



How to Connect the Expressway Cluster to Other Systems

This chapter explains the following:

- [Neighboring Between Expressway Clusters, on page 1](#)
- [Configure Endpoints to Work With a Cluster, on page 1](#)
- [Add the Expressway to Cisco TMS, on page 5](#)

Neighboring Between Expressway Clusters

You can neighbor your local Expressway cluster to a remote cluster. The remote cluster might be a neighbor, traversal client, or traversal server to the local system. When a call is received on the local Expressway and is passed via the relevant zone to the remote cluster, it gets routed to whichever peer in that neighbor cluster has the lowest resource usage (peers in maintenance mode are not considered). That peer then forwards the call to one of the following:

- A locally registered endpoint, if the endpoint is registered to that peer
- A peer, if the endpoint is registered to another peer in the cluster
- An external zone, if the endpoint is located elsewhere

Configuration instructions are provided in the *Expressway Administrator Guide*.

Configure Endpoints to Work With a Cluster

When configuring endpoints it's desirable for them to know about all the Expressway peers in a cluster. So that at initial registration or later, if endpoints lose connection to their Expressway peer, they can register with another peer in the cluster. This section lists the available configuration methods (in preferred order) for SIP endpoints and H.323 endpoints respectively.

For more details about DNS SRV and round-robin DNS, see the URI dialing section in the *Expressway Administrator Guide* and [Cluster Name and DNS SRV Records](#).



Note SIP and H.323 endpoints behave differently.

SIP Endpoints

The options are listed in preference order for providing resilience of connectivity of endpoints to a cluster of Expressways where one or more Expressway cluster peers become inaccessible. The choice of option will depend on what functionality the endpoint you are using supports.

Option 1 – SIP Outbound (Preferred)



Important For endpoints running Cisco Collaboration Endpoint software, this option is not supported from version CE8.0.

SIP outbound allows an endpoint to be configured to register to two or more Expressway peers simultaneously. The benefit of this is that if the connection between one peer and the endpoint breaks, a connection from the endpoint to the other peer remains. With the endpoint registering to both peers simultaneously, there is no break in service while the endpoint realizes that its registration has failed, before it registers to a different peer. Thus, at no time is the endpoint unreachable.

Configuration of SIP outbound is endpoint specific, but typically will be:

- Proxy 1
 - Server discovery = Manual
 - Server Address = DNS name of cluster peer or IP address of cluster peer
- Proxy 2
 - Server discovery = Manual
 - Server Address = DNS name of a different cluster peer or IP address of a different cluster peer
- Outbound = On

Option 2 – DNS SRV (2nd Choice)

To use this option, there must be a DNS SRV record available for the DNS name of the Expressway cluster that defines an equal weighting and priority for each cluster peer.

On each SIP endpoint configure the SIP Settings as:

- Server discovery = Manual
- Server Address = DNS name of the Expressway cluster

If the endpoint supports DNS SRV, on startup the endpoint issues a DNS SRV request and receives a DNS SRV record back defining an equal weighting and priority for each cluster peer.

The endpoint then tries to register with a relevant cluster peer (having taken into account the priority / weightings). If that peer is not available, the endpoint will try and register to another listed peer at the same

priority, or if all peers at that priority have been tried, a peer at the next lower priority. This is repeated until the endpoint can register with a Expressway.

The endpoint will continue to use the first Expressway that it registered to for re-registrations and for calls. If it ever loses connection to its Expressway, it will use the DNS SRV entry to find a new Expressway to register to, starting at the highest priority.

To minimize DNS traffic, the DNS SRV cache timeout should be set to a fairly long time, such as 24 hours.

Option 3 – DNS Round-Robin (3rd Choice)

To use this option, there must be a DNS A-record available for the DNS name of the Expressway cluster that supplies a round-robin list of IP addresses.

On each SIP endpoint configure the SIP Settings as:

- Server discovery = Manual
- Server Address = DNS name of the Expressway cluster

If the endpoint does not support DNS SRV, on startup the endpoint will perform a DNS A-record lookup. The DNS server will have been configured to support round-robin DNS, with each of the cluster peer members defined in the round-robin list.

The endpoint will take the address given by the DNS lookup and will then try and register with the relevant cluster peer. If that is not available, then the endpoint will perform another DNS lookup and will try to connect to the new Expressway peer that it is given. (The DNS server will have supplied the next cluster peer's IP address.) This is repeated until the endpoint can register with a Expressway.

The endpoint will continue to use the first Expressway that it registered to for re-registrations and for calls. If it ever loses connection to its Expressway it will perform another DNS lookup to find a new Expressway to register to (the DNS server providing a Expressway in the round-robin sequence).

DNS cache timeout should be set to a fairly short time (for example, 1 minute or less) so that if a Expressway is not accessible the endpoint is quickly pointed at a different Expressway.

Option 4 – Static IP (Least Preferred)

Use this option if the Expressway cluster does not have a DNS name.

On each SIP endpoint configure the SIP Settings as:

- Server discovery = Manual
- Server Address = IP address of a Expressway peer

On startup the endpoint will try and register with the Expressway at the specified IP address. If that is not available, then the endpoint will continue trying at regular intervals. This is repeated until the endpoint can register with the Expressway.

The endpoint will continue to use the first Expressway that it registered to for re-registrations and for calls. If it ever loses connection then it will keep on trying to register to that Expressway until it is accessible again.

H.323 Endpoints

The options are listed in preference order for providing resilience of connectivity of endpoints to a cluster of Expressways where 1 or more Expressway cluster peers become inaccessible. The choice of option will depend on what functionality the endpoint you are using supports.

Option 1 – DNS SRV (Preferred)

To use this option, there must be a DNS SRV record available for the DNS name of the Expressway cluster that defines an equal weighting and priority for each cluster peer.

On each H.323 endpoint, configure the Gatekeeper Settings as:

- Discovery = Manual
- IP Address = DNS name of the Expressway cluster

If the endpoint supports DNS SRV, on startup the endpoint issues a DNS SRV request and receives a DNS SRV record back defining an equal weighting and priority for each cluster peer.

The endpoint then tries to register with a relevant cluster peer (having taken into account the priority / weightings). If that peer is not available, the endpoint will try and register to another listed peer at the same priority, or if all peers at that priority have been tried, a peer at the next lower (higher numbered) priority.

This will be repeated until the endpoint can register with a Expressway. On registering with the Expressway, the Expressway will respond with the H.323 “Alternate Gatekeepers” list containing the list of Expressway cluster peer members.

The endpoint will continue to use the first Expressway that it registered to for re-registrations and for calls. If it ever loses connection to its Expressway then it will select an “Alternate Gatekeeper” from the list it was supplied with.

DNS SRV cache timeout should be set to a fairly long time (e.g. 24 hours) to minimize DNS traffic.

Option 2 – DNS Round-Robin (2nd Choice)

To use this option, there must be a DNS A-record available for the DNS name of the Expressway cluster that supplies a round-robin list of IP addresses.

On each H.323 endpoint configure the Gatekeeper Settings as:

- Discovery = Manual
- IP Address = DNS name of the Expressway cluster

If the endpoint does not support DNS SRV, on startup the endpoint will perform a DNS A-record lookup. The DNS server will have been configured to support round-robin DNS, with each of the cluster peer members defined in the round-robin list.

The endpoint will take the address given by the DNS lookup and will then try and register with the relevant cluster peer. If that peer is not available, then the endpoint will perform another DNS lookup and will try to connect to the new Expressway peer that it is given. (The DNS server will have supplied the next cluster peer’s IP address.)

This will be repeated until the endpoint can register with a Expressway. On registering with the Expressway, the Expressway will respond with the H.323 ‘Alternate Gatekeepers’ list containing the list of Expressway cluster peer members.

The endpoint will continue to use the first Expressway that it registered to for re-registrations and for calls. If it ever loses connection then it will select an “Alternate Gatekeeper” from the list it was supplied with.

DNS cache timeout should be set to a fairly short time (e.g. 1 minute or less) so that on failure to reach a Expressway at startup, the endpoint is quickly pointed at a different Expressway.

Option 3 – Static IP (Least Preferred)

Use this option if the Expressway cluster does not have a DNS name.

On each H.323 endpoint configure the Gatekeeper Settings as:

- Discovery = Manual
- IP Address = IP address of a Expressway peer

On startup the endpoint will try and register with the Expressway at the specified IP address. If that is not available, then the endpoint will continue trying at regular intervals.

This will be repeated until the endpoint can register with the Expressway. On registering with the Expressway, the Expressway will respond with the H.323 “Alternate Gatekeepers” list containing the list of Expressway cluster peer members.

The endpoint will continue to use the first Expressway that it registered to for re-registrations and for calls. If it ever loses connection then it will select an “Alternate Gatekeeper” from the list it was supplied with.

Add the Expressway to Cisco TMS

For more detail about Cisco TMS administration, see Cisco TelePresence Management Suite Administrator Guide , for your version, at [Cisco Telepresence Management Suite \(TMS Maintain and Operate Guide page\)](#)

On the Expressway

Step 1 Go to **System > SNMP**.

- a) **SNMP mode** is set to *v3 plus Cisco TMS support* or *v2c*.
- b) **Community name** is set to public.

(If SNMP was previously disabled, an alarm may appear indicating the need for a restart. If so, restart the system via **Maintenance > Restart options**.)

Step 2 Go to **System > External manager** and ensure that:

- a) **Address** is set to the IP address or FQDN of Cisco TMS.
- b) **Path** is set to `tms/public/external/management/SystemManagementService.asmx`.
- c) If the **Protocol** is HTTPS and **Certificate verification mode** is On then you must load the relevant certificates before the connection can become ‘Active’.

(If the **Protocol** is HTTP or **Certificate verification mode** is Off, no certificates need to be loaded.)

Step 3 Click **Save**.

The Status section of the External manager page should show a State of ‘Active’ or ‘Initialising’¹.

1

On the Cisco TMS

Step 1 Select **Systems > Navigator**.

Step 2 Select (or create) an appropriate folder in which to put the Expressway (in the example below the folder has been called “Cluster”):



Step 3 Click **Add Systems**.

Step 4 In section **1. Specify Systems by IP addresses or DNS names**, enter the IP address or DNS name of the Expressway.

Step 5 Click **Next**.

Step 6 Look for "green tick" sign for System added.

Note When you add an Expressway to TMS, the TMS UI shows it as a VCS. This is a known issue.

Step 7 Click **Finish Adding Systems**, **Add System despite warnings** or **Add More Systems** as appropriate.

¹ Cisco TMS may force the protocol to be HTTPS. The configuration for this is found in **Administrative Tools > Configuration > Network settings**. The protocol will be forced to HTTPS if, in the **TMS Services** section **Enforce Management Settings on Systems** is set to *On* and in the **Secure-Only Device Communication** section **Secure-Only Device Communication** is set to *On*.