Single Sign-On

Single Sign-On

Single sign-on (SSO) is an authentication and authorization process. (Authentication proves that you are the user you say that you are, and authorization verifies that you are allowed to do what you want to do.) SSO allows you to sign in to one application and then securely access other authorized applications without a prompt to resupply user credentials. SSO permits Cisco supervisors or agents to sign on only once with a username and password. Supervisors and agents gain access to all of their Cisco browser-based applications and services within a single browser instance. By using SSO, Cisco administrators can manage all users from a common user directory and enforce password policies for all users consistently.

Note Before enabling SSO in Unified CCE, ensure to sign in to the Cisco Unified Intelligence Center OAMP interface and perform the Unified CCE User Integration operation (Cluster Configuration > UCCE User Integration) once manually to import the Supervisors with the required roles.

SSO is an optional feature whose implementation requires you to enable the HTTPS protocol across the enterprise solution.

You can implement single sign-on in one of these modes:

- **SSO** - Enable *all* agents and supervisors in the deployment for SSO.
- **Hybrid** - Enable agents and supervisors *selectively* in the deployment for SSO. Hybrid mode allows you to phase in the migration of agents from a non-SSO deployment to an SSO deployment and enable SSO for local PGs. Hybrid mode is useful if you have third-party applications that don't support SSO, and some agents and supervisors must be SSO-disabled to sign in to those applications.
- **Non-SSO** - Continue to use existing Active Directory-based and local authentication, without SSO.

SSO uses Security Assertion Markup Language (SAML) to exchange authentication and authorization details between an identity provider (IdP) and an identity service (IdS). The IdP authenticates based on user credentials, and the IdS provides authorization between the IdP and applications. The IdP issues SAML assertions, which are packages of security information transferred from the IdP to the service provider for user authentication. Each assertion is an XML document that contains trusted statements about a subject including, for example, username and privileges. SAML assertions are digitally signed to ensure their authenticity.

The IdS generates an authentication request (also known as a SAML request) and directs it to the IdP. SAML does not specify the method of authentication at the IdP. It may use a username and password or other form of authentication, including multi-factor authentication. A directory service such as LDAP or AD that allows you to sign in with a username and a password is a typical source of authentication tokens at an IdP.

Cisco IdS has now shifted to asymmetric key encryption for signing the tokens generated for authentication. This allows any client with the matching public key to easily and conveniently authorize any other client that has a token that is signed using the matching private key. You can access the public key using the Cisco IdS CLIs that are described in Access Public Key Signing Certificate, on page 21. The public key can be freely distributed without any security concerns. All solution components monitor the public encryption key exposed by Cisco IdS using the REST APIs for their token authentication purposes. For more information about the SSO SDK, see Cisco Finesse REST API with SSO Guide.

Note Due to the change in Cisco IdS token mechanism starting 12.6.2, agents must log out and log in to Finesse Desktop after Cisco IdS is upgraded to 12.6(2). To avoid this requirement, install 12.6(2) ES02. For more information, see the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide or Cisco Packaged Contact Center Enterprise Installation and Upgrade Guide.

Prerequisites

The Identity Provider must support Security Assertion Markup Language (SAML) 2.0. See the *Compatibility Matrix* for your solution at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.htmlhttps://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html for details.

Contact Center Enterprise Reference Design Support for Single Sign-On

Unified CCE supports single sign-on for these reference designs:

- 2000 Agents
- 4000 Agents

- 12000 Agents
- 24000 Agents
- Contact Director (Maximum of 24000 agents, Each target system must include a dedicated Cisco IdS deployment.)

Coresidency of Cisco Identity Service by Reference Design

Reference Design	Unified CCE
2000 Agent	Cisco IdS is coresident with Unified Intelligence Center and Live Data on a single VM.
4000 Agent	Standalone Cisco IdS VM
12000 Agent	Standalone Cisco IdS VM
24000 Agent	Standalone Cisco IdS VM

Single Sign-On Support and Limitations

Note the following points that are related to SSO support:

- To support SSO, enable the HTTPS protocol across the enterprise solution.
- SSO supports agents and supervisors only. SSO support is not available for administrators in this release.
- In the 12,000 Agent Reference Design, a maximum of 12,000 agents use SSO at one time.
- SSO supports multiple domains with federated trusts.
- SSO supports only contact center enterprise peripherals.
- SSO support is available for Agents and Supervisors that are registered to remote or main site PG in global deployments.

Note the following limitations that are related to SSO support:

- SSO support is not available for third-party Automatic Call Distributors (ACDs).
- The SSO feature does not support Cisco Finesse IP Phone Agent (FIPPA).
- The SSO feature does not support Cisco Finesse Desktop Chat.
- In Hybrid mode,
  - When an agent in SSO mode tries to log in to CUIC, and if the agent does not exist in CUIC, the agent cannot log in to CUIC.
  - When a Supervisor in SSO mode tries to log in to CUIC, and if the Supervisor user does not exist in CUIC, the Supervisor cannot log in to CUIC. For the Supervisor to log in to CUIC, perform Unified CCE User Integration. For more information on Unified CCE User Integration, see *Administration Console User Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.

Single Sign-On Configuration Flow

Note To ensure that token validations based on token lifetimes are correctly applied, it is mandatory that you synchronize the time in Cisco IdS, IdP, and all IdS clients, including VPN-Less reverse proxy hosts, to the same NTP source (preferred) or to the same NTP stratum.

Note It is recommended that the Administrator configures SSO from the IdS publisher node.

1. Install the appropriate release of the CCE solution. For more information, see Cisco Unified Contact Center Enterprise Installation and Upgrade Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html
2. Install the Cisco Identity Service (Cisco IdS). For more information, see Cisco Unified Contact Center Enterprise Installation and Upgrade Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html
3. Configure an Identity Provider (IdP).
4. Configure System Inventory.
5. Configure the Cisco IdS.
6. Register and test SSO-compatible components with the Cisco IdS.
7. Choose the SSO mode.
8. Enable multiple users at once for SSO by using the SSO migration tool, or enable users one at time by using the configuration tools.

Configure an Identity Provider (IdP)

To support SSO for the contact center solution, configure an Identity Provider (IdP) that is compliant with the Security Assertion Markup Language 2.0 (SAML v2) Oasis standard. The IdP stores user profiles and provides authentication services to the contact center solution.

Note For a current list of supported Identity Provider products and versions, see the *Contact Center Enterprise Compatibility Matrix*.

This section provides sample configuration information for Microsoft AD FS.

Follow this sequence of tasks to configure the Identity Provider.

Sequence	Task
1	Install and Configure Active Directory Federation Services, on page 5

Sequence	Task
2	Set Authentication Type. See Authentication Types, on page 5.
4	Enable Signed SAML Assertions, on page 9
5	Optionally Customize the AD FS Sign-In Page in Windows Server to Allow User ID, on page 10

Install and Configure Active Directory Federation Services

Follow Microsoft instructions and guidelines to install Microsoft Active Directory Federation Services (AD FS).

For example, see *Active Directory Federation Services Overview* at https://technet.microsoft.com/en-us/library/hh831502(v=ws.11).aspx

- For AD FS 2.0, see *AD FS Content Map* at http://aka.ms/adfscontentmap.
- For AD FS in Windows Server, see *AD FS Technical Reference* at https://docs.microsoft.com/en-us/windows-server/identity/active-directory-federation-services.

Note SSO for Unified CCE supports IdPs other than MS, and AD FS. For the list of supported IdPs see the Compatibility matrix https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html

Note Cisco IdS does not support AD FS Automatic Certificate Rollover. If the AD FS certificate gets rolled over, then re-establish the trust relationship between the IdS and AD FS.

Authentication Types

Cisco Identity Service supports form-based authentication and Kerberos windows authentication of the Identity Provider.

For information on enabling form-based authentication in ADFS, see Microsoft documentation:

- For ADFS 2.0 see https://social.technet.microsoft.com/wiki/contents/articles/1600.ad-fs-2-0-how-to-change-the-local-authentication-type.aspx
- For ADFS 3.0 see https://blogs.msdn.microsoft.com/josrod/2014/10/15/enabled-forms-based-authentication-in-adfs-3-0/

For Kerberos authentication to work, ensure to disable the form-based authentication.

Integrate Cisco IdS with AD FS

Follow these steps to integrate the Cisco IdS with AD FS.

SUMMARY STEPS

1. In the Server Manager, open **AD FS Management**.
2. For form-based authentication, set the **Authentication Methods** for **Intranet** to **Forms Authentication**.
3. Download LAN SP metadata and reverse-proxy cluster SP metadata from the Cisco IdS publisher.
4. Download the IdP metadata file, `federationmetadata.xml`, from the following location:
5. Do one of the following to upload the IdP metadata file, you downloaded at step 4, to the Cisco Ids server:
6. Follow these steps to create a Relying Party Trust.
7. Do the following to set the properties for the Relying Party Trust created at Step 5. Right-click on the Relying Party Trust and click **Properties**. In the **Properties** window:
8. In the list of Relying Party Trusts, right-click on your Relying Party Trust, and select the option to edit the Rules/Claim Issuance Policy from the menu.
9. In the **Edit Claim Rules**/**Edit Claim Issuance Policy** window that opens, click **Add Rule** and then click **OK**.
10. In the **Add Transform Claim Rule Wizard** that opens, follow these steps to create the first claim:
11. Repeat steps 8 and 9 to open the **Add Transform Claim Rule** wizard. In the **Add Transform Claim Rule** wizard, follow these steps to create the second claim:
12. Click **OK**.

DETAILED STEPS

Step 1 In the Server Manager, open **AD FS Management**.

Step 2 For form-based authentication, set the **Authentication Methods** for **Intranet** to **Forms Authentication**.

Step 3 Download LAN SP metadata and reverse-proxy cluster SP metadata from the Cisco IdS publisher.

- Open the **Identity Service Management** console at `https://<CiscoIdS server address>:8553/idsadmin`

  From the menu on the left, select **Settings**. In the **IdS Trust** tab, download the XML file.

- In Unified CCE Administration, go to **Infrastructure Settings**> **Device Configuration** > **Identity Service** > **Identity Service Settings**.

  In the **IdS Trust** tab, download the XML file.

Note Ensure your browser's security settings allow downloads from the Cisco IdS site.

Step 4 Download the IdP metadata file, `federationmetadata.xml`, from the following location:

`https://<ADFS Server FQDN>/federationmetadata/2007-06/federationmetadata.xml`

Step 5 Do one of the following to upload the IdP metadata file, you downloaded at step 4, to the Cisco Ids server:

- In the **Identity Service Management** console, select **Settings** > **IdS Trust**.

  Click **Next** and then click **Upload Idp Metadata**.

- In the **Unified CCE Administration** console, navigate to **Infrastructure Settings** > **Device Configuration** > **Identity Service** > **Identity Service Settings** > **Ids Trust**.

  Click **Next** and then click **Upload Idp Metadata**.

Note Cisco IdS supports SAML self-signed certificates for authorization and authentication.

Step 6 Follow these steps to create a Relying Party Trust.

a) In the Server Manager, open **AD FS Management**.
b) Select the **Add Relying Party Trust** option from the AD FS menu.
c) In the **Add Relying Party Trust** wizard, click **Select Data Source**.
d) Select the **Import data about the relying party from a file** option and then click **Browse** to the open the SAML SP metadata XML file you downloaded at Step 3 and click **Next**.
e) In the **Display name** field, enter a unique name for the relying party and click **Next**.
f) *This step is applicable only for Windows Server 2012 R2*. In the **Configure Multi-factor Authentication Now** step, select **I do not want to configure multi-factor authentication settings for the relying party at this time.**
g) Select the option that permits all users and click **Next**.
h) Skip the option to edit the Rule/Claim Issuance Policy for now (you edit the policy from Step 8 onwards) and click **Close** to complete adding the relying party trust.

Step 7 Do the following to set the properties for the Relying Party Trust created at Step 5. Right-click on the Relying Party Trust and click **Properties**. In the **Properties** window:

- Configure the following under the **Identifiers** tab:

Field	Description
Display name	The unique name of the identifier.
Relying party identifier	FQDN of the publisher node of Cisco Identity Server from which you downloaded the Cisco IdS metadata file at step 3.
	FQDN of the subscriber node of Cisco Identity Server.

- Under the **Advanced** tab, choose **SHA-256** from the **Secure hash algorithm** field.

Step 8 In the list of Relying Party Trusts, right-click on your Relying Party Trust, and select the option to edit the Rules/Claim Issuance Policy from the menu.

Step 9 In the **Edit Claim Rules**/**Edit Claim Issuance Policy** window that opens, click **Add Rule** and then click **OK**.

Step 10 In the **Add Transform Claim Rule Wizard** that opens, follow these steps to create the first claim:

a) In the **Choose Rule Type** step, select **Send LDAP Attributes as Claims** from the **Claim rule template** drop-down list and click **Next**.
b) In the **Configure Claim Rule** step, configure the following:

Field	Description
Claim Rule Name	Enter "NameID"
Attribute Store	Select **Active Directory**.

Field	Description
Mapping of LDAP Attributes to Outgoing Claims	If the identifier is a Security Account Name (SAM), do the following: • Select **SAM-Account-Name** as one of the LDAP attributes and set the **Outgoing Claim Type** to "uid." • Select **User-Principal-Name** as one of the LDAP attributes and set the **Outgoing Claim Type** to "user_principal". If the identifier is a User Principal Name (UPN), do the following: • Select **User-Principal-Name** as one of the LDAP attributes and set the **Outgoing Claim Type** to "uid." • Select **User-Principal-Name** again as the LDAP attribute and set the **Outgoing Claim Type** to "user_principal." The "uid" identifies the authenticated user in the claim sent to the applications. The "user_principal" identifies the authentication realm of the user in the assertion sent to Cisco Identity Service.

c) Click **Finish**.

Step 11 Repeat steps 8 and 9 to open the **Add Transform Claim Rule** wizard. In the **Add Transform Claim Rule** wizard, follow these steps to create the second claim:

a) In the **Choose Rule Type** step, select **Send Claims Using a Custom Rule** from the **Claim rule template** drop-down list and click **Next**.

b) In the **Configure Claim Rule** step, configure the following:

1. In the **Claim rule name** field, enter the FQDN of the Cisco Identity Server publisher's primary node.
2. Add the following to the **Custom Rule** field:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] =>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"]
=
"http://<AD FS Server FQDN>/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"]
 =
"<fully qualified domain name of Cisco IdS>");
```

c) Edit the script as follows:

- Replace **<ADFS Server FQDN>** to match exactly (including case) the ADFS server FQDN (fully qualified domain name.)
- Replace **<Cisco IdS server FQDN>** to match exactly (including case) the Cisco Identity Server FQDN.

Step 12 Click **OK**.

Enable Signed SAML Assertions

Enable Signed SAML Assertions for the Relying Party Trust (Cisco Identity Service).

Step 1 Click **Start** and type **powershell** in the Search field to display the Windows Powershell icon.

Step 2 Right-click on the Windows Powershell program icon and select **Run as administrator**

Note All PowerShell commands in this procedure must be run in Administrator mode.

Step 3 Run the command, **Set-ADFSRelyingPartyTrust -TargetName <Relying Party Trust Display Name> -SamlResponseSignature "MessageAndAssertion"**.

Note Set <Relying Party Trust Display Name> to exactly match (including case) the Identifier tab of the Relying Party Trust properties.

For example:

```
Set-ADFSRelyingPartyTrust -TargetName CUICPub.PCCERCDN.cisco.com
-SamlResponseSignature "MessageAndAssertion".
```

Step 4 Navigate back to the Cisco Identity Service Management window.

Step 5 Click **Settings**.
By default **IdS Trust** tab is displayed.

Step 6 Click **Next** as you have already downloaded the required metadata.

Step 7 Click **Next** as you have already established trust relationship between IdP and IdS.

The configured IdP Entity ID is listed.

Note If reverse-proxy is configured for IdP, the IdP proxy url is listed at the bottom of the page.

Step 8 Click **Test SSO Setup** to test the required entity where the **SSO Status** displays **Needs Validation**.
SSO Status can be **Successful**, **Unsuccessful**, or **Needs Validation**.

Note If **Unsuccessful**, ensure that the claim you created on the AD FS is enabled or the rule has the correct names for IdS and AD FS.

Administrator client machine requires connectivity to reverse-proxy nodes for validating SSO connection with reverse-proxy.

Multi-Domain Configuration for Federated ADFS

In Multi-Domain Federation in ADFS, an ADFS in one domain provides federated SAML authentication for users in other configured domains. In such cases, additional configuration is required:

- Primary ADFS Configuration that refers to the ADFS to be used in IdS.

- Federated ADFS Configuration that refers to the ADFS, whose users can log in via IdS, thus is the primary ADFS.

Federated ADFS Configuration

In each federated ADFS, create the relying party trust for primary ADFS and the claim rules configured.

Primary ADFS Configuration

Before you begin

In the Claim Provider Trust, ensure that the **Pass through or Filter an Incoming Claim** rules are configured with pass through all claim values as the option

Step 1 Name ID

Step 2 Choose Name ID from Incoming Claim Type drop box

Step 3 Choose **Transient** as the option for Incoming NameID format

Step 4 uid: This is a custom claim. Enter the value uid in the **Incoming Claim Type** drop box.

Step 5 user_principal: This is a custom claim. Type the value user_principal in the **Incoming Claim Type** drop box.

In the relying party trust for IdS, add **Pass though or Filter an Incoming Claim** rules with pass through all claim values as the option.

Step 6 NameIDFromSubdomain

Step 7 Choose Name ID from Incoming Claim Type drop box

Step 8 Choose Transient as the option for Incoming NameID format

Step 9 uid: This is a custom claim. Type the value uid in the Incoming Claim Type drop box

Step 10 user_principal: This is a custom claim. Type the value user_principal in the Incoming Claim Type drop box

Kerberos Authentication (Integrated Windows Authentication)

Before you begin

The CCE solution supports Kerberos authentication.

Optionally Customize the AD FS Sign-In Page in Windows Server to Allow User ID

By default, the sign-in page presented to SSO users by AD FS in Windows Server requires a username that is a UPN. Usually this is an email format, for example, user@cisco.com. If your contact center solution is in a single domain, you can modify the sign-in page to allow your users to provide a simple User ID that does not include a domain name as part of the user name.

There are several methods you can use to customize the AD FS sign-in page. Look in the Microsoft AD FS in Windows Server documentation for details and procedures to configure alternate login IDs and customize the AD FS sign-in pages.

The following procedure is an example of one solution.

Step 1 In the AD FS **Relying Party Trust**, change the NameID claim rule to map the chosen LDAP attribute to **uid**.

Step 2 Click the Windows **Start** control and type **powershell** in the Search field to display the Windows Powershell icon.

Step 3 Right-click on the Windows Powershell program icon and select **Run as administrator**

All PowerShell commands in this procedure must be run in Administrator mode.

Step 4 To allow sign-ins to AD FS using the sAMAccountName, run the following Powershell command:

```
Set-AdfsClaimsProviderTrust -TargetIdentifier "AD AUTHORITY" -AlternateLoginID sAMAccountName
-LookupForests myDomain.com
```

In the LookupForests parameter, replace `myDomain.com` with the forest DNS that your users belong to.

Step 5 Run the following commands to export a theme:

```
mkdir C:\themeExport-AdfsWebTheme –Name default –DirectoryPath c:\theme
```

Step 6 Edit `onload.js` in `C:\theme\script` and add the following code at the bottom of the file. This code changes the theme so that the AD FS sign-in page does not require a domain name or an ampersand, "@", in the username.

```
// Update the placeholder text to not include the domain
var userNameInput = document.getElementById("userNameInput");
if (userNameInput) {
 userNameInput.setAttribute("placeholder", "Username");
}

// Override submitLoginRequest to not have the "@" check
Login.submitLoginRequest = function () {
 var u = new InputUtil();
 var e = new LoginErrors();
 var userName = document.getElementById(Login.userNameInput);
 var password = document.getElementById(Login.passwordInput);
 if (!userName.value) {
  u.setError(userName, e.userNameFormatError);
  return false;
 }
 if (!password.value) {
  u.setError(password, e.passwordEmpty);
  return false;
 }
 document.forms['loginForm'].submit();
 return false;
};
```

Step 7 In Windows PowerShell, run the following commands to update the theme and make it active:

```
Set-AdfsWebTheme -TargetName custom -AdditionalFileResource
@{Uri='/adfs/portal/script/onload.js';path="c:\theme\script\onload.js"}

Set-AdfsWebConfig -ActiveThemeName custom
```

Set the Principal AW for Single Sign On

Note This procedure is applicable only for Packaged CCE 4K or 12K agent reference design.

During deployment, the first SideA AW machine in the CSV file is the Principal AW.

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.

After deployment, you can change the Principal AW by selecting a different AW on the Inventory page. Set the AW on which you make most of your configuration changes as the Principal AW.

Step 1 In Unified CCE Administration, choose **Inventory** to open the **Inventory** page.

Step 2 Set the Principal AW:

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

Note You can only specify one Principal AW for each Unified CCE system.

The Edit CCE AW window opens.

b) Check the **PrincipalAW** check box.

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

d) Click **Save**.

Set Up the System Inventory for Single Sign-On

Packaged CCE deployment automatically associates the Unified CCE AW, Unified Intelligence Center, and Finesse with a default Cisco Identity Service (Cisco IdS). However, if you have an external HDS in your deployment, you must manually associate it with a default Cisco IdS.

Step 1 In Unified CCE Administration, navigate to **System** > **Deployment**.

Step 2 Click the pencil icon for the External HDS for 2000 Agents deployment.

Step 3 Click the Search icon next to **Default Identity Service**.
The **Select Identity Service** popup window opens.

Step 4 Enter the machine name for the Cisco IdS in the **Search** field or choose the Cisco IdS from the list.

Step 5 Click **Save**.

Note If you are working with a Cisco IdS cluster, perform these steps on the Cisco IdS primary publisher node. For CCE 4000, 12000, and 24000 Agents deployment, ensure that the Principal AW is configured and functional before using the Single Sign-On tool in Unified CCE Administration. Also, add the SSO-capable machines to the Inventory, and select the default Cisco IdS for each of the SSO-capable machines.

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 that are related to security, identify clients of the Cisco IdS service, and set log levels. If desired, enable Syslog format.

Note

- Unified CCE AW, Unified Intelligence Center, Finesse, and external HDS gets automatically associated with a default Cisco Identity Service (Cisco IdS).
- Make sure that the Principal AW is configured, and is functional before using the Single Sign-On tool in the Unified CCE Administration. Also, add the SSO-capable machines to the Inventory.

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

Step 1 In the Unified CCE Administration, choose **Overview** > **Infrastructure Settings** > **Device Configuration**.

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

The **Identity Service Nodes**, **Identity Service Settings**, and **Identity Service Clients** tabs appear.

Step 2 Click **Identity Service Nodes**.
You can view the overall Node level and identify which nodes are in service. You can also view 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 3 Click **Identity Service Settings**.

Step 4 Click **Security**.

Step 5 Click **Tokens**.
Enter the duration for the following settings:

- **Refresh Token Expiry** -- Refresh token is used to get new Access tokens. This parameter specifies the duration after which the Refresh token expires. The default value is 10 hours. The minimum value is 2 hours. The maximum is 24 hours.
- **Authorization Code Expiry** -- Authorization code is used to get Access tokens from Cisco IdS. This parameter specifies the duration after which the Authorization code expires. The default value is 1 minute, which is also the minimum. The maximum is 10 minutes.
- **Access Token Expiry** -- Access token contains security credentials used to authorize clients for accessing resource server. This parameter specifies the duration after which the Access token expires. The default value is 60 minutes. The minimum value is 5 minutes. The maximum is 120 minutes.

Step 6 Click **Save**.

Step 7 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. An Administrator regenerates the Encryption/Signature key when it is exposed or compromised. Regenerating the certificates for token signing requires all agents to logout and relogin to the Cisco Finesse desktop. Therefore ensure that you plan for downtime to your Contact Center before you regenerate the public-private key pair that Cisco IdS uses to authenticate agents. After you regenerate the new key pair, you must reboot Cisco IdS so that the agents can relogin to their applications. Ensure that you CA sign the regenerated public-private key pair, if required and then reupload it to the clients that are dependent on the public-private key pair. For example, if you are using the digital channels service, you must reupload the private-public key pair on to Control Hub for your agents to resume with the Manage Digital Channel gadget. For instructions, see *Provision Webex Connect digital services for your organization*.
- Regenerate the **SAML Certificate** by clicking **Regenerate**. A message appears to say that the SAML certificate regeneration is successful. SAML certificate is regenerated when it expires or when IdS relying party trust configuration on IdP is deleted.

  Note Establish the trust relationship again whenever the Encryption keys or SAML certificates are regenerated.

Step 8 Click **Save**.

Step 9 Click **Identity Service Clients**.
On the **Identity Service Clients** tab, you can view the existing Cisco IdS clients, with the client name, client ID, and a redirect URL. To search for a particular client, click the Search icon above the list of names and type the name of client.

Step 10 To add a client on the **Identity Service Clients** tab:

a) Click **New**.
b) Enter the name of client.
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 11 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 12 Click **Identity Service Settings**.

Step 13 Click **Troubleshooting** to perform some optional troubleshooting.

Step 14 From the **Log Level** drop-down list, set the local log level by choosing **Error**, **Warning**, **Info** (the default), **Debug**, or **Trace**.

Step 15 To receive errors in Syslog format, enter the name of the Remote Syslog Server in the **Host** (Optional) field.

Step 16 Click **Save**.

You can now:

- Register components with the Cisco IdS.

- Enable (or disable) SSO for the entire deployment.

Note If SSO is enabled in the deployment, then import all the IdS server nodes certificate into Cisco Finesse, CUIC, and LiveData component trust store.

Install Certification Authority (CA) Certificate

To eliminate browser security warnings each time you sign in, obtain an application and root certificate signed by a CA. To obtain the application and a root certificate, use the Certificate Management utility from Cisco Unified Operating System Administration.

To open Cisco Unified Operating System Administration in your browser, enter: https://fqdn of IdS server:8443/cmplatform.

Sign in using the username and password for the Application User account created during IdS installation.

If you want to install CA signed certificates for IdS instead of out of the box self-signed certificates, you need to install the certificates on both the Cisco IdS nodes.

Step 1 Log in to Cisco Unified Operating System Administration.

Step 2 Navigate to **Security** > **Certificate Management** and then click **Find** to list all the certificates. The **Certificate List** page is displayed.

Step 3 Click **Generate CSR**. The **Generate Certificate Signing Request** window is displayed.

Step 4 Select **tomcat** from the **Certificate Purpose** list. By default, **tomcat** is selected.

Step 5 Ensure that the default values are retained in the **Distribution**, **Common Name**, **Parent Domain**, **Key Type**, **Key Length**, and **Hash Algorithm** fields.

Step 6 Click **Generate** to generate the CSR.

Step 7 Click **Close**. The **Certificate List** page is displayed.

Step 8 Click **Download CSR**. The **Download Certificate Signing Request** window is displayed.

Step 9 Select **tomcat** from the **Certificate Purpose** list and click **Download CSR**.

Step 10 Use the downloaded CSR and share it with the certificate authority to obtain the public certificate.

Step 11 Log in to Cisco Unified Operating System Administration again and navigate to **Security** > **Certificate Management**, and then click **Find** to list all the certificates. The **Certificate List** page is displayed.

Step 12 Click **Upload Certificate/Certificate chain**. The **Upload Certificate/Certificate chain** window is displayed.

Step 13 Select **tomcat** from the **Certificate Purpose** list.

Step 14 Click the **Choose File** button and navigate to select the certificate chain that includes the certificated obtained from the certiciate authority and then click **Open**.

Step 15 Click **Upload** to upload the certificate.

Step 16 Click **Close**. The **Certificate List** page is displayed.

Step 17 After successfully uploading the certificate, navigate to **Security** > **Certificate Management**.

Step 18 Click **Find** to open the list of certificates. The **Certificate List** page is displayed. Verify that the uploaded certificates are listed.

Step 19 Restart the nodes using the CLI command *utils system restart*.

Note

- To avoid the certificate exception warning, you must access the servers using the Fully Qualified Domain Name (FQDN). Ensure that the Distribution field in the CSR is the FQDN of the server
- Ensure that the Certificate Authority (CA) certificate is RSA-signed.

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.

Hostname or IP Address Change

If you change the Hostname or IP Address of the Cisco IdS server, then perform the following:

- Re-generate the SAML certificate.
- Re-establish trust relationship between IdP and IdS.
- If the components are registered earlier, then
  - Re-register all the SSO components.
  - Perform the SSO Test to check if all the SSO components are registered. Verify that the test is successful for each component.

Single Sign-On and the Agent Tool

When the global SSO-enabled setting is Hybrid, you can use the Unified CCE Administration Agent Tool to enable agents individually for single sign-on.

In the tool, check the **Single Sign-On** check box to require a selected agent to sign in with SSO authentication. For supervisors and for agents with single sign-on (SSO) enabled, the username is the user's Active Directory or SSO account username.

Note The check box is disabled when the global SSO mode is set to SSO or non-SSO.

To update agent records in bulk, use the Bulk Jobs Agent content file.

Migration Considerations Before Enabling Single Sign-On

Administrator User and Single Sign-On in Unified Intelligence Center

During installation, Cisco Unified Intelligence Center creates an administrator user. This user is not enabled for SSO, as the user is known only to Unified Intelligence Center.

When you enable SSO, this administrator user is no longer able to log in to the Unified Intelligence Center and perform administrative tasks. These tasks include configuring datasources and setting permissions for other users, for example. To avoid this situation, perform the following steps before enabling SSO.

1. Create a new SSO user who has the same roles and permissions as those of the administrator user.
2. Log in to the CLI.
3. Run the following command:

   utils cuic user make-admin *username*

in which the user name is the complete name of the new user, including the authenticator prefix as shown on the Unified Intelligence Center User List page.

The command, when performed, provides all the roles to the new user and copies all permissions from the administrator user to this new user.

Note

- The administrator's group memberships are not copied to the new user by this CLI command and must be manually updated. The new user, now a Security Administrator, can set up the group memberships.
- For any entity (for example, reports or report definitions), if this new user's permissions provide higher privileges than the administrator, the privileges are left intact. The privileges are not overwritten by this CLI command.

Browser Settings and Single Sign-On

If you have enabled single sign-on and are using Chrome, Edge Chromium (Microsoft Edge), or Firefox, verify that the browser options are set as shown in the following table. These settings specify that you do not want a new session of the browser to reopen tabs from a previous session.

Browser	Browser options to verify when using SSO
Chrome	**1.** Open Chrome. **2.** Click the **Customize and control Google Chrome** icon. **3.** Click **Settings**. **4.** In the **On startup** section of the **Settings** page, verify that the **Open the New Tab page** option is selected.
Edge Chromium (Microsoft Edge)	**1.** Open Microsoft Edge. **2.** Click the **Settings and more (Alt+F)** (...) icon. **3.** Click **Settings**. **4.** On the **Settings** page, click **On startup**, and verify that the **Open a new tab** radio button is selected.
Firefox	**1.** Open Firefox. **2.** Click the **Open menu** icon. **3.** Click **Options**. **4.** In the **Startup** section of the **General** page, verify that either the home page or a blank page is chosen in the **When Firefox starts** drop-down list.

Migrate Agents and Supervisors to Single Sign-On Accounts

If you are enabling SSO in an existing deployment, you can set the SSO state to hybrid to support a mix of SSO and non-SSO users. In hybrid mode, you can enable agents and supervisors selectively for SSO making it possible for you to transition your system to SSO in phases.

Use the procedures in this section to migrate groups of agents and supervisors to SSO accounts using the SSO Migration content file in the Unified CCE Administration Bulk Jobs tool. You use the Administration Bulk Jobs tool to download a content file containing records for agents and supervisors who have not migrated to SSO accounts. You modify the content file locally to specify SSO usernames for the existing agents and supervisors. Using the Administration Bulk Jobs tool again, you upload the content file to update the agents and supervisors usernames; the users are also automatically enabled for SSO.

If you do not want to migrate a user, delete the row for that user.

Important While the Finesse agent is logged in, changing the login name prevents the agent from answering or placing calls. In this situation, the agent can still change between *ready* and *not_ready* state. This affects all active agents, independent of whether SSO is enabled or disabled. Should you need to modify a login name, do so only after the corresponding agent is logged out. Note too that SSO migration (moving a non-SSO agent to be SSO-enabled, by either hybrid mode or global SSO mode) should not be done when the agent is logged in.

Step 1 In Unified CCE Administration, navigate to **Manage** > **Bulk Jobs**.

Step 2 Download the SSO Migration bulk job content file.

a) Click **Templates.**

The **Download Templates** popup window opens.

b) Click the **Download** icon for the SSO Migration template.

c) Click **OK** to close the **Download Templates** popup window.

Step 3 Enter the SSO usernames in the SSO Migration content file.

a) Open the template in Microsoft Excel. Update the **newUserName** field for the agents and supervisors whom you want to migrate to SSO accounts.

The content file for the SSO migration bulk job contains these fields:

Field	Required?	Description
userName	Yes	The user's non-SSO username.
firstName	No	The user's first name.
lastName	No	The user's last name.
newUserName	No	The user's new SSO username. Enter up to 255 ASCII characters. If you want to enable a user for SSO, but keep the current username, leave **newUserName** blank, or copy the value of **userName** into **newUserName**.

b) Save the populated file locally.

Step 4 Create a bulk job to update the usernames in the database.

a) Click **New** to open the **New Bulk Job** window.
b) Enter an optional **Description** for the job.
c) In the **Content File** field, browse to the SSO Migration content file you completed.

The content file is validated before the bulk job is created.

d) Click **Save**.

The new bulk job appears in the list of bulk jobs. Optionally, click the bulk job to review the details and status for the bulk job. You can also download the log file for a bulk job.

What to do next

After all of the agents and supervisors in your deployment are migrated to SSO accounts, you can enable SSO globally in your deployment.

Allowed Operations by Node Type

The Cisco IdS cluster contains a publisher and a subscriber node. A publisher node can perform any configuration and access token operations. The operations that a subscriber node can perform depends on whether the publisher is connected to the cluster.

This table lists which operations each type of node can perform.

Table 1: Single Sign-On Allowed Operations

Operation	Allowed on Publisher	Allowed on Subscriber
Upload IdP metadata	Always	Never
Download SAML SP metadata	Always	Never
Regenerate SAML Certificate	Always	Never
Regenerate Token Encryption/Signing Key	Always	Never
Update AuthCode/Token Expiry	Always	Only when publisher is connected
Download Token Public Key	Always	Always
Add/Update/Delete Cisco IdS client configuration	Always	Only when publisher is connected
View Cisco IdS client configuration	Always	Always
View Cisco IdS status	Always	Always
Set Troubleshooting Log Level	Always	Always

Operation	Allowed on Publisher	Allowed on Subscriber
Set Remote Syslog server	Always	Always

Configure SAML Certificate Secure Hash Algorithm from SHA-1 to SHA-256

This procedure is useful for upgrades from version 11.x where the only Secure Hash Algorithm supported was SHA-1.

After the expiry of SHA-1, the administrator must configure SHA-256..

Perform this procedure after the upgrade has completed successfully.

Step 1 From browser in AD FS Server, login to Cisco IdS admin interface `https://<Cisco IdS server address>:8553/idsadmin`.

Step 2 Click **Settings**.

Step 3 Click **Security** tab.

Step 4 Click **Keys and Certificates**.

Note After this step, Single Sign On will stop working until you complete Step 8.

Step 5 Regenerate SAML Certificate with SHA-256 Secure Hash Algorithm. In the SAML Certificate section, change Secure Hash algorithm dropdown menu to SHA-256 and then click **Regenerate** button

Step 6 Download new metadata file. Click on **IdS Trust** tab and then click download button.

Step 7 Change Secure Hash Algorithm in AD FS Relaying Party Trust configuration. In AD FS server, open AD FS Management. Go to **ADFS ->Trust Relationships->Relying Party Trusts**, right click on existing Relying Party Trust for Cisco IdS and then click on Properties. In the Advanced Tab, change the Secure Hash Algorithm to **SHA-256.** Click **Apply**.

Step 8 Update Relying party trust on AD FS. From AD FS Server, run the following Powershell command:

```
Update-AdfsRelyingPartyTrust -MetadataFile <path to Step 6 new MetaData File> -TargetName
        <Relying Party Trust Display Name>
```

Access Public Key Signing Certificate

Login to the Cisco IdS admin console, and then run the following commands to access the public key signing certificate:

- **show ids token csr**—Displays the CSR corresponding to the public key that is used to validate the tokens.
- **show ids token certificate**—Displays the X.509 token certificate.
- **show ids token public_key**—Displays the base64 encoded public key that is used for VPN-less SSO authentication.

Single Sign-On Log Out

For a complete logout from all applications, sign out of the applications and close the browser window. In a Windows desktop, log out of the Windows account. In a Mac desktop, quit the browser application.

Note Users enabled for single sign-on are at risk of having their accounts misused by others if the browser is not closed completely. If the browser is left open, a different user can access the application from the browser page without entering credentials.