Common Upgrade Tasks

Upgrade Voice and Data Gateways

Perform the following procedure on each machine that hosts gateways that are used for TDM ingress, Outbound Option dialer egress, and VXML processing.

Procedure

Step 1 For VXML gateways only, perform this step. For all other gateways, proceed to the next step.

Run the `#copy tftp flash <IP Address> <filename>.bin` command to copy the flash from a remote machine to the gateway.

Step 2 Run the `#sh flash` command to check the version.

Step 3 Run the following commands in order:

a) `#conf t`

b) `#no boot system flash: <old image>`

c) `#boot system flash: <new image>`

d) `#wr`

e) `#reload`

Step 4 Run the `#sh version` command to verify that the new version shows in the gateway.

Bring Upgraded Side A into Service

After the Side A Unified CCE Logger, Call Router, and Administration & Data Server are upgraded, follow this procedure to bring Side A into service.

The logger and distributor services run with existing service logon account and is authorized by service security group in the domain. If you want to run logger and distributor services with local authorization, then you have to modify the service accounts using **Service Account Manager** Tool.

For more information on how to run Service Account Manager tool, see the *Staging Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Before you begin

If the External DBLookUp is configured update the External DBLookUp registry value using the CCEDataProtect Tool. For more information, see **Configure External DBLookUp Registry Value using CCEDataProtect Tool** procedure in the *Administration Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-maintenance-guides-list.html.

Note If the external remote database is on SQL Server 2017 version, you have to install the ODBC Driver 17 manually on the server hosting the external database. Download the ODBC Driver 17 from Microsoft.

Procedure

Step 1 Use Unified CCE Service Control to stop all Unified CCE services on the side B Call Router and Logger. However, before stopping Side B Router and Logger, also make sure that all non-upgraded Adminitration and Data Servers are stopped and shutdown, before starting the upgraded Side A Logger and Router servers.

Step 2 Manually start the Unified CCE services on the Side A Call Router and Logger, and the upgraded Administration & Data Server. Verify the following basic operations of the Side A Central Controller categories:

Category	Operation
General	• Setup logs indicate no errors or failure conditions. • AD domain has all users. • Schema upgrade is successful for all databases (no loss of data integrity or loss of data). • All component services start without errors. • Calls are successfully processed.
Call Router	• The Rtsvr logs indicate that the upgraded Administration & Data Server has connected successfully.

Category	Operation
Logger	• Recovery process that is not required, no activity other than process start up. • Users are in correct domain. • Configuration information is passed to Call Router. • Replication process begins when HDS comes online.
Administration & Data Server	• The updateAW process logs indicate that the Administration & Data Server is waiting for work. • Replication process begins with no errors.[1]
Security	• Specified users are able to use configuration manager.
Script Editor	• Previous settings for users are present when application is opened. • Validate All script yields the same results that the preupgrade test yielded. • You can open, edit, delete, or create new scripts.
ICMDBA	• Import or Export functionality is present. • Database space allocation and percent used are correct.

[1] During replication, data from Config_Message_Log table is replicated from Logger database to AW database. A purge mechanism is also introduced for Config_Message_Log table in AW Database. The default retention period is set to 90 days. To change the retention period, modify the following registry key:

```
Cisco Systems,
```

```
Inc.\ICM\<instancename>\Distributor\RealTimeDistributor
\CurrentVersion\Recovery\CurrentVersion\Purge\Retain\System\ConfigMessageLog
```

Step 3 Use Unified CCE Service Control to set the Unified CCE services to Automatic Start on each of the upgraded Unified CCE components.

Step 4 Verify production system operation while running with the upgraded Side A Call Router and Side A Logger.

Verify Operation of Upgraded Side B Call Router and Logger

Before you begin

The logger and distributor services that are run with existing service logon account and is authorized by service security group in the domain. If you want to run logger and distributor services with local authorization, then you have to modify the service accounts using Service Account Manager Tool.

For more information on how to run Service Account Manager tool, see the *Staging Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Procedure

Step 1 Before bringing Side B into service, manually synchronize Logger B to Logger A using ICMDBA.

Step 2 Start the Side B Call Router and Logger services.

As each node starts up, it searches for the other server components and attempts to register with them. If you completed the ICM-CCE-Installer and network testing successfully, no major errors should occur.

To verify whether a process is up, use the Diagnostic Framework Portico ListProcess option, available through the Unified CCE Tools shortcut that is created by the installer.

In order to add configuration data, the Central Controller, and Administration & Data Servers must be running.

Verify that the Unified CCE processes have no errors:

Category	Operation
Call Routers	• Router: Running and synchronized with peer. • Rtsvr: Indicates no connectivity to Administration & Data Server currently.
Loggers	• Logger: Connected to its respective database and synchronized with peer. MDS is in service. • Replication: No connectivity to Administration & Data Server HDS currently.

Step 3 To start the Unified CCE Distributor services, verify that the Unified CCE processes have no errors.

Category	Operation
Call Routers	• Router: Running and synchronized with peer. • CCAgent: In service, and without any errors. • Rtsvr: Feed activated to Administration & Data Server.
Loggers	• Logger: Connected to its respective database and synchronized with peer. MDS is in service. • Replication: Connected to the Administration & Data Server.
Administration & Data Server	• Updateaw: Displays "Waiting for new work." • Iseman: Listen thread waiting for client connection. (Exists only if Internet Script Editor is configured). • Replication: Replication and recovery client connection initialized. [2]

[2] **Note** During replication, data from Config_Message_Log table is replicated from Logger database to AW database. A purge mechanism is also introduced for Config_Message_Log table in AW Database. The default retention period is set to 90 days. To change the retention period, modify the following registry key:

```
Cisco Systems, Inc.\ICM\<instancename>\Distributor\RealTimeDistributor
\CurrentVersion\Recovery\CurrentVersion\Purge\Retain\System\ConfigMessageLog
```

Step 4 Validate the following settings from the system diagram for the Production Environment and make the required changes before you place the systems in production:

a) Clear event logs.
b) Remove any media from drives.
c) Ensure that all services are set to Manual Start. Services are not set to Automatic Start until after the implementation testing in the production environment.

Step 5 Verify overall system operation.

Step 6 Enable configuration changes.

a) Set the following registry key to 0 on the Side A and Side B Call Routers of the system: **HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\Router<A/B>\Router\CurrentVersion\Configuration\Global\DBMaintenance**.
b) Verify that configuration changes can be made.

Step 7 Upgrade any other Administration & Data Servers or HDSs using the steps that are documented in Migrate HDS Database and Upgrade Unified CCE Administration & Data Server.

Disable Outbound Options High Availability (If Applicable)

Before you begin

If Outbound Options High Availability is enabled, you must disable it on source machines before you perform the upgrade.

Before proceeding with the following steps, ensure that Outbound Options feature is in maintenance mode. There must not be any customer records getting imported to Outbound database. The outbound campaigns must not be active and outbound callflow must not be in progress.

Perform the following steps on Side A:

Procedure

Step 1 Launch **Websetup**. Navigate to **Component Management** > **Loggers**.

Step 2 Edit the **Logger** and navigate to **Additional Options**. Uncheck **Enable High Availability** under **Outbound Option** and click **Next**.

Step 3 Enable **Stop and then start(cycle) the Logger Service for this instance (if it is running)** checkbox . Click **Next** to complete the setup.

Step 4 Repeat similar steps (steps 1, 2, and 3) for side B.

What to do next

You can enable Outbound Options High Availability after the upgrade is successful.

Upgrade Cisco JTAPI Client on PG

If you upgrade Unified Communications Manager (Unified CM) in the contact center, also upgrade the JTAPI client that resides on the PG. To upgrade the JTAPI client, uninstall the old version of the client, restart the server, and reinstall a new version. You install the JTAPI client using the Unified Communications Manager Administration application.

To install the JTAPI client for the Unified CM release that you have upgraded to, see the Install Cisco JTAPI Client on PG topic.

Before you begin

Before you perform this procedure, you must:

- Uninstall the old JTAPI client from the Unified Communications Manager PG
- Restart the PG server.

Database Performance Enhancement

After you perform a Common Ground or a Technology Refresh upgrade, complete the procedures described in this section to enhance the performance of the database. This is a one-time process and must be run only on the Logger and AW-HDS databases during a maintenance window.

- Performance Enhancement of TempDB, on page 6 (You can skip this when performing a Technology Refresh upgrade)
- Performance Enhancement of Logger Database, on page 7
- Performance Enhancement of AW-HDS Database, on page 8

Performance Enhancement of TempDB

Perform this procedure on Logger, Rogger, AW-HDS-DDS, AW-HDS and HDS-DDS machines to get the benefits of TempDB features for SQL Server. For more information about the SQL Server TempDB Database and its use, see the Microsoft SQL Server documentation for TempDB Database.

Note This procedure applies to the Common Ground upgrade process only.

Note If the Performance Enhancement of TempDB procedure is already completed on 12.5(1), then do not repeat the same procedure upon upgrading to 12.5(2).

Procedure

Step 1 Use **Unified CCE Service Control** to stop the Logger and Distributor services.

Step 2 Login to **SQL Server Management Studio** and run the following queries on the primary database.

- To modify the existing TempDB Initial size to the recommended value:

```
ALTER DATABASE tempdb MODIFY FILE
   (NAME = 'tempdev', SIZE = 800, FILEGROWTH = 100)
ALTER DATABASE tempdb MODIFY FILE
   (NAME = 'templog', SIZE = 600, FILEGROWTH = 10%)
```

- To add multiple TempDB files:

```
USE [master];
GO
ALTER DATABASE [tempdb] ADD FILE (NAME = N'tempdev2', FILENAME = N'<SQL Server TempDB
path>' , SIZE = 800 , FILEGROWTH = 100);
ALTER DATABASE [tempdb] ADD FILE (NAME = N'tempdev3', FILENAME = N'<SQL Server TempDB
path>' , SIZE = 800 , FILEGROWTH = 100);
ALTER DATABASE [tempdb] ADD FILE (NAME = N'tempdev4', FILENAME = N'<SQL Server TempDB
path>' , SIZE = 800 , FILEGROWTH = 100);
GO
```

Note

- For example,

```
<SQL Server TempDB path> = C:\Program Files\Microsoft SQL
Server\MSSQL12.MSSQLSERVER\MSSQL\DATA\tempdev2.ndf
```

- Make sure that you modify the values in the query based on the machines. For more information, see Increase Database and Log File Size for TempDB.

Step 3 Restart the SQL Services.

Step 4 Start the Logger and Distributor services.

Performance Enhancement of Logger Database

Perform this procedure on Side A and Side B of the Logger database.

Procedure

Step 1 Use the Unified CCE Service Control to stop the Logger service.

Step 2 From the command prompt, run the **RunFF.bat** file which is located in the `<ICM install directory>:\icm\bin` directory.

Step 3 Proceed with the application of fill factor to Unified ICM databases.

Note: Based on the size of the database, it takes several minutes to several hours to apply fill factor to the database. For example, it takes anywhere between 2 to 3 hours for a 300-GB HDS. After the process is completed, the log file is stored in `<SystemDrive>:\temp\<DatabaseName>_Result.txt`.

Step 4 Use the Unified CCE Service Control to start the Logger service.

Troubleshooting Tips

See the `RunFF.bat/help` file for more information.

Performance Enhancement of AW-HDS Database

Procedure

Step 1 Use the Unified CCE Service Control to stop the Distributor service.

Step 2 From the command prompt, run the **RunFF.bat** file which is located in the `<ICM install directory>:\icm\bin` directory.

Step 3 Proceed with the application of fill factor to Unified ICM databases.

Note: Based on the size of the database, it takes several minutes to several hours to apply fill factor to the database. For example, it takes between 2 to 3 hours for a 300-GB HDS. After the process is completed, the log file is stored in `<SystemDrive>:\temp\<DatabaseName>_Result.txt`.

Step 4 Use the Unified CCE Service Control to start the Distributor service.

Troubleshooting Tips

See the `RunFF.bat/help` file for more information.

Improve Reporting Performance

To improve the performance of the reporting application, modify the following Windows settings on the database servers (AW-HDS, AW-HDS-DDS, HDS-DDS).

- Increase the Paging File Size to 1.5 times the server's memory.

  To change the Paging File Size, from the Control Panel search for Virtual Memory. In the Virtual Memory dialog box, select **Custom size**. Set both **Initial size** and **Maximum size** to 1.5 times the server memory.

- Set the server's **Power Options** to **High Performance**.

  From the Control Panel, select **Power Options**. By default, the **Balanced** plan is selected. Select **Show additional plans** and select **High performance**.

In SQL Server, disable **Auto Update Statistics** for AW and HDS databases.

In the SQL Server Management Studio, right-click the database name in the Object Explorer and select **Properties**. Select the **Options** page. In the **Automatic** section of the page, set **Auto Create Statistics** and **Auto Update Statistics** to **False**.

Reduce Reserved Unused Space for HDS and Logger

Enable trace flag 692 on HDS database server to reduce the growth of reserved unused space on the AW-HDS, AW-HDS-DDS, HDS-DDS database servers and Logger database, after you upgrade or migrate to Microsoft SQL 2017 or 2019. For more information about the trace flag 692, see the Microsoft Documentation.

Procedure

Run the following command to enable trace flag 692 on HDS database server and Logger database:

```
DBCC TRACEON (692, -1);
GO
```

Note An increase in the unused space may lead to unexpected purge trigger in HDS and Logger, trace flag 692 helps in mitigating this unexpected purge issue. After you enable the trace flag, there will be an increase of 10% to 15% CPU for a short duration. If the trace flag needs to be retained, the server startup options has to be updated using the -T(upper case) option. For more information, see https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/database-engine-service-startup-options?view=sql-server-ver15.

Update User Role

To update the User Role in the database for the existing users, do the following in any one of the AW (distributor) machines:

- Go to the link https://software.cisco.com/download/home/268439622/type and select User Role Update Bulk Tool from the list.
- Download the file UserRoleUpdateScript_1201.zip and extract it.
- Open Windows Powershell and run the script UserRoleUpdate.PS1.

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 11 2. Create Trusted CA-Signed Server or Application Certificate , on page 11 3. Upload and Bind CA-Signed Certificate, on page 13
Customer Voice Portal (CVP) Call Server/CVP Reporting Server[3]	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 20
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 20
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 20
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

[3] 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 21
  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 12.

- 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 12.

Import CA Certificate into AW Machines

Procedure

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

Step 2 Run the following command:

Important If you are not employing the 12.5(1a) installer or not having ES55 (mandatory OpenJDK ES), then use JAVA_HOME instead of CCE_JAVA_HOME.

```
cd %CCE_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 24.

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

- `cd %CCE_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[4], Rogger[5], PGs, and HDS)	Import CCE Component Certificates, on page 15 Import Diagnostic Framework Portico Certificate into AW Machines, on page 16
	Cisco Finesse	Import VOS Components Certificate, on page 17
	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 15
Rogger		

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

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):

Important If you are not employing the 12.5(1a) installer or not having ES55 (mandatory OpenJDK ES), then use JAVA_HOME instead of CCE_JAVA_HOME.

- `cd %CCE_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 24.

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:

Important If you are not employing the 12.5(1a) installer or not having ES55 (mandatory OpenJDK ES), then use JAVA_HOME instead of CCE_JAVA_HOME.

- `cd %CCE_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 24.

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):

Important If you are not employing the 12.5(1a) installer or not having ES55 (mandatory OpenJDK ES), then use JAVA_HOME instead of CCE_JAVA_HOME.

- `cd %CCE_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, AWDB, 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.

Note After the successful upgrade, the CAs that are unapproved by Cisco are removed from the platform trust store. You can add them back, if necessary.

- For information about the list of CAs that Cisco supports, see the Cisco Trusted External Root Bundle at https://www.cisco.com/security/pki.
- For information about adding a certificate, see Insert a new tomcat-trust certificate.

Related Topics

Export Self-Signed Live Data Certificates, on page 19
Import Self-Signed Live Data Certificates, on page 20
Set Up Certificates for Live Data
Set up Microsoft Certificate Server for Windows Server, on page 21

Self-Signed Certificates and Third-Party CA Certificates

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

On Server	Import Certificates From
Finesse	Live Data and Cisco Unified Intelligence Center
Live Data	AW Database Cisco Unified Intelligence Center
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.

Related Topics

Import Self-Signed Live Data Certificates, on page 20

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.

Related Topics

Export Self-Signed Live Data Certificates, on page 19

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.

Deploy Root Certificate for Browsers

In environments where group policies are enforced via the Active Directory domain, the root certificate can be added automatically to each user's browser. Adding the certificate automatically simplifies user requirements for configuration.

Note To avoid certificate warnings, each user must use the fully-qualified domain name (FQDN) of the Finesse server to access the desktop.

Procedure

Step 1 On the Windows domain controller, navigate to **Administrative Tools** > **Group Policy Management**.

Note Users who have strict Group Policy defined on the Finesse Agent Desktop are required to disable **Cross Document Messaging** from **Group Policy Management** to ensure proper functioning of Finesse on browser.

Step 2 Right-click Default Domain Policy and select **Edit**.

Step 3 In the Group Policy Management Console, go to **Computer Configuration** > **Policies** > **Window Settings** > **Security Settings** > **Public Key Policies**.

Step 4 Right-click Trusted Root Certification Authorities and select **Import**.

Step 5 Import the *ca_name*.cer file.

Step 6 Go to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies** > **Certificate Services Client - Auto-Enrollment**.

Step 7 From the Configuration Model list, select **Enabled**.

Step 8 Sign in as a user on a computer that is part of the domain and open browser.

Step 9 If the user does not have the certificate, run the command **gpupdate.exe /target:computer /force** on the user's computer.

Set Up CA Certificate for Internet Explorer Browser

After obtaining and uploading the CA certificates, either the certificate must be automatically installed via group policy or all users must accept the certificate.

In environments where users do not log directly in to a domain or group policies are not utilized, every Internet Explorer user in the system must perform the following steps once to accept the certificate.

Procedure

Step 1 In Windows Explorer, double-click the *ca_name*.cer file (in which *ca_name* is the name of your certificate) and then click **Open**.

Step 2 Click **Install Certificate** > **Next** > **Place all certificates in the following store**.

Step 3 Click **Browse** and select **Trusted Root Certification Authorities**.

Step 4 Click **OK**.

Step 5 Click **Next**.

Step 6 Click **Finish**.

A message appears that states you are about to install a certificate from a certification authority (CA).

Step 7 Click **Yes**.

A message appears that states the import was successful.

Step 8 To verify the certificate was installed, open Internet Explorer. From the browser menu, select **Tools** > **Internet Options**.

Step 9 Click the **Content** tab.

Step 10 Click **Certificates**.

Step 11 Click the **Trusted Root Certification Authorities** tab.

Step 12 Ensure that the new certificate appears in the list.

Step 13 Restart the browser for certificate installation to take effect.

Note If using Internet Explorer 11, you may receive a prompt to accept the certificate even if signed by private CA.

Set Up CA Certificate for Firefox Browser

Every Firefox user in the system must perform the following steps once to accept the certificate.

Note To avoid certificate warnings, each user must use the fully-qualified domain name (FQDN) of the Finesse server to access the desktop.

Procedure

Step 1 From the Firefox browser menu, select **Options**.

Step 2 Click **Advanced**.

Step 3 Click the **Certificates** tab.

Step 4 Click **View Certificates**.

Step 5 Click **Authorities**.

Step 6 Click **Import** and browse to the *ca_name*.cer file (in which *ca_name* is the name of your certificate).

Step 7 Check the **Validate Identical Certificates** check box.

Step 8 Restart the browser for certificate installation to take effect.

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:

Important If you are not employing the 12.5(1a) installer or not having ES55 (mandatory OpenJDK ES), then use JAVA_HOME instead of CCE_JAVA_HOME.

```
cd %CCE_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>
```