IM and Presence Service Configuration for SIP Federation

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

Add a SIP Federated Domain

Note SIP federation and Remote Call Control (RCC) do not work together on the same IM and Presence Service cluster. This is because for SIP federation a user cannot be licensed for both Cisco IM and Presence Service and Microsoft Lync/S4B, but for RCC a user must be licensed for Cisco IM and Presence Service and Microsoft Lync/S4b at the same time.

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.

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 **Inter-domain to Lync/S4B**

Step 6 If you are configuring federation with Microsoft, 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

This section explains the concept of 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 each local IM and Presence Service domain so that other domains can discover the IM and Presence Service node through DNS SRV. Each of the DNS SRV records must resolve to the same public IP address.

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 5061where *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. 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.

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

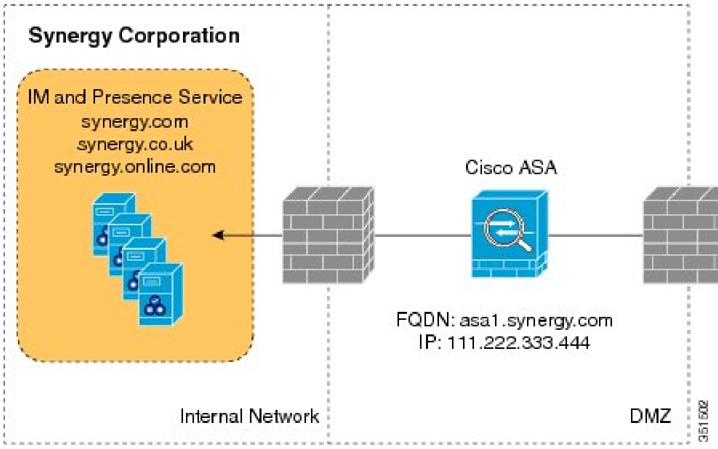
```
nslookupset type=srv _sipfederationtls._tcp.domain
```

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

SIP DNS SRVs in an Interdomain Federation Deployment

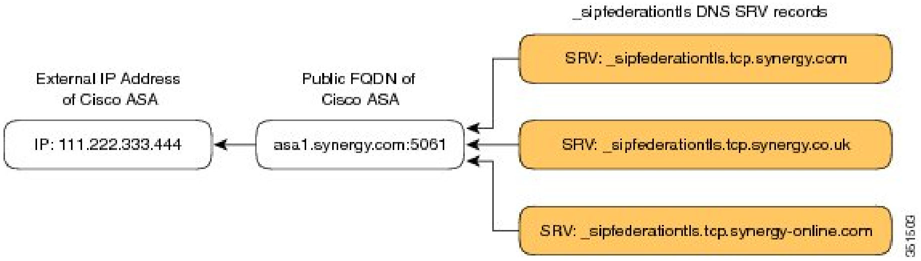
In the following example, multiple local domains must all resolve to the same Public FQDN and a DNS SRV record must be published for each domain that is hosted in the IM and Presence Service deployment. The following figure shows an example interdomain federation deployment with three local domains. You must publish a _sipfederationtls DNS SRV record for each domain.

Figure 1: Multiple Domains in a SIP-Based Federated Interdomain Deployment



Each DNS SRV record must resolve to the FQDN of the external (public) IP address of the Cisco Expressway-C that is deployed in the DMZ (port 5061), as shown in the following figure.

Figure 2: SIP DNS SRV Resolving to FQDN of the Cisco Expressway-C


_sipfederationtls DNS SRV records
SRV: _sipfederationtls.tcp.synergy.com
SRV: _sipfederationtls.tcp.synergy.co.uk
SRV: _sipfederationtls.tcp.synergy-online.com
External IP Address of Cisco ASA
IP: 111.222.333.444
Public FQDN of Cisco ASA
asa1.synergy.com:5061
351503

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.

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 a Microsoft server.
- The Next Hop Port number is **5061**.
- The Route Type value is **domain**.
- The Protocol Type is **TLS**.

Step 3 Click **Save**.

Configure Federation Routing Parameters

Before you begin

Use this procedure if you need to reset the Federation routing parameter. By default, this paramter is set at installation to the FQDN of the publisher node automatically. The IM and Presence Service passes this value to each subscriber node.

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 From the **Service** drop-down, choose **Cisco SIP Proxy**.

Step 4 In the **Federation Routing Parameters (Clusterwide)** section, enter a public FQDN value for the **Federation Routing IM and Presence FQDN** and click **Save**.

Note

- 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.

What to do next

If you changed the Federation Routing FQDN parameter on the IM and Presence Service, restart the Cisco 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 XCP Router, this causes a restart of all XCP services on the IM and Presence Service.

Configuration of Security Settings on IM and Presence Service

Note This procedure is only applicable if you do not have Cisco Expressway-C in your federation deployment, for example, if you deploy federation within your enterprise and you want a secure TLS connection.

Note Microsoft Lync does not support EC ciphers. When selecting EC ciphers you must choose either non-EC ciphers only, or a mixture of EC and non-EC ciphers. EC ciphers must not be selected on their own.

Note `Default_Cisco_SIP_Proxy_Peer_Auth_TLS_Context`, supports the selection of additional stronger ciphers. You can select the appropriate cipher based on the required configuration. You must ensure that the selected cipher list aligns with the peer's supported ciphers before configuring Interdomain Federation.

Create a New TLS Peer Subject

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

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 a Microsoft server, 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.

Step 4 Enter the name of the external server in the Description field.

Step 5 Click **Save**.

Configuration of Security Settings on IM and Presence Service

Note This procedure is only applicable if you do not have Cisco Expressway-C in your federation deployment, for example, if you deploy federation within your enterprise and you want a secure TLS connection.

Note Microsoft Lync does not support EC ciphers. When selecting EC ciphers you must choose either non-EC ciphers only, or a mixture of EC and non-EC ciphers. EC ciphers must not be selected on their own.

Note `Default_Cisco_SIP_Proxy_Peer_Auth_TLS_Context`, supports the selection of additional stronger ciphers. You can select the appropriate cipher based on the required configuration. You must ensure that the selected cipher list aligns with the peer's supported ciphers before configuring Interdomain Federation.

Configuration Workflow for SIP Federation with AOL

- Establish an AOL license to enable AOL Federation, see License Requirements for AOL Federation, AOL Routing Information Requirements and AOL Provisioning Information Requirements.
- Configure federated domains on the IM and Presence Service for AOL federation, see Add a SIP Federated Domain, on page 1.
- Configure DNS SRV records, see DNS Configuration for SIP Federation, on page 2. If you are not using DNS, see the next step).
- Configure the routing for AOL federation, see Configure Static Routes Using TLS, on page 3.
- (Optional) Verify and configure the Default Federation Routing Domain for AOL hosted domains.
- (Optional) Configure the email address for federation feature, see Turn On Email for Federation.
- Configure the TLS security settings and certificates on the IM and Presence Service, see Configuration of Security Settings on IM and Presence Service, on page 5 and Security Certificate Exchange Between Cisco Adaptive Security Appliance and the AOL SIP Access Gateway.
- Configure the Cisco Adaptive Security Applicance for AOL, see AOL SIP Access Gateway for information on AOL FQDN, server port, and the public IP address.
- (Optional) Configure a load balancer for redundancy, see Load Balancer Configuration for Redundancy for SIP 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:

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

Turn On the SIP Federation Service

Turn on the Cisco XCP SIP Federation Connection Manager service. This turns on the SIP Federation feature for each user that you provision. You must complete this task on each node in the cluster.

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.