CHAPTER 3

Configuring Cisco Unified Presence for Federation

January 26, 2009

Adding a Federated Domain

When you add a Federation Domain entry on Cisco Unified Presence, the presence gateway and the incoming ACL for the federated domain entry are automatically added. Note that you cannot see the presence gateway that is associated with a federated domain on the Cisco Unified Presence GUI. You can see the incoming ACL associated with a federated domain on the Cisco Unified Presence GUI, but you cannot modify or delete it. You can only delete the incoming ACL when you delete the (associated) Federated Domain entry.

Procedure

Step 1 Select **Cisco Unified Presence Administration > Presence > Inter Domain 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.

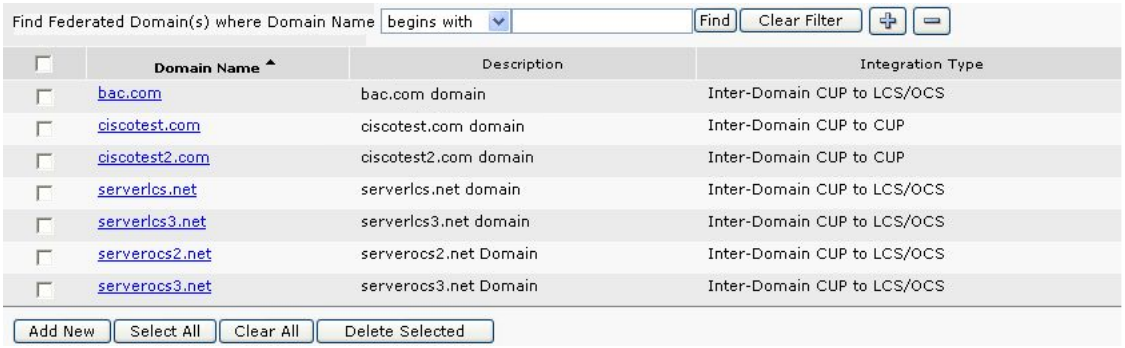
Step 5 Select **CUP to LCS/OCS** from the Integration Type menu.

Step 6 Click **Save**.

Note

- If you are federating between one Cisco Unified Presence enterprise deployment and another, select **CUP to CUP** as the integration type.
- The text string you enter in the Description field is displayed to the user in the Cisco Unified Personal Communicator privacy preferences available from the Manage Domains tab. Therefore make sure you enter a domain name that is easily-recognizable to the end user in this field.

Figure 3-1 Adding a Federated Domain



What To Do Next

Configuring the Federation Routing Parameter, page 3-3

Enabling Email for Federation

When you enable Cisco Unified Presence to use the email address for interdomain federation, Cisco Unified Presence changes the SIP URI of each federated contact from ‘userid@domain’ to the email address of the contact.

Before You Begin

Before enabling Cisco Unified Presence to use the email address for interdomain federation, note the following:

- If you have not yet attempted to federate with the foreign domain, and you wish to enable email for federation, we recommend that you enable this setting *before* the end users begin to add any federated contacts.
- You must alert the system administrator of the foreign domain that you are using email address for federation, and that the end users in the foreign domain must specify an email address when adding a federated contact to their contact list.
- If you are already federating with the foreign domain, and you wish to enable email for federation, *before enabling this setting*, you must alert the system administrator of the foreign domain that the end users in the foreign domain must remove the existing federated contacts in their contact list, and add these federated contacts again specifying an email address.

Procedure

Step 1 Select **Cisco Unified Presence Administration > Presence > Settings.**

Step 2 Check **Enable Email ID for Federation**.

Step 3 Read the warning message, and click **OK**.

Step 4 Click **Save**.

Configuring the Federation Routing Parameter

Before You Begin

- When you first install Cisco Unified Presence, the federation routing parameter is automatically set to the FDQN of the publisher node and is then passed down to each subscriber node.
- If you are upgrading (to Cisco Unified Presence 7.0.3 or later) from a previous version, the federation routing parameter is automatically set to the FDQN of the publisher node only if the value was not already set.

Procedure

Step 1 Select **Cisco Unified Presence Administration > System > Service Parameters**.

Step 2 Select the Cisco Unified Presence server from the Server menu.

Step 3 Select **Cisco UP SIP Proxy** from the Service menu.

Step 4 Enter the FQDN value for the **Federation Routing CUP FQDN** parameter in the Federation Routing Parameters (Clusterwide) section.

Note
- This FQDN value must correspond to the sip_federationtls entry in the public DNS for that Cisco Unified Presence domain.
- If the external FQDN (the hostname portion) is different to internal FQDN, you must specify the external FQDN in this field.

Step 5 Click **Save**.

Creating a new TLS Peer Subject

When you import the Cisco Adaptive Security Appliance security certificate onto Cisco Unified Presence, the Cisco Adaptive Security Appliance is automatically added as a TLS Peer Subject on Cisco Unified Presence. Therefore you do not need to manually add Cisco Adaptive Security Appliance as a TLS peer subject on Cisco Unified Presence.

Procedure

Step 1 Select **Cisco Unified Presence Administration > System > Security > TLS Peer Subjects**.

Step 2 Click **Add New**.

Step 3 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 Access Edge or Access Proxy server in the Description field.

Step 5 Click **Save**.

What To Do Next

Adding the TLS Peer to the Selected TLS Peer Subjects List, page 3-4

Adding the TLS Peer to the Selected TLS Peer Subjects List

Before You Begin

Complete the steps in Creating a new TLS Peer Subject, page 3-3.

Procedure

Step 1 Select **Cisco Unified Presence Administration > System > Security > TLS Context Configuration**.

Step 2 Click **Find**.

Step 3 Click **Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context**.

Step 4 Select all cyphers from the list of available TLS ciphers.

Step 5 Click the down arrow to move these cipher selections 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 down arrow to move the selected TLS peer subject to **Selected TLS Peer Subjects**.

Step 8 Check **Disable Empty TLS Fragments** if you are federating with Microsoft OCS.

Step 9 Click **Save**.

What To Do Next

DNS Configuration, page 3-5

DNS Configuration

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

In the Cisco Unified Presence enterprise deployment, you need to configure a DNS SRV record that points to _sipfederationtls._tcp.<*CUP_domain*> over port 5061where <*CUP_domain*> is the name of the Cisco Unified Presence domain. This DNS SRV should point to the public FQDN of the routing Cisco Unified Presence server.

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

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

```
nslookup
set type=srv
_sipfederationtls._tcp.<domain>
```

Configuring Static Routes Using TLS

If the Cisco Unified Presence server cannot discover the external domain using DNS SRV, you must configure a static route on Cisco Unified Presence that points to the external interface of the foreign domain.

Procedure

Step 1 Select **Cisco Unified Presence Administration > Presence > Routing > Static Routes**.

Step 2 Configure the static route parameters as follows:

- The Destination Pattern value needs to be reversed. It must be in the following format ‘.com.domain.*’, for example ‘.com.cisco.*’.
- The Next Hop value is the external Access Edge FQDN or IP address.
- The Next Hop Port number is **5061**.
- The Route Type value is **domain**.
- The Protocol Type is **TLS**.

Step 3 Click **Save**.

Related Topics

Configuring the Cisco Unified Presence Domain from the CLI, page 3-6

Configuring the Cisco Unified Presence Domain from the CLI

If you have not enabled DHCP, use this procedure to configure the Cisco Unified Presence domain from the CLI.

Procedure

Step 1 Log in to the administrator CLI on Cisco Unified Presence.

Enter this command to display the current network settings:

```
show network eth0
```

Step 2 If the domain is not configured and DHCP is disabled, configure the domain to be the same as the Cisco Unified Presence proxy domain. Enter this command:

```
set network domain <domain name>.
```

Step 3 Enter **y** at the prompt to confirm the changes.

This server automatically restarts. This can take up to 5 minutes.

Step 4 When the sever had restarted, enter this command to confirm you have configured the domain:

```
show network eth0
```