Integrate ECE with PCCE in Version 12.0 and Higher

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Terminology

Prerequisite Steps

Integration Steps

- Step 1. Configure SSL Certificates
  - Step 1.1. Generate a Certificate
  - Step 1.2. Bind Certificate to Website
- Step 2. Configure Partition Administrator SSO
  - Step 2.1. Obtain Active Directory (AD) Certificate and Create Keystore.
  - Step 2.2. Configure ECE with AD Lightweight Directory Access Protocol (LDAP) Access Information.
- Step 3. Validate Configuration File
- Step 4. Add ECE to PCCE Inventory
  - Step 4.1. Upload ECE Web Server Certificate to the Java Keystore
  - Step 4.2. Add the ECE Data Server to Inventory
  - Step 4.3. Add the ECE Web Server to Inventory
- Step 5. Integrate ECE with PCCE
- Step 6. Validate ECE Integration

Troubleshoot

- File Names and Locations on ECE
- File Names and Locations on PCCE
- Trace Level Configuration
- Log File Collection

Related Information

Introduction

This document describes the steps to integrate Enterprise Chat and Email (ECE) with Packaged Contact Center Enterprise (PCCE) in versions 12.0 and higher

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Enterprise Chat and Email (ECE) 12.x
- Packaged Contact Center Enterprise (PCCE) 12.x

Components Used

The information in this document is based on these software versions:

- ECE 12.5(1)
- PCCE 12.5(1)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

PCCE version 12.0 introduced a new management interface known as the Single Pane of Glass (SPOG). Almost all management of the contact center and related applications is now performed in this interface. In order to properly integrate both ECE and PCCE you must complete several steps that are unique to this integration. This document guides you through this process.

Terminology

Throughout this document, these terms are used.

- Enterprise Chat and Email (ECE) – ECE is a product that allows email and chat requests to be routed to contact center agents in the same way that voice calls are.
- Single Pane of Glass (SPOG) – SPOG is the way that PCCE Administration is done in version 12.0 and higher. SPOG is a complete rewrite of the CCE Administration tool that was used in versions prior to 12.0.
- Certificate Authority (CA) – An entity that issues digital certificates in accordance with a public key infrastructure (PKI) model.

  There are two types of CAs that you can encounter.

  - Public CA – A public CA is one that has its root and intermediate certificates included with most browsers and operating systems. Some common Public CAs include, IdenTrust, DigiCert, GoDaddy, and GlobalSign.
  - Private CA – A private CA is one that exists inside of a company. Some private CAs are signed by public CAs, but most often these are standalone CAs and the certificates that they issue are only trusted by computers in that organization.

  Within either of the two CA types, there are two types of CA servers.

  - Root CA Server – The root CA server signs its own certificate. In the standard, multi-tier PKI deployment, the Root CA is offline and inaccessible. The Root CA in this model also only issues certificates to another CA server known as an Intermediate CA. Some companies choose to use only a single-tier CA. In this model, the Root CA issues certificates intended for use by an entity other than another CA server.
  - Intermediate CA Server – The intermediate or Issuing CA server issues certificates intended for use by an entity other than another CA server.
- Microsoft Management Console (MMC) – An application included with Microsoft Windows that

allows various snap-ins to be loaded. You can use the snap-ins to build a customized console for server administration. There are many different snap-ins included with Windows. A short list of examples include Certificates, Device Manager, Disk Management, Event Viewer, and Services.

- Network Load Balancer (NLB) – A device or application that presents multiple physical resources to end-users with a common physical name. NLBs are very common with web applications and services. NLBs can be implemented in many ways. When used with ECE, the NLB must be configured in a way that ensures user sessions return to the same physical back-end web server by use of cookie-insert or an equivalent method. This is referred to as a sticky session with cookie-insert. Sticky session simply refers to a load balancer's ability to return a user's session to the same physical back-end server for all interactions.
    - Secure Sockets Layer (SSL) Passthrough – SSL passthrough is a method in which the SSL session exists between the end-user device and physical web server where the user's session was assigned. SSL passthrough does not allow cookie-insert as the HTTP session is physically encrypted at all times. Most NLBs support sticky session with SSL Passthrough by use of stick tables which monitor the serverhello and clienthello portion of the session setup and store the unique values in a table. When the next request that matches these values is presented to the NLB, the stick table can be used to return the session to the same back-end server.
    - SSL Offload – When an NLB is configured for SSL offload, there are two SSL sessions or tunnels that exist for any given end-user session. The first is between the end-user device and the virtual IP (VIP) configured on the NLB for the web site. The second is between the back-end IP of the NLB and the physical web server where the user's session is assigned. SSL offload does support cookie-insert as the HTTP stream is fully decrypted while on the NLB where additional HTTP cookies can be inserted and session inspection can be performed. SSL offload is often used when the web application does not require SSL but is instead done for security. The current versions of ECE do not support access to the application in a non-SSL session.

Prerequisite Steps

There are several prerequisites that must be completed before you start to integrate the two systems.

- Minimum PCCE Patch Level
    - Version 12.0(1) – ES37
    - Version 12.5(1) – No current minimum for base functionality
- Minimum ECE Patch Level

  It is recommended that ECE run latest Engineering Special (ES) available.

    - Version 12.0(1) – ES3 + ES3_ET1a
    - Version 12.5(1) – No current minimum for base functionality
- Configuration Items

  Ensure that you associate the ECE_Email, ECE_Chat, and ECE_Outbound Media Routing Domains (MRDs) with the correct Application Instance.

    - For the PCCE 2000 Agent deployment model, the Application Instance is MultiChannel and is preconfigured when PCCE is deployed.
    - For the PCCE 4000/12000 Agent deployment model, the Application Instance can be any name and must be created by whoever is performing the integration. The best practice is to use the form of {site}_{peripheral_set}_{application_instance}.
      If you installed PCCE with the site name as Main, peripheral set as PS1, and application instance as Multichannel, then the Application Instance name is Main_PS1_Multichannel.

Note: The Application Instance name is case sensitive. Ensure that you type the name correctly

when you add the ECE Web Server to Inventory.

Integration Steps

The details for all steps in this document are all covered in the documentation for both ECE and PCCE, but they are not shown in a list nor are they all in the same document. See the links included at the end of this document to for additional details.

Step 1. Configure SSL Certificates

You must generate a certificate to be used by the ECE web server. You can use a self-signed certificate, but it is often easier to use a CA-signed certificate. Self-signed certificates are no less secure than CA-signed certificates, there are fewer steps to initially create the certificate, but when the certificate needs to be replaced, you must remember to upload the new certificate to the Java keystores on all PCCE Administration Data Servers. If you use a CA-signed certificate, you only need to upload the root and, if present, intermediate certificates to the keystores.

If you have multiple web servers in your deployment, you must review these guidelines. The specific steps required to configure a network loadbalancer are outside of the scope of this document. Please contact your load balancer vendor for assistance if required.

- While not required, a load balancer greatly simplifies the implementation
- Access to the ECE application on each web server must use SSL regardless of the load balancer method used
- The load balancer can be configured either as SSL passthrough or SSL offload
- If SSL passthrough is chosen:
  - You must perform all certificate operations from one server
  - Once the certificate is properly configured, you must export the certificate and ensure that the private key is included to a personal information exchange (PFX) file
  - You must copy the PFX file to all other web servers in the deployment, then import the certificate into IIS
- If SSL offload is chosen, each web server can be configured with their own individual SSL certificate

Note: If you have multiple web servers and choose SSL passthrough on your web server, or if you wish to have a common certificate on all servers, you must choose one web server to perform step 1 on, then import the certificate to all other web servers.
If you choose SSL offload, then you must perform these steps on all web servers. You must also generate a certificate to use on your load balancer.

Step 1.1. Generate a Certificate

You can skip this section if you have already created or obtained a certificate, otherwise choose one of the two options.

Option 1. Use a Self-signed Certificate

1. Navigate to IIS Administration.
2. Select the server name in the Connections tree on the left.

3. Locate **Server Certificates** in the center pane and double-click to open it.
4. Select **Create Self-Signed Certificate...** from the Actions pane on the right.
5. In the **Create Self-Signed Certificate** window, choose and enter a name in the **Specify a friendly name for the certificate:** box. This name is how the certificate appears in the selection process in the next major step. This name does not need to match the common name of the certificate and does not affect how the certificate appears to the end user.
6. Ensure that **Personal** is selected in the **Select a certificate store for the new certificate:** drop-down box.
7. Select **OK** to create the certificate.
8. Proceed to the next major step, **Bind certificate to website**.

Option 2. Use a CA-signed Certificate

CA-signed certificates require that you generate a Certificate Signing Request (CSR). The CSR is a text file that is then sent to the CA where it is signed and then the signed certificate along with the required CA certificates are returned and the CSR fulfilled. You can choose to do this through IIS Administration or through the Microsoft Management Console (MMC). The IIS Administration method is much easier with no special knowledge required but only allows you to configure the fields that are included in the certificate's Subject attribute and change the bit length. MMC requires additional steps and that you possess a thorough knowledge of all the fields required in a valid CSR. It is strongly recommended that you use MMC only if you have moderate to expert experience with certificates creation and management. If your deployment requires ECE to be accessed by more than one fully-qualified name or if you are required to change any part of the certificate except the subject and bit length, you must use the MMC method.

1. Via IIS Administration

   Use these steps to generate a Certificate Signing Request (CSR) through IIS Manager.

   1. Navigate to IIS Administration.
   2. Select the server name in the Connections tree on the left.
   3. Locate **Server Certificates** in the centre pane and double-click to open it.
   4. Select **Create Certificate Request...** from the Actions pane on the right. The **Request Certificate** wizard appears.
   5. On the **Distinguished Name Properties** page, enter the values in the form for your system. All fields must be entered. Select **Next** to continue.
   6. On the **Cryptographic Service Provider Properties** page, leave the default selection for **Cryptographic service provider:**. Change the **Bit length:** drop-down to a minimum of **2048**. Select **Next** to continue.
   7. On the **File Name** page, select a place where you wish to save the CSR file.
   8. Provide the file to the CA. When you have received the signed certificate, copy it to the web server and proceed to the next step.
   9. In the same location in IIS Manager, select **Complete Certificate Request** in the **Actions** pane. The wizard appears.
   10. On the **Specify Certificate Authority Response** page, choose the certificate provided by your CA. Give a name in the **Friendly name** box. This name is how the certificate appears in the selection process in the next major step. Ensure that the **Select a certificate store for the new certificate:** drop-down is set to **Personal**.
   11. Select **OK** to complete the certificate upload.
   12. Proceed to the next major step, **Bind certificate to website**.
2. Via Microsoft Management Console (MMC)

   Use these steps to generate a CSR through MMC. This method allows you to customize every aspect of the CSR.

1. Right-click the Start button and select Run.
2. Type **mmc** in the run box and select **OK**.
3. Add the Certificate snap-in to the MMC window.
    1. Select **File**, then **Add/Remove Snap-in...**. The **Add or Remove Snap-ins** box appears.
    2. In the list on the left, locate **Certificates**, and select **Add >**. The Certificates snap-in box appears.
    3. Select the option **Computer account** then select **Next >**.
    4. Ensure that **Local computer: (the computer this console is on)** is selected on the **Select Computer** page, then select **Finish**.
    5. Select **OK** to close the **Add or Remove Snap-ins** box.
4. Generate the CSR
    1. In the left pane, expand **Certificates (Local Computer)** then **Personal** and select the **Certificates** folder.
    2. Right-click the **Certificates** folder and navigate to **All Tasks > Advanced Operations >** then select **Create Custom Request...**. The **Certificate Enrollment** wizard appears.
    3. Select **Next** on the introduction screen.
    4. On the **Select Certificate Enrollment Policy** page, select **Proceed without enrollment policy**, listed under **Custom Request**, then select **Next**.
    5. On the **Custom request** page, ensure that the **Template** selected is **(No template) CNG key**, and the **Request format** is proper for your CA. **PKCS #10** does work with the Microsoft CA. Select **Next** to proceed to the next page.
    6. On the **Certificate Information** page, select the drop-down beside the word **Details**, then select the **Properties** button. The **Certificate Properties** form appears.
    7. It is beyond the scope of this document to give all options for the **Certificate Properties** form. Please reference Microsoft documentation for details. Here are a few notes and tips on this form.
        - Ensure that you populate all required values in the **Subject name:** section of the **Subject:** tab
        - Ensure that the value provided for **Common name** is also provided in the **Alternative name:** section
        - Set the **Type:** to **DNS**, type the URL into the **Value:** box, then select the **Add >** button
        - If you wish to use several URLs to access ECE, provide each alternate name in this same field and select **Add >** after each
        - Ensure that you set the **Key size** on the **Private Key** tab to a value greater than 1024.
        - If you plan to export the certificate to use on multiple web servers, as is often done in an HA install, ensure that you select **Make private key exportable**. Failure to do this results in the inability to export the certificate at a later time
        - The values that you enter and the selections that you make are not validated. You must ensure that you provide all required information or the CA can be unable to complete the CSR
    8. Once you have made all selections select, **OK** to return to the wizard. Select **Next** to proceed to the next page.
    9. On the **Where do you want to save the offline request?** page, select a file name in a location you are able to access. For most CAs, you must select **Base 64** as the format.
    10. Provide the file to your CA. When they have signed it and returned the certificate to you, copy the certificate to the web server and proceed with the last steps.
    11. In the Certificate management snap-in for MMC, navigate to **Certificates (Local Computer)** > **Personal**, right-click **Certificates**, and choose **All Tasks > Import...**. The **Certificate Import Wizard** appears.
    12. Select **Next** on the introductory screen.
    13. On the **File to import** screen, select the certificate that has been signed by your CA, then select **Next**.

14. Ensure you select **Place all certificates in the following store**.
15. Ensure that **Personal** is selected in the **Certificate store:** box, then select **Next**.
16. Review the final screen, then select **Finish** to complete the import.
17. Close the MMC console. If you are prompted to save the console settings, select **No**. This does not affect the certificate import.
18. Proceed to the next major step, **Bind certificate to website**.

Step 1.2. Bind Certificate to Website

⚠ **Caution**: You must ensure that the hostname field is left blank and the Require Server Name Indication option is not selected in the Edit Site Binding box. If either of these is configured SPOG fails when it attempts to communicate with ECE.

---

1. Open Internet Information Services (IIS) Manager if you have not done so previously.
2. In the **Connections** pane on the left, navigate to **Sites** and select **Default Web Site**.

   Ensure that you select the correct site name if you chose to use a site name other than Default Web Site.

3. Select **Bindings...** from the **Actions** pane at the right. The **Site Bindings** box appears.
    1. If there is not a row with the **Type**, **https** and **Port**, **443**, complete the following. Otherwise, proceed to the next major step.
        1. Select the **Add...** button, the **Add Site Binding** box appears.
        2. Select **https** in the **Type:** drop-down.
        3. Ensure that the **IP address:** drop-down shows **All Unassigned** and the **Port:** field is **443**.
        4. Ensure that you leave the **Host name:** field blank and the **Require Server Name Indication** option unselected.
        5. In the **SSL certificate:** drop-down, select the certificate name that corresponds to the one you created previously.
            - If you are unsure which certificate to choose, use the **Select...** button to view and search the certificates present on the server
            - Use the **View...** button to view the chosen certificate and verify that the details are correct
        6. Select **OK** to save your selection.
    2. Select the row that shows **https** in the Type column, then select the **Edit...** button. The **Edit Site Binding** box appears.
        1. Ensure that the **IP address:** drop-down shows **All Unassigned** and the **Port:** field is **443**.
        2. Ensure that the **Host name:** field has been left blank and the **Require Server Name Indication** option is not selected.
        3. In the **SSL certificate:** drop-down, select the certificate name that corresponds to the one you created previously.
            - If you are unsure which certificate to choose, use the **Select...** button to view and search the certificates present on the server
            - Use the **View...** button to view the chosen certificate and verify that the details are correct
        4. Select **OK** to save your selection.
    3. Select **Close** to return to IIS Manager.
4. Close the IIS Manager.

Step 2. Configure Partition Administrator SSO

The Partition Administrator SSO configuration allows ECE to automatically create a Partition level User

account for any administrator that opens the ECE gadget in SPOG.

Note: You must configure Partition Administrator SSO even if you do not plan to enable Agent or Supervisor SSO.

Step 2.1. Obtain Active Directory (AD) Certificate and Create Keystore.

This step can required to address the recent security changes that Microsoft announced. If the update is not applied and changes not made to the domain, then this can be skipped.

For details, please see, Microsoft KB4520412 details.

1. Obtain the SSL certificate, in Base 64 format, from your AD server that you provide in the Partition Administrator Configuration form. One method is shown.
    1. Use a workstation to download and install a copy of OpenSSL for Windows from, OpenSSL. The Light edition is adequate.
    2. Launch the OpenSSL command prompt.
    3. Run this command. Replace the server name with the fully qualified name of your Global Catalog domain controller.
    openssl s_client -connect gcdcsrv01.example.local:3269
    4. In the output, locate the Server certificate line.

```
C:openssl s_client -connect 14.10.162.6:3269
CONNECTED(00000003)
depth=1 DC = com, DC = massivedynamic, CN = MassiveDynamic Enterprise CA
verify error:num=20:unable to get local issuer certificate
verify return:0
---
Certificate chain
 0 s:
   i:/DC=com/DC=massivedynamic/CN=MassiveDynamic Enterprise CA
 1 s:/DC=com/DC=massivedynamic/CN=MassiveDynamic Enterprise CA
   i:/C=US/OU=pki.uclabservices.com/O=Cisco Systems Inc/CN=UCLAB Services Root
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIH1DCCBbygAwIBAgITJwAAAAbAAn/HKFuWCQAAAAAABjANBgkqhkiG9w0BAQsF
ADBcMRMwEQYKCZImiZPyLGQBGRYDY29tMR4wHAYKCZImiZPyLGQBGRYObWFzc2l2
ZWR5bmFtaWMxJTAjBgNVBAMTHE1hc3NpdmVEeW5hbWljIEVudGVycHJpc2UgQ0Ew
HhcNMjAwNDE1MDAxNDM0WhcNMjEwNDE1MDAxNDM0WjAAMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAxFajhqjrWqQHfqTXg+SXP5pzvNVrTHIigrAam8D0
```

    5. Copy the output from the start of, "-----BEGIN CERTIFICATE-----" through "-----END CERTIFICATE-----". Ensure that the BEGIN CERTIFICATE and END CERTIFICATE lines are included.
    6. Paste the information you have copied into a new text file, then save this to the computer with a crt extension.
2. Copy the certificate file to one of the Application servers.
3. Open an RDP session to the Application server where you copied the certificate.
4. Create a new Java keystore.
    1. Open a command prompt on the Application Server.
    2. Change to the ECE Java Development Kit (JDK) bin directory.
    3. Run this command. Replace the values as appropriate.
    keytool -import -trustcacerts -alias mydomaincontroller -file C:\temp\domainctl.crt -keystore c:\ece\pcce\mydomain.jks -storepass MyP@ssword

5. In versions earlier than 12.6, copy the keystore to the same path on all other Application Servers in your environment. With version 12.6, copy the keystore to a location accessible from the workstation where you configure ECE.

Step 2.2. Configure ECE with AD Lightweight Directory Access Protocol (LDAP) Access Information.

1. From a workstation or computer with **Internet Explorer 11**, navigate to the Business partition URL.

Tip: The Business partition is also known as Partition 1. For most installs, the Business partition can be accessed through a URL similar to, https://ece.example.com/default.

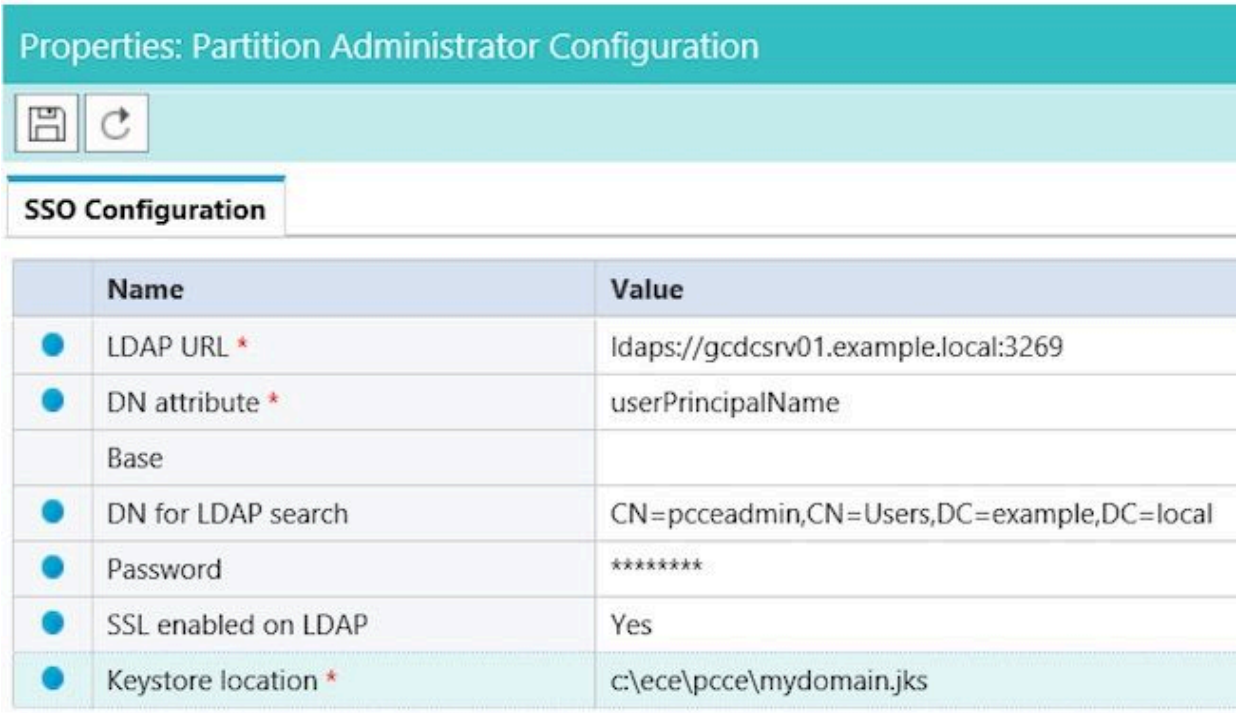
---

2. Login as **pa** and provide the password for your system.
3. After you have successfully logged in, select the **Administration** link on the initial console.
4. Navigate to the **SSO Configuration** folder, **Administration > Partition: default > Security > SSO and Provisioning**.
5. In the top pane on the right, select the **Partition Administration Configuration** entry.
6. In the bottom pane on the right, enter the values for your Lightweight Directory Access Protocol (LDAP) and AD.
    1. **LDAP URL** – As a best practice, use the name of a Global Catalog (GC) Domain Controller. If you do not use a GC, you can see an error in the ApplicationServer logs as follows.
    Exception in LDAP authentication <@>
    javax.naming.PartialResultException: Unprocessed Continuation Reference(s); remaining name 'DC=example,DC=com'
        - Non-secure Global Catalog port is 3268
        - Secure Global Catalog port is 3269
    2. **DN attribute** – This must be userPrincipalName.
    3. **Base** – This is not required if you use a GC, otherwise, you must provide the base proper LDAP format.
    4. **DN for LDAP search** – Unless your domain allows anonymous bind, you must provide the distinguished name of a user with the ability to bind to LDAP and search the directory tree.

    Tip: The easiest way to find the correct value for the user is to use the Active Directory Users and Computers tool. These steps show how to find this value.

    ---

        1. From the **View** menu, select the **Advanced Features** option.
        2. Navigate to the user object, then right-click and choose **Properties**.
        3. Select the **Attributes** tab.
        4. Select the **Filter** button, then select **Only show attributes with values**.
        5. Find **distinquishedName** in the list, then double-click to view the value.
        6. Highlight the value shown, then copy and paste it to a text editor.
        7. Copy and paste the value from the text file into the **DN for LDAP search** field.
        The value must be similar to, CN=pcceadmin, CN=Users, DC=example, DC=local
    5. **Password** – Provide the password for the specified user.
    6. **SSL enabled on LDAP** – This field can be considered mandatory for most customers.
    7. **Keystore location** – This must be the location of the keystore where you imported the SSL certificate from AD. In the example, this is c:\ece\pcce\mydomain.jks, as shown in the image:



7. Select the icon of the floppy disk to save the changes.

Step 3. Validate Configuration File

Completion of this section is mandatory for all 12.0 installs. For any version other than 12.0, you may be able to skip this section.
There are two additional scenarios with all versions where this step can be required. The first is when ECE has been installed in a high-availability setup. The second, and more common is when the host name of the web server does not match the name you use to access ECE. For example, if you install the ECE Web server on a server with the host name, UCSVRECEWEB.example.com, but users access the ECE web pages with the URL, chat.example.com, then this section must be completed. If the server's hostname and the URL that you access ECE with are the same and if you have installed version 12.5 or higher, you can skip this step and complete the section.

Replace {ECE_HOME} with the physical location where you have installed ECE. For instance, if you have installed ECE at **C:\Cisco**, then replace {ECE_HOME} with **C:\Cisco** in each location.

Tip: Use a text editor such as Notepad++ instead of notepad or Wordpad as these do not interpret the line endings properly.

---

1. Open a remote desktop session to all ECE web servers in your deployment.
2. Navigate to this path, **{ECE_HOME}\eService\templates\finesse\gadget\spog**.
3. Locate the **spog_config.js**file and make a backup copy in a safe location.
4. Open the current **spog_config.js**file in a text editor.
5. Locate these two lines and update them to match your deployment.
   The web_server_protocol must be https, update if required.
   Update the web_server_name to match the fully qualified name that you allocated to use to access ECE. Example: **ece.example.com**
   - var web_server_protocol = "https";
   - var web_server_name = "ece.example.com";
6. Save the changes.
7. Repeat on all other web servers in your deployment.

Step 4. Add ECE to PCCE Inventory

As of 12.0, PCCE has 3 different deployment options, 2000 Agent (2K Agent), 4000 Agent (4K Agent), and 12000 Agent (12K Agent). These three deployment options can be separated into two groups, 2K Agent and the 4K/12K Agent. They are separated this way as there are several fundamental differences in how they look in SPOG. A very high-level comparison of the two methods follows this paragraph. This document does not give specific steps to add a component to the inventory. Please see the links at the end of this document for the specific details on this process. This section covers specific details that must be verified when you add ECE to PCCE. This document also assumes that your PCCE Installation is complete and that you are able to access and configure other aspects of the solution.

- 2K Agent Deployment
  - Initial configuration of the PCCE components is done entirely through CCE Administration and is automated
  - New components are added in the Inventory Page through a pop-up box where you enter the details such as the IP or Hostname and any necessary credentials or component-specific configuration
- 4K and 12K Agent Deployment
  - Much of the initial configuration mirrors the steps used for UCCE
  - Components are added via a Comma-Separated Values (CSV) file that you download from CCE Administration, populate per your specific install, then upload
  - The initial deployment requires some specific components to be included in the first CSV file
  - Components that were not added when the system was set up initially are added via CSV files that contain the information required

Step 4.1. Upload ECE Web Server Certificate to the Java Keystore

1. If self-signed certificates are used
   1. Open a remote desktop connection to the primary, side-A Administration Data Server (ADS).
   2. Open Internet Explorer 11 as administrator and navigate to the ECE business partition.
   3. Select the icon of a padlock at the right side of the URL bar then choose **View Certificates**.
   4. In the **Certificate** box, select the **Details** tab.
   5. Select **Copy to File...** near the bottom of the tab.
   6. In the **Certificate Export Wizard**, select **Next** until you reach the **Export File Format** page. Ensure that you select **Base-64 encoded X.509 (.CER)** format.
   7. Save the certificate to a location such as **c:\Temp\certificates** on the ADS server to complete the export.
   8. Copy the certificate to all other ADS servers.
   9. Open an administrative command prompt.
   10. Change to the Java home directory, then to the bin directory. The Java home directory can be accessed with as follows. **cd %JAVA_HOME%\bin**
   11. Back up the current **cacerts** file. Copy the **cacerts** file from **%JAVA_HOME%\lib\security** to another location.
   12. Run this command to import the certificate that you saved previously. If your keystore password is not 'changeit', update the command to match your install.
       keytool -keystore ../lib/security/cacerts -storepass changeit -import -alias <FQDN of ECE server> -file <Location where you saved certificate>
   13. Restart the ADS Server.
   14. Repeat steps 8-12 on the other ADS servers.
2. If CA-signed certificates are used
   1. Obtain the root and intermediate certificate in DER/PEM format and copy them to a location such as **C:\Temp\certificates** on all ADS servers.

> **Note**: Contact your CA Administrator to obtain these certificates.

2. Open a remote desktop connection to the primary, side-A ADS.
3. Open an administrative command prompt.
4. Change to the Java home directory, then to the bin directory. The Java home directory can be accessed with as follows. **cd %JAVA_HOME%\bin**
5. Back up the current **cacerts** file. Copy the **cacerts** file from **%JAVA_HOME%\lib\security** to another location.
6. Run this command to import the certificate that you saved previously. If your keystore password is not 'changeit', update the command to match your install.
   keytool -keystore ../lib/security/cacerts -storepass changeit -trustcacerts -import -alias <Name of CA root> -file <Location where you saved the root certificate>
7. Repeat Step 6. and import the intermediate certificate if present.
8. Restart the ADS Server.
9. Repeat steps 2-12 on all other ADS servers.

Step 4.2. Add the ECE Data Server to Inventory

- While the Data server must exist in the system inventory, no direct communication is done between the PCCE ADS and data server
- When ECE is deployed in the 1500-agent deployment, the Data server is the Services Server
- When ECE is installed in an HA configuration, add only the side-A Services server

Step 4.3. Add the ECE Web Server to Inventory

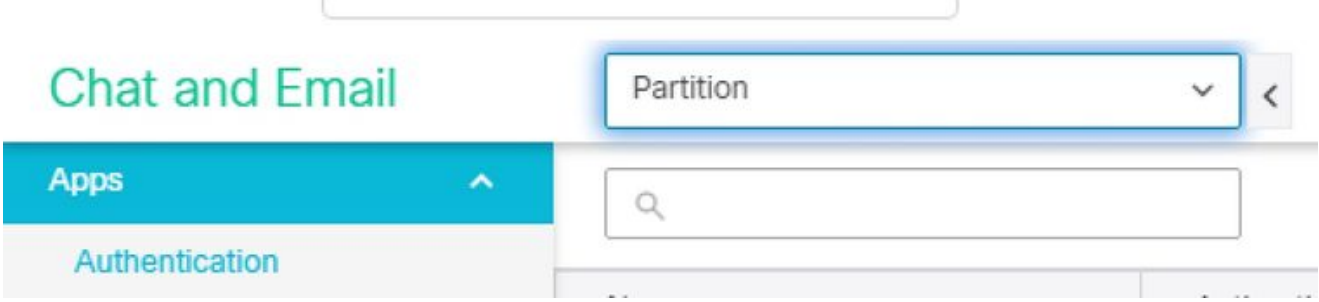
- Ensure that you add the web server with the fully qualified name
  - This name must match either the common name in the ECE certificate or must be listed as one of the Subject Alternative Name (SAN)s
  - You must not use just the host name or IP address
- The user name and password for ECE must be the pa login credentials
- Ensure that the Application Instance is correct
  - The Application Instance name is case sensitive
  - For the 2000 Agent PCCE deployments, the Application Instance is MultiChannel
  - For the 4000/12000 Agent PCCE deployments, the Application Instance contains the site and peripheral set as part of the name
- When ECE is installed with more than one web server, for instance in the 1500 Agent deployment or in a 400 Agent HA deployment, you can use either the URL that points to your load balancer or the URL that points to each individual web server as the fully qualified name of the web server. The best practice is to use a load balancer.
- If you have more than one ECE deployment, or if you choose to add each individual web server in deployment with more than one, you much choose the correct web server when you open the ECE gadget in SPOG.

Step 5. Integrate ECE with PCCE

1. Log in to CCE Administration as an administrator.
2. Select the **Email and Chat** card, then the **Email and Chat** link as shown in the image.



3. Review the current selected server in the Device Name dropdown. If you added both web servers in an HA install, you can choose either web server. If you add a second ECE deployment to your system at a later time, ensure that you select the appropriate server before you continue.
4. In the drop-down next to **Chat and Email**, select **Partition** or **Global** as shown in the image.



5. In the top menu, select **Integration**, then select the arrow beside **Unified CCE** and select the second **Unified CCE** as shown in the image.



6. Populate the values in the **AWDB Details** tab for your install, then select the **Save** button.
7. Select the **Configuration** tab and complete this as follows.
    1. Select the drop-down beside **Application Instance** and select the Application Instance created for ECE.

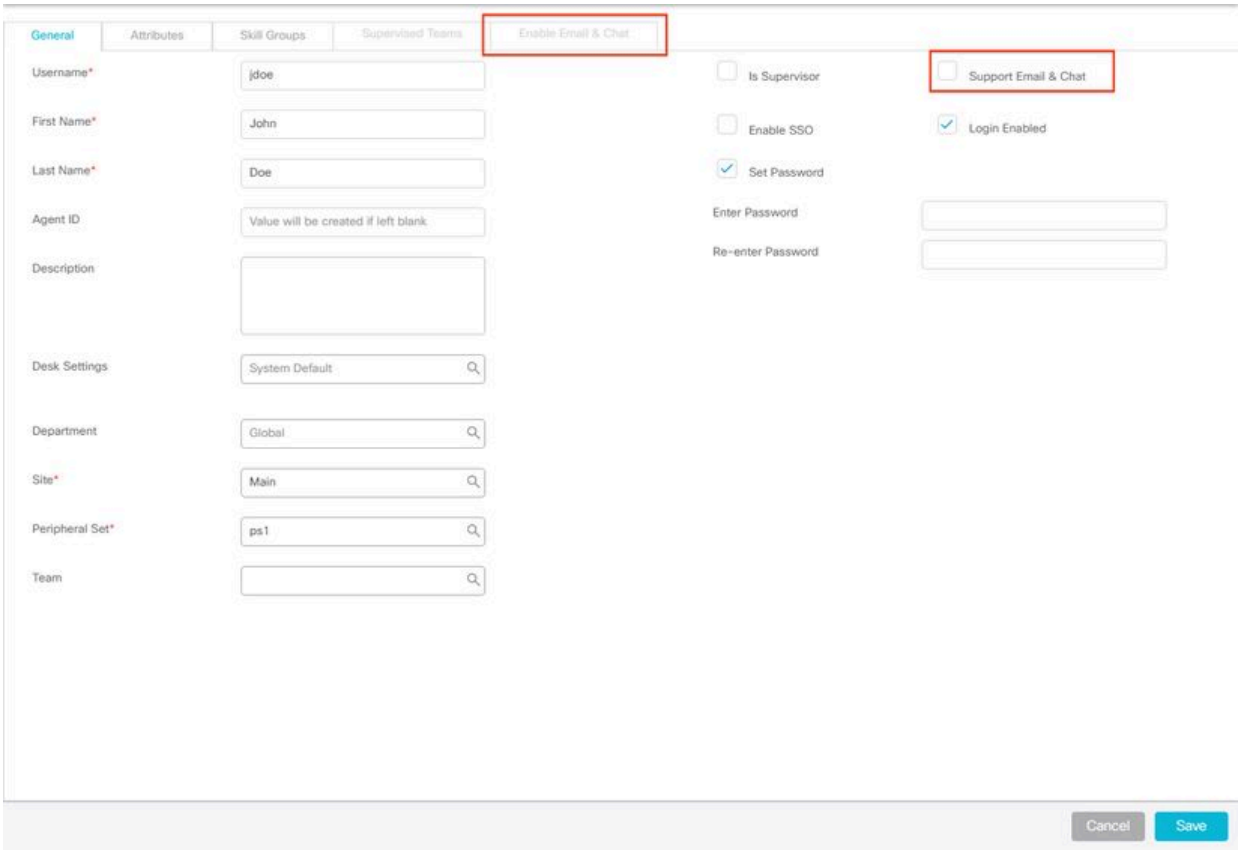
    > **Note**: This must not be the Application Instance which starts with UQ.

    2. Select the green circle with white plus sign button select the Agent PG.
        1. Select the Agent PG (or Agent PGs if more than one).
        2. Select **Save** once you have added all Agent PGs.

    > **Warning**: Once you select **Save** the system is permanently connected to PCCE and cannot be undone. If are errors made in this section, you must ECE uninstall completely and drop all databases, then install ECE as if it is a fresh install.

Step 6. Validate ECE Integration

1. In CCE Administration, check that there are no alerts shown in the top status bar. If there are alerts, select the word **Alerts** and review the Inventory page to ensure that none of the alerts are for the ECE servers.
2. Select **Users** then **Agents** in the navigation bar on the left.
3. Select an agent from the list and verify this.
    1. You now see a new check-box for **Support Email & Chat** on the **General** tab.
    2. You now see a new tab labeled **Enable Email & Chat** as shown in the image.



4. Enable a test agent for ECE.
    1. Select the **Support Email & Chat** check-box and note that the **Enable Email & Chat** tab is now able to be selected.
    2. Select the **Enable Email & Chat** tab and provide value in the **Screen Name** field.
    3. Select **Save** to update the user.
    4. You receive a success message.
5. Verify that ECE has been updated.
    1. Select the **Overview** navigation button, then select the **Email and Chat** card and link.
    2. In the drop-down next to **Chat and Email**, select the name that corresponds to the agent's department.

Note: The Service department in ECE holds all objects that belong to the Global department in PCCE. The department name Service is, therefore, a reserved value.

---

    1. In the top menu, select **User Management** then select **Users** in the menu under **Chat and Email**.
    2. Validate that you see the new agent in the list.

Troubleshoot

It is recommended that you download several tools and keep them on the ECE Servers. These make it far easier to troubleshoot and maintain the solution over time.

- A text editor such as Notepad++
- A archive tool such as 7-Zip
- One of the many Tail for Windows programs
  A few examples are:
    - Baretail
    - Tail for Win32

In order to troubleshoot issues with integration, you must first be aware of some key log files and the location of each.

1. ## File Names and Locations on ECE

   There are many logs on the ECE system, these are just the ones which are most helpful when you attempt to troubleshoot an issue with integration.

Log File	Server	Name Convention	Description
Application Server	C/A	eg_log_{HOSTNAME}_ApplicationServer.log	Logs from the Wildfly Server
External Agent Assignment	C/S	eg_log_{HOSTNAME}_EAAS-process.log	Interaction with MR PG
External Agent Messaging	C/S	eg_log_{HOSTNAME}_EAMS-process.log	Interaction with CTI Server
Root logs	C/A/M/S	egpl_root_{HOSTNAME}.log	Inter-process logs, HazelCast, general errors
Component status	C/A/M/S	eg_log_{HOSTNAME}_component-status.log	Process start and file copy completion
Process Launcher	C/A/M/S	eg_log_{HOSTNAME}_ProcessLauncher.log	General logs for service and process start-up
Distributed Services Manager	C/S	eg_log_{HOSTNAME}_DSMController.log	Logs that show the process start and stop on Services server

   Server Key:

   - C = Collocated Server
   - A = Application Server
   - S = Services Server
   - M = Messaging Server

   Most log files also have two other logs that are associated with them.

   - eg_log_{SERVERNAME}_{PROCESS}.log – Primary process log
   - eg_log_dal_connpool_{SERVERNAME}_{PROCESS}.log – Connection pool usage
   - eg_log_query_timeout_{SERVERNAME}_{PROCESS}.log – Updated when a query fails due to time out

2. ## File Names and Locations on PCCE

   PCCE logs for integration issues are all located on the side-A ADS. Here are the logs which are most important as you troubleshoot integration issues. Each of these is located in, **C:\icm\tomcat\logs**.

Log File	Name Convention	Description
CCBU	CCBU.{YYYY}-{MM}-{DD}T{hh}-{mm}-{ss}.{msec}.startup.log	Primary log for CCE Admin and all related web applications
CCBU Error	Error.{YYYY}-{MM}-{DD}T{hh}-{mm}-{ss}.{msec}.startup.log	Errors that are seen by the CCE Admin and related web applications
Catalina	catalina.{YYYY}-{MM}-{DD}.log	Tomcat native log, shows certificate errors
Tomcat stdout	tomcat9-stdout.{YYYY}-{MM}-{DD}.log	Standard Out log messages from Tomcat
Tomcat stderr	tomcat9-stderr.{YYYY}-{MM}-{DD}.log	Standard Error log messages from Tomcat

Of these logs, the first three are the most frequently requested and reviewed.

Use these steps to set trace levels and collect the required logs.

3. ## Trace Level Configuration

This section only applies to ECE. The logs that are required from PCCE have their trace level set by Cisco and are unable to be changed.

1. From a workstation or computer with **Internet Explorer 11**, navigate to the System partition URL.

   Tip: The System partition is also known as Partition 0. For most installs, the System partition can be accessed through a URL similar to, https://ece.example.com/system

2. Log in as **sa** and provide the password for your system.
3. After you have successfully logged in, select the **System** link on the initial console.
4. In the **System** page, expand **System** > **Shared Resources** > **Logger** > **Processes**.
5. In the top, right-hand pane, find the process that you wish to change the trace level and select it.
   Note: In an HA system and in a system with more than one Application Server, processes are listed more than once. To ensure that you capture the data, set the trace level for all servers that contain the process.
6. In the bottom, right-hand pane, select the drop-down for **Maximum trace level** and select the appropriate value.
   There are 8 trace levels defined in ECE. The 4 in this list are those which are used most often.
   - 2 - Error – Default trace level for processes
   - 4 - Info – Trace level generally used for issue resolution
   - 6 - Dbquery – Often helpful for to diagnose issues early in the setup or more complex issues
   - 7 - Debug – Very verbose output, only required in the most complex issues

   Note: Do not leave any process at 6 – Dbquery or higher for any extended length of time, and generally only with TAC guidance.

   Keep most processes trace level, 2-Error. If you select level 7 or 8, you must also select a maximum duration. When the maximum duration time is met, the trace level returns to the last level set.
   After the system is set up, change these four processes to trace level 4.

- EAAS-process
- EAMS-process
- dx-process
- rx-process

7. Select the save icon to set the new trace level.

4. Log File Collection

1. Open a Remote Desktop Session to the server where the process logs that are needed.
2. Navigate to the log file location.
    1. ECE Servers

       Logs are written as follows.

       - By default, logs are written files with a maximum size of 5MB
       - When one log file reaches the configured maximum, it is renamed in the format, {LOGNAME}.log.{#}
       - ECE keeps the previous 49 log files plus the current file
       - The current log always ends with.log and no number after
       - Logs are neither archived or compressed
       - Most logs have a common structure
       - Log files use <@> to separate the sections
       - Logs are always written in GMT+0000 time

       ECE logs are located in different places based on the specific install.

       1. 400 Agent Deployments
          1. Single-sided
             - Server: Collocated Server
             - Location: **{ECE_HOME}\eService_RT\logs**
          2. High-Availability
             - Servers: Both Collocated Servers
             - Location: **{ECE_HOME}\eService\logs**
             - Directory created for the Distributed File System (DFS) share contains only logs for installation and upgrades.
             - Only the server that owns the Distributed Systems Maanger (DSM) role writes logs for the components that are part of the Services Role
                - DSM role owner can be found on the Processes tab of Windows Task Manager. There are 10-15 Java processes on this server that are not on the secondary server.
                - Components under DSM include, EAAS, EAMS, Retriever, Dispatcher, Workflow, and so on.
       2. 1500 Agent Deployments
          - Logs located on the server that hosts the role
          - Location: **{ECE_HOME}\eService\logs**
          - With the exception of the Services server, all servers operate and write logs for all processes associated with the component
          - In a high availability deployment, the Services server operates in Active/Standby configuration
          - Only the server that owns the Distributed Systems Maanger (DSM) role writes logs
          - DSM role owner can be identified by the number of processes seen in Windows Task Manager. There are 10-15 Java processes that run on the

primary server and only 4 Java processes on the secondary server

2. PCCE Servers
    - The required logs from PCCE are located at, **C:\icm\tomcat\logs**
    - Tomcat logs are not rolled over or archived
    - Logs are written in local server time

3. Collect all logs that were created or modified after the issue was observed.
   A complete explanation of the logs and the issues that are seen is beyond the scope of this document. Some common issues, what to review, and some possible solutions are as follows.
    - Certificate Related Issues
        - Certificate Not imported
            - Behavior: When you attempt to open the ECE gadget in SPOG, you see the error, "An error occurred while loading the page. Please contact administrator."
            - Check: The Catalina log on PCCE for errors similar to these javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target
            - Resolution: Ensure that you have imported the ECE Web Server Certificate, or the appropriate CA certificates into keystore on the ADS
        - Certificate Mismatch
            - Behavior: When you attempt to open the ECE gadget in SPOG, you see an error which indicates that the certificate's common name or subject alternate name does not match the configured name.
            - Check: Validate the SSL Certificate
            - Resolution: Ensure that either the Common Name field in the Subject, or one of the DNS fields in the Subject Alternate Name contains the fully-qualified name that you have entered into SPOG as the Web Server name.
    - System Issues
        - Service Not Started
            - Behavior: When you attempt to open the ECE gadget in SPOG, you see the error, "The webpage at https://{url} might be temporarily down or it may have moved permanently to a new address."
            - Check: Validate that the Windows Service - Cisco Service has been started on all ECE servers with the exception of the Web server. Review the Root logs on the Application Server for errors
            - Resolution: Start the Cisco Service on all ECE services.
    - Configuration Issue
        - LDAP Configuration
            - Behavior: When you attempt to open the ECE gadget in SPOG, you see the error, "An error occurred while loading the page. Please contact administrator."
            - Check: Increase the trace level of the Application Server to level 7- Debug, then attempt the login again and review the Application Server log. Search for the word LDAP.
            - Resolution: Validate LDAP configuration for Partition Administrator SSO to ensure that it is correct.

Related Information

These are the key documents you must review thoroughly before you start any ECE installation or integration. This is not a comprehensive list of ECE documents.

⚠ **Caution**: Most ECE documents have two versions. Please ensure that you download and use the versions that are for PCCE. The document title has either **for Packaged Contact Center Enterprise** or **(For PCCE)** or **(For UCCE and PCCE)** after the version number.

Ensure that you check the start page for Cisco Enterprise Chat and Email documentation for any updates prior to any install, upgrade, or integration.

https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/series.html

- 12.0
  - Enterprise Chat and Email Installation and Configuration Guide
  - Enterprise Chat and Email Upgrade Guide
  - Enterprise Chat and Email Administrator's Guide
- 12.5
  - Enterprise Chat and Email Installation and Configuration Guide
  - Enterprise Chat and Email Upgrade Guide
  - Enterprise Chat and Email Administrator's Guide