IM and Presence Service Configuration for XMPP Federation

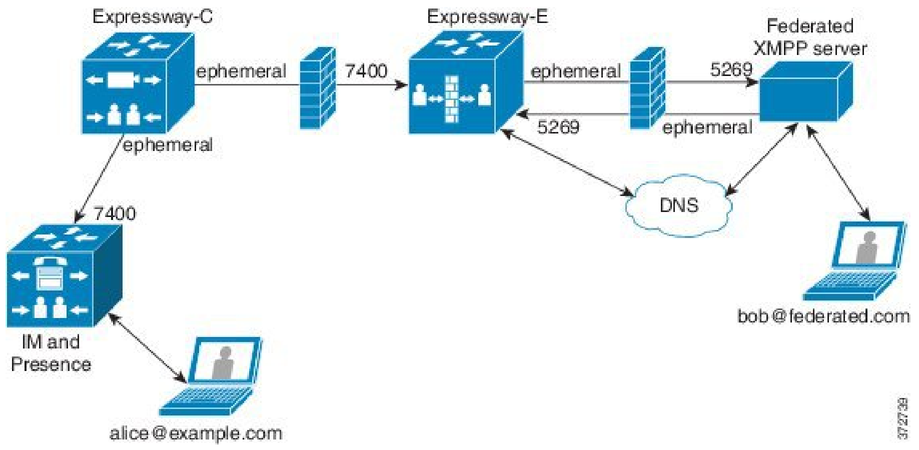
This section provides information on IM and Presence Service Configuration for XMPP Federation.

External XMPP Federation through Cisco Expressway

The preferred method for deploying external XMPP federation is through Cisco Expressway. Cisco Expressway enables users registered to IM and Presence Service to communicate via the Expressway-E with users from a different XMPP deployment. The following diagram shows how XMPP messages are routed from an on-premises IM and Presence Service 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.

Note The Expressway-C and Expressway-E combination is shown here, however the same external XMPP federation functionality is also available when using a VCS Control and VCS Expressway combination. Refer to Cisco Expressway Administrator Guide (X8.2) for more information about the Expressway series option or Cisco TelePresence Video Communication Server Administrator Guide (X8.2) for more information about the VCS option.

Figure 1: External XMPP Federation through Cisco Expressway



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

Supported Federations

Expressway-E supports XMPP federation with the following enterprises:

- Cisco Unified Communications Manager IM and Presence Service Release 9.1 or later
- Cisco WebEx Connect Release 6.x
- XMPP standards-compliant servers

Supported Deployment Configurations

The following XMPP federation deployment options are available:

- external XMPP federation only (terminated on Cisco Expressway)
- internal XMPP federation only (terminated on IM and Presence Service)
- internal and external XMPP federation (terminated on IM and Presence Service) but requires you to configure your firewall to allow inbound connections.

For more information about external XMPP federation through Cisco Expressway, see Cisco Expressway Administrator Guide (X8.2)

Restrictions

- Simultaneous internal XMPP federation terminated on IM and Presence Service and external XMPP federation terminated on Cisco Expressway is not supported.

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

- Expressway-E does not support XMPP address translation (of email addresses, for example). If you are using Expressway-E for XMPP federation, you must use native presence Jabber IDs from IM and Presence Service.

Configure General Settings for XMPP Federation

This section explains the method to Configure General Settings for XMPP Federation.

XMPP Federation Overview

The IM and Presence Service supports XMPP federation with the following enterprises:

- Cisco WebEx Messenger Release 7.x
- IBM Sametime Release 8.2 and 8.5
- IM and Presence Release 9.x or greater

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 the IM and Presence Service, following the procedures we describe in this chapter.

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 cluster.

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 CA authority.
- 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 Servicc 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 off by default.

Procedure

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

In the XMPP Federation Node Status drop-down list, choose **On** .

Step 2 Click **Save**.

Troubleshooting Topics

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.

What to do next -

Configure Security Settings for XMPP Federation

Configure Security Settings for XMPP Federation

Before you begin

- Determine whether the external domain that you are federating with supports TLS connections.
- The TLS and SASL specific settings are only configurable if you select the SSL mode “TLS Optional” or “TLS Required”.
- If you are configuring federation between the IM and Presence Service and IBM using TLS, you must configure the SSL mode “TLS Required”, and you must enable SASL.

Procedure

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

Step 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 domIM and Presence Service ain, and uses the server dialback mechanism to verify the identity of the other server.
b) TLS Optional - attempts to establish a TLS connection with the external domain. If the 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.

Step 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.

Step 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.

Step 5 Check the **Enabling SASL on outbound connections** check box to ensure that the IM and Presence Service sends a SASL auth id to the external domain if the external server requests SASL EXTERNAL.

Step 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 the IM and Presence Service. The IM and Presence Service does not accept any packets from the external server until DNS validates the identity of the external server.

Step 7 Click **Save**.

Tip

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

Related Information

Turn On XMPP Federation on a Node

DNS Configuration for XMPP Federation

This section provides an overview of DNS Configuration for XMPP Federation.

DNS SRV Records for XMPP Federation

To allow the IM and Presence Service to discover a particular XMPP federated domain, the federated enterprise must publish the _xmpp-server DNS SRV record in its public DNS server. Similarly, the 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 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 Communications Manager 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 IM and Presence Administration** and choose **Presence** > **Domains**.

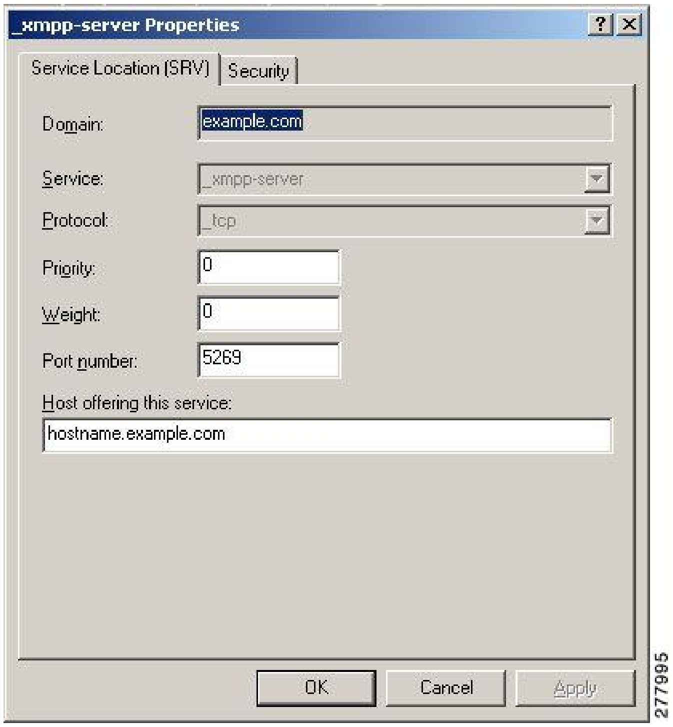
You can also use the **Email Domains for Federation** window to view the list of all email domains in the system if the email address for federation feature is enabled. Log in to the **Cisco Unified IM and Presence Administration** user interface. Choose **Presence** > **Inter-Domain Federation** > **Email 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 2: DNS SRV for _xmpp-server



Domain: example.com

Service: _xmpp-server

Protocol: _tcp

Priority: 0

Weight: 0

Port number: 5269

Host offering this service: hostname.example.com

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 the 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 5269 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. The IM and Presence Service routes all incoming requests from external domains to the node running federation. Internally the IM and Presence Service reroutes the requests to the correct node for the user. The 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 the IM and Presence Service enterprise domain. As a result, the 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 for each domain, the DNS lookup returns multiple results; the IM and Presence Service can route the request to any of the servers that DNS publishes. Internally the IM and Presence Service reroutes the requests to the correct node for the user. The IM and Presence Service routes outgoing requests to any of the nodes running XMPP federation.

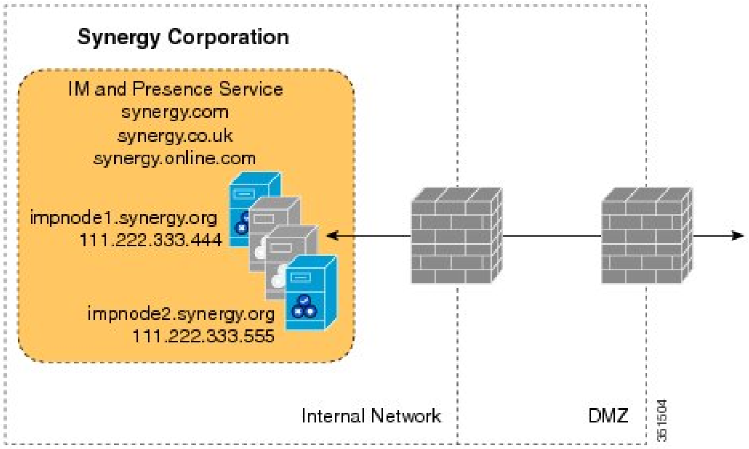
If you have multiple nodes running XMPP federation, you can still choose to publish only one node in the public DNS. With this configuration, the IM and Presence Service routes all incoming requests to that single node, rather than load-balancing the incoming requests across the nodes running XMPP federation.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

XMPP DNS SRVs in an Interdomain Federation Deployment

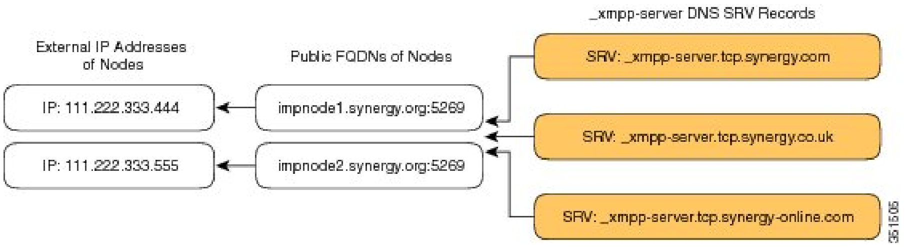
In the following example interdomain federation deployment, two IM and Presence Service nodes are enabled for XMPP federation. A DNS SRV record must be published for each domain that is hosted in the IM and Presence Service deployment. The following figure shows an example interdomain federation deployment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

Figure 3: Multiple Domains 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 4: XMPP DNS SRV Resolving to Public FQDNs of IM and Presence Service Nodes


_xmpp-server DNS SRV Records
External IP Addresses of Nodes
Public FQDNs of Nodes
SRV: _xmpp-server.tcp.synergy.com
IP: 111.222.333.444
impnode1.synergy.org:5269
SRV: _xmpp-server.tcp.synergy.co.uk
IP: 111.222.333.555
impnode2.synergy.org:5269
SRV: _xmpp-server.tcp.synergy-online.com
351505

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

Related Information -

DNS SRV Records for Chat Feature for XMPP Federation

DNS SRV Records for Chat Feature for XMPP Federation

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 to use some arbitrary port other than 5269, for example, 25269. 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 XCP XMPP Federation Connection Manager on the chat node.

For information on configuring the Chat feature on the IM and Presence Service, see *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Maanger* .

Related Information -

DNS SRV Records for Chat Feature for XMPP Federation

Configure DNS SRV Record for Chat Node for XMPP Federation

Procedure

Step 1 To retrieve the chat node alias:

a) Log in to the **Cisco Unified CM IM and Presence Administration** user 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`

Step 2 In the public DNS server for the `example.com` domain, create the StandAloneCluster domain.

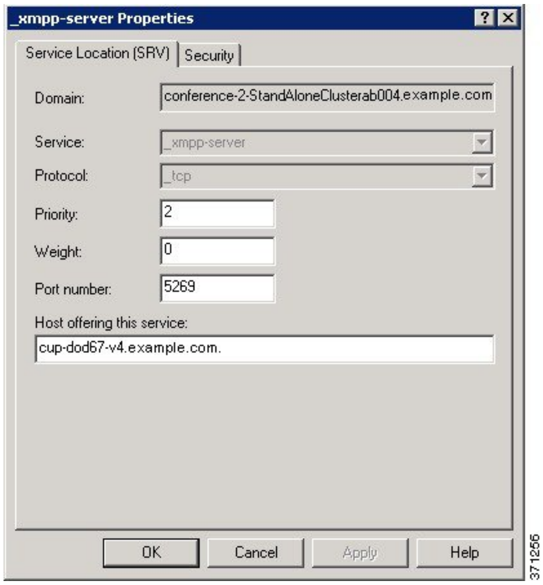
Step 3 In the StandAloneClusterdomain, create the conference-2domain.

Step 4 In the conference-2 domain, create the _tcp domain.

Step 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 a sample DNS configuration records.

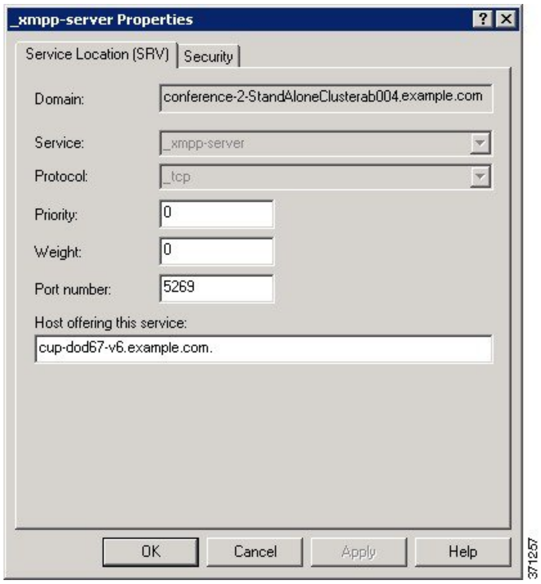
Note If the text conference server alias is `conference-2-StandAloneCluster.example.com` then the domain in Step 2 is conference-2-StandAloneCluster, and you skip Step 3. In Step 4, create the _tcp domain under conference-2-StandAloneCluster.

Figure 5: IPv4 DNS SRV Record for _xmpp-server for Chat Feature



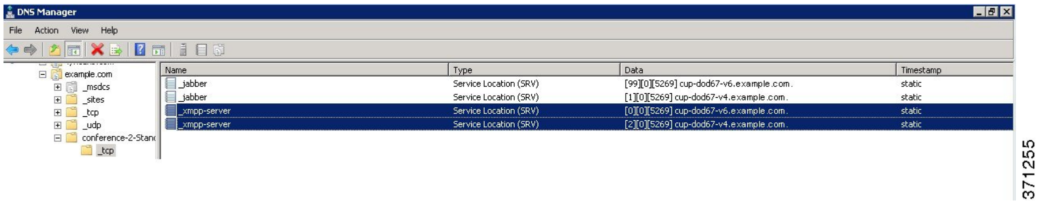
Domain: conference-2-StandAloneClusterab004.example.com
Service: _xmpp-server
Protocol: _tcp
Priority: 2
Weight: 0
Port number: 5269
Host offering this service: cup-dod67-v4.example.com.

Figure 6: IPv6 DNS SRV Record for _xmpp-server for Chat Feature



Domain: conference-2-StandAloneClusterab004.example.com
Service: _xmpp-server
Protocol: _tcp
Priority: 0
Weight: 0
Port number: 5269
Host offering this service: cup-dod67-v6.example.com.

Figure 7: DNS Configuration for Chat Feature



Name	Type	Data	Timestamp
_jabber	Service Location (SRV)	[99][0][5269] cup-dod67-v6.example.com.	static
_jabber	Service Location (SRV)	[1][0][5269] cup-dod67-v4.example.com.	static
_xmpp-server	Service Location (SRV)	[0][0][5269] cup-dod67-v6.example.com.	static
_xmpp-server	Service Location (SRV)	[2][0][5269] cup-dod67-v4.example.com.	static

Configure MFT on XMPP Federation Without TLS

In this scenario, you must perform the following two extra steps for the MFT over XMPP Federation feature to work:

1. Extract file transfer aliases.
2. Create the DNS SRV records for file transfer aliases extracted in the previous step.

Before you begin

- Configure DNS SRV records for XMPP Federation. For more information, see DNS SRV Records for XMPP Federation, on page 5.
- Configure the Managed File Tranfer (MFT) feature as described in the Configuration and Administration of the IM and Presence Service guide for your release of Unified CM.

Procedure

Step 1 To extract the file transfer aliases:

a) On each IM and Presence Service node where MFT is configured, create a CLI session and run **file build log cisco_xcp_config_mgr**.
b) Download the newly created archive and open `cm-5.xml` file.
c) The file transfer alias is stored with other MFT parameters in a common section of the file. In this example, you can find the file transfer alias in the following line:

```
<host-filter xmlns="http://www.jabber.com/config/cm/aft">
filetransfer-4-StandAloneClusterd41e3.cow.com

</host-filter>
```

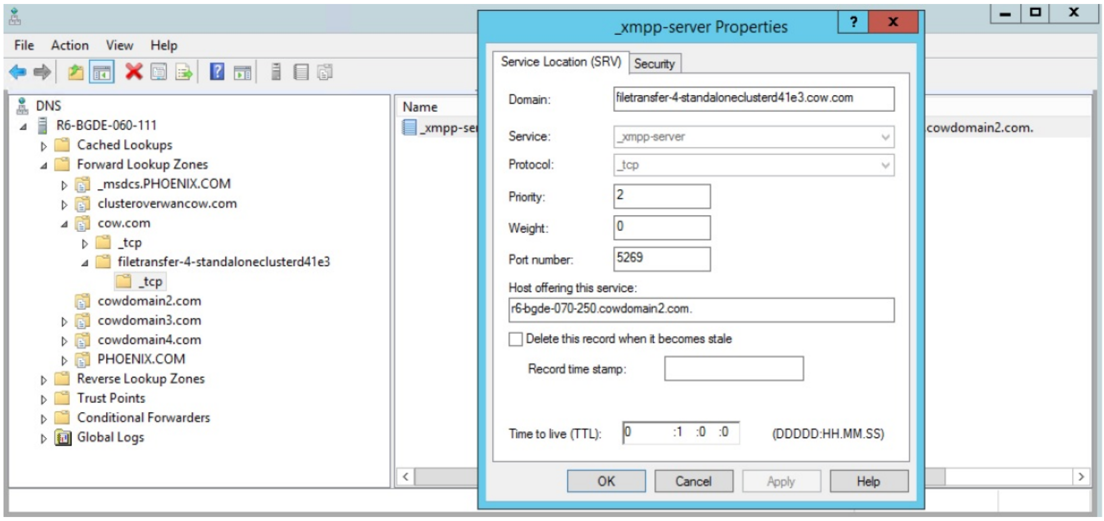
Important You must extract the file transfer aliases from each IM and Presence Service node which has MFT configured individually. Each node has its own unique alias that needs to be added to the DNS servers.

Step 2 Add aliases to the DNS server.

The file transfer alias extracted in the previous step belongs to the IM and Presence Service Publisher node (**r6-bgde-070-250.cowdomain2.com**) on the local side. We will use this alias as an example of how DNS records should be added.

The domains need to be added to DNS servers in the same way as the chat node aliases as described in Configure DNS SRV Record for Chat Node for XMPP Federation, on page 9.

In the following screenshot, you can view the DNS SRV record for the file transfer alias.



_xmpp-server Properties

Domain: filetransfer-4-standaloneclusterd41e3.cow.com

Service: _xmpp-server

Protocol: _tcp

Priority: 2

Weight: 0

Port number: 5269

Host offering this service: r6-bgde-070-250.cowdomain2.com.

☐ Delete this record when it becomes stale

Record time stamp:

Time to live (TTL): 0 :1 :0 :0 (DDDDD:HH.MM.SS)

Configure MFT on XMPP Federation with TLS

In this scenario, you must perform another step after extracting file transfer aliases and adding DNS SRV records as described in Configure MFT on XMPP Federation Without TLS, on page 11.

Perform the following steps on the local side:

Before you begin

Note

- We recommend that you use this method to configure MFT on XMPP Federation.
- To manually add file transfer aliases to the certificate, you must generate a CSR for the Multi SAN certificate. This is not possible in single node deployments. This is a limitation of this method.
- Use the following settings on the XMPP federation page on both sides:
    - **Security mode** must be set to TLS required.
    - The **Require client-side security certificates** checkbox must be checked.

For MFT on XMPP TLS federation to work, the cup -xmpp-s2s certificate must contain file transfer aliases. On IM and Presence Service, these file transfer aliases are not added automatically to the Certificate Signing Request (CSR). This default behavior can be overcome on a multinode IM and Presence Service cluster by generating and signing a Multi SAN certificate. However, on a single node cluster, it is impossible to generate a Multi SAN certificate CSR.

- Configure DNS SRV records for XMPP Federation. For more information, see DNS SRV Records for XMPP Federation, on page 5.
- Configure the Managed File Transfer (MFT) feature as described in the Configuration and Administration of the IM and Presence Service guide for your release of Unified CM.

Procedure

Step 1 After extracting the file transfer aliases from all the nodes of the local cluster, generate a CSR for the MultiSan certificate.

Step 2 Log in to the **Cisco Unified IM and Presence OS Administration** page and choose **Security** > **Certificate Management**.

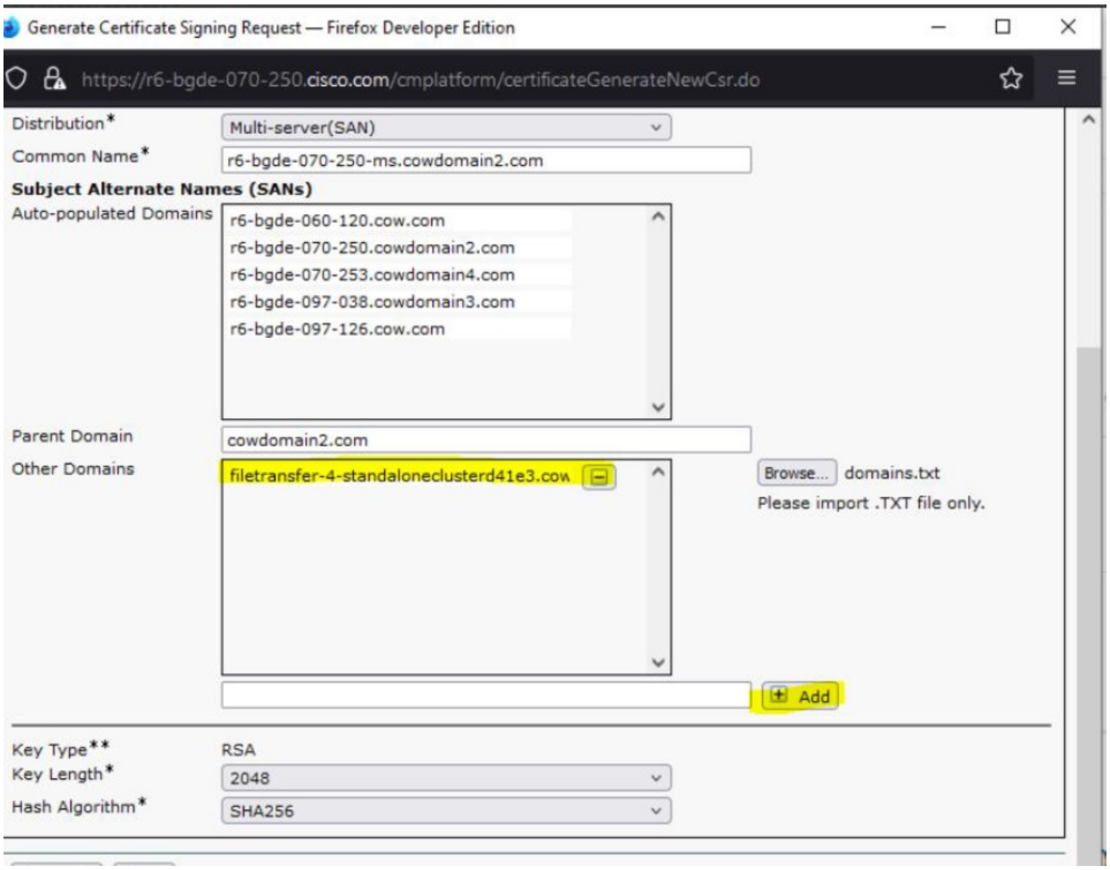
The **Certificate List** window appears.

Step 3 Click **Generate CSR**.

Step 4 From the **Certificate Purpose** drop-down list, choose **cup-xmpp-s2s**.

Step 5 From the **Distribution** drop-down list, choose **Multi-server(SAN)**.

Step 6 In the **Other Domains** section, add all file transfer aliases from the local cluster as shown in the following screenshot.



Generate Certificate Signing Request — Firefox Developer Edition

https://r6-bgde-070-250.cisco.com/cmplatform/certificateGenerateNewCsr.do

Distribution* Multi-server(SAN)

Common Name* r6-bgde-070-250-ms.cowdomain2.com

Subject Alternate Names (SANs)

Auto-populated Domains
r6-bgde-060-120.cow.com
r6-bgde-070-250.cowdomain2.com
r6-bgde-070-253.cowdomain4.com
r6-bgde-097-038.cowdomain3.com
r6-bgde-097-126.cow.com

Parent Domain cowdomain2.com

Other Domains filetransfer-4-standaloneclusterd41e3.cow

Key Type** RSA

Key Length* 2048

Hash Algorithm* SHA256

Step 7 Sign the cup-xmpp-s2s certificate using Certificate Authority.

Step 8 Upload the Root certificate and the newly signed Multi-SAN certificate according to the steps described in Upload a CA-Signed Certificate for XMPP Federation.

Step 9 Upload the Root certificate in the cup-xmpp-trust on the federated side.

Note Repeat all the above steps on the federated side.

Policy Settings Configuration for XMPP Federation

This section provides various 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** - The 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 the 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 the IM and Presence Service to send outbound broadcasts to the specified domain, but the IM and Presence Service does not receive responses.

Related Information -

Configure Policy for XMPP Federation

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, the IM and Presence Service restarts all the XCP services.

Procedure

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

Step 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.

Step 3 To configure a domain on the policy exception list:

a) Click **Add New**.
b) Specify the domain name or the hostname of the external server.
c) Specify the direction to apply the policy exception.
d) Click **Save** on the policy exception window.

Step 4 Click **Save** on the policy window.

Tip:

See the Online Help for federation policy recommendations.

Related Information -

Policy Exception Configuration

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 following NAT commands:

Procedure

	Command or Action	Purpose
Step 1	`nat (inside,outside) source static obj_host_private_imp1_ip obj_host_public_imp_ip service`	
Step 2	`obj_udp_source_eq_5269 obj_udp_source_eq_5269`	
Step 3	`nat (inside,outside) source static obj_host_private_imp1_ip obj_host_public_imp_ip service`	
Step 4	`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)
Step 5	`nat (inside,outside) source static obj_host_private_imp2_ip obj_host_public_imp_ip service`	
Step 6	`obj_udp_source_eq_5269 obj_udp_source_eq_25269`	
Step 7	`nat (inside,outside) source static obj_host_private_imp2_ip obj_host_public_imp_ip service`	
Step 8	`obj_tcp_source_eq_5269 obj_tcp_source_eq_25269`	

	Command or Action	Purpose
Step 9	**nat (inside,outside) source static** *obj_host_private_imp3_ip* *obj_host_public_imp_ip* **service**	
Step 10	*obj_udp_source_eq_5269* *obj_udp_source_eq_35269*	
Step 11	**nat (inside,outside) source static** *obj_host_private_imp3_ip* *obj_host_public_imp_ip* **service**	
Step 12	*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)
Step 13	**nat (inside,outside) source static** *obj_host_private_imp2_ip* *obj_host_public_imp2_ip* **service**	
Step 14	*obj_udp_source_eq_5269* *obj_udp_source_eq_5269*	
Step 15	**nat (inside,outside) source static** *obj_host_private_imp2_ip* *obj_host_public_imp2_ip* **service**	
Step 16	*obj_tcp_source_eq_5269* *obj_tcp_source_eq_5269*	
Step 17	**nat (inside,outside) source static** *obj_host_private_imp3_ip* *obj_host_public_imp3_ip* **service**	
Step 18	*obj_udp_source_eq_5269* *obj_udp_source_eq_5269*	
Step 19	**nat (inside,outside) source static** *obj_host_private_imp3_ip* *obj_host_public_imp_ip* **service**	
Step 20	*obj_tcp_source_eq_5269* *obj_tcp_source_eq_5269*	**Related Information -** Cisco Adaptive Security Appliance Configuration for SIP Federation

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 CM IM and Presence Administration, see Turn On XMPP Federation on a Node, on page 4.

Procedure

Step 1 Log in to the **Cisco Unified IM and Presence Serviceability** user interface. Choose **Tools** > **Service Activation**.

Step 2 From the Server drop-down list, select the server.

Step 3 Click **Go**.

Step 4 In the IM and Presence Service area, click the button next to the **Cisco XCP XMPP Federation Connection Manager** service.

Step 5 Click **Save**.

Related Information -

Serviceability Configuration for Federation