Manage General Settings

For Packaged CCE, Manage > Settings has two tabs: *General* and *Access*.

This chapter explains the tools on the *General* tab, which you use to manage general system settings: System Information, System Settings, System Deployment, and Agent Trace.

The tools on the *Access* tab are explained in Manage Administrators.

System Administrators have access to tools on the System menu. Unless a custom role gives them access, other administrators cannot use the System menu, and supervisors do not see this menu.

System Information

The System Information tool for Packaged CCE contains the General and Capacity Info tabs.

General

The General tab provides the following information:

- The deployment type.
- The software version of Unified CCE that is currently deployed.

Capacity Info

Open the Capacity Info tab to see a table that provides following capacity information:

Column	Description
Status	The status column shows where your system stands with respect to the capacity limit. The status icons are: • Green for 0-75% of capacity. • Yellow for 76-95%. • Orange for 96-99%. • Red for when you are at 100%.
Number of Configured	Shows the name of the object.
At Most	Shows the maximum capacity of each configurable object that is allowed.
Actual	Shows the number of objects currently configured on your system.
% Used	Shows the percentage of the maximum capacity represented by your configuration.

The **arrow** icon at the right of each row opens the tool where you can view, add, edit, and delete the objects to maintain the capacity, if you have access to that tool.

Peripheral Gateways

This display-only tool shows details about the peripheral gateways and peripherals in your deployment.

Click the **Site** tab to view the details of peripheral gateways and peripherals configured for that site.

Settings

The **Unified CCE Administration** > **System** > **Settings** tool has various tabs such as Global, Main Site, and the configured remote sites. Navigate to the required tab to configure the settings.

System Settings for Global

This tab contains the following sections:

- Congestion Control
- Agent
- Call Reporting
- Script

Congestion Control

You can review congestion control fields in this section. This section contains the following fields:

Field	Description
Congestion Control fields	• **Treatment Mode** This display-only field shows Treat call with DN default label. • **System Default Label** This display-only field is blank for Packaged CCE and Packaged CCE Lab Mode deployments. If your system was changed from another deployment type, this field retains the system default label for that deployment. • **Maximum Calls Per Second** This display-only field displays the current value for maximum calls per second for the deployment.

Agent

Enter values in this section to define system-level values for agents. This section contains the following fields:

Field	Required?	Description
Minimum Password Length	yes	Enter a value between 0 and 32 to set the minimum required length for passwords. Changing this value affects new passwords only and does not apply to existing ones.
Username Case Sensitivity	no	Check this check box to indicate that all usernames are case-sensitive. Leave it unchecked to indicate that case does not matter.

Call Reporting

Enter values in this section to define system-level values for calls. This section contains the following fields:

Field	Required?	Description
Bucket Interval	yes	Click the **magnifying glass** icon to display the popup list of configured bucket intervals. Select a bucket interval to use as the system default. You can change the bucket interval for individual call types, skill groups, and precision queues. (See Call Type, Skill Groups, and Precision Queues.)
Call Type	yes	Click the **magnifying glass** icon to display the popup list of configured call types. Select a call type to use as the system default. You can change the call type for individual Dialed Number.

Field	Required?	Description
Service Level Type	yes	From the drop-down menu, select an option to configure the default method by which the system software calculates the service level type. You can change the service level type for individual call types and precision queues. You have the following service level options: • **Ignore Abandoned Calls:** This selection excludes abandoned calls from the service level calculation. • **Abandoned Calls have Negative Impact:** Select this if you want only calls that are answered within the service level threshold time to be counted as treated calls. The service level is negatively affected by calls that abandon within the service level time. • **Abandoned Calls have Positive Impact:** Select this if you consider a call abandoned within the service level threshold time as a treated call. Abandoned calls have a positive impact on the service level.
Service Level Threshold	yes	Enter a value in seconds, from 0 to 2,147,483,647, for the maximum time that a caller spends in a queue before being connected to an agent. This value is used in reports to identify the percentage of calls that are answered within that time threshold, enabling you to see whether agents are meeting the target goal. Set the value to 0 seconds if you do not want a service level threshold to be set for calls. The value here sets the system default for service level threshold. You can change the value for individual call types and precision queues. (See Call Type and Precision Queues.)
Abandon Call Wait Time	yes	Enter a value in seconds (between 1 and 14400) to configure the minimum time an incoming call must be queued before the call is considered abandoned if the caller hangs up.
Answered Short Call Threshold	no	Enter a value in seconds (between 0 and 14400) to configure the maximum duration for a short call. Calls with a duration below that value are considered short. Set the threshold to factor out short calls from handle times.
Reporting Interval	yes	From the drop-down menu, select **15 Minutes** or **30 Minutes** to configure the system to store historical information in 15-minute or half-hour summaries. The Unified CCE PG sends these records to the Logger, which in turn writes them to the Central Database. Note that the 15-minute interval requires a larger amount of database space than the 30-minute interval.

Script

Use this section to set the number of retained script versions.

Field	Description
Script Versions to Retain	Enter a value from 1 to 100 to define the maximum number of versions of each routing script you want to maintain in the database. When you select a number, the system automatically deletes the oldest version when the limit is exceeded.

System Settings for Main Site

This tab contains the following sections:

- Agent
- Labels

Agent

Enter values in this section to define system-level values for agents. This section contains the following fields:

Field	Required?	Description
Desk Settings	yes	Click the **magnifying glass** icon to display the popup list of configured desk settings. This list shows only global desk settings. The desk settings you select will be the system default for all agents. You can change the desk settings for individual agents. (See Add and Maintain Agents.)
Agent Phone Line Control	yes	Select Single Line or All Lines to indicate whether all agents supported on the agent peripheral can have one or more than one line configured. **Important** • If you select All Lines, you must access Cisco Unified Communications Manager to set Busy Trigger to 1 and Max Number of Calls to 2 for each phone. Use the Unified Communications Manager Bulk Administration tool to change these settings for all agent devices. • If you change the Agent Phone Line Control setting, you must restart the peripheral gateways for the change to take effect. To restart the PGs, access the Unified CCE PG on Side A and Side B. Open Service Control and restart all PG services on Side A and Side B.

Labels

Use this section to view and edit labels for Unified CM, Outbound, and Unified CVP. This section contains the following fields:

Field	Description
Unified CM Label	This field contains a 10 digit string that matches the Unified CM route pattern.
Outbound Label	This field contains a 10 digit string that matches the IOS Voice Gateway dial-peer.

Field	Description
Unified CVP Label	This field contains a 10 digit string that matches the CVP dialed number pattern. When this label is used for all Unified CVP routing clients, the **Same Label for All Unified CVPs** check box is checked. To use a different label for each Unified CVP routing client, uncheck the **Same Label for All Unified CVPs** check box, and enter a 10 digit string in each routing client field.

System Settings for Remote Site

The system settings vary based on the type of peripheral gateways configured for a particular remote site.

PGs Configured	Settings
Agent	Agents, Unified CM Label
VRU	Unified CVP Label
Multichannel	Outbound Label

If a remote site has all the PGs configured, the settings options are same as that of Main Site. If it has a combination of two PGs configured, the respective combination of settings appears.

System Inventory for Packaged CCE 2000 Agents Deployment

Note The System Inventory shows IPv4 addresses only.

The System Inventory is a visual display of the machines in your deployment, including: Virtual Machine Hosts (ESXi servers), Virtual Machines (VMs) on Side A, VMs on Side B, External Machines, Gateways, and Cisco Virtualized Voice Browsers (VVB). You can access the System Inventory after you have completed the change to a Packaged CCE deployment.

Access the System Inventory by navigating to **Unified CCE Administration** > **System** > **Deployment**.

System Inventory contents are updated when you select or change the deployment type and after regular system scans. If a system scan detects VMs that do not conform to Packaged CCE requirements, the **Configure your deployment** pop-up window opens automatically, detailing the errors. You can access the System Inventory again after you have corrected the errors and completed the **Configure your deployment** pop-up window.

For more details about the Packaged CCE requirements, see **Server Status** pop-up window, see Monitor Server Status Rules , on page 15.

Restriction Departmental administrators cannot add, edit, or delete information in the System Inventory. Global administrators who are configured as "read-only" cannot add, edit, or delete information in the System Inventory.

Table 1: System Inventory Layout and Actions

Item	Notes	Actions
Validate	If a system scan detects an error or warning for validation rules, the **Validate** button appears above the Solution Inventory. After you have corrected the errors or warnings, click **Validate** to run an immediate scan and verify that you corrected the problem.	Click **Validate**.

Item	Notes	Actions
Side A	This panel shows all VMs on Side A.	The System Inventory displays read-only information for the following VMs: • **Unified CCE Rogger** • **Unified CCE PG** • **Unified CVP** • **Unified CM Subscriber 1**(if on-box) The following VMs are editable. Click the VM **pencil** icon to edit the following fields: • **Unified CCE AW-HDS-DDS**—Diagnostic Framework Service Domain, Username, and Password. • **Unified CM Publisher**(if on-box)—AXL Username and Password. These are the credentials for connecting to the Unified CM Publisher. • **CUIC-LD-IdS Publisher**—Username and Password for Unified Intelligence Center Administration. Username and Password for Identity Service Administration. • **Unified CVP Ops Console Server**—Username and Password for the System CLI. **Note** Updating the Unified CVP Operations Console Server initiates a scan for gateways. The pop-up window closes when the scan for gateways is finished. • **Finesse Primary**—Username and Password for Cisco Finesse Administration. You can launch the administration tool for these VMs by clicking the VM **arrow** icon: • **CUIC-LD-IdS Publisher** • **Unified CVP Ops Console Server** • **Finesse Primary**

Item	Notes	Actions
Side B	This panel shows all VMs on Side B.	The System Inventory displays read-only information for the following VMs: • **Unified CCE Rogger** • **Unified CCE PG** • **Unified CCE AW-HDS-DDS** • **Unified CVP** • **Unified CM Subscriber 2**(if on-box) • **Unified CVP Reporting** • **CUIC-LD-IdS Subscriber** • **Finesse Secondary** • **Enterprise Chat and Email**

Item	Notes	Actions
External Machines	This section shows all external machines in the deployment, and can include any of the following: **Note** • Unified CM Subscriber machines are dedicated to the contact center. When you configure an external Unified CM Publisher, its Unified CM Subscribers are added to the System Inventory automatically.	

Item	Notes	Actions
		You can add, edit, or delete External Machines as follows: **To add:** **1.** Click **Add External Machine**. **2.** Complete all required fields. • For all machines, enter the IP address, hostname, or fully qualified domain name (FQDN) of the machine in the **Hostname** field. **Note** The system does not support IP address change. Use the hostname if you foresee a change in IP address. This is applicable for all the **Hostname/ IP Address** fields. The system attempts to convert the value you enter to FQDN. • For SocialMiner, also enter the SocialMiner Administration Username and Password. The system validates the credentials, and then automatically enables and configures the **CCE Configuration for Multichannel** settings in SocialMiner Administration. These settings are used for both Agent Request and Task Routing. The system also automatically creates a Task feed in SocialMiner for Task Routing, including the associated campaign and Connection to CCE notification. For more information, see the *Cisco Packaged Contact Center Enterprise Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html. • For the Unified CM Publisher, also enter the AXL Username and Password.

Item	Notes	Actions
		The system validates the AXL information, connects to the Unified CM Publisher, and then automatically adds the Unified CM Subscribers to the System Inventory. **3.** Click **Save**. **To edit:** **1.** Click the machine **pencil** icon. **2.** Edit fields as needed. Click **Save**. **Note** If you edit the Unified CM Publisher, the Unified CM Subscribers associated with the publisher are updated automatically. You cannot edit Unified CM Subscribers from the System Inventory. **To associate the external HDS with a default Cisco Identity Service (IdS) for single sign-on:** **1.** Click the pencil icon on the external HDS. **2.** Click the Search icon next to **Default Identity Service**. **3.** Enter the machine name for the Cisco IdS in the Search field or choose the Cisco IdS from the list. **4.** Click **Save**. **To delete**, click the **x** on the machine. Confirm the deletion. **Note** If you delete the Unified CM Publisher, the Unified CM Subscribers are also deleted automatically, and the Configure Deployment pop-up window opens. Enter the name, IP address, AXL username, and AXL password for the Unified CM Publisher in your deployment. You can open the administration tool for these external machines by clicking the **arrow** icon in the machine box:

Item	Notes	Actions		
		• **Unified CM Publisher** • SocialMiner • **MediaSense**		
		Gateways		The System Inventory displays the read-only name and address for each gateway.

Item	Notes	Actions		
			The system scans for gateways every time you edit fields in the **Unified CVP Ops Console Server** pop-up window. It is common practice to add inbound gateway information (hostname, IP Address) in the CVP OAMP, but not to configure outbound gateway information. If both inbound and outbound gateways are configured in the CVP OAMP, the System Inventory displays gateway information used for inbound and outbound calls.	

Item	Notes	Actions
Cisco Virtualized Voice Browsers (VVB)	The system scans for Cisco VVBs every time you edit fields in the **Unified CVP Ops Console Server** pop-up window.	The System Inventory displays the read-only address and version for each Cisco VVB.

Note If you change the password of any of the Packaged CCE components, you must update the password in the respective VM in the system inventory.

Monitor Server Status Rules

In Packaged CCE 2000 Agents deployment, the Inventory displays the total number of alerts for machines with validation rules. Click the alert count to open the **Server Status** popup window, which lists all of the rules for that machine and indicates which have warnings and errors. Rules are grouped by these categories:

Server Status Category	Description	Example Rules
Configuration	Rules for installation and configuration of a component. These rules identify problems with mismatched configuration between components, missing services, and incorrectly configured services.	**Unified CCE Rogger:** The trace level must be set to normal to ensure performance. **Unified CVP:** The names of the SIP Server Groups on CVP containing Communications Manager addresses must match the Communications Manager Cluster Fully Qualified Domain Name.
Operations	Rules for the runtime status of a component. These rules identify services and processes that cannot be reached, are not running, or are not in the expected state.	**Unified CCE Rogger:** The central controller agent process (ccagent.exe) must be in service for both PGs. **Unified CVP:** The Diagnostic Portal, AXL, REST or SOAP service on this machine must be in service. **Note** Webex Experience Management and Call Transcript should be reachable on Network.

Server Status Category	Description	Example Rules
System Health	Metrics to monitor the CPU, memory, and disk usage of a component's Virtual Machine (VM) as reported by ESXi over the last 10 minutes. The memory and CPU usage may differ slightly from system tools reported by the VM itself. For VM Hosts, these metrics also include datastore performance information.	**All:** Memory usage as reported by ESXi - 17%
VM	VM requirements for a component.	**All:** VMware Tools must be up to date
System Validation	Rules for Unified CCE database and configuration settings. These rules identify whether the configuration of objects in your deployment match the requirements and limits for Packaged Contact Center Enterprise. **Note** The System Validation category is available only for the Side A Unified CCE AW-HDS-DDS.	**Side A Unified CCE AW-HDS-DDS:** Agent Desk Settings: Ring No Answer Times must not be set. **Side A Unified CCE AW-HDS-DDS:** Application Gateway **Side A Unified CCE AW-HDS-DDS:** Application Instance: Exactly 1 Application Instance must be defined and its application type must be <Other>.

Agent Trace

Enabling agent trace allows you to track and report on every state an agent passes through. You might enable agent trace if you have concerns about the productivity or performance of one or more agents.

Important Enabling trace can affect system performance, as it requires additional network bandwidth and database space. Typically, you use this feature for short-term tracking of specific agents. The system imposes a configuration limit on the number of agents for whom you can enable trace.

Use this tool to view, add, and remove agents for whom agent trace is enabled.

To add trace to an agent:

1. Navigate to **Unified CCE Administration** > **System** > **Agent Trace**.
2. Click **Add** to open the **Add Agents with Trace Enabled** popup window. Use the sort and search features to navigate the list.
3. Click one or more agent usernames to give them the trace-enabled status.
4. Close **Add Agents with Trace Enabled** to return to the list.
5. Click **Save** on the List window to confirm the trace status for the agents you added. Click **Revert** before you save to remove an agent from the Trace Enabled list.

To remove trace from an agent:

1. On the **List of Agents with Trace Enabled** window, locate the agent whose trace status you want to remove.
2. Click the **x** icon to clear trace status for that agent.
3. Click **Save** on the List window to confirm the removal. To cancel, click **Revert**.

Log Collection

Important Only set trace level to detailed and run log collection during off-peak hours. Do not run log collection during heavy call load.

Use the Log Collection tool to collect logs for these components:

- Unified CCE
- Unified CVP
- Unified Communications Manager
- Finesse
- Unified Intelligence Center

Unless limited by their role, administrators have full access to Log Collection. Supervisors have no access to this tool.

You can select individual or multiple components for log collection, and specify the start and end time for the logs. The maximum duration for log collection is eight hours. The logs for all selected components are consolidated into a single downloadable zip file. You can run one log collection at a time.

For most components, you can specify whether normal or detailed logs are collected using the **Trace Levels** option. Click **Trace Levels** to view the current trace level for each component and, if necessary, change it for future log collection.

The **Current Trace Level** for each component can be Normal, Detailed, or Custom. Custom indicates that the level has been set outside of **Unified CCE Administration** and does not match the Normal or Detailed settings for that component.

System wide trace levels are gathered periodically. If a trace level is changed outside of **Unified CCE Administration**, it may several minutes before the new trace level appears in the **Log Collection** tool.

To use Log Collection to debug a problem:

1. Change trace level to detailed by clicking **Trace Levels**, and selecting **Detailed** from the pull-down menus for the relevant components. Click **Update Trace Levels** to apply the changes.
2. Recreate the problem in your deployment or wait until the problem occurs again.
3. Return to the Log Collection tool and collect logs for the appropriate date and time interval, during which detailed trace level was selected. For example, if you set the trace level to detailed on 01/27/2014 at 09:00, you can collect detailed logs for intervals after that date and time. (See directions below.)
4. When you have finished debugging the problem, return the trace level to **Normal**.

To collect log files:

1. Navigate to **Unified CCE Administration** > **System** > **Log Collection**.
2. Check each component for which you want to collect logs, or check **All Components**.
3. Select a **Start Time** and **End Time** for log collection by clicking the **calendar** icon. Pick a date and time from the popup window, and then click anywhere outside the popup window to save your selection.
4. Click **Collect Logs**.

   The new log collection appears in the list with an **in progress** icon in the Status column. When the log collection is complete, its **download** and **trash can** icons are enabled automatically.

Note If errors are encountered during log collection, the Status column shows an **error** icon. Hover over the icon to view the tooltip which explains the error. If the Unified CCE Administration service restarts during log collection, a **cancelled** icon appears in the status column. You can delete log collections that have errors or have been cancelled; you cannot download these collections.

5. Click the **download** icon to download the log zip file.

To delete a stored log collection, click the **trash can** icon for that collection in the list.