Integration of Customer Instance with Shared Management

- Certificates for Unified Contact Center Enterprise Web Administration, on page 1
- Single Sign-on Integration, on page 14
- Unified CCDM Integration, on page 21
- Cisco UCDM Integration, on page 48
- ASA Integration, on page 51
- Session Border Controller Integration, on page 59
- Cisco Prime Collaboration Assurance Integration for Small Contact Center Deployment Model, on page 60

Certificates for Unified Contact Center Enterprise Web Administration

Note

- You must import self-signed certificates of solution components into the AW machines, if you are not using CA-signed certificates.
- Make sure that the certificates in the keystore pertain to the fully qualified domain name (FQDN) of the servers. If you have changed the domain name or hostname, be sure to update the certificates in the keystore.

CA Certificates

The following table outlines the CA certificate tasks for each component.

Components	Tasks
Unified CCE Components	1. Generate CSR, on page 3 2. Create Trusted CA-Signed Server or Application Certificate , on page 3 3. Upload and Bind CA-Signed Certificate, on page 5
Customer Voice Portal (CVP) Call Server/CVP Reporting Server[1]	See *Configuration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html
Email and Chat	See *Enterprise Chat and Email Installation and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/series.html
Cisco Unified Communications Manager (CUCM)	See *Security Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html
Cisco Unified Intelligence Center (CUIC)	Obtain and Upload Third-party CA Certificate, on page 11
Cisco Finesse	See *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html Deploy Certificate in Browsers
Live Data	Obtain and Upload Third-party CA Certificate, on page 11
Cisco Identity Service (IdS)	1. From the IdS server, generate and download a Certificate Signing Requests (CSR). 2. Obtain Root and Application certificates from the third-party vendor. 3. Upload the appropriate certificates to the IdS server. For more information, see https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-configuration-examples-list.html. Ensure to run the instructions in IdS server.
Cloud Connect	Obtain and Upload Third-party CA Certificate, on page 11
Virtualized Voice Browser (VVB)	See *Configuration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html

Components	Tasks
Customer Collaboration Platform	See *Security Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html

[1] CA certificate instructions for CVP Reporting Server are similar to CVP call server.

Generate CSR

This procedure explains how to generate a Certificate Signing Request (CSR) from Internet Information Services (IIS) Manager.

Procedure

Step 1 Log in to Windows and choose **Control Panel** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.

Step 2 In the **Connections** pane, click the server name.
The server **Home** pane appears.

Step 3 In the **IIS** area, double-click **Server Certificates**.

Step 4 In the **Actions** pane, click **Create Certificate Request**.

Step 5 In the **Request Certificate** dialog box, do the following:

a) Specify the required information in the displayed fields and click **Next**.
b) In the **Cryptographic service provider** drop-down list, leave the default setting.
c) From the **Bit length** drop-down list, select 2048.

Step 6 Specify a file name for the certificate request and click **Finish**.

Create Trusted CA-Signed Server or Application Certificate

You can create CA-signed certificate in any one of the following ways:

- Create certificate internally. Do the following:
  1. Set up Microsoft Certificate Server for Windows Server, on page 12
  2. Download the CA-signed certificate on each component server. Do the following:
     a. Open the CA server certificate page (*https://<CA-server-address>/certsrv*).
     b. Click **Request a Certificate** and then click **advanced certificate request**. Then do the following:
        1. Copy the Certificate Request content in the **Base-64-encoded certificate request** box.
        2. From the **Certificate Template** drop-down list, choose Web Server.
        3. Click **Submit**.
        4. Choose **Base 64 encoded**.
        5. Click **Download certificate** and save it to the desired destination folder.

c. On the CA server certificate page, click **Download a CA Certificate, Certificate Chain, or CRL**, and then do the following:

1. Select the Encoding method as **Base 64**.
2. Click **Download CA Certificate** and save it to the desired destination folder.

3. Import the Root CA and Intermediate Authority certificates into Windows trust store of every component. For more information on how to import CA certificates into Windows trust store, see *Microsoft* documentation.
4. Import the Root CA and Intermediate Authority certificates into Java keystore of every component. For more information, see Import CA Certificate into AW Machines, on page 4.

- Obtain certificate from a trusted Certificate Authority (CA). Do the following:

1. Send the CSR to a trusted Certificate Authority (CA) for sign-off.
2. Obtain the CA-signed application certificate, Root CA certificate, and Intermediate Authority certificate (if any).
3. Import the Root CA and Intermediate Authority certificates into Windows trust store of every component. For more information on how to import CA certificates into Windows trust store, see *Microsoft* documentation.
4. Import the Root CA and Intermediate Authority certificates into Java keystore of every component. For more information, see Import CA Certificate into AW Machines, on page 4.

Import CA Certificate into AW Machines

Procedure

Step 1 Log in to the AW-HDS-DDS Server.

Step 2 Run the following command:

```
cd %JAVA_HOME%\bin
```

Step 3 Copy the Root or intermediate certificates to a location in AW Machine.

Step 4 Run the following command and remove the existing certificate:

```
keytool.exe -delete -alias <AW FQDN> -keystore ..\lib\security\cacerts
```

Step 5 Enter the truststore password when prompted.

The default truststore password is **`changeit`**.

Note To change the truststore password, see Change Java Truststore Password, on page 13.

Step 6 At the AW machine terminal, run the following command:

- `cd %JAVA_HOME%\bin`
- `keytool -import -file <path where the Root or intermediate certificate is stored> -alias <AW FQDN> -keystore ..\lib\security\cacerts`

Step 7 Enter the truststore password when prompted.

Step 8 Go to Services and restart Apache Tomcat.

Upload and Bind CA-Signed Certificate

Upload CA-Signed Certificate to IIS Manager

This procedure explains how to upload a CA-Signed certificate to IIS Manager.

Before you begin

Ensure that you have the Root certificate, and Intermediate certificate (if any).

Procedure

Step 1 Log in to Windows and choose **Control Panel** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.

Step 2 In the **Connections** pane, click the server name.

Step 3 In the **IIS** area, double-click **Server Certificates**.

Step 4 In the **Actions** pane, click **Complete Certificate Request**.

Step 5 In the **Complete Certificate Request** dialog box, complete the following fields:

a) In the **File name containing the certification authority's response** field, click the **…** button.

b) Browse to the location where signed certificate is stored and then click **Open**.

c) In the **Friendly name** field, enter the FQDN of the server.

Step 6 Click **OK** to upload the certificate.
If the certificate upload is successful, the certificate appears in the **Server Certificates** pane.

Bind CA-Signed Certificate to IIS Manager

Bind CCE Web Applications

This procedure explains how to bind a CA Signed certificate in the IIS Manager.

Procedure

Step 1 Log in to Windows and choose **Control Panel** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.

Step 2 In the **Connections** pane, choose **<server_name>** > **Sites** > **Default Web Site**.

Step 3 In the **Actions** pane, click **Bindings...**.

Step 4 Click the type **https** with port 443, and then click **Edit...**.

Step 5 From the **SSL certificate** drop-down list, select the uploaded signed Certificate Request.

Step 6 Click **OK**.

Step 7 Navigate to **Start** > **Run** > **services.msc** and restart the IIS Admin Service.

If IIS is restarted successfully, certificate error warnings do not appear when the application is launched.

Bind Diagnostic Framework Service

This procedure explains how to bind a CA Signed Certificate in the Diagnostic Portico.

Procedure

Step 1 Open the command prompt.

Step 2 Navigate to the Diagnostic Portico home folder using:

cd <ICM install directory>:\icm\serviceability\diagnostics\bin

Step 3 Remove the current certificate binding to the Diagnostic Portico tool using:

DiagFwCertMgr /task:UnbindCert

Step 4 Open the signed certificate and copy the hash content (without spaces) of the Thumbprint field. Run the following command:

DiagFwCertMgr /task:BindCertFromStore /certhash:<hash_value>

If certificate binding is successful, it displays "The certificate binding is VALID" message.

Step 5 Validate if the certificate binding was successful using:

DiagFwCertMgr /task:ValidateCertBinding

Note DiagFwCertMgr uses port 7890 by default.

If certificate binding is successful, it displays "The certificate binding is VALID" message.

Step 6 Restart the **Diagnostic Framework** service by running the following command:

sc stop "diagfwsvc"

sc start "diagfwsvc"

If Diagnostic Framework restarts successfully, certificate error warnings do not appear when the application is launched.

Self-Signed Certificates

The following table lists components from which self-signed certificates are generated and components into which self-signed certificates are imported.

Note To establish a secure communication, run the commands (given in the links below) in the Command Prompt as an Administrator (right click over the **Command Prompt** and select **Run as administrator**).

Import Self-signed Certificates to Target Server	Generate Self-signed Certificates from Source Component Server	Links
AW Machines	Unified CCE Components (Router, Logger[2], Rogger[3], PGs, and HDS)	Import CCE Component Certificates, on page 7 Import Diagnostic Framework Portico Certificate into AW Machines, on page 8
	Cisco Finesse	Import VOS Components Certificate, on page 9
	Cisco Unified Intelligence Center (CUIC) Publisher and Subscriber	
	Cisco Identity Service (IdS) Publisher and Subscriber	
	Cloud Connect	
	Customer Collaboration Platform	
Logger	AW	Import CCE Component Certificates, on page 7
Rogger		

[2] Router and Logger are applicable only for 12000 Agent deployments.
[3] Applicable only for 2000 and 4000 Agent deployments.

Related Topics

Import CCE Component Certificates, on page 7
Import Diagnostic Framework Portico Certificate into AW Machines, on page 8

Import CCE Component Certificates

This procedure explains how to import self-signed certificates from a source CCE component sever to a target server.

Important The certificate CommonName (CN) must match the Fully Qualified Domain Name (FQDN) provided for the CCE components in the CCE Inventory.

Procedure

Step 1 Log in to the required CCE component server.

Step 2 From the browser (*https://<FQDN of the CCE component server>*), download the certificate.

If you want to regenerate a certificate instead of using the existing certificate, run the following commands:

a) From the **Cisco Unified CCE Tools** folder, launch the **SSL Encryption Utility**.
b) Go to the **Certificate Administration** tab and click **Uninstall**.

c) Click **Yes** to confirm uninstallation of certificate.

A message is displayed upon successful uninstallation of the certificate.

d) Click **Install** to generate a new certificate.

Step 3 Copy the certificate to a location in the target server.

Step 4 Run the following command at the target server (machine terminal):

- `cd %JAVA_HOME%\bin`
- `keytool -import -file <path where self-signed certificate is copied> -alias <FQDN of component Server> -keystore ..\lib\security\cacerts`

Step 5 Enter the truststore password when prompted.

The default truststore password is **changeit**.

Note To change the truststore password, see Change Java Truststore Password, on page 13.

Step 6 Go to Services and restart Apache Tomcat on target servers.

Import Diagnostic Framework Portico Certificate into AW Machines

Generate Diagnostic Framework Portico self-signed certificate on each CCE component server and import them into all AW Machines.

Procedure

Step 1 Log in to the CCE component server.

Step 2 From the Cisco Unified CCE Tools, open the Diagnostic Framework Portico.

Step 3 Download the self-signed certificate from the browser.

Step 4 Copy the certificate to a location in AW Machine.

Step 5 Run the following command at the AW machine terminal:

- `cd %JAVA_HOME%\bin`
- `keytool -import -file <path where self-signed certificate is copied> -alias <FQDN of the CCE component Server> -keystore ..\lib\security\cacerts`

Note The alias name of the CCE component server must be different from the alias name given while creating the CCE component server's self-signed certificate.

Step 6 Enter the truststore password when prompted.

The default truststore password is **changeit**.

Note To change the truststore password, see Change Java Truststore Password, on page 13.

Step 7 Go to Services and restart Apache Tomcat.

Import VOS Components Certificate

This procedure explains how to import self-signed certificates from a source VOS component sever to a target server.

Important The certificate CommonName (CN) must match the Fully Qualified Domain Name (FQDN) provided for the respective component servers in the CCE Inventory.

Procedure

Step 1 Sign in to the **Cisco Unified Operating System Administration** on the source component server using the URL (*https://<FQDN of the Component server>:8443/cmplatform*).

Step 2 From the **Security** menu, select **Certificate Management**.

Step 3 Click **Find**.

Step 4 Do one of the following:

- If the tomcat certificate for your server is not on the list, click **Generate Self-signed**. When the certificate generation is complete, reboot your server.
- If the tomcat certificate for your server is on the list, click the certificate to select it. (Ensure that the certificate you select includes the hostname for the server.)

Step 5 Download the self-signed certificate that contains hostname of the primary server.

Step 6 Copy the certificate to a location in the target server.

Step 7 Run the following command as an administrator at the target server (machine terminal):

- `cd %JAVA_HOME%\bin`
- `keytool -import -file <path where self-signed certificate is copied> -alias <FQDN of component Server> -keystore ..\lib\security\cacerts`

Step 8 Enter the truststore password when prompted.

The default truststore password is **`changeit`**.

Step 9 Go to Services and restart Apache Tomcat.

Certificates for Live Data

Certificates and Secure Communications

For secure Cisco Finesse, Cisco Unified Intelligence Center, and Live Data server-to-server communication, perform any of the following:

- Use the self-signed certificates provided with Live Data.

Note When using self-signed certificates, agents must accept the Live Data certificates in the Finesse desktop when they sign in before they can use the Live Data gadget.

- Obtain and install a Certification Authority (CA) certificate from a third-party vendor.
- Produce a Certification Authority (CA) certificate internally.

Self-Signed Certificates and Third-Party CA Certificates

For secure Cisco Finesse, Cisco Unified Intelligence Center, and Live Data server-to-server communication, you must set up security certificates (Applicable for both Self-Signed and Third-Party CA Certificates):

- For Cisco Finesse and Cisco Unified Intelligence Center servers to communicate with the Live Data server, you must to import the Live Data certificates and Cisco Unified Intelligence Center certificates into Cisco Finesse, and the Live Data certificates into Cisco Unified Intelligence Center.

On Server	Import Certificates From
Finesse	Live Data and Cisco Unified Intelligence Center
Live Data	None
Cisco Unified Intelligence Center	Live Data

Export Self-Signed Live Data Certificates

Live Data installation includes the generation of self-signed certificates. If you choose to work with these self-signed certificates (rather than producing your own CA certificate or obtaining a CA certificate from a third-party certificate vendor), you must first export the certificates from Live Data and Cisco Unified Intelligence Center, as described in this procedure. You must export from both Side A and Side B of the Live Data and Cisco Unified Intelligence Center servers. You must then import the certificates into Finesse, importing both Side A and Side B certificates into each side of the Finesse servers.

As is the case when using other self-signed certificates, agents must accept the Live Data certificates in the Finesse desktop when they sign in before they can use the Live Data gadget.

Procedure

Step 1 Sign in to Cisco Unified Operating System Administration on Cisco Unified Intelligence Center (https://*hostname of Cisco Unified Intelligence Center server*/cmplatform).

Step 2 From the **Security** menu, select **Certificate Management**.

Step 3 Click **Find**.

Step 4 Do one of the following:

- If the tomcat certificate for your server is on the list, click the certificate to select it. (Ensure that the certificate you select includes the hostname for the server.)
- If you are using self-signed certificate, do the following:
  a. Click **Generate New**.

b. When the certificate generation is complete, restart the Cisco Tomcat service and the Cisco Live Data NGNIX service.

c. Restart this procedure.

Step 5 Click **Download .pem file** and save the file to your desktop.

Be sure to perform these steps for both Side A and Side B.

Step 6 After you have downloaded the certificates from Cisco Unified Intelligence Center, sign in to Cisco Unified Operating System Administration on the Live Data server (http://hostname of LiveData server/cmplatform), and repeat steps 2 to 5. This is applicable only for Standalone LiveData.

What to do next

You must now import the Live Data and Cisco Unified Intelligence Center certificates into the Finesse servers.

Import Self-Signed Live Data Certificates

To import the certificates into the Finesse servers, use the following procedure.

Procedure

Step 1 Sign in to Cisco Unified Operating System Administration on the Finesse server using the following URL:

http://*FQDN of Finesse server*:8443/cmplatform

Step 2 From the **Security** menu, select **Certificate Management**.

Step 3 Click **Upload Certificate**.

Step 4 From the **Certificate Name** drop-down list, select **tomcat-trust**.

Step 5 Click **Browse** and browse to the location of the Cisco Unified Intelligence Center certificate (with the **.pem** file extension).

Step 6 Select the file, and click **Upload File**.

Step 7 After you have uploaded the Cisco Unified Intelligence Center certificate repeat steps 3 to 6 for Live Data certificates.This is applicable only for standalone Live Data.

Step 8 After you upload both the certificates, restart Cisco Finesse Tomcat on the Finesse server.

What to do next

Be sure to perform these steps for both Side A and Side B.

Obtain and Upload Third-party CA Certificate

You can use a Certification Authority (CA) certificate provided by a third-party vendor to establish an HTTPS connection between the Live Data, Cisco Finesse, Cisco Unified Intelligence Center servers, and Cloud Connect servers.

To use third-party CA certificates:

- From the **Cisco Unified Operating System Administrator** of Live Data, Cisco Finesse, Cisco Unified Intelligence Center, and Cloud Connect servers, generate and download a Certificate Signing Requests (CSR).
- Obtain root and application certificates from the third-party vendor.
- Upload the appropriate certificates to the Live Data, Unified Intelligence Center, Cisco Finesse, and Cloud Connect servers.

Follow the instructions provided in the *Unified CCE Solution: Procedure to Obtain and Upload Third-Party CA certificates (Version 11.x)* technical note at https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-enterprise-1101/200286-Unified-CCE-Solution-Procedure-to-Obtai.html .

Produce Certificate Internally

Set up Microsoft Certificate Server for Windows Server

This procedure assumes that your deployment includes a Windows Server Active Directory server. Perform the following steps to add the Active Directory Certificate Services role on the Windows Server domain controller.

Before you begin

Before you begin, Microsoft .Net Framework must be installed. See Windows Server documentation for instructions.

Procedure

Step 1 In Windows, open the **Server Manager**.

Step 2 In the **Quick Start** window, click **Add Roles and Features** .

Step 3 In the **Set Installation Type** tab, select **Role-based or feature-based installation** , and then click **Next**.

Step 4 In the **Server Selection** tab, select the destination server then click **Next**.

Step 5 In the **Server Roles** tab, check the **Active Directory Certificate Services** box, and then click the **Add Features** button in the pop-up window.

Step 6 In the **Features** and **AD CS** tabs, click **Next** to accept default values.

Step 7 In the **Role Services** tab, verify that **Certification Authority**, **Certification Authority Web Enrollment**, **Certificate Enrollment Web Service**, and **Certificate Enrollment Policy Web Service** boxes are box is checked, and then click **Next**.

Step 8 In the **Confirmation** tab, click **Install**.

Step 9 After the installation is complete, click the **Configure Active Directory Certificate Service on the destination server** link.

Step 10 Verify that the credentials are correct (for the domain Administrator user), and then click **Next**.

Step 11 In the **Role Services** tab, check the **Certification Authority**, **Certification Authority Web Enrollment**, **Certificate Enrollment Web Service**, and **Certificate Enrollment Policy Web Service** boxes box, and then click **Next**.

Step 12 In the **Setup Type** tab, select **Enterprise CA**, and then click **Next**.

Step 13 In the **CA Type** tab, select **Root CA**, and then click **Next**.

Step 14 In the **Private Key**, **Cryptography**, **CA Name**, **Validity Period**, and **Certificate Database** tabs, click **Next** to accept default values.

Step 15 In the following tabs, leave the default values, and click **Next**.

a. **CA for CES**

b. **Authentication Type for CES**

c. **Service Account for CES**

d. **Authentication Type for CEP**

Step 16 Review the information in the **Confirmation** tab, and then click **Configure**.

Download CA certificate

This procedure assumes that you are using the Windows Certificate Services. Perform the following steps to retrieve the root CA certificate from the certificate authority. After you retrieve the root certificate, each user must install it in the browser used to access Finesse.

Procedure

Step 1 On the Windows domain controller, run the CLI command certutil -ca.cert *ca_name*.cer, in which *ca_name* is the name of your certificate.

Step 2 Save the file. Note where you saved the file so you can retrieve it later.

Change Java Truststore Password

This procedure explains how to change a truststore password in a Windows machine.

Procedure

Step 1 Log in to the Windows machine.

Step 2 Run the following command:

```
cd %JAVA_HOME%\bin
```

Step 3 Change the truststore password by running the following command:

```
keytool.exe -storepasswd -keystore ..\lib\security\cacerts
Enter keystore password:  <old-password>
New keystore password:  <new-password>
Re-enter new keystore password:  <new-password>
```

Single Sign-on Integration

Establish Trust Relationship for Cisco IdS

To enable applications to use Cisco Identity Service (Cisco IdS) for Single Sign-On, perform the metadata exchange between the Cisco IdS and the Hosted 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://<Unified CCX server address>:8553/idsadmin`.
     - In Administration, navigate to **System** > **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 authentication.
- If the IdP certificates are automatically rolled-over, manually renewed, or updated by the administrator, then re-establish the trust relationship between the IdS and the IdP.

Integrate the Customer Instance to the Shared ADFS

Integrate Cisco IdS to the Shared Management 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**.

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-1** 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**.

Federate the Customer ADFS to the Shared Management ADFS

Add Claim Description for Customer ADFS

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 Customer ADFS

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

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 Shared Management ADFS

Note Add the claim rules for Claim Provider Trust in Hosted (Shared Management) ADFS (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**.

Optionally Customize the ADFS Sign-In Page in Windows Server to Hide Federated Domains List

Follow the procedure to automatically redirect the end-user to their organization. This is required when your Contact Center solution has multi-domain federations with partners and does not want to display the list of IdPs that it is federated with.

Procedure

Step 1 Open the **Windows Powershell** of Hosted AD FS.

Step 2 Enter the **`Set-ADFSClaimsProviderTrust -TargetName "<adfsCPName>" -OrganizationalAccountSuffix @("<mydomain>")`** command.

In the mentioned command, **<adfsCPName>** represents **AD FS Claim Provider Trust Name** and **<mydomain>** represents **Organization Domain Name**.

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 On the Download SAML SP Metadata and Upload IdP Metadata windows, click Next as you have already established trust relationship between IdP and IdS.

Step 7 On the AD FS authentication window, provide the login credentials.

Step 8 On successful SSO setup, the message "SSO Configuration is tested successfully" is displayed.

Note If you receive the error message "An error occurred", ensure that the claim you created on the AD FS is enabled.

If you receive the error message "IdP configuration error: SAML processing failed", ensure that the rule has the correct names for Ids and AD FS.

Unified CCDM Integration

Unified CCDM is generally hosted on shared management level across multiple customer instances. This chapter describes how to configure multiple customer instances from a shared Unified CCDM.

This section describes the following steps:

- Configure Unified CCE Servers in Unified CCDM Cluster, on page 21
- Configure Unified CVP Servers in Unified CCDM Cluster, on page 29
- Create Users in Active Directory, on page 31
- Configure Unified CCE for Partitioned Internet Script Editor, on page 31
- Deployment Specific Configurations, on page 33
- Configure IDP, on page 39

Configure Unified CCE Servers in Unified CCDM Cluster

Unified CCE components must be configured before Unified CCDM can connect to them for Provisioning. Complete the following procedures to configure Unified CCE for Unified CCDM connectivity

- Unified CCE Prerequisites, on page 21
- Setup Unified CCE Servers in Unified CCDM Cluster, on page 26
- Create an Equipment Mapping, on page 28

Unified CCE Prerequisites

Before you integrate Unified CCE with Unified CCDM, you must setup SQL agents and CMS server. Complete the following procedures for prerequisites configurations.

- Configure Unified CCE AW Database(AWDB) for Unified CCDM, on page 21
- Configure the Unified CCE AW for Provisioning, on page 22

Configure Unified CCE AW Database(AWDB) for Unified CCDM

Before configuring AWDB, ensure that you create a two-way trust relationship between forests if:

- your CCDM and the Unified CCE domains are in seperate forests
- your customer domains and Unified CCE domains are in seperate forests

- your customer domains and CCDM domains are in seperate forests

If you use SQL Server Authentication to connect Unified CCDM to

Unified CCE

, no configuration of the Administrative Workstation Database (AWDB) is required. If you do not use the SQL authentication, you must configure the AWDB to connect the Unified CCDM to Unified CCE.

Complete the following procedure to configure AWDB:

Procedure

Step 1 Log in to the Unified CCE Admin Workstation Server with local administrative privileges.

Step 2 Open **SQL Server Management Studio** and click **Connect** to establish connection with the server.

Step 3 Expand **Security** folder and choose **Logins**.

Step 4 Right-click Logins and choose **New Logins**.

Step 5 To add SQL logins for both the Side A and Side B Unified CCDM Servers (this includes Web server, CCDM Domain administrator and Database server on both the sides).

Configure the General page as follows:

a. In the Login Name field, enter the name for the machine in the following format: <DOMAIN>\<Unified CCDM-HOSTNAME>$.

b. Choose Windows Authentication unless you are connecting to a server on another domain.

c. Select Default language as **English**.

Configure the User Mapping page as follows:

a. In the Users mapped to this login field, check hcs_awdb database.

b. In the Database role membership for field, check the following roles to grant to the AWDB login: **public** and **db_datareader**.

Step 6 Click **OK**.

Step 7 Repeat steps 1 to 6 for Side B if Unified CCE AW server is dual-sided.

Configure the Unified CCE AW for Provisioning

For each Unified CCE instance that Unified CCDM Resource Management connects to must meet the following criteria:

-
- Configure an Application Instance on the Unified CCE distributor machine (AW) for Unified CCDM to connect to Unified CCE. Configure the Application Instance with Application Type as **Cisco Voice**.

Note The application instance for CCDM is provided as part of the load base configuration. For more information, see Application Instance List from Load Base Configuration. The default name of the Application Instance is **CCDM** as per the Load Base configuration.

- If the AW is dual-sided, each Unified CCE AW must connect to a different RMI registry port on the Unified CCDM Database Server.

Each Unified CCE instance requires a distinct primary distributor AW to connect to Unified CCDM resource management.

Set Up CMS Server on Unified CCE

A new application connection must be defined on each configured Unified CCE

instance for each Database Server. This ensures that in a dual-sided system, the alternate side can also connect to the Unified CCE in a failover scenario.

Complete the following procedure to set up the Configuration Management Service (CMS) server on each Unified CCE:

Before you begin

Before configuring the Unified CCDM server cluster you must ensure that the CMS Server(s) are set up correctly on each Unified CCE for each Unified CCDM Database Server. Firstly, check that the CMS Node option was selected when the Admin Workstation was configured. You can determine if this was the case by looking for a cmsnode and a cms_jserver process running on the Unified CCE.

Procedure

Step 1 In Unified CCE Admin Workstation Server Side A, open **CMS Control** application.

Step 2 Under **Application** tab, click **Add** and configure the following in the **Application Connection Details** page.

a) **Administration & Data Server Link** - Enter the name of the Unified CCDM Database Server. This should be in all capital letters, with Server appended, for example, CCDMDBServer.

b) **Administration & Data Server RMI Registry Port** - Enter the Unified CCE AW port number for the Unified CCDM provisioning service to connect to. This is usually 2099. If the Unified CCDM provisioning service connects to multiple Unified CCE instances, it is required that each instance should use a different port.

When you configure CMS server onUnified CCE at Side B, use a different RMI registry port.

c) **Application link** - Enter the name of the Unified CCDM Database Server. This should be in all capital letters, with Client appended, for example, CCDMDBClient.

d) **Application RMI registry port** - Enter the Unified CCDM Database Server port number for the Unified CCE AW to connect to.

This should be rather the same as for the Administration & Data Server RMI Registry Port. Each Unified CCE AW must connect to a different port on the Unified CCDM Database Server. You should record this information for future use.

e) **Application host name**- Enter the server name, for example, Unified CCDM.
f) Click **OK** to save the changes and to close the **Application Connection Details**.

Step 3 Click **OK** to save your changes and to close the **CMS Control Console**.

Step 4 Repeat steps 1-3 to set up CMS Server on Cisco Unified CCE Admin Workstation Server (Side A) for Unified CCDM Database Server Side B.

Enure that you use the same ports used for Side A Unified CCDM Database Server under **Application Connection Details**.

Note If the CMS JServer process fails to connect Unified CCDM, restart the Unified CCE Enterprise Distributor service.

Create Conditional Forwarders for Customer Domain

Complete the following procedure to create conditional forwarder.

Before you begin

Note You need to complete this procedure only for Cisco Hosted Collaboration Solution for Contact Center deployments.

Procedure

Step 1 Go to DNS Manager.
Step 2 Click the **Conditional Forwarder**.
Step 3 Right-click and select **New Conditional Forwarder**.
Step 4 Enter the DNS domain name.
Step 5 In the IP address field, click and enter the NAT IP address of the Service Provider domain.
Step 6 Click **OK**.

Create Forwarders for Customer Domain

Complete the following procedure to create forwarders.

Before you begin

Note You need to complete this procedure only for Cisco Hosted Collaboration Solution for Contact Center deployments.

Procedure

Step 1 Go to DNS Manager.
Step 2 Right-click the domain name.
Step 3 Click **Properties**.
Step 4 Click the **Forwarders** tab and then click **Edit**.
Step 5 In the IP address field, click and enter the NAT IP address of the Service Provider domain.
Step 6 Click **OK** to create forwarders and then click **Apply** and **Ok**.

Create Conditional Forwarders for Service Provider Domain

Complete the following procedure to create conditional forwarder.

Procedure

Step 1 Go to DNS Manager.
Step 2 Click the **Conditional Forwarder**.
Step 3 Right-click and select **New Conditional Forwarder**.
Step 4 Enter the DNS domain name.
Step 5 In the IP address field, click and enter the NAT IP address of the customer domain.
Step 6 Click **OK**.

Create Forwarders for Service Provider Domain

Procedure

Step 1 Go to DNS Manager.
Step 2 Right-click the **Domain Name**.
Step 3 Click **Properties**.
Step 4 Click the **Forwarders** tab and then click **Edit**.
Step 5 In the IP address field, click and enter the NAT IP address of the customer domain.
Step 6 Click **OK** to create forwarders and then click **Apply** and **Ok**.

Create Two-Way Forest Trust

Complete the following procedure from the customer domain controller to create a two-way forest trust:

Procedure

Step 1 Right-click the domain under the **Active Directory Domains and Trusts**.
Step 2 Click **Properties**.
Step 3 Click the **Trust** tab and then click **New Trust**.
Step 4 Click **Next**.
Step 5 Enter the service provider domain name and click **Next**.
Step 6 Select the **Forest Trust** option and click **Next**.
Step 7 Select the option **Two-way Trust** and click **Next**.
Step 8 Select the option **Both this domain and specified domain** and click **Next**.
Step 9 Enter the authentication username for the customer and a password for the specified domain and click **Next**.

You must have the administrator privileges to create the trust.

Step 10 Select the option **Forest-wide authentication** and then click **Next** until you reach Confirm Outgoing Trust.
Step 11 Select the option **Yes, confirm the outgoing trust**, and click **Next**.
Step 12 Select the option **Yes, confirm the incoming trust**, and click **Next**.
Step 13 Click **Finish**.

Launch the Integrated Configuration Environment

Complete the following procedure to launch the Integrated Configuration Environment (ICE) in the Unified CCDM data server.

Procedure

Step 1 Open the **Integrated Configuration Environment** application.
Step 2 On the **Database Connection** page, enter:
a) The **Server Name** field default value is **current machine**.
b) In the **Database Name** field, accept the default value (Portal).
c) In the **Authentication** field, accept the default value.
Step 3 Click **Test** to test the connection to the database server for the first time. If the test fails, check the **Database Connection** settings.
Step 4 Click **OK** to open the ICE.

When ICE starts, the Cluster Configuration tool is the default tool. You can use the **Tool** drop-down list in the toolbar to switch to other ICE tools.

Setup Unified CCE Servers in Unified CCDM Cluster

Complete the following procedure to configure Unified CCE for Unified CCDM:

Procedure

Step 1 Launch **Integrated Configuration Environment** on Unified CCDM Database Server Side A, see Launch the Integrated Configuration Environment, on page 26.

Step 2 In the ICE Cluster Configuration tool, from **Tool** drop-down list, select **Cluster Configuration**.

Step 3 Click **Configure Cisco Unified Contact Enterprise Servers**.

Step 4 From **Select Task** drop-down list, select **Add a New Instance** and click **Next**.

Step 5 In **Specify Resource Name**, specify a name for the instance you want to configure. Click **Next**.

Step 6 In **Select Required Components**, select the required components in the deployment and click **Next**.

- **Admin Workstation** - This is a required component in all configurations.
- **Provision Components (ConAPI/Unified config)** - Select this option if you require resource management.

Step 7 In **Configure Redundancy**, select whether you want to configure a single-sided or a dual-sided setup.

Step 8 In **Configure AW Server**, enter the primary server name and IP address.

Note If Unified CCE is dual-sided, then enter the secondary server name and the IP address also.

Step 9 In **Configure Connection Details**, enter authentication details to connect to the Admin Workstation database.

a) **Windows Authentication**: This is a default authentication mode.

b) **SQL Authentication**: Specify the SQL Server User name and the corresponding password to connect to the databases.

Step 10 In **Select Unified CCE Instance**, select the AW instance for the deployment and click **Next**.

Step 11 In **Configure Cisco Unified Contact Center Enterprise Server** window, configure **Unified Config Web Services** as follows:

- Enter the domain username and password for primary Unified CCE Admin workstation server in **Configure Primary Unified Config Web Service** page and click **Next**.
- If Unified CCE is dual-sided, then enter the domain username and password for secondary Unified CCE Admin Workstation server in **Configure Secondary Unified Config Web Service** page and Click **Next**.

Note Use the domain account credentials to login, username format must be *username@domain.com*.

Step 12 If you selected the option ConAPI Server (Provisioning) option in Step 4, enter the following details:

- **Local Registry Port** - Enter the port number of the Unified CCE for the Unified CCDM Provisioning service to connect. Default port is 2099. Ensure that you enter the same Unfied CCDM Database Server port number configured in the Application RMI registery port of the Set Up CMS Server on Unified CCE , on page 23.
- **Remote Registry Port** - Enter the port number of the Unified CCDM Database Server for the Unified CCE to connect. Default port is 2099. Ensure that you enter the same Unified CCE AW port number configured in the Administration & Data Server RMI Registry Port of the Set Up CMS Server on Unified CCE , on page 23.
- **Local Port** - Select this as the designated port for live provisioning traffic between the Unified CCE and Unified CCDM servers. Assign a unique port for each Unified CCE. Configure the firewall between the Unified CCE and Unified CCDM server to allow two-way traffic on this port.

Note If Unified CCE is dual-sided, enter the same port details configured for Side B in Set up CMS Server on Unified CCE.

Step 13 In **Configure ConAPI Application Instance** dialog box, enter the following details and click **Next**:

- **Application Name** - Name of the application to be used for provisioning Unified CCE from Unified CCDM. Enter the value as **CCDM** (pre-configured as part of load base configurations).
- **Application Key** - Use the password for the application you specified above.

Step 14 In **Multi Media Support** dialog box, select **Yes** if you are using a Cisco Unified WIM and EIM application instance to provide support for non-voice interactions. The default is **No**.

Step 15 In **Purge On Delete** dialog box, select **Yes** if you want to purge items from the Unified CCE automatically when they are deleted from Unified CCDM. The default is **Yes**.

Step 16 In the Supervisor Active Directory Integration dialog box, select **Yes** if you want to enable support for associating existing Active Directory user accounts for Unified CCE Supervisors. The default is **No**. If you select **Yes**, enter the following:

a. In **Configure Active Directory Connections**, enter the addresses of both primary and secondary domain controllers and configure the required security settings to connect. Click **Next**.

b. In the **Select Supervisor Active Directory Location**, select the required active directory and click **Next**.

Step 17 Review the details in the Summary page and click **Next** to apply the changes to the model.

Step 18 When the Unified CCE is successfully configured click **Exit** to close the wizard and then click **Save** to retain your changes to the database.

Create an Equipment Mapping

Complete the following procedure to create an equipment mapping between a tenant and the Unified CCE equipment.

Note To create a equipment mapping for SCC deployment, see Deployment Specific Configurations, on page 33.

Procedure

Step 1 Launch **Integrated Configuration Environment** on Unified CCDM Database Server Side A, see Launch the Integrated Configuration Environment, on page 26.

Step 2 From **Tool** drop-down list, select **Cluster Configuration**. Select **Equipment Mapping** tab.

Step 3 In the folder tree, right-click on root folder and select **Add Tenant**.

Step 4 Provide name for the new tenant.

Step 5 Create tenant for all customer.

Example:

Cust1CCE

Step 6 Select newly added Customer Tenant, in adjoining pane, check Unified Contact Center equipment check-box that you want to associate with the selected tenant.

Step 7 In the right-hand pane, choose **Default Import Location**.

Using Default Import Location, all the resources imported to selected tenant in Unified CCDM.

Step 8 Click **Save**.

Configure Unified CVP Servers in Unified CCDM Cluster

- Setup Unified CVP Servers in Unified CCDM Cluster, on page 29
- Equipment Mapping for CVP with CCDM , on page 30

Setup Unified CVP Servers in Unified CCDM Cluster

The Configure Cisco Unified CVP Servers wizard configures Cisco Unified CVP server clusters. A Cisco Unified CVP server cluster consists of a Unified CVP Operations Console and, optionally, one or more call servers. To configure a Cisco Unified CVP server cluster:

Procedure

Step 1 Launch **Integrated Configuration Environment** on Unified CCDM Database Server Side A, see Launch the Integrated Configuration Environment, on page 26.

Step 2 In ICE Cluster Configuration tool, select the **Setup** tab and click **Configure Cisco Unified CVP Servers** to start the wizard.

Step 3 Select **Add a New Instance** and click **Next**.

Step 4 In **Specify Unified CVP Operations Console Resource Name** dialog box, specify a name for the Unified CVP operations console and click **Next**.

Step 5 In **Select Version** dialog box, specify the version of Unified CVP that is running on the CVP cluster you are configuring and click **Next**.

Step 6 In **Configure Unified CVP Operations Console** dialog box, enter the following:

- **Primary Server**:
  - **Sever Name**: This is the non-domain qualified machine name where the Cisco Unified CVP Operations Console is deployed.
  - **Server Address**: This defaults to Server Name. You can change this to an IP Address or a domain qualified name of the server.
- **Secondary Server**: This option is always disabled.

Step 7 Click **Next**.

Step 8 In **Configure Primary Unified Config Web Service** dialog box (only shown when the selected Unified CVP version is 10.0 or later), enter the following details:

- **URL**: This is the auto-generated URL of the primary unified config web service on the Unified CVP cluster
- **User Name**: This is a username with appropriate access to the Unified CVP that the web service is running on
- **Password**: This is the password for the user

Step 9 Click **Next**.

Step 10 In **Select Number of Call Servers** dialog box, specify the number of CVP call servers in the CVP cluster and click **Next**.

Note All CVP call servers must be on the same Unified CCE as the Unified CVP operations console.

Step 11 If you specified at least one call server:

a. In **Specify Unified CVP Call Server 1 Resource Name** dialog box, enter a name for the call server.

b. In **Configure Unified CVP Call Server 1** dialog box, enter the following:

- **Primary Server**:
  - **Sever Name**: This is the non-domain qualified machine name where the Cisco Unified CVP call server.
  - **Server Address**: This defaults to Server Name. You can change this to an IP Address or a domain qualified name of the server.
- **Secondary Server**: This option is always disabled.

c. Click **Next**.

Note Repeat this step to configure more than one call server.

Step 12 Optional, In **Configure** Unified CCE **Server** dialog box, select the Unified CCE servers that is linked to the configured unified CVP instance.

Step 13 The **Summary** dialog box, provides the brief details of the Unified CVP cluster being configured and the settings you have chosen.

Step 14 Check the details, click **Next**.

Step 15 A confirmation message is displayed to indicate that the wizard has completed successfully. Click **Exit** to close the wizard.

Step 16 Click the **Save** icon.

Equipment Mapping for CVP with CCDM

For small contact center deployment model once the CVP integrated, by default CVP will get imported under unallocated folder.

Procedure

Step 1 Open **Integrated Configuration Environment** application, select **Cluster Configuration** > **Equipment Mapping** tab.

Step 2 In the folder tree, right-click on **Root** and click on **Add Tenant** and provide the name for Tenant.

Note You can also use existing Unified CCE Customer tenant to map unified CVP.

Step 3 Create Tenant for all CVP customer instances.

Example:

Cust1CVP

Step 4 Select newly added Tenant, in the adjoining pane, check the check box next to each item of Unified CVP that you want to associate with the selected Tenant.

Step 5 In right hand pane, select **Default Import Location** to import all the resources to selected tenant in Unified CCDM.

Step 6 Click **Save**.

Create Users in Active Directory

You must create a user in active directory to create a tenant or sub-customer from CCDM.

Procedure

Step 1 Log in to **Active Directory Domain**.

Step 2 Open **Active Directory Users and Computers** and click **User**.

Step 3 Right-click **User** and select **New** > **User**

Step 4 Enter **First Name**, **Last Name**, **user logon name** and click **Next**.

Step 5 Enter **Password** and retype the same password in **Confirm Password** field.

Step 6 Check **user cannot change password** check box.

Step 7 Check **Password never expires** check box and click **Next**.

Step 8 Click **Finish**.

Configure Unified CCE for Partitioned Internet Script Editor

Cisco's Internet Script Editor (ISE) can be integrated with Unified CCDM, which allows routing scripts and the resources within those routing scripts to be partitioned using Unified CCDM security. ISE users can see only the scripts and the resources within those scripts that they are authorized to access, according to the Unified CCDM security model. For example, when creating a routing script element to route to a dialed number, the ISE user will only see the dialed numbers that the corresponding Unified CCDM user is authorized to access. Similarly, when viewing the available routing scripts, the ISE user will only see the scripts available to the corresponding Unified CCDM user.

ISE integration with Unified CCDM uses the Unified CCDM Analytical Data Web Service to implement the secure partitioning, and requires specific configuration settings in both Unified CCE and Unified CCDM in order to work properly.

Note

- Secure partitioning using Unified CCDM is currently only supported for the Cisco Internet Script Editor (ISE). Users of the standard Script Editor on the Unified CCE AW will still see all resources on their associated Unified CCE instance.
- For Small contact Center Deployment model, see Integration of Small Contact Center Agent Deployment for Partition Internet Script Editor with CCDM, on page 39

• Configure Unified CCE Admin Workstation for Internet Script Editor, on page 32
• Create User
• Assign Roles to Users
• Install Internet Script Editor , on page 33
• Provision Routing Script Using Internet Script Editor

Configure Unified CCE Admin Workstation for Internet Script Editor

Complete the following procedure to configureUnified CCE Admin Workstation for Internet Script Editor integration with Unified CCDM

Procedure

Step 1 Log In to Unified CCE Web Setup and navigate to **Component Management** >**Administration & Data server**, check the **Administrator** & **Data server** check-box and click **Edit**.

Step 2 Click **Next** until you see Database and Options tab, in Database and Options tab select the following options.

a) Select **Internet Script Editor (ISE) Server.**
b) Select **Authorization Server**.
c) Enter the name of the Authorization Server.
This is the Unified CCDM App/Web Server that will be used to apply Unified CCDM security to partition the resource data.
d) Enter the port that has Unified CCDM Analytical Data Services Web Service hosted.
By default, this port is 8087. If this is changed for your installation, enter the value that your installation uses.
e) Click **Next**.

Step 3 In Central Controller Connectivity tab enter the following details.

a) Enter the IP addresses for Router Side A, Router Side B, Logger Side A, Logger Side B, in **Central Controller Connectivity** section
b) Enter the domain name in **Central Controller Domain**.
c) Select the radio button **Central Controller Side A preferred** in **Central Controller Preferred Side** and click **Next**

Step 4 In **Summary** tab, click **Finish**

Step 5 Ensure that the firewall is configured on the server running the Unified CCE AW to allow inbound traffic from ISE on the appropriate port.

Step 6 Ensure that the specified Authorization Server port on the Unified CCDM Authorization Server has been configured in the firewall to allow inbound HTTPS traffic.

Install Internet Script Editor

Procedure

Step 1 Download the Internet Script Editor from AW machine `https://localhost/install/iScriptEditor.htm`

Step 2 Save `iscripteditor.exe` in a shared location for the particular customer/sub customer.

Step 3 Double-click `iscripteditor.exe` file.
Displays **Cisco ICM Internet Script Editor Setup** window

Step 4 Click **Next**.

Step 5 Select the folder to install files and click **Next**.

Step 6 After installation, click **Finish**.

Deployment Specific Configurations

- Integration of Small Contact Center Agent Deployment for UCCE with CCDM, on page 33
- Integration of Small Contact Center Agent Deployment for Partition Internet Script Editor with CCDM, on page 39

Integration of Small Contact Center Agent Deployment for UCCE with CCDM

- Create Customer Definition, on page 33
- Map Equipment for Small Contact Center Deployment, on page 34
- Create User
- Assign Permission to Sub-customer Tenant and User
- Resource Allocation for Small Contact Center Agent Deployment, on page 35
- Naming Convention for the Resources in Small Contact Center Agent Deployment Model , on page 38

Create Customer Definition

Procedure

Step 1 Log in to AW machine and Open the **Configuration Manager**.

Step 2 Select **Explorer Tools** > **ICM Instace Explorer**.

Step 3 Click **Retrieve** and select the ICM Instance for SCC Deployment.

Step 4 Click **Add Customer Definition**.

Step 5 In **Name** field, enter the name of the sub customer definition.

Example:

SubCust1

Step 6 From **Network VRU** drop-down list, select **CVP_Network_VRU** option.

Step 7 Click on **Save**.

Note Repeat the same steps for all Sub Customer.

Map Equipment for Small Contact Center Deployment

Complete the following procedure to create an equipment mapping between a tenant or folder and the Unified CCE equipment for Small Contact Center.

Before you begin

Integrate AW with CCDM. For more information on How to Integrate AW, See Setup Unified CCE Servers in Unified CCDM Cluster, on page 26

Procedure

Step 1 In the ICE Cluster Configuration tool, select **Equipment Mapping** tab.

Step 2 In the folder tree, right-click on root, click **Add Tenant** and provide the name for tenant.

Create tenant for all sub customers.

Example:

SubCust1

Step 3 Select the newly created Sub Customer Tenant and In the adjoining pane select the check box or check boxes next to each item of Unified CCE equipment that you want to associate with the selected Tenant.

Step 4 In right-hand side pane, choose **Customer Resource Mapping** and click + icon.

Step 5 From **Type** drop-down list, select **Remote Tenant** option.

Step 6 From **Resource** drop-down list, select the customer definition created for sub customer.

Step 7 Click **Active Directory Configuration** tab and configure as follows:

a) Check **Configure Active Directory Settings** check-box.
b) In **Primary Domain Controller** field, enter Sub-customer Domain Controller IP address.
c) Click **Next** and ensure that domain controller name is correct.
d) Click **Update**.

Step 8 Select **Small Contact Center Settings** tab and configure as follows:

a) Check **Enable Small Contact Center** check-box.
b) In **Department Name** field, enter department name for the sub-customer domain.
c) Click **Create Department**.

Step 9 Click **OK**.

Step 10 Repeat the above steps for all sub customers.

Step 11 Click the unallocated folder and select the Unified CCE folder that is integrated. In the adjoining pane, check each item of Unified CCE equipment check-box that you want to associate with the selected Tenant and check **Default Import** check box.

Note By Default all the Configuration under Unified CCE will get imported under **Unallocated** folder.

Step 12 Click on **Save**

Resource Allocation for Small Contact Center Agent Deployment

- Move Resource to Sub Customer Tenant, on page 37
- Map Labels to the Network VRU Type, on page 38

* Configuration done by Sub Customer User

** Configurations provided in load base configuration which gets imported to Unallocated folder

*** Configurations are moved to sub customer domain from unallocated folder and configurations are done by service provider

Parameters	Configuration done by Sub Customer	Configuration done by Service Provider	Notes
Peripheral and Routing Client		** & ***	Peripherals, routing client of CUCM and MR are moved under Sub Customer Tenant.
Logical Interface Controller		** & ***	Logical Interface Controller for CUCM and MR peripheral are moved under Sub Customer Tenant.
Physical Interface Controller		** & ***	Physical Interface Controller for CUCM and MR peripheral are moved under Sub Customer Tenant.
Network VRU		**	Network VRU for Type10 and Type2 are given in Day1 configuration. Default, it is available under Unallocated Folder.
ECC Variable	*	**	ECC Variables are given in Day1 Configuration. Default, it is available under Unallocated Folder. and also the array size should be within the limitation

Parameters	Configuration done by Sub Customer	Configuration done by Service Provider	Notes
Network VRU Script	*	** & ***	Network VRU Script given in Day1 configuration. Default, it is available under Unallocated Folder. **Note** Since it is mapped to the customer definition "HCS for CC" in day1 config , this can be used by the subcustomer whose customer definition is HCS for CC. Sub customer user creates Network VRU Script specific to sub customer in his own Tenant.
Application Instance		** & ***	This item cannot be moved under any Tenant/folder, but service provider can create based on Customer request in AW
Media Class		**	
Media Routing Domain		**	Default MRDs given in Day1 Configuration. Default, it is available under Unallocated Folder.
Agent	*		
Agent Team	*		
Agent Desktop	*		

Parameters	Configuration done by Sub Customer	Configuration done by Service Provider	Notes
Call Type	*		
Department	*		
Dialed Number	*		
Enterprise Skill Group	*		
Label	*		Labels given in the day1 configuration will be imported under Unallocated folder. Service provider will map the label with Network VRU Type in the AW, based on Customer's request. For more information on how to map label to the network VRU Types, see Map Labels to the Network VRU Type, on page 38.
Person	*		
Precision Attribute	*		
Precision Queue	*		
Skill Group	*		
User Variable	*		
Outbound		***	All the Outbound configuration will be done in AW by the Service Provider and those configurations will be moved to Sub Customer Tenant.

Move Resource to Sub Customer Tenant

Procedure

Step 1 Log In to CCDM Portal with Tenant Administrator Credentials.

Step 2 Click the burger icon and select **Resource Manager** > **Unallocated** > **SCC Tenant Folder**.

Step 3 Click on the tree structure and select the parameters which should be move to sub customer Tenant.

Example:

Select Routing Client specific to sub-customer.

Step 4 Click on **Move** and select the **Sub Customer Tenant**.

Step 5 Click on **Save** and click on **OK**.

Repeat the steps for all the parameters that has to be moved under Sub Customer Tenant.

Map Labels to the Network VRU Type

Note This action will be performed by the Service Provider based on Sub Customer's request.

Procedure

Step 1 Login to AW machine.

Step 2 Navigate to **Configuration Manager -> Explore Tools -> Network VRU Explorer**.

Step 3 Click on **Retrieve** expand the **unassigned** tree structure.

Step 4 Right Click on the label that you want to map to Network VRU Type10.

Step 5 Click on **Cut** option.

Step 6 Select and right click the Network VRU Type 10 to which you want to map the label.

Step 7 Click on **paste** and Click on **Save**.

Associate Department with an Agent

Procedure

Step 1 Log in to CCDM portal.

Step 2 Click the burger icon.

Step 3 Select **Provisioning** > **Resource Manager**.

Step 4 Select the **Tenant** > **Agent**.

Step 5 Click on the tenant which we you want to associate to the department.

Step 6 Click **Advanced** tab.

Step 7 From **Department** drop-down list, select the required department.

Step 8 Click **Save**.

Naming Convention for the Resources in Small Contact Center Agent Deployment Model

This table describes the examples of the naming conventions to be followed for the resources in the small contact center agent deployment model.

Parameters	Sub Customer1	Sub Customer2
Dialed Numbers	Enterprise Name: 9220000001<RoutingClient> , Dialed Number String: 9220000001 OR Enterprise Name: PlayAgentGreeting<RoutingClient> Dialed Number String: PlayAgentGreeting	Enterprise Name: 9330000001<RoutingClient> , Dialed Number String: 9330000001 OR Enterprise Name: PlayAgentGreeting<RoutingClient> Dialed Number String: PlayAgentGreeting
Call Type	Enterprise Name: CT1Cust1	Enterprise Name: CT1Cust2
Agent	Enterprise Name: 10101010 LogIn Name: 10101010 Agent ID: 6001	Enterprise Name: 20202020 LogIn Name: 20202020 Agent ID: 6001
Skill Group	Enterprise Name: Skg1Cust1 Peripheral Number: 7001	Enterprise Name: Skg1Cust2 Peripheral Number: 7001
Network VRU Script	Enterprise Name: AgentGreetingCust1 VRU Script Name: PM,-a,,Cust1	Enterprise Name: AgentGreetingCust2 VRU Script Name: PM,-a,,Cust2
Network VRU Labels	Name: 9999500001 Label: 9999500001<RoutingClient>	Name: 9999500001 Label: 9999500001<RoutingClient>
Routing Script	Name: Script1	Name: Script1

Integration of Small Contact Center Agent Deployment for Partition Internet Script Editor with CCDM

Complete the following procedure in the sequence to configure CCDM to integrate with the Internet Script Editor.

Note These steps should be repeated for each sub customer.

- Configure Unified CCE Admin Workstation for Internet Script Editor, on page 32
- Create User
- Assign Permission to Sub-customer Tenant and User
- Install Internet Script Editor , on page 33
- Provision Routing Script Using Internet Script Editor

Configure IDP

- Configure Metadata Exchange to IDP, on page 40
- Add Identity Server on Hosted AD FS, on page 40
- Add the Claim Rules, on page 41
- Configure AD FS for Federated Scenario, on page 43

Configure Metadata Exchange to IDP

Procedure

Step 1 Open ICE tool.

Step 2 From the **Tool** drop-down list, select **System Properties**.

Step 3 Select **Global Properties** > **Login Authentication Configuration**.

Step 4 In the **AD FS Metadata URL** field, enter the metadata URL of the AD FS server.
https://<ADFSServer>/federationmetadata/2007-06/federationmetadata.xml

Step 5 From the **Enabled Login Types**, check the **ADFS Logins (adfs)** check box.

Step 6 Click **Save**.

Step 7 Open command prompt and perform `iisreset` in all CCDM servers.

Add Identity Server on Hosted AD FS

Follow the procedure to manually add the Unified CCDM identity server:

Procedure

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

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

Step 3 Select **Add Relying Party Trusts**, then click **Start**.

Step 4 Select **Enter data about the relying party manually**, then click **Next**.

Step 5 Enter the appropriate display name, then click **Next**.

Example:

Unified CCDM Identity Server

Step 6 Select **AD FS profile**, then click **Next**.

Step 7 In the **Configure Certificate** step, click **Next**.

Note Unified CCDM does not support an optional token encryption certificates.

Step 8 Check the **Enable support for the WS-Federation Passive protocol** check box.

Step 9 In the **Relying Party WS-Federation Passive Protocol URL** field, enter the following URL of identity server AD FS endpoint:

```
https://<CCDM web server fqdn name>/identity/adfs
```

Note The URL must use AD FS trusted SSL certificate.

Step 10 Click **Next**.

Step 11 In the **Relying party trust identifier** pane, enter the following URL of the identity server:

```
https://<CCDM web server fqdn name>/identity
```

Step 12 Click **Add**, then click **Next**.

Step 13 Do not configure multi-factor authentication settings for the relying party trust, then click **Next**.

Step 14 Select **Permit all user to access this relying trust party**, and click **Next**.

Step 15 Review the settings, click **Next** to add the relying party trust to the AD FS configuration database.

Note To edit claim rules immediately, check the **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes** check box.

Step 16 Click **Close**.

Step 17 Repeat the steps for each identity server.

Add the Claim Rules

Follow the procedure on Hosted AD FS to add the claim rules for Unified CCDM:

Procedure

Step 1 Select **Unified CCDM trust**, then click **Edit Claim Rules**.

Step 2 In the **Issuance Transform Rules** tab, click **Add Rule**.

Step 3 From the **Claim Rule Template** drop-down list, select **Send LDAP Attributes as Claims**, then click **Next**.

Step 4 Add the required claims individually.

Claim Rule Name	Store	LDAP Attribute	Outgoing Claim Type	Mandatory
AD: SID as NameID	Active Directory	objectSid (type directly)	Name ID	Yes
AD: UPN as Name	Active Directory	User-Principal-Name	Name	Yes
AD: GivenName	Active Directory	Given-Name	Given Name	Optional
AD: Surname	Active Directory	Surname	Surname	Optional
AD: Email	Active Directory	E-Mail-Addresses	E-Mail-Address	Optional

Important Name ID of each claim rule must be unique. Therefore, always use SID as Name ID.

Step 5 Click **Finish**.

Step 6 Click **Add Rule**, and select the **Transform an Incoming Claim** and complete the Add Transform Claim Wizard:

Claim Rule Name	Incoming Claim Type	Outgoing Claim Type	Mandatory
TFN: Windows Account Name as Name	Windows Account Name	Name	Yes

Step 7 After adding the claim rules, click **Finish**.

Automatic User Provisioning

This is an alternate procedure to provision users.

Procedure

Step 1 Select **Unified CCDM trust**, then click **Edit Claim Rules**.

Step 2 In the **Issuance Transform Rules** tab, click **Add Rule**.

Step 3 Select **Send Group Membership as a Claim** as the claim rule template, and click **Next**.

Step 4 Add the following additional claims rules:

Claim Rule Name	User's Group	Outgoing Claim Type	Outgoing Claim Value
AD: Role = Supervisor	<windows group>	Role	Supervisor
AD: Role = Advanced	<windows group>	Role	Advanced

Step 5 After adding the claim rules, click **Finish**.

Set up AD FS

Procedure

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

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

Step 3 Select **Active Directory** > **Edit Claim Rules**.

Step 4 In the **Edit Claim Rules for Active Directory** dialog box, click **Add Rule**.

Step 5 From the **Claim Rule Template** drop-down list, select **Send LDAP Attributes as Claims**, then click **Next**.

Step 6 In the **Claim Rule Name** field, enter the Pass-thru DN.

Step 7 From the **Attribute Store** drop-down list, select the **Active Directory**.

Step 8 Map the LDAP Attribute to the Ongoing Claim type.

In the **LDAP Attribute (Select or type or add more)** column, enter **`distinguishedname`**. In the **Ongoing Claim Type (Select or type or add more)** column, enter **`http://temp.org/claims/DistinguishedName`**.

Step 9 Click **Finsh** and **OK**, restart the server.

Map Tenants to AD FS

Procedure

Step 1 Select **Unified CCDM trust**, then click **Edit Claim Rules**.

Step 2 In the **Issuance Transform Rules** tab, click **Add Rule**.

Step 3 In the **Add Transform Claim Rule Wizard** window, select **Send Claims Using a Custom Rule**, then click **Next**.

Step 4 Enter the claim rule name.

Claim rule name format: `AD: Tenant(<TenantPath>)`

Step 5 Enter the following custom rule text.

```
c:[Type == "http://temp.org/claims/DistinguishedName", Value =~ "^.*()$"]
=> issue(Type = "http://egain.net/claims/identity/tenant", Value = "/");
```

Example:

```
c:[Type == "http://temp.org/claims/DistinguishedName", Value =~ "^.*()$"]
=> issue(Type = "http://egain.net/claims/identity/tenant", Value = "qacce");
```

Step 6 Click **Finish**.

Configure AD FS for Federated Scenario

Note Create the Federated trust between Hosted AD FS and Customer AD FS.

Add Claim Rules for Relying Party Trust

Note Add the claim rules for Relying Party Trust in Customer AD FS.

Procedure

Step 1 Select the Relying party trust at the Customer AD FS, then click **Edit Claim Rules**.

Step 2 In the **Issuance Transform Rules** tab, click **Add Rule**.

Step 3 From the **Claim Rule Template** drop-down list, select **Send LDAP Attributes as Claims**, then click **Next**.

Step 4 Add the required claims individually:

Claim Rule Name	Store	LDAP Attribute	Outgoing Claim Type	Mandatory
AD: SID as Primary SID	Active Directory	objectSid (type directly)	Primary SID	Yes
AD: UPN as Name	Active Directory	User-Principal-Name	Name	Yes

Claim Rule Name	Store	LDAP Attribute	Outgoing Claim Type	Mandatory
AD: GivenName	Active Directory	Given-Name	Given Name	Optional
AD: Surname	Active Directory	Surname	Surname	Optional
AD: Email	Active Directory	E-Mail-Addresses	E-Mail-Address	Optional

Important Name ID of each claim rule must be unique. Therefore, always use SID as Name ID.

Step 5 Click **Finish**.

Step 6 Add another rule, from the **Claim Rule Template** drop-down list, select **Pass Through or Filter an Incoming Claim**, then click **Next**.

Claim Rule Name	Incoming Claim Type	Select Pass through all claim values	Mandatory
AD: Windows Account Name	Windows account name	Yes	Yes

Step 7 After adding the claim rules, click **Finish**.

Automatic User Provisioning

This is an alternate procedure to provision users.

Procedure

Step 1 Select the Relying party trust at the Customer AD FS, then click **Edit Claim Rules**.

Step 2 In the **Issuance Transform Rules** tab, click **Add Rule**.

Step 3 Select **Send Group Membership as a Claim as the claim rule template**, and click **Next**.

Step 4 Add the following claims rules:

Claim Rule Name	User's Group	Outgoing Claim Type	Outgoing Claim Value
AD: Role = Supervisor	<windows group>	Role	Supervisor
AD: Role = Advanced	<windows group>	Role	Advanced

Step 5 After adding the claim rules, click **Finish**.

Add Claim Rules for Claim Provider Trust

Note Add the claim rules for Claim Provider Trust in Hosted AD FS.

Procedure

Step 1 Select the Claims provider trust at the Hosted AD FS, then click **Edit Claim Rules**.

Step 2 In the **Acceptance Transform Rules** tab, click **Add Rule**.

Step 3 In the **The Add Transform Claim Rule Wizard** window, select **Pass Through or Filter an Incoming Claim**, then click **Next**.

Step 4 Add the required claim rule individually:

Claim Rule Name	Incoming Claim Type	Select Pass through all claim values	Mandatory
SID	Primary SID	Yes	Yes
Name	Name	Yes	Yes
GivenName	Given Name	Yes	Optional
Surname	Surname	Yes	Optional
EmailAddress	E-Mail-Address	Yes	Optional
Windows Account Name	Windows account name	Yes	Optional
Name ID	Name ID	Yes	Optional

Important
- Name ID of each claim rule must be unique. Therefore, always use SID as Name ID.
- For the Windows account name claim, select **Pass through only claim values that start with a specific value**.

Step 5 Once the claims have been set up, click **Finish**.

Automatic User Provisioning

This is an alternate procedure to provision users.

Procedure

Step 1 Select the Claims provider trust at the Hosted AD FS, then click **Edit Claim Rules**.

Step 2 In the **Acceptance Transform Rules** tab, click **Add Rule**.

Step 3 In the **The Add Transform Claim Rule Wizard** window, select **Pass Through or Filter an Incoming Claim**, then click **Next**.

Step 4 Add the following claims rules:

Claim Rule Name	Incoming Claim Type	Select Pass through only a specific claim value	Incoming Claim Value
Role = Advanced	Role	Yes	Advanced

Claim Rule Name	Incoming Claim Type	Select Pass through only a specific claim value	Incoming Claim Value
Role = Supervisor	Role	Yes	Supervisor

Step 5 Create custom rule, select **Send Claims Using a Custom Rule** as the claim rule template, then click **Next**.

- Enter the claim rule name.
- Enter the Custom Rule in the following format:

```
=> issue(Type = "http://egain.net/claims/identity/tenant", Value = "/<tenantname>",
Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"]
 = "urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified");
```

Step 6 After adding the claim rules, click **Finish**.

Add Pass through Claims

Note Add the claim rules for Relying Party Trust in Hosted AD FS.

Procedure

Step 1 Select the Relying party trust at the Hosted AD FS, then click **Edit Claim Rules**.

Step 2 In the **Issuance Transform Rules** tab, click **Add Rule**.

Step 3 In the **The Add Transform Claim Rule Wizard** window, select **Transform an Incoming Claim**, then click **Next**.

Step 4 Add the required claim rule individually:

Claim Rule Name	Incoming Claim Type	Outgoing Claim Type	Mandatory
Federation: Transform Primary SID as Name ID	Primary SID	Name ID	Yes

Step 5 In the **The Add Transform Claim Rule Wizard** window, select **Pass Through or Filter an Incoming Claim**, then click **Next**.

Step 6 Add the required claim rule individually:

Claim Rule Name	Incoming Claim Type	Select Pass through all claim values	Mandatory
Name	Name	Yes	Yes
GivenName	Given Name	Yes	Optional
Surname	Surname	Yes	Optional

Claim Rule Name	Incoming Claim Type	Select Pass through all claim values	Mandatory
EmailAddress	E-Mail-Address	Yes	Optional
Windows Account Name	Windows account name	Yes	Optional
Name ID	Name ID	Yes	Optional

Important
- Name ID of each claim rule must be unique. Therefore, always use SID as Name ID.
- For the Windows account name claim, select **Pass through only claim values that start with a specific value**.

Step 7 After the claims have been set up, click **Finish**.

Automatic User Provisioning

This is an alternate procedure to provision users.

Procedure

Step 1 Select the Relying party trust at the Hosted AD FS, then click **Edit Claim Rules**.

Step 2 In the **Issuance Transform Rules** tab, click **Add Rule**.

Step 3 In the **The Add Transform Claim Rule Wizard** window, select **Pass Through or Filter an Incoming Claim**, then click **Next**.

Step 4 Add the following claims rules:

Claim Rule Name	Incoming Claim Type	Pass through any specific claim value	Incoming Claim Value
Role = Advanced	Role	Yes	Advanced
Role = Supervisor	Role	Yes	Supervisor

Step 5 Create custom rule, select **Send Claims Using a Custom Rule** as the claim rule template, then click **Next**.
- Enter the claim rule name.
- Enter the Custom Rule in the following format:

```
c:[Type == "http://egain.net/claims/identity/tenant"]=> issue(claim = c);
```

Step 6 After adding the claim rules, click **Finish**.

Cisco UCDM Integration

Basic Configuration of Unified Communication Domain Manager

- Add Customer, on page 48
- Setup Cisco Unified Communication Manager Servers, on page 48
- Configure Network Device List, on page 49
- Add Site, on page 50
- Add Customer Dial Plan, on page 50
- Add Site Dial Plan, on page 50

Add Customer

Procedure

Step 1 Log in to Cisco Unified Communications Domain Manager as provider or reseller admin.

Step 2 Ensure that hierarchy path is set to appropriate level.

Note You can add customers under both provider and reseller. To add a customer under provider you must login as provider. To add customer under reseller you can login as either provider or reseller.

Step 3 Navigate to **Customer Management** > **Customer**.

Step 4 Provide necessary details in the following:

a) Enter **Name**.
b) Enter **Description**.
c) Enter **Domain Name**.
d) Check **Create Local Admin** check box.
e) Keep the default values for **Clone Admin role** and **Default Admin Role**.
f) Enter **Default Admin** password and confirm in **Confirm** password text box.

Step 5 Click **Save**.

Note If you want to delete customer and retain Unified Communication Manager configurations, see Disassociate Unified Communication Manager from UCDM.

Setup Cisco Unified Communication Manager Servers

Procedure

Step 1 Log in to Cisco Unified Communications Domain Manager as provider or reseller or customer admin.

Step 2 Ensure that hierarchy path is set to appropriate level.

Note Shared instances should be created at provider or reseller level and dedicated instances should be created at customer level.

Step 3 Navigate to **Device Management** > **CUCM** > **Servers**.

Step 4 Click **Add**.

Step 5 Enter **CUCM Server Name**.

Step 6 Check **Publisher** check box to configure publisher node.

Step 7 Enter **Cluster Name**.

Note Uncheck **Publisher** check box, choose **Cluster Name** from the drop-down list to integrate subscriber node.

Step 8 In **Network Address** tab:

a) Choose **Service_Provider_Space** from **Address Space** drop-down list.
b) Enter IP address of CUCM in **IPV4 Address** field.
c) Enter **Hostname**, default hostname is CUCM Server name.
d) Enter **Domain**.
e) Enter **description**.

Step 9 In **Credentials** tab:

a) Choose **Admin** from **Credential Type** drop-down list.
b) Enter CUCM user ID in **User ID** text box.
c) Enter CUCM password in **Password** text box.
d) Choose appropriate access type from **Access Type** drop-down list.
e) Enter **description**.

Step 10 Click **Save**.

Configure Network Device List

Procedure

Step 1 Login to Cisco Unified Communications Domain Manager as a provider or reseller admin.

Step 2 Navigate to **Customer Management** > **Network Device Lists**. Choose a particular customer from hierarchy tree.

Step 3 Click **Add**.

Step 4 Enter **Network Device List Name**.

Step 5 Enter **Description** for Network Device List.

Step 6 Default, IP address of HCM-F is selected from **Cisco HCM-F** drop-down list.

Step 7 Expand **Cisco Unified CM** tab and choose **cisco unified communication manager** instance from the drop-down list.

Step 8 Click **Save**.

Add Site

Procedure

Step 1 Log in to Cisco Unified Communications Domain Manager as a Provider, Reseller, or, Customer admin.

Step 2 Ensure that hierarchy path is set to appropriate level.

Step 3 Navigate to **Site Management** > **Sites**.

Step 4 Click **Add**.

Step 5 Provide necessary details in the following:

a) Enter **Site Name**.
b) Enter **Description**.
c) Check **Create Local Admin** check box.
d) Enter **Default Admin Password** and confirm in **Confirm Password** text box.
e) Choose **Country** from drop-down list.
f) Choose **Network Device List** from the drop-down list.

Step 6 Click **Save**.

Note In dedicated options for Small Contact Centers, one customer and a site per customer is created in UCDM for each sub-customer. In shared options for Small Contact Centers, one customer and a site in UCDM are shared across multiple sub-customers.

Add Customer Dial Plan

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer.

Step 2 Ensure that hierarchy is set to appropriate customer level.

Step 3 Navigate to **Dial Plan Management** > **Customer** > **Dial Plan**.

Step 4 Click **Add**.

Step 5 Click **Save**.

Note
- Customer ID is Unique, auto-generated, read-only number allocated to the customer
- If Site Location Code is not specified, by default Dial Plan Type will set to Type_4

Add Site Dial Plan

Before you begin

Ensure Customer Dial Plan is created, see Add Customer Dial Plan, on page 50.

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer.

Step 2 Ensure that hierarchy is set to appropriate site.

Step 3 Navigate to **Dial Plan Management** > **Site** > **Management**.

Step 4 Click **Add**.

Step 5 Enter **Extension Length** value, it ranges from 1 - 11.

Step 6 Click **Save**.

Site information is loaded in to Cisco Unified Communication Manager, it can be identified using Customer ID and Site ID in its prefix.

Note This step takes few minutes to provision the site dial plan.

ASA Integration

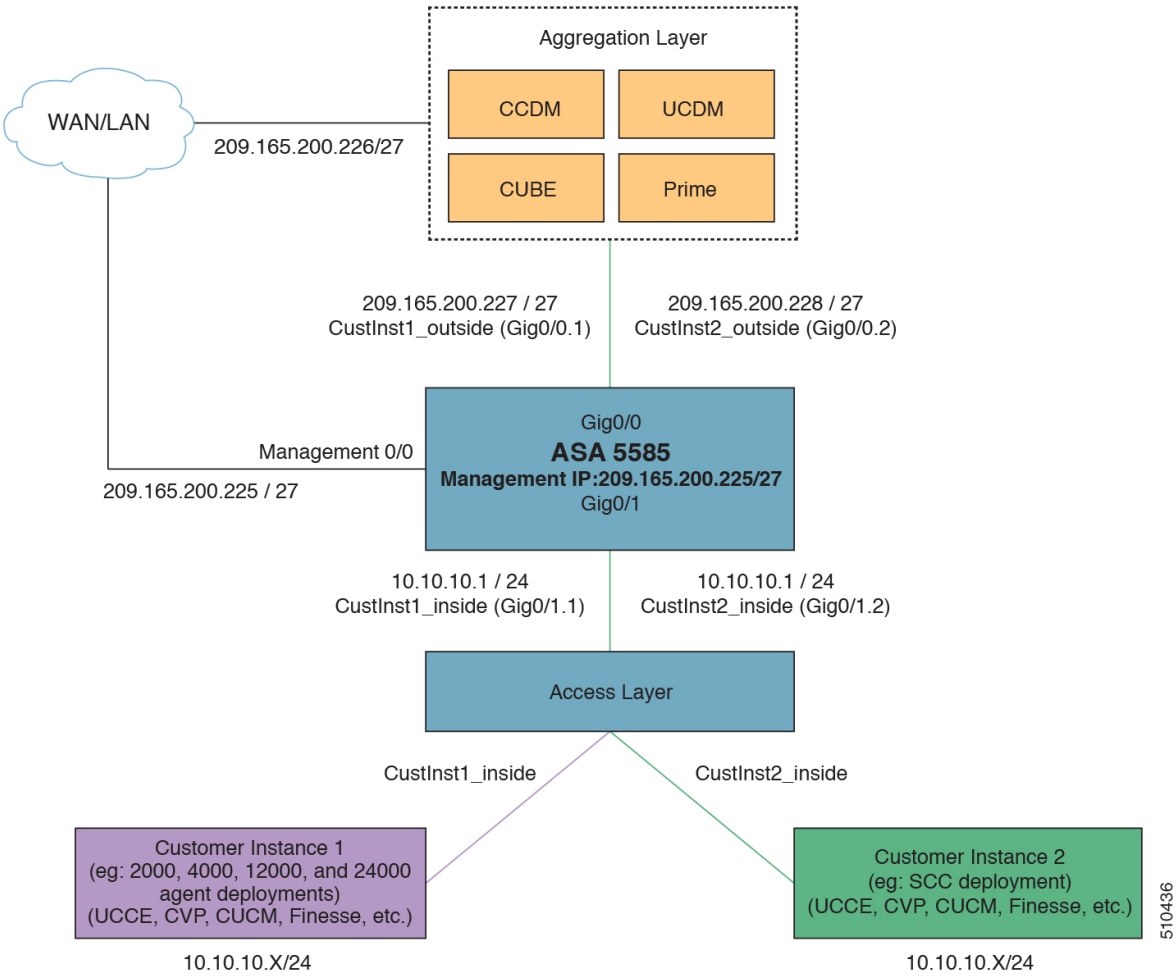
This section covers the configuration procedures required in Cisco ASA to integrate the customer instances for all types of HCS for CC deployment.

- Integration of ASA for HCS for CC Deployment model, on page 51
- Integration of ASA for Small Contact Center Deployment Model, on page 55

Integration of ASA for HCS for CC Deployment model

For the 2000, 4000, 12000, and 24000 agent deployment models the following configuration in Cisco ASA is required to integrate the customer instance components with the shared components. The following figure illustrates the deployment of different types with a Single ASA.

Figure 1: Customer Instances of Two Different Deployment Types Integrated with Shared Components



Repeat the Below procedures to integrate ASA for each customer instance. Required VLAN ID's and sub-interface ID for each customer instances will be different. Hence, IP addresses can be reused for these deployments:

- Configure Interfaces in the System Execution Space, on page 52
- Configure Security Contexts, on page 53
- Configure Interfaces in the Customer Instance Context, on page 54
- Configure Access-list in the Customer Instance Context, on page 55

Configure Interfaces in the System Execution Space

Procedure

Step 1 Navigate to global configuration mode:

```
hostname/context_name#changeto system
hostname#configure terminal
hostname(config)#
```

Step 2 Navigate to the interface Gigabit Ethernet 0/1 and enter the following command:

```
hostname(config)#interface gigabitethernet 0/1
hostname(config-if)#no shut
```

Step 3 Navigate to the sub-interface and enter the following commands, to assign the sub-interface to the customer_instance context and vlan ID inside the customer_instance:

```
hostname(config-if)#interface GigabitEthernet0/1.X
hostname(config-if)#vlan x
hostname(config-if)#no shut

hostname(config-if)#interface GigabitEthernet0/0.X
hostname(config-if)#vlan x
hostname(config-if)#no shut
```

Step 4 Repeat the above steps to assign a sub interface for each Customer instance.

Example:

For 2000 agent customer instance:

```
hostname(config)#interface  Gigabit Ethernet 0/1
hostname(config-if)#no shut

hostname(config-if)#interface GigabitEthernet0/1.1
hostname(config-if)#vlan 2
hostname(config-if)#no shut

hostname(config-if)#interface GigabitEthernet0/0.1
hostname(config-if)#vlan 340
hostname(config-if)#no shut
```

For 4000 agent customer instance:

```
hostname(config-if)#interface GigabitEthernet0/1.2
hostname(config-if)#vlan 4
hostname(config-if)#no shut

hostname(config-if)#interface GigabitEthernet0/0.2
hostname(config-if)#vlan 341
hostname(config-if)#no shut
```

Configure Security Contexts

Procedure

Step 1 Create customer_instance context in System Execution Space:

```
hostname(config)#context customer_instance
```

Step 2 Configure the customer_instance context definitions:

```
hostname(config-ctx)#description customer_instance context (optional)
hostname(config-ctx)#allocate-interface GigabitEthernet0/1.1 cust_inside invisible
```

```
hostname(config-ctx)#allocate-interface GigabitEthernet0/0.1 cust_outside invisible
hostname(config-ctx)#config-url disk0:/ customer_instance.cfg
```

Configure Interfaces in the Customer Instance Context

Procedure

Step 1 Navigate to customer_instance context configure mode:

```
hostname#changeto context customer_instance
hostname/customer_instance#configure  terminal
hostname/customer_instance(config)#
```

Step 2 Configure the interfaces for customer instances:

a) Navigate to the interface cust_inside:

```
hostname/customer_instance(config)#interface gigabitethernet0/1.1
```

b) Specify the name to inside interface of the customer_instance context:

```
hostname/customer_instance(config-if)#nameif inside_if_name
```

c) Enter the IP address of customer_instance of inside interface

```
hostname/customer_instance(config-if)#ip address ip_address subnet_mask
```

d) Navigate to the interface cust_outside:

```
hostname/customer_instance(config-if)#interface gigabitethernet0/0.1
```

e) Specify the name to outside interface of the customer_instance context:

```
hostname/customer_instance(config-if)#nameif outside_if_name
```

f) Enter the IP address of customer_instance of outside interface:

```
hostname/customer_instance(config-if)#ip address ip_address subnet_mask
```

Example:

```
hostname#changeto context 2000deployment
hostname/2000deployment#configure terminal
hostname/2000deployment(config)#interface gigabitethernet0/1.1
hostname/2000deployment(config-if)#nameif inside
hostname/2000deployment(config-if)#ip address 10.10.10.1 255.255.255.0
hostname/2000deployment(config-if)#interface gigabitethernet0/0.1
hostname/2000deployment(config-if)#nameif outside
hostname/2000deployment(config-if)#ip address 209.165.200.227 255.255.255.224
hostname/2000deployment(config-if)#exit
hostname/2000deployment(config)#exit
hostname/2000deployment#changeto context 4000deployment
hostname/4000deployment#configure terminal
hostname/4000deployment(config)#interface gigabitethernet0/1.2
hostname/4000deployment(config-if)#nameif inside
hostname/4000deployment(config-if)#ip address 10.10.10.1 255.255.255.0
hostname/4000deployment(config-if)#interface gigabitethernet0/0.2
hostname/4000deployment(config-if)#nameif outside
hostname/4000deployment(config-if)#ip address 209.165.200.228 255.255.255.224
```

Configure Access-list in the Customer Instance Context

Configure the access-list to allow IP traffic. The access-list is applied to both outside and inside interfaces:

Procedure

Step 1 Create the access-list for both outside and inside IP traffic:

```
hostname/customer_instance(config)#access-list access_list_name_outside extended permit ip
 any any
hostname/customer_instance(config)#access-list access_list_name_inside extended permit ip
any any
```

Step 2 Apply the access-list for both outside and inside IP traffic:

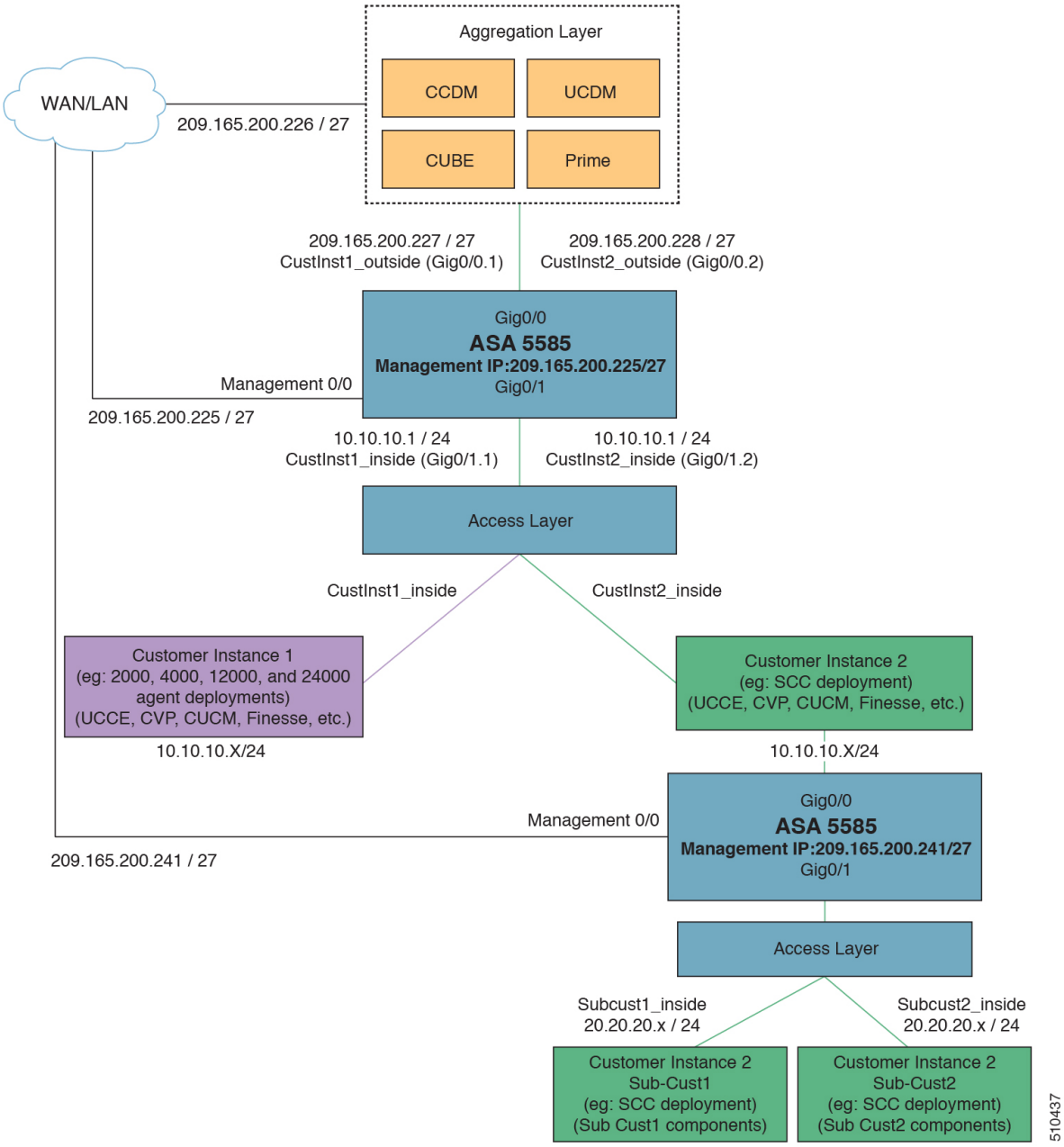
```
hostname/customer_instance(config)#access-group access_list_name_outside in interface
outside_if_name
hostname/customer_instance(config)#access-group access_list_name_inside in interface
inside_if_name
```

Note Allow or deny IP address in access-list as per the requirement of the network.

Integration of ASA for Small Contact Center Deployment Model

Small contact center deployment model requires two Cisco ASAs, one is to integrate the Small Contact Center customer instance with the shared components and another one is to integrate sub customer instances with the small contact center customer instance.

The following figure illustrates the deployments of 2000,4000, 12000, 24000 agents, and small contact center instances with two Cisco ASAs.



Integrate ASA for Small contact center with shared components, then Integrate ASA for Small contact center customer instance with sub-customer instance. For more information on installing and configuring ASA, for more information see *Install and Configure ASA Firewall and NAT* section of *Installing and upgrading guide for Cisco Hosted Collaboration Solution for Contact Center* http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html.

After Installing the ASA, repeat the below procedures for each sub-customer instance. Required VLAN ID's and sub-interface ID for sub-customer instances will be different. Hence, IP addresses can be reused for these deployments.

- Configure Interfaces in the System Execution Space, on page 57

• Configure Security Contexts for each Sub-customer Context, on page 58
• Configure Interfaces in each Sub-Customer Instance Context, on page 58
• Configure Access-list in the Sub-customer Instance Context, on page 59

Configure Interfaces in the System Execution Space

Procedure

Step 1 Navigate to global configuration mode:

```
hostname/context_name# changeto system
hostname# configure terminal
hostname(config)#
```

Step 2 Navigate to the interface Gigabit Ethernet 0/1 and enter the following command:

```
hostname(config)#interface gigabitethernet 0/1
hostname(config-if)#no shut
```

Step 3 Navigate to the sub-interface and enter the following commands, to assign the sub-interface to the sub-customer_instance context and vlan ID inside the sub-customer_instance:

```
hostname(config-if)#interface GigabitEthernet0/1.X
hostname(config-if)#vlan x
hostname(config-if)#no shut

hostname(config-if)#interface GigabitEthernet0/0.X
hostname(config-if)#vlan x
hostname(config-if)#no shut
```

Step 4 Repeat the above steps to assign a sub interface for each sub-customer instance.

Example:

For sub-cust1

```
hostname(config)#interface  gigabitethernet0/1
hostname(config-if)#No shut

hostname(config-if)#interface gigabitethernet0/1.1
hostname(config-if)#vlan 10
hostname(config-if)#no shut

hostname(config-if)#interface GigabitEthernet0/0.1
hostname(config-if)#vlan 11
hostname(config-if)#no shut
```

For sub-cust2

```
hostname(config-if)#interface gigabitethernet0/1.2
hostname(config-if)#vlan 20
hostname(config-if)#no shut

hostname(config-if)#interface gigabitethernet0/0.2
hostname(config-if)#vlan 21
hostname(config-if)#no shut
```

Configure Security Contexts for each Sub-customer Context

Procedure

Step 1 Create sub-customer_instance context in System Execution Space:

```
hostname(config)#context sub-customer_instance
```

Step 2 Configure the customer_instance context definitions:

```
hostname(config-ctx)#description sub-customer_instance context (optional)
hostname(config-ctx)#allocate-interface GigabitEthernet0/1.1 subcustX_inside invisible
hostname(config-ctx)#allocate-interface GigabitEthernet0/0.1 subcustX_outside invisible
hostname(config-ctx)#config-url disk0:/ sub-customer_instance.cfg
```

Example:

```
hostname/admin#changeto system
hostname#configure terminal
hostname(config)#context sub-cust1
hostname(config-ctx)#description sub-customer_1 context
hostname(config-ctx)#allocate-interface gigabitethernet0/1.1 sub-cust1_inside invisible
hostname(config-ctx)#allocate-interface gigabitethernet0/0.1 sub-cust1_outside invisible
hostname(config-ctx)#config-url disk0:/ sub-cust1.cfg
hostname(config-ctx)#context sub-cust2
hostname(config-ctx)#description sub-customer_2 context
hostname(config-ctx)#allocate-interface gigabitethernet0/1.2 sub-cust2_inside invisible
hostname(config-ctx)#allocate-interface gigabitethernet0/0.2 sub-cust2_outside invisible
hostname(config-ctx)#config-url disk0:/ sub-cust2.cfg
```

Configure Interfaces in each Sub-Customer Instance Context

Procedure

Step 1 Navigate to sub-customer_instance context configure mode:

```
hostname#changeto context sub_customer_instance_name
hostname/sub_customer_instance#configure  terminal
hostname/sub_customer_instance (config)#
```

Step 2 Configure the interfaces for sub-customer instances:

a) Navigate to the interface sub-cust_inside:

```
hostname/sub_customer_instance (config)#interface gigabitethernet0/1.1
```

b) Specify the name to inside interface of the sub-customer_instance context:

```
hostname/sub_customer_instance (config-if)#nameif inside_if_name
```

c) Enter the IP address of sub-customer_instance of inside interface

```
hostname/sub_customer_instance (config-if)#ip address ip_address subnet_mask
```

d) Navigate to the interface sub-cust_outside:

```
hostname/sub_customer_instance (config-if)#interface gigabitethernet0/0.1
```

e) Specify the name to outside interface of the sub-customer_instance context:

```
hostname/sub_customer_instance (config-if)#nameif outside_if_name
```

f) Enter the IP address of sub-customer_instance of outside interface:

```
hostname/sub_customer_instance (config-if)#ip address ip_address subnet_mask
```

Example:

```
hostname#changeto context sub-cust1
hostname/sub-cust1#configure terminal
hostname/sub_cust1(config)#interface sub-cust1_inside
hostname/sub_cust1(config-if)#nameif inside
hostname/sub_cust1(config-if)#ip address 20.20.20.1 255.255.255.0
hostname/sub_cust1(config-if)#interface sub-cust1_outside
hostname/sub_cust1(config-if)#nameif outside
hostname/sub_cust1(config-if)#ip address 10.10.10.254 255.255.255.0
hostname/sub_cust1(config)#interface sub-cust2_inside
hostname/sub_cust1(config-if)#nameif inside
hostname/sub_cust1(config-if)#ip address 20.20.20.1 255.255.255.0
hostname/sub_cust1(config-if)#interface sub-cust2_outside
hostname/sub_cust1(config-if)#nameif outside
hostname/sub_cust1(config-if)#ip address 10.10.10.254 255.255.255.0
```

Configure Access-list in the Sub-customer Instance Context

Configure the access-list to allow IP traffic. The access-list is applied to both outside and inside interfaces:

Procedure

Step 1 Create the access-list for both outside and inside IP traffic.

```
hostname/sub_customer_instance(config)#access-list access_list_name_outside extended permit
 ip any any
hostname/sub_customer_instance(config)#access-list access_list_name_inside extended permit
 ip any any
```

Step 2 Apply the access-list for both outside and inside IP traffic.

```
hostname/sub_customer_instance(config)#access-group access_list_name_outside in interface
outside_if_name
hostname/sub_customer_instance(config)#access-group access_list_name_inside in interface
inside_if_name
```

Note Allow or deny IP address in access-list as per the requirement of the network.

Session Border Controller Integration

For information on integrating CUBE Enterprise as the SBC in the aggregation layer, see Cisco Hosted Collaboration Solution - Deploying Multiple Virtual Forwarding (mVRF) using the Cisco Unified Border Element Enterprise Edition.

For information on integrating third-party Session Border Controller in the aggregation layer, see http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html

Cisco Prime Collaboration Assurance Integration for Small Contact Center Deployment Model

- Customer Management for Prime Collaboration Assurance, on page 60
- Add Cluster, on page 60
- Add Contact Center Components, on page 61

Customer Management for Prime Collaboration Assurance

Procedure

Step 1 Login to Prime using the URL *https://<IP_address_of_Prime_Collaboration_application/* .
Step 2 Go to **Administration** > **Customer Management**.
Step 3 Click **Add**.
Step 4 In **General Info** tab, enter the **Customer Name**.
Step 5 Click **Next** and then **Save**.

Add Cluster

Procedure

Step 1 Log into HCM-F using administrator credentials.
Step 2 Choose **Cluster Management** > **Cluster**, and click **Add New**.
Step 3 Enter the cluster name.
Step 4 Choose the customer from the drop-down list.
Step 5 Choose **CC** for the cluster type from the drop-down list.
Step 6 Choose the cluster application version from the drop-down list.
Step 7 Choose PCA as the host name from the Application Monitoring the Cluster drop-down list.
Step 8 Click **Save**.

Add Contact Center Components

Customer Contact components includes Rogger, AW-HDS, Agent Peripheral Gateway, VRU Peripheral Gateway, CVP, CVP OAMP, and CVP RSA.

Procedure

Step 1 Log in to HCM-F using administrator credentials.

Step 2 Choose **Application Management** > **Cluster Application**.

Step 3 In the **General Information** section, configure the following.

a) Click **Add New**.
b) Choose **UCCE** from the **Application Type** drop-down list.

Choose **CVP** for CVP, CVP OAMP, CVP RSA , choose **UCCE** for Rogger, AW-HDS, Agent Peripheral Gateway, or VRU Peripheral Gateway.

c) Enter the host name of the CC component.
d) Choose a cluster from the drop-down list.
e) Click **Save**.

Step 4 In the **Credentials** section, configure the following.

a) Click **Add New**.
b) Choose **SNMP _V2** from the **Credential Type** drop-down list.
c) Enter the **Community Srting** configured on CC Component.
d) Choose **Read Only** option for the access type.
e) Click **Save**.
f) Click **Add New**.
g) Choose **ADMIN** from the **Credential Type** drop-down list.
h) Enter the administrator credentials.

For CVP, CVP OAMP, CVP RSA use User ID as **`wsmadmin`** and password configured for OAMP web UI

i) Choose **Read Only** option for the Access Type .
j) Click **Save**.

Step 5 In **Network Addresses** section, configure the following.

a) Click **Add New**.
b) Choose **Application Space** from the **Network Space** drop-down list.
c) Enter the IPV4 Address and the hostname.
d) Click **Save**.
e) Click **Add New**.
f) Choose **Service Provider Space** from **Network Space** drop-down list.
g) Enter the NAT IPV4 Address and Hostname.
h) Click **Save**.

Note Follow the same procedure to add AW-HDS, Agent Peripheral Gateway,VRU Peripheral Gateway, CVP, CVP OAMP, and CVP RSA. Cisco Unified IC is not supported.