Chat and Presence Federation Using Expressway Deployment Guide (X14.0.2)

First Published: 2021-07-22

CONTENTS

CHAPTER 4 **XMPP Federation through IM and Presence Service** **27**

CHAPTER 5 **IM and P Federation with Microsoft-Based Organizations** **29**

Preface

- Change History, on page 1

Change History

Table 1: Deployment Guide Change History

Date	Change	Reason
July 2021	Updated the section on "Where to Find Information".	Publishing the guide for X14.0.2 release.
December 2019	Remove inactive link to TechZone article.	Correction
September 2019	• Correct configuration summary for Microsoft federations. • Clarify high-level configuration requirements. • Updated software version from X8.11.1 to X8.11.4.	Clarification
September 2018	• Clarify routing behavior for NOTIFY messages in IM and P Federation with Microsoft-Based Organizations. • Updated software version from X8.11 to X8.11.1, as version X8.11 is no longer available.	Clarification Software withdrawn

Date	Change	Reason
July 2018	• Remove port reference information. Clarified information about self-signed certificates. Remove (duplicate) information about IM and Presence Service federations. Added IM&P federation with Microsoft. Updated troubleshooting to clarify no dynamic move of users between IM&P nodes on failover. • Combined VCS and Expressway versions of document. • Renamed document from "*Cisco Unified Communications XMPP Federation*" to "*Chat and Presence Federation Using Cisco Expressway*".	X8.11.x release and document reorganization
July 2017	Updated prerequisites and document layout.	X8.10 release
November 2015	New template applied.	X8.7 release
December 2014	First release of document.	

CHAPTER 2

Introduction

- Introduction, on page 3

Introduction

This Expressway guide also now applies to VCS. Any VCS-specific information is noted where necessary in the guide. (Older VCS guides on Cisco.com are still valid for the VCS versions they apply to-as specified on the title page of each guide.)

The guide describes how to configure external XMPP federation from an on-premise IM and Presence Service server through Cisco Expressway or through the IM and Presence Service. It also summarizes how to federate an IM and Presence Service deployment, using SIP, with organizations that have Microsoft as their UC/collaboration solution. In the context of this guide, "federation" means to connect users in two or more organizations using collaboration technologies.

Expressway or IM and Presence Service for XMPP Federation - How to Decide

The table outlines which features are supported by Expressway and IM and Presence Service respectively. It may help you to decide which is the most suitable XMPP federation deployment option.

⚠️

Caution   If you deploy external XMPP federation through Expressway, do not activate XMPP federation on IM and Presence Service. Or if you opt for XMPP federation through IM and Presence Service, do not activate XMPP federation on Expressway.

Table 2: Feature comparison by deployment option

Feature	Expressway	IM and Presence Service
Email address translation	No	Yes
Multiple clusters	No (single cluster only)	Yes
Static routes	Yes	No
Internal federation	No	Yes

Feature	Expressway	IM and Presence Service
External federation terminated from DMZ	Yes	No
Dual federation (internal and external)	No	Yes (external federation not terminated from DMZ)
Managed file transfer and peer-to-peer file transfer	No	Yes

Terminology

Note Do not use the domain names and other example values from this document in your test or production deployments. You must change the example values to represent your own environment.

- *Federation*: Connecting users in two or more organizations using collaboration technologies.

- *Our organization*: An organization using on-premises collaboration infrastructure to federate with other organizations.

- *Traversal server / client zones*: Special zones on the Expressway-E and Expressway-C that enable the pair to traverse calls across firewalls. You can use Unified Communications zones instead.

- *Outbound* and *Inbound*: Generally, calls initiated from inside our organization's network to another organization or remote user are Outbound. Calls initiated from outside our organization's network, to users or spaces in our network, are Inbound.

Where to Find Information

For instructions about configuring XMPP federation on IM and Presence Service through Cisco Expressway, use this guide.

For instructions about configuring XMPP federation through the IM and Presence Service, use the Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager guide.

For information on "IM and Presence Service Configuration for SIP Open Federation" feature support, see "*IM and Presence Service Configuration for SIP Open Federation*" chapter of the Interdomain Federation Guide for the IM and Presence Service, Release 14.

If you deploy IM and Presence Service federation with Microsoft-based organizations, Microsoft documentation on Skype for Business PowerShell cmdlets is available here: https://docs.microsoft.com/en-us/

XMPP Federation through Expressway

XMPP Federation through Expressway

External XMPP federation enables users registered to Cisco Unified Communications Manager IM and Presence Service, to communicate via the Expressway-E with users from a different XMPP deployment.

Note This section describes XMPP federation as managed through Expressway, but it can also be managed through the IM and Presence Service, as described later in this guide.

The diagram shows XMPP message routing from the on-premises IM & Presence server, through the Expressway-C and Expressway-E Collaboration Edge solution, to the federated XMPP server. It also shows the ports and connections as the messages traverse DMZ firewalls. The "example.com" organization is using an Expressway federation model (left of picture), while the "federated.com" organization (right of picture) is using an IM and Presence Service in DMZ federation model.

Figure 1: Message routing for XMPP federation
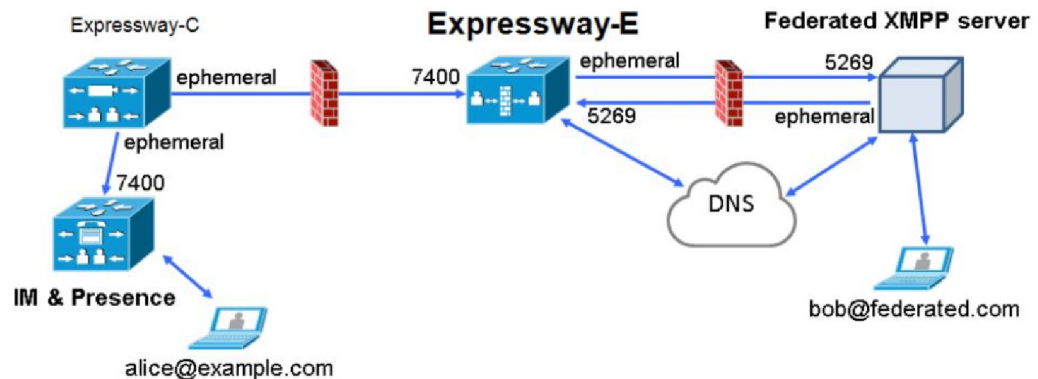
Supported Systems XMPP through Expressway

Expressway-E supports XMPP federation with the following products:

- Expressway X8.2 or later

- Cisco Unified Communications Manager IM and Presence Service 9.1.1 or later

- Cisco Webex Connect Release 6.x

- Cisco Jabber 9.7 or later

- Other XMPP standards-compliant servers

Limitations

- When using Expressway for XMPP federation, the Expressway-E handles the connection to the remote federation server and can only use Jabber IDs to manage XMPP messages. Expressway-E does not support XMPP address translation (of email addresses, for example).

  If you, as an external user, try to chat with a user in an enterprise through federation, you must use the enterprise user's Jabber ID to contact them through XMPP. If their Jabber ID does not match their email address (especially if their Jabber ID uses an internal user ID or domain) you are unable to have federation, as you won't know the enterprise user's email address. We therefore recommend that enterprises configure their Unified CM nodes to use the same address for a user's Jabber ID and email when using Expressway for XMPP federation. This limitation does not apply to users contacting each other within the enterprise (not using federation) even when federation is handled by Expressway-E. You can configure IM and Presence Service to use either the Jabber ID or the Directory URI (typically email) for non-federated use cases.

  To make a user's Jabber ID resemble a user's email address, so that the federated partner can approximate email addresses for federation, set the following:

  1. Unified CM Lightweight Directory Access Protocol (LDAP) attribute for User ID to be the user's sAMAccountName

  2. IM and Presence Service presence domain to be the same as the email domain.

  3. Your email address to the same as samaccountname@presencedomain.

- Simultaneous internal federation managed by IM and Presence Service and external federation managed by Expressway is not supported. If only internal federation is required then you must use interdomain federation on IM and Presence Service. The available federation deployment configuration options are:

  - External federation only (managed by Expressway).

  - Internal federation only (managed by IM and Presence Service).

  - Internal and external federation managed by IM and Presence Service but requires you to configure your firewall to allow inbound connections.

Prerequisites

- Interdomain XMPP Federation must be **disabled** on the IM and Presence Service before you enable XMPP federation on Expressway:

  Go to **Cisco Unified CM IM and Presence Administration** > **Presence** > **Inter Domain Federation** > **XMPP Federation** > **Settings** and ensure that **XMPP Federation Node Status** is set to *Off*.

- XMPP federation is only supported on a single Expressway cluster.

- An Expressway-C (cluster) and Expressway-E (cluster) must be configured for Mobile and Remote Access (MRA) to Unified Communications services, as described in the *Mobile and Remote Access via Cisco Expressway Deployment Guide*. If only XMPP federation is required (video calls and remote registration to Unified CM are not required), these items do not have to be configured:

  - Domains that support *SIP registrations and provisioning on Unified CM* or that support *IM and Presence services on Unified CM*

  - Unified CM servers (you must still configure the IM&P servers)

  - HTTP server allow list

  > **Note**   The Federated communications are available to both on-premises clients (connected directly to IM and Presence Service) and off-premises clients (connected to IM and Presence Service through MRA).

- SIP and XMPP federations are separate and do not impact on each other. For example, it's possible to deploy SIP federation on IM and Presence Service and external XMPP federation on Expressway.

- If you deploy external XMPP federation through Expressway, do not activate the Cisco XCP XMPP federation Connection Manager feature service on the IM and Presence Service.

- If you intend to use both Transport Layer Security (TLS) and group chat, the Expressway-C and Expressway-E server certificates must include in their list of subject alternate names the **Chat Node Aliases** that are configured on the IM and Presence Service servers. Use either the XMPPAddress or DNS formats.

  > **Note**   The Expressway-C automatically includes the chat node aliases in its certificate signing requests (CSRs), providing it has discovered a set of IM and Presence Service servers.

  When generating CSRs for the Expressway-E we recommend that you copy-paste the chat node aliases from the equivalent **Generate CSR** page on the Expressway-C. For details, see Server Certificate Requirements for Unified Communications.

Task Flow for XMPP Federation through Expressway

This table outlines the tasks required to deploy XMPP federation on Expressway:

Task	See
Validate email addresses for federation	XMPP Federation through Expressway
Ensure IM and Presence Service is operational and has XMPP federation turned off	XMPP Federation through Expressway
Complete Server Certificate Requirements	Server Certificate Requirements for Unified Communications
Configure the local domains for XMPP federation on Expressway-C	Configuring Expressway for External XMPP Federation
Configure Expressway-E for XMPP federation	Configuring Expressway for External XMPP Federation
Configure how XMPP servers for federated domains and chat node aliases are located using either DNS lookups or static routes	Configuring Expressway for External XMPP Federation
Configure the allow and deny lists for federated domains and chat node aliases	Configuring Expressway for External XMPP Federation
Publish DNS SRV records for XMPP federation (if not using static routes)	DNS SRV Records for XMPP Federation
Check that the correct firewall ports are open	See the *Cisco Expressway IP Port Usage Configuration Guide*, for your version, on the Cisco Expressway Series Configuration Guides page.
Check the status of XMPP federation	Checking XMPP Federation Status, on page 20
To troubleshoot your connection	Troubleshooting External XMPP Federation

Server Certificate Requirements for Unified Communications

Cisco Unified Communications Manager Certificates

Two Cisco Unified Communications Manager certificates are significant for Mobile and Remote Access:

- *CallManager* certificate

- *tomcat* certificate

These certificates are automatically installed on the Cisco Unified Communications Manager and by default they are self-signed and have the same common name (CN).

We recommend using CA-signed certificates. However, if you do use self-signed certificates, the two certificates must have different common names. The Expressway does not allow two self-signed certificates with the same CN. So, if the *CallManager* and *tomcat* self-signed certificates have the same CN in the Expressway's trusted CA list, the Expressway can only trust one of them. This means that either secure HTTP or secure SIP, between Expressway-C and Cisco Unified Communications Manager, will fail.

Also, when generating *tomcat* certificate signing requests for any products in the Cisco Collaboration Systems Release 10.5.2, you need to be aware of CSCus47235. You need to work around this issue to ensure that the FQDNs of the nodes are in the certificates as Subject Alternative Name (SAN) entries. The *Expressway X8.5.3 Release Note* on the Release Notes page has details of the workarounds.

IM and Presence Service Certificates

Two IM and Presence Service certificates are significant if you use XMPP:

- *cup-xmpp* certificate
- *tomcat* certificate

We recommend using CA-signed certificates. However, if you do use self-signed certificates, the two certificates must have different common names. The Expressway does not allow two self-signed certificates with the same CN. If the *cup-xmpp* and *tomcat* (self-signed) certificates have the same CN, Expressway only trusts one of them, and some TLS attempts between Cisco Expressway-E and IM and Presence Service servers will fail. For more details, see CSCve56019.

Expressway Certificates

The Expressway certificate signing request (CSR) tool prompts for and incorporates the relevant Subject Alternative Name (SAN) entries as appropriate for the Unified Communications features that are supported on that Expressway.

The following table shows which CSR alternative name elements apply to which Unified Communications features:

Add these items as subject alternative names	When generating a CSR for these purposes			
	Mobile and Remote Access	**Jabber Guest**	**XMPP Federation**	**Business to Business Calls**
Unified CM registrations domains (despite their name, these have more in common with service discovery domains than with Unified CM SIP registration domains)	Required on Expressway-E only	-	-	-
XMPP federation domains	-	-	Required on Expressway-E only	-
IM and Presence chat node aliases (federated group chat)	-	-	Required	-
Unified CM phone security profile names	Required on Expressway-E only	-	-	-

(Clustered systems only) Expressway cluster name	Required on Expressway-E only	Required on Expressway-E only	Required on Expressway-E only	-

Note

- You may need to produce a new server certificate for the Expressway-C if chat node aliases are added or renamed. Or when IM and Presence nodes are added or renamed, or new TLS phone security profiles are added.

- You must produce a new Expressway-E certificate if new chat node aliases are added to the system, or if the Unified CM or XMPP federation domains are modified.

- You must restart the Expressway for any new uploaded server certificate to take effect.

More details about the individual feature requirements per Expressway-C / Expressway-E are described below.

Expressway-C Server Certificate Requirements

The Expressway-C server certificate needs to include the following elements in its list of subject alternate names:

- **Unified CM phone security profile names**: The names of the **Phone Security Profiles** in Unified CM that are configured for encrypted TLS and are used for devices requiring remote access. Use the FQDN format and separate multiple entries with commas.

  Having the secure phone profiles as alternative names means that Unified CM can communicate via TLS with the Expressway-C when it is forwarding messages from devices that use those profiles.

- **IM and Presence chat node aliases (federated group chat)**: The **Chat Node Aliases** (e.g. chatroom1.example.com) that are configured on the IM and Presence servers. These are required only for Unified Communications XMPP federation deployments that intend to support group chat over TLS with federated contacts.

  The Expressway-C automatically includes the chat node aliases in the CSR, providing it has discovered a set of IM&P servers.

  We recommend that you use DNS format for the chat node aliases when generating the CSR. You must include the same chat node aliases in the Expressway-E server certificate's alternative names.

Figure 2: Entering subject alternative names for security profiles and chat node aliases on the Expressway-C's CSR generator

Expressway-E Server Certificate Requirements

The Expressway-E server certificate needs to include the following elements in its list of subject alternative names (SAN):

- **Unified CM registrations domains**: All the domains which are configured on the Expressway-C for Unified CM registrations. Required for secure communications between endpoint devices and Expressway-E.

  The Unified CM registration domains used in the Expressway configuration and Expressway-E certificate, are used by Mobile and Remote Access clients to lookup the `_collab-edge` DNS SRV record during service discovery. They enable MRA registrations on Unified CM and are primarily for service discovery.

  These service discovery domains may or may not match the SIP registration domains. It depends on the deployment, and they don't have to match. One example is a deployment that uses a .local or similar private domain with Unified CM on the internal network, and public domain names for the Expressway-E FQDN and service discovery. In this case, you need to include the public domain names in the Expressway-E certificate as SANs. There is no need to include the private domain names used on Unified CM. You only need to list the edge domain as a SAN.

  Select the *DNS* format and manually specify the required FQDNs. Separate the FQDNs by commas if you need multiple domains. You may select *CollabEdgeDNS* format instead, which simply adds the prefix `collab-edge.` to the domain that you enter. This format is recommended if you do not want to include your top-level domain as a SAN (see example in following screenshot).

- **XMPP federation domains**: The domains used for point-to-point XMPP federation. These are configured on the IM&P servers and should also be configured on the Expressway-C as domains for XMPP federation.

  Select the *DNS* format and manually specify the required FQDNs. Separate the FQDNs by commas if you need multiple domains. Do not use the *XMPPAddress* format as it may not be supported by your CA and may be discontinued in future versions of the Expressway software.

- **IM and Presence chat node aliases (federated group chat)**: The same set of **Chat Node Aliases** as entered on the Expressway-C's certificate. They are only required for voice and presence deployments which will support group chat over TLS with federated contacts.

Note	You can copy the list of chat node aliases from the equivalent **Generate CSR** page on the Expressway-C.

Figure 3: Entering subject alternative names for Unified CM registration domains, XMPP federation domains, and chat node aliases, on the Expressway-E's CSR generator

See *Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway Configuration Guides page.

Configuring Expressway for External XMPP Federation

This section describes how to configure the Expressway for external XMPP federation.

Before You Begin

1. Make sure that the items specified in "Prerequisites" are complete.

2. Some supporting systems configuration needs to be in place:

    a. DNS. An internal DNS configured with forward and reverse lookups for Expressway-E, Expressway-C.

    b. External DNS. An external DNS configured with forward lookup for the Expressway-E cluster FQDN.

    c. Traversal Zones. A traversal server zone (Expressway-E) and a traversal client zone (Expressway-C).

    d. NTP. All servers must be internally synchronized to the same time source.

Configuring Local Domains for XMPP Federation on Expressway-C

You must configure the local domain names for which you want to provide XMPP federated services.

Step 1   On Expressway-C, go to **Configuration** > **Domains**.

Step 2   Click **New** (or click **View/Edit** if the required domain already exists).

Step 3   Enter your local `Domain name` to be federated.

Step 4   Set **XMPP federation** to *On*.

Step 5   Click **Save**.

Step 6   Repeat for any other local domains requiring federation.

Note	• A single Expressway cluster can support multiple IM and Presence Service clusters using the same presence domain.
	• XMPP federation of multiple IM and Presence Service clusters with multiple Expressway clusters is not supported.
	• Each IM and Presence Service cluster needs to be discovered by Expressway-C.

Configuring Expressway-E for XMPP Federation

We recommend that XMPP federation configuration changes are made "out of hours". Enabling XMPP federation will restart the XCP router on all Expressway-E systems within the cluster. This will temporarily interrupt any existing mobile and remote access IM&P client sessions. Depending on the number of clients, full client reconnection may take several minutes. (See Impact of Configuration Changes on a Live System for more information.)

Step 1   On Expressway-E, go to **Configuration** > **Unified Communications**.

Step 2   Set **XMPP federation support** to *On*.

When you apply this change, you may need to restart the XCP Routers on the IM&P server(s). The other settings on this page do not require a restart.

Step 3   Configure the remaining fields as described in the table below.

Step 4   Click **Save**.

Your changes are applied. If you toggled **XMPP federation support**, you will be required to confirm that you want to restart the XCP router on the Expressway-C.

You may also need to restart the Unified CM IM&P XCP router services that are connected to the associated Expressway-C.

Step 5   Log on to each IM and Presence server to check for notifications that you need to restart the XCP Routers. If you do need to restart them:

    a)   In **Cisco Unified IM and Presence Serviceability**, go to **Tools** > **Control Center - Network Services**.

    b)   Scroll down to the **IM and Presence Services** section and select **Cisco XCP Router**.

    c)   Click **Restart**.

This causes a restart of all XCP services on the IM and Presence Service. The service restart may take several minutes.

d) Repeat on each IM and Presence server.

You could use the **utils service** CLI option (accessed via the Cisco Unified IM and Presence Operating System) to restart the services instead.

Table 3: Settings for XMPP Federation

Settings	Description
Use static routes	Indicates whether a controlled list of static routes are used to locate the federated XMPP domains and chat node aliases, rather than DNS lookups. See Configuring How XMPP Servers for Federated Domains and Chat Node Aliases Are Located.
Dialback secret	Enter the dialback secret to use for identity verification with federated XMPP servers. If you have multiple Expressway-E systems in the same deployment, they must all be configured with the same dialback secret. For more information about server dialback, see http://xmpp.org/extensions/xep-0220.html
Security mode	Indicates if a TLS connection to federated XMPP servers is required, preferred, or not required. • *TLS required*: The system guarantees a secure (encrypted) connection with the foreign domain. • *TLS optional*: The system attempts to establish a TLS connection with the foreign domain. If it fails to establish a TLS connection, it reverts to TCP. • *No TLS*: The system will not establish a TLS connection with the foreign domain. It uses a non-encrypted connection to federate with the foreign domain. In all cases, server dialback is used to verify the identity of the foreign server. The foreign server must be configured to use server dialback. **Note** SASL External is not a supported configuration on the local server. Foreign servers may be configured to use SASL, but SASL exchanges will not be supported by the local server. The default, and recommended setting, is *TLS required*.

Settings	Description
Require client-side security certificates	Controls whether the certificate presented by the external client is verified against the Expressway's current trusted CA list and, if loaded, the revocation list.
	This setting does not apply if **Security mode** is *No TLS*.
	Note The federated domain name and any chat node aliases must be present in the certificate's subject alternate name, regardless of this setting.
Privacy mode	Controls whether restrictions are applied to the set of federated domains and chat node aliases.
	• *Off*: No restrictions are applied.
	• *Allow list*: Federation is allowed only with the domains and chat node aliases specified in the allow list.
	• *Deny list*: Federation is allowed with any domain or chat node alias except for those specified in the deny list.
	Note Any domains or chat node aliases that are configured as static routes are included automatically in the allow list.
	The default is *Allow list*.
	See Configuring the Allow and Deny Lists for Federated Domains and Chat Node Aliases.

Configuring How XMPP Servers for Federated Domains and Chat Node Aliases Are Located

You can use DNS lookups to locate the XMPP servers for federated domains and chat node aliases, or you can configure the addresses of specific XMPP servers.

To Use DNS Lookups

Step 1   On Expressway-E, go to **Configuration** > **Unified Communications**.

Step 2   Set **Use static routes** to *Off*.

Step 3   Click **Save**.

> **Note**   All XMPP federated partners must publish in DNS the addresses of their XMPP servers as described in DNS SRV Records for XMPP Federation, on page 19.

To Use Static Routes

Step 1   Contact the partners with whom you are federating to get a list of their chat node aliases.

Step 2   On Expressway-E, go to **Configuration** > **Unified Communications**.

Step 3   Set **Use static routes** to *On* and click **Save**.

Step 4   Click **Configure static routes for federated XMPP domains**.

Step 5   On the **Federated static routes** page, click **New**.

Step 6   Enter the details of the static route:

Field	Description
Domain	The federated XMPP domain or chat node alias.
Address	The IP address or Fully Qualified Domain Name (FQDN) of an XMPP server for this federated domain or chat node alias.

Step 7   Click **Save**.

Step 8   Add as many additional static routes as required.

You can specify additional routes to alternative addresses for the same domain or chat node alias (all routes have an equal priority).

Note	• If there are no static routes defined for a federated domain or chat node alias, the system will use DNS instead.
	• If static routes are defined for the federated domain or chat node alias, but the remote system cannot be contacted over those routes, the system will not fall back to DNS.
	• If **Privacy mode** is set to *Allow list* and **Use static routes** is *On*, any domains (or chat node aliases) that are configured as static routes are included automatically in the allow list.

Configuring the Allow and Deny Lists for Federated Domains and Chat Node Aliases

The allow and deny lists are used to control restrictions to the set of federated domains and chat node aliases. If **Privacy mode** is set to *Allow list* or *Deny list*, you must add the domains and chat node aliases with which you want to allow or deny federated connections. This function manages restrictions at the domain / chat node alias level.

Individual user-based privacy is controlled by each client / end-user.

Allow list and deny list modes are mutually exclusive. A domain/alias cannot be allowed and denied at the same time.

When federation is first enabled, **Privacy mod**e is set to *Allow list* by default. In effect this puts the system in "lockdown" mode — you will not be allowed to connect with any federated domains or chat node aliases until you add them to the allow list, configure static routes, or change the **Privacy mode** setting.

Step 1   On Expressway-E, go to **Configuration** > **Unified Communications**.

Step 2   Set **Privacy mode** as appropriate:

- *Off*: No restrictions are applied.

- *Allow list*: Federation is allowed only with the domains and chat node aliases specified in the allow list.

- *Deny list*: Federation is allowed with any domain or chat node alias except for those specified in the deny list.

Step 3   Click **Save**.

Step 4   To manage the domains and chat node aliases in the allow or deny lists, click either **Federation allow list** or **Federation deny list** as appropriate.

In the resulting page you can add, modify, or delete the items in the allow/deny list. Wildcards or regexes are not allowed in the names; it must be an exact match.

Note   All domains and chat node aliases that are configured as static routes are included automatically in the allow list.

Delayed Cisco XCP Router Restart

The delayed Cisco XCP Router restart feature is part of Cisco Hosted Collaboration Solution (HCS) and is only available when the Expressway-E is in multitenant mode. The Expressway-E enters multitenant mode when you add a second Unified CM traversal zone with a new SIP domain.

Note   In multitenant mode, you must configure the system hostname on the **System** > **DNS** page of the Cisco Expressway-E to match the hostname configured in DNS (case-specific before X8.10.1, case insensitive from X8.10.1). Otherwise Cisco Jabber clients will be unable to register successfully for MRA.

Multitenancy allows a service provider to share an Expressway-E cluster among multiple tenants. Each tenant has a dedicated Expressway-C cluster that connects to the shared Expressway-E cluster.

Certain configuration changes on the Expressway-E cluster, or a customer's Expressway-C cluster, require a restart of the Cisco XCP Router on each Expressway-E in the shared cluster. The restart is required for Cisco XCP Router configuration changes to take effect across all nodes in a multitenant Expressway-E cluster. The restart affects all users across all customers.

To reduce the frequency of this restart, and the impact on users, you can use the delayed Cisco XCP Router restart feature.

Note   Without the delayed restart feature enabled, the restart happens automatically and occurs each time you save any configuration change that affects the Cisco XCP Router. If multiple configuration changes are required, resulting in several restarts of the Cisco XCP Router, it can adversely affect users. We strongly recommend that multitenant customers enable the delayed Cisco XCP Router restart feature.

The delayed restart feature lets you control when the restart takes place. You can make a batch of configuration changes - followed by a single Cisco XCP Router restart – and apply all the changes at once. A delayed restart

generates the latest configuration and performs a Cisco XCP Router restart on each node in the multitenant Cisco Expressway-E cluster.

When a restart of the Cisco XCP Router occurs, all XMPP clients (such as Cisco Jabber) across all customers go offline for a few minutes and then reconnect. Because of this impact, we recommend that you take advantage of the delayed restart capability.

Once enabled, you can carry out the restart manually or set it to be schedule-based. In either mode, you can initiate the restart at any time and the system determines which Cisco XCP Router instances require a restart, performing the restart only as needed. When you set the restart to be scheduled, the restart happens at the scheduled time, but again only as needed. We recommend doing the Cisco XCP Router restart during off-peak hours whenever possible.

Note
- Nodes on the latest configuration are not impacted. This action disconnects all external XCP-based users connected through the delayed nodes during the restart.

- All nodes will be on the latest configuration after the restart.

Important More information about multitenancy, see *Multitenancy with Cisco Expressway* on the Cisco Hosted Collaboration Solution page.

How to Configure Delayed Restarts

Use the following methods to configure delayed restarts.

To Configure the Delayed Cisco XCP Router Restart

Step 1 Go to **Configuration** > **Unified Communications** > **Delayed Cisco XCP Router restart**.

Step 2 Under **Configuration**, turn **Delayed Cisco XCP Router restart** *On*.

Step 3 If you do not enable **Scheduled Restart,** you must initiate the restart manually using the **Restar**t button.

Configuration changes do not happen automatically.

To Schedule the Restart

Step 1 Under **Configuration**, turn **Scheduled Restart** *On* and set the time that all nodes in the multi-tenant Expressway-E cluster are updated each day. Only nodes that are not running on the latest configuration are impacted.

Step 2 Set the time that the restart takes place each day using the **Scheduled restart time (UTC)** option.

Configuration Changes That Require a Restart of the Cisco XCP Router

If you make any system configuration changes in the following areas a restart of the Cisco XCP Router takes place:

- XMPP federation

- Internal/external Ethernet

- Hostname or IP address

- DNS

- NTP

- Option keys

- QoS

- Clustering

- Zones

- MRA

- Domains

- Maintenance mode

- Cisco XCP Router delayed restart

- Cisco XCP Router / XMPP changes through networking

- Server-to-server communication to IM and Presence Service

- Changes to the logging flags for any of the above

☞

| Important | More information about configuration changes, see *Impact of Configuration Changes on a Live System* in the Cisco Unified Communications XMPP Federation guide. |

DNS SRV Records for XMPP Federation

If federating parties are not using static routes to access federated XMPP services, suitable DNS SRV records must be published.

_xmpp-server records

You must publish an **_xmpp-server** DNS SRV record in DNS for your local domain so that remote enterprises can access your federated XMPP services.

For example:

Domain	Service	Protocol	Priority	Weight	Port	Target host
ciscoexample.com	xmpp-server	tcp	0	0	5269	expe.ciscoexample.com

Similarly, to allow federating parties to discover a particular XMPP federated domain (if they are not using static routes), the federated enterprise must publish an **_xmpp-server** DNS SRV record in its public DNS server.

For example:

Domain	Service	Protocol	Priority	Weight	Port	Target host
federated.com	xmpp-server	tcp	0	0	5269	xmppserver.federated.com

All enterprises must publish the service on port 5269. The published FQDNs must also be resolvable in DNS to an IP address.

Group Chat

If you configure the Group Chat feature on a Unified CM IM&P server in an XMPP federation deployment, you must publish DNS SRV records for the federated chat node aliases.

To allow IM and Presence Service to discover a particular XMPP federated chat node alias, the federated enterprise must publish an `_xmpp-server` DNS SRV record in its public DNS server. Similarly, IM and Presence Service must publish the same DNS SRV record in DNS for its domain.

For example:

Domain	Service	Protocol	Priority	Weight	Port	Target host
chatroom1.example.com	xmpp-server	tcp	0	0	5269	expe.ciscoexample.com

Both enterprises must publish the service on port 5269. The published FQDN must also be resolvable to an IP address in DNS.

Alternatively, to use group chat aliases on federated servers, you can configure static routes on the Expressway-E (**Configuration** > **Unified Communications** > **Federated static routes**) for each chat node alias.

Note
- The chat node aliases are configured on Unified CM IM&P Administration (**Messaging** > **Group Chat Server Alias Mapping**).

- Internal users do not need to use DNS to discover chat nodes; they get the chat room details from their local IM&P servers.

- If you are using group chat over TLS, ensure that the Expressway-C and Expressway-E server certificate include in their list of subject alternate names (using either XMPPAddress or DNS formats) all of the Chat Node Aliases that are configured on the IM and Presence Service servers.

See "Chat configuration on IM and Presence" for more information about point-to-point instant messaging and group chat.

Checking XMPP Federation Status

XMPP federation status information is available on the Expressway-E only.

You can go to **Status** > **Unified Communications** to check the primary status of the XMPP federation service.

Normally, **XMPP Federation** should be Active.

If there are problems with the service, such as connectivity issues with the Expressway-C, the status will show as *Inactive*. In this case, you should also review the Unified Communications status page on the associated Expressway- C for more guidance as to what is causing the problem.

Viewing Federated Connections

To view the current federated connections being managed by the Expressway-E:

Step 1   On the Expressway-E, go to **Status** > **Unified Communications**.

Step 2   Click **View federated connections** in the **Advanced status information** section.

This shows all the current connections passing through that Expressway-E.

It displays the **IP Address** of the client, and the **Direction** (*Incoming* or *Outgoing*) of the communication.

Connections are closed after 10 minutes of inactivity.

Note   In clustered systems:

- An aggregated view is not displayed; only connections routed through the current peer are displayed.

- In 2-way connections, the inbound and outbound communications may be managed by different peers.

Troubleshooting External XMPP Federation

This section describes how to troubleshoot an external XMPP federation deployment and describes the impact of making configuration changes on a live system.

Checking System Status

If you encounter issues with the XMPP federation status service, check the **Status** > **Unified Communications** page on both the Expressway-C and the Expressway-E. This will highlight any basic connection or configuration problem and provide information and links to help correct the problem.

General Configuration Checklist

Ensure that the following Expressway configuration items are specified correctly:

- Port 5269 is open in both directions between the internet and Expressway-E in the DMZ.

- DNS settings: host name, domain name and default DNS server (**System** > **DNS**).

- An accessible NTP server (**System** > **Time**).

- An active Unified Communications traversal zone on the Expressway-C and its associated Expressway-E (**Status** > **Zones**).

- **Unified Communications mode** is set to *Mobile* and *remote access* on both the Expressway-C and the Expressway-E (**Configuration** > **Unified Communications** > **Configuration**).

- **XMPP federation support** is *On* on the Expressway-E (**Configuration** > **Unified Communications** > **Configuration**).

- If static routes are enabled, ensure that the appropriate routes for the federated XMPP domains have been added to the Expressway-E (**Configuration** > **Unified Communications** > **Federated static routes**).

- At least one domain is configured on the Expressway-C with **XMPP federation set** to *On* (**Configuration** > **Domains**).

- IM &Presence servers have been discovered on the Expressway-Cand have an active status (**Configuration** > **Unified Communications** > **IM and Presence servers**).

Discovery, Connectivity and Firewall Issues

Observe the following:

- If using DNS lookup, check that `_xmpp-server` public DNS records exist for the domains and chat node aliases of all federated parties, and that they use port 5269.

- Check that port 5269 is open in both directions between the internet and Expressway-E in the DMZ.

- If the Expressway-C cannot connect to XCP on the Expressway-E remote host:

    - Check that the firewall has not blocked port 7400.

    - If the Expressway-E is running dual network interfaces, ensure that the traversal zone on the Expressway-C is connected to the internally-facing interface on the Expressway-E.

- Be aware that inbound and outbound connections can be routed through different cluster peers.

- If the address of an IM and Presence Service node has changed, or a new peer has been added to an IM and Presence Service cluster, go to **Configuration** > **Unified Communications** > **IM and Presence Service** nodes and click **Refresh Servers**. You must then save the updated configuration.

- If an IM and Presence Service node fails over to a different node after an outage, the affected users **are not dynamically moved to the other node**. Expressway does not support this functionality, and it has not been tested.

Certificates and Secure TLS Connections

If you have configured secure TLS connections, ensure that:

- Valid server certificates are installed, they are in date and not revoked.

- Both the remote and local server certificates must contain a valid domain in the Subject Alternative Name (SAN). This applies even if **Require client-side security certificates** is disabled.

- If **Require client-side security certificates** is enabled, ensure that the server certificate is signed by a CA and is not locally signed.

- Certificate Authority (CA) certificates are installed.

- If you are using group chat over TLS, ensure that the Expressway-C and Expressway-E server certificates include in their list of subject alternate names (using either XMPPAddress or DNS formats) all of the **Chat Node Aliases** that are configured on the IM and Presence servers.

- Ensure that compatible security settings (TLS required, optional, no TLS) exist on your system and the remote federated system.

See Server Certificate Requirements for Unified Communications for more information.

Checking the Event Log

Check the Event Log on the Expressway-E for XMPP events.

Events related to XMPP federation are tagged with **Module="XMPPFederation"**. There are no XMPP-related logs on the Expressway-C.

Performing Diagnostic Logging

When performing diagnostic logging (**Maintenance** > **Diagnostics** > **Diagnostic logging**), set the **develop.xcp.federation** support log (**Maintenance** > **Diagnostics** > **Advanced** > **Support Log configuration**) to debug level.

Disabling Interdomain XMPP Federation on Unified CM IM&P

Before you begin

You must choose whether to enable Interdomain XMPP Federation on IM and Presence Service or on Expressway.

To disable Interdomain Federation on IM and Presence Service, perform the following operations in exactly the order shown:

Step 1   Disable Interdomain Federation on the IM&P servers:

    a) Go to **Cisco Unified CM IM and Presence Administration** > **Presence** > **Inter Domain Federation** > **XMPP Federation** > **Settings**.

    b) Set **XMPP Federation Node Status** to *Off*.

Step 2   Refresh the set of discovered IM&P servers on Expressway-C.

Step 3   Restart all of the Unified CM IM&P XCP Router services that are connected to that Expressway-C.

Impact of Configuration Changes on a Live System

In general, we recommend that XMPP federation configuration changes are made "out of hours". This section describes the impact that configuration changes will have on current clients using XMPP federation and any Jabber clients using mobile and remote access.

Expressway-C Configuration Changes

Domains

Any domain configuration changes, when one or more existing domains are configured for *IM and Presence services on Unified CM* or *XMPP Federation* will result in an automatic restart of the XCP router on both Expressway-C and Expressway-E.

The end-user impact is temporary loss of federation and any Jabber clients using mobile and remote access will be temporarily disconnected. The clients will automatically reconnect after a short period.

Unified Communications mode

Setting the **Unified Communications mode** to *Off* or to *Jabber Guest services'* will stop the XCP router on both Expressway-C and Expressway-E.

- This will remove the Expressway-E XMPP federation node from all discovered IM&P servers. A notification will appear on the IM&P administration interface to restart the XCP router on all affected IM&P nodes.

- The end-user impact is that all IM&P sessions will be disconnected. That is, there is a loss of federation, IM&P sessions over mobile and remote access will be disconnected, and sessions directly homed on the IM&P node will be dropped. When the XCP router is restarted on each IM&P node, all XCP functionality on that node will be disrupted.

Discovered IM & Presence Servers

Adding or deleting an IM & Presence publisher will require a restart of the XCP router on each IM & Presence node associated with that publisher only if **XMPP Federation** is enabled.

- This will cause a restart of the XCP router on Expressway-C.

- The end-user impact should be minimal. They will be unable to send or receive IM & Presence updates for a few seconds.

Expressway-E Configuration Changes

Unified Communications Mode

Setting the **Unified Communications mode** to *Off* or to *Jabber Guest services'* will stop the XCP router on both Expressway-C and Expressway-E.

- This will remove the Expressway-E XMPP federation node from all discovered IM&P servers. A notification will appear on the IM&P administration interface to restart the XCP router on all affected IM&P nodes.

- The end-user impact is that all IM&P sessions will be disconnected. That is, there is a loss of federation, IM&P sessions over mobile and remote access will be disconnected, and sessions directly homed on the IM&P node will be dropped. When the XCP router is restarted on each IM&P node, all XCP functionality on that node will be disrupted.

Note Turning the **Unified Communications Mode** back to *On* will reinsert the XMPP federation node and have the same impact on the IM&P servers.

XMPP Federation Support

Changing the **XMPP federation support** setting will restart the Expressway-E XCP router.

- This will result in the addition/removal of the Expressway-E XMPP federation node from all discovered IM & Presence servers. A notification will appear on the IM&P administration interface to restart the XCP router on all affected IM&P nodes.

- The end-user impact is that all IM&P sessions will be disconnected. That is, there is a loss of federation, IM&P sessions over mobile and remote access will be disconnected, and sessions directly homed on the IM&P node will be dropped. When the XCP router is restarted on each IM&P node, all XCP functionality on that node will be disrupted.

Other XMPP Federation Settings

Changing any of the other XMPP federation settings, such as static routes, security and privacy settings, or the allow/deny lists, will only result in a restart of the XMPP Federation Connection Manager service on the Expressway- E.

End-users may notice a temporary disruption to federation; any mobile and remote access IM&P sessions will remain connected.

Client Reconnection Times After Loss of Service

The time taken for a client to reconnect to the XMPP service depends on the re-login limits specified in the **Cisco Server Recovery Manager** service parameters on the IM&P server.

See the *High Availability Client Login Profiles* section in Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager for the IM&P version that you are running.

Temporary or Partial Loss of IM and Presence Service Federation

XMPP federation for IM and Presence Service via Expressway relies on a persistent TCP connection to the federated server. If a federated server becomes unavailable due to a graceful shutdown, Expressway will immediately seek to reestablish a connection with the federated server or with another server advertised by the federated partner.

If, however, the federated server fails abruptly, it can take up to 15 minutes for Expressway to discover the TCP connection outage and attempt reconnection. During this time, a partial or full loss of IM and Presence Service connectivity with the federated partner may occur.

XMPP Federation through IM and Presence Service

XMPP Federation through IM and Presence Service

This federation enables IM and Presence Service users in one enterprise domain to exchange presence information and Instant Messaging (IM) with users in external domains. This scenario does not involve Expressway.

👉

Important This section only provides summary information. For configuration information and other details about deploying XMPP federation managed by IM and Presence Service, see Interdomain Federation on IM and Presence Service for Cisco Unified Communications Manager.

Supported Systems XMPP through IM and P

IM and Presence Service, Release 9.1.1 or later, supports XMPP federation with the following enterprises:

- Cisco WebEx Messenger Release 7.x.

- Cisco Unified Presence Release 8.x.

- IM and Presence Service Release 9.x or later.

- Any other XMPP-standards compliant server.

Configuration Basics

IM and Presence Service does not support XMPP federation between an IM and Presence Service Release 9.x enterprise and a Cisco Unified Presence Release 7.x enterprise.

If you want to enable XMPP federation with an external domain, ensure that the external domain was not previously configured as a SIP federated domain on Cisco Unified Presence. An example of how to do this follows:

Example: A Cisco Unified Presence deployment with ciscoexample.com was historically configured as a SIP-based federation. But ciscoexample.com has now added XMPP support, so the local administrator now wants to enable an XMPP-based federation. To allow this, the administrator first deletes ciscoexample.com as a SIP-federated domain on Cisco Unified Presence.

When IM and Presence Service is federating with Cisco WebEx Enterprise, it's not possible for WebEx Connect client users to invite IM and Presence Service users to temporary or persistent chat rooms. This is due to a design constraint on the WebEx Connect client.

To allow the IM and Presence Service to federate over XMPP, you must enable and configure XMPP federation on IM and Presence Service.

If you have multiple IM and Presence Service clusters, you must enable and configure XMPP federation on at least one node per cluster. The XMPP federation configuration must be identical across clusters. The **Diagnostics Troubleshooter** compares the XMPP federation configuration across clusters, and reports if the XMPP federation configuration is not identical across clusters.

If you deploy Cisco Adaptive Security Appliance for firewall purposes, see the following topics in Interdomain Federation on IM and Presence Service for Cisco Unified Communications Manager:

- Topics related to integration preparation, for considerations on routing, scale, public IP addresses, and the Certification Authority.

- Task to configure the Cisco Adaptive Security Appliance, for information on configuring prerequisite information such as hostname, timezone, clock, and so on.

Task Flow Summary to Deploy XMPP Federation Through IM and Presence Service

Task
Configure IM and Presence Service for XMPP federation
Configure Security for XMPP federation
(Optional) Configure the email for federation feature
Turn on XMPP federation service
Configure the Cisco Adaptive Security Appliance for XMPP federation
Troubleshooting XMPP federation through IM and Presence Service

C H A P T E R 5

IM and P Federation with Microsoft-Based Organizations

- IM and P Federation with Microsoft-Based Organizations, on page 29

IM and P Federation with Microsoft-Based Organizations

Unlike the federations described elsewhere in this guide, these federations with Microsoft are SIP-based and not XMPP-based.

This section applies if you want to deploy an IM&P federation with an organization that uses Microsoft as its collaboration services solution. It enables users registered to Cisco Unified Communications Manager IM and Presence Service to exchange chat messages with Microsoft users in an external organization, via the Expressway. We illustrate an example deployment, the signaling connections, and some sample dial plan rules. For completeness, the diagrams illustrate multiple elements together, but in reality, most deployments will not have all the elements.

Fundamentals of IMP Federation with Microsoft-Based Organizations

Supported Systems IM and P through Microsoft

Expressway-E supports IM&P Federation with Microsoft, with the following products:

- Expressway X8.9 or later. X8.11.x or later is recommended.

- Cisco Unified Communications Manager IM and Presence Service 11.5(1)SU3 or later. 11.5(1)SU4 or later is recommended.

- Lync 2013 Server, Skype for Business Server, or Office 365. (We do not interoperate with "consumer" versions of Skype.)

Signaling and Dial Plan

Figure 4: Outbound Signaling
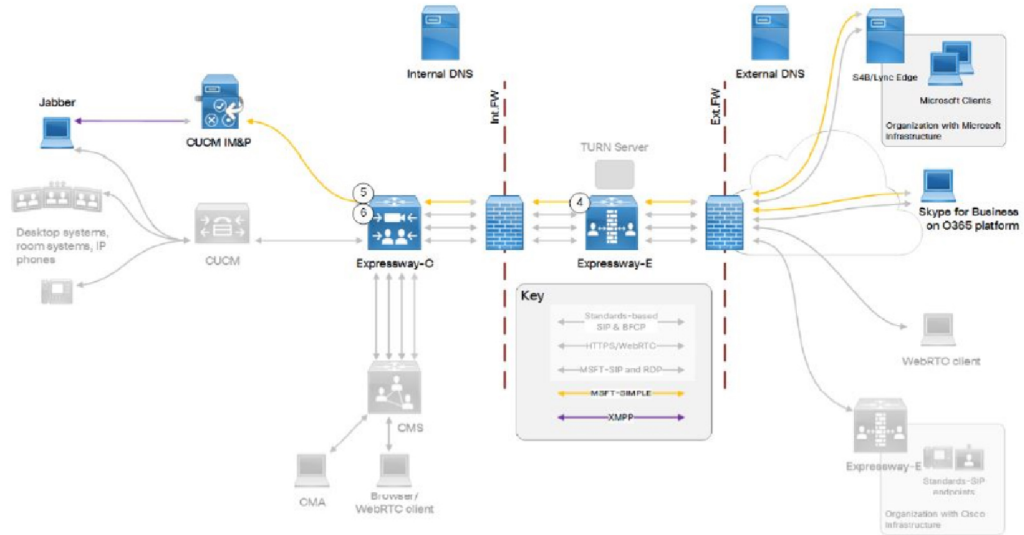
The table details the rules in a sample outbound dial plan.

Table 4: Sample Outbound Dial Plan Rules

Arrow #	Rule Hosted On	Rule Order/Priority	From	Pattern and Logic	To
1	Cisco Unified Communications Manager IM and Presence Service		Jabber	*@msexample.com	Static route to Expressway-C
2	Expressway-C		IM&P neighbor zone	*MicrosoftSIP IM&P* for .*@msexample\.com **On successful match** *Stop*	Traversal client zone
3	Expressway-E	Lowest priority rule = highest priority number	Traversal server zone	*Microsoft SIP IM&P for Any alias* **On successful match** *Stop* This rule is required due to the way we handle More About Configuring Search Rules on Expressway.	DNS zone

The figure illustrates Inbound Signaling.

Figure 5: Inbound Signaling

The table details the rules in a sample inbound dial plan.

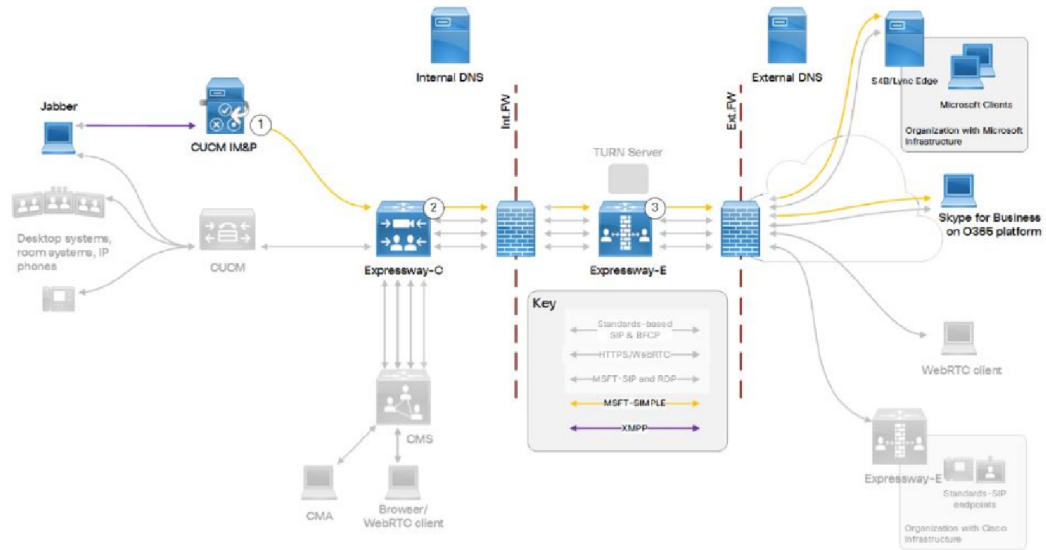*Table 5: Sample Inbound Dial Plan Rules*

Arrow #	Rule Owner	Rule Order/Priority	From	Pattern and Logic	To
4	On Expressway-E		Default zone	*Microsoft SIP IM&P* for .*@ciscoexample\.com **On successful match** *Stop*	Traversal server zone
5	On Expressway-C		Traversal client zone	*Microsoft SIP IM&P* for .*@ciscoexample\.com **On successful match** *Stop*	IM&P neighbor zone
6	On Expressway-C		Traversal client zone	*Microsoft SIP IM&P* for .*IMP1-public\.ciscoexample\.com.* **On successful match** *Stop* This rule is required due to the way we handle More About Configuring Search Rules on Expressway.	IM&P neighbor zone

Configuration Summary

This federation is based on TLS throughout.

Process Summary for Microsoft Federation

1. On the IM and Presence Service:

   a. As request messages for SIP federation are routed based on the FQDN, the FQDN of the routing IM and Presence Service node (publisher) must be publicly resolvable.

   b. Turn on SIP Federation services for each IM and Presence cluster node (enable *Cisco XCP SIP Federation Connection Manager*).

   c. Assign a DNS SRV record for IM and Presence, so that Microsoft entities can route traffic to the IM and Presence service through Expressway.

   d. Add a Federated domain entry for each Microsoft domain that you want to federate with (use the *OCS/Lync/S4B* integration type).

   e. Create a static route that points to the Expressway-C for all traffic matching each federated domain.

   For example, to route all traffic for *msexample.com*, use the format `.com.msexample.*`.

   Define TLS as the protocol, the next hop as the FQDN or IP address of the Expressway-C, the next hop port as 5061, and the route type as Domain.

   f. Add Expressway as a TLS peer subject, and then configure a TLS Context to include the new peer subject.

   g. Add inbound access control list (ACL) entries for each Expressway-C server IP address, so that the IM and Presence Service accepts unsolicited traffic from those IP addresses without authentication. For multicluster deployments, do this on each IM and Presence cluster.

   h. Restart the Cisco XCP Router.

   For detailed information about this process, see the Interdomain Federation Guide for the IM and Presence Service, Release 12.5(1) on Cisco.com - or the relevant guide for your software version if you are running an earlier version.

2. Configure Expressway for federation with Microsoft:

   a. On Expressway-C, configure a neighbor zone to the IM and Presence Service cluster. The Expressway-C zone configuration must point to the IM and Presence Service port for TLS Peer Authentication. By default, port 5062. (To confirm the relevant port - on Cisco Unified CM IM and Presence Administration, go to **System** > **Application Listeners** and navigate to **Default Cisco SIP Proxy TLS Listener - Peer Auth**.)

   b. Configure search rules to route NOTIFY messages (see below).

   c. Disable the Presence Server. Go to **Applications** > **Presence** and set **SIP SIMPLE Presence Server** to *Off*. In multicluster Expressway deployments, you need a neighbor zone and search rules for each cluster.

3. Exchange certificates between the various servers in your federation deployment. For details, see the "Exchange Certificates" section of the *Interdomain Federation Guide for the IM and Presence Service*.

More About Configuring Search Rules on Expressway

Usually NOTIFY messages do not need special routing consideration because they're in the same dialog as SUBSCRIBE messages sent between clients to request presence status and should follow the same route. However, Expressway does not hold information about SUBSCRIBE dialogs, so you need specific search rules to route the NOTIFY messages.

Process Summary

To create search rules, go to **Configuration** > **Dial Plan** > **Search Rules** and select **New**.

- **Outbound rule**: From X8.11.x, outbound NOTIFY messages are handled like any other SIP message. So, the outbound rule on Expressway-E needs to match the following (of course broader rules may be implemented, such as Traffic type = *All Sip Variants*):

    - Traffic type = *Microsoft IM and Presence*

    - Mode = *Any Alias*

    - Target = *DNS Zone* (Expressway-E)

- **Inbound rule**: You need an inbound search rule (on Cisco Expressway-C) to match on the **Federation Routing IM/P FQDN** of the IM and Presence Service cluster. This cluster-wide SIP proxy parameter is configured on the IM and Presence Service publisher at **System** > **Service Parameters** > **SelectPublisher** > **Cisco SIP Proxy** > **Federation Routing Parameters**. Here we use the example value **IMP1-public.ciscoexample.com** for the Federation Routing IM/P FQDN of the cluster.

    Also create a DNS A record so that Expressway-C can resolve the Federation Routing IM/P FQDN. This DNS A record must *not* have a pointer record (PTR) associated with it.

Dial Plan Summary

On the Expressway-E:

- Search rule to route Microsoft SIP IM&P for .*@msexample\.com from traversal server zone to DNS zone.

- Search rule to route Microsoft SIP IM&P for .*@ciscoexample\.com from default zone to traversal server zone.

On the Expressway-C:

- Search rule to route Microsoft SIP IM&P for the named federation domain .*@msexample\.com from IM&P neighbor zone to traversal client zone.

- Search rule to route Microsoft SIP IM&P for local domain .*@ciscoexample\.com from traversal client zone to IM&P neighbor zone.

- Our architecture requires this rule for presence: search rule to route Microsoft SIP IM&P from traversal client zone to IM&P neighbor zone. The rule must match a regular expression that includes the SIP Proxy service parameter **Federation Routing IM/P FQDN**, configured in the target IM and Presence Service cluster.

    For example, use .*IMP1-public\.ciscoexample\.com.* to match presence traffic for the FQDN given above.

Detailed Examples of Search Rules

Name	Py	Pcl	SIP variant	Source	RMBA?1 [1]	Mode	Pattern type	Pattern string	Behavior	On match	Target
IMP Public to IMP	20	SIP	MS IM&P	Any	No	Alias pattern match	Regex	.*imp1-public\uc\local.*	Leave	Stop	IMP
uc. local MSIMP to IMP	20	SIP	MS IM&P	Any	No	Alias pattern match	Regex	.*@uc\.local.*	Leave	Stop	IMP

[1] RMBA? = Request must be authenticated?

DNS Summary

This section provides summary information and examples about DNS records for this federation.

External DNS Records

The external DNS needs to be configured with the records required for your deployment. This table contains some example records that may apply:

Table 6: DNS Configuration Summary

Purpose	Record type	Example entry	Port	Resolves to target
Resolve Expressway-E cluster FQDN to peer IP addresses.	A/AAAA	`expe.example.com`	NA	Public IP address of one Expressway-E cluster peer. Create one record for each peer in the Expressway-E cluster (Up to 6 records).
Discover destination for calls to third party Microsoft infrastructure domain(outside of your control, but needs to be there for federation to succeed).	SRV	`_ sipfederationtls._ tcp. msb2bexample.com.`	5061	Public address of Microsoft Skype for Business Edge server / cluster

Purpose	Record type	Example entry	Port	Resolves to target
Discover user destination for calls from third party Microsoft infrastructure domain.	SRV	`_ sipfederationtls._ tcp.example.com.`	5061	FQDN of Skype for Business Edge. For example,`s4be.example.com`

Limitations Related to DNS

DNS Load Balancing by Microsoft Skype for Business (also applies to Microsoft Lync Server)

Microsoft Skype for Business does not attempt to use DNS SRV load balancing when routing calls or messages to federated domains. The Microsoft Skype for Business Edge servers always choose the DNS SRV record with the lowest priority and highest weight and ignore all others. When the priorities and weights are equal, they choose one and ignore all others.

Microsoft best practices recommend that you configure round-robin A/AAAA record load balancing, using the A record sip.domain.com. That is, the DNS SRV record for SIP federation should have only one entry that targets a single round-robin A/AAAA record that includes all of your Expressway-E cluster peers.

For example,

- Create the SRV record _sipfederationtls._tcp.ciscoexample.com. with a single entry targeting

  `sip.ciscoexample.com`

- Create an A/AAAA record for `sip.ciscoexample.com` that targets either the public IP address of the Expressway-E, or multiple A/AAAA records for round-robin service of all the Expressway-E peers in the cluster.

Domain Namespace Compatibility for Microsoft Skype for Business (also applies to Microsoft Lync Server)

Microsoft Skype for Business requires the federated edge servers to be in the same DNS namespace (domain/subdomain) as the federated SIP domain. Otherwise federation will fail without additional configuration on the Skype for Business servers. We recommend that the DNS SRV records for SIP federation resolve to a target in the same DNS namespace, so that open SIP federation will work from the Microsoft side without additional configuration.

For example, if you intend to federate Microsoft infrastructure with the domain **exp.ciscoexample.com**, you will create the SRV record **_sipfederationtls._tcp.exp.ciscoexample.com**. The target of that DNS SRV must be an A/AAAA record in the subdomain **exp.ciscoexample.com** (such as **sip.exp.ciscoexample.com**). If the DNS SRV target is outside that namespace, such as **sip.ciscoexample.com**, the Microsoft side will not allow the connection.

Internal DNS Records

If you can split your DNS to give different results internally, then we recommend that you create different records for the following purposes. These records must be resolvable by Expressway-C.

Table 7: DNS Configuration Summary

Purpose	Record type	Example entry	Resolves to
For Expressway-C to resolve the Federation Routing IM/P FQDN of the IM and Presence Service cluster.	A	`IMP1-public.ciscoexample.com`	IP address of the IM and Presence Service publisher