Single Sign-on Administration

Single Sign-on Administration

Set up the System Inventory for Single Sign-On

Set up the System Inventory before configuring the Cisco Identity Service (Cisco IdS) and the components for single sign-on. By default, the System Inventory displays a list of all AWs, Routers, and Peripheral Gateways in the deployment.

The Principal AW (Admin Workstation) is responsible for managing background tasks that are run periodically to sync configuration with other solution components, such as SSO management, Smart Licensing, etc.

Select the Principal AW to manage to register the components with the Cisco IdS and enabling them for SSO. Add the remaining SSO-capable machines to the System Inventory, and select the default Cisco IdS for each of the SSO-capable machines.

Step 1 In Unified CCE Administration, navigate to **Features** > **Single Sign-On**.

Step 2 Set the Principal AW:

a) Click the AW that you want to be the Principal AW.

> **Note** If the AW is coresident with the Router, you can set the Principal AW on the Router.
>
> You can only specify one Principal AW for each Unified CCE system.

The **Edit AW** popup window opens.

b) Check the **Principal AW** check box on the General tab.

c) Enter the Unified CCE Diagnostic Framework Service domain, username, and password.

These credentials must be for a domain user who is a member of the Config security group for the instance. These credentials must be valid on all CCE components in your deployment (Routers, PGs, AWs, and so on).

d) Click **Save**.

Step 3 Add the SSO-capable machines to the System Inventory:

a) Click **New**.

The **Add Machine** popup window opens.

b) From the **Type** drop-down, select one of the following types of machines:

- **Finesse Primary**
- **CUIC, LD, IdS Publisher**, for the coresident Unified Intelligence Center, Live Data, and Cisco IdS machine available in the 2000 agent or Progger (Lab only) reference design
- **Unified Intelligence Center Publisher**, if you're using a standalone Unified Intelligence Center
- **Identity Service Primary**, if you're using a standalone Cisco IdS

c) In the **Hostname** field, enter the FQDN, IP address, or hostname of the machine.

Note If you don’t enter the FQDN, the system converts the value you enter to FQDN.

d) Enter the machine's Administration credentials.

e) Click **Save**.
The machine and its related Subscriber or Secondary machine are added to the System Inventory.

f) Repeat this procedure to add all of the SSO-capable machines in the deployment.

Step 4 Select the default Identity Service for each of the following machines:

- All Unified CCE AW servers
- Finesse Primary and Secondary
- Unified Intelligence Center Publisher and Subscriber

Note If you're using a coresident CUIC, LD, Ids Publisher and Subscriber, you don't need to set the default Cisco IdS for those machines.

In a standalone deployment, select the Cisco IdS that's deployed on the same Data Center Side (A or B) as the machine that you're configuring. For example, in the Reference Deployment:

- Select the Identity Service Publisher (IdS A) for AW-HDS-DDS 1, AW-HDS 3, Finesse 1 Pub, Finesse 2 Pub, CUIC Pub, and CUIC Sub 1.
- Select the Identity Service Subscriber (Ids B) for AW-HDS-DDS 2, AW-HDS 4, Finesse 1 Sub, Finesse 2 Sub, CUIC Sub 2, and CUIC Sub 3.

For details on the Reference Deployment, see *Solution Design Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.

a) Click a machine to open the **Edit Machine** popup window.

b) Click the Search icon next to **Default Identity Service** to open the **Select Identity Service** popup window.

c) Enter the machine name for the Cisco IdS in the Search field and choose the Cisco IdS from the list.

d) Click **Save**.

What to do next

Be sure to update the System Inventory if you change your deployment:

- If you add or remove contact center solution components from your deployment, make the corresponding changes in the System Inventory.
- If you add or remove Cisco Identity Service machines or coresident CUIC-LD-IdS machines, update the System Inventory appropriately and reconfigure the Cisco IdS. Reassociate the components with a default Cisco IdS.

Configure the Cisco Identity Service

The Cisco Identity Service (Cisco IdS) provides authorization between the Identity Provider (IdP) and applications.

When you configure the Cisco IdS, you set up a metadata exchange between the Cisco IdS and the IdP. This exchange establishes a trust relationship that then allows applications to use the Cisco IdS for single sign-on. You establish the trust relationship by downloading a metadata file from the Cisco IdS and uploading it to the IdP. You can then select settings related to security, identify clients of the Cisco IdS service, and set log levels and, if desired, enable Syslog format.

Note If you are working with a Cisco IdS cluster, perform these steps on the Cisco IdS primary publisher node.

Be sure that the Principal AW is configured and functional before using the **Features** > **Single Sign-On** tool in Unified CCE Administration.

Step 1 In Unified CCE Administration, navigate to **Features** > **Single Sign-On**.

Note Use a log in name in the format *username@FQDN* to log in to the Unified CCE Administration.

Step 2 Click **Identity Service Management**.

Result:

The Cisco Identity Service Management window opens.

Step 3 Enter your user name, and then click **Next**.

Step 4 Enter your password, and then click **Sign In**.

Note If a custom logon message is set up in Cisco Unified OS Administration, the message appears in a pop-up window. Click ok to acknowledge the message to log in. For more information about setting up custom messages, see the *Configure Custom Logon Message* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

The Cisco Identity Service Management page opens, showing the **Nodes**, **Settings**, and **Clients** icons in the left pane.

Step 5 Click **Nodes**.
The **Nodes** page opens to the overall Node level view and identifies which nodes are in service. The page also provides the **SAML Certificate Expiry** details for each node, indicating when the certificate is due to expire. The node **Status** options are **Not Configured**, **In Service**, **Partial Service**, and **Out of Service**. Click a status to see more information. The star to the right of one of the Node names identifies the node that is the primary publisher.

Step 6 Click **Settings**.

Step 7 Click **IdS Trust**.

Step 8 To begin the Cisco IdS trust relationship setup between the Cisco IdS and the IdP, click **Download Metadata File** to download the file from the Cisco IdS Server.

Step 9 Click **Next**.

Step 10 To upload the trusted metadata file from your IdP, browse to locate the file.
The **Upload IdP Metadata** page opens and includes the path to the IdP. When the file upload finishes, you receive a notification message. The metadata exchange is now complete, and the trust relationship is in place.

Step 11 Clear the browser cache.

Step 12 Enter the valid credentials, when page is redirected to IdP.

Step 13 Click **Next**.
The **Test SSO Setup** page opens.

Step 14 Click **Test SSO Setup**.
A message appears telling you that the Cisco IdS configuration has succeeded.

Step 15 Click **Settings**.

Step 16 Click **Security**.

Step 17 Click **Tokens**.
Enter the duration for the following settings:

- **Refresh Token Expiry** -- The default value is 10 hours. The minimum value is 2 hours. The maximum is 24 hours.
- **Authorization Code Expiry** -- The default value is 1 minute, which is also the minimum. The maximum is 10 minutes.
- **Access Token Expiry** -- The default value is 60 minutes. The minimum value is 5 minutes. The maximum is 120 minutes.

Step 18 Set the **Encrypt Token** (optional); the default setting is **On**.

Step 19 Click **Save**.

Step 20 Click **Keys and Certificates**.
The **Generate Keys and SAML Certificate** page opens and allows you to:

- Regenerate the **Encryption/Signature key** by clicking **Regenerate**. A message appears to say that the Token Registration is successful and advises you to restart the system to complete the configuration.
- Regenerate the **SAML Certificate** by clicking **Regenerate**. A message appears to say that the SAML certificate regeneration is successful.

Step 21 Click **Save**.

Step 22 Click **Clients**.
The **Clients** page identifies the existing Cisco IdS clients, providing the client name, the client ID, and a redirect URL. To search for a particular client, click the Search icon above the list of names and type the client's name.

Step 23 To add a client:

a) Click **Add Client**.
b) Enter the client's name.
c) Enter the Redirect URL. To add more than one URL, click the plus icon.
d) Click **Add** (or click **Clear** and then click the X to close the page without adding the client).

Step 24 To edit or delete a client, highlight the client row and click the ellipses under **Actions**. Then:

- Click **Edit** to edit the client's name, ID, or redirect URL. On the **Edit Client** page, make changes and click **Save** (or click **Clear** and then click the X to close the page without saving edits).
- Click **Delete** to delete the client.

Step 25 Click **Settings**.

Step 26 From the **Settings** page, click **Troubleshooting** to perform some optional troubleshooting.

Step 27 Set the local log level by choosing from **Error**, **Warning**, **Info** (the default), **Debug**, or **Trace**.

Step 28 To receive errors in Syslog format, enter the name of the Remote Syslog Server in the Host (Optional) field.

Step 29 Click **Save**.

You can now:

- Register components with the Cisco IdS.
- Enable (or disable) SSO for the entire deployment.

Register Components and Set Single Sign-On Mode

If you add any SSO-compatible machines to the System Inventory after you register components with the Cisco IdS, those machines are registered automatically.

Before you begin

- Configure the Cisco Identity Service (Cisco IdS).
- Disable popup blockers. It enables viewing all test results correctly.

Step 1 In the Unified CCE Administration, navigate to **Features** > **Single Sign-On**.

Step 2 Click the **Register** button to register all SSO-compatible components with the Cisco IdS.

The component status table displays the registration status of each component.

If a component fails to register, correct the error and click **Retry**.

Step 3 Click the **Test** button. When the new browser tab opens, you may be prompted to accept a certificate. In order for the page to load, accept any certificates. Then, when presented with a log in dialog, log in as a user with SSO credentials.

The test process verifies that each component has been configured correctly to reach the Identity Provider, and that the Cisco IdS successfully generates access tokens. Each component that you are setting up for SSO is tested.

The component status table displays the status of testing each component.

If a test is unsuccessful, correct the error, and then click **Test** again.

Test results are not saved. If you refresh the page, run the test again before enabling SSO.

Step 4 Select the SSO mode for the system from the **Set Mode** drop-down menu:

- Non-SSO: This mode disables SSO for all agents and supervisors. Users log in using existing Active Directory-based local authentication.

- Hybrid: This mode allows you to enable agents and supervisors selectively for SSO.
- SSO: This mode enables SSO for all agents and supervisors.

The component status table displays the status of setting the SSO mode on each component.

If the SSO mode fails to be set on a component, correct the error, and then select the mode again.