Applications

- Configuring Conference Factory, on page 1
- About Presence, on page 3
- B2BUA (Back-to-Back User Agent) Overview, on page 7
- About FindMe, on page 15
- Cisco TMS Provisioning (Including FindMe), on page 18
- Hybrid Services and Connector Management, on page 21
- Cisco Webex Edge, on page 23

Configuring Conference Factory

The **Conference Factory** page (**Applications** > **Conference Factory**) allows you to enable and disable the Conference Factory application, and configure the alias and template it uses.

The Conference Factory application allows the Expressway to support the Multiway feature, subject to Multiway-compliant endpoints and conference bridges (see Cisco TelePresence Multiway Deployment Guide). Multiway enables endpoint users to create a conference while in a call even if their endpoint does not have this functionality built in.

Check with your Cisco representative for an up-to-date list of the Cisco endpoints and infrastructure products that support Multiway.

Conference creation process

When Multiway is activated from the endpoint:

1. The endpoint calls a pre-configured alias which routes to the Conference Factory on the Expressway.
2. The Expressway replies to the endpoint with the alias that the endpoint should use for the Multiway conference. This alias will route to an MCU.
3. The endpoint then places the call to the MCU using the given alias, and informs the other participating endpoints to do the same.

The configurable options are:

Field	Description	Usage tips
Mode	Enables or disables the Conference Factory application.	
Alias	The alias that will be dialed by the endpoints when the Multiway feature is activated. This must also be configured on all endpoints that may be used to initiate the Multiway feature. An example could be **multiway@example.com**.	
Template	The alias that the Expressway tells the endpoint to dial to create a Multiway conference on the MCU.	To ensure that each conference has a different alias, you should use %% as a part of the template. The %% will be replaced by a unique number each time the Expressway receives a new conference request.
Number range start / end	The first and last numbers in the range that replaces %% in the template used to generate a conference alias.	For example, your **Template** could be **563%%@example.com** with a range of 10 - 999. The first conference will use the alias **563010@example.com**, the next conference will use **563011@example.com** and so on up to **563999@example.com**, after which it will loop round and start again at **563010@example.com**. **Note** The %% represents a fixed number of digits – with leading zeroes where required – based upon the length of the upper range limit.

Note

- Use a different **Template** on each Expressway in your network that has the Conference Factory application enabled. If your Expressway is part of a cluster, the template must be different for each cluster peer.
- The alias generated by the template must be a fully-qualified SIP alias, and must route to the MCU. The MCU must be configured to process this alias. No other special configuration is required on the MCU in order to support the Conference Factory application.
- The **SIP mode** setting must be set to *On* (**Configuration** > **Protocols** > **SIP**) for the Conference Factory application to function. If you want to be able to initiate calls to the Conference Factory from H.323 endpoints, you must also set **H.323 mode** to *On* (**Configuration** > **Protocols** > **H.323**), and ensure that **H.323 <-> SIP interworking mode** is set to *Registered only* or *On* (**Configuration** > **Protocols** > **Interworking**).

See Cisco TelePresence Multiway Deployment Guide for full details on how to configure individual components of your network (endpoints, MCUs and Expressways) in order to use Multiway in your deployment.

About Presence

Presence is the ability of endpoints to provide information to other users about their current status - such as whether they are offline, online, or in a call. Any entity which provides presence information, or about whom presence information can be requested, is known as a presentity. Presentities publish information about their own presence status, and also subscribe to the information being published by other presentities and FindMe users.

Endpoints that support presence, such as Jabber Video, can publish their own status information. The Expressway can also provide basic presence information on behalf of endpoints that do not support presence, including H.323 endpoints, as long as they have registered with an alias in the form of a URI.

If FindMe is enabled, the Expressway can also provide presence information about FindMe users by aggregating the information provided by each presentity configured for that FindMe user.

The Presence application on the Expressway supports the SIP-based SIMPLE standard and is made up of two separate services. These are the Presence Server and the Presence User Agent. These services can be Configuring Presence separately.

The Presence status pages provide information about the presentities who are providing presence information and the users who are requesting presence information on others. The status pages are organized into:

- Publishers
- Presentities
- Subscribers

Note Any one presentity can only subscribe to a maximum of 100 other presentities, and can only have a maximum of 100 other presentities subscribed to it.

Presence is supported by clustering.

Presence Server

The Presence Server application on the Expressway is responsible for managing the presence information for all presentities in the SIP domains for which the Expressway is authoritative. The Presence Server can manage the presence information for locally registered endpoints and presentities whose information has been received via a SIP proxy (such as another Expressway).

The Presence Server is made up of the following services, all of which are enabled (or disabled) simultaneously when the Presence Server is enabled (or disabled):

- **Publication Manager**: Receives PUBLISH messages, which contain the status information about a presentity, and writes this information to the Presence Database. PUBLISH messages are generated by presence-enabled endpoints and by the Presence User Agent.
- **Subscription Manager**: Handles SUBSCRIBE messages, which request information about the status of a presentity. Upon receipt of a SUBSCRIBE message, the Subscription Manager sends a request to the Presentity Manager for information about that presentity, and forwards the information that is returned

to the subscriber. The Subscription Manager also receives notifications from the Presentity Manager when a presentity's status has changed, and sends this information to all subscribers.

- **Presentity Manager**: An interface to the Presence Database. It is used to support Expressway features such as FindMe and the PUA, where the presence information provided by a number of different devices must be aggregated in order to provide an overall presence status for one particular presentity. When the Presentity Manager receives a request from the subscription manager for information on a presentity, it queries the Presence Database for all information available on all the endpoints associated with that particular presentity. The Presentity Manager then aggregates this information to determine the presentity's current status, and returns this to the Subscription Manager.
- **Presence Database**: Stores current presence information received in the form of PUBLISH messages. Also sends NOTIFY messages to the Presentity Manager to inform it of any changes.

Presence and device authentication

The Presence Server accepts presence PUBLISH messages only if they have already been authenticated:

- The authentication of presence messages by the Expressway is controlled by the authentication policy setting on the Default Subzone (or relevant alternative subzone) if the endpoint is registered (which is the usual case), or by the authentication policy setting on the Default Zone if the endpoint is not registered.
- The relevant **Authentication policy** must be set to either *Check credentials* or *Treat as authenticated*, otherwise PUBLISH messages will fail, meaning that endpoints will not be able to publish their presence status.

See Presence and authentication policy for more information.

Presence User Agent

Endpoints that do not support presence can have status published on their behalf by the Expressway. The service that publishes this information is called the Presence User Agent (PUA).

The PUA takes information from the local registration database and the call manager and determines, for each endpoint that is currently locally registered, whether or not it is currently in a call. The PUA then provides this status information via a PUBLISH message.

For the PUA to successfully provide presence information about a locally registered endpoint:

- The endpoint must be registered with an alias in the form of a URI.
- The domain part of the URI must be able to be routed to a SIP registrar that has a presence server enabled. (This could be either the local Presence Server, if enabled, or another Presence Server on a remote system.)

When enabled, the PUA generates presence information for all endpoints registered to the Expressway, including those which already support presence. The status information provided by the PUA is either:

- *online* (registered but not in a call)
- *in call* (registered and currently in a call)

Aggregation of presence information

When enabled, the PUA generates presence information for all endpoints registered to the Expressway, including those which already support presence. However, endpoints that support presence may provide other,

more detailed status, for example away or do not disturb. For this reason, information provided by the PUA is used by the Presentity Manager as follows:

- Where presence information is provided by the PUA and one other source, the non-PUA presence information will always be used in preference to the PUA presence information. This is because it is assumed that the other source of information is the presentity itself, and this information is more accurate.
- Where presence information is provided by the PUA and two or more other sources, the Presence Server will aggregate the presence information from all presentities to give the "highest interest" information, e.g. *online* rather than *offline*, and *in call* rather than *away*.
- If no information is being published about an endpoint, either by the endpoint itself or by the PUA, the endpoint's status will be *offline*. If the PUA is enabled, the *offline* status indicates that the endpoint is not currently registered.

FindMe presence

When the Presentity Manager receives a request for information about the presences of a FindMe alias, it looks up the presence information for each endpoint that makes up that FindMe alias. It then aggregates this information as follows:

- If the FindMe alias is set to *Individual* mode, if any one of the endpoints making up that FindMe is in a call the FindMe presentity's status will be reported as *in call*.
- If the FindMe alias is set to *Group* mode, if any one of the endpoints is online (i.e. not in call or offline) then the FindMe presentity's status will be reported as *online*.

Registration refresh period

The PUA will update and publish presence information on receipt of:

- A registration request (for new registrations)
- A registration refresh (for existing registrations)
- A deregistration request
- Call setup and cleardown information

For non-traversal H.323 registrations the default registration refresh period is 30 minutes. This means that when the PUA is enabled on an Expressway with existing registrations, it may take up to 30 minutes before an H.323 registration refresh is received and *available* presence information is published for that endpoint.

It also means that if an H.323 endpoint becomes unavailable without sending a deregistration message, it may take up to 30 minutes for its status to change to *offline*. To ensure more timely publication of presence information for H.323 endpoints, you should decrease the H.323 registration refresh period (using **Configuration** > **Protocols** > **H.323** > **Gatekeeper** > **Time to live**).

The default registration refresh period for SIP is 60 seconds, so it will take no more than a minute for the PUA to publish updated presence information on behalf of any SIP endpoints.

Configuring Presence

The **Presence** page (**Applications** > **Presence**) allows you to enable and configure Presence services on the Expressway.

These services can be enabled and disabled separately from each other, depending on the nature of your deployment. Both are disabled by default.

Note **SIP mode** must be enabled for the Presence services to function.

Presence User Agent

The PUA provides presence information on behalf of registered endpoints.

- *Enabled*: If the PUA is enabled, it will publish presence information for all locally registered endpoints, whether or not those endpoints are also publishing their own presence information. Information published by the PUA will be routed to a Presence Server acting for the endpoint's domain. This could be the local Presence Server, or (if this is disabled) a Presence Server on another system that is authoritative for that domain.
- *Disabled*: If the PUA is disabled, only those endpoints that support presence will publish presence information. No information will be available for endpoints that do not support presence.

You can also configure the **Default published status for registered endpoints**. This is the presentity status published by the Presence User Agent for registered endpoints when they are not "In-Call". The options are either *Online* or *Offline*.

Note

- If this is set to *Online*, any permanently registered video endpoints and FindMe entries that include those endpoints will appear as permanently "Online".
- The status of non-registered endpoints always appears as "Offline".
- "Online" status appears as "Available" in Lync clients.

Presence Server

The Presence Server manages the presence information for all presentities in the SIP domains for which the Expressway is authoritative.

- *Enabled*: If the local Presence Server is enabled, it will process any PUBLISH messages intended for the SIP domains for which the local Expressway is authoritative. All other PUBLISH messages will be proxied on in accordance with the Expressway's SIP routing rules.

Note SIP routes are configured using the CLI only.

- The Presence Server requires that any messages it receives have been pre-authenticated (the Presence Server does not do its own authentication challenge).You must ensure that the subzone through which PUBLISH messages are being received has its **Authentication policy** is set to either *Check credentials* or *Treat as authenticated*, otherwise the messages will be rejected.

- *Disabled*: If the local Presence Server is disabled, the Expressway will proxy on all PUBLISH messages to one or more of its neighbor zones in accordance with its locally configured call routing rules. The local Expressway will do this regardless of whether or not it is authoritative for the presentity's domain. If one of these neighbors is authoritative for the domain, and has a Presence Server enabled, then that neighbor will provide presence information for the presentity.

Regardless of whether or not the Presence Server is enabled, the Expressway will still continue to receive PUBLISH messages if they are sent to it from any of the following sources:

- Locally registered endpoints that support presence
- The local PUA (if enabled)
- Remote SIP Proxies

Note Presence Server is automatically enabled when the **Starter Pack** option key is installed.

Recommendations

- **Expressway-E and Expressway-C**: The recommended configuration for an Expressway-E when acting as a traversal server for an Expressway-C is to enable the PUA and disable the Presence Server on the Expressway-E, and enable the Presence Server on the Expressway-C. This will ensure that all PUBLISH messages generated by the PUA are routed to the Expressway-C.
- **Expressway neighbors**: If you have a deployment with two or more Expressways neighbored together, you are recommended to enable only one presence server per domain. This will ensure a central source of information for all presentities in your network.
- **Expressway clusters**: For information about how Presence works within a cluster.

Note Any defined transforms also apply to any Publication, Subscription or Notify URIs handled by the Presence Services.

B2BUA (Back-to-Back User Agent) Overview

A B2BUA operates between both endpoints of a SIP call and divides the communication channel into two independent call legs. Unlike a proxy server, the B2BUA maintains complete state for the calls it handles. Both legs of the call are shown as separate calls on the **Call status** and **Call history** pages.

B2BUA instances are hosted on the Expressway. They are used in the following scenarios:

- To apply media encryption policy. This usage does not require any explicit B2BUA configuration.
- To support ICE messaging. The only B2BUA-related configuration required is to define the set of Configuring B2BUA TURN Servers required to support ICE calls.

- To route SIP calls between the Expressway and a Microsoft SIP domain. This requires manual configuration of Configuring Microsoft Interoperability and the set of Configuring B2BUA TURN Servers available for use by the B2BUA.

Configuring B2BUA TURN Servers

Go to **Applications** > **B2BUA** > **B2BUA TURN servers** to enter details of the TURN servers that are needed by the Expressway B2BUA instances. The page lists the currently configured TURN servers and lets you create, edit and delete them.

The B2BUA chooses which TURN server to offer via random load-balancing between all of the available servers. There is no limit to the number of servers that can be configured for the B2BUA to choose from.

The TURN servers are automatically used by B2BUA instances for ICE messaging when it is enabled on a zone or subzone.

If you want to use the TURN servers for Microsoft interoperability, you must enable **Offer TURN services** (See Configuring Microsoft Interoperability).

Table 1: TURN Server Configuration Details

Field	Description
TURN server address	The IP address of a TURN server to offer when establishing ICE calls (for example, with a Microsoft Edge server). The TURN server must be RFC 5245 compliant, for example an Expressway-E TURN server.
TURN server port	The listening port on the TURN server.
Description	A free-form description of the TURN server.
TURN services username and password	The username and password that are required to access the TURN server.

About Microsoft Interoperability

Expressway interoperability with Microsoft is based on a back-to-back user agent (B2BUA) which handles SIP calls between the Expressway and the Microsoft Skype for Business infrastructure.

Note From version X8.9, you can interoperate with Microsoft infrastructure without using the B2BUA on the Expressway. You can instead use session classification search rules to route calls to Cisco Meeting Server, which does the transcoding. See *Cisco Meeting Server with Cisco Expressway Deployment Guide* on the Expressway Configuration Guides page (previously called the *Cisco Expressway Traffic Classification Deployment Guide*).

Capabilities

- Interwork between Microsoft ICE and standards-based media for Cisco collaboration endpoints and bridges.
- Call hold, call transfer and Multiway support for calls with Microsoft clients, and can share FindMe presence information with Microsoft infrastructure.
- Transcoding of Microsoft client screen sharing (RDP) to H.264.
- Filter the messaging and presence traffic from Microsoft SIP and redirect it towards appropriate servers such as IM and Presence Service nodes, while handling voice/video traffic on the Expressway.

Configuration Summary

- Selecting the Microsoft interoperability service on a dedicated Expressway.
- Adding the *Microsoft Interoperability key*.
- Configuring Microsoft Interoperability.
- Configuring the B2BUA's Trusted Hosts — the devices that may send signaling messages to the B2BUA.
- Configuring B2BUA TURN Servers — TURN servers available for use by the B2BUA when establishing ICE calls.
- Setting up search rules to route calls to the Microsoft domain, through the automatically configured zone, to the B2BUA.

  When you enable the B2BUA, the Expressway automatically creates a non-configurable neighbor zone called **To Microsoft destination via B2BUA**; this zone must be the target of your search rules.

  The zone is not automatically deleted when you disable the B2BUA; Also, the old zone name (To Microsoft Lync Server via B2BUA) persists if you already had this zone when you upgraded to X8.8.
- Restarting the Microsoft Interoperability Service, if required. The system notifies you if you must restart the service.

Why do I need the Microsoft Interoperability Option Key?

You need this key on the Expressway-C (on each peer if the Expressway-C is clustered) if you are using the Expressway to modify traffic between Microsoft collaboration infrastructure and standards-based infrastructure. This includes:

- Microsoft SIP to standard SIP call interworking
- Screen share transcoding (RDP to H.264 in BFCP)
- Microsoft SIP message and presence forwarding (SIP Broker)

You do not need this key if you are using the Expressway to route Microsoft traffic without modifying it. For example, if you are using the Expressway search rules to send Microsoft variant SIP traffic to be interworked by a Cisco Meeting Server.

Features and Limitations

- Maximum simultaneous call capability is 100 calls *including* Large systems. The exception is M5-based Small systems, which have a limit of 75 calls.
- A call routed through an external transcoder counts as 2 calls.
- If a call is routed through the Microsoft interoperability B2BUA, the B2BUA always takes the media and always remains in the signaling path. The call component that is routed through the B2BUA can be identified in the call history details as having a component type of *Microsoft interoperability*.
- The Microsoft interoperability service does not consume additional call licenses beyond what is required by the call leg between the endpoint and the Expressway.
- If all configured external transcoders reach their capacity limits, any calls that would normally route via a transcoder will not fail; the call will still connect as usual but will not be transcoded.
- You can use multiple TURN servers with the Microsoft interoperability service. TURN servers are required for calls traversing a Microsoft Edge server.
- You can apply bandwidth controls to the call leg between the endpoint and the B2BUA, but not to the call leg between the B2BUA and the Microsoft infrastructure. However, because the B2BUA forwards the media it receives without any manipulation, any bandwidth controls you apply to the Expressway to B2BUA leg will implicitly apply to the B2BUA to Microsoft leg.
- The non-configurable neighbor zone (named "**To Microsoft destination via B2BUA**") uses a special zone profile of *Microsoft interoperability*. You cannot select this profile for any manually configured zones.
- **Intradomain Microsoft Interoperability with Expressway and Cisco Meeting Server**

  If you use Meeting Server for Microsoft Interoperability, a limitation currently applies to the following intradomain/intracompany scenario:

  *You deploy separate Microsoft and standards-based SIP networks in a **single domain** and in a configuration that has an Expressway-E/Cisco VCS Expressway **directly facing** a Microsoft front end server (because you use internal firewalls between subnetworks, or for any other reason). For example, Cisco Unified Call Manager in one (sub)network and Microsoft in a second (sub)network, inside the same domain.*

  In this case we do not generally support Microsoft Interoperability between the two networks, and calls between Meeting Server and Microsoft will be rejected.

  Workaround: If you are not able to deploy the intradomain networks without an intervening Expressway-E/VCS Expressway (you cannot configure Meeting Server <> Expressway-C/VCS Control <> Microsoft), a workaround is to deploy an Expressway-C/VCS-C in each subnet, with an Expressway-E/VCS-E to traverse between them. That is:

  Meeting Server <> Expressway-C/VCS Control <> Firewall <> Expressway-E/VCS Expressway <> Firewall <> Expressway-C/VCS Control <> Microsoft

For more information about configuring Expressway for Microsoft Interoperability:

- See the *Cisco Expressway IP Port Usage Configuration Guide*, for your version, on the Cisco Expressway Series Configuration Guides page.
- See Cisco Expressway with *Microsoft Infrastructure Deployment Guide* on the Expressway Configuration Guides page.

Configuring Microsoft Interoperability

Go to **Applications** > **B2BUA** > **Microsoft interoperability** > **Configuration** to configure and enable the B2BUA connection to the Microsoft environment.

The configurable options are described in the table:

Field	Description	Usage tips
Configuration section:		
Microsoft interoperability	Enables or disables the Microsoft interoperability service.	
Destination address	The IP address or Fully Qualified Domain Name (FQDN) of the Hardware Load Balancer, Director or Front End Processor to which the Expressway sends the signaling messages.	You must also configure the IP addresses of the Configuring the B2BUA's Trusted Hosts. These are the Microsoft systems that may send signaling messages to the Expressway.
Listening port	The IP port on the Hardware Load Balancer, Director or Front End Processor to which the Expressway sends the signaling messages.	
Signaling transport	The transport type used for connection to the Microsoft infrastructure. The default is *TLS*.	
FindMe integration section:		
Register FindMe users as clients to Microsoft server	Controls whether to register FindMe users to the Microsoft registrar so that it can forward calls to FindMe aliases and share FindMe presence information. Default is *Yes*.	This feature only applies if FindMe is enabled. **Note** FindMe users can only register to Microsoft infrastructure if the FindMe ID is a valid user in the Active Directory (in the same way that Microsoft clients can only register if they have a valid account enabled in AD).
Microsoft domain	The SIP domain in use on the Microsoft server. This must be selected from one of the SIP domains already configured on the Expressway.	Only FindMe names with this domain will be registered to the Microsoft server.
Remote Desktop Protocol section:		
Enable RDP transcoding for this B2BUA	Controls whether the B2BUA offers Remote Desktop Protocol transcoding. This feature requires the **Microsoft Interoperability** option key. Default is *No*.	You should enable this option if you want Microsoft client users to be able to share their screens with Cisco Collaboration endpoints / conference participants.
SIP broker section:		

Field	Description	Usage tips
Enable broker for inbound SIP	Toggles the SIP broker, and opens a list of destination presence servers. The broker inspects Microsoft SIP, and routes the SIP SIMPLE to IM and Presence Service nodes that you enter.	If the broker is not enabled, then the B2BUA attempts to process all inbound SIP from Microsoft. If it receives SIP SIMPLE, it tries to route it as if it were SIP audio/video traffic. The SIP SIMPLE will probably be rejected by the call control infrastructure in this case.
Listening port on presence destination servers	This is the port configured on the IM and Presence Service nodes.	
Destination presence server 1..6	IP address, hostname, or FQDN of the IM and Presence Service node.	Enter up to 6. The Expressway polls them regularly to determine liveness state, and routes traffic to them using a round-robin algorithm.
TURN section:		
Offer TURN services	Controls whether the B2BUA offers TURN services. Default is *No*.	This is recommended for calls traversing a Microsoft Edge server. To configure the associated TURN servers, click Configuring B2BUA TURN Servers.
Advanced settings: You should only modify the advanced settings on the advice of Cisco customer support.		
Encryption	Controls how the B2BUA handles encrypted and unencrypted call legs. *Required*: Both legs of the call must be encrypted. *Auto*: Encrypted and unencrypted combinations are supported. The default is *Auto*.	A call via the B2BUA comprises two legs: one leg from the B2BUA to a standard video endpoint, and one leg from the B2BUA to the Microsoft client. Either leg of the call could be encrypted or unencrypted. A setting of *Auto* means that the call can be established for any of the encrypted and unencrypted call leg combinations. Thus, one leg of the call could be encrypted while the other leg could be unencrypted.

Field	Description	Usage tips
B2BUA media port range start/end	The port range used by the B2BUA for handling media.	Ensure that the port range does not overlap with other port ranges used by this Expressway or this Expressway's TURN server. You may need to increase this range if you **Enable RDP Transcoding for this B2BUA**, because desktop sharing increases the number of media ports required per call.
Hop count	Specifies the Max-Forwards value to use in SIP messages. Default is 70.	
Session refresh interval	The maximum time allowed between session refresh requests for SIP calls. Default is 1800 seconds.	For further information see the definition of *Session-Expires* in RFC 4028.
Minimum session refresh interval	The minimum value the B2BUA will negotiate for the session refresh interval for SIP calls. Default is 500 seconds.	For further information see the definition of *Min-SE header* in RFC 4028.
Port on B2BUA for Expressway communications	The port used on the B2BUA for communicating with the Expressway.	
Port on B2BUA for Microsoft call communications	The port used on the B2BUA for call communications with the Microsoft server. Default is 65072.	
RDP TCP port range start / end	Defines the range of TCP ports on which the transcoder instances listen for RDP media. Default is 6000 - 6099. **Note** Save the page and restart the Microsoft interoperability service to apply your changes.	Each simultaneous RDP transcoding session created on the B2BUA requires a receiving port. The range is limited to 100 as this is the maximum possible number of simultaneous transcode sessions.
RDP UDP port range start / end	Defines the range of UDP ports from which the transcoder instances transmit H.264 media. Default is 6100 - 6199. **Note** Save the page and restart the Microsoft interoperability service to apply your changes.	Each simultaneous RDP transcoding session created on the B2BUA requires a port to send out the resulting H.264 media. The range is limited to 100 as this is the maximum possible number of simultaneous transcode sessions.

Field	Description	Usage tips
Maximum RDP transcode sessions	Limits the number of simultaneous RDP transcoding sessions on this Expressway. Default is 10. **Note** Save the page and restart the Microsoft interoperability service to apply your changes.	Higher values will mean that more system resources can be consumed by RDP transcoding, which could impact other services. Maximum is 100. Recommended maximum RDP transcode sessions: • Medium OVA systems: 10 • Large OVA / CE1200 systems: 20 (From X8.10, it's no longer necessary to have a 10 Gbps NIC for Large system scale. Subject to your bandwidth constraints, the capacity of a Large system is possible with a 1 Gbps NIC.)

Configuring the B2BUA's Trusted Hosts

Go to **Applications** > **B2BUA** > **Microsoft Interoperability** > **Trusted hosts**) to specify the Microsoft hosts from which the Expressway will trust SIP signaling.

The interoperability service does not accept messages from any addresses that are not on the trusted hosts list.

Note Trusted host verification only applies to calls initiated by Microsoft clients that are inbound to the Expressway video network. It is not necessary to configure trusted hosts if calls are only ever to be initiated from the Expressway video network.

The Expressway currently has a nominal limit of 25 trusted hosts. If there are more than 25 trusted hosts, the Expressway raises an alarm.

In practice, you can have more than 25 trusted hosts if you need them in your deployment. We recommend that you keep the number below 50, and you can safely ignore the alarm. If you need to go beyond 50, we recommend adding another Gateway Expressway.

The configurable options are:

Field	Description	Usage tips
Name	An optional free-form description of the trusted host.	The name is not used as part of the “trusted” criteria. It is only to help you distinguish between multiple hosts without relying on the IP addresses.
IP address	The IP address of the trusted host.	

Field	Description	Usage tips
Type	The type of device that may send signaling messages to the B2BUA. *Microsoft infrastructure*: This includes Hardware Load Balancers, Directors and Front End Processors	

Restarting the Microsoft Interoperability Service

Sometimes you need a restart to apply changes to the Microsoft interoperability service. The system raises an alarm if you need a restart.

When you restart this service, the Expressway does not restart, but it does drop any calls that are being managed by the B2BUA.

Procedure

Step 1 Go to **Applications** > **B2BUA** > **Microsoft interoperability** > **Restart service....**

Step 2 Check the number of active calls currently in place.

Step 3 Click **Restart**.

The service restarts after a few seconds. You can check the service status on the Configuring Microsoft Interoperability page.

Clustered Expressway Systems

You must restart the Microsoft interoperability service on every peer. Configure, restart and verify the service on the primary before restarting the service on other peers.

About FindMe

FindMe is a form of User Policy, which is the set of rules that determines what happens to a call for a particular user or group when it is received by the Expressway.

The FindMe feature lets you assign a single FindMe ID to individuals or teams in your enterprise. By logging into their FindMe account, users can set up a list of locations such as “at home” or “in the office” and associate their devices with those locations. They can then specify which devices are called when their FindMe ID is dialed, and what happens if those devices are busy or go unanswered. Each user can specify up to 15 devices and 10 locations.

This means that potential callers can be given a single FindMe alias on which they can contact an individual or group in your enterprise - callers won’t have to know details of all the devices on which that person or group might be available.

To enable this feature you must purchase and install Desktop System or TelePresence Room System registration licenses.

End-User FindMe Account Configuration

Users can configure their FindMe settings using Cisco TMS provisioning. If TMS provisioning is enabled, users manage their FindMe settings by logging in to Cisco TMS using their FindMe account. User account and FindMe data is provided from Cisco TMS to Expressway by the TMS Provisioning Extension services.

Expressway looks for an attribute named **distinguishedName** to search the user in the LDAP server.

Note Make sure LDAP server user records have a valid attribute named **distinguishedName**.

See FindMe Deployment Guide for more details about setting up FindMe accounts.

How are Devices Specified?

When configuring their FindMe account, users are asked to specify the devices to which calls to their FindMe ID are routed.

It is possible to specify aliases and even other FindMe IDs as one or more of the devices. However, care must be taken in these situations to avoid circular configurations.

For this reason, we recommend that users specify the physical devices they want to ring when their FindMe ID is called by entering the alias with which that device has registered.

Principal devices

A FindMe user's account should be configured with one or more principal devices. These are the main devices associated with that account.

Users are not allowed to delete or change the address of their principal devices. This is to stop users from unintentionally changing their basic FindMe configuration.

Principal devices are also used by the Expressway to decide which FindMe ID to display as a **Caller ID** if the same device address is associated with more than one FindMe ID. Only an administrator (and not FindMe users themselves) can configure which of a FindMe user's devices are their principal devices.

FindMe Process Overview

When the Expressway receives a call for a particular alias it applies its User Policy as follows:

- It first checks to see if FindMe is enabled. If so, it checks if the alias is a FindMe ID, and, if it is, the call is forwarded to the aliases associated with the active location for that user's FindMe configuration.
- If FindMe is not enabled, or the alias is not a FindMe ID, the Expressway continues to search for the alias in the usual manner.

Note User Policy is invoked after any Call Policy configured on the Expressway has been applied. See Call Routing Process for more information.

Recommendations when Deploying FindMe

- The FindMe ID should be in the form of a URI, and should be the individual's primary URI.
- Endpoints should not register with an alias that is the same as an existing FindMe ID. You can prevent this by including all FindMe IDs on the Deny List.

Example

Users at Example Corp. have a FindMe ID in the format **john.smith@example.com**. Each of the user's endpoints are registered with a slightly different alias that identifies its physical location. For example their office endpoint is registered with an alias in the format **john.smith.office@example.com** and their home endpoint as **john.smith.home@example.com**.

Both of these endpoints are included in the list of devices to ring when the FindMe ID is dialed. The alias **john.smith@example.com** is added to the Deny List, to prevent an individual endpoint registering with that alias.

Configuring FindMe

The **FindMe configuration** page (**Applications** > **FindMe**) is used to enable and configure About FindMe.

The configurable options are:

Field	Description	Usage tips
FindMe mode	Determines whether or not FindMe is enabled, and if a third-party manager is to be used. *Off*: Disables FindMe. *Remote service*: Enables FindMe and uses a FindMe manager located on an off-box system (for example,TMS).	Call Policy is always applied regardless of the FindMe mode. If you enable FindMe, you must ensure a **Cluster name** is specified (you do this on the Clustering page).
Caller ID	Determines how the source of an incoming call is presented to the callee. *Incoming ID*: Displays the address of the endpoint from which the call was placed. *FindMe ID*: Displays the FindMe ID associated with the originating endpoint's address.	Using *FindMe ID* means that if the recipient subsequently returns that call, all the devices associated with that FindMe account will be called. The FindMe ID is only displayed if the source endpoint has been authenticated (or treated as authenticated). If it is not authenticated the Incoming ID is displayed. See About Device Authentication for more details.

The following options apply when **FindMe mode** is *Remote service*:

Field	Description
Protocol	The protocol used to connect to the remote service.
Address	The IP address or domain name of the remote service.

Field	Description
Path	The URL of the remote service.
Username	The username used by the Expressway to log in and query the remote service.
Password	The password used by the Expressway to log in and query the remote service.

Management and Storage of FindMe Data

If you use FindMe and want to use Cisco TMS to manage your FindMe data, you must configure Cisco TMSPE services to provide the Expressway with FindMe data.

Cisco TMS Provisioning (Including FindMe)

Cisco TMS provisioning is the mechanism through which the Expressway uses provisioning data for the following services:

- User account, device, and phone book data used by Expressway to service Expressway Provisioning Server from endpoint devices
- FindMe account configuration data used by Expressway to provide About FindMe

How to enable TMS provisioning services

From X8.11, TMS provisioning services are off by default in the Expressway for new systems (if you are upgrading an existing system to X8.11 or later, your current settings are retained). To enable TMS provisioning, services follow the steps below:

Note Although provisioning is supported on both the Cisco Expressway-C and the Cisco Expressway-E, for deployments with a paired Expressway-C and Expressway-E, we recommend that you use it on the Cisco Expressway-C.

1. (One-time only) If not already enabled, you need to enable provisioning services on the Expressway:
   a. Go to **System** > **Administration**.
   b. In the **Services** area, set **Provisioning services** to *On*.

      This makes the **System** > **TMS Provisioning Extension services** page accessible in the interface. From here you can connect to the Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE) and its provisioning services for users, devices, FindMe and phone books.
2. Go to **System** > **TMS Provisioning Extension services**.
3. Specify your connection details for the Cisco TMSPE (for assistance, see Configuring TMS Provisioning Extension Services).
4. Enable one or more provisioning services (users, devices, FindMe and phone books). For each service you want:

a. Set **Connect to this service** to *Yes*.

b. If you don't want the default values, optionally define a **Polling interval** or **Connection**.

   For Devices, you need to specify a **Base Group**. An ID which identifies the Expressway or cluster in the Cisco TMSPE.

Size limitations for clusters and provisioning

An Expressway cluster of any size supports up to:

- 10,000 FindMe accounts
- 10,000 users for provisioning
- 200,000 phonebook entries

Note Even if the device registration capacity limit of your system is greater, you are limited to 10,000 FindMe accounts/users and 10,000 provisioned devices per cluster.

If you need to provision more than 10,000 devices, your network will require additional Expressway clusters with an appropriately designed and configured dial plan.

See Cisco TMS Provisioning Extension Deployment Guide for full information about how to configure provisioning in Cisco TMS and Expressway.

Cisco TMSPE services used for provisioning

When TMS provisioning is enabled, Expressway uses the following Cisco TMSPE services (hosted on Cisco TMS) to provide the Expressway / Expressway cluster with data:

Service	Description
User Preference	Provides data that enables the Expressway to configure a device with settings that apply to a specific user (a user is essentially a SIP URI). Devices such as Jabber Video are configured entirely using this service. Also provides connection details to a TURN server; typically the Expressway-E.
FindMe	Provides details of user FindMe accounts, in particular the locations and devices associated with each FindMe ID. This allows the Expressway to apply its User Policy, and to be able to change a caller's source alias to its corresponding FindMe ID.
Phone books	Provides data that allows users to search for contacts in phone books. Access to phone books is controlled on a per user basis according to any access control lists that have been defined (within Cisco TMS).

Service	Description
Devices	Exchanges provisioning licensing information between the Expressway and Cisco TMS. Information is exchanged every 30 seconds — the Expressway is provided with the current number of free licenses available across the range of Expressway clusters being managed by Cisco TMS, and the Expressway updates Cisco TMS with the status of provisioning licenses being used by this Expressway (or Expressway cluster). If the Devices service is not active, the Expressway's Provisioning Server will not be able to provision any devices.

Status information for Cisco TMSPE services

Service status information is displayed on the TMS Provisioning Extension service status page.

- The Expressway periodically polls Cisco TMSPE services to ensure the data held on Expressway is kept up to date. The polling interval can be defined for each service. In typical deployments you are recommended to use the default settings which provide frequent (every 2 minutes) updates to FindMe and user provisioning data, and daily updates to phone book data.

  With clustered Expressways, only one of the cluster peers maintains the physical connection to Cisco TMS. The data obtained from Cisco TMS is then shared between other peers in the cluster through the Expressway's cluster replication mechanism.

- You can do an immediate resynchronization of data between Expressway and Cisco TMS at any time by clicking **Perform full synchronization** on the **TMS Provisioning Extension services** page. This will result in a few seconds lack of service on the Expressway while data is deleted and refreshed. If you only need to apply recent updates in Cisco TMS to the Expressway, click **Check for updates** instead.

Changing configuration settings for Cisco TMSPE services

We strongly recommend using Cisco TMS to make any changes to Cisco TMSPE services settings. Although you can configure the services on the Expressway (**TMS Provisioning Extension services** page), changes made through this page **are not applied in Cisco TMS**.

Expressway Provisioning Server

If device provisioning is enabled, the Expressway Provisioning Server provides provisioning-related services to provisioned devices, using data supplied by Cisco TMS through the Cisco TMS Provisioning (Including FindMe) mechanism.

Expressway supports only the Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE) services to provide the Expressway with provisioning and FindMe data. In this mode all provisioning and FindMe data is managed and maintained exclusively within Cisco TMS.

Provisioning Licenses

There is a limit to the number of devices that can be provisioned concurrently by the Provisioning Server. Expressway and Cisco TMS manage the number of available provisioning licenses by exchanging information through the Cisco TMSPE Devices service. If the Devices service is not active, the Expressway's Provisioning Server will not be able to provision any devices.

The Expressway is provided with the current number of free licenses available across the range of Expressway clusters being managed by Cisco TMS, and the Expressway updates Cisco TMS with the status of provisioning licenses being used by this Expressway (or Expressway cluster). License limits can be managed at a per device type basis.

Some devices, including Jabber Video 4.x, do not inform the Expressway when they sign out (unsubscribe) from being provisioned. The Expressway manages these devices by applying a 1 hour timeout interval before releasing the license.

Provisioning and Device Authentication

The Provisioning Server requires that any provisioning or phone book requests it receives have already been authenticated at the zone or subzone point of entry into the Expressway. The Provisioning Server does not do its own authentication challenge and will reject any unauthenticated messages.

See Device Provisioning and Authentication Policy for more information.

Hybrid Services and Connector Management

If you want to register Expressways for Hybrid Services, see the Hybrid Services documentation to get more detailed information, including how to do first time deployments of Hybrid Services.

What are Hybrid Services and what do they do?

Cisco Webex Hybrid Services tie your premises-based solutions into the Cisco Collaboration cloud to deliver a more capable, better integrated collaboration user experience.

Which services can I use?

When you purchase Hybrid Services, you get access to Cisco Webex Control Hub - an administrative interface to the Cisco Webex cloud. From the Control Hub you can walk through deployment aids for each hybrid service, and enable features for your users.

What software do I need?

The on-premises components of Hybrid Services are called “connectors”, and the Expressway software contains a management connector to manage registration and other connectors.

The management connector is dormant until you register Expressway to the cloud. When you register, the management connector is automatically downloaded, installed, and upgraded if a newer version is available.

The Expressway then downloads any other connectors that you selected using Control Hub. They are not started by default and you need to do some configuration before they'll work.

After this configuration, the connectors automatically download and upgrade based on the software upgrade schedule that you set in Control Hub. No manual intervention is required.

How do I install, upgrade, or downgrade?

The connectors are not active by default, and will not do anything until you configure and start them. You can do this on new interface pages that the connectors install on the Expressway.

Connector upgrades are made available through Control Hub, and the management connector will download the new versions to Expressway when you have authorized the upgrade.

You can also deregister, which disconnects your Expressway from Cisco Webex and removes all connectors and related configuration.

Note Because cloud-delivered services are constantly in development to deliver new features and functionality, the minimum supported Expressway version for Hybrid Services may also change. You must ensure that your registered Expressways are up to date so that your Hybrid Services deployment remains functional and can be officially supported. See the Expressway version support statement for more information.

Where can I read more about Hybrid Services?

Hybrid Services are continuously developed and may be published more frequently than Expressway. This means that information about Hybrid Services is maintained in the Hybrid Services documentation, and several Expressway interface pages link out to that site.

Connector Proxy

If you want to register Expressways for Hybrid Services, see the Hybrid Services documentation to get more detailed information, including how to do first time deployments of Hybrid Services.

What is this proxy for?

Use the **Applications** > **Hybrid Services** > **Connector Proxy** page if this Expressway needs a proxy to connect to Cisco Webex. This proxy is not used by the Expressway for other purposes.

What kind of traffic goes through this proxy?

The proxy must be capable of handling outbound HTTPS and secure web socket connections. It must also allow those connections to be initiated by the Expressway using either basic authentication or no authentication.

What details do I need to configure the proxy?

You'll need the address of the proxy, the port it's listening on, and the basic authentication username and password (if your proxy requires authentication).

Cisco Webex CA Root Certificates on Expressway-E

The Cisco Webex cloud CA root certificates are packaged in the Expressway software and you can click **Get certificates** to start using them to validate incoming certificates. You can click **Remove certificates** to reverse this decision if necessary.

The Expressway-E needs to trust these CAs so that it can authenticate the server certificates from Collaboration Cloud, to make the encrypted connections needed by some Expressway-based hybrid services.

Note The Expressway-E cannot register for hybrid services. It must be connected by a secure traversal zone to the Expressway (or cluster) that is registered to the Cisco Webex cloud.

Root certificates from the following CAs will be installed when you click **Get certificates**:

- O=The Go Daddy Group, Inc., OU=Go Daddy Class 2 Certification Authority
- O=GoDaddy.com, Inc., CN=Go Daddy Root Certificate Authority - G2
- O=QuoVadis Limited, CN=QuoVadis Root CA 2
- O=VeriSign, Inc., OU=Class 3 Public Primary Certification Authority
- O=thawte, Inc., OU=Certification Services Division, OU=(c) 2006 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA
- O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
- O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA

If you prefer to manually maintain the trusted CA list, go to **Maintenance** > **Security** > **Trusted CA certificate** page. See Managing the Trusted CA Certificate List for more help.

Related Reading

- Cisco Webex Signing CAs
- Supported Certificate Authorities for Cisco Webex

Cisco Webex Edge

Using Webex Edge Connect - and no Expressway-C

For business to business cases (not for MRA) from X12.5.5 we successfully tested using Cisco Webex Edge Audio with the Webex Edge Connect product, and without an Expressway-C. So Expressway-E connects to Cisco Unified Communications Manager without Expressway-C. No traversal or firewall is required for this scenario, and Expressway E connects the Webex Cloud directly to Cisco Unified Communications Manager. The tested configuration uses standard Webex Edge Audio over the internet, with a Neighbor zone between Cisco Unified Communications Manager and Expressway -E. The Webex zone media encryption mode needs to be “On” (the default is “Auto”).

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