System Menu

- Access Server Menu, on page 1
- Cloud Connect, on page 2
- Unified CM Configuration, on page 5
- System Parameters, on page 5
- Single Sign-On (SSO), on page 11
- Custom File Configuration, on page 13
- Standalone Cisco Unified Intelligence Center, on page 13
- License Information, on page 15
- Language Information, on page 23
- Logout Menu, on page 24

Access Server Menu

Choose **System** > **Server** from the Cisco Unified CCX Administration menu bar to access the **List Servers** web page. Use the **List Servers** web page to view, add, remove, and view servers in the cluster.

Note **Before installing Unified CCX on the second node, you must configure the second server using this procedure. Installation of second node will fail if you do not perform this configuration**.

To view, modify, or delete the server configuration information of any server, click the respective hyperlink in the **Host Name/IP Address** field. The **Server Configuration** web page opens to display Host Name/IP Address, MAC Address, and Description of the server. Update the values in the fields and click **Save** to save the changes. Click **Delete** to delete the configuration information of a server.

Note You cannot delete the publisher.

Configure Server

To configure a new server that needs to be added to form a Unified CCX cluster for a High Availability setup, complete the following steps.

Step 1 Click the **Add New** icon in the toolbar in the upper left corner of the **List Servers** web page or the **Add New** button at the bottom of the **List Servers** web page to add the new server.

The Server Configuration web page appears.

Note
- The **Add New** button is disabled when two servers are added to the cluster in a High Availability setup.
- A warning message appears when you click the **Add New** button without having a High Availability license.

Step 2 Complete the following fields:

Field	Description
Host Name/IP Address	Hostname or IP address of the server that you want to add.
MAC Address	MAC address of the server that you want to add.
Description	Description of the server that you want to add.

Step 3 Click **Add** to add details of the new server.

Server Deletion

This section describes how to delete a server from the Unified CCX. In Unified CCX administration, you cannot delete the first node that is also called as the publisher node, but you can delete the subscriber node.

Step 1 Choose **System > Server** from the Cisco Unified CCX Administration menu bar to access the List Servers web page.

Step 2 Select the subscriber node and click **Delete** to delete the configuration information of the server.

Step 3 Power off the subscriber node.

Note When a subscriber node is removed from a cluster, its certificates still exist in the publisher node. The administrator must manually remove the following:
- The certificate of the subscriber node from the trust-store of the publisher node.
- The certificates of the publisher from the trust-store of the removed subscriber node.

Step 4 Run the **utils system restart** command to restart the publisher node.

Cloud Connect

Cloud Connect enables on-premise Unified CCX solution to integrate with different cloud services. The Cloud Connect services are responsible for interacting with Webex Experience Management (WXM) cloud service

for presenting surveys to users and access analytics on the survey responses to understand the Customer Experience trends.

Note To use cloud services, memory requirement is different. If you do not have the required memory an error message is displayed. For the appropriate memory requirements, see *Solution Design Guide for Unified Contact Center Express* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-implementation-design-guides-list.html.

Use the **Cloud Connect** page to perform the following:

- Check the status of Cloud Connect.
- Register and Deregister Unified CCX with Cisco Webex Cloud.
- Enable and Disable Cloud Services.
- Check Cluster Information.
- Check the status of the nodes in the cluster.

For more information, see *Cloud Connect* chapter in *Cisco Unified Contact Center Express Features Guide*.

Actions

The following table lists the actions that you can perform on this page:

Action	Procedure
Register	To use the Cisco Webex Cloud features. **Note** Ensure that all the Prerequisites are met. 1. Select the **I have received the email for the account creation in Cisco Webex Cloud and have successfully created an account in Cisco Webex Cloud** checkbox. 2. Click **Register**. The **Cisco Webex Control Hub** page is displayed. Follow the on-screen instructions to register.
Deregister	Click **Deregister**. The **Cisco Webex Control Hub** page is displayed. Follow the on-screen instructions to deregister.
Deployment Name	Enter a name to identify the Unified CCX system. By default, **Deployment ID** is displayed.
Test Connection	Click **Test Connection** to check the Unified CCX connectivity with **Cisco Webex Cloud**. In a HA environment, the connection is tested for both the nodes.

Action	Procedure
Enable Data Streaming to Cisco Webex Cloud	To publish the Unified CCX data to a database that is available in cloud: 1. In the **Cluster Information** table, enter the **Deployment Name**. 2. In the **Cloud Services** table, select the **Enable** checkbox for **Data Streaming to Cisco Webex Cloud**. 3. Click **Update**.

Cluster Information

The details of **Cluster Information** table are as follows:

Field	Description
Deployment ID	Mac address of the system.
Deployment Name	Name to identify the Unified CCX system.
HTTP Proxy	HTTP Proxy value that is used by Cloud Connect. **Note** If you have configured HTTP Proxy settings in the previous versions of Unified CCX, after upgrading, you must click **Update** to get the previously configured HTTP Proxy value. If there is a mismatch of HTTP Proxy value between **System Parameters** page and **Cloud Connect** page, a **Warning** icon is displayed. Click **Update** to get the updated proxy value.

Cloud Services

You can enable and disable the cloud services that are listed. The following cloud service is available:

- **Data Streaming to Cisco Webex Cloud**

Cluster Status

The **Cluster Status** table lists the **Host Name** and **Status** of each node. The status can be any one of the following:

- In Service
- In Maintenance
- Not Configured
- Out of Service
- Unknown

Adjacent to each status, there is a link to **View Status**. Click the link to download a text file that has the status details of the node. This file is used to debug issues with Cloud Connect.

Unified CM Configuration

Choose **System** > **Unified CM Configuration** from the Unified CCXAdministration menu bar to access the Unified CM Configuration web page.

Use the Unified CM Configuration web page to update the following information:

- The Unified CM AXL provider used for Unified CCX AXL requests for agent authentication and SQL queries.
- The Unified CM JTAPI provider used by the Unified CCX Engine Unified CM Telephony subsystem to control and monitor CTI ports and route points.
- The Unified CM RmCm -JTAPI provider used by the Unified CCX Engine RmCm subsystem to control and monitor the agent phones and extensions.

System Parameters

Note When you configure a parameter for the primary node, same value is reflected for the secondary node.

The System Parameters configuration web page displays the following fields.

Table 1: System Parameters

Field	Description
Generic System Parameters	
System Time Zone	The system or primary time zone is the same as local time zone of the primary Unified CCX node configured during installation. Display only. Unified CCX Administration uses this primary time zone to display time-related data. **Note** If you have changed the primary time zone, reboot both the nodes in the Unified CCX cluster.
Network Deployment Parameters (displayed only in a HA over WAN deployment)	
Network Deployment Type	Displays the network deployment type as LAN or WAN only if we have more than one node. Display only.
Internationalization Parameters	
Customizable Locales	Use to specify a unique locale. Default value is blank.

Field	Description
Default Currency	Default currency, such as American dollars (USD), Euros, and so on. This is a mandatory field. Converts currency amounts in a playable format when no currency designator is specified Default: American Dollar [USD]
Media Parameters	
Codec	The Codec chosen during installation for this Unified CCX server. Unified CCX supports packetization intervals of 20 ms, 30 ms, or 60 ms. Default value is 30 ms. **Note** After changing the Codec, ensure that you restart Unified CCX Engine on all nodes for the settings to take effect.
MRCP Version	Select appropriate version of the protocol for ASR and TTS. When you select **MRCPv1** or **MRCPv2**, ensure that the appropriate port changes are done for MRCP ASR and MRCP TTS Servers. **Note** When you upgrade, the default value is **MRCPv1**. After changing the MRCP version, ensure that you restart Unified CCX Engine on all nodes for the settings to take effect.
Default TTS Provider	Default TTS (Text-to-Speech) provider. Default: By default, no TTS provider is configured. Select a provider from the drop-down list to configure it as the default. The system uses the default TTS provider to determine which provider to use if the TTS request does not explicitly specify the provider to use.
User Prompts override System Prompts	When enabled, custom recorded prompt files can be uploaded to the appropriate language directory under Prompt Management to override the system default prompt files for that language. By default, this is disabled.

Field	Description
SRTP	SRTP (Secure Real-Time Protocol) protects the confidentiality of the media with cryptographic procedures. When enabled, a secure media for communication (SRTP) is established between callers and CTI port. Before you enable SRTP, ensure that the CUCM Cluster Security Mode is set to Mixed mode. **Note** When SRTP is enabled, a secure JTAPI connection is established between the following subsystems and Unified CM: • Unified CM Telephony • RmCm After enabling or disabling SRTP, ensure that you restart Unified CCX Engine on all nodes for the settings to take effect. An SRTP-enabled HA setup requires distinct RmCm provider users. So, the system generates a separate **RmCm Provider User Id** with suffix "_ccxsub" for the subscriber node. Associate devices and device profiles only with the **RmCm Provider User Id** that is configured in the **Cisco Unified CM Configuration** page (primary RmCm user). During data synchronization, the devices and device profiles that are associated only with system-generated RmCm user are removed and synchronized with that of primary RmCm user.
Application Parameters	
Supervisor Access	The Administrator uses this option to allow certain privileges to supervisors (all supervisors have the same privilege). The options are: • No access to teams—The supervisor logs into the Supervisor page, but will not be able to see any team information (No RmCm info). • Access to all teams—The supervisor logs into the Supervisor page, and will be able to see all the teams (RmCm information). • Access to supervisor teams only—The supervisor logs into the Supervisor page, and can see the teams that they supervise. When this option is selected, only the Primary Supervisor can see the team-specific information. The secondary supervisor will not be able to see the team-specific information. Default: No access to teams **Note** A supervisor who does not have administrator privileges can add, modify, or remove skills from an agent.

Field	Description
Max Number of Steps that have run	The maximum number of steps an application can run before the Unified CCX Engine terminates the script or application. This is a mandatory field. This limitation is intended to prevent a script from running indefinitely. Default value is 1000. **Note** Do not change the default value.
Additional Tasks	This field allows you to control the creation of additional threads that the Unified CCX server internally initializes based on licensed Unified IP IVR ports. This is a mandatory field. Default value is 0.
Default Session Timeout	Maximum amount of time (in minutes) a user-defined mapping ID remains in the session object memory after the session is moved to the idle state. During this duration, the session remains accessible even if you have terminated that session. Use this setting to configure the time required to perform your after-call work (for example, writing variables to a database before clearing the session). This is a mandatory field. The default value is 30 minutes. If you reduce this number, you also reduce the system memory usage comparatively. You can add a user-defined mapping ID to a session using the Session Mapping step in the script editor. Once assigned, you can use this mapping ID to get the session object from another application instance. By doing so, other applications obtain access to the session context. See the *Cisco Unified Contact Center Express Getting Started with Scripts* for more information.
Enterprise Call Info Parameter Separator	A character used Get/Set Enterprise Call Info steps in the Unified CCX Editor to act as a delimiter for call data. This is a mandatory field. Default value is | (bar).
Agent State after Ring No Answer	Radio button determining how agent state should be set after a Ring No Answer event. This is a mandatory field. The options are: • Ready—If an agent does not answer a Unified CCX call, the Agent State is set to Ready. • Not Ready (default)—If an agent does not answer a Unified CCX call, the Agent State is set to Not Ready.

Field	Description
Change Agent State to Not Ready when Agent Busy on Non ACD Line	Radio button that enables the agent's state to change from Ready state to Not Ready state when the monitored Non ACD lines are used for Incoming or Outgoing calls. The options are: • Enable—Enables the state change of the agent in this scenario. • Disable (default)—Disables any state change of the agent in this scenario. This is not applicable if the Non ACD lines are shared lines. **Note** When a call is transferred from the ACD to the Non ACD monitored line on the same phone, the agent remains in the Talking state instead of Ready until the Non ACD call ends.
Number of Direct Preview Outbound seats	The maximum number of Direct Preview Outbound seats. The configuration of Outbound seats is done during the initial configuration or setup phase, after the installation. **Note** This is a mandatory field. This field is displayed only if you have a Premium license. The maximum number of direct preview outbound seats that can be configured is limited by the Premium Seat Count. If there is an invalid entry during configuration, an error message is displayed.
Live Data - Short Term Reporting Duration	This parameter applies to Live Data reports that are available to agents and supervisors on Finesse desktops. For certain fields in the live data reports, you can set a short-term value to 5, 10 or 15 minutes. Long-term value is always set to 30 minutes.
Persistent Connection	Radio button that determines whether to establish persistent connection to a remote device. The options are: • Enable (default)—Establishes persistent connection. • Disable—Does not establish persistent connection.
System Ports Parameters	
RMI Port	The port number used by the Unified CCXCVD to serve RMI requests. This is a mandatory field. Default value is 6999. **Note** After changing the RMI Port, ensure that you restart the system for the settings to take effect. On a high availability setup, restart both the nodes.

Field	Description
RmCm TCP Port	TCP port number on which the CTI server component of the RmCm subsystem opens the server socket and listens to the clients. All CTI server clients, such as Sync Server, and IP Phone Agent Server, use this port number. This is a read-only field and cannot be modified. Default value is 12028.
Proxy Parameters	
HTTP	• **Host Name**: Fully qualified domain name (FQDN) of the HTTP proxy server. Do not enter the IP address. • **Port**: Port number that is used to connect to the HTTP proxy server. Range is from 1 to 65535.
SOCKS Proxy	• **Host Name**: Fully qualified domain name (FQDN) of the SOCKS proxy server. Do not enter the IP address. • **Port**: Port number that is used to connect to the SOCKS proxy server. Range is from 1 to 65535.
SOCKS Username	Username of the SOCKS proxy server.
SOCKS Password	Password of the SOCKS proxy server.
Note Proxy parameters changes are automatically notified to Customer Collaboration Platform.	
Agent Settings	
Agent State after Ring No Answer	Radio button determining how agent state should be set after a Ring No Answer event. This is a mandatory field. The options are: • Ready—If an agent does not answer a Unified CCX call, the Agent State is set to Ready. • Not Ready (default)—If an agent does not answer a Unified CCX call, the Agent State is set to Not Ready.

Field	Description
Change Agent State to Not Ready when Agent Busy on Non ACD Line	Radio button that enables the agent state to change from the Ready state to the Not Ready state when the monitored Non ACD lines are used for Incoming or Outgoing calls. The options are: • Enable—Enables the state change of the agent. • Disable (default)—Disables any state change of the agent. This is not applicable if the Non ACD lines are shared lines. When you choose an option, a popup message informs you that this setting will be applied globally to all the teams except for the teams that have chosen to override this global setting. Click **OK** to continue or **Cancel** to discard the change. **Note** The popup message appears only if **Change Agent State to Not Ready when Agent Busy on Non ACD Line** is configured at a team level. To configure this functionality at a team level, you must install UCCX 12.5(1) SU1 ES01.
Agent Device Selection	Radio button that enables the support for the agent device selection feature which allows the agent to select the desired device (Desk Phone with EM, Desk Phone without EM, or Jabber) at the time of Finesse desktop login. The options are: • Enable—Select this option to enable the agent to select the active device at the time of Finesse desktop login. **Note** When the Agent Device Selection feature is enabled, both primary and secondary extensions can be shared with multiple devices. However, ensure that the devices using the shared extensions are not used at the same time. • Disable (default)—Select this option to disable the agent from selecting the active device at the time of Finesse desktop login. **Note** When you enable or disable the Agent Device Selection feature, restart the Unified CCX Engine on all the nodes.

Single Sign-On (SSO)

Use Single Sign-On (SSO) page to register, test, enable, and disable Single Sign-On.

Before you begin

Ensure you access the Cisco Unified CCX Administration page through a Fully Qualified Domain Name URL instead of IP address.

You need to configure Cisco Identity Service and enable trust relationship between Cisco Identity Service and Identity Provider.

For vendor specific configuration of the Identity Provider see, *Configure the Identity Provider for UCCX based on SSO* at https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200612-Configure-the-Identity-Provider-for-UCCX.html.

If Cisco Identity Service is not configured, it displays the status as `Cisco Identity Service is not configured` and provides the link to configure or update `Click here to update Cisco Identity Service configuration`. The steps 2 to 4 are disabled till the Cisco Identity Service is configured. The changes take effect when the page is refreshed.

If Cisco Identity Service is configured, it displays the status as `Cisco Identity Service is configured successfully` with the link to update `Click here to update Cisco Identity Service configuration`.

Step 1 Choose **System** > **Single Sign-On (SSO)** from the Unified CCX Administration menu to access the Single Sign-On page. The page displays the Cisco Identity Service configuration status, options to register, test, enable, and disable Single Sign-On.

Note If the `Cisco Identity Service` is configured successfully, then the **Register** option is enabled.

Step 2 Click **Register** on the Single Sign-On page to onboard the Single Sign-On components.
A status message is displayed on the screen to notify the status of the registration of the components. A **red** color icon indicates failure in the operation that has run. A **green** color icon indicates successful run operation. A **grey** color icon indicates the inability to capture the status of the operation that has run.

Step 3 Perform all the following prerequisites before the **SSO Test**. All the check boxes have to be checked for the **Test** option to be enabled.

a) Configure and Perform LDAP Sync in Cisco Unified CM.
b) Assign Cisco Unified CCX Administrator rights to one or more Enterprise users.
c) Assign Reporting Capability to Cisco Unified CCX Administrator (assigned in Administrator Capability View) and run the CLI command utils cuic user make-admin CCX\<Admin's User ID> to provide administrator rights to the Cisco Unified CCX Administrator in Cisco Unified Intelligence Center. Use the configured user with Unified CCX Administrator rights for the SSO Test operation.

Note
- Ensure that the browser based pop-up blocker is disabled for the **SSO Test** to work.
- For the **SSO Test** to be successful, the root domain of both the Unified CCX nodes must be the same.

Step 4 Click **Test** on the Single Sign-On page to test the status of registration of each component. You will be redirected to the Identity Provider for authentication.
A status message is displayed on the screen to notify the test status of the registered components. Single Sign-On test results are not persisted and will be lost when the page is reloaded. If the **SSO Test** is successful then the **Enable** option is enabled.

Step 5 Click **Enable** on the Single Sign-On page to enable each component for Single Sign-On.

Note

- When SSO is enabled and if the enterprise user is unable to log in, the recovery URLs can be used to log in. For troubleshooting purpose the enterprise user or system user chosen during the installation can login to Unified CCX Administration and Unified CCX Serviceability through the following recovery URL to bypass the enterprise Identity Provider and Cisco Identity Service. However, this is not possible when SSO is enabled and the usual login URL is used.
  - URL for Cisco Unified CCX Administration : `https://<ipaddress/fqdn>/appadmin/recovery_login.htm`
  - URL for Cisco Unified CCX Serviceability : `https://<ipaddress/fqdn>/uccxservice/recovery_login.htm`
- To disable SSO in an SSO enabled Cisco Unified Contact Center Express solution, click **Disable** on the **Single Sign-On (SSO)** page. After SSO is disabled, you have to perform **SSO Test** again to enable SSO.

The page displays the status of each component being enabled for Single Sign-On or not.

You may close this page and open a new window of the browser to access the Cisco Unified CCX Administration. This automatically redirects you to the page to enter your credentials for the authentication with the Single Sign-On identity provider.

Note User IDs are case-sensitive when logging into the Unified CCX Administration web interface. To make them case-insensitive, you must install 12.5(1) SU1 ES02.

Custom File Configuration

Use the Custom Classes Configuration web page to specify the classpath for custom classes.

Choose **System** > **Custom File Configuration** from the Unified CCXAdministration menu bar to access the Custom Classes Configuration area.

Note Restart Unified CCX engine and Unified CCX administration services to use the custom files in scripts.

Standalone Cisco Unified Intelligence Center

Obtain and Upload SSL Certificates

Before configuring the standalone Cisco Unified Intelligence Center, you must obtain the SSL certificates from the Cisco Unified Intelligence Center nodes and upload them into the Unified CCX Tomcat trust store.

To download the SSL certificates from the standalone Cisco Unified Intelligence Center do the following:

1. Sign in to **Cisco Unified OS Administration** interface on the Cisco Unified Intelligence Center server.
2. Select **Security** > **Certificate Management.**

   The **Certificate List** window appears.
3. In **Find Certificate List where** field, select **Certificate** and **contains** from the drop-down lists. Enter the search criteria as **tomcat** and then click **Find** to filter the certificate.

   The **Certificate List** displays the list of tomcat certificates.
4. Select the self-signed tomcat certificate.

   The **Certificate Details** dialog box is displayed.
5. Click **Download .PEM File**.
6. Save the .PEM file to your local drive.

To upload the self-signed tomcat certificates to the Unified CCX Tomcat trust store, do the following:

1. Sign in to the **Cisco Unified OS Administration** interface on the Cisco Unified CCX server.
2. Select **Security** > **Certificate Management**.

   The **Certificate List** window appears.
3. In the **Certificate List**, click **Upload Certificate/Certificate chain**.

   The **Upload Certificate/Certificate chain** dialog box appears.
4. From the **Certificate Purpose** drop-down list, select **tomcat-trust**.
5. In the **Upload File** field, click **Browse** and select the certificate.
6. Click **Upload File**.
7. In the CLI, restart the system using the command `utils system restart` for the changes to take effect.

Access Standalone Cisco Unified Intelligence Center Configuration

To access the Cisco Unified Intelligence Center standalone configuration webpage, perform the following steps:

Step 1 Click **System** > **Standalone CUIC configuration** to configure standalone Cisco Unified Intelligence Center.

Step 2 Enter **FQDN** (Fully Qualified Domain Name), **DataSource Name**, **Username**, and **Password** of standalone Cisco Unified Intelligence Center.

Step 3 Click **Save**.
If the configuration is successful, a status message appears. Otherwise, an error message appears.

Note Configurations may fail due to either of the following reasons:

- An error in input validation (DataSource Name, Username or Password).
- A failure in connectivity between Cisco Unified Intelligence Center and the Unified CCX servers.

License Information

License Management

From the Unified CCX Administration menu bar, select **Systems** > **License Management**. Based on the upgrade and usage scenarios, one of the following pages is displayed:

Page Displayed	Condition
License Management	For customers who have upgraded from Unified CCX Release 11.6(2) or earlier.
Classic License Management	For customers who have upgraded from Unified CCX Release 12.0.
Smart Licensing	This page is available only for the following customers: • Who want to migrate from Classic Licensing to Smart Licensing. • Who have newly installed Unified CCX Release 12.5.
Smart License Management	For customers who have enabled or migrated to Smart Licensing.

Use the **License Management** page to select the appropriate Unified CCX license. This page lists **Classic Licensing** and **Smart Licensing** options. By default, **Smart Licensing** is selected.

Select one of the licenses and click **Next**.

The **License Management** page is displayed for the first time after the upgrade. After you select one of the licenses, the **Classic License Management** page or the **Smart License Management** page is displayed respectively.

Classic License Management

Use this page to manage Classic License (Add, View, and Delete).

Add License

To add a new license, perform the following steps:

1. From the Unified CCX Administration menu bar, select **Systems** > **License Management**. The **Classic License Management** page is displayed.
2. On the **Classic License Management** page, in the **Add New License** section, click **Browse** to select the Unified CCX license file.
3. Select the appropriate license file and click **Upload**.

View License Information

On the **Classic License Management** page, you can view the license files and the details of the configured licenses in the **View Licenses** section. You can select an uploaded license from the **Licenses** drop-down list. When you select **Cumulative License Information** from the list, the following details are listed:

- **Configured Licenses**
  - Package
  - Total IVR Ports
  - Cisco Unified CCX Premium Seats
  - High Availability
  - Cisco Unified CCX Preview Outbound Dialer
  - Cisco Unified CCX Quality Manager Seats
  - Cisco Unified CCX Advanced Quality Manager Seats
  - Cisco Unified CCX Workforce Manager Seats
  - Cisco Unified CCX Compliance Recording Seats
  - Cisco Unified CCX Maximum Agents
- **Inbound**
  - Available Inbound IVR Ports
- **Outbound**
  - Cisco Unified CCX Licensed Outbound IVR Ports
  - Cisco Unified CCX Outbound IVR Ports In Use
  - Cisco Unified CCX Licensed Outbound Agent Seats
  - Cisco Unified CCX Outbound Agent Seats In Use

Note All the license details that are mentioned may not be displayed. The license details are displayed as per the procurement.

Delete Licenses

You can delete only temporary licenses. You cannot delete permanent licenses. To delete a temporary license, select the required license from the **Licenses** drop-down list and click **Delete**. Click **OK** in the confirmation dialog box.

Note It is a good practice to remove redundant or expired license files before you upload new ones. Remove old temporary license files (that are expired) from the server. For the changes to take effect, you must reboot Unified CCX after uploading or deleting the licenses.

Migrate to Smart Licensing

To migrate to smart licensing, on the **Classic License Management** page, click **Smart Licensing**.

Smart Licensing

Use this page to select and enable the appropriate **Smart License Type**. After you enable the required **Smart License Type**, from the next login, **Smart License Management** page is displayed. The license types that are listed and available for selection depends on the type of installation.

Step 1 Select one of the following license types:

- **Unified IP IVR**
- **Unified CCX**
  - **Lab**
    - **NPS**
    - **NFR**
  - **Production**
    - **Flex**
    - **Perpetual Enhanced**
    - **Perpetual Premium**

Note For more information on the license types, see Cisco Contact Center Ordering Guide.

Step 2 Click **Enable**.
A confirmation message is displayed.

Step 3 Click **Yes** to enable Smart Licensing.

What to do next

You must register this Product Instance with **Cisco Smart Software Manager** to use Smart Licensing.

Smart License Management

The **Smart License Management** page provides the summary and detailed information on system license usage as it is reported to **Cisco Smart Software Manager (Cisco SSM)** or **Cisco Smart Software Manager On-Prem (Cisco SSM On-Prem)**. Licenses are assigned to your Smart Account and are not node-locked to a device. That is, a single license can be used by multiple users but only one at a time.

Note **Not Node-Locked:** The same license can be used across multiple systems (nodes) but only on one node at a time.

Field	Description
Status	Displays the status of the actions that are performed on this page.
License Type Details	
Current License Type	Displays the type of license that was selected in the **Enable Smart Licensing** page. To select a different license type, click the link. The **Enable Smart Licensing** page is displayed.
License Control Displays the status of **Overage Allowance** that was configured while registering the product instance. After you register the product instance, a link is provided to update the **Overage Allowance**. **Overage Allowance** is enabled by default. You can update **Overage Allowance** only when the product instance is in the registered state. When you click the update link, the **License Control** window displays the following options:	
Current License Type	Displays the type of license that was selected in the **Enable Smart Licensing** page.
Overage Allowance	You can **Enable** or **Disable**. By default **Enable** is selected, which allows you to use more licenses than you have purchased. If you want to limit the usage of licenses to the purchased quantity or less, select **Disable**. Enter the number that you want to allow in the fields that are displayed as per the **Current License Type**. For more information on license types, see the *Overview* section of *Smart Licensing* chapter in *Cisco Unified Contact Center Express Features Guide*.
I have purchased High Availability License	If you have deployed a HA, this check box is displayed, which has to be selected.
Registration Information Displays the status of registration. If you have registered, the `You have registered successfully` message is displayed, else displays the procedure to register.	
Transport Settings	Use Transport Settings button to configure different settings through which Cisco Unified CCX can connect to Cisco SSM or Cisco SSM On-Prem.

Field	Description
Register	Use the Register button to register Cisco Unified CCX with Cisco SSM or Cisco SSM On-Prem. By default this button is disabled. You have to first configure **Transport Settings** to enable this button. After you successfully register, this button is disabled.
Smart License Details	
Registration Status	Displays the current registration status. The following are the statuses: • Registered • Unregistered or Unidentified • Unregistered-Registration Expired • Reservation In Progress • Registered - Specific License Reservation
Authorization Status	Displays one of the following status information: • Evaluation mode—Product is not registered with Cisco. • Evaluation Expired—Product evaluation period has expired. • In Compliance—Product is in authorized or in compliance state. • Not Authorized—Product is in not-authorized state. • Authorization Expired—Authorization has expired for the product. This issue usually occurs when the product has not communicated with Cisco for 90 consecutive days. After 90-days, the product instance is put into Enforcement state. • Out of Compliance—Product is in out-of-compliance state because of insufficient licenses. • Unidentified—Unable to determine current registration status. • Authorized-Reserved—License Reservation is enabled and the license usage is in-compliance state. • Not Authorized-Reserved—License Reservation is enabled, and the license usage is in out-of-compliance state.
Smart Account Name	Displays the Smart Account name. It is created from the **Request a Smart Account** option in **Administration** section of the software.cisco.com. It is the primary account that is created to represent the customer and all licenses of a company are assigned to this Smart Account. It also manages licenses of all Cisco products.
Virtual Account Name	Displays a self-defined construct to reflect the organization, which is created and maintained by the administrator on Cisco SSM or Cisco SSM On-Prem. Licenses and product instances can be distributed across virtual accounts.

Field	Description
Serial Number	Unique identifier of the product instance.
Export-Controlled Functionality	Displays one of the following status information: • Allowed—Cisco Unified CCX registered to Smart Account that allows export-controlled functionality. • Not Allowed—Cisco Unified CCX not registered to Smart Account that allows export-controlled functionality. Specifies if the Export-Controlled functionality was enabled in the token with which the product was registered. **Note** The Allow export-controlled functionality on the products that are registered with this token check box is not displayed for the Smart Accounts that are not permitted to use the Export-Controlled functionality.
Actions	This drop-down list gets activated after you successfully register the Smart License. It lists the following type of actions that can be performed: • Renew Authorization—Use this option to manually renew the authorization. The license authorization is renewed automatically every 30 days. If the product instance is not connected to Cisco SSM or Cisco SSM On-Prem, the authorization expires after 90 days. If you select the Cisco SSM On-Prem option, Cisco SSM On-Prem must have an internet connection to connect to Cisco SSM for authorization. • Renew Registration—Use this option to manually renew the registration. The initial registration is valid for one year. Registration is automatically renewed every six months, provided the product is connected to Cisco SSM or Cisco SSM On-Prem. If the Cisco SSM On-Prem option is selected, Cisco SSM On-Prem must have an internet connection to connect to Cisco SSM. • Reregister—When you select this option, the **Smart Licensing Product Registration** window is displayed. Enter the appropriate Product Instance Registration Token and click **Reregister**. • Deregister—Use this option to deregister Unified CCX from Cisco SSM or Cisco SSM On-Prem and release all the licenses from the current virtual account. All license entitlements that are used for the product instance are released to the virtual account and is available for other product instances. **Note** If Unified CCX is unable to connect to Cisco SSM or Cisco SSM On-Prem, and the product instance is deregistered, a confirmation message is displayed. This message notifies you to remove the product instance manually from Cisco SSM or Cisco SSM On-Prem to free up licenses.
License Usage	

Field	Description
License Name	Displays the different licenses as per the license type that is selected in the Smart Licensing page.
Reserved Count	Displays the number of licenses that are reserved. This column is displayed only when the specific License Reservation is enabled.
Reported Usage	Displays the number of licenses that are used by this product instance as per the details that was last reported.
Status	Displays the status of each license. The different statuses for the product instance are as follows: • Authorization Expired—The authorized period has expired. • Evaluation—This entitlement is in Evaluation mode. • Evaluation Expired—Evaluation period has expired. • In-compliance—In-compliance (authorized). • No License in Use—There are no licenses that are in use. • Invalid—In Error state. • Invalid Tag—The entitlement tag is invalid. • Not Applicable—Enforcement mode is not applicable. • Out of Compliance—Out-of-compliance (unauthorized). • Waiting—Waiting response from Cisco SSM or Cisco SSM On-Prem for entitlements that are submitted. • Authorized-Reserved—Reserved licenses are in-compliance. • Not Authorized-Reserved—Reserved licenses are out-of-compliance.

Configure Transport Settings for Smart Licensing

Configure the connection mode between Unified CCX and Cisco SSM.

Step 1 From Unified CCX Administration, navigate to **System** > **License Management**.

Step 2 Click **Transport Settings** to set the connection method.

Step 3 Select the connection method to Cisco SSM:

- **Direct**—Unified CCX connects directly to Cisco SSM on cisco.com. This is the default option.
- **Transport Gateway**—Unified CCX connects to Cisco SSM On-Prem for smart licensing. Enter the Cisco SSM On-Prem URL.
- **HTTP/HTTPS Proxy**—Unified CCX connects to a proxy server, which connects to Cisco SSM. Enter the Fully Qualified Domain Name (FQDN) of the proxy server along with the port.

Step 4 Click **Save** to save the settings.

Register with Cisco Smart Software Manager

The product instance has 90 days of evaluation period, within which, the registration must be completed. Else, the product instance gets into the enforcement state.

Register your product instance with Cisco SSM or Cisco SSM On-Prem to exit the Evaluation or Enforcement state.

Note After you register the product instance, you cannot change the license type. To change the license type, deregister the product instance.

Step 1 In , navigate to **Overview** > **Infrastructure Settings** > **License Management.**

Step 2 From Unified CCX Administration, navigate to **System** > **License Information**.

Step 3 Click **Register**.

Note
- Before you register the product instance, ensure to select the **License Type** and the communication mechanism in **Transport Settings**.

Step 4 In the **Smart Software Licensing Product Registration** dialog box, paste the product instance registration token that you generated from Cisco SSM or Cisco SSM On-Prem.

For information on generating the Registration Token, see the *Obtain the Product Instance Registration Token* section in Cisco Unified Contact Center Express Features Guide.

License Control pane is displayed with the **Overage Allowance** option. By default **Enable** is selected, which allows you to use more licenses than you have purchased.

If you want to limit the usage of licenses to the purchased quantity or less, select **Disable**. Enter the number that you want to allow in the fields that are displayed as per the **Current License Type**.

If you have deployed a HA, the **I have purchased High Availability License** check box is displayed, which has to be selected.

For more information on license types, see the *Overview* section of *Smart Licensing* chapter in *Cisco Unified Contact Center Express Features Guide*.

Step 5 Click **Register** to complete the registration process.

After registration, the **Smart Licensing Status** displays the following details.

Table 2: Smart Licensing Status

Smart License Status	Description
On Unsuccessful Registration	
Registration Status	Unregistered

Smart License Status	Description
License Authorization Status	Evaluation
Export-Controlled Functionality	Not Allowed
On Successful Registration	
Registration Status	Registered (Date and time of registration)
License Authorization Status	Authorized (Date and time of authorization)
Export-Controlled Functionality	Not Allowed
Smart Account	The name of the smart account
Virtual Account	The name of the virtual account
Product Instance Name	The name of the product instance
Serial Number	The serial number of the product instance

Entitlements are a set of privileges customers and partners receive when purchasing a Cisco service agreement. Using Smart Licensing, you can view the License consumption summary for the entitlements of different license types. The License consumption summary displays the License Name, Usage Count, and Status against each entitlement name.

License usage information is updated automatically every 15 minutes.

For more information, see *License Information*.

Language Information

Customized Unified CCX languages such as American English, Canadian French, and so on are installed with Unified CCX.

Use the Languages Configuration web page to:

- Enable languages that can be used to play prompts and grammars through Cisco Unified IP IVR.

Choose **System** > **Language Information** from the Cisco Unified CCX Administration menu bar to access the Languages Configuration web page. The Languages Configuration web page opens to display the following fields and buttons.

Field	Description
Choose IVR Language	

Field	Description
Language	You can choose a language that you wish to use with Unified IP IVR. You can select the language from the drop-down list. You can also specify the group and country-specific information for the language by selecting the desired radio button and check box respectively. Some languages have only one choice. US English (en_US) is the default. You may set the chosen language in **Set IVR Language** option. The chosen language doesn't get automatically set and the value is not persisted after it is chosen.
Set IVR Language	
IVR Language	This field is for setting the IVR language, which could be either one of the selected IVR languages or country-specific or a user-defined language entered using the **Edit** button. This is a mandatory field and you can choose from the drop-down list. Click **Edit** to add a new Language option. Default: English (United States) [en_US]

Logout Menu

To exit Unified CCXAdministration without closing your web browser, you can perform one of the following:

- Choose **System** > **Logout** from the Unified CCXAdministration menu bar.
- Click the **Logout** link displayed in the top right corner of any Cisco Unified CCX Administration web page.

The system logs you out of Unified CCX and displays the Unified CCX Authentication web page.

Note You can also exit Unified CCXAdministration by closing your web browser.