP address but the call may not succeed if the endpoint is on a private network or behind a firewall. For this reason you are recommended to place calls to registered endpoints via other address formats, such as its AOR or H.323 ID. Similarly, callers outside of your network should not try to contact endpoints within your network using their IP addresses.

Calls to known IP addresses

Expressway considers an IP address to be “known” if the IP address is a locally registered endpoint or it falls within the IP address range of one of the subzone membership rules configured on the Expressway.

SIP user agents (and H.323 endpoints) register with either the Default Subzone or a customized Subzone based on membership rules, and interworking timing is different depending on the call flow.

The SIP IP dialing is always treated as UDP and the expected behavior on Expressway. Expressway servers is as follows:

1. Call from Default Subzone to Custom Subzone1 -> Proceed SIP-to-SIP native call — if the unit registered on Subzone1 is not registered as SIP UDP, experience delay until server performs interworking as native protocol fails.
2. Call from Subzone1 to Default Subzone -> Fallback SIP-to-H.323 Interworking Call immediately.
3. Call from Subzone1 to Subzone1 -> Proceed SIP-to-SIP native call — if the unit registered on Subzone1 is not registered as SIP UDP, experience delay until server performs interworking as native protocol fails.
4. Call from Subzone1 to Subzone2 -> Proceed SIP-to-SIP native call — if the unit registered on Subzone2 is not registered as SIP UDP, experience delay until server performs interworking as native protocol fails.
5. Call from Default Subzone to Default Subzone -> Fallback SIP-to-H.323 Interworking Call immediately.

Calls to unknown IP addresses

Although the Expressway supports dialing by IP address, it is sometimes undesirable for the Expressway to place a call directly to an IP address that is not local. Instead, you may want a neighbor to place the call on behalf of the Expressway, or not allow such calls at all. The **Calls to unknown IP addresses** setting (on the [Configuring Dial Plan Settings](#) page) configures how the Expressway handles calls to IP addresses which are not on its local network, or registered with it or one of its neighbors.

Expressway always attempts to place calls to known IP addresses (provided there is a search rule for *Any IP Address* against the Local Zone).

All other IP addresses are considered to be “unknown” and are handled by the Expressway according to the **Calls to Unknown IP addresses** setting:

- *Direct*: The Expressway attempts to place the call directly to the unknown IP address without querying any neighbors.
- *Indirect*: The Expressway forwards the search request to its neighbors in accordance with its normal search process, meaning any zones that are the target of search rules with an *Any IP Address* mode. If a match is found and the neighbor’s configuration allows it to connect a call to that IP address, the Expressway will pass the call to that neighbor for completion. This is the default setting.
- *Off*: The Expressway will not attempt to place the call, either directly or indirectly to any of its neighbors.

This setting applies to the call's destination address before any zone transforms, but after any pre-search transforms, Call Policy or User Policy rules are applied.



Note As well as controlling calls, this setting also determines the behavior of provisioning and presence messages to SIP devices, as these messages are routed to IP addresses.

Calling unregistered endpoints

An unregistered endpoint is any device that is not registered with an H.323 gatekeeper or SIP registrar. Although most calls are made between endpoints that are registered with such systems, it is sometimes necessary to place a call to an unregistered endpoint. There are two ways to call to an unregistered endpoint:

- Dialing its URI. The local Expressway must be configured to support URI dialing, and a DNS record must exist for that URI, which resolves to the unregistered endpoint's IP address.
- Dialing its IP address.

Recommended configuration for firewall traversal

When an Expressway-E is neighbored with an Expressway-C for firewall traversal, you should typically set **Calls to unknown IP addresses** to *Indirect* on the Expressway-C and *Direct* on the Expressway-E. When a caller inside the firewall attempts to place a call to an IP address outside the firewall, it will be routed as follows:

1. The call goes from the endpoint to the Expressway-C with which it is registered.
2. As the IP address being called is not registered to that Expressway, and its **Calls to unknown IP addresses** setting is *Indirect*, the Expressway does not place the call directly. Instead, it queries its neighbor

Expressway-E to see if that system is able to place the call on the Expressway-C's behalf. You must configure a search rule for *Any IP Address* against the traversal server zone.

3. The Expressway-E receives the call, and because its **Calls to unknown IP addresses** setting is *Direct*, it will make the call directly to the called IP address.

About URI Dialing

A URI address typically takes the form **name@example.com**, where **name** is the alias and **example.com** is the domain.

URI dialing can make use of DNS to enable endpoints registered with different systems to locate and call each other. Without DNS, the endpoints would need to be registered to the same or neighbored systems in order to locate each other.

URI Dialing Without DNS

Without the use of DNS, calls made by a locally registered endpoint using URI dialing will be placed only if the destination endpoint is also locally registered, or is accessible via a neighbor system. This is because these endpoints would be located using the [Search and Zone Transformation Process](#), rather than a DNS query.

If you want to use URI dialing from your network without the use of DNS, you would need to ensure that all the systems in your network were connected to each other by neighbor relationships - either directly or indirectly. This would ensure that any one system could locate an endpoint registered to itself or any another system, by searching for the endpoint's URI.

This does not scale well as the number of systems grows. It is also not particularly practical, as it means that endpoints within your network will not be able to dial endpoints registered to systems outside your network (for example when placing calls to another company) if there is not already a neighbor relationship between the two systems.

If a DNS zone and a DNS server have not been configured on the local Expressway, calls to endpoints that are not registered locally or to a neighbor system could still be placed if the local Expressway is neighbored (either directly or indirectly) with another Expressway that has been configured for URI dialing via DNS. In this case, any URI-dialed calls that are picked up by search rules that refer to that neighbor zone will go via that neighbor, which will perform the DNS lookup.

This configuration is useful if you want all URI dialing to be made via one particular system, such as an Expressway-E.

If you do not want to use DNS as part of URI dialing within your network, then no special configuration is required. Endpoints will register with an alias in the form of a URI, and when calls are placed to that URI the Expressway will query its local zone and neighbors for that URI.

If the Expressway does not have DNS configured and your network includes H.323 endpoints, then in order for these endpoints to be reachable using URI dialing:

- an appropriate transform should be written to convert URIs into the format used by the H.323 registrations. An example would be a deployment where H.323 endpoints register with an **alias**, and incoming calls are made to **alias@domain.com**. A local transform is then configured to strip the **@domain**, and the search is made locally for **alias**. See [Stripping @domain for Dialing to H.323 Numbers](#) for an example of how to do this.

SIP endpoints always register with an AOR in the form of a URI, so no special configuration is required.

URI Dialing With DNS

By using DNS as part of URI dialing, it is possible to find an endpoint even though it may be registered to an unknown system. The Expressway uses a DNS lookup to locate the domain in the URI address and then queries that domain for the alias. See the [URI Resolution Process Using DNS](#) section for more information.

URI dialing via DNS is enabled separately for outgoing and incoming calls.

Outgoing calls

To enable your Expressway to locate endpoints using URI dialing via DNS, you must:

- Configure at least one DNS zone and an associated search rule.
- Configure at least one DNS server.

This is described in the [URI Dialing via DNS for Outgoing Calls](#) section.

Incoming calls

To enable endpoints registered to your Expressway to receive calls from non-locally registered endpoints using URI dialing via DNS, you must:

- Ensure all endpoints are registered with an AOR (SIP) or H.323 ID in the form of a URI
- Configure appropriate DNS records, depending on the protocols and transport types you want to use

This is described in the [URI Dialing via DNS for Incoming Calls](#) section.

Firewall traversal calls

To configure your system so that you can place and receive calls using URI dialing through a firewall, see the [URI Dialing and Firewall Traversal](#) section.

URI Resolution Process Using DNS

When the Expressway attempts to locate a destination URI address using the DNS system, the general process is as follows:

H.323

1. The Expressway sends a query to its DNS server for an SRV record for the domain in the URI. (If more than one DNS server has been configured on the Expressway, the query will be sent to all servers at the same time, and all responses will be prioritized by the Expressway with only the most relevant SRV record being used.) If available, this SRV record returns information (such as the FQDN and listening port) about either the device itself or the authoritative H.323 gatekeeper for that domain.

- If the domain part of the URI address was resolved successfully using an H.323 Location SRV record (that is, for `_h323ls`) then the Expressway will send an A/AAAA record query for each name record returned. These will resolve to one or more IP addresses, and the Expressway then sends, in priority order, an LRQ for the full URI to those IP addresses.

- If the domain part of the URI address was resolved using an H.323 Call Signaling SRV record (that is, for `_h323cs`) then the Expressway will send an A/AAAA record query for each name record returned. These will resolve to one or more IP addresses, and the Expressway then routes the call, in priority order to the IP addresses returned in those records. (An exception to this is where the original dial string has a port specified - for example, `user@example.com:1719` - in which case the address returned is queried via an LRQ for the full URI address.)

2. If a relevant SRV record cannot be located:

- If the **Include address record** setting for the DNS zone being queried is set to *On*, the system will fall back to looking for an A or AAAA record for the domain in the URI. If such a record is found, the call will be routed to that IP address and the search will terminate.



Note If the A and AAAA records that are found at this domain are for systems other than those that support SIP or H.323, the Expressway will still forward the call to this zone, and the call will therefore fail. For this reason, you are recommended to use the default setting of *Off*.

- If the **Include address record** setting for the DNS zone being queried is set to *Off*, the Expressway will not query for A and AAAA records and instead will continue with the search, querying the remaining lower priority zones.

SIP

The Expressway supports the SIP resolution process as outlined in [RFC 3263](#). An example of how the Expressway implements this process is as follows:

1. The Expressway sends a NAPTR query for the domain in the URI. If available, the result set of this query describes a prioritized list of SRV records and transport protocols that should be used to contact that domain. If no NAPTR records are present in DNS for this domain name then the Expressway will use a default list of `_sips._tcp.<domain>`, `_sip._tcp.<domain>` and `_sip._udp.<domain>` for that domain as if they had been returned from the NAPTR query.
 - The Expressway sends SRV queries for each result returned from the NAPTR record lookup. A prioritized list of A/AAAA records returned is built.
 - The Expressway sends an A/AAAA record query for each name record returned by the SRV record lookup.

The above steps will result in a tree of IP addresses, port and transport protocols to be used to contact the target domain. The tree is sub-divided by NAPTR record priority and then by SRV record priority. When the tree of locations is used, the searching process will stop on the first location to return a response that indicates that the target destination has been contacted.

2. If the search process does not return a relevant SRV record:

- If the **Include address record** setting for the DNS zone being queried is set to *On*, the system will fall back to looking for an A or AAAA record for the domain in the URI. If such a record is found, the call will be routed to that IP address and the search will terminate.



Note If the A and AAAA records that are found at this domain are for systems other than those that support SIP or H.323, the Expressway will still forward the call to this zone, and the call will therefore fail. For this reason, you are recommended to use the default setting of *Off*.

- If the **Include address record** setting for the DNS zone being queried is set to *Off*, the Expressway will not query for A and AAAA records and instead will continue with the search, querying the remaining lower priority zones.

URI Dialing via DNS for Outgoing Calls

When a user places a call using URI dialing, they will typically dial an address in the form **name@example.com** from their endpoint. Below is the process that is followed when a URI address is dialed from an endpoint registered with your Expressway, or received as a query from a neighbor system:

1. The Expressway checks its [Configuring Search Rules](#) to see if any of them are configured with a **Mode** of either:
 - *Any alias*, or
 - *Alias pattern match* with a pattern that matches the URI address
2. The associated target zones are queried, in rule priority order, for the URI.
 - If one of the target zones is a DNS zone, the Expressway attempts to locate the endpoint through a DNS lookup. It does this by querying the DNS server configured on the Expressway for the location of the domain as per the [URI Resolution Process Using DNS](#). If the domain part of the URI address is resolved successfully the request is forwarded to those addresses.
 - If one of the target zones is a neighbor, traversal client or traversal server zones, those zones are queried for the URI. If that system supports URI dialing via DNS, it may route the call itself.

Adding and configuring DNS zones

To enable URI dialing via DNS, you must configure at least one DNS zone. To do this:

Procedure

- Step 1** Go to **Configuration > Zones > Zones**.
- Step 2** Click **New**. You are taken to the **Create zone** page.
- Step 3** Enter a **Name** for the zone and select a **Type** of *DNS*.
- Step 4** Configure the DNS zone settings as follows:

Field	Guidelines
Hop count	<p>When dialing by URI via DNS, the hop count used is that configured for the DNS zone associated with the search rule that matches the URI address (if this is lower than the hop count currently assigned to the call).</p> <p>If URI address isn't matched to a DNS zone, the query may be forwarded to a neighbor. In this case, the hop count used will be that configured for the neighbor zone (if this is lower than the hop count currently assigned to the call).</p>
H.323 and SIP modes	The H.323 and SIP sections allow you to filter calls to systems and endpoints located via this zone, based on whether the call is located using SIP or H.323 SRV lookups.
Include address record	<p>This setting 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.</p> <p>You are recommended to use the default setting of <i>Off</i>, meaning that the Expressway will not query for A and AAAA records, and instead will continue with the search, querying the remaining lower priority zones. This is because, unlike for NAPTR and SRV records, there is no guarantee that the A/AAAA records will point to a system capable of processing the relevant SIP or H.323 messages (LRQs, Setups, etc.) - the system may instead be a web server that processes http messages, or a mail server that processes mail messages. If this setting is <i>On</i>, when a system is found using A/AAAA lookup, the Expressway will send the signaling to that destination and will not continue the search process. If the system does not support SIP or H.323, the call will fail.</p>
Zone profile	For most deployments, this option should be left as <i>Default</i> .

Step 5 Click **Create zone**.

Configuring search rules for DNS zones

If you want your local Expressway to use DNS to locate endpoints outside your network, you must:

- [Configuring DNS Servers for ENUM and URI Dialing](#) used by the Expressway for DNS queries
- Create a DNS zone and set up associated search rules that use the **Pattern string** and **Pattern type** fields to define the aliases that will trigger a DNS query

For example, rules with:

- a **Pattern string** of `*@.*` and a **Pattern type** of *Regex* will query DNS for all aliases in the form of typical URI addresses.
- a **Pattern string** of `(?!.*@example.com$).*` and a **Pattern type** of *Regex* will query DNS for all aliases in the form of typical URI addresses except those for the domain *example.com*.

To set up further filters, configure extra search rules that target the same DNS zone. You do not need to create new DNS zones for each rule unless you want to filter based on the protocol (SIP or H.323) or use different hop counts.



Note You are not recommended to configure search rules with a **Mode** of *Any alias* for DNS zones. This will result in DNS always being queried for all aliases, including those that may be locally registered and those that are not in the form of URI addresses.

URI Dialing via DNS for Incoming Calls

DNS record types

The ability of the Expressway to receive incoming calls (and other messages, such as registrations) made using URI dialing via DNS relies on the presence of DNS records for each domain the Expressway is hosting.

These records can be of various types including:

- A records, which provide the IPv4 address of the Expressway
- AAAA records, which provide the IPv6 address of the Expressway
- Service (SRV) records, which specify the FQDN of the Expressway and the port on it to be queried for a particular protocol and transport type.
- NAPTR records, which specify SRV record and transport preferences for a SIP domain.

You must provide an SRV or NAPTR record for each combination of domain hosted and protocol and transport type enabled on the Expressway.

Incoming call process

When an incoming call has been placed using URI dialing via DNS, the Expressway will have been located by the calling system using one of the DNS record lookups described above. The Expressway will receive the request containing the dialed URI in the form `user@example.com`. This will appear as coming from the Default Zone. The Expressway will then search for the URI in accordance with its normal [Call Routing Process](#), applying any pre-search transforms, Call Policy and FindMe policy, then searching its Local Zone and other configured zones, in order of search rule priority.

SRV record format

The format of SRV records is defined by [RFC 2782](#) as:

`_Service._Proto.Name TTL Class SRV Priority Weight Port Target`

For the Expressway, these are as follows:

- **_Service** and **_Proto** will be different for H.323 and SIP, and will depend on the protocol and transport type being used.
- **Name** is the domain in the URI that the Expressway is hosting (such as **example.com**).
- **Port** is the IP port on the Expressway that has been configured to listen for that particular service and protocol combination.
- **Target** is the FQDN of the Expressway.

Configuring H.323 SRV Records

Annex O of [ITU Specification: H.323](#) defines the procedures for using DNS to locate gatekeepers and endpoints and for resolving H.323 URL aliases. It also defines parameters for use with the H.323 URL.

The Expressway supports the location, call and registration service types of SRV record as defined by this Annex.

Location service SRV records

Location records are required for gatekeepers that route calls to the Expressway. For each domain hosted by the Expressway, you should configure a location service SRV record as follows:

- **_Service** is **_h323ls**
- **_Proto** is **_udp**
- Port is the port number that has been configured from **Configuration > Protocols > H.323** as the **Registration UDP port**.

Call signaling SRV records

Call signaling SRV records (and A/AAAA records) are intended primarily for use by non-registered endpoints which cannot participate in a location transaction, exchanging LRQ and LCF. For each domain hosted by the Expressway, you should configure a call signaling SRV record as follows:

- **_Service** is **_h323cs**
- **_Proto** is **_tcp**
- Port is the port number that has been configured from **Configuration > Protocols > H.323 >** as the **Call signaling TCP port**.

Registration service SRV records

Registration records are used by devices attempting to register to the Expressway. For each domain hosted by the Expressway, you should configure a registration service SRV record as follows:

- **_Service** is **_h323rs**
- **_Proto** is **_udp**
- Port is the port number that has been configured from **Configuration > Protocols > H.323** as the **Registration UDP port**.

Configuring SIP SRV Records

[RFC 3263](#) describes the DNS procedures used to resolve a SIP URI into the IP address, port, and transport protocol of the next hop to contact.

If you want the Expressway to be contactable using SIP URI dialing, you should configure an SRV record for each SIP transport protocol enabled on the Expressway (that is, UDP, TCP or TLS) as follows:

- Valid combinations of **_Service** and **_Proto** are:
 - **_sips._tcp**

- **_sip._tcp**
 - **_sip._udp** (although not recommended)
- Port is the IP port number that has been configured from **Configuration > Protocols > SIP** as the port for that particular transport protocol.

_sip._udp is not recommended because SIP messages for video systems are too large to be carried on a packet based (rather than stream based) transport. UDP is often used for audio only devices. Also, UDP tends to be spammed more than TCP or TLS.

Example DNS Record Configuration

A company with the domain name **example.com** wants to enable incoming H.323 and SIP calls using URI addresses in the format **user@example.com**. The Expressway hosting the domain has the FQDN **expressway.example.com**.

Their DNS records would typically be as follows:

- SRV record for **_h323ls._udp.example.com** returns **expressway.example.com**
- SRV record for **_h323cs._tcp.example.com** returns **expressway.example.com**
- SRV record for **_h323rs._tcp.example.com** returns **expressway.example.com**
- NAPTR record for **example.com** returns
 - **_sip._tcp.example.com** and
 - **_sips._tcp.example.com**
- SRV record for **_sip._tcp.example.com** returns **expressway.example.com**
- SRV record for **_sips._tcp.example.com** returns **expressway.example.com**
- A record for **expressway.example.com** returns the IPv4 address of the Expressway.
- AAAA record for **expressway.example.com** returns the IPv6 address of the Expressway.

How you add the DNS records depends on the type of DNS server you are using. Instructions for setting up two common DNS servers are given in the DNS configuration section.

For locally registered H.323 endpoints to be reached using URI dialing, either:

- The H.323 endpoints should register with the Expressway using an address in the format of a URI
- An appropriate transform should be written to convert URIs into the format used by the H.323 registrations. An example would be a deployment where H.323 endpoints register with an alias, and incoming calls are made to **alias@domain.com**. A local transform is then configured to strip the **@domain**, and the search is made locally for alias. See [Stripping @domain for Dialing to H.323 Numbers](#) for an example of how to do this.

SIP endpoints always register with an AOR in the form of a URI, so no special configuration is required.

Several mechanisms could have been used to locate the Expressway. You may want to enable calls placed to **user@<IP_address>** to be routed to an existing registration for **user@example.com**. In this case you would configure a [About Pre-Search Transforms](#) that would strip the **IP_address** suffix from the incoming URI and replace it with the suffix of **example.com**.

URI Dialing and Firewall Traversal

If URI dialing via DNS is being used in conjunction with firewall traversal, DNS zones should be configured on the Expressway-E and any Expressways on the public network only. Expressways behind the firewall should not have any DNS zones configured. This will ensure that any outgoing URI calls made by endpoints registered with the Expressway will be routed through the Expressway-E.

In addition, the DNS records for incoming calls should be configured with the address of the Expressway-E as the authoritative proxy for the enterprise (see the DNS Configuration Examples section for more information). This ensures that incoming calls placed using URI dialing enter the enterprise through the Expressway-E, allowing successful traversal of the firewall.

About ENUM Dialing

ENUM dialing allows an endpoint to be contacted by a caller dialing an E.164 number - a telephone number - even if that endpoint has registered using a different format of alias.

Using ENUM dialing, when an E.164 number is dialed it is converted into a URI using information stored in DNS. The Expressway then attempts to find the endpoint based on the URI that has been returned.

The ENUM dialing facility allows you to retain the flexibility of URI dialing while having the simplicity of being called using just a number - particularly important if any of your callers are restricted to dialing using a numeric keypad.

The Expressway supports outward ENUM dialing by allowing you to configure ENUM zones on the Expressway. When an ENUM zone is queried, this triggers the Expressway to transform the E.164 number that was dialed into an ENUM domain which is then queried for using DNS.



Note

ENUM dialing relies on the presence of relevant DNS NAPTR records for the ENUM domain being queried. These are the responsibility of the administrator of that domain.

ENUM Dialing Process

When the Expressway attempts to locate a destination endpoint using ENUM, the general process is as follows:

1. The user dials the E.164 number from their endpoint.
2. The Expressway converts the E.164 number into an ENUM domain as follows:
 - a. The digits are reversed and separated by a dot.
 - b. The name of the domain that is hosting the NAPTR records for that E.164 number is added as a suffix.
3. DNS is then queried for the resulting ENUM domain.
4. If a NAPTR record exists for that ENUM domain, this will advise how the number should be converted into one (or possibly more) H.323/SIP URIs.
5. The Expressway begins the search again, this time for the converted URI as per the [URI Dialing via DNS for Outgoing Calls](#).



Note This is considered to be a completely new search, and so pre-search transforms and Call Policy will therefore apply.

Enabling ENUM Dialing

ENUM dialing is enabled separately for incoming and outgoing calls.

Outgoing calls

To allow outgoing calls to endpoints using ENUM, you must:

- Configure at least one ENUM zone, and
- Configure at least one DNS Server

This is described in the [ENUM Dialing for Outgoing Calls](#) section.

Incoming calls

To enable endpoints in your enterprise to receive incoming calls from other endpoints via ENUM dialing, you must configure a DNS NAPTR record mapping your endpoints' E.164 numbers to their SIP/H.323 URIs. See the [ENUM dialing for Incoming Calls](#) section for instructions on how to do this.



Note If an ENUM zone and a DNS server have not been configured on the local Expressway, calls made using ENUM dialing could still be placed if the local Expressway is neighbored with another Expressway that has been appropriately configured for ENUM dialing. Any ENUM dialed calls will go via the neighbor. This configuration is useful if you want all ENUM dialing from your enterprise to be configured on one particular system.

ENUM Dialing for Outgoing Calls

For a local endpoint to be able to dial another endpoint using ENUM via your Expressway, the following conditions must be met:

- There must be a NAPTR record available in DNS that maps the called endpoint's E.164 number to its URI. It is the responsibility of the administrator of the enterprise to which the called endpoint belongs to provide this record, and they will only make it available if they want the endpoints in their enterprise to be contactable via ENUM dialing.
- You must [Configure Zones and Search Rules for ENUM Dialing](#) on your local Expressway. This ENUM zone must have a DNS Suffix that is the same as the domain where the NAPTR record for the called endpoint is held.
- You must configure your local Expressway with the address of at least one [Configure DNS Servers for ENUM and URI Dialing](#) that it can query for the NAPTR record (and if necessary any resulting URI).

After the ENUM process has returned one or more URIs, a new search will begin for each of these URIs in accordance with the [URI Dialing via DNS for Outgoing Calls](#). If the URIs belong to locally registered endpoints, no further configuration is required. However, if one or more of the URIs are not locally registered, you may also need to configure a DNS zone if they are to be located using a DNS lookup.

Calling process

The Expressway follows this process when searching for an ENUM (E.164) number:

1. The Expressway initiates a search for the received E.164 number as it was dialed. It follows the usual [Call Routing Process](#).
2. After applying any pre-search transforms, the Expressway checks its [Configuring Search Rules](#) to see if any of them are configured with a **Mode** of either:
 - *Any alias*, or
 - *Alias pattern match* with a pattern that matches the E.164 number
3. The target zones associated with any matching search rules are queried in rule priority order.
 - If a target zone is a neighbor zone, the neighbor is queried for the E.164 number. If the neighbor supports ENUM dialing, it may route the call itself.
 - If a target zone is an ENUM zone, the Expressway attempts to locate the endpoint through ENUM. As and when each ENUM zone configured on the Expressway is queried, the E.164 number is transformed into an ENUM domain as follows:
 - a. The digits are reversed and separated by a dot.
 - b. The **DNS suffix** configured for that ENUM zone is appended.
4. DNS is then queried for the resulting ENUM domain.
5. If the DNS server finds at that ENUM domain a NAPTR record that matches the transformed E.164 number (that is, after it has been reversed and separated by a dot), it returns the associated URI to the Expressway.
6. The Expressway then initiates a new search for that URI (maintaining the existing hop count). The Expressway starts at the beginning of the search process (applying any pre-search transforms, then searching local and external zones in priority order). From this point, as it is now searching for a SIP/H.323 URI, the process for [About URI Dialing](#) is followed.

In this example, we want to call Fred at Example Corp. Fred's endpoint is actually registered with the URI **fred@example.com**, but to make it easier to contact him his system administrator has configured a DNS NAPTR record mapping this alias to his E.164 number: **+44123456789**.

We know that the NAPTR record for **example.com** uses the DNS domain of **e164.arpa**.

1. We create an ENUM zone on our local Expressway with a **DNS suffix** of **e164.arpa**.
2. We configure a search rule with a **Pattern match mode** of *Any alias*, and set the **Target** to the ENUM zone. This means that ENUM will always be queried regardless of the format of the alias being searched for.
3. We dial **44123456789** from our endpoint.

4. The Expressway initiates a search for a registration of **44123456789** and the search rule of *Any alias* means the ENUM zone is queried.



Note Other higher priority searches could potentially match the number first.

5. Because the zone being queried is an ENUM zone, the Expressway is automatically triggered to transform the number into an ENUM domain as follows:
 - a. The digits are reversed and separated by a dot: **9.8.7.6.5.4.3.2.1.4.4**
 - b. The **DNS suffix** configured for this ENUM zone, **e164.arpa**, is appended. This results in a transformed domain of **9.8.7.6.5.4.3.2.1.4.4.e164.arpa**.
6. DNS is then queried for that ENUM domain.
7. The DNS server finds the domain and returns the information in the associated NAPTR record. This tells the Expressway that the E.164 number we have dialed is mapped to the SIP URI of **fred@example.com**.
8. The Expressway then starts another search, this time for **fred@example.com**. From this point the process for URI dialing is followed, and results in the call being forwarded to Fred's endpoint.

Configuring Zones and Search Rules for ENUM Dialing

To support ENUM dialing, you must configure an ENUM zone and related search rules for each ENUM service used by remote endpoints.

Adding and configuring ENUM zones



-
- Note**
- Any number of ENUM zones may be configured on the Expressway. You should configure at least one ENUM zone for each DNS suffix that your endpoints may use.
 - Normal search rule pattern matching and prioritization rules apply to ENUM zones.
 - You must also [Configuring DNS Servers for ENUM and URI Dialing](#) to be used when searching for NAPTR records.
-

To set up an ENUM zone:

Procedure

- Step 1** Go to **Configuration > Zones > Zones**.
- Step 2** Click **New**. You are taken to the **Create zone** page.
- Step 3** Enter a **Name** for the zone and select a **Type** of *ENUM*.
- Step 4** Configure the ENUM zone settings as follows:

Field	Guidelines
Hop count	The Configuring Hop Counts specified for an ENUM zone is applied in the same manner as hop counts for other zone types. The currently applicable hop count is maintained when the Expressway initiates a new search process for the alias returned by the DNS lookup.
DNS suffix	The suffix to append to a transformed E.164 number to create an ENUM host name. It represents the DNS zone (in the domain name space) to be queried for a NAPTR record.
H.323 mode	Controls if H.323 records are looked up for this zone.
SIP mode	Controls if SIP records are looked up for this zone.

Step 5 Click **Create zone**.

Configuring search rules for ENUM zones

If you want locally registered endpoints to be able to make ENUM calls via the Expressway, then at a minimum you should configure an ENUM zone and a related search rule with:

- A **DNS suffix** of **e164.arpa** (the domain specified by the ENUM standard).
- A related search rule with a **Mode** of *Any alias*.

This results in DNS always being queried for all types of aliases, not just ENUMs. It also means that ENUM dialing will only be successful if the enterprise being dialed uses the **e164.arpa** domain. To ensure successful ENUM dialing, you must configure an ENUM zone for each domain that holds NAPTR records for endpoints that callers in your enterprise might want to dial.

You can then set up search rules that filter the queries sent to each ENUM zone as follows:

- Use a **Mode** of *Alias pattern match*
- Use the **Pattern string** and **Pattern type** fields to define the aliases for each domain that will trigger an ENUM lookup

For example, you want to enable ENUM dialing from your network to a remote office in the UK where the endpoints' E.164 numbers start with **44**. You would configure an ENUM zone on your Expressway, and then an associated search rule with:

- **Mode** of *Alias pattern match*
- **Pattern string** of **44**
- **Pattern type** of *Prefix*

This results in an ENUM query being sent to that zone only when someone dials a number starting with **44**.

Configuring transforms for ENUM zones

You can configure transforms for ENUM zones in the same way as any other zones (see the [Search and Zone Transformation Process](#) section for full information).

Any ENUM zone transforms are applied before the number is converted to an ENUM domain.

For example, you want to enable ENUM dialing from your network to endpoints at a remote site using a prefix of 8 followed by the last 4 digits of the remote endpoints' E.164 number. You would configure an ENUM zone on your Expressway and then an associated search rule with:

- **Mode** of *Alias pattern match*
- **Pattern string** of `8(d{4})`
- **Pattern type** of *Regex*
- **Pattern behavior** of *Replace*
- **Replace string** of `44123123(1)`

With this configuration, it is the resulting string (`44123123xxxx`) that is converted into an ENUM domain and queried for via DNS.

To verify you have configured your outward ENUM dialing correctly, use the [Locate tool](#) (**Maintenance > Tools > Locate**) to try to resolve an E.164 alias.

ENUM dialing for Incoming Calls

For your locally registered endpoints to be reached using ENUM dialing, you must configure a DNS NAPTR record that maps your endpoints' E.164 numbers to their URIs. This record must be located at an appropriate DNS domain where it can be found by any systems attempting to reach you by using ENUM dialing.

About DNS domains for ENUM

ENUM relies on the presence of NAPTR records to provide the mapping between E.164 numbers and their URIs.

[RFC 3761](#), which is part of a suite of documents that define the ENUM standard, specifies that the domain for ENUM - where the NAPTR records should be located for public ENUM deployments - is **e164.arpa**. However, use of this domain requires that your E.164 numbers are assigned by an appropriate national regulatory body. Not all countries are yet participating in ENUM, so you may want to use an alternative domain for your NAPTR records. This domain could reside within your corporate network (for internal use of ENUM) or it could use a public ENUM database such as <http://www.e164.org>.

Configuring DNS NAPTR records

ENUM relies on the presence of NAPTR records, as defined by [RFC 2915](#). These are used to obtain an H.323 or SIP URI from an E.164 number.

The record format that the Expressway supports is:

order preference flag service regex replacement

where,

- **order** and **preference** determine the order in which NAPTR records are processed. The record with the lowest order is processed first, with those with the lowest preference being processed first in the case of matching order.
- **flag** determines the interpretation of the other fields in this record. Only the value **u** (indicating that this is a terminal rule) is currently supported, and this is mandatory.

- **service** states whether this record is intended to describe E.164 to URI conversion for H.323 or for SIP. Its value must be either **E2U+h323** or **E2U+SIP**.
- **regex** is a regular expression that describes the conversion from the given E.164 number to an H.323 or SIP URI.
- **replacement** is not currently used by the Expressway and should be set to . (the full stop character).

Non-terminal rules in ENUM are not currently supported by the Expressway. For more information on these, see section 2.4.1 of [RFC 3761](#).

For example, the record:

```
IN NAPTR 10 100 "u" "E2U+h323" "!^(.*)$!h323:\1@example.com!"
```

would be interpreted as follows:

- **10** is the **order**
- **100** is the **preference**
- **u** is the **flag**
- **E2U+h323** states that this record is for an H.323 URI
- **!^(.*)\$!h323:\1@example.com!** describes the conversion:
 - **!** is a field separator
 - The first field represents the string to be converted. In this example, **^(.*)\$** represents the entire E.164 number
 - The second field represents the H.323 URI that will be generated. In this example, **h323:\1@example.com** states that the E.164 number will be concatenated with **@example.com**. For example, **1234** will be mapped to **1234@example.com**.
- Shows that the replacement field has not been used.

Configuring DNS Servers for ENUM and URI Dialing

DNS servers are required to support ENUM and URI dialing:

- **ENUM dialing**: To query for NAPTR records that map E.164 numbers to URIs
- **URI dialing**: To look up endpoints that are not locally registered or cannot be accessed via neighbor systems

To configure the DNS servers used by the Expressway for DNS queries:

Procedure

- Step 1** Go to the **DNS** page (**System > DNS**).

- Step 2** Enter in the **Address 1** to **Address 5** fields the IP addresses of up to 5 DNS servers that the Expressway will query when attempting to locate a domain. These fields must use an IP address, not a FQDN.
-

Configuring Call Routing and Signaling

The **Call routing** page (**Configuration** > **Call routing**) is used to configure the Expressway's call routing and signaling functionality.

Call Signaling Optimization

Calls are made up of two components - signaling and media. For traversal calls, the Expressway always handles both the media and the signaling. For non-traversal calls, the Expressway does not handle the media, and may or may not need to handle the signaling.

The **Call signaling optimization** setting specifies whether the Expressway removes itself, where it can, from the call signaling path after the call has been set up. The options for this setting are:

- *Off*: The Expressway always handles the call signaling.
 - The call consumes either an RMS Call license or a Registered Call license on the Expressway.
- *On*: The Expressway handles the call signaling when the call is one of:
 - A traversal call
 - An H.323 call that has been modified by Call Policy or FindMe such that:
 - The call resolves to more than one alias
 - The source alias of the call has been modified to display the associated FindMe ID
 - The FindMe has a “no answer” or “busy” device configured
 - One of the endpoints in the call is locally registered
 - A SIP call where the incoming transport protocol (UDP, TCP, TLS) is different from the outgoing protocol

In all other cases the Expressway removes itself from the call signaling path after the call has been set up. The Expressway does not consume a call license for any such calls, and the call signaling path is simplified. This setting is useful in a [hierarchical dial plan](#), when used on the directory Expressway. In such deployments the directory Expressway is used to look up and locate endpoints and it does not have any endpoints registered directly to it.

Call Loop Detection Mode

Your dial plan or that of networks to which you are neighbored may be configured in such a way that there are potential signaling loops. An example of this is a [structured dial plan](#), where all systems are neighbored together in a mesh. In such a configuration, if the [Configuring Hop Counts](#) are set too high, a single search

request may be sent repeatedly around the network until the hop count reaches 0, consuming resources unnecessarily.

The Expressway can be configured to detect search loops within your network and terminate such searches through the **Call loop detection mode** setting, thus saving network resources. The options for this setting are:

- *On*: The Expressway will fail any branch of a search that contains a loop, recording it as a level 2 “loop detected” event. Two searches are considered to be a loop if they meet all of the following criteria:
 - Have same call tag
 - Are for the same destination alias
 - Use the same protocol
 - Originate from the same zone
- *Off*: The Expressway will not detect and fail search loops. You are recommended to use this setting only in advanced deployments.

Identifying Calls

Each call that passes through the Expressway is assigned a Call ID and a Call Serial Number. Calls also have a Call Tag assigned if one does not already exist.

Call ID

The Expressway assigns each call currently in progress a different Call ID. The Call ID numbers start at 1 and go up to the maximum number of calls allowed on that system.

Each time a call is made, the Expressway will assign that call the lowest available Call ID number. For example, if there is already a call in progress with a Call ID of 1, the next call will be assigned a Call ID of 2. If Call 1 is then disconnected, the third call to be made will be assigned a Call ID of 1.

The Call ID is not therefore a unique identifier: while no two calls in progress at the same time will have the same Call ID, the same Call ID will be assigned to more than one call over time.



Note The Expressway web interface does not show the Call ID.

Call Serial Number

The Expressway assigns a unique Call Serial Number to every call passing through it. No two calls on an Expressway will ever have the same Call Serial Number. A single call passing between two or more Expressways will be identified by a different Call Serial Number on each system.

Call Tag

Call Tags are used to track calls passing through a number of Expressways. When the Expressway receives a call, it checks to see if there is a Call Tag already assigned to it. If so, the Expressway will use the existing Call Tag; if not, it will assign a new Call Tag to the call. This Call Tag is then included in the call’s details when the call is forwarded on. A single call passing between two or more Expressways will be assigned a

different Call Serial Number each time it arrives at an Expressway (including one it has already passed through) but can be identified as the same call by use of the Call Tag. This is particularly useful if you are using a [remote syslog server](#) to collate events across a number of Expressways in your network.

The Call Tag also helps identify loops in your network - it is used as part of the automatic [Configuring Call Routing and Signaling](#) feature, and you can also search the Event Log for all events relating to a single call tag. Loops occur when a query is sent to a neighbor zone and passes through one or more systems before being routed back to the original Expressway. In this situation the outgoing and incoming query will have different Call Serial Numbers and may even be for different destination aliases (depending on whether any transforms were applied). However, the call will still have the same Call Tag.



Note If a call passes through a system that is not an Expressway or TelePresence Conductor then the Call Tag information will be lost.

Identifying Calls in the CLI

To control a call using the CLI, you must reference the call using either its Call ID or Call Serial Number. These can be obtained using the command:

xStatus Calls

This returns details of each call currently in progress in order of their Call ID. The second line of each entry lists the Call Serial Number, and the third lists the Call Tag.

Disconnecting Calls

Disconnecting a call using the web interface



Note If your Expressway is part of a cluster you have to be logged into the peer through which the call is associated to be able to disconnect the call.

To disconnect one or more existing calls using the web interface:

Procedure

- Step 1** Go to the **Calls** page (**Status > Calls**).
 - Step 2** If you want to confirm the details of the call, including the Call Serial Number and Call Tag, click **View**. Click the back button on your browser to return to the **Calls** page.
 - Step 3** Select the box next to the calls you want to terminate and click **Disconnect**.
-

Disconnecting a call using the CLI

To disconnect an existing call using the CLI, you must first obtain either the call ID number or the call serial number (see [Identifying Calls](#)). Then use either one of the following commands as appropriate:

- **xCommand DisconnectCall Call: <ID number>**
- **xCommand DisconnectCall CallSerialNumber: <serial number>**

While it is quicker to use the call ID number to reference the call to be disconnected, there is a risk that in the meantime the call has already been disconnected and the call ID assigned to a new call. For this reason, the Expressway also allows you to reference the call using the longer but unique call serial number.



Note When disconnecting a call, only the call with that Call Serial Number is disconnected. Other calls with the same Call Tag but a different Call Serial Number may not be affected.

Limitations when disconnecting SIP calls

Call disconnection works differently for H.323 and SIP calls due to differences in the way the protocols work. For H.323 calls, and interworked calls, the **Disconnect** command actually disconnects the call.

For SIP calls, the **Disconnect** command causes the Expressway to release all resources used for the call; the call will appear as disconnected on the Expressway. However, endpoints will still consider themselves to be in the call. SIP calls are peer-to-peer, and as the Expressway is a SIP proxy it has no authority over the endpoints. Releasing the resources on the Expressway means that the next time there is any signaling from the endpoint to the Expressway, the Expressway will respond with a “481 Call/Transaction Does Not Exist” causing the endpoint to clear the call.



Note Endpoints that support SIP session timers (see [RFC 4028](#)) have a call refresh timer which allows them to detect a hung call (signaling lost between endpoints). The endpoints will release their resources after the next session-timer message exchange.
