CCE Orchestration

Overview

The Orchestration feature provides partners and administrators an option to automatically download software updates and simplify the installation and rollback processes. The Orchestration framework is built within the Cloud Connect server that connects to the Cisco hosted cloud software repository. This framework provides the ability to check and download new software updates as and when they are available and notify the administrators via email about the new updates along with the release notes. Orchestration currently supports installation and rollback of Cisco Engineering Specials (ES), Service Updates (SU), Minor Releases (MR), and Microsoft Patches.

Email Notification

The Cloud Connect server checks for new software updates daily at a predefined time. When the new software updates are available, an email notification is sent. This email notification consists of available software updates details along with the release notes and is triggered to the administrators who have subscribed for it.

Email notifications are also sent to provide updates on the success and failure of any upgrade, rollback, or switch forward procedure. These notifications include details such as:

- Specific nodes on which the upgrade, rollback, or switch forward is initiated.
- Cloud Connect server name from where the procedure is triggered.
- Time (Cloud Connect server time) at which the procedure is started.
- Details about build versions of the respective nodes. For example, for an upgrade procedure, it shows both the version from which it is upgraded (FromVersion) and the version to which it is upgraded (ToVersion).
- Status of the procedure for respective nodes to indicate whether the procedure is successful or has failed; the subject line of the email indicates the overall status: success, failure, or partial success.

Cloud Connect server downloads the available software from Cisco software repository every day at the configured time. Email notification is triggered from Cloud Connect server to subscribed users with software download failure details. Also, Cisco software artifactory will trigger an email notification with entitlement or compliance failure details to the email address mapped to CCO ID that is used to generate the Artifactory API key.

Note

- If the option "All nodes" is selected during the upgrade, an email notification is sent about the success or failure at each stage of upgrade.
- The name of the deployment is shown in the subject line of the email, depending on the configuration in the inventory file.
- For patch install or rollback, email notifications are not sent to indicate whether the procedure is successful or if it is a failure.

Orchestration in CCE Deployment

The Orchestration feature is part of the Cloud Connect node that is configured in the CCE deployment.

To access this feature, Cloud Connect must be added to the inventory in the Unified CCE Administration console.

For more information, see *Initial Configuration for Cloud Connect* section in the *Cisco Unified Contact CenterEnterprise Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-maintenance-guides-list.html.

System Requirements

Cloud Connect 12.5(x) is obsolete. Cloud Connect 12.6(x) is required.

VOS Component Upgrade

Refer below for the minimum software version required to enable this feature for the following components:

- Finesse
- CUIC/LD/IDS/Co-resident
- VVB

Apply the ES **ucos.orchestration.enable-12.5.1.cop.sgn** on the above-mentioned components with 12.5(1) version to on-board and orchestrate VOS nodes from Cloud Connect server.

Note The ES **ucos.orchestration.enable-12.5.1.cop.sgn** must be applied on both the publisher and subscriber target nodes. This Mandatory ES is not required for onboarding the above-mentioned components with 12.6(x) version. After you install this ES on target VOS node, you will not be able to run commands in the same session. You must restart the session on target nodes to use the Orchestration CLI commands.

Note

- Before you begin the VOS node upgrade from 12.6(1) to 12.6(2), check if the **ucos.keymanagement.v02.cop.sgn** is applied on the base version. If not, you must install it; else the upgrade will fail. Restart the VOS node after installing **ucos.keymanagement.v02.cop.sgn**.
- Before you begin the VOS node upgrade from 12.5(1) to 12.6(2), check if the **ucos.keymanagement.v01.cop.sgn** is applied on the base version. If not, you must install it; else the upgrade will fail. Restart the VOS node after installing **ucos.keymanagement.v01.cop.sgn**

Windows Component Upgrade

Manually install mandatory ES23 on Unified CVP 12.5 (1) and ES66 on Unified ICM 12.5 (1) to onboard and orchestrate Windows nodes from Cloud Connect server.

Note For 12.5(1) Windows and VOS nodes, ES is required to onboard and orchestrate from Cloud Connect server. Mandatory ES is not required for onboarding target Windows and VOS components with 12.6(x) version.

Orchestration Support using Cloud Connect Server

Cloud Connect 12.6(x) supports orchestration in the following scenarios:

- Unified CCE 12.5(x) ES, Unified CCE 12.6(x) ES and Windows Updates can be orchestrated from Cloud Connect 12.6(x)
- Unified CCE 12.5(x) to Unified CCE 12.6(x), software upgrade can be orchestrated from Cloud Connect 12.6(x)

See System Requirements, on page 2 for minimum software requirement to enable orchestration for the above supported model.

Parallel Running of CLI

Parallel running of same or different CLIs on Cloud Connect server is disabled for Orchestration. However, parallel running of CLIs is allowed for the following commands:

- set cloudconnect orchestration config
- show cloudconnect orchestration config
- utils image-repository show
- utils deployment compatibility-check
- utils deployment show in-progress
- utils system inventory export
- utils system inventory import
- utils deployment show progress-HA

- email configuration-related commands, see Configure Email Notification.
- utils set software-download time
- utils set software-download bandwidth

Orchestration Deployment Task Flow

CLI to configure artifactory URL and API key, on page 7
Generate the Artifactory API Key, on page 5
CLI to configure proxy for orchestration, on page 6
Onboard VOS Nodes to Orchestration Control Node, on page 11
Onboard Windows nodes to orchestration control node, on page 12
Add Deployment Type and Deployment Name, on page 14
Validate Onboarded Nodes for Orchestration, on page 14
Configure Email Notification, on page 15
Configure Windows Server for Updates (Optional), on page 17

Administration Task Flow

Check Installed Software Version and Patches, on page 17
Install or Rollback Patch or Upgrade Cloud Connect Server , on page 18
List Available Patches for Specific Node or Group of Nodes, on page 19
Install Patch to Specific Node or Group of Nodes, on page 19
Roll Back Patch from Specific Node or Group of Nodes, on page 20
Install Windows Updates to Specific Node or Group of Nodes, on page 21
Roll Back Windows Update from Specific Node or Group of Nodes, on page 23
Enable or Disable Compatibility Enforcement, on page 24
Initiate maintenance mode for a specific node(s), on page 25
List Available Upgrade Options , on page 26
Upgrade a Specific Node or Group of Nodes or All Nodes , on page 26
Perform Switch Forward on Specific VOS Node or Group of Nodes , on page 28
Roll Back Upgrade from Specific Node or Group of Nodes, on page 28
Check Last Known Orchestration Operation Status on Remote Node, on page 30
Check Status, on page 29
Start Unified ICM Services, on page 30

Maintenance Task Flow

Deployment Tasks

Generate the Artifactory API Key

To generate the Artifactory API Key, follow the steps below:

Note It is mandatory for the CCO ID used to generate API keys to have necessary software upgrade entitlements. The CCO ID used by the partner or customer should have a valid SWSS (service contract) or Flex subscription in order to have the necessary entitlement.

- Login to https://devhub-download.cisco.com/console/ using your CCO Username and Password.
- Navigate to '**Manage Download Key** page.
- Click Generate Key option to Generate the API key. Option to **View** and **Revoke** Key is available in **Manage Download Key** page.
- Click on the Copy option to copy the API key to the clipboard.

Note You must log into https://devhub-download.cisco.com/console once every six months to extend the validity of the API key.

Note Cisco recommends not to use the same Artifactory API key generated by a single CCO ID across multiple deployments. For multiple deployments such as test, pre-production, production, and so on, generate the Artifactory API key for each deployment using different CCO IDs. Artifactory API key generated by a single CCO ID can be used in both publisher and subscriber of Cloud Connect in a single deployment.

CLI to configure proxy for orchestration

You can enable proxy configuration for orchestration to check and fetch updates from the Cisco-hosted cloud artifactory.

To configure the proxy for orchestration, run the **set cloudconnect orchestration config** command. To view the proxy configured for orchestration, run the **show cloudconnect orchestration config** command.

Table 1: Set Command Table

Command	**set cloudconnect orchestration config**
Description	This command enables the proxy configuration for orchestration to check and fetch updates from the Cisco-hosted cloud artifactory.
Expected Inputs	In the *Proxy Configured* prompt, enter **Yes** to enable the proxy or **No** to turn-off the proxy. If you choose to enable the proxy, you will be prompted to enter the Proxy Host and Proxy Port details. **Note** • Proxy Host should be the proxy server FQDN or IP address. • Proxy is turned off by default. • Orchestration supports only HTTPS proxy.
Expected Outcome	This CLI enables or turns-off the proxy for orchestration based on user input.

Note You can run this command only from the publisher node of the Cloud Connect server. The proxy configuration replicates automatically from the publisher node to the subscriber node when the **set cloudconnect orchestration config** command is run successfully on the publisher node.

Table 2: Show Command Table

Command	**show cloudconnect orchestration config**
Description	This command displays the proxy configuration for orchestration to check and fetch updates from the Cisco-hosted cloud artifactory.
Expected Inputs	NA

Expected Outcome	Proxy Host and Proxy Port details will be displayed if proxy is enabled.

CLI to configure artifactory URL and API key

Cisco hosts all the software artifacts in a cloud-based artifactory. The Cloud Connect server uses this artifactory to download and notify new updates.

Configure the Cloud Connect server with Cisco-hosted software Artifactory URL, Repository Name, and API Key. Run the command **utils image-repository set**. Refer to the **Set Command** table.

To view the configured Artifactory URL, Repository Name, and API Key in the Cloud Connect server, run the command **utils image-repository show**. Refer to the **Show Command** table.

Note You can run the **utils image-repository set** command only in the publisher node of the Cloud Connect server. The replication of image repository configuration occurs automatically from the publisher node to the subscriber node when you run this command with successful results on the publisher node.

Note Before running the command **utils image-repository set** on the CLI, access the link https://software.cisco.com/download/eula and accept the End User License Agreement (EULA)

Table 3: Set Command Table

Command	**utils image-repository set**

Description	

This command allows you to configure the Cisco hosted software Artifactory URL, Artifactory Repository Name, and API Key. For information on API Key, refer to the Generate the Artifactory API Key section. This command validates the below:

- If the Cisco.com ID used to generate the API key has entitlement to download the Cisco Contact Center software.
- If the EULA is signed by the Cisco.com ID that generates the API key.
- If the Cisco.com ID that generates the API key has the customer company's full address that is updated in the Cisco.com profile and validated by Cisco.
- If the Cloud Connect server is deployed in embargoed countries where software download is restricted.
- If the user has valid authentication token that is associated with the API key.

If the user doesn't have a valid authentication token associated with the API key, then the user has to sign in to https://devhub-download.cisco.com/console/ to extend the validity of the API key.

If compliance validation fails, the Cisco.com ID user must perform the below-mentioned actions:

- For EULA compliance failure, confirm that you have read and agreed to be bound by the terms of Cisco EULA. Access the link https://software.cisco.com/download/eula to view and accept the agreement.
- For customer company's address verification failure, access the link https://rpfa.cloudapps.cisco.com/rpfa/profile/profile_management.do to update the address.
- For Entitlement failure, where Cisco service contract information indicates that you're not authorized to download the Contact Center software, perform one or more of the following actions:
  - Identify the product name and MDFID of the Contact Center product for which the entitlement failed. To find the product name and corresponding MDFID of the product, check the CLI log for the keyword **Entitlement check failed for MDFID**. Refer to the Serviceability section for the command to retrieve the CLI log.
  - The service contract or subscription containing coverage for the product may not be associated to the Cisco.com user ID. To associate the relevant service contract to the Cisco user ID, use the **Cisco Profile Manager**, and select **Add Access** to request access to the contract (which can now be done using the Serial Number of the product).

	• If your software is covered by a Smart License subscription, go to Cisco Software Central to request access to your company's Smart Account in the **Administration** section. Contact your Cisco representative, partner, or reseller to ensure that the product is covered by a service contract or subscription that is associated with your Cisco.com user ID. Use the Partner Locator link to locate your nearest partner. For assistance, contact your Cisco Accounts Manager or Partner. To expedite your request, include the following information: • User ID (Cisco.com ID used to generate the API key) • Contact Name • Company Name • Contract Number • Product ID or MDFID, Product Name, and Release • You can obtain access to U.S. export-restricted software by completing the K9 agreement form. **Note** Upon successful configuration of artifactory details, artifacts are downloaded locally to the Cloud Connect server periodically at the configured time. During artifact download, the compliance validation is done. The Cisco.com ID user performs the above-mentioned actions for any compliance failure during artifact download.
Expected Inputs	User should input Artifactory URL, Artifactory Repository Name, and API Key. The Cisco-hosted software Artifactory URL is https://devhub-download.cisco.com/binaries and Artifactory Repository Name is `ent-platform-release-external`. **Note** Cisco recommends not to use the same Artifactory API key generated by a single CCO ID across multiple deployments. For multiple deployments such as test, pre-production, production, and so on, generate the Artifactory API key for each deployment using different CCO IDs. Artifactory API key generated by a single CCO ID can be used in both publisher and subscriber of Cloud Connect in a single deployment. CLI provides an option to the customer to choose between using export-restricted and unrestricted software, based on the entitlement associated with the Cisco.com ID. For example, VVB has export-restricted and unrestricted software.

Expected Outcome	This CLI validates the entitlement associated with the Cisco.com ID and connection to the Cisco-hosted software artifactory using the given configuration. Based on successful validation, the artifactory details are configured in the Cloud Connect server.

Note Use the command **utils image-repository set** to change export-restricted or unrestricted software in the deployment. Use the CLI **utils initiate software-download** to enforce the cleanup and download the restricted vs unrestricted software.

Note On the successful configuration of artifactory details, artifacts are downloaded locally to the Cloud Connect server at the scheduled or default time. Orchestration operations such as patch install, rollback, or upgrade can be performed only after the artifacts are downloaded. If you need to download the artifacts immediately after the configuration, use the **utils initiate software-download** CLI. Usage of orchestration-related CLI is blocked during download, and this duration depends on the number of artifacts to be downloaded.

Note Before you configure the bandwidth using the **utils set software-download bandwidth** command, make sure the software is downloaded locally for the first time after the artifactory is successfully configured using the **utils image-repository set** command. To download the artifacts immediately after the configuration, use the **utils initiate software-download** command.

Table 4: Show Command Table

Command	**utils image-repository show**
Description	This command displays the configured Cisco-hosted software Artifactory URL, Repository Name, and the API Key (the mix of hash and last 4 characters of key) in the Cloud Connect server.
Expected Inputs	NA
Expected Outcome	Displays the configured Artifactory URL, Repository Name, and the API Key.

Onboard VOS Nodes to Orchestration Control Node

The onboarding process helps to establish a password-less connection between the Cloud Connect node and the VOS nodes.

Prerequisites:

- Ensure that the Cloud Connect server and target nodes maintain the minimum software versions that are required as outlined in System Requirements.
- If you are using self-signed certificates, import the self-signed Tomcat certificate of the Cloud Connect server into the VOS nodes which you have to onboard. Ensure to import both Cloud Connect publisher

and subscriber node certificates on all VOS publisher and subscriber nodes. For details, see Self-Signed Certificate, on page 40.

To onboard Finesse, CUIC, VVB, IDS, LD to a Cloud Connect server, run the **utils system onboard initiate** command from the publisher node of the respective VOS cluster that you wish to onboard. The publisher node of the Cloud Connect server must be up and running when onboarding is initiated from VOS node. When the onboarding is initiated from VOS node, FQDN of the Cloud Connect server must be used.

Command	**utils system onboard initiate**
Description	This command is used to onboard a VOS node such as Finesse, CUIC, VVB, etc., to a Cloud Connect server.
Expected Inputs	When run, the command prompts for: • Cloud Connect server FQDN • Cloud Connect application username • Password
Expected Outcome	The nodes are onboarded to the Cloud Connect server orchestration inventory. A message is displayed indicating the status.

Note If the system (cluster) onboards to the Cloud Connect server with partial error, check the reason for the error and correct it. Then, run the **utils system onboard update** command instead of running the **utils system onboard initiate** command.

Note Onboarding is allowed only when all the publisher and subscriber nodes in the Cloud Connect server are reachable.

Note If the Cloud Connect server is corrupted and redeployed by doing fresh install, the administrator has to run **utils system onboard remove** from the VOS node and then run **utils system onboard initiate** to onboard the VOS nodes again.

Onboard Windows nodes to orchestration control node

The onboarding process helps to establish a password-less connection between the Cloud Connect node and the Windows nodes. To onboard the Windows-based nodes to orchestration control node, perform the following steps:

Procedure

Step 1 Configure SSH public key on the Windows nodes by following the steps in the section Configure SSH public key on Windows nodes, on page 39.

Step 2 From the cloud connect server, run the **utils system inventory export** command to download the inventory to an SFTP server. For details, see Export and Import of Nodes Managed by Orchestration Control Node, on page 36.

Step 3 Edit the inventory file to include the Windows components. Refer to the default template section in the inventory file.

Note
- The syntax, alignment, and indentation must be exactly the same as mentioned in the inventory file.
- Ensure the CRLF line endings are of UNIX-Style. Use a Linux-based or a Mac OS-based editor to create the Windows inventory file.

The following fields in the inventory file are mandatory.

Field	Description
ProductName	The **ProductName** mentioned in the inventory file must be in uppercase and cannot be changed. For example, CVPREPORTING, CVPSERVER, CVPOAMP, DISTRIBUTOR, LOGGER, PG, ROGGER or ROUTER.
Pair under product	This is a user-defined pair name.
Hostname	This can be a valid IP, or hostname, or FQDN name of the target node.
Side of the deployment	It can either be A or B.
User configured on host	This is the username for which the SSH keys are configured in Step 1. **Note** The user must have either domain admin or local administrator privilege. **Note** User name can be in User Principal Name (UPN) format or Domain username (domain\username) format for domain administrator or local administrator user name. Example: UPN format : administrator@stooges.icm Domain Administrator: stooges\administrator Local Administrator: administrator

Step 4 Import the inventory back from the SFTP server by running the command **utils system inventory import** on the Cloud Connect publisher node. For details, see Export and Import of Nodes Managed by Orchestration Control Node, on page 36.

Add Deployment Type and Deployment Name

An administrator can edit the inventory file to add the details of the deployment.

Procedure

Step 1 Download the inventory to an SFTP server by running the utils system inventory export command. For details, see Export and Import of Nodes Managed by Orchestration Control Node, on page 36.

Step 2 Edit the following strings in the inventory file, if required.

- **deploymentType**: This field is used for compatibility check during an upgrade or rollback or switch forward procedure. The supported deployment types are:
  - UCCE-2000-Agents
  - UCCE-4000-Agents
  - PCCE-2000-Agents
  - PCCE-4000-Agents

  Note Orchestration is not supported for 12000, 24000 and 36000 agent deployment models.

  Ensure that the values entered in this field conform to the above format. The deployment type is case sensitive.

- **deploymentName**: Provide a unique name for the deployment.

  This name appears in the subject line of the email notification. If it is not configured, the subject line of the email notification contains only the type of procedure and the overall status.

Note The administrator can update or edit the default values, if required, based on their deployment type and preferred deployment name.

Step 3 Import the inventory back from the SFTP server by running the utils system inventory import command on the Cloud Connect publisher node. For details, see Export and Import of Nodes Managed by Orchestration Control Node, on page 36.

Validate Onboarded Nodes for Orchestration

To validate the onboarding of VOS and Windows nodes, and to check whether the Orchestration feature is ready to be used, run the **utils deployment test-connection** command.

Command	utils deployment test-connection

Description	This command is used to validate whether password-less SSH connection is successful between the onboarded nodes and the Cloud Connect server. You can test the connection to all nodes on the deployment or to a specific group or individual nodes.
Expected Inputs	NA
Expected Outcome	Shows whether the inventory is accurate and the Cloud Connect node is able to connect to the managed hosts.

Configure Email Notification

If an email notification is configured, the Cloud Connect server checks the Cisco-hosted artifact repository periodically at scheduled times and sends email notifications along with the release notes when new software updates are available. Administrators can decide when to apply a patch or perform an upgrade. Email notifications are not triggered if no new software updates are available.

Note The SMTP server referred to in this section is the mail server that is used within the customer organization for their internal email communication.

Perform the following procedures in the same sequence as given here.

1	Set up Email Notification, on page 15
2	Validate Email Configuration, on page 16
3	Subscribe to Email Notification, on page 16
4	Configure Email Notification, on page 15

Set up Email Notification

Configure the email notification by running the following set of commands:

- Set the IP address or hostname of the SMTP server by running the **set smtp-host** command.

Command	**set smtp-host**
Description	This command is used to set the IP address or hostname of the SMTP server.
Expected Inputs	SMTP server IP Address/HostName
Expected Outcome	The SMTP address is updated.

- Set the email address from which emails are triggered by running the **set smtp-from-email** command.

Command	**set smtp-from-email**
Description	This command is used to set the email address from which the emails are triggered. This email address is not monitored and therefore not used for replying to any emails.
Expected Inputs	When run, this command takes an input for a complete email address.

Expected Outcome	Configures the email address from which email notifications are triggered.

- Enable or disable SMTP authentication by running the **set smtp-use-auth** command.

Command	**set smtp-use-auth**
Description	This command is used to enable or disable SMTP authentication. By default, this is disabled.
Expected Inputs	The command takes an input for the values Enable or Disable.
Expected Outcome	SMTP authentication type is updated.

- Set the username to be used for SMTP server connection by running the **set smtp-user** command. This is an optional configuration that needs to be set only when the SMTP authentication is enabled.

Command	**set smtp-user**
Description	This command is used to set the username to be used for SMTP server connection.
Expected Inputs	The command takes an input for the username to be used for SMTP authentication.
Expected Outcome	Configures the SMTP username.

- Set the password for SMTP server connection by running the **set smtp-pswd** command. This is an optional configuration that needs to be set only when the SMTP authentication is enabled.

Command	**set smtp-pswd**
Description	This command is used to set the password for SMTP server connection. The password is stored in an encrypted format. To change the password, run this command again.
Expected Inputs	The command prompts for a password for the SMTP connection.
Expected Outcome	Configures the SMTP password.

Validate Email Configuration

Validate the configuration by running the **utils smtp test-connection** command.

Command	**utils smtp test-connection**
Description	This command is used to establish a connection to the SMTP server using the given configuration.
Expected Inputs	NA
Expected Outcome	Shows whether SMTP connection is successful or not.

Subscribe to Email Notification

Subscribe to email notifications by running the **utils smtp subscribe** command. Specify the email addresses to which the email notifications must be sent.

Command	utils smtp subscribe
Description	This command is used to specify the email addresses that subscribe to the email notifications. For example: `utils smtp subscribe <emailaddress1,emailaddress2,.....emailaddressesN>`
Expected Inputs	Comma-separated list of valid email addresses.
Expected Outcome	Email addresses provided are subscribed for notification.

Configure Windows Server for Updates (Optional)

Microsoft Windows update configuration needs to be done on the target Windows node. Microsoft Windows updates can be downloaded in one of following ways on the target Windows node:

- by directly connecting to the Microsoft server;
- from the Windows update server configured. To deploy or configure Windows server update services, refer to https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/deploy-windows-server-update-services.

Administration Tasks

Note Before upgrade or rollback of nodes managed by Orchestration, make sure to take backup as suggested by respective component documentation. Backup has to be done manually.

Note In case the upgrade or rollback on VOS node fails, then the respective VOS node restart is mandatory before attempting the next upgrade or rollback on the same node. If the administrator does not restart, the next attempt to upgrade or rollback might fail.

Check Installed Software Version and Patches

To check the currently installed software version and patches on a node or group of nodes or all nodes in either Windows or VOS systems, run the **utils deployment show status** command.

Command	utils deployment show status
Description	This command is used to check the currently installed software version and patches for the selected Windows or VOS node individually or group of nodes or for all nodes in the inventory by selecting the option 'All Nodes in the inventory'.
Expected Inputs	Select the node or group of nodes or all nodes from the inventory.

Expected Outcome	Displays information about the installed software version and the patches for the selected node or group of nodes or all nodes from the inventory. If there is no patch installed, a message "No patch installed" is displayed to indicate that along with software version.

Install or Rollback Patch or Upgrade Cloud Connect Server

To install a patch or to roll back a previously installed patch on Cloud Connect server or to upgrade Cloud Connect Server to next available version, run the **utils system upgrade initiate** command. The **Local Repository** option in this command lists the patches and upgrade options available from Cisco artifactory for patch install or rollback or upgrade on Cloud Connect server. This command can be run separately on the Cloud Connect publisher and subscriber nodes.

Note The Cloud Connect publisher should be upgraded before upgrading the subscriber. The switch version on publisher should be done first before doing switch version on subscriber, use **utils system switch version** command to switch between versions.

Note The **Local Repository** option is also available on the Cisco Unified OS Administration web page of Cloud Connect server. Select this option to install a patch or to roll back a previously installed patch on Cloud Connect server or to upgrade Cloud Connect Server to next available version.

Command	**utils system upgrade initiate**
Description	This command is used to initiate the patch install or to roll back the previously installed patch on Cloud Connect server or to upgrade Cloud Connect Server to the next available version. The patches and upgrade options available for patch install or rollback or upgrade are listed from Cisco artifactory.
Expected Inputs	Select the **Local Repository** option to list the patches and upgrade options available for patch install or rollback or upgrade. Select the patch to install or roll back or upgrade option to upgrade Cloud Connect server.
Expected Outcome	The selected patch for install or rollback is installed on Cloud Connect server or selected upgrade option is used to upgrade the Cloud Connect server.

Note The **Local Repository** option is used only after the Cisco Artifactory is successfully configured on Cloud Connect server. See CLI to configure artifactory URL and API key, on page 7 for configuring Cisco artifactory.

Note Optionally, to receive email notification about the status of the patch installation or rollback or upgrade for Cloud Connect server, provide the SMTP host server details when prompted by the CLI.

Note Patch install or roll back or upgrade on Cloud Connect server initiated using **utils system upgrade initiate** command can be canceled using **utils system upgrade cancel** command. The **utils system upgrade status** command can be used to check the status.

List Available Patches for Specific Node or Group of Nodes

To get a list of available patches for a specific node or group of nodes in the inventory, run the **utils patch-manager list** command.

Command	**utils patch-manager list**
Description	This command is used to get a list of patches available for installation for a specific node or group of nodes based on the selected option.
Expected Inputs	Select a node or group of nodes based on the inventory.
Expected Outcome	Displays information about available patches for the selected node or group of nodes.

Install Patch to Specific Node or Group of Nodes

To install patch to a specific node or group of nodes, run the **utils patch-manager install** command.

Command	**utils patch-manager install**
Description	This command is used to install patches on a specific node or group of nodes onboarded to the Cloud Connect inventory.

Expected Inputs	From the list of Windows/VOS nodes displayed, select the node or group of Windows/VOS nodes on which the patch needs to be installed. Once you select the nodes, only the nodes for which patches are available will be displayed. For example, if you select 3 nodes and Windows/VOS patches are available for only 1 of them, you are asked to proceed with only one node. Confirm to proceed. You are also asked to confirm whether the target node needs to be rebooted after installing the patch. Selection of components such as Finesse, CVP Call Server, IdS, and PG with software version 12.6(x) will provide the options "With maintenance mode" and "Without maintenance mode".. If you select a group of nodes with some nodes on 12.6(x) and some nodes below 12.6(x), then "With maintenance mode" or "Without maintenance mode" option will not be available. In this case if "With maintenance mode" option is required, then the individual node with 12.6(x) can be selected separately. If you select "With maintenance mode" option, the maintenance mode is initiated for the selected node to failover active traffic gracefully or shutdown the services gracefully without interrupting the active traffic or causing outage for new traffic before installing the patch and automatically rebooting. If you select, "Without maintenance mode" option, you are initially asked to confirm to proceed. Next, you are asked to provide confirmation on rebooting the node after installing the patch.
Expected Outcome	The selected patch is installed on the selected node or group of nodes.

Note To start Unified ICM services, post the successful completion of patch install with reboot on Unified ICM nodes. See Start Unified ICM Services.

Note You can check the status of the patch install which is currently in-progress. For more information, see Check Status, on page 29.

Note Maintenance mode for IDS co-resident in 2000 Agents Deployment model is not supported

Roll Back Patch from Specific Node or Group of Nodes

To roll back a previously installed patch on a specific node or a group of nodes, run the **utils patch-manager rollback** command.

Command	**utils patch-manager rollback**

Description	This command is used to roll back previously installed patches on a specific node or group of nodes. In case of Windows-based nodes, the latest applied patch is allowed to roll back. In case of VOS-based nodes, the latest applied ES is rolled back.
Expected Inputs	From the list of Windows/VOS nodes displayed, select the node or group of Windows/VOS nodes on which the patch needs to be rolled back. Once you select the nodes, only the nodes for which Windows/VOS patch rollback is available will be displayed. For example, if you select 3 nodes and Windows/VOS patch rollback is available for only 1 of them, you are asked to proceed with only one node. There is also a message displayed indicating that the machine would restart after the patch is rolled back. Confirm to proceed. Selection of components such as Finesse, CVP Call Server, IdS, and PG with software version 12.6(x) will provide the options "With maintenance mode" and "Without maintenance mode". If you select a group of nodes with some nodes on 12.6(x) and some nodes below 12.6(x), then "With maintenance mode" or "Without maintenance mode" option will not be available. In this case if "With maintenance mode" option is required, then the individual node with 12.6(x) can be selected separately. If you select "With maintenance mode" option, the maintenance mode is initiated for the selected node to failover active traffic gracefully or shutdown the services gracefully without interrupting the active traffic or causing outage for new traffic before rollback and automatically rebooting. If you select, "Without maintenance mode" option, you are initially asked to confirm to proceed. Next, you are asked to provide confirmation on rebooting the node after rollback.
Expected Outcome	The previously installed patch is rolled back on the selected node or group of nodes.

Note To start Unified ICM services, post the successful completion of patch roll back with reboot on Unified ICM nodes. See Start Unified ICM Services

Note You can check the status of patch rollback which is currently in-progress. For more information, see Check Status, on page 29.

Install Windows Updates to Specific Node or Group of Nodes

To install Windows updates to a node or group of nodes or all Windows nodes, run the **utils patch-manager ms-patches install** command.

Note Before running this command, refer to the recommended guidelines in the *Microsoft Security Updates* section of the *SecurityGuide for CiscoUnified 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.

Microsoft Windows updates are NOT hosted on Cisco-hosted Software Artifactory. You must configure the target Windows node to fetch the Microsoft Windows updates, either by directly connecting to the Microsoft Server via Internet or from the Windows Update Server. For more details, refer to the Configure Windows Server for Updates (Optional) section. The **utils patch-manager ms-patches install** command will not list the available Windows updates for the administrator to choose for the target node. Instead, it will check the available updates for the below listed Windows update categories and install all the available updates:

- Application
- Connectors
- DefinitionUpdates
- DeveloperKits
- FeaturePacks
- Guidance
- ServicePacks
- Tools
- UpdateRollups
- CriticalUpdates
- SecurityUpdates
- Updates

The administrator can control the installation of Windows updates using Windows Update Server, instead of directly connecting to the Microsoft Server via Internet. Ansible log, generated during the running of **utils patch-manager ms-patches install** CLI, captures the details of the Windows updates, along with the Knowledge Base (KB) number of the updates that were installed on the target node. Refer to the Serviceability section for the command to retrieve the Ansible log.

Command	**utils patch-manager ms-patches install**
Description	This command is used to install the latest Windows updates to a node or a group of Windows nodes or all Windows nodes.

Expected Inputs	From the list of Windows nodes displayed, select the node or group of Windows nodes or all Windows nodes to which the updates need to be applied. You can also select all the Windows nodes in the inventory. Once you select the nodes, only the nodes for which Windows updates are available will be displayed. For example, if you select 3 nodes and Windows updates are available for only 1 of them, you are asked to proceed with only one node. Confirm to proceed. You are asked to confirm whether the target nodes needs to be rebooted after installing the updates. Selection of components such as CVP Call Server and PG with software version 12.6(x) will provide the options "With maintenance mode" and "Without maintenance mode". If you select a group of nodes with some nodes on 12.6(x) and some nodes below 12.6(x), then "With maintenance mode" or "Without maintenance mode" option will not be available. In this case if "With maintenance mode" option is required, then the individual node with 12.6(x) can be selected separately. If you select "With maintenance mode" option, the maintenance mode is initiated for the selected node to failover active traffic gracefully or shutdown the services gracefully without interrupting the active traffic or causing outage for new traffic before installing the update and automatically rebooting. If you select, "Without maintenance mode" option, you are initially asked to confirm to proceed. Next, you are asked to provide confirmation on rebooting the node after installing the patch.
Expected Outcome	The selected Windows updates are installed on the selected node or group of nodes or all Windows nodes.

Roll Back Windows Update from Specific Node or Group of Nodes

To roll back Windows update from a specific node or group of nodes or all Windows nodes, run the **utils patch-manager ms-patches rollback** command.

Note

- Before running this command, refer to the recommended guidelines in the *Microsoft Security Updates* section of the *SecurityGuide for CiscoUnified 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
- Listing of Windows updates available for rollback is not supported.

Command	**utils patch-manager ms-patches rollback**
Description	This command is used to roll back a specific Windows update from a specific node or group of nodes or all Windows nodes.

Expected Inputs	Select the node or group of Windows nodes or all Windows nodes on which the rollback needs to be performed. You can also select all the Windows nodes in the inventory for rollback. Provide the Knowledge Base (KB) number you want to rollback. You are asked to confirm whether the target nodes need to be rebooted after rollback. Selection of components such as CVP Call Server and PG with software version 12.6(x) will provide the options "With maintenance mode" and "Without maintenance mode". If you select a group of nodes with some nodes on 12.6(x) and some nodes below 12.6(x), then "With maintenance mode" or "Without maintenance mode" option will not be available. In this case if "With maintenance mode" option is required, then the individual node with 12.6(x) can be selected separately. If you select "With maintenance mode" option, the maintenance mode is initiated for the selected node to failover active traffic gracefully or shutdown the services gracefully without interrupting the active traffic or causing outage for new traffic after rollback and automatically rebooting. If you select, "Without maintenance mode" option, you are initially asked to confirm to proceed. Next, you are asked to provide confirmation on rebooting the node after rollback.
Expected Outcome	The selected Windows updates are rolled back.

Enable or Disable Compatibility Enforcement

You can enable or disable compatibility enforcement. When the compatibility enforcement is enabled, it ensures that the upgrade, rollback, or switch forward is as per the compatibility matrix published by Cisco for reference design-based deployment. To enable or disable compatibility enforcement, run the **utils deployment compatibility-check** command.

Note By default, the compatibility enforcement is enabled.

When the compatibility enforcement is disabled, the Orchestration framework does not enforce upgrade, rollback, or switch forward as per the compatibility matrix published by Cisco.

Command	**utils deployment compatibility-check**
Description	This command is used to enable or disable compatibility enforcement.
Expected Inputs	User confirmation to proceed with enabling or disabling compatibility enforcement.
Expected Outcome	Message about the success or failure of enabling or disabling compatibility enforcement.

Note You can run this command only from the publisher node of the Cloud Connect server. The compatibility configuration replicates automatically from the publisher node to the subscriber node when the **utils deployment compatibility-check** command is run with successful results on the publisher node.

Initiate maintenance mode for a specific node(s)

Initiating maintenance mode allows the components to failover gracefully or shutdown the services gracefully (depending on the selected components) without interrupting the active traffic or causing outage to new traffic. This ensures that the system can be taken down for maintenance activity such as installing new software updates, restarting services etc. Currently, maintenance mode is supported for PG, CVP server, IdS, and Finesse.

Note Ensure that not all CVP servers are put into maintenance mode at same time, so that incoming call traffic can be distributed.

To initiate maintenance mode for a specific node in the inventory, run the **utils system maintenance initiate** command.

Command	**utils system maintenance initiate**
Description	This command is used to initiate maintenance mode for a specific node based on the selected option. Currently, the initiate maintenance command is available for Finesse, CVP Call Server, IdS, and PG components.
Expected Inputs	When run, this command prompts you to select a node based on the inventory.
Expected Outcome	Information about success or failure of the initiate maintenance command for a selected node is displayed.

Note The **utils system maintenance initiate** is applicable for target nodes on CCE 12.6(1) and above.

Note If either the Publisher or Subcriber or the active/inactive node is already in maintenance mode in any of the components, the other server cannot be initiated for maintenance.

Note You can check the status of system maintenance initiate which is currently in-progress. For more information, see Check Status, on page 29.

Note Maintenance mode for IDS co-resident in 2000 Agents Deployment model is not supported

List Available Upgrade Options

To get a list of available upgrade options for VOS and Windows nodes individually or for group of nodes or for all nodes in the inventory, run the **utils upgrade-manager list** command.

Command	**utils upgrade-manager list**
Description	This command is used to get a list of upgrade options available for the selected VOS or Windows node or group of nodes or all nodes in the inventory by selecting the option "All nodes in the inventory"..
Expected Inputs	Select a node or group of nodes or all nodes based on the inventory.
Expected Outcome	Displays information about available upgrade options for selected VOS or Windows nodes or group of nodes or all nodes in the inventory. If the selected node or group of nodes or all nodes are already running the latest software version, a message is displayed to indicate that.

Upgrade a Specific Node or Group of Nodes or All Nodes

To perform software version upgrades on VOS or Windows nodes or All nodes in the deployment (VOS and Windows nodes together), run the **utils upgrade-manager upgrade** command from the Cloud Connect server. It is recommended to run this command during a maintenance window as the procedure involves system restart that will cause service outage.

For the selected VOS or Windows component for upgrade, a compatibility check is performed in the background based on the configured deployment type to ensure that all the associated components are onboarded. If the components are onboarded and the required dependent components are either in same target upgrade version or backward compatible version, the upgrade procedure begins. However, if the components are not onboarded, you have to onboard them first or if the versions are not compatible, upgrade them to the required version. For example, if you select to upgrade the Rogger nodes to 12.6(1) version, the inter-component compatibility check is run for the Rogger dependent components such as Finesse, CVP, VVB, CUIC. These must already be in 12.6(1) version and PG must be backward compatible version, that is, 12.5(1) .

Note The sub-components sequence dependencies are not validated as part of the upgrade compatibility. Refer to the upgrade guides of the respective components for the correct sequence. For example, in case of CVP, we have sub-components such as Operations Console, Unified CVP Reporting Server and Unified CVP Server. These must be upgraded in the required sequence.

For VOS node/cluster, switch forward is optional at the end of upgrade. If administrators opt for switch forward, the target node is restarted and the active/inactive partition is switched. If they decide not to switch forward, the upgraded version remains in the inactive partition of the target node. Switch forward for these nodes can be performed later. For details, see Perform Switch Forward on Specific VOS Node or Group of Nodes , on page 28.

For VOS cluster, the upgrade or the switch forward procedure is performed first on the publisher and then on the subscriber nodes. If switch forward is performed immediately after an upgrade, the overall procedure takes a significant amount of time; hence plan the maintenance window accordingly.

For selecting "All nodes" option during upgrade, make sure that all the VOS and Windows nodes onboarded are on the same software version. Stage-wise upgrade is performed for the solution components as per the *CCE Installation and Upgrade guide*. In case of any component upgrade failure during the process, the upgrade does not proceed to the next stage. The administrator has to upgrade individual components by selecting the respective individual VOS or Windows nodes.

Command	**utils upgrade-manager upgrade**
Description	This command is used to upgrade VOS or Windows nodes or group of nodes or All nodes in the deployment (VOS and Windows nodes together) in the inventory.
Expected Inputs	Select the Windows or VOS node or group of nodes or all nodes in the deployment (VOS and Windows nodes together) that you want to upgrade. From the list of upgrade options available for the selected node or group of nodes or all nodes, select the appropriate option and confirm. A compatibility check is then run in the background. To select "All nodes" upgrade option, make sure that all the VOS and Windows nodes onboarded and the components are on the same software version. Once the upgrade procedure begins, you can see the progress details for each of the machines. You can also see the elapsed time since the procedure started.
Expected Outcome	The selected node or group of nodes or all nodes is upgraded.

Note

- For faster upgrades, the Cloud Connect server downloads locally all the new software updates from the Cisco hosted repository at a predefined time.
- To start the Unified ICM services, post the successful completion of upgrade with reboot on Unified ICM nodes. See Start Unified ICM Services.
- Upgrade of all nodes to CCE 12.6(2) will be supported for the following scenarios:
  - All CCE components are on 12.6(1)
  - All CCE components are on 12.5(1)
  - All ICM and VOS components are on 12.5(2) and all CVP components are on 12.5(1)

Note You can check the status of upgrade which is currently in-progress. For more information, see Check Status, on page 29.

Perform Switch Forward on Specific VOS Node or Group of Nodes

Administrators can perform switch forward on target VOS nodes independently. When the active partition is on lower version and the inactive partition is on higher version, run the **utils upgrade-manager switch-forward** command to perform a switch forward. It is recommended to run this command during a maintenance window as the procedure involves system restart that will cause service outage.

Command	**utils upgrade-manager switch-forward**
Description	This command is used to switch forward on target VOS node/cluster from Cloud Connect server.
Expected Inputs	Select the VOS node/cluster on which you want to perform the switch forward. You will see the details of the current active/inactive versions. Confirm to proceed with the switch forward. A compatibility check is then run in the background. • If there are components whose versions are not compatible or the components are not onboarded as per the compatibility requirements, a list of those components is displayed. Upgrade or switch forward the listed components to the required software versions and re-run this command. • If the versions of the associated components are compatible with the node's inactive version, then the switch forward procedure continues. Once the switch-forward procedure begins, you can see the progress details for each of the machines. You can also see the elapsed time since the procedure started.
Expected Outcome	The system restarts and the current version of the system is on a higher version.

Note You can check the status of switch forward which is currently in-progress. For more information, see Check Status, on page 29.

Roll Back Upgrade from Specific Node or Group of Nodes

To roll back an upgrade on VOS or Windows nodes, run the **utils upgrade-manager rollback** command from the Cloud Connect server. It is recommended to run this command during a maintenance window as the procedure involves system restart that will cause service outage.

For the selected VOS or Windows component for rollback, a compatibility check is performed in the background to ensure that all the associated components are onboarded and the versions are compatible. If the components are onboarded and the versions are compatible with each other, the rollback procedure begins. However, if the components are not onboarded, you have to onboard them first or if the versions are not compatible, roll them back to the required version.

For VOS nodes/cluster, the rollback (switch backward) must be initiated from an active higher version to an inactive lower version of the node. Also, the publisher node of the managed cluster must be rolled back before the subscriber node of the cluster.

Command	utils upgrade-manager rollback
Description	This command is used to roll back an upgrade on VOS or Windows nodes.
Expected Inputs	Select the Windows node or VOS node/cluster on which you want to perform the rollback. The rollback option is listed for the selected node or group of nodes. Select the appropriate option and confirm. A compatibility check is then run in the background. • If there are components whose versions are not compatible or if the components are not onboarded as per the compatibility requirements, a list of these components is displayed. Roll back the listed components to the required software versions and then re-run this command. • If the versions of the associated components are compatible with the selected node's rollback version, then the rollback procedure begins. Once the rollback procedure begins, you can see the progress details for each of the machines. You can also see the elapsed time since the procedure started.
Expected Outcome	The selected node or group of nodes is rolled back.

Note To start Unified ICM services, post the successful completion of roll back upgrade with reboot on Unified ICM nodes. See Start Unified ICM Services.

Note You can check the status of rollback which is currently in-progress. For more information, see Check Status, on page 29.

Check Status

To check the current status of patch manager install, patch manager rollback, upgrade manager upgrade, upgrade manager rollback, switch-forward, or system maintenance initiate, run the **utils deployment show in-progress** command. You can run this command if connectivity to CLI is lost after initiating any of above procedures.

Command	utils deployment show in-progress
Description	This command is used to check the current status of any patch manager install, patch manager rollback, upgrade manager upgrade, upgrade manager rollback, switch-forward or system maintenance initiate. It also shows the subsequent progress, if applicable, for each node on which the procedure is initiated. If there is no procedure in progress, this command gives the last successful/failed procedure status.

Expected Inputs	NA
Expected Outcome	Shows the current status of the patch manager install, patch manager rollback, upgrade manager upgrade, upgrade manager rollback, switch-forwardor system maintenance initiate for each node. If there is no patch manager install, patch manager rollback, upgrade manager upgrade, upgrade manager rollback, switch-forward, or system maintenance initiate, then you see the status of the previous upgrade, rollback, or maintenance.

Check Last Known Orchestration Operation Status on Remote Node

To check the last known orchestration operation status (last completed state or last known state when the operation is in progress or when the remote node is not reachable) on the remote node, run the **utils deployment show progress-HA** command. This command is applicable for patch manager install, patch manager rollback, upgrade manager upgrade, upgrade manager rollback, ms patch install, ms patch rollback, switch-forward, system maintenance initiate, and Unified ICM services start.

This command can be used only in Cloud Connect High Availability setup

Command	**utils deployment show progress-HA**
Description	This command is used to check the last known operation status run on remote node. This will only display the snapshot of the last known operation status and will not display the continuous status changes for the operation that is currently in progress. This command can be used to check the last known operation status on the remote node when the Cloud Connect node is not reachable.
Expected Inputs	NA
Expected Outcome	The snapshot of the last known operation status is displayed.

Note Last known orchestration operation status will not be synchronized to remote node, in case of communication loss to remote node after initiating the orchestration operation and operation being completed before re-establishing the communication.

Start Unified ICM Services

To start Unified ICM services from Cloud Connect server, run the **utils system icm-services start** command.

Command	**utils system icm-services start**
Description	This command is used to start the Unified ICM services from Cloud Connect server. This CLI will present the user with a list of Unified ICM hosts configured in the inventory, and the admin can select individual or group of Unified ICM hosts.

Expected Inputs	User should choose individual or group of Unified ICM hosts from the list. User should give confirmation yes/no to proceed with start of Unified ICM services
Expected Outcome	As part of CLI output, there are two kinds of messages which displays success as shown below: • When the Unified ICM services are started successfully from stop state, the message "**Services started**" is displayed. • When the Unified ICM services are already up and running, the message "**Services running**" is displayed.

Maintenance Tasks

CLI to configure software download schedule

To change the default schedule for the software download from the Cisco-hosted software artifactory or to change the previously configured software download schedule, run the **utils set software-download time** command.

Command	**utils set software-download time**
Description	This command changes the default or the previously configured schedule for the software download from the Cisco-hosted software artifactory.
Expected inputs	Displays the currently configured software download time and prompts you to enter the new time (HH:MM in 24-hours format).
Expected outcome	Displays the success or failure message for the software download time configuration.

Note

- Cisco recommends that you change the default software download schedule based on your preference.
- Make sure that you configure the time for software download on the publisher and subscriber separately.
- Cisco recommends to set different software download time in Cloud Connect publisher and subscriber, preferably 1 hour apart. For example, if Cloud Connect publisher is set with the download time 3:00 AM, then set Cloud Connect subscriber with the download time 4:00 AM. Avoid using 1:00 AM and 5:00 AM for the software download as this time conflicts with other automatic orchestration operation.
- Default software download time is 2:00 AM Cloud Connect server time.

CLI to configure the bandwidth for Orchestration software download

To configure the bandwidth that the Orchestration feature uses to download the software from Cisco hosted software artifactory to Cloud Connect server, run the **utils set software-download bandwidth** command.

Note Before you configure the bandwidth using the **utils set software-download bandwidth** command, make sure the software is downloaded locally for the first time after the artifactory is successfully configured using the **utils image-repository set** command. To download the artifacts immediately after the configuration, use the **utils initiate software-download** command.

Command	**utils set software-download bandwidth**
Description	This command configures the bandwidth that the Orchestration feature uses to download software.
Expected inputs	When run, this command prompts for the following: • Your confirmation with yes or no for turn-on or turn-off the bandwidth configuration. • Enter a valid bandwidth value if you have chosen to turn-on the bandwidth configuration. **Note** • Make sure to suffix the bandwidth value with M for Mbps, K for Kbps and None for Bytes per second.
Expected outcome	Following are the outcomes: • Displays the success or failure message when you turn-on or turn-off the bandwidth configuration. • If you have turned-on the bandwidth configuration and entered a valid value, this CLI validates and configures the entered bandwidth value.

Note

- Make sure that you configure the bandwidth for software download, on the publisher and subscriber separately.
- Software download bandwidth control is disabled by default. The maximum available bandwidth is used during software download. This might have an impact on the features supported by Cloud Connect only during software download.
- Cisco recommends minimum10-Mbps bandwidth for optimal software download. If you configure the bandwidth to a value that is lesser than 10-Mbps, the duration of the software download increases and the orchestration operations cannot be performed during the software download duration. If you configure the bandwidth to a value that is greater than the maximum available bandwidth, the software download uses only the maximum available bandwidth.
- Proxy configured for orchestration might have an impact on the maximum available bandwidth for software download. Check the proxy configuration and ensure the configured bandwidth will be available for the software download when proxy is used for orchestration.

Enforce software download from Cisco hosted software artifactory

To initiate software download from Cisco hosted software artifactory to cloud connect server, run the **utils initiate software-download** command.

Command	**utils initiate software-download**
Description	This command initiates the software download from Cisco hosted software artifactory to Cloud Connect server.
Expected inputs	User confirmation with yes or no to proceed with software download.
Expected outcome	Displays the CLI message about the success or failure for the software download initiated.

Note

- Software download must be planned during off-peak hours as it consumes network bandwidth and resources. The duration of the download depends on the number of software that needs to be downloaded.
- Periodic software download happens everyday at 2 AM or at the time configured by admin. Use this CLI to initiate software download before the next scheduled download.
- Software download needs to be initiated in the publisher and the subscriber separately. While software download is in progress on the publisher, you can run the orchestration operation from the subscriber, or vice-versa.
- This CLI only initiates the software download and the download starts after prerequisites are met.

Update VOS Nodes Onboarded to Orchestration Control Node

To update VOS based nodes that have been onboarded, run the **utils system onboard update** command from the publisher node in the VOS node/cluster that you want to update.

Command	**utils system onboard update**
Description	This command is used to update a node/cluster on a Cloud Connect node.
Expected Inputs	When run, this command prompts for: • Cloud Connect server FQDN • Cloud Connect application username and password
Expected Outcome	The existing node/cluster is updated in the Cloud Connect node inventory.

Remove VOS Nodes from Orchestration Control Node

To remove any existing VOS-based node or cluster, run the **utils system onboard remove** command from the publisher node in the VOS node/cluster that you want to remove.

Command	**utils system onboard remove**

Description	This command is used to remove a node/cluster from a Cloud Connect node.
Expected Inputs	When run, this command prompts for: • Cloud Connect server FQDN • Cloud Connect application username and password
Expected Outcome	The node/cluster is successfully removed from the Cloud Connect node inventory.

Update Windows Nodes Onboarded to Orchestration Control Node

The update procedure is similar to the onboarding procedure described in Onboard Windows nodes to orchestration control node, on page 12.

Note If SSH connection is already established, skip Step 1 in the above procedure.

Validate Updated Nodes Onboarded for Orchestration

The procedure to validate updated nodes that have been onboarded is the same as described in Validate Onboarded Nodes for Orchestration, on page 14.

Configure Email Configuration

You can check your email configuration details by running the respective commands as described below:

- Get the IP address and hostname of the SMTP server by running the **show smtp-host** command.

Command	**show smtp-host**
Description	This command is used to get the IP address or hostname of the SMTP server.
Expected Inputs	NA
Expected Outcome	Shows the configured IP address or host name of the SMTP server.

- Get the email address from which the emails are triggered by running the **show smtp-from-email** command.

Command	**show smtp-from-email**
Description	This command is used to get the email address from which the emails are triggered. This email address is not monitored and therefore not used for replying to any emails.
Expected Inputs	NA
Expected Outcome	Shows the email address from which the emails are triggered.

- See if SMTP authentication is enabled or not by running the **show smtp-use-auth** command.

Command	show smtp-use-auth
Description	This command is used to know if SMTP authentication is enabled or not.
Expected Inputs	NA
Expected Outcome	SMTP authentication : <enable/disable>

- Get the username for SMTP server connection by running the **show smtp-user** command.

Command	show smtp-user
Description	This command is used to show the user name to be used for SMTP server connection.
Expected Inputs	NA
Expected Outcome	Shows the SMTP username.

- See if the SMTP password is set or not by running the **show smtp-pswd** command.

Command	show smtp-pswd
Description	This command is used to know if the SMTP password is set or not. To reset the password, run the **set smtp-pswd** command.
Expected Inputs	NA
Expected Outcome	Shows whether the SMTP password is set or not.

- See the email addresses subscribed for notification by running the **utils smtp show subscriptions** command.

Command	utils smtp show subscriptions
Description	This command is used to get a list of all the email addresses subscribed for email notification.
Expected Inputs	NA
Expected Outcome	Shows the email addresses that are subscribed for email notification. If there is no email address subscribed, a message is displayed indicating it.

Delete Configuration for Email Notification

To remove the configuration for email notifications, run the **utils smtp remove-config** command.

Command	utils smtp remove-config
Description	This command is used to remove the SMTP configuration from the control node. Email notification will no longer be sent to the subscribed email addresses. This command removes only the SMTP configuration, not the subscribed email addresses.

Expected Inputs	NA
Expected Outcome	SMTP configuration is deleted.

Unsubscribe Email Notification

To unsubscribe from email notifications, run the **utils smtp unsubscribe** command.

Command	**utils smtp unsubscribe**
Description	This command is used to remove one or more email addresses from the existing list of subscribers for email notification. **Note** You can get a list of subscribed email addresses using the **utils smtp show subscriptions** command.
Expected Inputs	Provide a comma-separated list of the email addresses to unsubscribe. For example: **utils smtp unsubscribe <emailaddress1,emailaddress2,.....emailaddressesN>** You can also remove all the subscribed email addresses from the subscription list at once. To do that, run **utils smtp unsubscribe all** and confirm.
Expected Outcome	Removes the email addresses you provided as the input from the subscription list.

Export and Import of Nodes Managed by Orchestration Control Node

To export inventory to an SFTP server, run the **utils system inventory export** command.

Command	**utils system inventory export**
Description	This command is used to export inventory to an SFTP server location. The inventory file can then be viewed and edited as required.
Expected Inputs	When run, this command prompts for: • SFTP Server: IP address of the SFTP remote server • SFTP User • SFTP User's Password • SFTP Directory: Location of the remote server directory where the inventory needs to be exported **Note** Provide the location only; the filename is *inventory.conf* by default.
Expected Outcome	Inventory is exported to the SFTP server location.

To import inventory to Cloud Connect server, run the **utils system inventory import** command.

Command	utils system inventory import
Description	This command is used to import inventory to Cloud Connect server.
Expected Inputs	When run, this command prompts for: • SFTP Server: IP address of the SFTP remote server • SFTP User • SFTP User's Password • SFTP Directory: Location of the remote server directory from where the inventory needs to be imported **Note** • Provide the location only. The filename is *inventory.conf* by default. • During inventory import, the *inventory.conf* filename should have the side information added for each node. For example, side: "A" /side: "B". During inventory import, the cluster information cannot be blank. It should have valid host details or a default value {}. For example, "ROGGER":{}
Expected Outcome	Inventory is imported to Cloud Connect server.

Note For information on adding deployment type and deployment name in the inventory file, see Add Deployment Type and Deployment Name, on page 14.

Export Current Patch Level Details

Available patches for nodes in the deployment can be obtained in either of the following ways:

- Email Notification
- Using the **utils patch-manager list** command.

Current patch levels can be exported in text file format using the **utils patch-manager export status** command.

Command	utils patch-manager export status
Description	This command is used to export the patch level details of a node or a group of nodes in a text file format.
Expected Inputs	Select the node(s) and enter the SFTP server details.
Expected Outcome	A text file with the current patch levels of the selected nodes is exported to the provided location. A success message is displayed along with the location where the file is saved.

Serviceability

Audit Logs

Audit trial for administrative operation that is initiated from Orchestration CLI on Cloud Connect is captured in Orchestration Audit logs. Audit trial captures the user, action and date/time details of the CLI operation.

- **file get activelog orchestration-audit/audit.log***

CLI Logs

Run the following command on the Cloud Connect node to retrieve CLI logs:

- **file get activelog platform/log/cli*.log**

Ansible Logs

Run the following commands on the Cloud Connect node to retrieve ansible-related logs:

- Current transaction logs: **file get activelog ansible/ansible.log**
- Historical logs: **file get activelog ansible/ansible_history.log**

Operation Status HA Synchronization Logs

Run the following command on the Cloud Connect node to retrieve synchronization-related logs:

- **file get activelog ansible/sync_ansible_log_to_remote_cc.log**

Email Notification-related Logs

Run the following commands on the Cloud Connect node to retrieve email-related logs:

- Current transaction logs:**file get activelog ansible/ansible_email_cron.log**

Software Download Logs

Run the following commands on the Cloud Connect node to retrieve software download-related logs:

- Current transaction logs:**file get activelog ansible/software_download_ansible.log**
- Historical logs:**file get activelog ansible/software_download_ansible_history.log**
- Process logs:**file get activelog ansible/software_download_process.log**

Note Software is downloaded separately on Cloud Connect publisher and subscriber.

Orchestration Logs in RTMT

You can also view the below-mentioned logs using the Real-Time Monitoring Tool (RTMT):

- Audit logs by selecting 'Orchestration Audit' as the Cloud Connect service
- Ansible logs by selecting 'Ansible Controller' as the Cloud Connect service

To download RTMT from Cloud Connect, access https://FQDN:8443/plugins/CcmServRtmtPlugin.exe.

For more information, refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide* at:https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

For logs on individual components, refer to the *Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Enable and View Windows Open SSH Logs

To enable and view open SSH logs, do the following:

- Make sure the sshd_config file *%programdata%\ssh\sshd_config* has the value as 'LogLevel DEBUG' and uncomment the line.
- Restart the service (select service name **OpenSSH SSH Server**).
- In the Windows Event Viewer, select option **`Show Analytic and Debug Logs`** from **View** on the top menu bar.
- Select **`Debug`** channel from OpenSSH folder.
- On the right hand side, under Actions from Debug channel, select **`Enable log`**.

To turn on file-based logging, do the following:

- In the sshd_config file *%programdata%\ssh\sshd_config*, set the value as "SyslogFacility LOCAL0" and uncomment the line.
- Restart the service (select service name **OpenSSH SSH Server**).
- The file based logs are collected at location *%programdata%\ssh\logs*.

Configure SSH public key on Windows nodes

This section describes how to establish password-less Secure Shell (SSH) connection between Cloud Connect server and Windows node (CVP and ICM) using an SSH public key. The Windows node can be in a Workgroup or Domain.

Note If the Windows node (CVP and ICM) version is 12.5, install 12.5 mandatory ES before performing this procedure. Mandatory ES is not applicable for 12.6(x) target nodes. See System Requirements, on page 2 for details.

1. Navigate to *%Users%\<logonUser>\.ssh* and create *authorized_keys* file, if it doesn't exist.

Note

- The *authorized_keys* extension type is **File** and you should not modify it.
- The user must have either domain admin or local administrator privilege.

2. Open the browser and enter the following Cloud Connect publisher URL: **https://<CloudConnectIP>:8445/inventory/controlnode/key**
3. Provide your Cloud Connect application admin credentials. Upon successful authentication, a REST API response fetches the Cloud Connect Public SSH Key.
4. Copy the public key value that appears between quotes in the API response into the *authorized_keys* file in *%Users%\<logonUser>\.ssh*.
5. Repeat steps 2, 3, and 4 to fetch the Cloud Connect subscriber public key (if Cloud Connect is HA setup).

Note You must copy the Cloud Connect publisher and subscriber public keys into a single *authorized_keys* file. The publisher and subscriber entries should be in separate lines and should not use any extra space, comma, or any special characters at the end of the line.

6. Restart the following OpenSSH services:
   - OpenSSH SSH Server
   - OpenSSH Authentication Agent

Note For more information on Windows security hardening, see the *Windows Server Hardening* section in the Security Guide for Cisco Unified ICM/Contact Center Enterprise.

Self-Signed Certificate

You must import the self-signed certificates of both Cloud Connect publisher and subscriber nodes to the VOS publisher and subscriber nodes.

Get Tomcat Certificate from Cloud Connect Server

Procedure

Step 1 Login to the Cloud Connect server using: `https://<cloud connect hostname>:8443/cmplatform`.

Step 2 Navigate to **Security** > **Certificate Management**.

Step 3 Click **Find**.

Step 4 Click on the Tomcat certificate of the Cloud Connect server.

Step 5 Download the *.PEM file* and save the file.

Import Cloud Connect Server Tomcat Certificate to VOS Nodes

Procedure

Step 1 Login to the VOS node server using: `https://<VOS node hostname>:8443/cmplatform`.

Step 2 Navigate to **Security** > **Certificate Management**.

Step 3 Click on Upload Certificate/Certificate Chain.

Step 4 Select 'tomcat-trust' from the drop-down list in the **Certificate Purpose** field.

Step 5 Click **Browse** to upload the Cloud Connect server *.PEM file*.

Step 6 Click **Upload**.

Step 7 Restart the specific VOS node by running the **utils system restart** command.

Things to Know

- Orchestration is not supported for CTIOS, Customer Collaboration Platform (CCP), ECE, CCDM, CCMP, and non-Contact Center Cisco products such as UCM, Unity Connection, CUBE gateways, CUSP, IM&P etc. Patches and upgrade operations for these components can be performed in a traditional manner.
- Orchestration is supported only for upgrades and patch install and not for tech refresh or fresh install.
- If any activity is blocked with a message `previous orchestration or upgrade operation is still in progress` even if there is no active operation, then restart Cloud Connect server.
- If one component ES has a dependency on another component ES, then they have to be taken into consideration by the administrator before initiating the patch installation from Cloud Connect server. The administrator should read the release notes that is notified through an email to understand the dependency. The Orchestration framework does not track this aspect automatically. For example, if an ES of Finesse has a dependency on an ES of Live Data and has to be installed in a specific order, then the administrator must consider this before initiating the patch installation from Cloud Connect server.
- Within Upgrade commands 'All Nodes' option for the Roll Back and Switch version commands are not available.
- Only Microsoft Exchange Server is supported for email notification; Office 365 and Gmail are not supported as of now.
- Email notifications are triggered about the available software upgrade from the publisher node of Cloud Connect server. If the publisher node is down at the trigger time, then the Admin will not receive any notification.
- All nodes option in *utils upgrade-manager list* CLI uses an internal cache, which is updated every day at 5 AM. The latest version of components that are upgraded before the cache update scheduled time will not be listed in All nodes option. The latest version of components can be listed by selecting the individual VOS or Windows or group of nodes option in the *utils upgrade-manager list* CLI. The cache update can be enforced by running the *utils system inventory import* CLI.
- For Packaged CCE deployment, only multistage upgrade is supported from Orchestration.

- For Packaged CCE deployment, CVPOAMP is not supported.