IM and Presence Service Configuration for XMPP Federation

Configure General Settings for XMPP Federation

DNS Configuration for XMPP Federation, page 4
Policy Settings Configuration for XMPP Federation, page 9
Configure the Cisco Adaptive Security Appliance for XMPP Federation, page 10
Email for Federation Enablement, page 12
Turn On XMPP Federation Service, page 12

Configure General Settings for XMPP Federation

XMPP Federation Overview

The 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 Release 9.x or greater

Note

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

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 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 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.
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 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 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.
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.

The required DNS record is:

```text
_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 1: DNS SRV for _xmpp-server**

![DNS SRV Properties](image)

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

**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 2: 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 3: 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 (NAT) to the internal IP address of the node. The FQDN of the nodes must be publicly resolvable to a public IP address.

**Related Topics**

- DNS SRV Records for Chat Feature for XMPP Federation, on page 6

**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**

<table>
<thead>
<tr>
<th>Deployment</th>
<th>Chat Request Routing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single public IP address, multiple nodes internally</td>
<td>To route all chat requests to the XMPP federation node, and then on to the chat node:</td>
</tr>
<tr>
<td></td>
<td>1. Configure the DNS SRV for the chat node alias to point to port 5269.</td>
</tr>
<tr>
<td></td>
<td>2. Configure a NAT command configured on Cisco Adaptive Security Appliance or firewall/NAT server that maps publicIPAddress:5269 to XMPPFederationNodePrivateIPAddress:5269.</td>
</tr>
<tr>
<td>Multiple public IP addresses, multiple nodes internally</td>
<td>If you have multiple public IP addresses, you can choose to route chat requests directly to the appropriate chat node.</td>
</tr>
<tr>
<td></td>
<td>1. Configure the DNS SRV for the chat node to use some arbitrary port other than 5269, for example, 25269.</td>
</tr>
<tr>
<td></td>
<td>2. Configure a NAT command on Cisco Adaptive Security Appliance or firewall/NAT server that maps textChatServerPublicIPAddress:25269 to textChatServerPrivateIPAddress:5269.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
</tbody>
</table>

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 Manager*.

**Related Topics**

Configure DNS SRV Record for Chat Node for XMPP Federation, on page 7

---

**Configure DNS SRV Record for Chat Node for XMPP Federation**

**Procedure**

**Step 1**

To retrieve the chat node alias:


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 StandAloneCluster domain, create the conference-2 domain.

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

**Step 5**
In the _tcp domain, create a new DNS SRV record for _xmpp-server. See the following figures for a sample DNS configuration.

*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 4: DNS SRV for "_xmpp-server" for Chat Feature*

*Figure 5: DNS Configuration for Chat Feature*
Related Topics

DNS SRV Records for XMPP Federation, on page 4

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 Topics

Configure Policy for XMPP Federation, on page 10
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 Topics

Policy Exception Configuration, on page 9

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:
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:

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
  obj_tcp_source_eq_5269 obj_tcp_source_eq_5269

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_5269
  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
  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
  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_imp_ip2_ip service
  obj_udp_source_eq_5269 obj_udp_source_eq_5269
  obj_tcp_source_eq_5269 obj_tcp_source_eq_5269

nat (inside,outside) source static obj_host_private_imp3_ip obj_host_public_imp_ip3_ip service
  obj_udp_source_eq_5269 obj_udp_source_eq_5269
  obj_tcp_source_eq_5269 obj_tcp_source_eq_5269
Email for Federation Enablement

When you turn on the email address for federation feature, the 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 users 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 userid 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.

To turn on email for XMPP federation, follow the same procedure as for SIP federation, see the procedure in the Related Topics section below.

Related Topics

Email Address for Federation Considerations
Turn On Email for 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 2.
Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in to the <strong>Cisco Unified IM and Presence Serviceability</strong> user interface. Choose <strong>Tools &gt; Service Activation</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>From the Server drop-down list, select the server.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Go</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the IM and Presence Services area, click the button next to the <strong>Cisco XCP XMPP Federation Connection Manager</strong> service.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

Related Topics

- Serviceability Configuration for Federation