Optional Configurations

Optional Configuration for Packaged CCE 2000 Agents Deployment

To configure optional components for Packaged CCE 2000 Agents deployment.

Task
Add and Maintain Remote Sites, on page 1
Add and Maintain External Machines, on page 5
Add PIMs to the Media Routing Peripheral Gateway, on page 15
Add Multichannel PIM to 2000 Agent Deployment, on page 16
Configure Email and Chat, on page 17
Configure Cisco Unified Customer Voice Portal Reporting Server
Configure VVB

Add and Maintain Remote Sites

You can add new remote sites to the 2000 Agents deployment type. Each remote site added appears as a separate tab. Click the + icon to open the **Add Remote Site** pop-up window. See Add Remote Site, on page 1 for more information.

Add Remote Site

Step 1 Navigate to **Unified CCE Administration** > **Infrastructure** > **Inventory**.

Step 2 Click the + icon to open the **Add Remote Site** page.

Step 3 On the **CCE PG** screen, enter the remote site information in the following fields:

Field	Description
Name	Enter a name for the site. Maximum length is ten characters. Valid characters are alphanumeric, period (.), and underscore (_). The first character must be alphanumeric. **Note** You cannot use the system reserved terms like core, main, and site.
Side A PG Hostname/ IP Address	Enter the hostname, IP address, or fully qualified domain name (FQDN) for Side A.
Side B PG Hostname/ IP Address	Enter the hostname, IP address, or fully qualified domain name (FQDN) for Side B.
Select PG Client Types to Configure	Select the required peripheral gateway client types. The subsequent screens appear as per the selected options. • If you select **Agent**, the **Unified CM** and **Finesse** screens appear. • If you select **VRU**, the **CVP** screen appears. • If you select **Multichannel**, the **Configure** screen appears.

Step 4 Click **Next**. The subsequent screens appear as per the selected PG client types.

Step 5 On the **Unified CM** page, you can either select an existing publisher or add a new one. If you select a publisher, the associated subscribers appear and you can select the subscriber details. To add a new publisher,

a) Select **Add a new CM Publisher**.
b) Enter the Hostname, Username, and Password.
c) Click **Save**.

Note You can add only one CM Publisher while creating a remote site.

Step 6 On the **Subscribers** section, select the following connection settings for the agent peripheral:

- Side A Connection
- Side B Connection
- Mobile Agent Codec

Step 7 Click **Next**.

Step 8 On the **Finesse** page, enter the Hostname, Username, and Password for the Finesse primary server.

Step 9 Click **Next**.

Step 10 On the **CVP** page, enter the Hostname/IP Address, Username, and Password of the Side A and Side B CVP Servers.

Step 11 Click **Next**.
The system performs the following Configuration tasks.

Component	Automated Configuration Tasks
Unified CCE PG	**Agent** • Downloads JTAPI from the Unified Communications Manager, and installs it on the Unified CCE PG. • Creates the CUCM Peripheral Gateway (PG) with the CUCM PIM. • Creates the CTI Server. **VRU** - Creates the VRU PG with two VRU PIMs. **Multichannel** - Creates the Multichannel PG.
Unified CCE Rogger	Updates the router configuration with the new PGs that are created as a part of the site.
Unified Communications Manager	• Creates the Application User that is used to configure the Agent PG.
Finesse	• Configures the CTI Server settings. • Configures the connection to the AW database.
Unified Customer Voice Portal	• Configures the Unified CVP Call Server components and adds them to the Main site Reporting Server. • Configures the Unified CVP VXML Server components. • Configures the Unified CVP Media Server components.

Note If one of the automated initialization tasks fail, the system reverts all the completed tasks.

Step 12 Click **Done** when all the tasks are complete. If there are configuration errors, you can click **Back** to edit the previous pages.

Step 13 For the configuration to take effect, do the following:

- Restart the router service.
- If you have selected the PG client type as VRU, restart the two newly configured CVP Call Servers .

What to do next

Note For all remote sites configured with Agent PG, you must add the Finesse Self Signed Certificate (if the solution does not have the CA certificate) to the AW Machine. For more information on how to add Finesse certificate to AW Machine, see the Import VOS Components Certificate .

Related Topics

Import VOS Components Certificate

Reconfigure Remote Site

Step 1 Navigate to **Unified CCE Administration** > **Infrastructure** > **Inventory**.

Step 2 Click the site you want to reconfigure.

Step 3 Click **Reconfigure** to open the **CCE PG** page.

Note You can only add PG client types.

Step 4 Click **Next** and proceed the same way as you add a new remote site.
Refer to Add Remote Site, on page 1 for more information.

Delete Remote Site

You can delete a remote site if the following are not associated to the remote site:

- Agents
- Teams
- Dialed Numbers
- Skill groups
- Routing Pattern
- SIP Server Groups
- Locations
- Script
- Dialer

Note Before deleting a remote site, you must stop all the services and processes running on the Cisco Finesse server of the remote site manually.

If remote sites has CVPs configured, make sure the following tasks are completed before deleting remote site:

- Dissociate CVP Server from CVP Reporting Server.
- If a site specific Reporting Server is used in Courtesy Call Back, replace the Reporting Server with another.
- Delete all Media Server associations with CVP.

Note Post deletion of remote site, delete the Packaged CCE ID from the ORM.properties file.

Step 1 Navigate to **Unified CCE Administration** > **Infrastructure** > **Inventory**.

Step 2 Click the remote site you want to delete.

Step 3 Click **Delete**.
A message appears asking if you are sure to delete the remote site.

Step 4 Click **Yes** to confirm.
The remote site disappears from the **Inventory** page.

Note The delete operation does not remove the remote site objects permanently from the database. If you want to recreate a site with same name, you must permanently delete these objects from **Configuration Manager** > **Tools** > **Miscellaneous Tools** > **Deleted Objects**.

Add and Maintain External Machines

Add External Machines

You can add the following external machines based on PG types configured on:

- Agent: None
- VRU: Unified CVP Reporting Server, Virtualized Voice Browser, Gateways, Media Server, and Unified SIP Proxy

Note For detailed steps on how to add a Media Server as an external machine, see Add Media Server as External Machine, on page 6

- Multichannel: Third-Party Multichannel, ECE Data Server (refers to ECE Data Server VM for 400 agents and Services Server VM for ECE 1500 agents), ECE Web Server, and Customer Collaboration Platform

If you are using any Multichannel applications (Customer Collaboration Platform, Enterprise Chat and Email, and Third-Party Multichannel), add them to the System Inventory external machines.

If your are using Webex Experience Management, then add Cloud Connect to the System Inventory external machine.

Before you begin

If you do not have a CA-signed certificate, import self-signed certificates for the external machines. For more information, see "Self-signed Certificates" section in *Packaged CCE Administration and Configuration Guide* .

Step 1 On the **Inventory** page, select the main site or remote site and in the **External Machines** section, click the + icon.

Step 2 Choose the machine type from the **Type** drop-down list.

Step 3 In the **Host Name** field, enter the hostname, IP address, or fully qualified domain name (FQDN) for the selected machine type.

Note The system attempts to convert the value you enter to FQDN.

Step 4 In the machine's **Administration** section, enter the administration username and password for the selected machine type.

Step 5 Click **Save**.

Note

- **Email and Chat:**
  - In Configuration Manager Tool, application instance and application path are to be created and associated to CUCM PG.
  - LDAP configuration needs to be done using Single Sign-On (for Partition Administrators) in the ECE Administration Web interface. For more information, see *Enterprise Chat and Email Administrator's Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-maintenance-guides-list.html.
- **VVB:**When you add VVB, the system will mark the machine as Out of Sync. Either wait for auto synchronization (which happens every 10 mins) or do manual synchronization.
- **Customer Collaboration Platform:**If you add Customer Collaboration Platform, the system automatically creates a Customer Collaboration Platform Task feed for Task Routing, including the associated campaign and Connection to CCE notification.

Add Media Server as External Machine

Step 1 In Unified CCE Administration, select **Infrastructure Settings** > **Inventory**.

Step 2 Select the main site or the remote site and in the **External Machines** section, click the + icon.

Step 3 In the **Add Machine** dialog box, complete the following fields:

Field	Required?	Description
Type	Yes	From the drop-down list, choose "Media Server".
Host Name/IP Address	Yes	Enter the hostname, IP address, or fully qualified domain name (FQDN) for the selected machine type. **Note** The system attempts to convert the value you enter to FQDN.
FTP		Configure FTP during off-peak hours. Do not do the configuration during heavy call load.
FTP Enabled	No	Indicates whether a Media Server has FTP enabled. A Media Server, which has FTP enabled, is automatically populated as a session variable to the VXMLServer. The (default) Agent Greeting recording application automatically uses the Media Servers in the inventory that have FTP enabled for the recording. If Microsoft FTP Service is not enabled in Windows Services Control Panel, then set it to Automatic and start the service.

Field	Required?	Description
Media Server Enabled **Note** Not applicable for external media servers.	No	Indicates whether CVP is a Media Server or not.
Anonymous Access	No	Indicates that this Media Server uses anonymous FTP access. In this case, the user name is specified as anonymous by default. The password field is not editable if you chose anonymous access.
Username and Password	No	These fields apply only if the FTP field is enabled and if the Anonymous Access field is disabled. In this case, enter the username and password.
Port	Yes	Enter a new port number or use the default port number (21).

Step 4 Click **Save**.

Note
- When a Media Server is added, configurations are propagated to all CVPs across sites.

Edit Machines

Edit Credentials

On the **Inventory** page, select the main site or a remote site and click the pencil icon to edit the following machines:

Machine	Editable Field
Unified CM Publisher	AXL Username and Password
Customer Collaboration Platform	Administration Username and Password
Enterprise Chat and Email and 3rd Party Multichannel	• Web Server: edit partition Administration User name and Password. • Data Server: none

Machine	Editable Field
Virtualized Voice Browser	Administration Username and Password A VVB can be set as a Principal VVB provided its Sync Status is "In Sync" and it supports Customer Virtual Assistant feature. To set a VVB as a Principal VVB, do the following: **Important** Do not perform any Customer Virtual Assistant configurations while setting a different VVB as a Principal VVB. **1.** Click **pencil** icon of the VVB. The **Edit Virtualized Voice Browser** window appears. **2.** Check the **Principal** check box. **3.** Enter Administrator username and password. **4.** Click **Save**.
Unified SIP Proxy	Administration Username and Password
Gateway	Administration Username and Password
Unified CVP Reporting	Windows Administration credentials
Cloud Connect	Administration Username and Password **Note** When a Cloud Connect is updated, configurations are propagated to all CVPs and Finesse across sites.
Media Server	FTP Enabled, Anonymous Access, FTP Credentials, and Port **Note** • When a Media Server is updated, configurations are propagated to all CVPs and across sites.

To delete an external machine on the main site or a remote site, click the **x** on the machine. Confirm the deletion.

Note

- You cannot delete the Virtualized Voice Browser and Unified SIP Proxy external machines if they are associated with a SIP Server Group. To delete these external machines, you must disassociate them from the SIP Server Group.
- You cannot delete the Gateway external machine if it is associated with Location. To delete this external machine, you must disassociate the Gateway from the Location.
- 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.
- When a Media Server is deleted, configurations are propogated to all CVPs across sites.

Update IP Address or Hostname

On the **Inventory** page, System and Config Administrators can update the IP address or hostname of the following machines.

- Core machines
- Optional machines

Note

- IP address/hostname change or rebuild can only be done from Side A AW machine. The AW machine credentials are shared with all CCE machines. Ensure that the Side A AW user is part of the local Administrators group on all CCE machines.
- If you have rebuilt a CCE_ROGGER or a CCE_AW, do not create a service account manually. Side A AW user account will be used as a service account for Logger and distributor services.
- While updating the inventory for routers in Unified CCE Administration, at least one side of the router needs to be running successfully if both the sides were rebuilt. If not, you must manually add the router on one side through the web setup.
- After updating the hostname in the virtual machine, regenerate and update CA or self-signed certificate on the machine. This should be done before updating the hostname in the inventory.

Related Topics

Update Core Machines, on page 9
Update Optional Machines, on page 10
Inventory File, on page 11

Update Core Machines

This procedure explains how to update the following Core machines:

In Main site: CCE_AW, CCE_ROGGER, CCE_PG, CVP, CM_PUBLISHER, CUIC_PUBLISHER (CUIC-LD-IDS co-resident), CUIC_SUBSCRIBER, FINESSE, and VM_HOST

In Remote site: CCE_PG, CVP, CM_PUBLISHER[1], CM_SUBSCRIBER, and FINESSE_PRIMARY

Note

- After updating the IP address or hostname in the Inventory for CVP, restart the CVP device.
- If you have changed the hostname of CCE_ROGGER in the virtual machine, restart the Apache Tomcat service on Side A AW. This should be done before updating the inventory with new hostname for CCE_ROGGER.

Before you begin

Disable auto discovery in the virtual machine. For more information, see Auto Discovery, on page 11.

Step 1 Navigate to the **Unified CCE Administration** > **Infrastructure** > **Inventory**.

Step 2 Choose **Update** > **Core Machines**.

Step 3 Click the **Download Present Inventory File** icon to get the Inventory File.

Step 4 Fill particulars in the Inventory File and save it. For more information, see Inventory File, on page 11

Step 5 Click the **Upload Updated Inventory File** icon to import the updated file.

Step 6 Click **Next** to start the inventory update process and see the progress of tasks.

- If the upload is successful, a green circle appears against each task.
- If the upload is unsuccessful, fix the errors that are shown and repeat steps 5 and 6.

Step 7 Click **Done**.

Update Optional Machines

This procedure explains how to update the following Optional machines:

CVVB, CVP_REPORTING, MEDIA_SERVER, GATEWAY, EXTERNAL_HDS, CUSTOMER_COLLABORATION_PLATFORM, CUSP, THIRD_PARTY_MULTICHANNEL, ECE, ECE_WEB_SERVER, CLOUD_CONNECT_PUB, CLOUD_CONNECT_SUB and THIRD_PARTY_GATEWAY.

Note After updating the IP address or hostname in the inventory for CVP Reporting Server, restart this device.

Before you begin

Disable auto discovery in the virtual machine. For more information, see Auto Discovery, on page 11.

Step 1 Navigate to the **Unified CCE Administration** > **Infrastructure** > **Inventory**.

Step 2 Choose **Update** > **Optional Machines**.

[1] Required only if it is already added in the Inventory as part of the same site.

Step 3 Click the **Download Present Inventory File** icon to get the Inventory File.

Step 4 Fill particulars in the Inventory File and save it. For more information, see Inventory File, on page 11

Step 5 Click the **Upload Updated Inventory File** icon to import the updated file.

Step 6 Click **Next** to start the inventory update process and see the progress of tasks.

- If the upload is successful, a green circle appears against each task.
- If the upload is unsuccessful, fix the errors shown, and repeat steps 5 and 6.

Step 7 Click **Done**.

Auto Discovery

Auto discovery is a process by which the inventory automatically detects and validates the change in IP address or hostname. You must disable auto discovery in the virtual machine before updating the IP address or hostname and enable it once the inventory update is complete. This procedure explains how to enable or disable auto discovery.

Note During Technology Refresh upgrade, auto discovery is disabled by default till all the core components are updated.

Step 1 Navigate to the **Unified CCE Administration** > **Infrastructure** > **Inventory**.

Step 2 Choose **Update** > **Auto Discovery**.

Step 3 If Auto Discovery Status is Enabled, click **Disable** to disable auto discovery.

Step 4 If Auto Discovery Status is Disabled, click **Enable** to enable auto discovery.

Note If you don't enable auto discovery, it gets enabled automatically after three days of disabling.

Step 5 Click **Done**.

Inventory File

The Inventory File in Packaged CCE 2000 Agent deployments contain the following fields.

Note If you are updating hostname for any of the following machines, restart Apache Tomcat service on all CCE_AW machines after the inventory update:

- CCE_AW
- FINESSE
- EXTERNAL_HDS
- CUIC

Table 1: Inventory File Details

Column	Description	Required for upload?	Editable field in downloaded inventory file	Permissible Values
name	Unique identifier for the machine	Yes	No	
machine Type	Machine Type	Yes	No	The following dependencies should be considered while updating the Inventory file. • Core machines should be updated together. • Update ECE and ECE_WEB_SERVER details together. • Update both publisher and subscriber details of a machine together. For example: CUIC_PUBLISHER and CUIC_SUBSCRIBER. • Update Side A and Side B details of a machine together. For example: CVP Side A and CVP Side B.
public Address	Public address	Yes	No	IP address or hostname of machines present in the inventory
private Address	Private address	Required for CCE_PG and CCE_ROGGER	No	IP address or hostname of machines present in the inventory
side	Side information	Yes	No	sideA sideB

Column	Description	Required for upload?	Editable field in downloaded inventory file	Permissible Values
connection Info	Connection information of the machine	Required for CCE_AW (Side A), CCE_PG (Side A), CM_PUBLISHER, CUIC_PUBLISHER, FINESSE (Side A), FINESSE_PRIMARY, ECE_WEB_SERVER, CVP, CVP_REPORTING, CUSP, GATEWAY, VM_HOST, CLOUD CONNECT PUBLISHER, CVVB, MEDIA_SERVER, CUSTOMER_ COLLABORATION_ PLATFORM ConnectionInfo is mandatory for the machines even if: • There is no IP address or hostname change. • The `isReinstalled` value is set to `No`.	Yes (only username and password are editable)	

Column	Description	Required for upload?	Editable field in downloaded inventory file	Permissible Values

				Enter the username and password in the following format:
				`userName=<user>&password=<password>`
				For AW, enter the username and password in the following format:
				`userName=<user@domain.com>&password=<password>`
				For information on the credentials of machines, see Table 4: Machine Credentials, on page 25.
				For CCE_PG update, provide the `userName` and `password` of CUCM application user.
				Note If you change the CUCM application user, ensure to update the inventory for both Side A and Side B CCE_PGs and set the `isReinstalled` value to `yes`. This makes sure that both sides of the PG machines have the same application user.
				Append the layout attribute to the username and password in the following format for VM_HOST:
				`userName=<user>&password=<password>;layout=<M3TRC or M4TRC or M5TRC or SPEC>`
				Note Provide Side A and Side B VMware ESXi server details in VM_HOST. Hardware layout is required only for Side A.
				For co-resident CUIC-LD-IDS, enter the username and password in the following format:

Column	Description	Required for upload?	Editable field in downloaded inventory file	Permissible Values
				`type=DIAGNOSTIC_PORTAL&userName=<CUIC username>&password=<CUIC password>;type=IDS&userName=<IDS username>&password=<IDS password>` **Note** • Replace Ampersand (&) or equal sign (=) in usernames or passwords with their respective URL-encoded values "%26" or "%3D". Semicolon (;) is a delimiter.
newpublic Address	new Public address	Yes	Yes	For IP address change: provide the new IP address. For IP address and hostname change: provide the new IP address. The new hostname is auto detected and updated in the inventory. For hostname change: provide the new IP address same as the old IP address. The new hostname is auto detected and updated in the inventory.
newprivate Address	new Private address	Required for CCE_PG and CCE_ROGGER	Yes	
is Reinstalled	is Reinstalled	Yes	Yes	Supported values are: `Yes`: if you are setting up a new virtual machine `No`: if you are using the existing virtual machine

Add PIMs to the Media Routing Peripheral Gateway

The Media Routing Peripheral Gateway (MR PG) is created during automated initialization.

Creating PIMs for the MR PG is optional. You can create the following PIMs on the Media Routing Peripheral Gateway:

- Outbound PIM

- Multichannel PIM for Customer Collaboration Platform
- Multichannel PIM for Enterprise Chat and Email (ECE)
- Multichannel PIM for a third-party multichannel application
- Multichannel PIM for Digital Routing

To create Dialed Numbers associated with the Multichannel PIMs, first do the following:

- Create the PIM using Peripheral Gateway Setup.
- Add an external machine in the Solution Inventory using the Unified CCE Administration System. Navigate to **Overview** > **Infrastructure** > **Inventory**. Scroll down and click **Add External Machine**.

Note If ECE Data Server is deployed on box, you do not need to create a Dialed Number associated with the PIM.

Note Refer to the *Cisco Packaged Contact Center Enterprise Features Guide* at https://www.cisco.com/en/US/products/ps12586/prod_maintenance_guides_list.html for directions on adding the Outbound PIM and the Multichannel PIMs.

Refer to the *Enterprise Chat and Email Installation Guide (for Packaged Contact Center Enterprise)* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html.

Add Multichannel PIM to 2000 Agent Deployment

Caution Before performing the step to enable the secured connection between the components, ensure that the security certificate management process is completed.

Before you begin

Only users who are part of the local Administrators group can run Peripheral Gateway setup.

Step 1 In the **Peripheral Gateway Component Properties** window, click **Add**.

Step 2 From the **Client Type** drop-down list, select **Media Routing**.

Step 3 From the **Available PIMS** list, select **MR PIM1**, then click **OK**.

Step 4 In the **Configuration** dialog box, check the **Enabled** check box.

Step 5 In the **Peripheral name** field, enter the peripheral name.

Step 6 In the **Peripheral ID** field, enter the logical controller ID of the Unified CCE component you are adding. The following are the names by which the Unified CCE components are represented in the database. Refer *Peripheral Gateway* page in CCE Admin to get the peripheral ID of the corresponding PIM.

- Name of Outbound is *Outbound*

- Name of ECE is *Multichannel*
- Name of CCP is *Multichannel2*
- Name of THIRD_PARTY_MULTICHANNEL is *MutliChannel3*
- Name of Digital Routing is *DigitalRouting*

Example:

If you are adding ECE, find the component of the name *Multichannel* in the database. Enter the logical controller ID of that component in the **Peripheral ID** field.

Step 7 In the **Application Hostname (1)** field, enter the hostname or the IP address of the ECE services server.

Step 8 In the **Application connection port (1)** field, enter the port number.

Note Use the port number that is on the ECE services server that PIM uses to communicate with the application. The default port is 38001.

Step 9 In the **Application Hostname (2)** field, leave the field blank.

Step 10 In the **Application connection port (2)** field, leave the field blank.

Step 11 In the **Heartbeat interval (sec)** field, enter `5`.

Step 12 In the **Reconnect interval (sec)** field, enter `10`.

Step 13 Check the **Enable Secured Connection** option.

This establishes a secured connection between the MR PIM and the application server.

Ensure that you provide the correct information in the application hostname(1) and Application Connection Port(1) fields.

Step 14 Click **OK**.

Configure Email and Chat

For the ECE configuration page to appear on the Unified CCE Administration, do the following:

Step 1 Configure LDAP in the **ECE Administration** Web Interface.

For more information, see Single Sign-On (for Partition Administrators) in the *Enterprise Chat and Email Administrator's Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-maintenance-guides-list.html.

Step 2 Accept the certificate in the **Unified CCE Administration**. Do the following:

a) Enter *https://<fqdn of ecewebserver>* in the address bar of the web browser.
b) Accept the certificate.
c) Reload the **Unified CCE Administration** page.

Optional Configuration for Packaged CCE 4000/12000 Agents Deployment

To configure optional components for Packaged CCE 4000 or 12000 Agents deployment.

Task
Remote Site, on page 18
Machines, on page 21
Peripheral Set, on page 34
Add PIMs to the Media Routing Peripheral Gateway, on page 15
Add Multichannel PIM to Packaged CCE 4000/12000 Agents Deployment, on page 33
Configure Email and Chat, on page 17
Configure Cisco Unified Customer Voice Portal Reporting Server
Configure VVB
Packaged CCE 4000 and 12000 Agent Supported Tools
Avaya Configurations, on page 37
ICM-to-ICM Gateway Configurations, on page 42

Remote Site

A remote site must have at least one peripheral set. Each remote site added appears as a separate tab.

Add and Maintain Remote Site

Step 1 Navigate to the **Unified CCE Administration** > **Infrastructure** > **Inventory**.

Step 2 Click the + icon to add a remote site.

Step 3 Enter the remote site name.

Step 4 Click **Download Template**.

Step 5 Fill the particulars in the file and save it.

Table 2: CSV Template Details

Column	Description	Required?	Permissible Values
name	Unique identifier for the machine	Yes	Name must start with an alphabet. Maximum length is limited to 128 characters. Valid characters are a-z, A-Z, 0-9, dot (.), underscore (_), or hyphen (-).
machineType	MachineType Enum name	Yes	Mandatory machines are: • CVP • FINESSE_PRIMARY • FINESSE_SECONDARY • CM_PUBLISHER • CM_SUBSCRIBER • CCE_PG Optional machines: • ECE (refers to ECE Data Server VM for 400 agents and Services Server VM for ECE 1500 agents) • ECE_WEB_SERVER • CVP_REPORTING • GATEWAY • CVVB • CUSP • THIRD_PARTY_ MULTICHANNEL • MEDIA_SERVER
publicAddress	Public address	Yes	Valid IP address or hostname

Column	Description	Required?	Permissible Values

connectionInfo	Connection information of the machine	Required for:
		• CUCM PUBLISHER
		• CVP
		• CVP REPORTING
		• CUSP
		• ECE WEB SERVER
		• EXTERNAL MEDIA SERVER
		• FINESSE PRIMARY
		• GATEWAY
			Enter the username and password in the following format:
			`UserName=<user>&password=<password>;`
			For details on the credentials of each component, see Edit Credentials, on page 25.
			Enabling CVP as a media server is optional. To enable CVP as the media server, append the following to the code snippet above:
			`mediaServer=<true or false>`
			Enabling FTP in a CVP server is optional. You can configure FTP only if CVP is enabled as a Media Server. To enable FTP, append the following to the code snippet above:
			`&ftpUserName=<ftp_username>`
			`&ftpPassword=<ftp_password>`
			`&ftpPort=<ftp_portnumber>`
			Example with both Media Server and FTP enabled:
			`userName=Windows_User_Name&`
			`password=Windows_Password;`
			`&mediaServer=true`
			`&ftpUserName=Sample_ftp_username>`
			`&ftpPassword=Sample_ftp_password>`
			`&ftpPort=20`
			To enable FTP in an external media server, add the following code snippet to the Connection Info column:
			`&ftpUserName=<ftp_username>`
			`&ftpPassword=<ftp_password>`
			`&ftpPort=<ftp_portnumber>`
			Note
			• Replace Ampersand (&) or equal sign (=) in usernames or passwords with their respective URL encoded values "%26" or "%3D".
			• Semicolon (;) delimits the Windows Administration credentials from FTP credentials.

privateAddress	Private address	Required for CCE_PG	Valid IP address or hostname
peripheralSetName	Peripheral set name	Required for PG, CUCM, Finesse, CVP	Name can start with an alphabet. Maximum length is limited to 10 characters. Valid characters are a-z, A-Z, 0-9, dot (.), or an underscore (_).

Column	Description	Required?	Permissible Values
side	Side information	Yes	sideA sideB

Step 6 Upload the file and click **Next**.

Step 7 Wait for validation to be completed and click **Done**.

During the validation, tasks are performed depending on the components defined in the CSV template.

If validation fails, then click **Back** to fix the issues in the file and upload it again.

The remote site that is created appears as a tab on the Inventory page.

Note
- Agent PG and PIMs are created only when Finesse and CUCM are present.
- Multichannel PGs are created. For adding PIMs, see the section "Add Multichannel PIM to Packaged CCE 4000/12000 Agents Deployment".
- VRU PG and PIMs are created only when CVP is present.
- Only one peripheral set must be created at a time.
- Live Data Configuration Services, TIP_PG and TIP_PG_TOS will be added in Machine_Service table only for Agent PG.

Related Topics

Add Multichannel PIM to Packaged CCE 4000/12000 Agents Deployment, on page 33

Delete Remote Site

Before you begin

To delete a remote site, you must:

- Delete all the SIP server groups, routing patters, and locations associated with the remote site.
- Delete the peripheral sets associated with the remote site.
- Disassociate CVP Reporting Server from CVP Server and courtesy callback.

Step 1 Navigate to **Unified CCE Administration** > **Infrastructure** > **Inventory**.

Step 2 Select the remote site you want to delete and click **Delete** > **Current Site**.
The remote site is deleted from the inventory.

Machines

You can configure machines for the main sites and remotes sites in the 4000 Agents and 12000 Agents deployment type.

Add and Maintain Machines

Before you begin

If you do not have a CA-signed certificate, import self-signed certificates for the external machines. For more information, see "Self-signed Certificates" section in *Packaged CCE Administration and Configuration Guide* .

Step 1 Navigate to the **Unified CCE Administration** > **Infrastructure** > **Inventory**.

Step 2 Go to **Import** > **Device** to add a machine.

Step 3 Click **Download Template**.

Step 4 Fill the particulars in the file and save it.

Table 3: CSV Template Details

Column	Description	Required?	Permissible Values
name	Unique identifier for the machine	Yes	Name must start with an alphabet. Maximum length is limited to 128 characters. Valid characters are a-z, A-Z, 0-9, dot (.), underscore (_), or hyphen (-).

Column	Description	Required?	Permissible Values
machineType	MachineType Enum name	Yes	Mandatory machines are: • AW • HDS • ECE (refers to ECE Data Server VM for ECE 400 agents and Services Server VM for ECE 1500 agents) • ECE_WEB_SERVER • CVP • CVP_REPORTING • CM_PUBLISHER • CM_SUBSCRIBER • FINESSE • FINESSE_PRIMARY • FINESSE_SECONDARY • GATEWAY • CVVB • CUSP • CUSTOMER_COLLABORATION_PLATFORM • THIRD_PARTY_MULTICHANNEL • MEDIA_SERVER • CLOUD CONNECT PUBLISHER • THIRD_PARTY_GATEWAY **Note** You can add Cloud Connect Publisher only in the main site. **Note** • HDS, AW, CUIC_SUBSCRIBER are only applicable for the main site. • Add FINESSE and CM together.
publicAddress	Public address	Yes	Valid IP address or hostname

Column	Description	Required?	Permissible Values

connectionInfo	Connection information of the machine	Required for:
		• CLOUD CONNECT PUBLISHER
		• CUCM PUBLISHER
		• CVP
		• CVP REPORTING
		• CUSP
		• ECE WEB SERVER
		• EXTERNAL HDS
		• EXTERNAL MEDIA SERVER
		• FINESSE PRIMARY
		• GATEWAY
		Note If you edit the Cloud Connect Publisher, the Cloud Connect Subscribers associated with the publisher are updated automatically. You cannot edit Cloud Connect Subscribers from the System Inventory.
			Enter the username and password in the following format:
			`UserName=<user>&password=<password>;`
			For details on the credentials of each component, see Table 4: Machine Credentials, on page 25.
			Enabling CVP as a media server is optional. To enable CVP as the media server, append the following to the code snippet above:
			`mediaServer=<true or false>`
			Enabling FTP in a CVP server is optional. You can configure FTP only if CVP is enabled as a Media Server. To enable FTP, append the following to the code snippet above:
			`&ftpUserName=<ftp_username>`
			`&ftpPassword=<ftp_password>`
			`&ftpPort=<ftp_portnumber>`
			Example with both Media Server and FTP enabled:
			`userName=Windows_User_Name&`
			`password=Windows_Password;`
			`&mediaServer=true`
			`&ftpUserName=Sample_ftp_username>`
			`&ftpPassword=Sample_ftp_password>`
			`&ftpPort=20`
			To enable FTP in an external media server, add the following code snippet to the Connection Info column:
			`&ftpUserName=<ftp_username>`
			`&ftpPassword=<ftp_password>`
			`&ftpPort=<ftp_portnumber>`
			Note
			• Replace Ampersand (&) or equal sign (=) in usernames or passwords with their respective URL encoded values "%26" or "%3D".
			• Semicolon (;) delimits the Windows Administration credentials from FTP credentials.

privateAddress	Private address	Required for CCE_PG	Valid IP address or hostname
peripheralSetName	Peripheral set name	Required for CUCM, Finesse, CVP	Name can start with an alphabet. Maximum length is limited to 10 characters. Valid characters are a-z, A-Z, 0-9, dot (.), or an underscore (_).

Column	Description	Required?	Permissible Values
side	Side information	Yes	sideA sideB

Step 5 Upload the file and click **Next**.

Step 6 Wait for validation to be completed and click **Done**.

During the validation, tasks are performed depending on the components defined in the CSV template. For more information about the tasks, see Automated Initialization Tasks for 4000 and 12000 Agent Deployments.

If validation fails, then click **Back** to fix the issues in the file and upload it again.

Related Topics

Automated Initialization Tasks for 4000 and 12000 Agent Deployments

Edit Machines

Edit Credentials

You can edit the credentials of any machine using this procedure.

Step 1 On the **Inventory** page, click the main site or a remote site to edit the following machines:

Table 4: Machine Credentials

Machine	Editable Field
AW	Diagnostic Framework Service Domain, Username, and Password You can also set a Principal AW machine in 4000 and 12000 Agent deployments. The credentials must be the same for all CCE machines.
Live Data	Administration Username and Password
Finesse	Administration Username and Password
Customer Collaboration Platform	Administration Username and Password
ECE Web Server	Application Instance, Partition Administration Username, and Password

Machine	Editable Field
Virtualized Voice Browser	Administration Username and Password A VVB can be set as a Principal VVB provided its Sync Status is "In Sync" and it supports Customer Virtual Assistant feature. To set a VVB as a Principal VVB, do the following: **Important** Do not perform any Customer Virtual Assistant configurations while setting a different VVB as a Principal VVB. **a.** Click the VVB to open the **Edit VVB** window. **b.** Check the **Principal** check box. **c.** Click **Save**.
CUSP	Administration Username and Password
CUIC Publisher	Administration Username and Password
CVP	Windows Administration Username and Password, Enable Media Server, FTP Enabled, Anonymous Access, FTP Credentials, and Port **Note** When a CVP (which acts as a Media Server) is updated, Media Server configurations are propagated to all other CVPs across sites.
Gateway	Administration Username and Password
CVP Reporting	Windows Administration Username and Password The **Deploy** check box initializes the CVP Reporting Server configuration. Initialization removes the existing call server association and Courtesy Callback configuration. To reassociate the call servers with the CVP Reporting server, see Configure Unified CVP Reporting Server. To reconfigure Courtesy Callback, see Courtesy Callback.
IDS Publisher	Administration Username and Password
Media Server	FTP Enabled, Anonymous Access, FTP Credentials, and Port **Note** • When a Media Server is updated, configurations are propagated to all CVPs across sites.
Unified CM Publisher	AXL Username and Password

Machine	Editable Field
Cloud Connect Publisher	Administration Username and Password **Note** If your are using Webex Experience Management, then add Cloud Connect to the System Inventory external machine. When a Cloud Connect Publisher is updated,configurations are propagated to all CVPs and Finesse across sites.
External HDS	Diagnostic Framework Service Domain, Username, and Password

Step 2 Edit the credentials.

If successful, you can see the message on the **Inventory** page; else, fix the errors that are shown before clicking **Save**.

Update IP Address or Hostname

On the **Inventory** page, System and Config Administrators can update the IP address or hostname of the following machines:

- Core machines
- Peripheral Set machines
- Optional machines

Note

- IP address/hostname change or rebuild can only be done from Principal AW machine. Ensure that the Principal AW user is part of the local Administrators group on all CCE machines.
- If you have rebuilt a CCE_ROGGER or a CCE_AW, do not create a service account manually. Side A AW user account will be used as a service account for Logger and distributor services.
- After updating the hostname in the virtual machine, upload the CA certificates or import the self-signed certificates into the machine. This should be done before updating the hostname in the inventory.

Related Topics

Update Core Machines, on page 27
Update Peripheral Set, on page 36
Update Optional Machines, on page 28
Auto Discovery, on page 11
Inventory File, on page 29

Update Core Machines

This procedure explains how to update the following Core machines:

CCE_AW, CCE_ROGGER, CCE_ROUTER, CCE_LOGGER, CUIC_PUBLISHER, CUIC_SUBSCRIBER, IDS_PUBLISHER, IDS_SUBSCRIBER, and LIVE_DATA

Note If you have changed the hostname of CCE_ROGGER or CCE_ROUTER in the respective virtual machines, restart the Apache Tomcat service on Principal AW. This should be done before updating the inventory with new hostname for these machines.

Step 1 Navigate to the **Unified CCE Administration** > **Infrastructure** > **Inventory**.

Step 2 Choose **Update** > **Core Machines**.

Step 3 Click the **Download Present Inventory File** icon to get the Inventory File.

Step 4 Fill particulars in the Inventory File and save it. For more information, see Inventory File, on page 29.

Step 5 Click the **Upload Updated Inventory File** icon to import the updated file.

Step 6 Click **Next** to start the inventory update process and see the progress of tasks.

- If the upload is successful, a green circle appears against each task.
- If the upload is unsuccessful, fix the errors shown, and repeat steps 5 and 6.

Step 7 Click **Done**.

Update Optional Machines

This procedure explains how to update the following Optional machines:

CVVB, CVP_REPORTING, MEDIA_SERVER, GATEWAY, EXTERNAL_HDS, CUSTOMER_COLLABORATION_PLATFORM, CUSP, THIRD_PARTY_MULTICHANNEL, ECE, ECE_WEB_SERVER, CLOUD_CONNECT_PUB, CLOUD_CONNECT_SUB and THIRD_PARTY_GATEWAY.

Note
- Before updating the IP address or hostname for Cloud Connect Subscriber, disable auto discovery in the virtual machine. For more information, see Auto Discovery, on page 11.
- After updating the IP address or hostname in the inventory for CVP Reporting Server, restart this device.

Step 1 Navigate to the **Unified CCE Administration** > **Infrastructure** > **Inventory**.

Step 2 Choose **Update** > **Optional Machines**.

Step 3 Click the **Download Present Inventory File** icon to get the Inventory File.

Step 4 Fill particulars in the Inventory File and save it. For more information, see Inventory File, on page 29.

Step 5 Click the **Upload Updated Inventory File** icon to import the updated file.

Step 6 Click **Next** to start the inventory update process and see the progress of tasks.

- If the upload is successful, a green circle appears against each task.

- If the upload is unsuccessful, fix the errors shown, and repeat steps 5 and 6.

Step 7 Click **Done**.

Inventory File

The Inventory File in Packaged CCE 4000 and 12000 Agent deployments contain the following fields.

Note

- While updating the inventory file, ensure to refer to the Machine Dependencies, on page 31.
- If you are updating hostname for any of the following machines, restart Apache Tomcat service on all CCE_AW machines after the inventory update:
  - CCE_AW
  - FINESSE
  - EXTERNAL_HDS
  - CUIC

Table 5: Inventory File Details

Column	Description	Required for upload?	Editable in downloaded inventory file?	Permissible Values
name	Unique identifier for the machine	Yes	No	
machine Type	Machine Type	Yes	No	
public Address	Public address	Yes	No	IP address or hostname of machines present in the inventory
private Address	Private address	Required for CCE_PG, CCE_ROGGER, CCE_ROUTER, and CCE_LOGGER	No	IP address or hostname of machines present in the inventory
side	Side information	Yes	No	sideA sideB

Column	Description	Required for upload?	Editable in downloaded inventory file?	Permissible Values
connection Info	Connection information of the machine	Required for CCE_AW, CCE_PG (Side A) CM_PUBLISHER, CUIC_PUBLISHER, FINESSE_PRIMARY, ECE_WEB_SERVER, CVP, CVP_REPORTING, CUSP, GATEWAY, IDS_PUBLISHER, LIVE_DATA, EXTERNAL_HDS, CLOUD CONNECT PUBLISHER, CVVB, MEDIA_SERVER, CUSTOMER_ COLLABORATION_ PLATFORM ConnectionInfo is mandatory for the machines even if: • There is no IP address or hostname change. • The `isReinstalled` value is set to `No`.	Yes (only username and password are editable)	Enter the username and password in the following format: `userName=<user>&password=<password>` Replace Ampersand (&) or equal sign (=) in usernames or passwords with their respective URL-encoded values "%26" or "%3D". For information on the credentials of machines, see Table 4: Machine Credentials, on page 25. For CCE_PG update, provide the `userName` and `password` of CUCM application user. **Note** If you change the CUCM application user, update the inventory for both Side A and Side B CCE_PGs and set the `isReinstalled` value to `yes`. This makes sure that both sides of the PG machines have the same application user.
newpublic Address	new Public address	Yes	Yes	For IP address change: provide the new IP address For IP address and hostname change: provide the new IP address. The new hostname is auto detected and updated in the inventory. For hostname change: provide the new IP address same as the old IP address. The new hostname is auto detected and updated in the inventory.
newprivate Address	new Private address	Required for CCE_ROUTER, CCE_LOGGER, CCE_ROGGER,CCE_PG	Yes	

Column	Description	Required for upload?	Editable in downloaded inventory file?	Permissible Values
is Reinstalled	is Reinstalled	Yes	Yes	Supported values are: `Yes`: if you are setting up a new virtual machine `No`: if you are using the existing virtual machine

Machine Dependencies

Detailed below are some of the machine dependencies which should be considered while updating the inventory file.

Note Each row in the table below specifies machines types that are dependent on each other. So, whenever you update a machine, ensure to provide other dependent machine types from the same row.

Dependent Machine Types
CCE_AW (include all AWs), CCE_ROGGER[2], CCE_LOGGER, and CCE_ROUTER[3]
CCE_PG, CM_PUBLISHER[4], CM_SUBSCRIBER, FINESSE_PRIMARY, and FINESSE_SECONDARY
CCE_PG and CVP (include all CVPs in the peripheral set)
ECE and ECE_WEB_SERVER

2 Applicable for 2000 and 4000 Agent deployments.
3 Logger and Router are applicable only for 12000 Agent deployments.
4 To be updated only if the publisher is already a part of the peripheral set.

Note

- Provide both publisher and subscriber details of a machine together. For example: CUIC_PUBLISHER and CUIC_SUBSCRIBER.
- Provide Side A and Side B details of a machine together. For example: CVP Side A and CVP Side B.
- If you are updating the IP address/hostname or rebuilding a CCE_PG, provide details of all PG client types (configured in the system), and dependent machine types in the inventory file. For example: If VRU and Multichannel PGs are configured in the system, provide side A and side B details for both the PGs and all CVP machines.
- If only MR PG is configured in the system, provide side A and side B details of this PG in the inventory file.

Delete Machine

You can delete the following machine types:

- CCE_AW
- HDS
- CVP_REPORTING
- CUIC_SUBSCRIBER
- CUSP
- GATEWAY
- CVVB
- EXTERNAL_THIRD_PARTY_MULTICHANNEL
- DC_EXTERNAL_THIRD_PARTY_MULTICHANNEL
- MEDIA_SERVER
- CLOUD CONNECT PUBLISHER
- THIRD_PARTY_GATEWAY

Note

- When a Cloud Connect Publisher is deleted, the corresponding Cloud Connect Subscriber is also deleted.
- You cannot delete the Principal VVB.
- When a Media Server is deleted, configurations are propagated to all CVPs across sites.

Step 1 To delete a machine individually, select that particular row and click **Delete (X)** icon at the end of the row.

Step 2 Click **Yes**.
If the deletion is successful, then a message is displayed that the machine was deleted successfully. If the deletion fails, then check the error message and resolve the issue before attempting to delete again.

Add PIMs to the Media Routing Peripheral Gateway

The Media Routing Peripheral Gateway (MR PG) is created during automated initialization.

Creating PIMs for the MR PG is optional. You can create the following PIMs on the Media Routing Peripheral Gateway:

- Outbound PIM
- Multichannel PIM for Customer Collaboration Platform
- Multichannel PIM for Enterprise Chat and Email (ECE)

- Multichannel PIM for a third-party multichannel application
- Multichannel PIM for Digital Routing

To create Dialed Numbers associated with the Multichannel PIMs, first do the following:

- Create the PIM using Peripheral Gateway Setup.
- Add an external machine in the Solution Inventory using the Unified CCE Administration System. Navigate to **Overview** > **Infrastructure** > **Inventory**. Scroll down and click **Add External Machine**.

Note If ECE Data Server is deployed on box, you do not need to create a Dialed Number associated with the PIM.

Note Refer to the *Cisco Packaged Contact Center Enterprise Features Guide* at https://www.cisco.com/en/US/products/ps12586/prod_maintenance_guides_list.html for directions on adding the Outbound PIM and the Multichannel PIMs.

Refer to the *Enterprise Chat and Email Installation Guide (for Packaged Contact Center Enterprise)* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html.

Add Multichannel PIM to Packaged CCE 4000/12000 Agents Deployment

Caution Before performing the step to enable the secured connection between the components, ensure that the security certificate management process is completed.

Before you begin

Only users who are part of the local Administrators group can run Peripheral Gateway setup.

Step 1 In the **Peripheral Gateway Component Properties** window, click **Add**.

Step 2 From the **Client Type** drop-down list, select **Media Routing**.

Step 3 From the **Available PIMS** list, select **MR PIM1**, then click **OK**.

Step 4 In the **Configuration** dialog box, check the **Enabled** check box.

Step 5 In the **Peripheral name** field, enter the peripheral name.

Step 6 In the **Peripheral ID** field, enter the logical controller ID of the Unified CCE component you are adding. The following are the names by which the Unified CCE components are represented in the database. Refer PG explorer tool using Configuration Manager to get the Peripheral ID of the corresponding PIM.

- Name of Outbound is *Outbound*
- Name of ECE is *MR1*
- Name of CCP is *MR2*

- Name of THIRD_PARTY_MULTICHANNEL is *MR3*
- Name of Digital Routing is *MR4*

Example:

If you are adding ECE, find the component of the name *MR1* in the database. Enter the logical controller ID of that component in the **Peripheral ID** field.

Step 7 In the **Application Hostname (1)** field, enter the hostname or the IP address of ECE services server.

Step 8 In the **Application connection port (1)** field, enter the port number.

Note Use the port number that is on the ECE services server that PIM uses to communicate with the application. The default port is 38001.

Step 9 In the **Application Hostname (2)** field, leave the field blank.

Step 10 In the **Application connection port (2)** field, leave the field blank.

Step 11 In the **Heartbeat interval (sec)** field, enter `5`.

Step 12 In the **Reconnect interval (sec)** field, enter `10`.

Step 13 Check the **Enable Secured Connection** option.

This establishes a secured connection between the MR PIM and the application server.

Ensure that you provide the correct information in the **Application Hostname(1)** and **Application Connection Port(1)** fields.

Step 14 Click **OK**.

Peripheral Set

Peripheral set is a collection of all components that are dependent on the peripheral gateway (including the peripheral gateway itself).

For example, Cisco Finesse, CVP. A main or remote site can have zero or more peripheral sets that are associated with it.

You can add a remote site even with a single VVB. This is helpful in getting control over the traffic, and keeping it local to the same data center.

For example, PSTN delivers SIP trunk to both the Data Centers (DCs). You must retain the traffic local to each DC. If the traffic is delivered to DC1, select the VVB and Nuance Speech Server (NSS) from DC1. If the traffic is delivered to DC2, select the VVB and NSS from DC2. This is achieved by adding a remote site only with VVB. From the VVB, NSS points to the SPOG.

Add and Maintain Peripheral Set

Step 1 Navigate to the **Unified CCE Administration** > **Infrastructure** > **Inventory**.

Step 2 Go to **Import** > **Peripheral Set** to add a peripheral set.
The **New Peripheral Set** wizard opens.

Step 3 Click **Download Template**.

Step 4 Fill the particulars in the file and save it.

Table 6: CSV Template Details

Column	Description	Required?	Permissible Values
name	Unique identifier for the machine	Yes	Name must start with an alphabet. Maximum length is limited to 128 characters. Valid characters are a-z, A-Z, 0-9, dot (.), underscore (_), or hyphen (-).
machineType	MachineType Enum name	Yes	Mandatory machine is CCE_PG. Optional machines are: • CVP • FINESSE_PRIMARY • FINESSE_SECONDARY • CM_PUBLISHER • CM_SUBSCRIBER • MEDIA_SERVER
publicAddress	Public address	Yes	Valid IP address or hostname

connectionInfo	Connection information of the machine	Required for CM_PUBLISHER, FINESSE_PRIMARY, ECE_WEB_SERVER, CVP, CVP_REPORTING, CUSP, GATEWAYand LIVE_DATA	Enter the username and password in the following format:
			`userName=<user>&password=<password>`
			Enabling CVP as a Media Server and configuring FTP is optional.
			Append the Media Server and FTP attributes to the username and password in the following format:
			`userName=<user>&password=<password>; mediaServer=<true or false>&ftpUserName=<ftp_username> &ftpPassword=<ftp_password> &ftpPort=<ftp_portnumber>`
			For more information on the FTP attributes, see FTP Section in the Add Media Server as External Machine, on page 6.
			Note • Replace Ampersand (&) or equal sign (=) in usernames or passwords with their respective URL encoded values "%26" or "%3D".
			• Semicolon (;) delimits the Windows Administration credentials from FTP credentials.
			• You can configure FTP only if CVP is enabled as a Media Server.

Column	Description	Required?	Permissible Values
privateAddress	Private address	Optional	Valid IP address or hostname
peripheralSetName	Peripheral set name	Required for PG, CUCM, Finesse, CVP	Name can start with an alphabet. Maximum length is limited to 10 characters. Valid characters are a-z, A-Z, 0-9, dot (.), or an underscore (_). **Note** Name must be unique. It cannot be reused even after that peripheral set is deleted.
side	Side information	Yes	sideA sideB

Step 5 Upload the file and click **Next**.

Step 6 Wait for validation to be completed and click **Done**.

During the validation, tasks are performed depending on the components defined in the CSV template.

If validation fails, then click **Back** to fix the issues in the file and upload it again.

Note
- Agent PG and PIMs are created only when Finesse and CUCM are present.
- Multichannel PGs are created. For adding PIMs, see the section "Add Multichannel PIM to Packaged CCE 4000/12000 Agents Deployment".
- VRU PG and PIMs are created only when CVP is present.
- Only one peripheral set must be created at a time.
- Live Data Configuration Services, TIP_PG and TIP_PG_TOS will be added in Machine_Service table only for Agent PG.

What to do next

Perform the PG configuration. For details, see the section "Configure Cisco Unified Contact Center Enterprise PG".

Related Topics

Add Multichannel PIM to Packaged CCE 4000/12000 Agents Deployment, on page 33

Update Peripheral Set

This procedure explains how to update the following peripheral set machines:

CCE_PG, CM_PUBLISHER, CM_SUBSCRIBER, FINESSE_PRIMARY, FINESSE_SECONDARY, and CVP

Note After updating the IP address or hostname in the Inventory for CVP, restart the CVP device.

Step 1 Navigate to the **Unified CCE Administration** > **Infrastructure** > **Inventory**.

Step 2 Go to **Import** > **Device** > **Add Machine** to add a machine to a peripheral set.
The **Add Machine** wizard is displayed.

Step 3 Click **Download Template**.
The .csv template is downloaded.

Step 4 Fill the particulars in the .csv template file and save it in the local folder. For more information, see Add and Maintain Peripheral Set, on page 34.

Step 5 Upload the .csv template file and click **Next**.

Step 6 Click **Done**.

Delete Peripheral Set

You can delete peripheral sets associated with the main site or remote sites.

Before you begin

To delete a peripheral set, you must delete:

- agents, skill groups, teams, and dialed numbers associated with it.
- all Media Server associations with CVP.

Step 1 Navigate to **Unified CCE Administration** > **Infrastructure** > **Inventory**.

Step 2 Select the peripheral set from main or remote site that you want to delete and click **Delete** > **Peripheral Set**.
The **Delete Peripheral Set from <site name>** popup window appears.

Step 3 Select a peripheral set from the **Peripheral Set** drop-down list.

Step 4 Click **Delete**.

Step 5 Click **Back** to delete another peripheral set. Else, click **Done** to return to the Inventory page.

Avaya Configurations

Note

- If you do not have a CA certificate, import self-signed certificates for Avaya PGs. For more information, see Self-signed Certificates.

The following table outlines the Avaya configuration tasks in Packaged CCE 4000 and 12000 Agent deployments.

Sequence	Avaya Configuration Tasks
1	In the PG Explorer tool, add Avaya Peripheral Gateway (with Avaya (Definity)) as the client type. For more information, see the section *Peripherals and Trunk Groups* in the *Configuration Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.
2	Configure Peripheral Gateway Setup Configure and Setup Avaya Peripheral Gateway, on page 39
3	Set up CTI Server
4	Set up CTI OS Server and CTI Desktop Client For information, see sections *CTI OS Server Installation* and *CTI Toolkit Desktop Client Installation* in the *CTI OS System Manager Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.
5	Restart Live Data for Avaya PG, on page 42

Note For detailed information about the required Avaya configurations, see chapter *Unified ICM Software Configuration* in the *Cisco Unified ICM ACD Supplement for Avaya Communication Manager Guide* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_12_0_1/Reference/Guide/ucce_b_cisco-unified-icm-acd-supplement-1201.html.

Related Topics

Routing Target Selection
Packaged CCE 4000 and 12000 Agent Supported Tools

Add Users to Local Security Group

Before you begin

Only Packaged CCE configuration users who have been added to the UcceConfig group in all the local distributors can access the Configuration Manager.

Step 1 Click **Server Manager** > **Tools** > **Computer Management**.

Step 2 Select **Local Users and Groups**.

Step 3 Double-click **Groups**.

Step 4 Right-click **UcceConfig**. Select **Properties**.

Step 5 Click **Add** and enter the user name in the **Edit the object names to select** text box. Click **Check Names** to validate the user name.

Step 6 After the user name is successfully validated, click **OK**.

Step 7 Click **Apply** and **OK** in the **Properties** dialog box.

Step 8 Close the **Computer Management** and **Server Manager** windows.

Configure Peripheral Gateway Setup Configure and Setup Avaya Peripheral Gateway

Before you begin

Only users who are part of the local Administrators group can run Peripheral Gateway setup.

Step 1 Open the **Peripheral Gateway Setup** tool from Unified CCE Tools on the desktop.

Step 2 Click **Add** in the **Instance Components** section.

Step 3 Click **Peripheral Gateway**.

Step 4 Complete the following steps in the Peripheral Gateway Properties dialog box.

a) Choose **Production Mode**. Do not set the Auto Start feature until after the installation is complete.
b) Specify whether the PG is part of a duplexed pair.
c) In the ID field, select from the drop-down list the PG device number as enabled in the Router.
d) If the PG is duplexed, specify whether you are installing Side A or Side B. If the PG is simplex, select Side A.
e) In the **Client Type Selection** section of the window, select the client type:

- For a CUCM PG: CUCM
- For a MediaRouting PG: MediaRouting
- For a VRU PG: VRU
- For a UCC Enterprise Gateway PG: UCC Enterprise Gateway

For an Avaya PG: Avaya (Definity)

Step 5 Click **Add**, and then click **Next**.

Step 6 Enter the Logical Controller ID generated while configuring the PG in the **PG Explorer** tool. Click **Add** and select **PIM 1** from the list. Click **OK**.

Step 7 Configure the PG properties:

a) To put the PIM into service, check the **Enabled** option. Enabling the PIM allows it to communicate with the peripheral when the Peripheral Gateway is running.
b) Enter the peripheral name in the **Peripheral name** field. Usually, the enterprise name from the associated Peripheral record is the most appropriate name to use. When creating peripheral names, use short descriptive names and keep the length to a minimum.
c) Enter the Peripheral ID in the **Peripheral ID** field. This is the ID that you created when you configured the PG in the PG Explorer tool.
d) For CUCM PG:

1. Enter the **Agent extension length**.
2. In the CUCM Parameters section, in the **Service** field, provide the IP address of the CUCM.
3. Enter the credentials of Application User that you created in CUCM.
4. Select the appropriate **Mobile Agent Codec**, and click **OK**.

e) For MR PG:

- To add MR PG for ECE:
  1. In the **Application Hostname (1)** field, enter the hostname or the IP address of the ECE services server. If you have installed two services servers for high availability, provide the information for the primary service server on Side A.
  2. In the **Application Connection Port (1)** field, enter the port number on the ECE services server that the PIM will use to communicate with the application. The default port is 38001.
  3. In the **Application Hostname (2)** and **Application Connection Port (2)** fields, enter the hostname or the IP address of the secondary ECE services server VM and port number on Side B.

     Note Set these values only if you have installed two services servers for high availability.

- To add MR PG for Customer Collaboration Platform:
  1. In the **Application Hostname (1)** field, enter the hostname or the IP address of the Customer Collaboration Platform.
  2. By default, Customer Collaboration Platform accepts the MR connection on Application Connection Port 38001. The Application Connection Port setting on Customer Collaboration Platform must match the setting on the MR PG as specified in the **Application Connection Port (1)** field.
  3. Leave the **Application Hostname (2)** and **Application Connection Port (2)** fields blank.

- To add MR PG for Digital Routing service:
  1. In the **Application Hostname (1)** and **Application Hostname (2)** fields, enter the hostname or the IP address of the Cloud Connect publisher and subscriber, respectively.

     Note Ensure to configure the **Application Hostname(1)** field to the network-nearest Cloud Connect. For example, if PIM-A is closer to the Cloud Connect publisher node, you must enter the IP address or hostname of the Cloud Connect publisher node in the **Application Hostname(1)** field and the IP address or hostname of the Cloud Connect subscriber node in the **Application Hostname (2)** field when configuring side "A".

  2. In the **Application Connection Port (1)** and **Application Connection Port (2)** fields, retain the default port number, that is 38001, which is the fixed port for the Digital Routing service.

- To add MR PG for Outbound Option:
  1. In the **Application Hostname (1)** field, enter the hostname or the IP address of the BA_IP Dialer.
  2. In the **Application Connection Port (1)** field, enter the connection port for the BA_IP Dialer. Otherwise, accept the default port number (38001) on the application server machine that the PIM uses to communicate with the application.

- To add MR PG for any third-party application:
  1. In the **Application Hostname (1)** field, enter the hostname or the IP address of the multichannel application server machine.
  2. In the **Application Connection Port (1)** field, enter the port number on the application server that the PIM will use to communicate with the application. The default port is 38001.
  3. If two applications interact with the Unified CCE, in the **Application Hostname (2)** field, enter the hostname or the IP address of the second application server machine. If you are using the hostname, the name must be in the hosts file.
  4. For two applications that interact with the Unified CCE, in the **Application Connection Port (2)** field, enter the port number on the second application server machine that is used by the PIM.

The below steps are common for any application server:

1. For **Heartbeat Interval** (seconds), specify how often the PG checks its connection to the call server. Use the default value.
2. For **Reconnect Interval** (seconds), specify how often the PG should try to reestablish a lost connection to the call server. Use the default value.
3. Check the **Enable Secured Connection** checkbox to enable secured connection.

   Enable Secured Connection establishes a secured connection between MR PIM and Application Server.

   Ensure that you provide the correct information in the Application Hostname(1) and Application Connection Port(1) fields.

f) For VRU PG:

1. In the **VRU host name** field, enter the name by which the VRU is known to the network.
2. In the **VRU connect port** field, enter the number of the VRU connection port that the PG connects to.
3. In the **Reconnect interval (sec)** field, specify how often, in seconds, the PG tries to re-establish a lost connection to the VRU. The default value is usually appropriate.
4. In the **Heartbeat interval (sec)** field, specify how often, in seconds, the PG checks its connection to the VRU. The default value is usually appropriate.
5. In the **DSCP** field, use the drop-down box to override the default value and set it to the desired DSCP value. The list of DSCP values in the drop-down box are the same as what are used during setup for connection between the Peripheral Gateway (PG) and the CallRouter. On an existing VRU PG system, this registry key does not exist. In that scenario, the PIM code uses CS3 as the default value when the VRU PIM process is activated.
6. Check the **Enable Secured Connection** checkbox to enable secured connection.

   This establishes a secured connection between VRU PIM and CVP.

Step 8 Configure PIM.

For more information, see *Cisco Unified ICM ACD Supplement for Avaya Communication Manager* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-technical-reference-list.html.

Step 9 Click **OK**.

Step 10 From the **Peripheral Gateway Component Properties** window, click **Next**. The **Device Management Protocol Properties** window appears.

a) Enter the appropriate settings and click **Next**. The **Peripheral Gateway Network Interfaces** window appears.

b) Configure the Private Interface and Public interfaces and click **Next**.

Note:

For the address input fields, use Fully Qualified Domain Names instead of IP addresses.

When there are two IP addresses configured on the public Network Interface Card (for IP-based prioritization), manually add two A-records on the DNS server. One A-record is for the high priority IP address and the other one is for the general priority IP address. The host part of the two DNS entires should be different from the hostname of Windows server. Use the new DNS entries to configure the public interfaces. This note applies to the Router and to all PG machines.

Step 11 In the **Check Setup Information window**, verify the setup information and click **Next**.

Step 12 When the **Setup Complete** window appears, click **Finish** .

Note When you add new PG, ensure that the PG ID is provided in the Router configuration. Provide the number that is assigned to the PG in the Enable Peripheral Gateway field in Web Setup

Restart Live Data for Avaya PG

When a new peripheral gateway that supports Live Data is deployed and started, its feed will not be available to the Live Data server automatically. Restart the Live Data server to start the feed from the newly deployed Peripheral Gateway.

Access the Live Data CLI and run the following command:

utils system restart

Note Restarting Live Data server impacts all CCE components.

ICM-to-ICM Gateway Configurations

The following table outlines the ICM-to-ICM Gateway configuration tasks in Packaged CCE 4000 and 12000 Agent deployments.

Sequence	ICM-to-ICM Gateway Configuration Tasks
1	Configure ICM-to-ICM Gateway For more information, see *ICM to ICM Gateway User Guide for Unified CCE* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html

Sequence	ICM-to-ICM Gateway Configuration Tasks
2	Remote ICM type application gateway global settings, on page 43

Related Topics

Routing Target Selection
Packaged CCE 4000 and 12000 Agent Supported Tools

Remote ICM type application gateway global settings

The configuration for Remote ICM Type Application Gateway can be performed by using **Configuration Manager** > **List Tools** > **Application Gateway List** > **.**

Following are the Remote ICM type Application Gateway global settings.

Table 7: Remote ICM type Application Gateway Global Setting

Name	Value
Abandon Timeout.	5000
ApplicationGatewayType	1
DateTimeStamp	NULL
ChangeStamp	0
ErrorThreshold	10
HeartbeatLimit	2
HeartbeatRetry	200
HeartbeatTimeout	300
HeartbeatInterval	15000
ID	2
LateTimeout	400
LinkTestThreshold	2
OpenTimeout	500
RequestTimeout	500
SessionRetry	30000
SessionRetryLimit	0

Optional Configuration for Packaged CCE Lab deployment

Remote Sites in Lab Mode

You can create remote sites in lab mode deployment. If you initiate your lab mode in simplex, you can create remote sites only with Side A machines.

Before you begin: If you do not have a CA-signed certificate, import self-signed certificates for all components. For more information, see "Self-signed Certificates" section in *Packaged CCE Administration and Configuration Guide* .

To add a remote site in lab mode deployment, see Add and Maintain Remote Sites, on page 1.

When you configure the simplex or duplex lab mode deployment, you can also add the following external machines for a remote site:

- Unified CM Publisher
- Unified CVP Reporting Server
- Unified SIP Proxy
- Virtualized Voice Browser
- Gateway
- Enterprise Chat and Email
- Third-party Multichannel
- Media Server

Note You can add Customer Collaboration Platform and Cloud Connect only in the main site.

To add, edit or delete the external machines on the remote site, see Add External Machines, on page 5 and Edit Credentials, on page 7 sections.

For more information on the configuration limits for external machines, see the *Solution Design Guide for Cisco Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html.