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.

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

Reference Design	Unified CCE
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.
- 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.

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

Operation	Allowed on Publisher	Allowed on Subscriber
Regenerate SAML Certificate	Always	Never
Regenerate Token Encryption/Signing Key	Always	Never
Update AuthCode/Token Expiry	Always	Only when publisher is connected
Enable/Disable Token Encryption	Always	Only when publisher is connected
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
Set Remote Syslog server	Always	Always

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.

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.

Related Topics

Configure the Cisco Identity Service, on page 5
Configure an Identity Provider (IdP), on page 11
Migrate Agents and Supervisors to Single Sign-On Accounts, on page 22
Register Components and Set Single Sign-On Mode, on page 19
Set up the System Inventory for Single Sign-On, on page 17
Set Up the System Inventory for Single Sign-On
Single Sign-On Migration and the Configuration Manager, on page 24

Single Sign-On Installation

Complete the installation or upgrade procedure. 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.

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.

Procedure

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**.

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 **New**.
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.

Related Topics

Configure the Identity Provider in Your Environment
Register Components and Set Single Sign-On Mode, on page 19

Establish Trust Relationship

To enable applications to use Cisco Identity Service (Cisco IdS) for Single Sign-On, perform the metadata exchange between the Cisco IdS and the Identity Provider (IdP).

- Download the SAML SP metadata file, `sp.xml`, on the Cisco IdS publisher primary node.
  1. Open Identity Service Management by doing either of the following:
     - Open the Identity Service Management window: `https://<Cisco IdS server address>:8553/idsadmin`.
     - In Unified CCE Administration, navigate to **Features** > **Single Sign-On** and click **Identity Service Management**.
  2. On the **Settings** > **IdS Trust** tab, download the SAML SP Metadata file, `sp.xml`.
- Download the Identity Provider Metadata file, federationmetadata.xml, from the IdP. For example,
  1. For AD FS, download the Identity Provider Metadata file from the IdP at the location:

     `https://<ADFSServer FQDN>/federationmetadata/2007-06/federationmetadata.xml`.
  2. On the **Identity Service Management** page, upload the Identity Provider Metadata file that was downloaded in the previous step.

The SAML SSO uses trust authentication certificates to exchange authentication and authorization details between the IdP (such as AD FS) and the Cisco IdS. This secures the communication between the servers.

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

Integrate Cisco IdS to the AD FS

Procedure

Step 1 In AD FS, be sure that the default Authentication Type is set to Forms. (Cisco Identity Service requires the Identity Provider to provide form-based authentication.) See the Microsoft AD FS documentation for details.

Step 2 In AD FS server, open **AD FS Management**.

Step 3 Right-click **AD FS** -> **Trust Relationships** -> **Relying Party Trust**.

Step 4 From the menu, choose **Add Relying Party Trust** to launch the **Add Relying Party Trust Wizard**.

Step 5 In the **Select Data Source** step, choose the option **Import data about the relying party from a file**.

Step 6 **Browse** to the `sp.xml` file that you downloaded from Cisco Identity Server and complete the import to establish the relying party trust.

Step 7 Select the step **Specify Display Name**, and add a significant name you can use to identify the Relying Party Trust.

Step 8 For AD FS in Windows Server, select the option **I do not want to configure multi-factor authentication settings for the relying party at this time** in the Step **Configure Multi-factor Authentication Now**.

This step does not appear in AD FS 2.0 or 2.1. Continue with the next step.

Step 9 In the Step Choose Issuance Authorization Rules, select the option **Permit all users to access this relying party** and click **Next**.

Step 10 Click **Next** again to finish adding the relying party.

Step 11 Right-click on the **Relying Party Trust** and click **Properties**. Select the **Identifiers** tab.

Step 12 On the **Identifiers** tab, configure the following:

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.
	FQDN of the subscriber node of Cisco Identity Server.

Step 13 Still in **Properties**, select the **Advanced** tab.

Step 14 Select **secure hash algorithm** as **SHA-256** and then click **OK**.

Note In the following steps, you configure two claim rules to specify the claims that are sent from AD FS to Cisco Identity Service as part of a successful SAML assertion:

- A claim rule with the following custom claims, as AttributeStatements, in the assertion:
  - **uid** - Identifies the authenticated user in the claim sent to the applications.
  - **user_principal** - Identifies the authentication realm of the user in the assertion sent to Cisco Identity Service.
- A second claim rule that is a NameID custom claim rule specifying the fully qualified domain name of the AD FS server and the Cisco IdS server.

Follow the steps to configure these rules.

Step 15 In **Relying Party Trusts**, right-click on the Relying Party Trust you created, and click **Edit Claim Rules**.

Step 16 Follow these steps to add a rule with **Send LDAP Attributes as Claims** as the Claim rule template.

a) In the **Issuance Transform Rules** tab, click **Add Rule**.
b) In the Step **Choose Rule Type**, select the claim rule template **Send LDAP Attributes as Claims** and click **Next**.
c) In the **Configure Claim Rule** step, in the **Claim rule name** field, enter **NameID**.
d) Set the **Attribute store** drop-down to **Active Directory**.
e) Set the table **Mapping of LDAP attributes to outgoing claim types** to the appropriate **LDAP Attributes** and the corresponding **Outgoing Claim Type** for the type of user identifier you are using:

- When the identifier is stored as a **SAM-Account-Name** attribute:
  1. Select an **LDAP Attribute**of **SAM-Account-Name**, and set the corresponding **Outgoing Claim Type** to **uid** (lowercase).
  2. Select a second **LDAP Attribute** of **User-Principal-Name** and set the corresponding **Outgoing Claim Type** to **user_principal** (lowercase).
- When the identifier is a UPN:
  1. Select an **LDAP Attribute**of **User-Principal-Name**, and set the corresponding **Outgoing Claim Type** to **uid** (lowercase).

2. Select a second **LDAP Attribute** of **User-Principal-Name** and set the corresponding **Outgoing Claim Type** to **user_principal** (lowercase).

Note The SAM-Account-Name or UPN choice is based on the User ID configured in the AW.

Step 17 Follow these steps to add a second rule with the template **custom claim rule**.

a) Select **Add Rule** on the **Edit Claim Rules** window.

b) Select **Send Claims Using Custom Rule**.

c) Set the name of rule to the **fully qualified domain name (FQDN)** of the Cisco Identity Server publisher (primary) node.

d) Add the following rule text:

```
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>");
```

e) 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 18 Add the following rules for Federated Scenario:

a) Add the rule for Name ID:

- In the **Issuance Transform Rules** tab, click **Add**.
- Select the claim rule template as **Pass Through or Filter an Incoming Claim**.
- In the **Configure Claim Rule** field, enter the claim rule name.
- Select **Incoming Claim type** to **Name ID**.
- Select Incoming name_ID format to Transient Identifier, then click **Finish**.

b) Add the rule for uid:

- In the **Issuance Transform Rules** tab, click **Add**.
- Select the claim rule template as **Pass Through or Filter an Incoming Claim**.
- In the **Configure Claim Rule** field, enter the claim rule name.

- In the **Incoming Claim type** field, enter **uid**, then click **Finish**.

c) Add the rule for user_principal:

- In the **Issuance Transform Rules** tab, click **Add**.
- Select the claim rule template as **Pass Through or Filter an Incoming Claim**.
- In the **Configure Claim Rule** field, enter the claim rule name.
- In the **Incoming Claim type** field, enter **user_principal**, then click **Finish**.

Step 19 Click **OK**.

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 11
2	Set Authentication Type. See Authentication Types, on page 12.
4	Enable Signed SAML Assertions, on page 12
5	Optionally Customize the AD FS Sign-In Page in Windows Server to Allow User ID, on page 13

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 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 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 and follow the steps provided in *Kerberos Authentication (Integrated Windows Authentication)*.

Enable Signed SAML Assertions

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

Procedure

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.

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.

Procedure

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
```

Federation between Identity Provider(IdP)

Add Claim Description for AD FS 1

Procedure

Step 1 Open **AD FS Management Console**, select **Service** > **Claim Descriptions**.

Step 2 Right click **Claim Descriptions** and select **Add Claim Descriptions**.

Step 3 Create uid claim description:

a) Enter the display name as **`uid`**.

b) Enter the claim identifier as **`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/uid`**.

c) Check the **Publish this claim description in federation metadata as a claim type that this Federation Service can accept** check box.

d) Check the **Publish this claim description in federation metadata as a claim type that this Federation Service can send** check box, then click **OK**.

Step 4 Create user_principal claim description:

a) Enter the display name as **`user_principal`**.

b) Enter the claim identifier as **`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/user_principal`**.

c) Check the **Publish this claim description in federation metadata as a claim type that this Federation Service can accept** check box.
d) Check the **Publish this claim description in federation metadata as a claim type that this Federation Service can send** check box, then click **OK**.

Important After creating claim descriptions, update federation metadata of the claim provider trust in Hosted AD FS.

Add Claim Rules for Relying Party Trust in the AD FS 1

Use this procedure to add the Claim rules for the Relying Party Trust in the Customer AD FS:

Procedure

Step 1 Open **AD FS Management Console**.

Step 2 Select **Trust Relationships** > **Relying Party Trusts**.

Step 3 Select and right click the appropriate Relying party trust, then select **Edit Claim Rules**.

Step 4 Add a rule with **Send LDAP Attributes as Claims** as the Claim rule template.

a) In the **Issuance Transform Rules** tab, click **Add Rule**. Select the claim rule template **Send LDAP Attributes as Claims**.
b) For **Configure Claim Rule**, set the rule name as **NameID**.
c) Select **Attribute store** to **Active Directory**.
d) Map the LDAP attribute **User-Principal-Name** to the **Outgoing Claim Type** of **user_principal** (lowercase).
e) Select one of the possible LDAP attributes that identifies application users and map it to **uid** (lowercase).

Note The rule that you create can use one of several possible LDAP attributes to identify the user. The exact mapping depends on which attribute the rule uses:

- When the identifier is stored as a **SAMAccountName** attribute:
  - The Outgoing Claim Type **uid** maps to the LDAP attribute **SAM-Account-Name**.
  - The Outgoing Claim Type **user_principal** maps to the LDAP attribute **User-Principal-Name**.
- When the identifier is a UPN:
  - The Outgoing Claim Type **uid** maps to the LDAP attribute **User-Principal-Name**.
  - The Outgoing Claim Type **user_principal** maps to the LDAP attribute **User-Principal-Name**.

Step 5 Add another rule with the template **custom claim rule**.

a) Select **Add Rule** on the **Edit Claim Rules** window.
b) Select **Send Claims Using Custom Rule**.
c) Set the name of rule to the **fully qualified domain name (FQDN)** of the Cisco Identity Server publisher (primary) node.

d) Add the following rule text:

```
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>");
```

- Set **<AD FS Server FQDN>** to match exactly (including case) the AD FS FQDN.
- Set **<fully qualified domain name of Cisco IdS>** to match exactly (including case) the Cisco Identity Server FQDN.

Step 6 Click **OK**.

Add Claim Rules for Claim Provider Trust in the AD FS 2

Note Add the claim rules for Claim Provider Trust in the ADFS where Cisco IDS is registered.

Procedure

Step 1 Open **AD FS Management Console**.

Step 2 Select **Trust Relationships** > **Claim Provider Trusts**.

Step 3 Select and right click the appropriate Claims provider trust, then select **Edit Claim Rules**.

Step 4 In the **Acceptance Transform Rules** tab, click **Add**.

Step 5 Add the rule for Name ID:

a) Select the claim rule template as **Pass Through or Filter an Incoming Claim**.
b) In the **Configure Claim Rule** field, enter the claim rule name.
c) Select **Incoming Claim type** to **Name ID**.
d) Select Incoming name_ID format to Transient Identifier, then click **Finish**.

Step 6 Add the rule for uid:

a) Select the claim rule template as **Transform an Incoming Claim**.
b) In the **Configure Claim Rule** field, enter the claim rule name.
c) Select **Incoming Claim type** to **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/uid**.
d) Select **Outgoing Claim type** to **uid**, then click **Finish**.

Step 7 Add the rule for user_principal:

a) Select the claim rule template as **Transform an Incoming Claim**.
b) In the **Configure Claim Rule** field, enter the claim rule name.
c) Select **Incoming Claim type** to **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/user_principal**.
d) Select **Outgoing Claim type** to `user_principal`, then click **Finish**.

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.

Procedure

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.

Reset Live Data Streaming Data Source After Upgrade and Migration

If you upgrade from Packaged CCE 11.0 to 11.5(1), and then switch from Packaged CCE to a Unified CCE: 4000 Agents Rogger deployment in which Unified Intelligence Center is installed coresident with Live Data and Cisco IdS, you must reset the Live Data Streaming Data Source.

In this situation, when you set up the coresident machine in the system inventory, the system generates a new username and password for the Live Data API service that does not match the existing credentials for the Live Data Streaming Data Source. As a result, the Live Data Streaming Data Source is no longer online.

Perform the following procedure to reset the Live Data Streaming Data Source:

Procedure

- After you add the coresident CUIC, LD, IdS machine to the system inventory, access the Live Data CLI and run the following command:

  set live-data cuic-datasource

Note For more information about Live Data CLI, see the Live Data CLI Commands section of the 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.

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.
- If you are using Internet Explorer, verify that:
  - It is not in the Compatibility Mode.
  - You are using the fully qualified domain name of AW to access the CCE Administration (for example, **https://<FQDN>/cceadmin**).

Procedure

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.

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 Internet Explorer, 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. No changes are required for Internet Explorer.

Browser	Browser options to verify when using SSO
Internet Explorer	**1.** Open Internet Explorer. **2.** Click the **Tools (Alt+X)** icon, and then click **Internet options**. **3.** In the **General** tab, click **Tabs**. **4.** From the **When a new tab is opened, open:** drop-down list, verify that the **Your first home page** option is selected.
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.

Browser	Browser options to verify when using SSO
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

Important Be aware that this release does not provide support for disabling SSO once it is enabled.

Customers electing global hybrid mode to incrementally add SSO-enabled users may subsequently move to global enablement, or global enablement may be configured directly. However, the transition of hybrid mode to global off, of per-agent disablement while in hybrid mode, or of switching global on to global off is not supported at this time.

Customers who attempt to disable SSO after enabling it may experience user account inconsistencies, such as cleared (pre-SSO) passwords, invalid passwords, and Cisco Unified Intelligence Center reporting issues for supervisor accounts introduced after SSO was enabled. For this reason, be sure to back up Logger databases using the Microsoft SQL Server Backup and Restore utility.

Contact the Cisco TAC for questions or assistance.

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.

Important You cannot change the SSO state of a person who meets either of these conditions:

- The person record is linked to user records on multiple peripherals.

  Remove the user records from all but one peripheral before changing the SSO state of this person.

- The person is a supervisor.

  Remove the supervisor status before changing the SSO state of this person.

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.

The content file returns the first 12,000 agents and supervisors who have not been migrated to SSO accounts. After you run the bulk job to update users from that group of records, you can download the SSO Migration content file again to update additional agent and supervisor records.

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

For instructions on how to setup SSO for Agent or Supervisor login, see the Configure the Cisco Identity Service, on page 5.

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.

Procedure

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.

When the bulk job completes, the agents and supervisors are enabled for SSO and their usernames are updated. You can open an individual user's record to see the changes.

Step 5 Repeat this procedure, if needed, to migrate additional agents and supervisors to SSO usernames.

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.

Single Sign-On Migration and the Configuration Manager

When the global SSO-enabled setting is Hybrid, you can use several of the existing Unified CCE Configuration Manager tools to either:

- Enable (or disable) users individually for single sign-on
- Prevent changes to system configuration information access

Tool	General description	New functionality specific to single sign-on
Agent Explorer (in Explorer Tools)	Allows you to view, and (if you have maintenance privileges) define, delete, or edit agent records, routes, peripheral targets, labels, and their relationships. You can also designate an agent as a supervisor.	Includes an **Enable single sign-on (SSO)** option. Check the check box to require a selected agent to sign in with SSO authentication. Uncheck the check box to require Unified CCE authentication. **Note** The check box is disabled when the global SSO-enabled setting is enabled or disabled.

Tool	General description	New functionality specific to single sign-on
Person Bulk Insert and Person Bulk Edit (in Bulk Configuration Tools)	Allow you to insert and update multiple configuration records in a single transaction from a single screen.	Allows you to view or change the person's SSO status. If the global SSO setting is hybrid, the person's SSO enabled setting is either: • **Yes** if the person uses SSO authentication • **No** if the person uses non-SSO authentication. (If global SSO is *enabled*, the person's SSO setting is ignored. All agents use SSO authentication. If global SSO is *disabled*, the person's SSO setting is ignored. All agents use non-SSO authentication.) **Note** In Import or Export files, the Person SSO Enabled setting is recorded in the file as a number: Yes = 1, No = 0. **Caution** Do not change the SSO state of any person who is a supervisor or who has user records on multiple peripherals.
Person List (in List Tools)	Allows you to list the persons currently defined in the database, to define new persons, and to view, edit, or delete the records of existing persons.	Includes an **Enable single sign-on (SSO)** option. Check the check box to require an agent associated with a selected Person to sign in with SSO authentication. Uncheck the check box to require Unified CCE authentication. **Note** The check box is disabled when the global SSO-enabled setting is enabled or disabled.

Tool	General description	New functionality specific to single sign-on
User List (in List Tools)	Allows you to list the users currently defined, associate new users with their Active Directory account, and view, edit, or delete the records of existing (nonsupervisor) users.	Prevents changes to Configuration Security Group membership or system information read-only access for SSO-enabled supervisors.

For more information, see the Explorer Tools online help, the Bulk Configuration Tools online help, or the List Tools online help.

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.

.

Perform this procedure after the upgrade has completed successfully.

Procedure

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>
```

Related Documentation

Refer to the following documents and other resources for more details about single sign-on.

See this information	Located here	For these details
Solution Design Guide for Cisco Unified Contact Center Enterprise	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html	Design considerations and guidelines for deploying the Cisco Unified CCE System.
Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html	How to monitor and manage Unified Contact Center Enterprise (Unified CCE) and Cisco Unified Intelligent Contact Management Enterprise (Unified ICM).
Release Notes for Cisco Unified Contact Center Enterprise Solutions	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-release-notes-list.html	New features and changes for this release of the Unified CCE solution.
Virtualization for Unified Contact Center Enterprise	https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html	Information about deploying Unified CCE (including single sign-on) on VMware.
Contact Center Enterprise Compatibility Matrix	https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html	Unified CCE requirements.
Configuration Manager: • Explorer Tools • List Tools	Online help	Changes to support single sign-on.
Unified CCE Administration Single Sign-On Tool	Online help	Changes to support single sign-on.
System Inventory Tool	This guide.	Information related to adding SSO-compatible components to the inventory.