IM and Presence Service Configuration for SIP Federation

IM and Presence Service Release 9.0 or later supports interdomain federation with Microsoft Lync. For IM and Presence Service Release 9.0 or later, any reference to interdomain federation with OCS also includes Microsoft Lync, unless explicitly stated otherwise.

- SIP Proxy Domain on the IM and Presence Service, page 1
- Add a SIP Federated Domain, page 1
- Routing Configuration on IM and Presence Service, page 2
- Configure Federation Routing Parameters, page 4
- Configuration of Security Settings on IM and Presence Service, page 5
- Routing Information Configuration for AOL Federation, page 7
- Email Address Configuration for Federation, page 9
- Turn On the SIP Federation Service, page 11

SIP Proxy Domain on the IM and Presence Service

If you change the SIP proxy domain on the IM and Presence Service before you configure federation, as part of the SIP proxy domain change procedure you must also change the Federation Routing IM and Presence FQDN parameter. For the correct sequence of steps for changing the SIP proxy domain on the IM and Presence Service, see Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager.

Add a SIP Federated Domain

Note

The IM and Presence Service, Release 9.0 supports SIP federation with AOL.
When you configure a federated domain entry, the IM and Presence Service automatically adds the incoming ACL for the federated domain entry. You can see the incoming ACL associated with a federated domain on the Cisco Unified CM IM and Presence Administration user interface, but you cannot modify or delete it. You can only delete the incoming ACL when you delete the (associated) federated domain entry.

If you are configuring SIP federation with AOL, note the following:

- The AOL network can comprise of both public communities and hosted networks. You must configure each of these domains as SIP federated domain of type AOL on the IM and Presence Service.
- To handle users in a hosted domain such as "user@acompany.com", you must configure a SIP federated domain of type AOL on the IM and Presence Service for "acompany.com".
- To handle users in domains "aol.com" and "aim.com", you only need to add one SIP federated domain for "aol.com" on the IM and Presence Service. The AOL network allows you to address "user@aim.com" as "user@aol.com".

Procedure

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

Step 2 Click Add New.

Step 3 Enter the federated domain name in the Domain Name field.

Step 4 Enter a description that identifies the federated domain in the Description field. This text string is displayed to the user in the Cisco Jabber Release 8.x privacy preferences available from the Manage Domains tab. Therefore make sure you enter a domain name that is easily-recognizable to the user.

Step 5 Choose one of these integrations:
   a) Inter-domain to OCS/Lync
   b) Inter-domain to AOL

Step 6 If you are configuring federation with Microsoft OCS, ensure that the check box for Direct Federation is unchecked.

Step 7 Click Save.

Step 8 After you add, edit, or delete a SIP federated domain, restart the Cisco XCP Router. Log in to the Cisco Unified IM and Presence Serviceability user interface. Choose Tools > Control Center - Network Services When you restart Cisco XCP Router, this causes a restart of all XCP services on the IM and Presence Service.

Routing Configuration on IM and Presence Service

DNS Configuration for SIP Federation

In the local IM and Presence Service enterprise, IM and Presence Service must publish a DNS SRV record for the IM and Presence Service domain to make it possible for other domains to discover the IM and Presence Service node through DNS SRV.
The Microsoft enterprise deployment requires the IM and Presence Service to publish a DNS SRV record for the IM and Presence Service domain because you configure the IM and Presence Service as a Public IM Provider on the Access Edge server.

In the IM and Presence Service enterprise deployment, you need to configure a DNS SRV record that points to `_sipfederationtls._tcp.imp_domain` over port 5061 where `imp_domain` is the name of the IM and Presence Service domain. This DNS SRV should point to the public FQDN of the routing IM and Presence Service node. This FQDN must be publicly resolvable.

In order for the IM and Presence Service to discover the external domain, a DNS SRV record must exist in the DNS server of the external domain that points to the FQDN of the external interface of the external domain.

If you configure SIP federation with AOL, AOL routes based on FQDN, so you just require the FQDN of the routing IM and Presence Service node to be publicly resolvable. AOL does not perform a DNS SRV lookup; instead it statically configures the FQDN of the IM and Presence Service so it requires this FQDN to be publicly resolvable.

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

```
nslookup -type=srv _sipfederationtls._tcp.domain
```

If the IM and Presence Service cannot resolve the external enterprise through a public DNS lookup, you must configure static routes in your deployment.

**Related Topic**

Configure Static Routes Using TLS, on page 3

---

**Configure Static Routes Using TLS**

**Note**

Static route configuration is only applicable to SIP federation.

If the IM and Presence Service node cannot discover the external domain using DNS SRV, you must configure a static route on IM and Presence Service that points to the external interface of the external domain.

**Procedure**

**Step 1**

Log in to the Cisco Unified CM IM and Presence Administration user interface. Choose Presence > Routing > Static Routes.

**Step 2**

Configure the static route parameters as follows:

- The destination pattern value must be configured such that the external enterprise domain is reversed. For example if the domain is "domaina.com" then the Destination Pattern value must be ".com.domaina.*".
- The Next Hop value is the FQDN or IP address of the external Access Edge for federation with Microsoft OCS, or the FQDN or IP address of the AOL SIP Access Gateway for federation with AOL.
- The Next Hop Port number is 5061.
The Route Type value is domain.

• The Protocol Type is TLS.

**Step 3** Click Save.

**Related Topics**

Configure an IM and Presence Service Domain from the CLI, on page 4

## Configure an IM and Presence Service Domain from the CLI

If you do not enable DHCP, use this procedure to configure the IM and Presence Service domain from the CLI.

**Procedure**

**Step 1** Log in to the administrator CLI on the IM and Presence Service. Enter this command to display the current network settings:

```
show network eth0
```

**Step 2** If no domain exists and you do not enable DHCP, configure the domain to be the same as the IM and Presence Service proxy domain. Enter this command:

```
set network domain domain_name
```

**Step 3** Enter y at the prompt to confirm the changes. The node automatically restarts. This can take up to 5 minutes.

**Step 4** When the node restarts, enter this command to confirm you have configured the domain:

```
show network eth0
```

## Configure Federation Routing Parameters

**Before You Begin**

When you first install the IM and Presence Service, the federation routing parameter is automatically set to the FQDN of the publisher node, the IM and Presence Service passes this value to each subscriber node.
Procedure

Step 1 Log in to the Cisco Unified CM IM and Presence Administration user interface. Choose System > Service Parameters.

Step 2 Choose the IM and Presence Service node from the Server drop-down list.

Step 3 Choose Cisco SIP Proxy from the Service drop-down list.

Step 4 Enter the public FQDN value for the Federation Routing IM and Presence FQDN parameter in the Federation Routing Parameters (Clusterwide) area.

  • This FQDN value must correspond to the _sipfederationtls entry in the public DNS for that IM and Presence Service domain. For example:

    ◦ If the presence server FQDN is imp1.cisco.com and the DNS SRV is _sipinternaltls._tcp.cisco.com (pointing to FQDN imp1-public.cisco.com), the Federation Routing FQDN can be imp1-public.cisco.com.

    ◦ If the presence server FQDN is imp1.cisco.com and the DNS SRV is _sipinternaltls._tcp.extcisco.com (imp1-public.ciscoext.com), the Federation Routing FQDN can be imp1-public.ciscoext.com.

Note This parameter does not apply for federation where there is a firewall (ASA) with TLS Proxy between the presence server and Lync Server and where the Direct Federation check box is checked under Presence > Inter-domain federation > SIP Federation.

  • If you assign users to the routing IM and Presence Service node, this FQDN value cannot be the same as the actual FQDN of the routing IM and Presence Service node.

Step 5 Click Save.

What to Do Next

If you changed the Federation Routing FQDN parameter on the IM and Presence Service, restart the Cisco UP XCP Router. Log in to the Cisco Unified Serviceability user interface, choose Tools > Control Center - Network Services in Cisco Unified Serviceability.

When you restart Cisco UP XCP Router, this causes a restart of all XCP services on the IM and Presence Service.

Related Topics

  Turn On Email for Federation, on page 11

Configuration of Security Settings on IM and Presence Service

Note This procedure is only applicable if you do not have Cisco Adaptive Security Appliance in your federation deployment, for example, if you deploy federation within your enterprise and you want a secure TLS connection.
Create a New TLS Peer Subject

When you import the Cisco Adaptive Security Appliance security certificate to the IM and Presence Service, the IM and Presence Service automatically adds the Cisco Adaptive Security Appliance as a TLS peer subject. Therefore you do not need to manually add the Cisco Adaptive Security Appliance as a TLS peer subject on the IM and Presence Service.

Procedure

Step 1 Log in to the Cisco Unified CM IM and Presence Administration user interface. Choose System > Security > TLS Peer Subjects.
Step 2 Click Add New.
Step 3 Enter one of the following values:
   a) If you configure SIP federation with Microsoft OCS, enter the external FQDN of the Access Edge Server in the Peer Subject Name field. This value must match the subject CN of the certificate that the Microsoft Access Edge server presents.
   b) If you configure SIP federation with AOL, enter the external FQDN of the AOL SIP Access Gateway. This value must match the subject CN of the certificate that the AOL SIP Access Gateway presents.
Step 4 Enter the name of the external server in the Description field.
Step 5 Click Save.

What to Do Next
Add TLS Peer to Selected TLS Peer Subjects List, on page 6

Related Topics
Import Self-Signed Certificate onto the IM and Presence Service

Add TLS Peer to Selected TLS Peer Subjects List

Before You Begin
Create a new TLS peer subject.
Procedure

Step 1 Log in to the Cisco Unified CM IM and Presence Administration user interface. Choose System > Security > TLS Context Configuration.
Step 2 Click Find.
Step 3 Click Default_Cisco_SIP_Proxy_Peer_Auth_TLS_Context.
Step 4 Choose all ciphers from the list of available TLS ciphers.
Step 5 Click the arrow to move these ciphers to Selected TLS Ciphers.
Step 6 From the list of available TLS peer subjects, click the TLS peer subject that you configured in the previous section.
Step 7 Click the arrow to move the TLS peer subject to Selected TLS Peer Subjects.
Step 8 Check the Disable Empty TLS Fragments check box when you federate with Microsoft OCS.
Step 9 Click Save.
Step 10 Restart the Cisco SIP Proxy service.

Note If you deploy AOL and Microsoft OCS federation on the same IM and Presence Service node, checking the Disable Empty TLS Fragments check box does not impact AOL federation.

Related Topics

Create a New TLS Peer Subject, on page 6

Routing Information Configuration for AOL Federation

Route SIP Requests for SIP Federation with AOL

Note The IM and Presence Service Release 9.0 supports SIP federation with AOL.

SIP federation with AOL enables the IM and Presence Service users to federate with the following users:

- Users of AOL public communities, for example, aim.com,aol.com.
- Users of an enterprise whose domain is hosted by AOL.
- Users of an external enterprise that federates with AOL. The IM and Presence Service could use AOL as a clearing house to federate with these external enterprises.

For example, AOL hosts an enterprise with a domain called "hosteddomain.com", and there is an enterprise federating with AOL with a domain called "acompany.com". You can add a SIP federation domain entry for each of these domains on the IM and Presence Service to allow the IM and Presence Service users to federate with users@hosteddomain.com and users@acompany.com.
The routing logic on the IM and Presence Service is enhanced to support routing to domains that federate through AOL. When you configure SIP federation with AOL, the IM and Presence Service routes messages based on the default federation routing domain. The default value for this domain is "aol.com".

**Note**

The routing described here is only applicable when you configure a federated domain of type "Inter-domain to AOL".

If the federated user belongs to one of the hosted domains in AOL (a domain other than aol.com), the IM and Presence Service performs the following steps:

**Procedure**

**Step 1** A lookup for a static route for the hosted domain. If no static route exists, the IM and Presence Service performs,

**Step 2** A DNS SRV lookup for hosted domain. If the lookup returns nothing, the IM and Presence Service performs,

**Step 3** A lookup for a static route for the default federation routing domain (aol.com by default). If no static route exists, the IM and Presence Service performs,

**Step 4** A DNS SRV lookup for the default federation routing domain (aol.com by default).

If the federated user is in the default AOL domain (user@aol.com), the IM and Presence Service performs the following steps:

**Step 5** A lookup for a static route for default AOL domain (aol.com by default). If no static route exists the IM and Presence Service performs,

**Step 6** A DNS SRV lookup for default federation routing domain (aol.com by default).

**Related Topics**

Change the Default Federation Routing Domain for SIP Federation with AOL, on page 8

**Change the Default Federation Routing Domain for SIP Federation with AOL**

**Note**

The IM and Presence Service, Release 9.0 supports SIP federation with AOL.

Generally you should not need to change the value of the default federation routing domain, unless the AOL enterprise changes the domain that the AOL server resolves to.

**Before You Begin**

Read the topic on routing SIP requests for SIP Federation with AOL
Procedure

Step 1 Log in to the Cisco Unified CM IM and Presence Administration user interface. Choose System > Service Parameters.

Step 2 Choose the IM and Presence Service node from the Server drop-down list.

Step 3 Choose Cisco SIP Proxy from the Service drop-down list.

Step 4 In the Federation Routing Parameters (Clusterwide) area, verify or edit the value of the Default Federation Routing Domain parameter.

Step 5 Click Save if you change the value of the Default Federation Routing Domain parameter.

Step 6 You need to restart the Cisco XCP Router if you change the value of the Default Federation Routing Domain parameter. Log in to the Cisco Unified IM and Presence Serviceability user interface. Choose Tools > Control Center - Network Services to restart the Cisco XCP Router.

Related Topics

Route SIP Requests for SIP Federation with AOL, on page 7

Email Address Configuration for Federation

Note This section applies to both SIP and XMPP federation.

Email Address for Federation Considerations

When you configure the IM and Presence Service to use the email address for SIP or XMPP federation, the IM and Presence Service changes the IM address of the local user from "userid@domain" to their 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, the 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, the IM and Presence Service defaults to using the 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, the IM and Presence Service drops these requests (even if a valid email address is configured for the user).
The IM and Presence Service does not support email aliases for the email address for federation feature.

**Note**
This feature applies to both SIP and XMPP federation.

### Email Domain for Federation

If the email domain for federation is different to the SIP Proxy domain value that you configure on the **Cluster Topology Settings** window on the **Cisco Unified CM IM and Presence Administration** user interface, follow these steps:

- Configure the **Federation Routing IM and Presence FQDN** parameter value under **Proxy Service Parameters** to contain the email domain for federation rather than the SIP Proxy domain. Note that this step applies to both XMPP and SIP federation.
- Make sure that you publish the email domain for the federation DNS SRV records in the public DNS server:
  - `_xmpp-server._tcp.email-domain`
  - `_sipfederationtls._tcp.email-domain`

### 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 the 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 the 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, the IM and Presence Service user does NOT need to change anything on the client when they connect to the IM and Presence Service, nor do they interact any differently with the IM and Presence Service node.

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

Step 1
Log in to the Cisco Unified CM IM and Presence Administration user interface. Choose Presence > Settings.

Step 2
Check the Enable use of Email Address when Federating check box.

Step 3
Read the warning message, and click OK.

Step 4
Click Save.

Step 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.

Related Topics
Configure Federation Routing Parameters, on page 4

Turn On the SIP Federation Service

You need to turn on the Cisco XCP SIP Federation Connection Manager service on each IM and Presence Service node. This turns on the SIP Federation feature for each user that you provision on the node. You must perform this procedure on each node in the cluster.
Procedure

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

Step 2 Choose the server from the Server drop-down list.

Step 3 Click Go.

Step 4 Click the button next to the Cisco XCP SIP Federation Connection Manager service in the IM and Presence Services section.

Step 5 Click Save.

Step 6 The Cisco SIP Proxy service must be running for SIP federation to work. Log in to the Cisco Unified IM and Presence Serviceability user interface. Choose Tools > Feature Services and verify that the Cisco SIP Proxy service is running.

Related Topics

Use of Logging for Federation