Cisco Unified Communications XMPP Federation

Deployment Guide

First Published: December 2014

Last Updated: October 2018

Cisco Expressway X8.10

IM and Presence Service 9.1.1 or later

Preface

Change History

Table 1 Deployment Guide Change History

Date	Change	Reason
October 2018	Clarify local domain must be configured for IM and Presence Service.	Clarification
March 2018	Updated Troubleshooting section to clarify no dynamic move of users between IM&P nodes if failover occurs.	
July 2017	Updated prerequisites section and documentation layout.	Republished for X8.10.
November 2015	New template applied.	Republished for X8.7.
December 2014	First release of document.	

Contents

Introduction

This deployment guide gives detailed instructions on configuring external XMPP federation from an on-premise IM and Presence Service Server through Cisco Expressway (Expressway) or, alternatively, through IM and Presence Service.

Deciding between Expressway or IM and Presence Service for XMPP Federation

The following table outlines features that are supported by Expressway and IM and Presence Service. Use this table to help you to decide on the most suitable XMPP federation deployment option to meet your needs.

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
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

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

How to use this Deployment Guide

For detailed instructions on configuring XMPP federation on IM and Presence Service via the Cisco Expressway solution, see Deploying Expressway for External XMPP Federation, page 8.

For detailed instructions on configuring XMPP federation via the IM and Presence Service option, see XMPP Federation through IM and Presence Service, page 25.

Related Documentation

You may require information contained in the following documents to set up your Unified Communications environment:

Cisco Expressway Administrator Guide

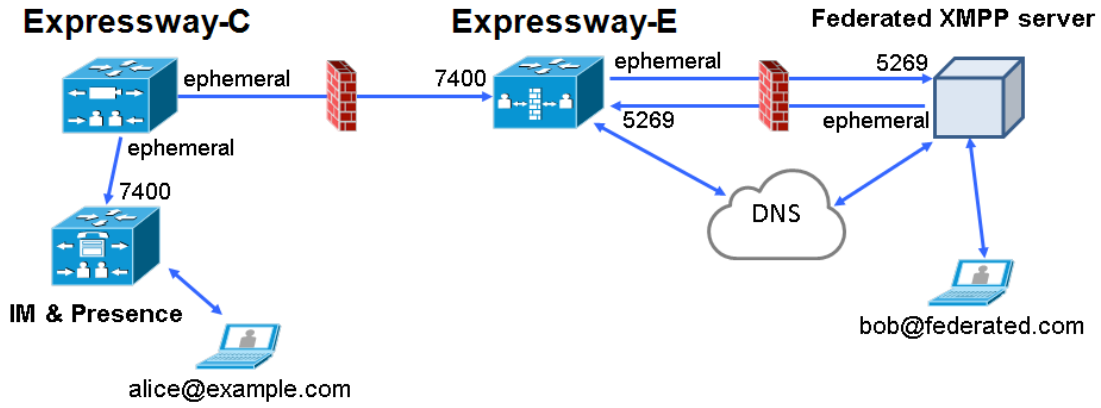
Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager.

Cisco VCS-Based XMPP Federation

Deploying Expressway for External XMPP Federation

External XMPP federation enables users registered to Unified CM IM & Presence to communicate via the Expressway-E with users from a different XMPP deployment.

The following diagram shows how XMPP messages are routed from your on-premises IM & Presence server via the Expressway-C and Expressway-E Collaboration Edge solution to the federated XMPP server. It also shows the ports and connections that are used as the messages traverse DMZ firewalls.



Please note the following:

- SIP and XMPP federations are separate and do not impact on each other. For example, it is 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 IM and Presence Service.

See *Cisco Unified Communications XMPP Federation using IM and Presence Service or Expressway* on the Expressway configuration guides page.

Supported Systems

- Expressway-Esupports XMPP federation with:
  - Expressway X8.2 or later.
  - Cisco Unified Communications ManagerIM and Presence Service 9.1.1 or later.
  - Cisco Jabber 9.7 or later.
  - Cisco Webex Connect Release 6.x.
  - Other XMPP standards-compliant servers.

Prerequisites

Before configuring your Expressway system for external XMPP federation:

- Ensure that you are running the following software versions:
  - Expressway X8.2 or later.
  - Unified CMIM and Presence Service 9.1.1 or later.

Note: XMPP federation can only be supported on a single Expressway cluster.

- Ensure that Interdomain XMPP federation has been **disabled** on Unified CMIM and Presence Service: Go to **Cisco Unified CM IM and Presence Service Administration > Presence > Inter Domain Federation > XMPP Federation > Settings** and ensure that **XMPP Federation Node Status** is set to *Off*.
- 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, attempt 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 the enterprise user's Jabber ID does not match their email address, especially if their Jabber ID uses an internal user ID or domain, you will be unable to have federation, as you will not know the enterprise user's email address. For this reason, we 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.

  Note: 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 such non-federated use cases.

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

  a. Setting the Unified CM Lightweight Directory Access Protocol (LDAP) attribute for User ID to be the user's sAMAccountName
  b. Setting the Unified CM IM and Presence Service presence domain to be the same as the email domain.
  c. Setting your email address so that it is the same as samaccountname@presencedomain.

- Simultaneous internal federation managed by Unified CM 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 Unified CM IM and Presence Service. The available federation deployment configuration options are:
  - External federation only (managed by Expressway).
  - Internal federation only (managed by Cisco Unified CM IM and Presence Service).
  - Internal and external federation managed by Cisco Unified CM IM and Presence Service, but requires you to configure your firewall to allow inbound connections.

  For more information, see Interdomain Federation on IM and Presence Service for Cisco Unified Communications Manager.
- 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 that 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. See Server Certificate Requirements for Unified Communications, page 12for more information.

For information about configuring your system for external XMPP federation, see:

- Configuring Expressway for External XMPP Federation, page 14
- DNS SRV Records for XMPP Federation, page 19
- Port usage for XMPP federation, page 20
- Checking XMPP federation status, page 20
-

Task Flow for XMPP Federation through Expressway

The below table outlines the tasks that need to be completed to successfully deploy XMPP federation on Expressway.

Task	See
Validate email addresses for federation	Deploying Expressway for External XMPP Federation, page 8
Ensure IM and Presence Service is operational and has XMPP federation turned off	Deploying Expressway for External XMPP Federation, page 8
Complete Server Certificate Requirements	Server Certificate Requirements for Unified Communications, page 12
Configure the local domains for XMPP federation on Expressway-C	Configuring Expressway for External XMPP Federation, page 14
Configure Expressway-E for XMPP federation	Configuring Expressway for External XMPP Federation, page 14
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, page 14
Configure the allow and deny lists for federated domains and chat node aliases	Configuring Expressway for External XMPP Federation, page 14
Publish DNS SRV records for XMPP federation (if not using static routes)	DNS SRV Records for XMPP Federation, page 19
Check that the correct firewall ports are open	Port usage for XMPP federation, page 20
Check the status of XMPP federation	Checking XMPP federation status, page 20
To troubleshoot your connection	Troubleshooting External XMPP Federation, page 21

Server Certificate Requirements for Unified Communications

Cisco Unified Communications Manager Certificates

The two Cisco Unified Communications Manager certificates that are significant for Mobile and Remote Access are the *CallManager* certificate and the *tomcat* certificate. These 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 for best end-to-end security between external endpoints and internal endpoints. However, if you do use self-signed certificates, the two certificates must have different common names. This is because the Expressway does not allow two self-signed certificates with the same CN. If the *CallManager* and *tomcat* self-signed certs have the same CN in the Expressway's trusted CA list, then it 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 within 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 Names. The *Expressway X8.5.3 Release Notes* have the details of the workarounds.

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-C only	–	–	–
(Clustered systems only) Expressway cluster name	Required on Expressway-C only	Required on Expressway-C only	Required on Expressway-C 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:

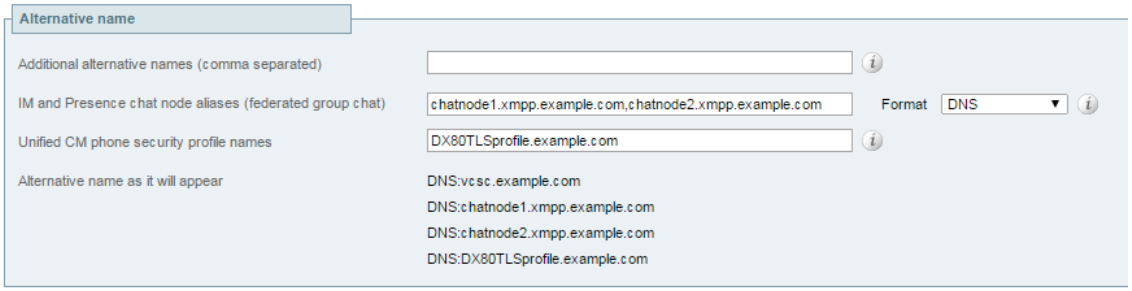
- **Unified CM phone security profile names**: the names of the **Phone Security Profiles** in Unified CM that are configured for encrypted TLS and are used for devices requiring remote access. Use the FQDN format and separate multiple entries with commas.

  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 1 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 of 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 MRA 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).

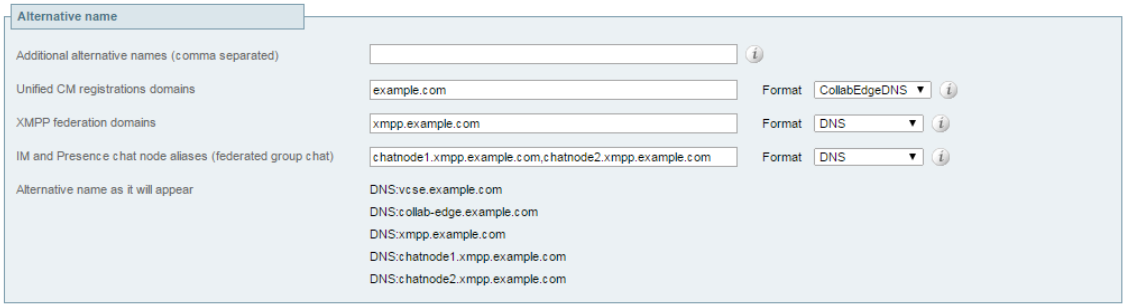
- **XMPP federation domains**: the domains used for point-to-point XMPP federation. These are configured on the IM&P servers and should also be configured on the Expressway-C as domains for XMPP federation.

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

Figure 2 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 takes you through the steps required to configure your Expressway for external XMPP federation.

Prerequisites

Ensure that you are running the following software versions:

- Expressway X8.2 or later. This document assumes X8.10
- Unified CM IM & Presence 9.1.1 or later

Note that XMPP federation can only be supported on a single Expressway cluster.

Before configuring your Expressway system for external XMPP federation:

- Ensure that Interdomain XMPP Federation has been **disabled** on Unified CM IM and Presence:
  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*.

  You must disable Interdomain Federation on Unified CM IM&P before enabling XMPP federation on Expressway.

- An Expressway-C (cluster) and Expressway-E (cluster) have been configured for Mobile and Remote Access to Unified Communications services, as described in *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), the following 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 that federated communications are available to both on-premises clients (connected directly to Unified CM IM&P) and off-premises clients (connected to Unified CM IM&P via mobile and remote access).
- If you intend to use both TLS and group chat, the Expressway-C and Expressway-E server certificates must include in their list of subject alternate names (using either XMPPAddress or DNS formats) the **Chat Node Aliases** that are configured on the IM&P servers. Note that the Expressway-C automatically includes the chat node aliases in its certificate signing requests (CSRs), providing it has discovered a set of IM&P 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.

  See Server Certificate Requirements for Unified Communications, page 12 for more information.

Configuring Local Domains for XMPP Federation on Expressway-C

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

1. On Expressway-C, go to **Configuration > Domains**.
2. Click **New** (or click **View/Edit** if the required domain already exists).
3. Enter your local **Domain name** to be federated.
4. Set **IM and Presence Service** to *On*. If **IM and Presence Service** is set to *Off*, the Expressway may raise an unexpected alarm.
5. Set **XMPP federation** to *On*.
6. Click **Save**.
7. 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.

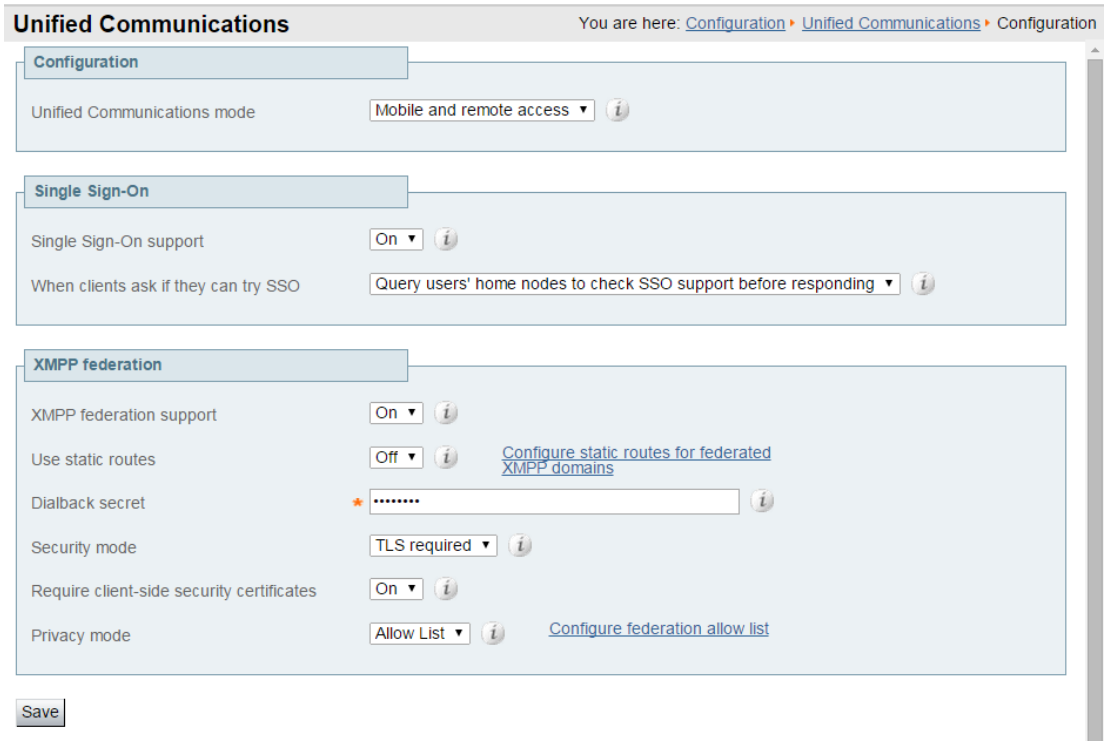
Configuring Expressway-E for XMPP Federation

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, page 23 for more information.)

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

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



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.

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 2 Settings for XMPP Federation

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, page 18 below.

Table 2 Settings for XMPP Federation (continued)

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 that 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*.
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 that 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 that 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, page 18 below.

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:

1. On Expressway-E, go to **Configuration > Unified Communications**.
2. Set **Use static routes** to *Off*.
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, page 19.

To use static routes:

1. Contact the partners with whom you are federating to get a list of their chat node aliases.
2. On Expressway-E, go to **Configuration > Unified Communications**.
3. Set **Use static routes** to *On* and click **Save**.
4. Click **Configure static routes for federated XMPP domains**.
5. On the **Federated static routes** page, click **New**.
6. Enter the details of the static route:

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.

7. Click **Save**.
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.

The 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 mode** is set to *Allow list* by default. In effect this puts the system in a 'lockdown' mode – you will not be allowed to connect with any federated domains or chat node aliases until you either add them to the allow list, configure static routes, or change the **Privacy mode** setting.

1. On Expressway-E, go to **Configuration > Unified Communications**.
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.
3. Click **Save**.
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.

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

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
example.com	xmpp-server	tcp	0	0	5269	vcse.example.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	vcse.example.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 that:

- 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.

Port usage for XMPP federation

This section summarizes the firewall ports that need to be opened for XMPP federation.

Outbound from Expressway-C (private) to Expressway-E (DMZ)

Purpose	Protocol	Expressway-C (source)	Expressway-E (listening)
XMPP	TCP	Ephemeral port	7400

Outbound from Expressway-E (DMZ) to public internet

Purpose	Protocol	Expressway-E (source)	Federated XMPP server (listening)
XMPP	TCP	Ephemeral port	5269

Inbound from public internet to Expressway-E (DMZ)

Purpose	Protocol	Federated XMPP server (source)	Expressway-E (listening)
XMPP	TCP	Ephemeral port	5269

From Expressway-C to IM and Presence Server

Purpose	Protocol	Expressway-C (source)	IM and Presence Server(listening)
XMPP	TCP	Ephemeral port	7400

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:

1. On the Expressway-E, go to **Status > Unified Communications**.
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 that 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 your external XMPP federation deployment and describes the impact of making configuration changes on a live system.

Checking the Basic Status of your System

If you encounter issues with the XMPP federation status service, you should first check the **Status > Unified Communications** page on both the Expressway-Cand the Expressway-E.

This will highlight any basic connection or configuration problems and provide information and links to help correct the problem.

General Configuration Checklist

Ensure that the following Expressway configuration items have been specified correctly:

- Port 5269 is open in both directions between the internet and Expressway-Ein 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-Cand its associated Expressway-E (**Status > Zones**).
- **Unified Communications mode** is set to *Mobile and remote access* on both the Expressway-C and 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 and Presence Service servers have been discovered on the Expressway-C and have an active status (**Configuration > Unified Communications > IM and Presence Service servers**).

Discovery, Connectivity, and Firewall Issues

- 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 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 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.
- 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.

Certificates and Secure TLS Connections

If you have configured secure Transport Layer Security (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 Service 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 [p.1] 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 and Presence Service

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

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

1. Disable Interdomain Federation on the IM and Presence Service servers:
   a. Go to **Cisco Unified CM IM and Presence Service Administration > Presence > Inter Domain Federation > XMPP Federation > Settings**.
   b. Set **XMPP Federation Node Status** to *Off*.
2. Refresh the set of discovered IM and Presence Service servers on Expressway-C.
3. Restart all of the Unified CM IM and Presence Service 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 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 the XCP router on both Expressway-C and Expressway-E.

- This will remove the Expressway-E XMPP federation node from all discovered IM and Presence Service servers. A notification will appear on the IM and Presence Service administration interface to restart the XCP router on all affected IM and Presence Service nodes.
- The end-user impact is that all IM and Presence Service sessions will be disconnected. IM and Presence Service sessions over mobile and remote access will be disconnected, and sessions directly homed on the IM and Presence Service node will be dropped. When the XCP router is restarted on each IM and Presence Service node, all XCP functionality on that node will be disrupted.

Discovered IM and Presence Service Servers

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

- The XCP Router on Expressway-C will restart.
- The end-user impact should be minimal. They will be unable to send or receive IM and Presence Service 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 the XCP router on both Expressway-C and Expressway-E. The same situation will result from resetting the mode to On.

- The Expressway-E XMPP federation node will be removed from all discovered IM and Presence Service servers. A notification will appear on the IM and Presence Service administration interface to restart the XCP router on all affected IM and Presence Service nodes.
- The end-user impact is that all IM and Presence Service sessions will be disconnected. IM and Presence Service sessions over mobile and remote access will be disconnected, and sessions directly homed on the IM and Presence Service node will be dropped. When the XCP router is restarted on each IM and Presence Service node, all XCP functionality on that node will be disrupted.

XMPP Federation Support

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

- The Expressway-E XMPP federation node will be added to or removed from all discovered IM and Presence Service servers. A notification will appear on the IM and Presence Service administration interface to restart the XCP router on all affected IM and Presence Service nodes.
- The end-user impact is that all IM and Presence Service sessions will be disconnected. IM and Presence Service sessions over mobile and remote access will be disconnected, and sessions directly homed on the IM and Presence Service node will be dropped. When the XCP router is restarted on each IM and Presence Service 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 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 and Presence Service 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 and Presence Service server.

Please refer to the *High Availability Client Login Profiles* section of the IM and Presence Service version you are running at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

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

This integration enables IM and Presence Service users in one enterprise domain to exchange presence information and Instant Messaging (IM) with users in external domains.

Supported Systems

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

- Cisco WebEx Messenger Release 7.x.
- IBM Sametime Release 8.2 and 8.5.
- Cisco Unified Presence Release 8.x.
- IM and Presence Service Release 9.x or later.
- Any other server that is XMPP-standards compliant.

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

Note: If you wish 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.

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

When IM and Presence Service is federating with WebEx Enterprise, it is 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, following the procedures described in this guide.

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, note the following:

- See topics related to integration preparation for considerations on routing, scale, public IP addresses, and the Certification Authority (CA).
- See the task to configure the Cisco Adaptive Security Appliance for information on configuring the prerequisite information such as the hostname, timezone, clock, and so on.

Intercluster and Multinode Deployments

Note: Any configuration procedures related to intercluster IM and Presence Service deployments can also be applied to multinode IM and Presence Service deployments.

For a single cluster, you only need to enable XMPP federation on one node in the cluster. A single DNS SRV record is published for the enterprise in the public DNS. This DNS SRV record maps to the IM and Presence Service node that is enabled for XMPP federation. All incoming requests from external domains are routed to the node running XMPP federation, based on the published SRV record. Internally IM and Presence Service reroutes the requests to the correct node for the user. The IM and Presence Service also routes all outgoing requests through the node running XMPP federation.

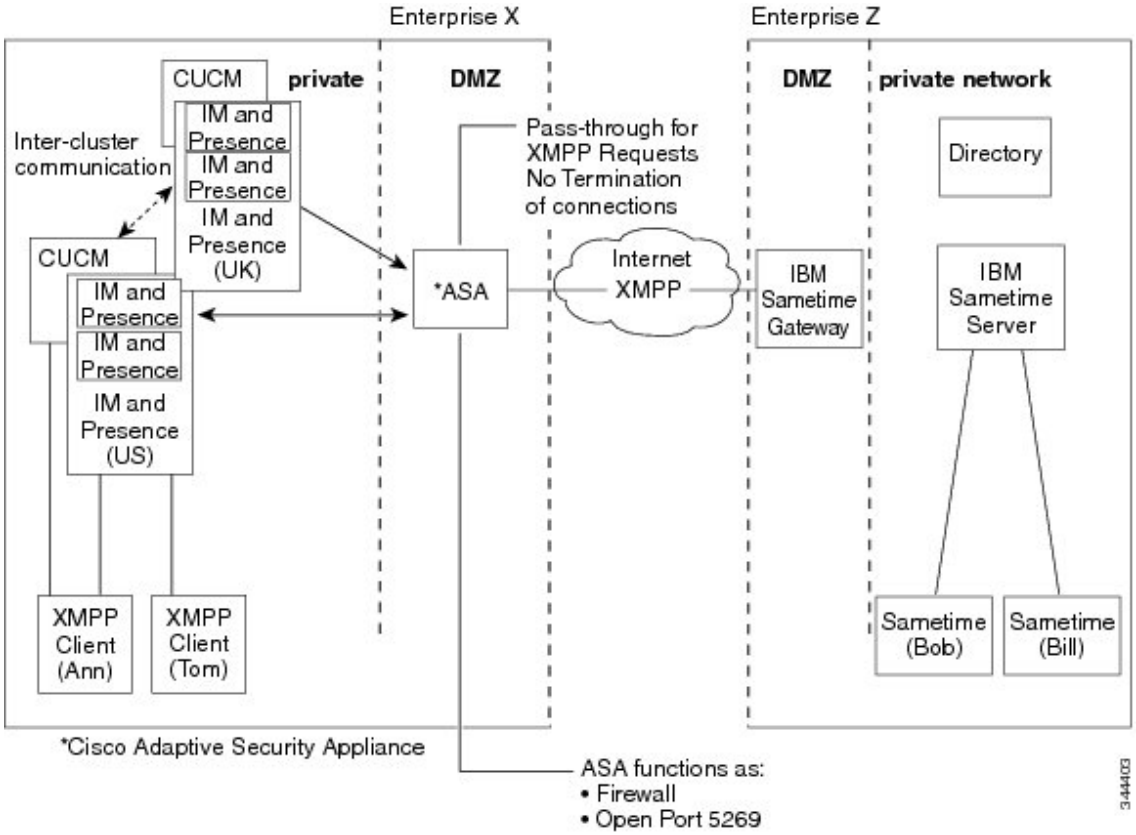
You can also publish multiple DNS SRV records, for example, for scale purposes, or if you have multiple IM and Presence Service clusters and you must enable XMPP federation at least once per cluster. Unlike SIP federation, XMPP federation does not require a single point of entry for IM and Presence Service enterprise domain. As a result, IM and Presence Service can route incoming requests to any one of the published nodes that you enable for XMPP federation.

In an intercluster and a multinode cluster IM and Presence Service deployment, when an external XMPP federated domain initiates a new session, it performs a DNS SRV lookup to determine where to route the request. If you publish multiple DNS SRV records, the DNS lookup returns multiple results; IM and Presence Service can route the request to any of the servers that DNS publishes. Internally IM and Presence Service reroutes the requests to the correct node for the user. IM and Presence Service routes outgoing requests to any of the nodes running XMPP federation within the cluster.

If you have multiple nodes running XMPP federation, you can still choose to publish only one node in the public DNS. With this configuration, IM and Presence Service routes all incoming requests through that single node, rather than load balancing the incoming requests across the nodes running XMPP federation.IM and Presence Service load-balances outgoing requests and sends outgoing requests to any of the nodes running XMPP federation within the cluster.

Example of XMPP Federated Network between IM and Presence Service and IBM Sametime

The following figure provides an example of an XMPP federated network between IM and Presence Service enterprise deployment and an IBM Sametime enterprise deployment. Transport layer Security (TLS) is optional for XMPP federation. Cisco Adaptive Security Appliance (ASA) acts only as a firewall for XMPP federation; it does not provide TLS proxy functionality or Port Address Translation (PAT) for XMPP federation.



There are two Domain Name System (DNS) servers within the internal IM and Presence Service enterprise deployment. One DNS server hosts the IM and Presence Service private address. The other DNS server hosts the IM and Presence Service public address and DNS SRV records for SIP federation (_sipfederationtls), and XMPP federation (_xmpp-server) with IM and Presence Service. The DNS server that hosts the IM and Presence Service public address is located in the local DMZ.

Task Flow for XMPP Federation through IM and Presence Service

The below table outlines the tasks that must be completed to successfully deploy XMPP federation through IM and Presence Service.

Task	See
Configure IM and Presence Service for XMPP federation	Configuring IM and Presence Service for XMPP Federation, page 28
Configure Security for XMPP federation	Security Certificate Configuration for XMPP Federation, page 42
(Optional) Configure the email for federation feature	Email Address for Federation Configuration , page 46
Turn on XMPP federation service	Turn on XMPP Federation Service, page 41
Configure the Cisco Adaptive Security Appliance for XMPP federation	Configure the Cisco Adaptive Security Appliance for XMPP Federation, page 39
Troubleshooting XMPP federation through IM and Presence Service	Troubleshooting an XMPP Federation Integration, page 54

Configuring IM and Presence Service for XMPP Federation

Configure General Settings for XMPP Federation on IM and Presence Service

XMPP Federation Overview

IM and Presence Service, Release 9.0 and later, supports XMPP federation with the following enterprises:

- Cisco WebEx Messenger Release 7.x
- IBM Sametime Release 8.2 and 8.5
- Cisco Unified Presence Release 8.x
- IM and Presence Service Release 9.x or later

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

Note: The preferred method for deploying external XMPP Federation is through the Expressway-C and Expressway-E Collaboration Edge solution.

When IM and Presence Service is federating with WebEx Enterprise, it is 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 IM and Presence Service to federate over XMPP, use the procedures in this guide to 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, note the following:

- See topics related to integration preparation for considerations on routing, scale, public IP addresses, and the Certification Authority (CA).
- See the task to configure the Cisco Adaptive Security Appliance for information on configuring the prerequisite information such as the hostname, timezone, clock, and so on.

Important Notes about Restarting Services for XMPP Federation

If you make a change to any of the XMPP federation settings, you must restart the Cisco XCP Router and the Cisco XCP XMPP Federation Connection Manager. To restart the services, log in to the **IM and Presence Serviceability** user interface:

- Cisco XCP Router, choose **Tools > Control Center - Network Services**
- Cisco XCP XMPP Federation Connection Manager, choose **Tools > Control Center > Feature Services**

When you restart the Cisco XCP Router service, the IM and Presence Service restarts all the XCP services.

If you enable or disable XMPP federation on a node, you must restart the Cisco XCP Router on all nodes within a cluster, not just on the node where XMPP federation has been enabled or disabled. For all other XMPP federation settings, a Cisco XCP Router restart is only required on the node to which the setting is being changed.

Turn on XMPP Federation on a Node

This setting is turned on by default.

Procedure

1. Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Presence > Inter Domain Federation > XMPP Federation > Settings**.
2. In the XMPP Federation Node Status drop-down list, choose **On**.
3. Click **Save**.

Note: You cannot start the XCP XMPP Federation Connection Manager service on the IM and Presence Service node, unless you turn on XMPP federation on the node.

Configure Security Settings for XMPP Federation

Before you begin

- Determine whether the external domain that you are federating with supports Transport Layer Security (TLS) connections.
- The TLS and Simple Authentication and Security Layer (SASL) settings are only configurable if you select the Secure Sockets Layer (SSL) mode "TLS Optional" or "TLS Required".
- If you are configuring federation between IM and Presence Service and IBM using TLS, you must configure the SSL mode "TLS Required", and you must enable SASL.

Procedure

1. Log in to the **Cisco Unified CM IM and Presence Service Administration** user interface. Choose **Presence > Inter Domain Federation > XMPP Federation > Settings.**

2. Choose a security mode from the drop-down list.
   a. No TLS - IM and Presence Service does not establish a TLS connection with the external domain. The system uses a non-encrypted connection to federate with the external domain, and uses the server dialback mechanism to verify the identity of the other server.
   b. TLS Optional - IM and Presence Service attempts to establish a TLS connection with the external domain. If IM and Presence Service fails to establish a TLS connection, it reverts to server dialback to verify the identity of the other server.
   c. TLS Required - The system guarantees a secure (encrypted) connection with the external domain.
3. Check the **Require client-side security certificates** check box if you want to enforce strict validation of certificates from external domain servers against an installed root CA certificate. This setting turns on, by default, if you select either TLS Optional or TLS Required security settings.

Note: If you are configuring XMPP federation with WebEx, do not check the **Require client-side security certificates** check box.

4. Check the **Enable SASL EXTERNAL on all incoming connections** check box to ensure that the IM and Presence Service advertises support for SASL EXTERNAL on incoming connection attempts and implements SASL EXTERNAL validation.
5. Check the **Enabling SASL on outbound connections** check box to ensure that IM and Presence Service sends a SASL auth id to the external domain if the external server requests SASL EXTERNAL.
6. Enter the dialback secret if you want to use DNS to verify the identity of an external server that is attempting to connect to IM and Presence Service. IM and Presence Service does not accept any packets from the external server until Domain Name System (DNS) validates the identity of the external server.
7. Click **Save**.

Tip: For further information on the security settings, see the Online Help.

Tip: If the node is part of an intercluster deployment, then you must configure each cluster with the same security settings. Run the **System Troubleshooter** to ensure that your configuration is consistent on all nodes.

DNS Configuration for XMPP Federation

DNS SRV Records for XMPP Federation

To allow IM and Presence Service to discover a particular XMPP federated domain, the federated enterprise must publish the _xmpp-server Domain Name Server (DNS) SRV record in its public DNS server. Similarly, IM and Presence Service must publish the same DNS SRV record in the DNS for its domain. Both enterprises must publish the port 5269. The published Fully Qualified Domain Name (FQDN) must also be resolvable to an IP address in DNS.

A DNS SRV record should be published for each domain in the IM and Presence Service deployment. You can use the **Cisco Unified CM IM and Presence Administration** user interface to view a list of all the domains. Go to the **Presence Domains** window to view a list of all domains in the system. Log in to **Cisco Unified CM IM and Presence Administration** user interface and choose **Presence > Domains**.

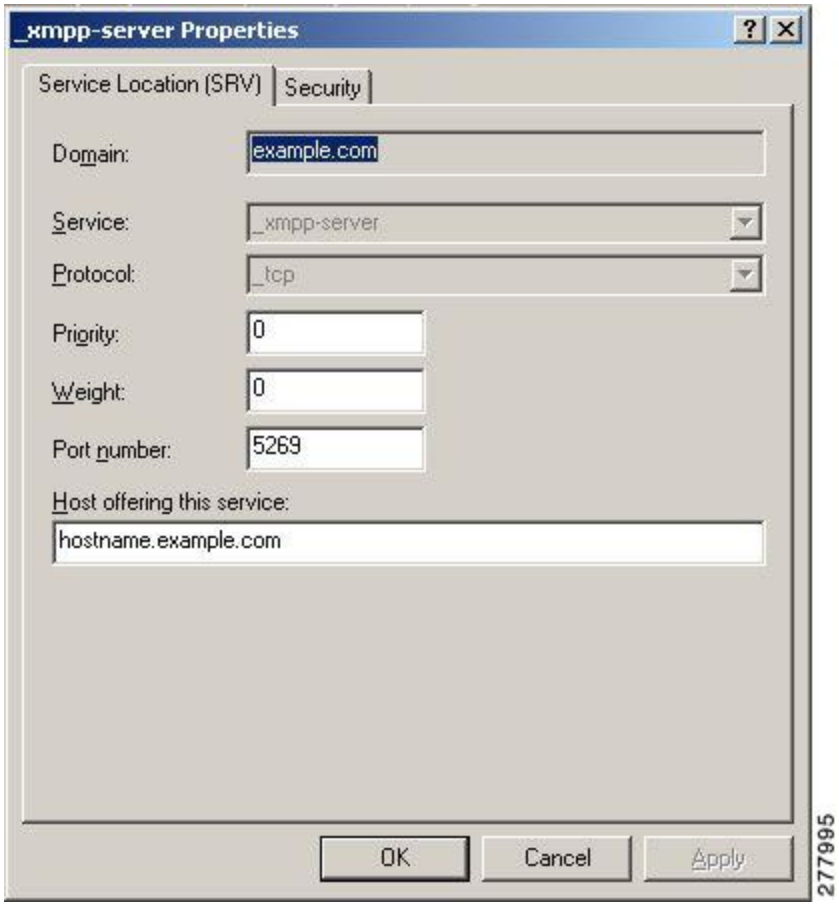
You can also use the Email Domains for Federation window to view the list of all email domains in the system if the email address for federation feature is enabled. Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Presence > Inter-Domain Federation > Email Federated Domains**.

The required DNS record is:

_xmpp-server._tcp.domain

The following figure shows a sample DNS configuration for the _xmpp-server DNS SRV record for the domain **example.com**.

Figure 3 DNS SRV for _xmpp-server



Two DNS records are needed for each server in the cluster: one DNS record for IPv4 and the second DNS record for IPv6. Indicate if the record is the IPv4 or IPv6 version using the hostname value in the **Host offering this service** field. For example:

- `hostname-v4.example.com` indicates that the DNS record is the IPv4 version.
- `hostname-v6.example.com` indicates that the DNS record is the IPv6 version.

If you have remote root access to IM and Presence Service, you can run `nslookup` to determine if the federated domain is discoverable.

Tip: Use this sequence of commands for performing a DNS SRV lookup:

```
nslookup
set type=srv _
xmpp-server._tcp.domain
```

(*domain* is the domain of the federated enterprise.)
This command returns an output similar to this example, where "example.com" is the domain of the federated server:

```
_xmpp-server._tcp.example.com service = 0 0 526 hostname.example.com.
```

For a single cluster, you only need to enable XMPP federation on one node in the cluster. You publish one DNS SRV record for the enterprise in the public DNS. IM and Presence Service routes all incoming requests from external domains to the node running federation. Internally IM and Presence Service reroutes the requests to the correct node for the user. IM and Presence Service also routes all outgoing requests to the node running XMPP federation.

You can also publish multiple DNS SRV records (for example, for scale purposes), or if you have multiple IM and Presence Service clusters and you must enable XMPP federation at least once per cluster. Unlike SIP federation, XMPP federation does not require a single point of entry for an IM and Presence Service enterprise domain. As a result, IM and Presence Service can route incoming requests to any one of the published nodes in the cluster that you enable for XMPP federation.

In an intercluster and a multinode cluster IM and Presence Service deployment, when an external XMPP federated domain initiates a new session, it performs a DNS SRV lookup to determine where to route the request.

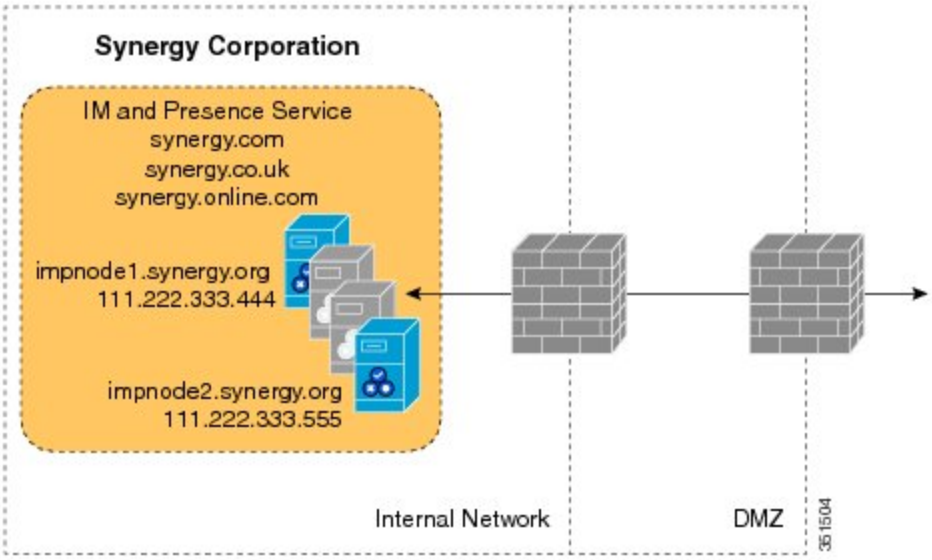
If you publish multiple DNS SRV records, the DNS lookup returns multiple results; IM and Presence Service can route the request to any of the servers that DNS publishes. Internally IM and Presence Service reroutes the requests to the correct node for the user. IM and Presence Service routes outgoing requests to any of the nodes running XMPP federation.

If you have multiple nodes running XMPP federation, you can still choose to publish only one node in the public DNS. With this configuration, IM and Presence Service routes all incoming requests to that single node, rather than load-balancing the incoming requests across the nodes running XMPP federation. IM and Presence Service load-balances outgoing requests and sends outgoing requests from any of the nodes running XMPP federation.

Note: Along with the DNS SRV records that you publish, you must also add the corresponding DNS A and AAAA records.

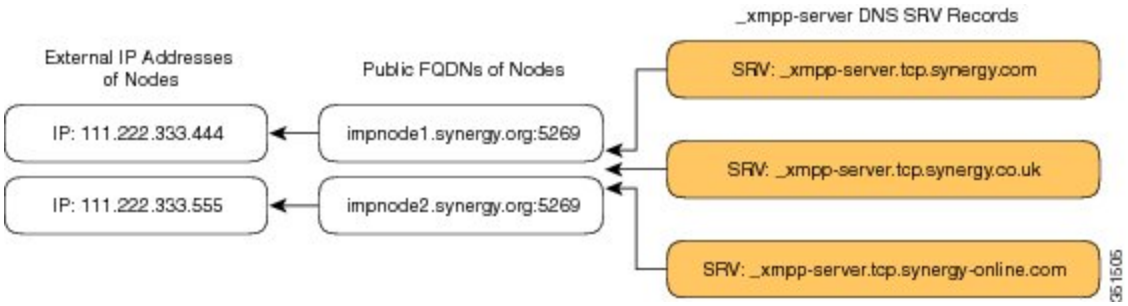
In the following example interdomain federation deployment, two IM and Presence Service nodes are enabled for XMPP federation. A DNS SRV record must be published for each domain that is hosted in the IM and Presence Service deployment. The following figure shows an example interdomain federation deployment with three local domains. You must publish an _xmpp-server DNS SRV record for each domain.

Figure 4 Multiple Domain in an XMPP-Based Federated Interdomain Deployment



Each DNS SRV record must resolve to the public FQDN of both IM and Presence Service nodes that are designated for XMPP federated traffic, and the FQDNs must resolve to the external IP addresses of the IM and Presence Service nodes.

Figure 5 XMPP DNS SRV Resolving to Public FQDNs of IM and Presence Service Nodes



Note: The firewalls that are deployed within the DMZ can translate the IP addresses to the internal IP address of the node. The FQDN of the nodes must be publicly resolvable to a public IP address.

DNS SRV Records for XMPP Federation Chat Feature

If you configure the Chat feature on an IM and Presence Service node in an XMPP federation deployment, you must publish the chat node alias in DNS.

The hostname, to which the DNS SRV record for the chat node resolves, resolves to a public IP address. Depending on your deployment, you may have a single public IP address or a public IP address for each chat node within your network.

Table 1. Chat Request Routing

Deployment	Chat Request Routing
Single public IP address, multiple nodes internally	To route all chat requests to the XMPP federation node, and then on to the chat node. 1. Configure the DNS SRV for the chat node alias to point to port 5269. 2. Configure a NAT command configured on Cisco Adaptive Security Appliance or firewall\NAT server that maps publicIPAddress:5269 to XMPPFederationNodePrivateIPAddress:5269.
Multiple public IP addresses, multiple nodes internally	If you have multiple public IP addresses, you can choose to route chat requests directly to the appropriate chat node. 1. Configure the DNS SRV for the chat node alias to point to port 5269. 2. Configure a NAT command on Cisco Adaptive Security Appliance or firewall\NAT server that maps textChatServerPublicIPAddress:25269 to textChatServerPrivateIPAddress:5269. **Note:** To allow the chat node to handle incoming federated text requests, you must turn on the Cisco XMPP Federation Connection Manager on the chat node.

For information on configuring the Chat feature on IM and Presence Service, see Configuring and Administration of IM and Presence Service on Cisco Unified Communications Manager.

Configure DNS SRV Record for XMPP Federation Chat Node

Procedure

1. To retrieve the chat node alias:
   a. Log in to the **Cisco Unified CM IM and Presence Administration** interface. Choose **Messaging > Group Chat Server > Alias Mapping.**
   b. Click **Find** to display a list of chat node aliases.
   c. Choose the chat node alias that you want to publish in DNS, for example: conference-2.StandAloneCluster.example.com
2. In the public DNS server for the `example.com` domain, create the StandAloneCluster domain.
3. In the StandAloneClusterdomain, create the conference-2domain.
4. In the conference-2 domain, create the _tcp domain.
5. In the _tcp domain, create two new DNS SRV records for _xmpp-server: one for IPv4 and another one for IPv6. See the following figures for sample DNS configuration records.

Note: If the text conference server alias is `conference-2-StandAloneCluster.example.com` then the domain in Step 2 is conference-2-StandAloneCluster, and you skip Step 3. In Step 4, create the _tcp domain under conference-2-StandAloneCluster.

Figure 6 IPv4 DNS SRV Record for _xmpp-server for Chat Feature

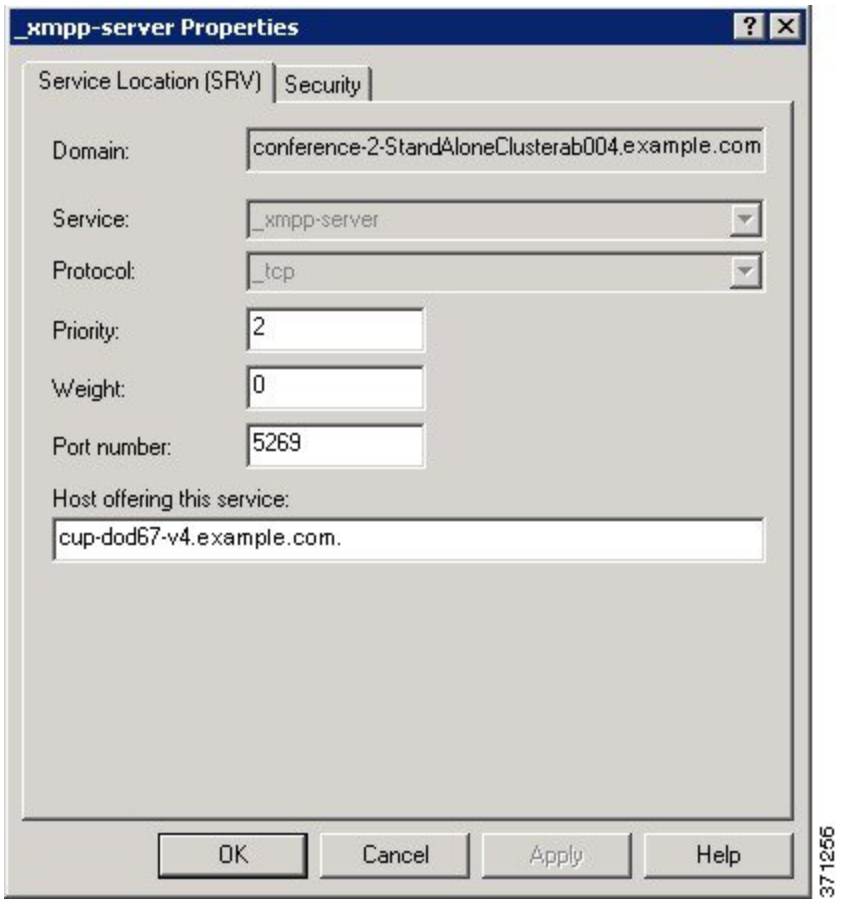


Figure 7 IPv6 DNS SRV Record for _xmpp-server for Chat Feature

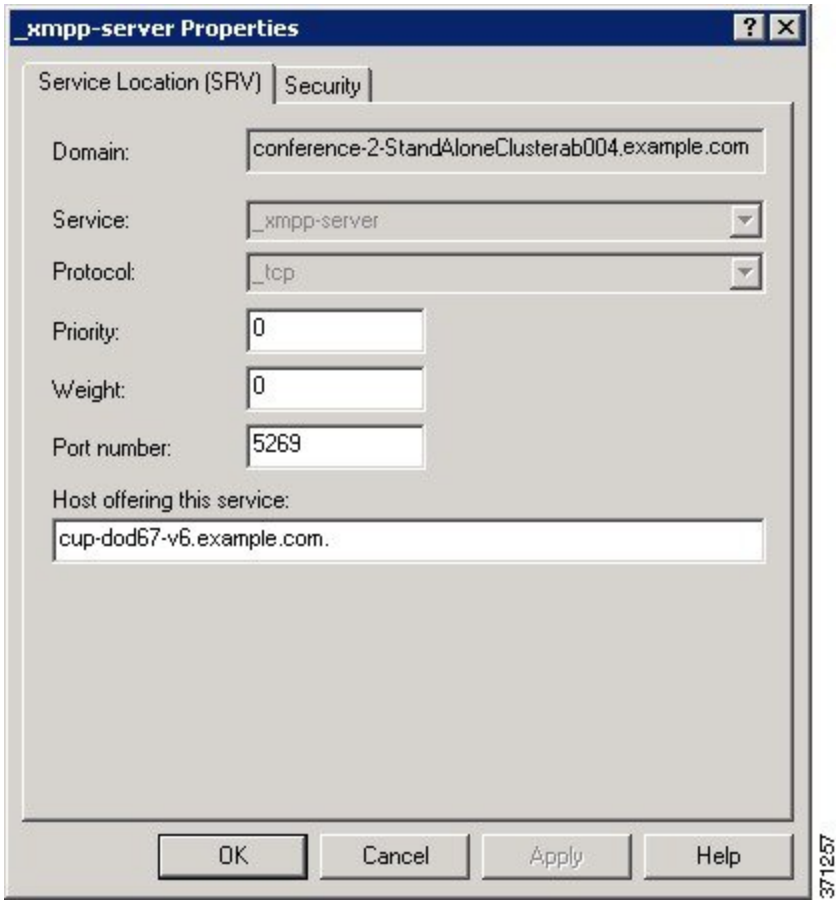
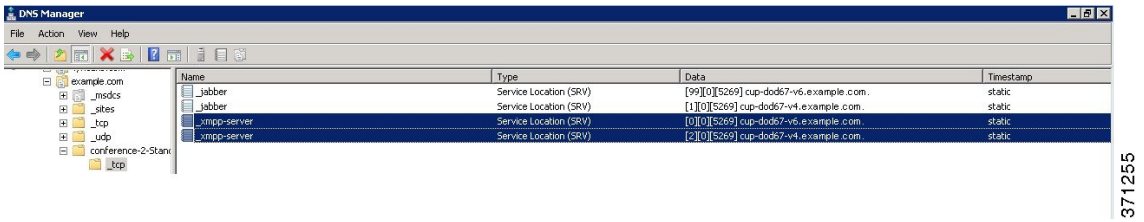


Figure 8 DNS Configuration for Chat Feature



Policy Settings Configuration for XMPP Federation

Policy Exception Configuration

You can configure exceptions to the default policy for XMPP federation. In the exception, you must specify the external domain to which you want to apply the exception, and a direction rule for the exception. When you configure the domain name for a policy exception, note the following:

- If the URI or JID of the user is **user@example.com**, configure the external domain name in the exception as **example.com**.
- If the external enterprise uses hostname.domain in the URI or JID of the user, for example **user@hostname.example.com**, configure the external domain name in the exception as **hostname.example.com**
- You can use a wildcard (*) for the external domain name in the exception. For example, the value ***.example.com** applies the policy on **example.com** and any subdomain of **example.com**, for example, **somewhere.example.com**.

You must also specify the direction that IM and Presence Service applies the policy exception. These direction options are available:

- **All federated packets from/to the above domain/host** – IM and Presence Service allows or denies all traffic going to and coming from the specified domain.
- **Only incoming federated packets from the above domain/host** – allow IM and Presence Service to receive inbound broadcasts from the specified domain, but the IM and Presence Service does not send responses.
- **Only outgoing federated packets to the above domain/host** – allow IM and Presence Service to send outbound broadcasts to the specified domain, but the IM and Presence Service does not receive responses.

Configure Policy for XMPP Federation

Caution: If you make a change to any of the XMPP federation settings, you must restart these services in the **Cisco Unified IM and Presence Serviceability** user interface: Cisco XCP Router (choose **Tools > Control Center – Network Services**), Cisco XCP XMPP Federation Connection Manager (choose **Tools > Control Center – Feature Services**). When you restart the Cisco XCP Router service, IM and Presence Service restarts all the XCP services.

Procedure

1. Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Presence > Inter Domain Federation > XMPP Federation > Policy**.
2. Choose the policy settings from the drop-down list:
   - **Allow** – IM and Presence Service permits all federated traffic from XMPP federated domains, except those domains that you explicitly deny on the policy exception list.
   - **Deny** –IM and Presence Service denies all federated traffic from XMPP federated domains, except those domains that you explicitly permit on the policy exceptions list.
3. To configure a domain on the policy exception list
   a. Click **Add New**.
   b. Specify the domain name or the host name of the external server.
   c. Specify the direction to apply the policy exception.
   d. Click **Save** on the policy exception window.
4. Click **Save** on the policy window.

Tip: See the Online Help for federation recommendations.

Configure the Cisco Adaptive Security Appliance for XMPP Federation

For XMPP federation, the Cisco Adaptive Security Appliance acts as a firewall only. You must open port 5269 for both incoming and outgoing XMPP federated traffic on the Cisco Adaptive Security Appliance.

These are sample access lists to open port 5269 on the Cisco Adaptive Security Appliance, Release 8.3.

Allow traffic from any address to any address on port 5269:

access-list ALLOW-ALL extended permit tcp any any eq *5269*

Allow traffic from any address to any single node on port 5269:

access-list ALLOW-ALL extended permit tcp any host *private_imp_ip_address* **eq** ***5269***

If you do not configure the access list above, and you publish additional XMPP federation nodes in DNS, you must configure access to each of these nodes, for example:

object network *obj_host_private_imp_ip_address*

#host *private_imp_ip_address*

object network *obj_host_private_imp2_ip_address*

#host*private_imp2_ip_address*

object network*obj_host_public_imp_ip_address*

#host *public_imp_ip_address*

Configure the the following NAT commands:

nat (inside,outside) source static *obj_host_private_imp1_ip obj_host_public_imp_ip* **service**

obj_udp_source_eq_5269 obj_udp_source_eq_5269

nat (inside,outside) source static *obj_host_private_imp1_ip obj_host_public_imp_ip* **service**

obj_tcp_source_eq_5269 obj_tcp_source_eq_5269

If you publish a single public IP address in DNS, and use arbitrary ports, configure the following:

(This example is for two additional XMPP federation nodes)

nat (inside,outside) source static*obj_host_private_imp2_ip obj_host_public_imp_ip* **service**

obj_udp_source_eq_5269 obj_udp_source_eq_25269

nat (inside,outside) source static *obj_host_private_imp2_ip obj_host_public_imp_ip* **service**

obj_tcp_source_eq_5269 obj_tcp_source_eq_25269

nat (inside,outside) source static *obj_host_private_imp3_ip obj_host_public_imp_ip* **service**

obj_udp_source_eq_5269 obj_udp_source_eq_35269

nat (inside,outside) source static *obj_host_private_imp3_ip obj_host_public_imp_ip* **service**

obj_tcp_source_eq_5269 obj_tcp_source_eq_35269

If you publish multiple public IP addresses in DNS all using port 5269, configure the following:

(This example is for two additional XMPP federation nodes)

nat (inside,outside) source static *obj_host_private_imp2_ip obj_host_public_imp2_ip* **service**

obj_udp_source_eq_5269 obj_udp_source_eq_5269

nat (inside,outside) source static ***obj_host_private_imp2_ip obj_host_public_imp2_ip*** **service**

obj_tcp_source_eq_5269 obj_tcp_source_eq_5269

nat (inside,outside) source static *obj_host_private_imp3_ip obj_host_public_imp3_ip* **service**

obj_udp_source_eq_5269 obj_udp_source_eq_5269

nat (inside,outside) source static *obj_host_private_imp3_ip obj_host_public_imp_ip* **service**

obj_tcp_source_eq_5269 obj_tcp_source_eq_5269

Turn on XMPP Federation Service

You need to turn on the Cisco XCP XMPP Federation Connection Manager service on each IM and Presence Service node that runs XMPP federation.

Once you turn on the Federation Connection Manager service from the Service Activation window, IM and Presence Service automatically starts the service; you do not need to manually start the service from the **Control Center - Feature Services** window.

Before you begin

Turn on XMPP Federation for the node from Cisco Unified Communications Manager IM and Presence Service Administration, see XMPP Federation through IM and Presence Service, page 25.

Procedure

1. Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools > Service Activation.**
2. From the Server drop-down list, select the server.
3. Click **Go**.
4. In the IM and Presence Services area, click the button next to the **Cisco XCP XMPP Federation Connection Manager** service.
5. Click **Save**.

Security Certificate Configuration for XMPP Federation

Security Certificate Configuration for XMPP Federation

To configure security for XMPP federation, you must complete the following procedures:

1. Verify that all local domains are created and configured on the system and, if necessary, manually create any missing local domains before you generate the cup-xmpp-s2s certificate.
2. Create the certificate once using one of the following types of certificates:
   - Self-signed certificate for XMPP federation.
   - CA-signed certificate for XMPP federation.
3. Import the root CA certificate.

You must repeat this procedure every time you federate with a new enterprise whose CA you do not already trust. Likewise, you should follow this procedure if the new enterprise uses self-signed certificates, where the self-signed certificates are uploaded instead of the root CA certificate.

Local Domain Validation for XMPP Federation

All local domains must be included in the generated cup-xmpp-s2s certificate. Before you generate the cup-xmpp-s2s certificate, validate that all local domains are configured and appear in the Domains window. Manually add any domains that are planned for, but that don't yet appear in the list of local domains. For example, a domain that does not currently have any users assigned normally does not appear in the list of domains.

Log in to the **Cisco Unified CM IM and Presence Administration** user interface, choose **Presence > Domains.**

After you have validated that all domains are created in the system, you can proceed to create the cup-xmpp-s2s certificate once using either a self-signed certificate or a CA-signed certificate for XMPP federation. If email address for federation is enabled, all email domains must also be included in the certificate.

If you add, update, or delete any local domains and regenerate the cup-xmpp-s2s certificate, you must restart the Cisco XCP XMPP Federation Connection Manager service. To restart this service, log in to the **Cisco Unified IM and Presence Serviceability** user interface and choose **Tools > Control Center - Feature Services**.

Multi-Server Certificate Overview

IM and Presence Service supports multi-server SAN based certificates for the certificate purposes of tomcat, cup-xmpp and cup-xmpp-s2s. You can select between a single-server or multi-server distribution to generate the appropriate Certificate Signing Request (CSR). The resulting signed multi-server certificate and its associated chain of signing certificates is automatically distributed to the other servers in the cluster on upload of the multi-server certificate to any of the individual servers in the cluster. For more information on multi-server certificates, see the New and Changed Features chapter of the Release Notes for Cisco Unified Communications Manager, Release 10.5 (1).

Use a Self-Signed Certificate for XMPP Federation

This section describes how to use a self-signed certificate for XMPP federation. For information about using a CA-signed certificate, see Use of a CA-Signed Certificate for XMPP Federation, page 43

Procedure

1. Log in to the **Cisco Unified IM and Presence Operating System Administration** user interface. Choose **Security > Certificate Management.**
2. Click **Generate Self-signed.**
3. From the Certificate Purpose drop-down list, choose `cup-xmpp-s2s` and click **Generate.**
4. Restart the Cisco XCP XMPP Federation Connection Manager service. Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools > Control Center - Network Services** to restart this service.
5. Download and send the certificate to another enterprise so that it can be added as a trusted certificate on their XMPP server. This can be a IM and Presence Service node or another XMPP server.

Use of a CA-Signed Certificate for XMPP Federation

This section describes how to use a CA-signed certificate. For information about using a self-signed certificate, see Use a Self-Signed Certificate for XMPP Federation, page 43. To use a CA-signed certificate complete the following

- Generate a Certificate Signing Request for XMPP Federation.
- Upload a CA-Signed Certificate for XMPP Federation.

Generate a Certificate Signing Request for XMPP Federation

This procedure describes how to generate a Certificate Signing Request (CSR) for a Microsoft Certificate Services CA.

Note: While this procedure is to generate a CSR for signing a Microsoft Certificate Services CA, the steps to generate the CSR (steps 1 to 3) apply when requesting a certificate from any Certificate Authority.

Configure the domain for the XMPP certificate, see Local Domain Validation for XMPP Federation, page 42

Procedure

1. Log in to the **Cisco Unified IM and Presence Operating System Administration** user interface. Choose **Security > Certificate Management**.
2. To generate the CSR, perform these steps:
   a. Click **Generate CSR**.
   b. From the Certificate Purpose drop-down list, choose **cup-xmpp-s2s** for the certificate name.
   c. Click **Generate**.
   d. Click **Close**, and return to the main certificate window.
3. To download the `.csr` file to your local machine.
   a. Click **Download CSR**.
   b. From Download Certificate Signing Request window, choose the `cup-xmpp-s2s.csr` file.
   c. Click **Download CSR** to download this file to your local machine.
4. Using a text editor, open the `cup-xmpp-s2s.csr` file.

5. Copy the contents of the CSR file.

   Note: You must copy all information from and including - BEGIN CERTIFICATE REQUEST to and including END CERTIFICATE REQUEST -

6. On your internet browser, browse to your CA server, for example: `http://<name of your Issuing CA Server>/certsrv`.
7. Click **Request a certificate.**
8. Click **Advanced certificate request**.
9. Click **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file**, or submit a renewal request by using a base-64-encoded PKCS #7 file.
10. Paste the contents of the CSR file (that you copied in step 5) into the Saved Request field.
11. Click **Submit**.
12. On your internet browser, return to the URL: `http://<name of your Issuing CA Server>/certsrv`.
13. Click **View the status of a pending certificate request**.
14. Click on the certificate request that you issued in the previous section.
15. Click **Base 64 encoded**.
16. Click **Download certificate**.
17. Save the certificate to your local machine:
    a. Specify a certificate file name `cup-xmpp-s2s.pem`.
    b. Save the certificate as type **Security Certificate**.

Troubleshooting Tip: If the list of supported domains on IM and Presence Service changes, then the `cup-xmpp-s2s` certificate must be regenerated to reflect the new domain list.

Upload a CA-Signed Certificate for XMPP Federation

Before you begin

Complete the steps in Generate a Certificate Signing Request for XMPP Federation, page 43.

Procedure

1. Log in to the **Cisco Unified IM and Presence Operating System Administration** user interface. Choose **Security > Certificate Management**.
2. Click **Upload Certificate/Certificate** chain.
3. Choose `cup-xmpp-s2s` for Certificate Name.
4. In the **Root Certificate** field, specify the name of the root certificate.
5. Click **Upload File**.
6. Browse to the location of the CA-signed certificate that you saved to your local machine.
7. Click **Upload File**.
8. Restart the Cisco XMPP Federation Connection Manager service. Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools > Control Center - Network Services** to restart this service.

Note: If you upload a multi-server certificate you must restart the XCP Router service on all IM and Presence Service nodes in the cluster.

If you migrate from self-signed to CA-signed certificates, the original self-signed certificates persist in the service trust store of the IM and Presence Service node. Leaving the original self-signed certificates in the service trust store is not an issue because no service presents them. However, if needed, you can delete these trust store certificates.

See the section Delete Self-Signed Trust Certificates in Part II, Chapter 11 – Security Configuration on IM and Presence Service, in the appropriate release of the Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager.

Import a Root CA Certificate for XMPP Federation

Note: This section describes how to manually upload the `cup-xmpp-s2s` trust certificates to IM and Presence Service. You can also use the Certificate Import Tool to automatically upload cup-xmpp-s2s trust certificates. To access the Certificate Import Tool, log in to the **Cisco Unified CM IM and Presence Service Administration** user interface. Choose **System > Security > Certificate Import Tool**, and see the Online Help for instructions on how to use this tool.

If IM and Presence Service federates with an enterprise, and a commonly trusted Certificate Authority (CA) signs the certificate of that enterprise, you must upload the root certificate from the CA to an IM and Presence Service node.

If IM and Presence Service federates with an enterprise that uses a self-signed certificate rather than a certificate signed by a commonly trusted CA, you can upload the self-signed certificate using this procedure.

Before you begin

Download the root CA certificate and save it to your local machine.

Procedure

1. Log in to the **Cisco Unified IM and Presence Service Operating System Administration** user interface. Choose **Security > Certificate Management** on IM and Presence Service.
2. Click **Upload Certificate/Certificate chain**.
3. Choose `cup-xmpp-trust` for Certificate Name.

Note: Leave the Root Name field blank.

4. Click **Browse**, and browse to the location of the root CA certificate that you previously downloaded and saved to you local machine.
5. Click **Upload File** to upload the certificate to the IM and Presence Service node.

Note: You must repeat this procedure every time you federate with a new enterprise whose CA you do not already trust. Likewise, you should follow this procedure if the new enterprise uses self-signed certificates, where the self-signed certificates are uploaded instead of the Root CA certificate.

Troubleshooting Tip: If your trust certificate is self-signed, you cannot turn on the **Require client-side certificates** parameter in the XMPP federation security settings window.

Email Address for Federation Configuration

Email for Federation Enablement

When you turn on the email address for federation feature, IM and Presence Service changes the JID of the local user to the email address of the contact.

If you have an intercluster deployment, you must turn on the email address for federation on all intercluster nodes in your deployment. You must then restart the Cisco XCP Router service after the email for federation feature is turned on.

In an XMPP federation deployment, the email address for federation feature does not currently support temporary or persistent chat rooms in a multicluster IM and Presence Service deployment.

In the deployment scenario where there are multiple IM and Presence Service clusters in the local domain, the local user's actual JID may be sent to the federated user. The only impact to the chat room is that the name that displays to the federated user is the user id of the local user, instead of the email address of the local user; all other chat room functionality operates as normal. This only occurs in temporary or persistent chat rooms with federated users.

Email Address for Federation Considerations

When you configure IM and Presence Service to use the email address for XMPP federation,IM and Presence Service swaps the IM address of the local user for the user's email address in all communications with a federated contact.

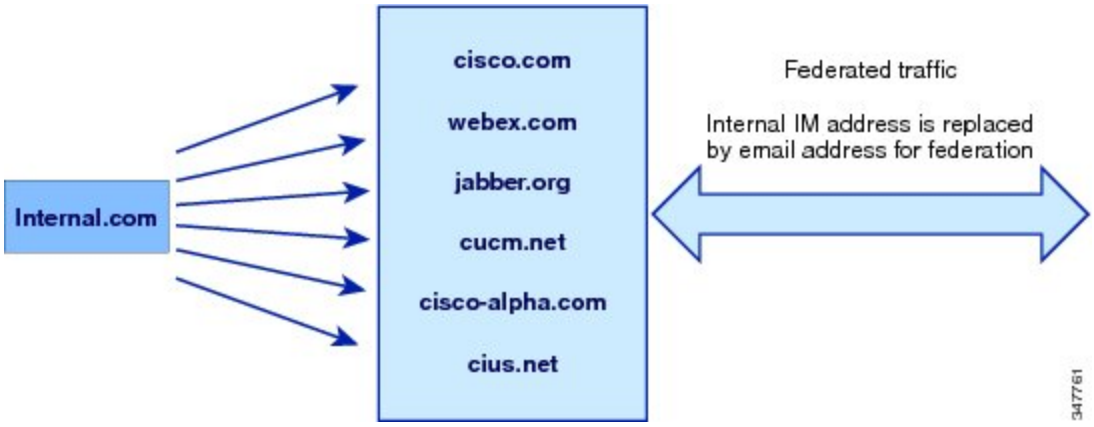
Before you turn on email address for interdomain federation, note the following:

- If you have not yet attempted to federate with the external domain, and you wish to turn on email for federation, we recommend that you turn on this setting before users begin to add any federated contacts.
- If you turn on email address for federation, and a user does not have an email address configured in Active Directory, IM and Presence Service uses the JID of the user for federation.
- A prerequisite for this feature is that the Cisco Unified Communications Manager Mail ID for each user must match the full email address for the user. If the Mail ID field for the user is empty or does not contain a full email address, IM and Presence Service defaults to using IM and Presence Service JID of the user for federation.
- If you turn on email address for federation, and a federated contact uses the JID of an IM and Presence Service user rather than using the email address, IM and Presence Service drops these requests (even if a valid email address is configured for the user).
- IM and Presence Service does not support email aliases for the email address for federation feature.

Email Address for Federation Support of Multiple Domains

The Email Address for Federation feature supports multiple domains. The following figure shows an example of multiple email domains that are being used for federated traffic.

Figure 9 Email Address for Federation support for multiple domains



If the local IM and Presence Service deployment is managing multiple email domains, you must publish the required DNS SRV records for each local email domain.

For XMPP federation, the cup-xmpp-s2s security certificate must have all local IM and email domains included as Subject Alt Names.

Email Domain Configuration Overview

Manually adding and editing email domains for use with the Email Address for Federation feature is optional since IM and Presence Service automatically reads all unique domains for each of the user's email addresses and uses that information for the Email Address for Federation feature.

If you have domains that have users who are not yet configured for IM and Presence Service but plan to configure those users, then you can manually add those domains to IM and Presence Service using the **Cisco Unified CM IM and Presence Administration** user interface. A domain that does not currently have any users assigned is not automatically listed as a local email domain in the user interface.

User domains that are used for Email Address for Federation are listed as system-managed domains on the **Email Domain** window in the **Cisco Unified CM IM and Presence Administration** user interface. These are not configurable with the user interface.

Information to Provide to the Administrator of an External Domain

Before you turn on email address for federation, you must alert the system administrator of the external domain to the following:

- You are using email address for federation, and that the users in the external domain must specify an email address when adding a federated contact to their contact list.
- If you are already federating with the external domain, and you wish to turn on email for federation, users in the external domain must remove the existing federated contacts in their contact list, and add these federated contacts again specifying an email address.

Information to Provide IM and Presence Service Users

When you turn on email address for federation, you must notify all IM and Presence Service users of the following:

- Federated contacts now use email addresses rather than the user_id@domain addresses.
- When adding new contacts to their contact list, federated contacts must now use the email address for IM and Presence Service users, rather than the user_id@domain.
- Existing IM and Presence Service contacts (on the federated watcher's contact list) that were added with user_id@domain must be removed, and added again using the email address for the IM and Presence Service user.
- Any messages that IM and Presence Service receives from federated contacts to the user_id@domain address are dropped (unless it happens to be the same as the email address configured in Active Directory, and the address configured in the users table on IM and Presence Service).
- If IM and Presence Service users already have federated contacts on their contact list, when these users sign in to the client again, the federated contact may get a pop-up containing the email address.

Note: When you turn on email address for federation, a IM and Presence Service user does NOT need to change anything on the client when they connect to IM and Presence Service, nor do they interact any differently with IM and Presence Service node.

Email Domain Management Interactions and Restrictions

- You can add or delete only administrator-managed domains that are associated with the local cluster.
- You cannot edit system managed domains.
- You cannot edit system-managed or administrator managed domains that are associated with other clusters.
- It is possible to have a domain configured on two clusters, but in use on only the peer cluster. This appears as a system-managed domain on the local cluster, but is identified as being in use on only the peer cluster.
- For XMPP federation over TLS, you must regenerate the TLS certificate cup-xmpp-s2s if adding or removing an IM address domain.

Email Address for Federation Configuration and Email Domain Management

Turn on Email for Federation

Note: If you have an intercluster deployment, you must turn on the email address for federation on any intercluster nodes in your deployment.

Procedure

1. Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Presence > Settings**.
2. Check the **Enable use of Email Address when Federating** check box.
3. Read the warning message, and click **OK**.
4. Click **Save**.
5. After you turn on email for federation, restart the Cisco XCP Router. Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools > Control Center - Network Services**.

View Email Domains

System-managed domains and local domains that are administrator-managed are displayed on the **Find and List Email Domains** window using the **Cisco Unified CM IM and Presence Administration** user interface. This window also specifies whether each administrator-managed domain was configured on the local cluster, peer cluster, or both.

Procedure

Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Presence > Inter-Domain Federation > Email Federated Domains**. The **Find and List Email Domains** window appears.

Add or Update Email Domain

You can manually add IM address domains to your local cluster and update existing IM address domains that are on your local cluster using the **Cisco Unified CM IM and Presence Administration** user interface.

You can enter a domain name of up to a maximum of 255 characters and each domain must be unique across the cluster. Allowable values are any upper or lower case letter (a-z, A-Z), any number (0-9), the hyphen (-), or the dot (.). The dot serves as a domain label separator. Domain labels must not start with a hyphen. The last label (for example, .com) must not start with a number. Abc.1om is an example of an invalid domain.

System-managed domains and local domains that are administrator-managed are displayed on the **Find and List Domains** window. This window also specifies whether each administrator-managed domain was configured on the local cluster, peer cluster, or both.

System-managed domains cannot be edited because they are in use. A system-managed domain automatically becomes an administrator-managed domain if there are no longer users on the system with that IM address domain (for example, due to user deletion). You can edit or delete administrator-managed domains.

Procedure

1. Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Presence > Inter-Domain Federation > Email Federated Domains**. The **Find and List Email Domains** window appears displaying all administrator-managed and system-managed email domains.
2. Perform one of the following actions:
   - Click **Add New** to add a new domain. The **Email Domain** window appears.
   - Choose the domain to edit from the list of domains. The **Email Domain** window appears.
3. Enter the new domain name in the **Domain Name** field, and then click **Save**.

Enter a unique domain name up to a maximum of 255 characters. Allowable values are any upper or lower case letter (a-z, A-Z), any number (0-9), the hyphen (-), or the dot (.). Domain labels must not start with a hyphen, and the last label (for example, .com) must not start with a number.

Tip: A warning message appears. If you are using TLS XMPP federation, you should proceed to generate a new TLS certificate.

Delete an Email Domain

You can delete administrator-managed email address domains that are in the local cluster using the **Cisco Unified CM IM and Presence Administration** user interface.

System-managed domains cannot be deleted because they are in use. A system-managed domain automatically becomes an administrator-managed domain if there are no longer users on the system with that email domain (for example, due to user deletion). You can edit or delete administrator-managed domains.

Note: If you delete an administrator-managed domain that is configured on both local and peer clusters, the domain remains in the administrator-managed domains list; however, that domain is marked as configured on the peer cluster only. To completely remove the entry, you must delete the domain from all clusters on which it is configured.

Procedure

1. Log in to the **Cisco Unified CM IM and Presence Administration** user interface. Choose **Presence > Inter-Domain Federation > Email Federated Domains**. The **Find and List Email Domains** window appears displaying all administrator-managed and system-managed email address domains.
2. Choose the administrator-managed domains to delete using one of the following methods, and then click **Delete Selected.**
   - Check the check boxes beside the domains to delete.

- Click **Select All** to select all domains in the list of administrator-managed domains.

3. Click **OK** to confirm the deletion or click Cancel.

Tip: Click **Clear All** to clear all selections.

Serviceability Configuration for Federation

Location of Log File for XMPP Federation

The following log file applies to XMPP federation:

`xmpp-cm-4_0000000X.log located in /var/log/active/epas/trace/xcp/log`

You can also capture logs with the Cisco Unified Real-Time Monitoring Tool (RTMT).

Turn on Logging for Federation

Procedure

1. Log on to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Trace > Configuration**.
2. From the Server drop-down list, chose the IM and Presence Service server, and click **Go**.
3. From the Service Group list box, choose **IM and Presence Services**, and click **Go**.
4. Perform one of the following steps:
   a. For SIP federation, choose the Cisco XCP SIP Federation Connection Manager service from the Service drop-down list, and click **Go**.
   b. For XMPP federation, choose the Cisco XCP XMPP Federation Connection Manager service from the Service drop-down list, and click **Go**.
5. Click **Trace On**.

Choose the Debug Trace Level in the Trace Filter Settings. If you want to enable Debug level on the traces choose Debug for Debug Trace Level.

How to Restart the Cisco XCP Router

Cisco XCP Router

If you make any configuration changes for SIP or XMPP federation configuration, you must restart the Cisco XCP Router on IM and Presence Service. If you restart the Cisco XCP Router, IM and Presence Service automatically restarts all active XCP services.

Note that you must restart the Cisco XCP Router, not turn off and turn on the Cisco XCP Router. If you turn off the Cisco XCP Router, rather than restart this service,IM and Presence Service stops all other XCP services. Subsequently when you then turn on the XCP router, IM and Presence Service does not automatically turn on the other XCP services; you need to manually turn on the other XCP services.

Restarting the Cisco XCP Router

Procedure

1. Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools > Control Center - Network Services**.

2. From the Server drop-down list, choose the server.
3. Click **Go**.
4. In the IM and Presence Services area, click the radio button next to the Cisco XCP Router service.
5. Click **Restart**.
6. Click **OK** when a message indicates that restarting may take a while.

Federation Integration Verification

Verify XMPP Federation Configuration

This procedure describes how to verify the configuration for a federated network between an IM and Presence Service Release 9.0 enterprise deployment, and either a WebEx, an IBM Sametime, or another IM and Presence Service Release 9.0 enterprise deployment.

The procedure below describes the procedure for an IM and Presence Service Release 9.0 and a WebEx deployment. Use this procedure as a guide to verify the other types of XMPP federations.

Procedure

1. Log on to the Cisco Jabber client or the third-party XMPP client connected to the IM and Presence Service Release 9.0 server.
2. Log on to two federated WebEx Connect clients.
3. Perform the following steps on the first WebEx Connect client:
   a. Add the IM and Presence Service user as a contact.
   b. A pop-up message displays on client of the IM and Presence Service user requesting that you accept, block, or ignore the presence subscription from the WebEx Connect user. Accept the subscription.
   c. Check that the IM and Presence Service user and the WebEx Connect user are able to see each other's availability.
4. Perform the following steps on the client of the IM and Presence Service user:
   a. Add the second WebEx Connect user as a contact.
   b. A pop-up should appear on the WebEx Connect client. Accept the subscription.
   c. Check that you can see the availability of the WebEx Connect user.
5. Toggle between the availability states on both the client of the IM and Presence Service user and the WebEx Connect client. Check that the availability state changes for the contacts on each client.
6. Initiate an IM from the client of the IM and Presence Service user to a WebEx Connect contact.
7. Check that the IM window displays on WebEx Connect client with the IM from the IM and Presence Service user.
8. Close the IM window on both clients.
9. Initiate an IM from the WebEx Connect user to the IM and Presence Service user.
10. Check that an IM window displays on the client of the IM and Presence Service user with the IM from the WebEx Connect user.
11. On the client of the IM and Presence Service user, perform the following steps:
    a. Block one of WebEx Connect users.

       Note: If you block from a third-party XMPP client, you only block IM; users can still exchange availability status. To block server-side IM and availability, the user configures their privacy settings from the IM and Presence Service Users' Options interface, or from the Privacy configuration on Cisco Jabber.
    b. Check that this WebEx Connect user now sees that the availability of the IM and Presence Service user as offline. The second WebEx Connect user should still be able to see availability status for the IM and Presence Service user.
    c. On the client of the IM and Presence Service user, the blocked WebEx Connect user should still appear as online, however, you cannot send an IM to the blocked WebEx Connect user.
12. Block the IM and Presence Service user from the WebEx Connect client.
13. Verify that the availability of the WebEx Connect user is no longer available on the client of the IM and Presence Service Service user.

Troubleshooting an XMPP Federation Integration

Check System Troubleshooter

If you deploy multiple IM and Presence Service clusters and you configure XMPP federation, you must turn on XMPP federation on at least one node per cluster.

You must configure the same XMPP federation settings and policy on each cluster; IM and Presence Service does not replicate the XMPP federation configuration across cluster.

The System Troubleshooter reports if XMPP federation settings across clusters are not synchronized. The System Troubleshooter performs the following checks:

Procedure

1. Verify the following :
   a. XMPP federation is enabled consistently across intercluster peers.
   b. The Secure Sockets Layer (SSL) Mode is configured consistently across intercluster peers.
   c. The "Required Valid client-side certificates" is configured consistently across intercluster peers.
   d. The Simple Authentication and Security Layer (SASL) settings are configured consistently across intercluster peers.
   e. The dialback secret is configured consistently across intercluster peers.
   f. The default Admin Policy for XMPP Federation is configured consistently across inter-cluster peers.
   g. The Policy hosts are configured consistently across inter-cluster peers.
2. Log in to the **Cisco Unified CM IM and Presence Service Administration** user interface. Choose **Diagnostics > System Troubleshooter**.
3. Ensure there are green check marks beside the following:
   - Verify the XMPP Federation settings match on all interclustered peers.
   - Verify that SASL settings have been correctly configured for all intercluster peers.
   - Verify that XMPP has been uniformly disabled or enabled on at least one node in each all clusters.
   - Verify that the default Admin Policy is consistent across all intercluster peers.
   - Verify that the Host Policy is consistent across all intercluster peers.

The **System Troubleshooter** provides recommended actions if it reports a problem with any of these checks.

Note: If all tests in **System Troubleshooter** are passed and problems with exchanging IM and availability still persist, check if the **Enable use of Email Address when Federating** setting on the Presence Settings page is configured consistently across intercluster peers.

High Availability for XMPP Federation

High availability for XMPP federation differs from the high availability model for other IM and Presence Service features because it is not tied to the two node sub-cluster model.

To provide high availability for XMPP federation, you must enable two or more IM and Presence Service nodes in your cluster for XMPP federation; having multiple nodes enabled for XMPP federation not only adds scale but it also provides redundancy in the event that any node fails.

High Availability for Outbound Request Routing

IM and Presence Service evenly load balances outbound requests from users within that cluster across all the XMPP federation enabled nodes in the cluster. If any node fails, IM and Presence Service dynamically spreads the outbound traffic across the remaining active nodes within the cluster.

High Availability for Inbound Request Routing

An additional step is required to provide high availability for inbound request routing. To allow an external domain to discover the local IM and Presence Service deployment, a DNS SRV record must be published on a public DNS server. This record resolves to an XMPP federation enabled node. The external domain then connects to the resolved address.

To provide high availability in this model, multiple DNS SRV records must be published for the local IM and Presence Service deployment. Each of these records resolve to one of the XMPP federation-enabled nodes within the local IM and Presence Service deployment.

These records provide a choice of DNS SRV records for the local deployment. If an XMPP federation enabled node fails, the external system has other options from which to connect to the local IM and Presence Service deployment.

Notes: Each published DNS SRV records must have the same priority and weight. This allows a spread of load across all published records, and also allows the external system to correctly reconnect to one of the other nodes with a DNS SRV record in the event of a failure.

DNS SRV records may be published for all or just a subset of XMPP federation enabled nodes. The greater the number of records published, the greater the redundancy in the system for inbound request handling.

If you configure the Chat feature on an IM and Presence Service node in an XMPP federation deployment, you can publish multiple DNS SRV records for chat node aliases also. This allows the external system to find another inbound route to that specific chat node through another XMPP federation node, should any XMPP federation-enabled node fail. Note that this is not high availability for the Chat feature itself, but an extension of the XMPP federation high availability feature for inbound requests addressed to chat node aliases.

Cisco Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)