System Menu

The System menu of the Unified CCX Administration system provides options for performing system-related tasks. Depending on the product package you purchased, the System menu contains some or all of the following menu options:

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, IPv6 Address (for dual IPv4/IPv6), 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.

Procedure

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.
IPv6 Address (for dual IPv4/IPv6)	IPv6 address of the server that you want to add. **Note** This field is required only when IPv6 is enabled on the Unified CCX server.
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.

Configure IPv6 Address

Follow this procedure to configure IPv6 addressing.

Procedure

Step 1   On the **List Servers** page, click on the server name link to edit the server details.

The **Server Configuration** web page opens.

Step 2   Enter the IPv6 address or remove it in the **IPv6 Address (for dual IPv4/IPv6)** field.

Step 3   Click **Save** to add the IPv6 address.

What to do next

Login to **Cisco Unified CCX Serviceability** page and click **Tools**>**Control Center - Network Services**. Restart the **Cisco Unified Intelligence Center Reporting** service.

Note Eventhough the CTI ports are registered with dual stack or only with IPv6, this is displayed as IPv4 in the Call Manager.

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.

Related Topics

Configure Unified Communications Manager Information

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)	

Field	Description
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.
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.
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.
Application Parameters	

Field	Description
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.
Max Number of Executed Steps	The maximum number of steps an application can execute 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).

Field	Description
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.
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	

Field	Description
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.
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.
Context Service Parameters	
If there are any changes that are made in the Context Service Parameters, validate that the change is successfully reflected in the **Context Service Status** page before making any subsequent changes. The changes in the Request Timeout can be validated in the exported file from the **Context Service Status** page.	
Mode	Radio button to select the connection mode to connect with Context Service. • Lab • Production Default value is Production. **Note** Context Service in the Lab mode creates the data in the lab work group. When Context Service switches to the production mode, the data that is created in the lab work group will no longer be available in the production mode and conversely. Lab mode is a workgroup that is created for test and debug.
Request Timeout	The number of milliseconds (ms) the system should wait before rejecting the Context Service cloud connectivity. Default value is 5000 milliseconds. Range is from 200 to 5000 milliseconds.
Proxy Type	Determines if the Http proxy is used for Context Service connectivity. Default value is None.
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.

Field	Description
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	Context Service parameters and Proxy parameters changes are automatically notified to SocialMiner.
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.
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.

Field	Description
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.

Related Topics

Manage System Parameters

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`.

Procedure

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 executed operation. A **green** color icon indicates success in executed operation. A **grey** color icon indicates the inability to capture the status of the executed operation.

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 execute 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 normal 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.

Access Standalone Cisco Unified Intelligence Center Configuration

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

Procedure

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

Use the License Information web pages to display the cluster licensing information and to upload additional licenses.

Choose **System** > **License Information** > **Add License(s)** or **Display License(s)** from the Cisco Unified CCX Administration menu bar to access the License Information web pages.

Add Licenses

From the Unified CCXAdministration menu bar:

Procedure

Step 1 Choose **System** > **License Information** > **Add License(s)**.

The License Information web page displays.

Step 2 In the License File field, enter the path for the license file or click **Browse** to locate the license file. Select the required license file and click **Open**.

Use this page to specify a license file and upload it to Unified CCX.

Step 3 Click **Upload** to upload the license file to Unified CCX.

Display Licenses

From the Unified CCXAdministration menu bar:

Procedure

Choose **System** > **License Information** > **Display License(s)**.

The License Information web page opens, displaying the details of the Configured License such as the license type, number of IVR ports, number of seats, maximum number of agents, and so on.

Note The License Information page displayed on click of **Display License(s)** menu option will also specify the expiry date in case of time-bound licenses.

For Unified CCX, if you have a premium license with an outbound license, this web page will display:

- The number of licensed IVR ports and dedicated IVR ports for IVR outbound.

- The number of licensed agent seats and concurrent agent seats for progressive and predictive agent outbound.

| Note | The number of In Use IVR ports and In Use agent seats are displayed only for the master node. |

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	
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.