Single Sign On

SSO Certificate Management

Use this procedure to create a self-signed or third-party-signed system certificate to use when setting up Single Sign-On (SSO) on the web proxy node on Cisco Unified Communications Domain Manager 10.6(1).

Note During customer onboarding this is customer specific.

Procedure

Step 1 Login as hcsadmin.

Step 2 Select **Single Sign On** > **Certificate Management**.

Step 3 Click **Add**.

Step 4 On the **Base** tab, enter a Name and Description for the certificate.

- For a self-signed certificate, leave **Generate Certificate Signing Request** unchecked.
- For a third-party-signed certificate, check **Generate Certificate Signing Request**.

Step 5 For a self-signed certificate, control when the certificate is valid by changing the **Valid From** and **Valid To** fields. These are measured in seconds and default to 0 (now) and 315360000 (10 years), respectively.

Step 6 (Optional) Change the Key Length from the default of 1024.

Step 7 Click the **Certificate Information** tab.

Step 8 Complete the required fields:

Field	Description
Common Name	Enter the FQDN for your server.

Field	Description
Country Code	A two-digit country code
State	An appropriate country subdivision
City	Your city
Organization	Your organization
Organization Unit	Your organization subunit

Step 9 Click **Save**.

Step 10 If you created a self-signed certificate you are done. If you requested a third-party-signed certificate, continue to the next step.

Step 11 Click the certificate you just created.

Step 12 Select **Action** > **Export Certificate Request**.

Step 13 Follow your organization's procedures to obtain the third-party signature for the certificate.

Step 14 Click the certificate.

Step 15 Select **Action** > **Upload Signed Certificate**.

Step 16 Browse to the signed certificate and click **OK**.

Configure Single Sign-On for Cisco Unified Communications Domain Manager

Follow these steps to configure self-service Single Sign-On (SSO) for Cisco Unified Communications Domain Manager (Unified CDM). The configuration applies to the customers and customer administrators associated with the IdP.

Note SSO support for administrative users is defined as follows:

- SSO is not supported for administrative users under **User Management** > **Local Admins** because their passwords are stored locally (and so are not available for SSO).
- SSO is supported for administrative users under **User Management** > **Users**, except for users with the Role set to SelfService.

Before You Begin

Create a self-signed or third-party-signed system certificate before you configure self-service SSO. For more information, see SSO Certificate Management, on page 1.

The Unified CDM server and the IdP (identify provider) server must be configured so that their clocks are synchronized.

Procedure

Step 1 Log in to Unified CDM as hcsadmin.

Step 2 Select **Single Sign On** > **SSO SP Settings**.

Step 3 Click **Add**.

Note Configure only one instance of SSO SP Settings.

Step 4 On the **Base** tab, select the System Certificate to use. To allow the SSO SP Setting to expire, enter a number of hours in the Validity field.

Note Specifying an unsigned third-party-signed certificate will result in an error.

Step 5 On the **SAML SP Settings Tab**, enter the FQDN of the Unified CDM server. Check **Sign Authn Requests** and **Want Assertions Signed** as required by your security environment.

Step 6 Click **Save**.

Step 7 To view the location of the Unified CDM SP metadata that you will upload to the IdP, select **Single Sign On** > **SSO SP Metadata**.

Point your browser to the URL shown here, and then save a copy of the SP metadata.

Step 8 Upload the SP metadata to the IdP.

Refer to your IdP documentation for details on configuring SSO on your IdP.

Note The IdP must release the UID and map it to an appropriate attribute. For example, an IdP that authenticates with Active Directory can map the uid SAML attribute to sAMAccountName in the Active Directory server.

Step 9 Download the IdP metadata from the IdP server.

Refer to your IdP documentation for details on downloading IdP metadata.

Step 10 Log in as Provider, Reseller, or Customer Admin, depending on your IdP configuration level.

Step 11 Select **Administration Tools** > **File Management** and upload the IdP metadata.

Step 12 Select **Single Sign On** > **SSO Identity Provider**.

Step 13 Click **Add** to add the SSO Identity Provider configuration.

Note Only one instance of an SSO Identity Provider can be configured for a hierarchy node.

Step 14 Complete the following fields:

Field	Description
Entity Id	Entity ID of the IdP. This can be extracted from the IdP metadata file. This field is mandatory.
Login URI	Login URI for the IdP. This is the URI that will be imbedded in SSO Login URL. It can contain only alphanumeric characters and forward slashes. This field is mandatory.
Local Metadata File	Choose the IdP metadata file. This field is mandatory and must be unique across the system.

Field	Description
SSO Enabled	Check to enable SSO for users synched in or created at the current hierarchy level. Unchecking this node will disable SSO for the users associated with the defined IdP.
Note	Reminder to upload the IdP metadata file
SSO Login URL	Read-only field displays the SSO Login URL to use.

Step 15 Click **Save** to save the SSO Identity Provider Configuration and enable SSO if selected.

Step 16 Select **Single Sign On** > **SSO User** to display enabled SSO users.

Use this URL for your SSO login: `https://<cucdm hostname>/sso/<login_URI>/login`