Upgrade Overview

Upgrade Overview

Unified CCE Redundant Central Controller Upgrade Flow

The Unified CCE central controller consists of the Logger, Router, and Administration & Data Server. When upgrading the Unified CCE portion of your Cisco Contact Center, the central controller is upgraded before the other Unified CCE components. While one side (Side A or B) of the redundant system is being upgraded, the other side (Side A or B) operates in stand-alone mode.

For redundant systems, the general flow for upgrading the Unified CCE central controller is as follows:

1. Upgrade the Side A Logger and Router along with the Administration & Data Server identified to be upgraded first to verify operations on the upgraded Side A Logger and Router.
2. Bring Side A into service and verify the operation. Side B is brought down as Side A is coming into service along with other non-upgraded Administration & Data Server(s).
3. Upgrade the Side B Logger and Router along with remaining Administration & Data Server(s).
4. Bring Side B into service and verify that duplexed operation begins.

Note For better performance, Media Routing PG (MR PG), Dialer, and Agent PG should be on the same VM.

Update VM Properties

Rather than re-create the VMs in the new version of the OVA, you can manually update the VM properties to match the new OVA. Before you upgrade the Unified CCE or Cloud Connect components, update the properties of each VM to match the appropriate OVA, as follows:

1. Stop the VM.
2. Update the properties of each VM to match the properties of the appropriate OVA. Check the *Virtualization for Unified Contact Center Enterprise* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html for descriptions of each OVA. Save your changes.

   See https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-cloud-connect.html for details on Cloud Connect.
3. Restart the VM.

Caution Be careful when you upgrade the virtual machine network adapters. Done incorrectly, this upgrade can compromise the fault tolerance of your Cisco Contact Center.

SQL Security Hardening

You can optionally apply SQL security hardening when running the installer. If your company employs custom security policies, bypass this option. Most other deployments benefit from SQL security hardening.

Note During Unified CCE installation on to Windows Server 2019 and SQL Server 2019, you should not select SQL Server Security Hardening optional configuration as a part of the installation. You can apply the SQL Security Hardening post installation using the Security Wizard tool.

For more information about SQL security hardening, see the *Security Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Self-signed Certificate for Unified CCE Web Application

Note As part of the upgrade of Unified CCE servers, self-signed certificates employed by Unified CCE web applications such as Unified CCE web administration tool and Websetup, may get regenerated. You must add the new certificates to the trust list on the appropriate end devices.

Upgrade Tools

During the upgrade process, use the following tools as required:

- ICM-CCE-Installer—The main Unified CCE installer. It copies all files into relevant folders, creates the base registries, and installs needed third-party software such as JRE, Apache Tomcat, and Microsoft .NET Framework.

Note Optionally, you can update the JRE installed by the Unified CCE Installer with a later version of the JRE. See Java Upgrades.

If the ICM-CCE installer installs JRE on the Windows platform, the system retains only the Cisco approved CA certificates in the java certificate store, and removes all the unapproved certificates.

Optionally, update the Apache Tomcat software. See Install Tomcat.

You cannot run the installer remotely. Mount the installer ISO file only to a local machine.

- Cisco Unified Intelligent Contact Management Database Administration (ICMDBA) Tool—Used to create new databases, modify or delete existing databases, and perform limited SQL Server configuration tasks.
- Domain Manager—Used to provision Active Directory.
- Web Setup—Used to set up the Call Routers, Loggers, and Administration & Data Servers.
- Peripheral Gateway Setup—Used to set up PGs, the CTI server, and the Outbound Option dialer.

- ICM12.6.1.exe—The Unified CCE patch installer. It copies all files into relevant folders, updates the registries, and installs needed third-party software such as JRE, Apache Tomcat, and Microsoft .NET Framework.
- AdminClientInstaller—Installs the Administration Client on a system that is not running other Unified CCE components.

  The AdminClientInstaller is delivered on the installation media with the installer.
- Administration Client Setup—Used to add, edit, or remove Administration Clients and Administration Client Instances.

  The Administration Client Setup is delivered on the installation media with the installer.
- Enhanced Database Migration Tool (EDMT)—A wizard application that is used for all upgrades to migrate the HDS, Logger, and BA databases during the upgrade process.

  You can download the EDMT from Cisco.com by clicking **Cisco Enhanced Data Migration Tool Software Releases**.

  The prerequisites for running EDMT are:

  - EDMT requires Microsoft® ODBC Driver 17 for SQL Server® and Visual C++ Redistributable for Visual Studio 2015 (or higher). The latest version of these packages can be downloaded from the Microsoft website. However, a copy of the same is also available in the **Prerequisites** folder of EDMT.

  The EDMT displays status messages during the migration process, including warnings and errors. Warnings are displayed for informational purposes only and do not stop the migration. On the other hand, errors stop the migration process and leave the database in a corrupt state. If an error occurs, restore the database from your backup, fix the error, and run the tool again.

Note

- You can select either **SQL Server Authentication** or **Windows Authentication** during database migration. In certain scenarios, for example, where the source and destination machines are in different domains, **SQL Server Authentication** can be used.
- If you are configuring SQL services to run as Virtual account (NT SERVICE) or Network Service account (NT AUTHORITY\NETWORK SERVICE), you must run EDMT as an administrator.
- The installer, not the EDMT, upgrades the AW database for the Administration & Data Server.

- User Migration Tool—A standalone Windows command-line application that is used for all upgrades that involve a change of domain. The tool imports the previously exported user accounts into the target domain during the upgrade.

  You can download the User Migration Tool from Cisco.com by clicking **ICM User Migration Tool Software**.

Note User Migration Tool cannot be used for migrating users that are SSO enabled.

- Regutil Tool—Used in Technology Refresh upgrades, exports the Cisco Systems, Inc. registry in the source machine during the preupgrade process. The output of the tool is required on the destination machine when running the Unified CCE Installer during the upgrade process.

  You can download the Regutil Tool from Cisco.com by clicking **Contact Center Enterprise Tools**.

- My Cisco Entitlements (MCE)—You can order software for upgrades in MCE if you have a valid SWSS or Flex contract. It is a secure one-stop platform where you can gain insights into your business, manage your Cisco products and services, and minimize risk.

  You can access MCE from https://www.cisco.com/c/en/us/products/software/my-cisco-entitlements.html .

Multistage Upgrade Workflow for 2000 Agents Deployment

Note The multistage upgrade workflow is applicable for solution deployments with both main site and remote site (if available).

A Unified CCE solution upgrade likely involves a multistage process; components are grouped in several stages for upgrading. At each stage in the upgrade, the upgraded components must interoperate with components that haven't yet been upgraded to ensure the overall operation of the contact center. Therefore, it's important to verify this interoperability during the planning stages of the upgrade.

Before upgrading a production system, perform the upgrade on a lab system that mirrors your production system to identify potential problems safely.

The following table details the required sequence for upgrading Unified CCE 2000 Agent Deployments components, and the minimum component groupings that must occur together within each stage. Follow each stage to completion within each maintenance window. Each maintenance window must accommodate any testing required to ensure system integrity and contact center operation.

You can combine more than one complete stage into a single maintenance window, but you can't break any one stage into multiple maintenance windows.

Upgrade the Unified CCE components as follows:

Note

- Upgrade Agent Desktop, CUIC, Live Data, and IdS server along with the Unified CCE Central Controller upgrade.
- After upgrading Finesse, IdS, and CUIC, import the IdS certificates to the Finesse and CUIC servers.
- Run Stage 3 and Stage 4 upgrades in the same maintenance window.

Note Components of the same type within a particular stage of the upgrade sequence should be on the same application and operating system version before proceeding to the next stage in upgrade sequence.

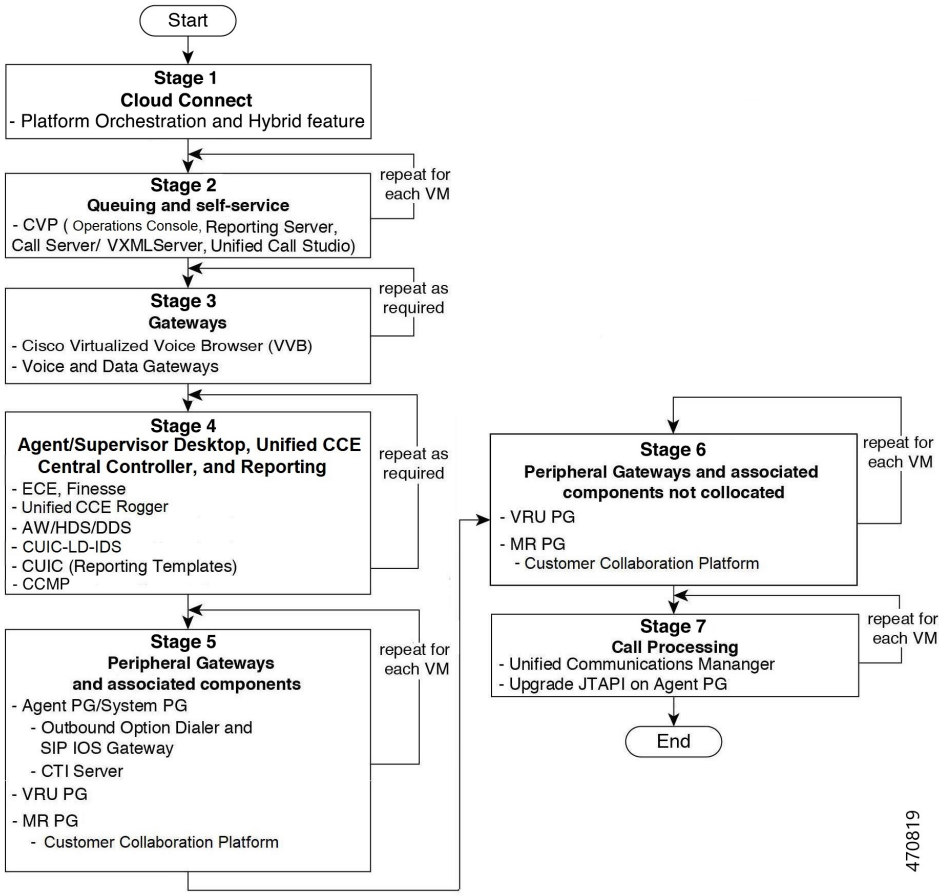
Stage	Component Group	Components	Notes
1	Platform Orchestration, Hybrid Features	Cloud Connect	If you have Cloud Connect in your environment, refer the **Update VM Properties** section in Upgrade Overview, on page 1 for Cloud connect upgrade prerequisite to increase the hard disk and RAM before you upgrade the component. Upgrade both the publisher and subscriber. For Cloud Connect upgrade instructions, see the Upgrade Cloud Connect section. If you don't have Cloud Connect in your environment, and you use any Hybrid feature or Orchestration, fresh install Cloud Connect. For fresh install instructions, see the Install Cloud Connect section.
2	Queuing and self-service	Cisco Unified Customer Voice Portal (CVP) (Operations Console, Reporting Server, Call Server/VXMLServer, Unified Call Studio)	You must upgrade all sites before proceeding to the next stage. For more information, see *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html.

Stage	Component Group	Components	Notes
3	Gateways	• IOS Gateways (If used for ingress access only. If used for Outbound Option Dialer, see Stage 5.) • IOS VXML Gateways • Cisco Virtualized Voice Browser	
4	Agent/Supervisor Desktop, Central Controller, and Reporting	• ECE • Cisco Finesse • Unified CCE Rogger • Admin & Data server (AW/HDS/DDS) • CUIC-LD-IDS • CUIC Reporting Templates • CCMP	• After you upgrade AW, import the self-signed certificate of all solution components (if applicable) to all AWs. • After you upgrade Finesse to Release 12.6(x) , to load any gadgets to Finesse, you must first import all self-signed certificates (if applicable) to Finesse. **Note** After upgrading cuic-ld-ids to 12.6, run the **utils finesse layout updateCuicGadgetUrl** command to update the gadget URL. For more information about Finesse, see *Cisco Finesse Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-installation-guides-list.html. For more information about ECE, see https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html • After you upgrade Live Data (LD), you must enable CORS on the LD box for Finesse and CUIC. For more information, see *Installation and Upgrade Guide for Cisco Unified Intelligence Center* Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html. • After you upgrade LD, you must import the Finesse certificate to LD.

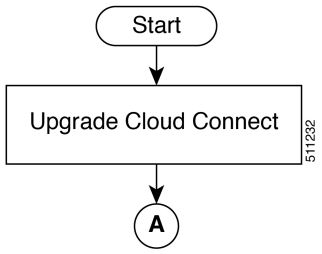
Stage	Component Group	Components	Notes
5	Peripherals	• Agent (Unified Communications Manager) PG • CTI Server • Outbound Option Dialer and SIP IOS Gateway	You can have many PGs located on different virtual machines. You can upgrade each PG virtual machine in its own maintenance window.
6	Peripherals	• MR PG, VRU PG • CRM connector	You can have many PGs located on different virtual machines. You can upgrade each PG virtual machine in its own maintenance window.
7	Call Processing	• Cisco Unified Communications Manager (Unified Communications Manager) • JTAPI on Agent (Unified Communications Manager) PG	You must install JTAPI client only when you upgrade to UCM 12.5. If you upgrade to CUCM 12.5 on the M4 servers, ensure that you deploy CUCM off-box. For more information, refer to *Virtualization for Unified Contact Center Enterprise* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html.

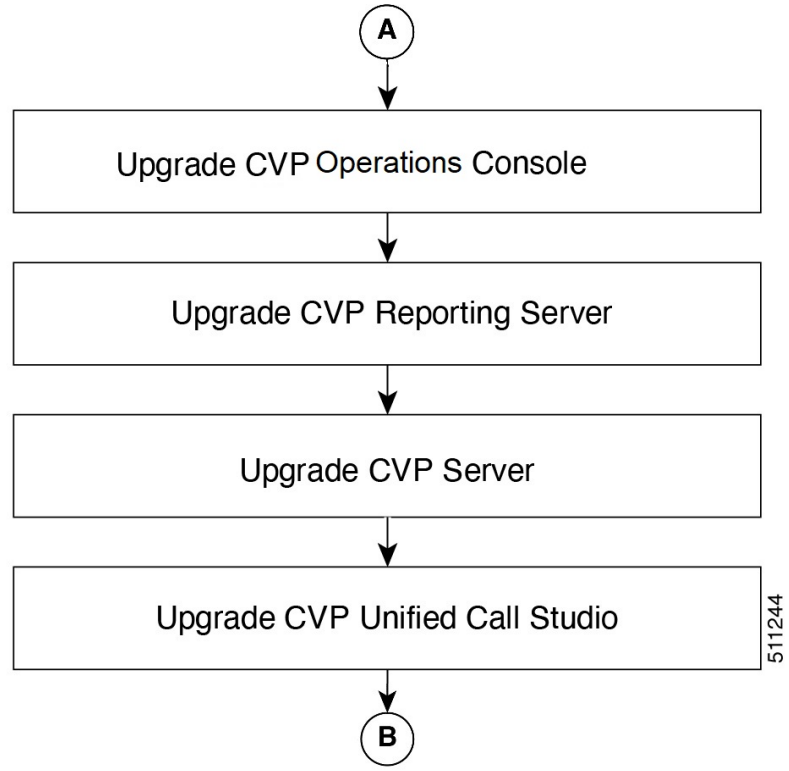
Upgrade Flowcharts

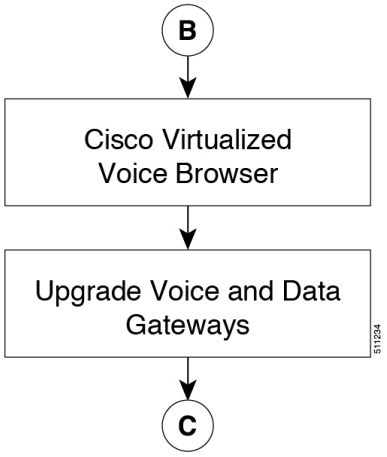
The following diagram illustrates the solution-level upgrade flow for the Unified CCE 2000 Agent Deployment solution upgrade.

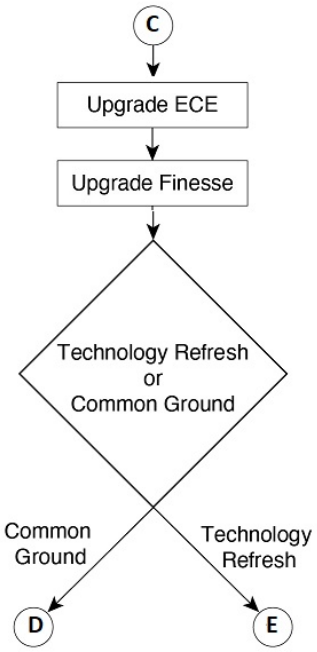


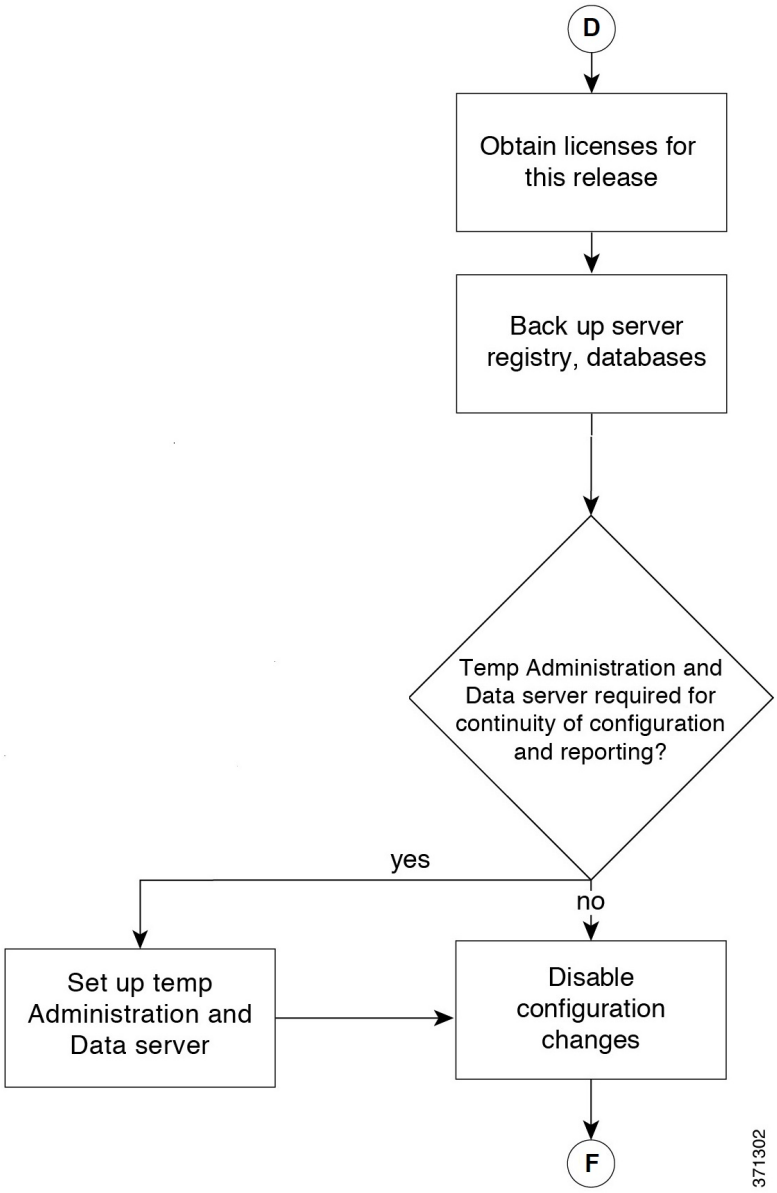
The following diagrams illustrate the stages of the component-level upgrade flows for the Unified CCE 2000 Agent Deployment solution upgrade. Each diagram covers one of the stages. The letter at the end of each flow indicates the start of the next flow that you are required to perform.

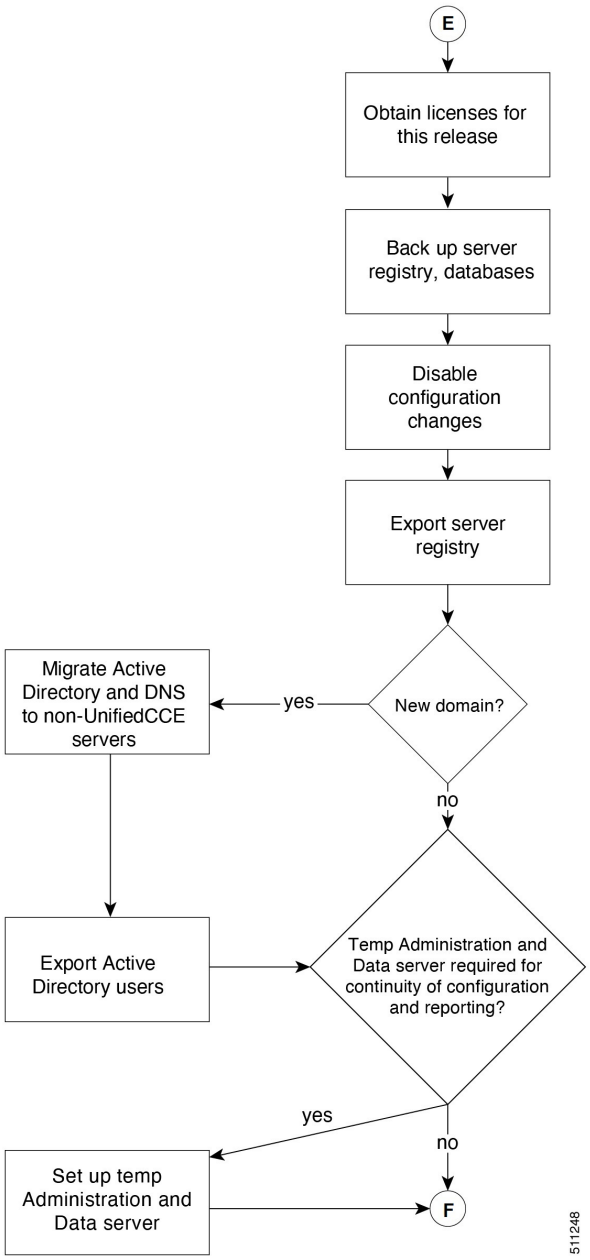


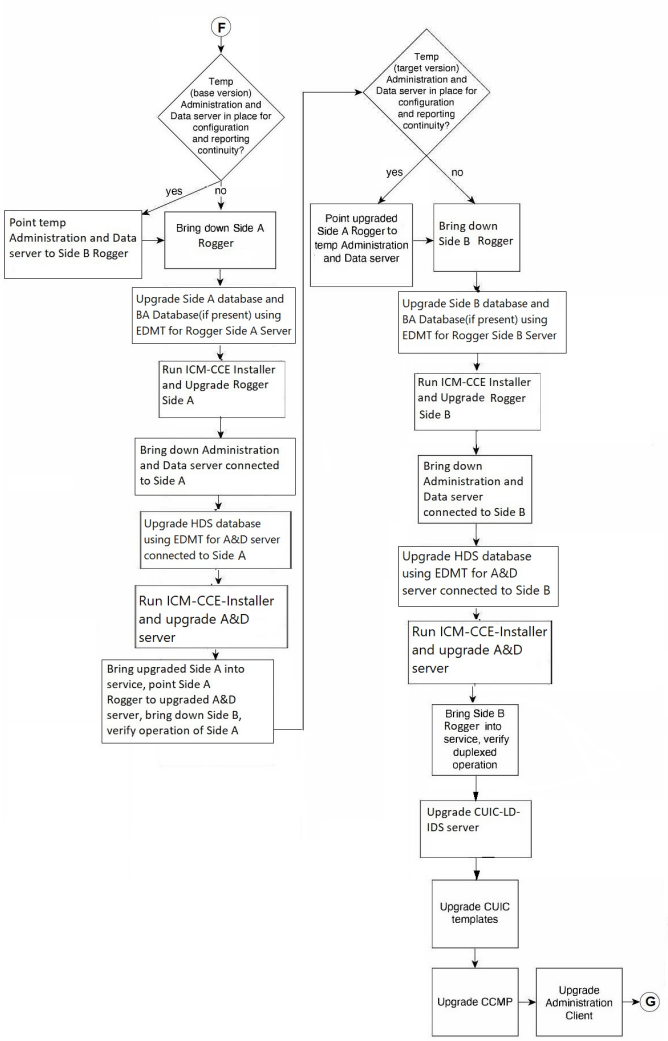

A
Upgrade CVP Operations Console
Upgrade CVP Reporting Server
Upgrade CVP Server
Upgrade CVP Unified Call Studio
511244
B

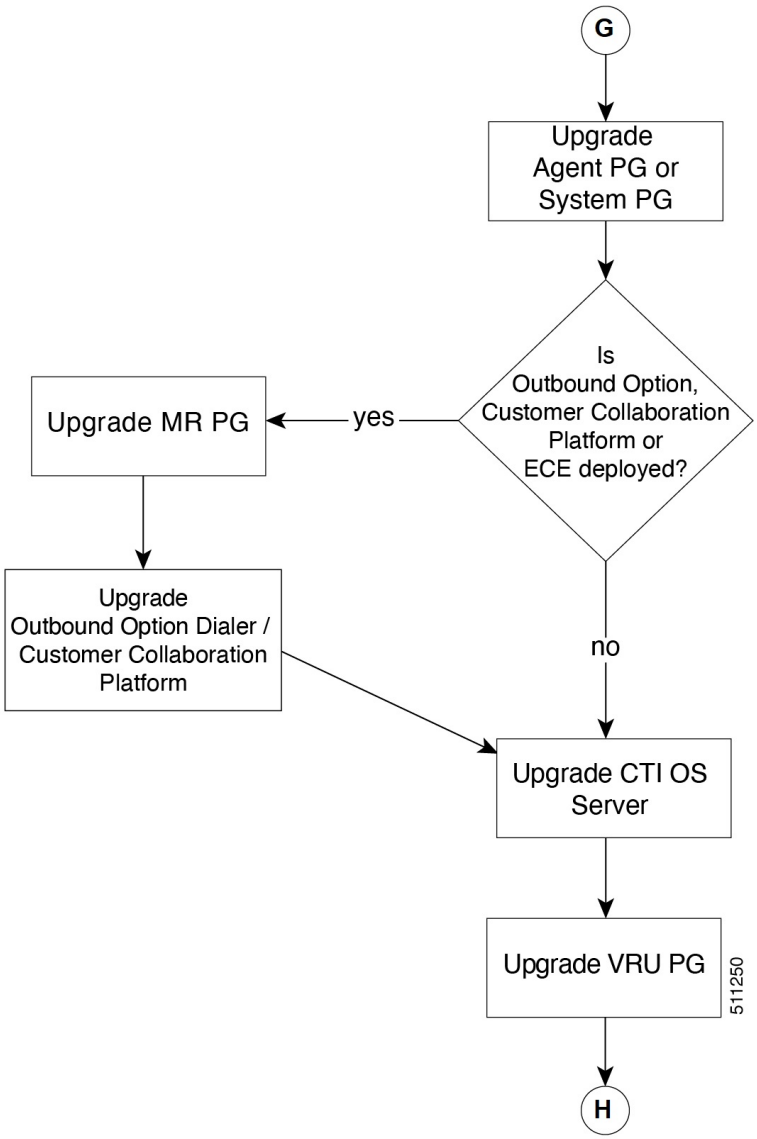

B
Cisco Virtualized Voice Browser
Upgrade Voice and Data Gateways
511234
C

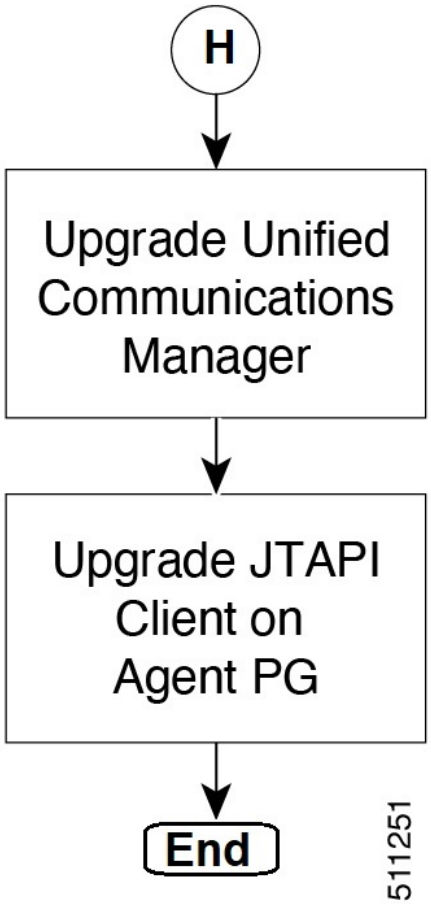

C
Upgrade ECE
Upgrade Finesse
Technology Refresh
or
Common Ground
Common
Ground
Technology
Refresh
D
E


D
Obtain licenses for this release
Back up server registry, databases
Temp Administration and Data server required for continuity of configuration and reporting?
yes
no
Set up temp Administration and Data server
Disable configuration changes
F
371302


E
Obtain licenses for this release
Back up server registry, databases
Disable configuration changes
Export server registry
New domain?
yes
Migrate Active Directory and DNS to non-UnifiedCCE servers
no
Export Active Directory users
Temp Administration and Data server required for continuity of configuration and reporting?
yes
no
Set up temp Administration and Data server
F
511248


F
Temp (base version) Administration and Data server in place for configuration and reporting continuity?
yes
no
Point temp Administration and Data server to Side B Rogger
Bring down Side A Rogger
Upgrade Side A database and BA Database(if present) using EDMT for Rogger Side A Server
Run ICM-CCE Installer and Upgrade Rogger Side A
Bring down Administration and Data server connected to Side A
Upgrade HDS database using EDMT for A&D server connected to Side A
Run ICM-CCE-Installer and upgrade A&D server
Bring upgraded Side A into service, point Side A Rogger to upgraded A&D server, bring down Side B, verify operation of Side A
Temp (target version) Administration and Data server in place for configuration and reporting continuity?
yes
no
Point upgraded Side A Rogger to temp Administration and Data server
Bring down Side B Rogger
Upgrade Side B database and BA Database(if present) using EDMT for Rogger Side B Server
Run ICM-CCE Installer and Upgrade Rogger Side B
Bring down Administration and Data server connected to Side B
Upgrade HDS database using EDMT for A&D server connected to Side B
Run ICM-CCE-Installer and upgrade A&D server
Bring Side B Rogger into service, verify duplexed operation
Upgrade CUIC-LD-IDS server
Upgrade CUIC templates
Upgrade CCMP
Upgrade Administration Client
G


G
Upgrade Agent PG or System PG
Is Outbound Option, Customer Collaboration Platform or ECE deployed?
yes
Upgrade MR PG
Upgrade Outbound Option Dialer / Customer Collaboration Platform
no
Upgrade CTI OS Server
Upgrade VRU PG
H
511250



Multistage Upgrade Workflow for 4000 Agents and above Deployments

A Unified CCE solution upgrade likely involves a multistage process; components are grouped in several stages for upgrading. At each stage in the upgrade, the upgraded components must interoperate with components that haven't yet been upgraded to ensure the overall operation of the contact center. Therefore, it's important to verify this interoperability during the planning stages of the upgrade.

Before upgrading a production system, perform the upgrade on a lab system that mirrors your production system to identify potential problems safely.

The following table details the required sequence for upgrading Unified CCE solution components, and the minimum component groupings that must occur together within each stage. Follow each stage to completion within each maintenance window. Each maintenance window must accommodate any testing required to ensure system integrity and contact center operation.

You can combine more than one complete stage into a single maintenance window, but you can't break any one stage into multiple maintenance windows.

Note

- For coresident configurations, upgrade CUIC/LiveData/IdS server along with the Unified CCE Central Controller upgrade.
- After you upgrade the Standalone Live Data server, upgrade the VMware Tools manually. After upgrading the VMware Tools, check the Check and upgrade VMware Tools before each power on box in **VM Options > VM Edit Settings**.

Upgrade the components that apply to your Unified CCE contact center as follows:

Note Components of the same type within a particular stage of the upgrade sequence should be on the same application and operating system version before proceeding to the next stage in upgrade sequence.

Note In case of 4K deployment, the Unified CCE components consist of Rogger VM instead of Router and Logger VMs.

Stage	Component Group	Components	Notes
1	Platform Orchestration, Hybrid Features	Cloud Connect	If you have Cloud Connect in your environment, refer the **Update VM Properties** section in Upgrade Overview, on page 1 for Cloud connect upgrade prerequisite to increase the hard disk and RAM before you upgrade the component. Upgrade both the publisher and subscriber. For Cloud Connect upgrade instructions, see the Upgrade Cloud Connect section. If you do not have Cloud Connect in your environment, and you use any Hybrid feature or Orchestration, fresh install Cloud Connect. For fresh install instructions, see the Install Cloud Connect section.
2	Queuing and self-service[1]	Cisco Unified Customer Voice Portal (CVP) (Operations Console, Reporting Server, Call Server/VXMLServer, Unified Call Studio)	• For more information, see *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html.

Stage	Component Group	Components	Notes
3	Gateways	• IOS Gateways (If used for ingress access only. If used for Outbound Option Dialer, see Stage 8.) • IOS VXML Gateways • Cisco Virtualized Voice Browser	
4	Identity Service (IdS)/Single Sign-On(SSO)	IdS Server	• Cisco IdS 12.6(2) upgrade requires all SSO clients to log out from SSO, before any of the upgraded nodes is brought online. To avoid this requirement, it's recommended that you install 12.6(2) ES02 on the upgraded node and wait for the access token to expire before commencing the secondary node upgrade. Without installing 12.6(2) ES02, graceful shutdown feature will not be available for Cisco IdS 12.6(2) upgrade. You can view the duration of access token expiry in the IdS administration portal under **Settings** > **Security** > **Tokens** > **Access Token Expiry**. Deployments using VPN-less access to Finesse desktop should also upgrade the reverse proxy to 12.6(2) before Cisco IdS is upgraded to 12.6(2). • SSO is an optional feature and exchanges authentication and authorization details between the IdS component and IdP provider. For more information, see Upgrade Flowcharts, on page 19. • For IdS upgrade, see the procedure as documented in the *Upgrades* section of *Unified Intelligence Center Installation and Upgrade Guide* at: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html

Stage	Component Group	Components	Notes
5	Agent and supervisor desktops	Cisco Finesse ECE	• To load any gadget to Finesse, you must first import the certificate to Finesse. **Note** For Finesse VM, you have to increase the RAM before upgrading. See https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html For more information, see *Cisco Finesse Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-installation-guides-list.html. • For more information about ECE, see https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html.

6	Reporting server	CUIC server	• After you upgrade Cisco Unified Intelligence Center (CUIC), you must:
			  • Enable CORS on the CUIC server, and add **`cors allowed_origin`** with the Finesse hostname.
			  • Import LD and Finesse certificates to CUIC.
			For more information, see *Installation and Upgrade Guide for Cisco Unified Intelligence Center* Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html.

7	Central Controller	• Unified CCE Router • Unified CCE Logger • Admin & Data server (AW/HDS/DDS) • Standalone Live Data (if Deployed) • CUIC Reporting Templates • CCMP • Administration Client	• After you upgrade AW, import the self-signed certificate of all solution components (if applicable) to all AWs. • After you upgrade Live Data (LD), you must enable CORS on the LD box for Finesse and CUIC. For more information, see *Installation and Upgrade Guide for Cisco Unified Intelligence Center* Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html. • After you upgrade LD, you must import the Finesse certificate to LD. **Note** For Live Data VM, increase the RAM before you upgrade the VM. See Cisco Collaboration Virtualization.

Stage	Component Group	Components	Notes
8	Peripherals	• Agent (Unified Communications Manager) PG or System PG, plus • CTI Server • CTI OS Server • Outbound Option Dialer and SIP IOS Gateway	You can have many PGs located on different virtual machines. You can upgrade each PG virtual machine in its own maintenance window. **Note** Media Routing PG (MR PG), Dialer, and Agent PG must be upgraded in the same window.
9	Peripherals	• MR PG (if not collocated with Agent PG on VM), plus VRU PG (if not collocated with Agent PG on VM) • Unified CCE Gateway PG (if not collocated with Agent PG on VM) • CRM connector	You can have many PGs located on different virtual machines. You can upgrade each PG virtual machine in its own maintenance window. **Note** Media Routing PG (MR PG), Dialer, and Agent PG must be upgraded in the same window.
10	Agent desktop client software	CTI OS (Agent/Supervisor Desktops)	You can have many desktops located in many different sites. You can upgrade CTI OS desktops in multiple maintenance windows; the later upgrade stages are not dependent on the completion of this stage.
11	Call Processing	• Cisco Unified Communications Manager (Unified Communications Manager) • JTAPI on Agent (Unified Communications Manager) PG	If you upgrade to CUCM 12.5 on the M4 servers, ensure that you deploy CUCM off-box. For more information, refer to *Virtualization for Unified Contact Center Enterprise* at http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html.

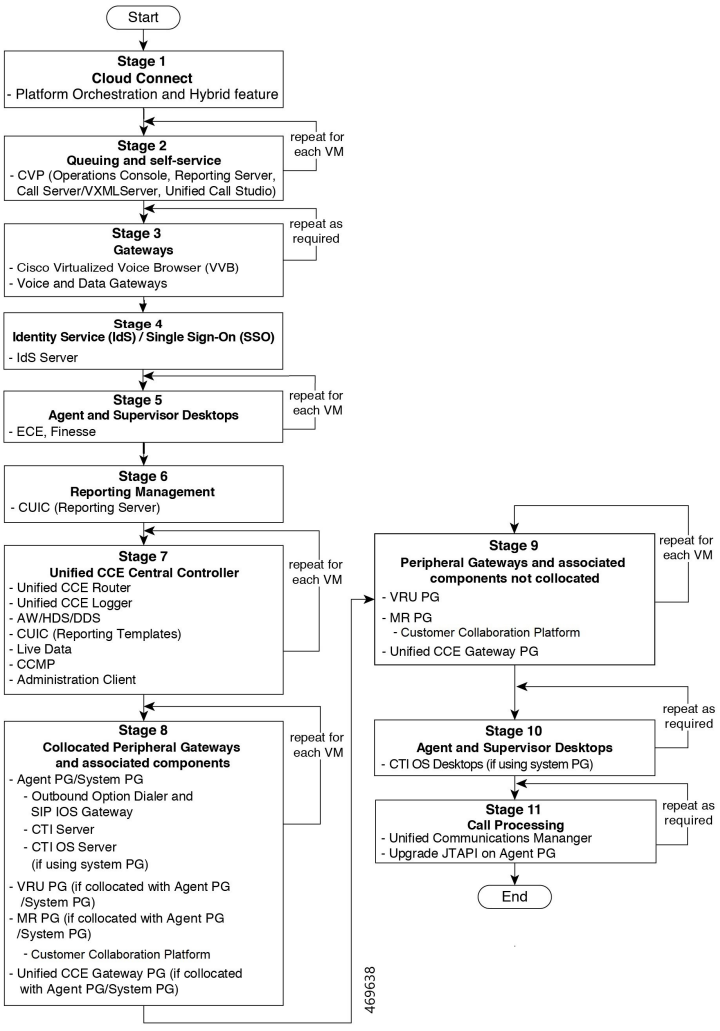
[1] If you are using Unified IP IVR for self-service and queueing, see Getting Started with Cisco Unified IP IVR.

Upgrade Flowcharts

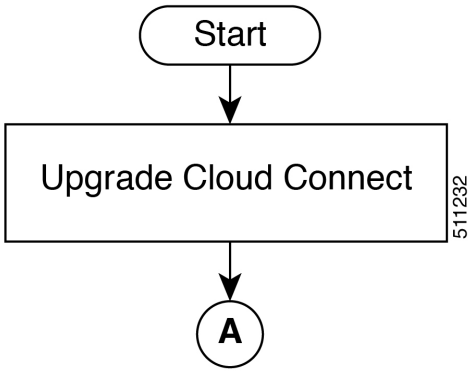
Note The multi-stage upgrade flowchart is not applicable for Centralized UCCE 2K deployments that essentially employ a co-resident CUIC/LiveData/IdS server, and have a single Agent PG VM pair.

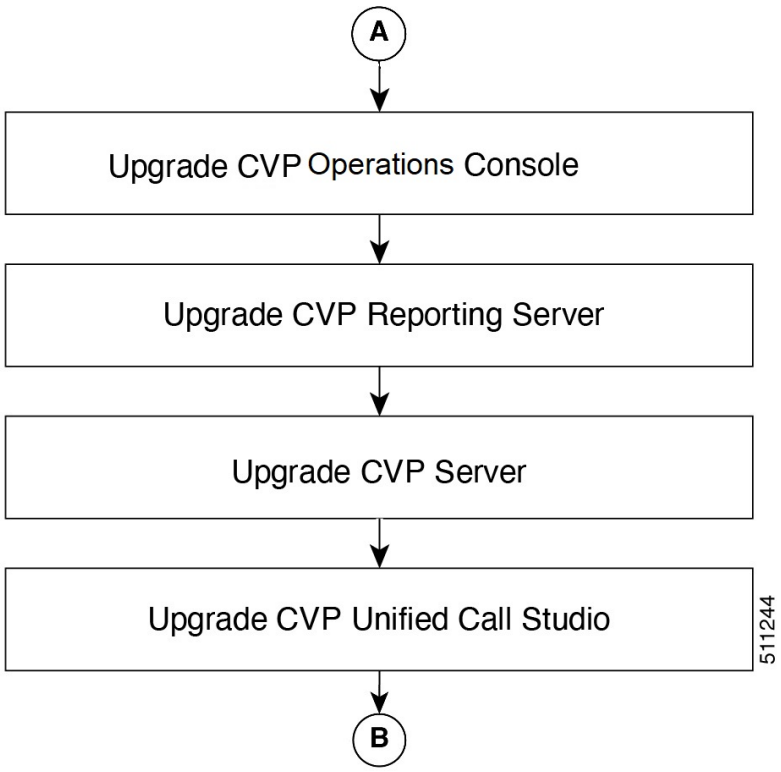
Note After upgrading Finesse, IdS, and CUIC, import IdS certificates on Finesse and CUIC servers.

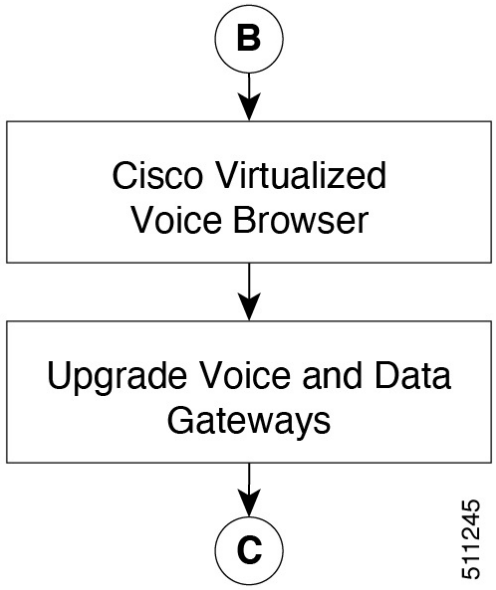
The following diagram illustrates the solution-level upgrade flow for Cisco Contact Center Enterprise solution upgrade.

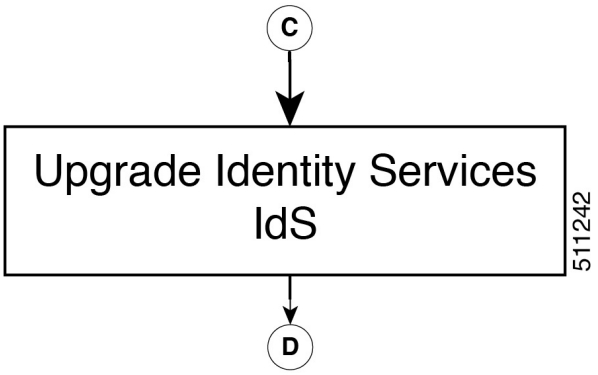


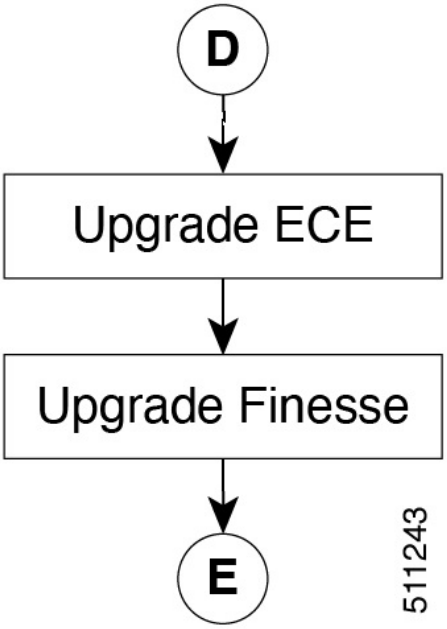
The following diagrams illustrate the stages of the component-level upgrade flows for a Cisco Unified Contact Center Enterprise solution upgrade. Each diagram covers one of the stages. The letter at the end of each flow indicates the start of the next flow that you are required to perform.

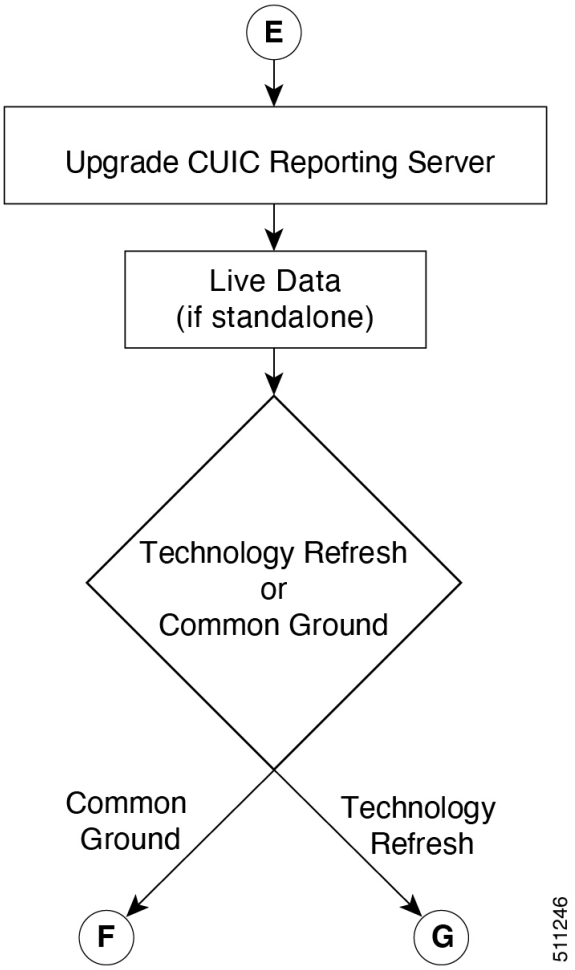

Start
Upgrade Cloud Connect
511232
A

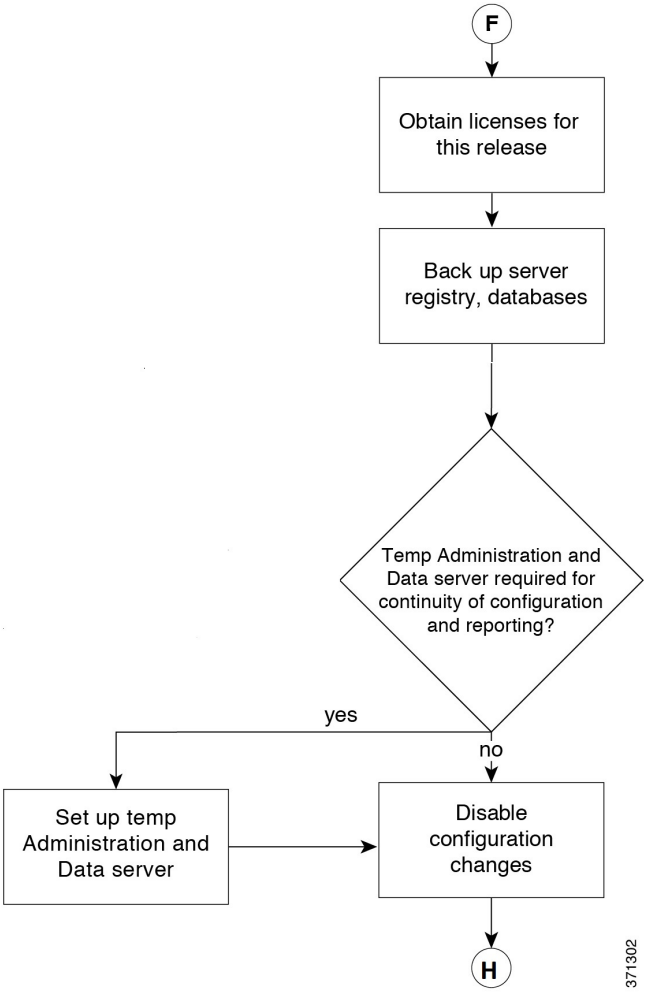

A
Upgrade CVP Operations Console
Upgrade CVP Reporting Server
Upgrade CVP Server
Upgrade CVP Unified Call Studio
511244
B

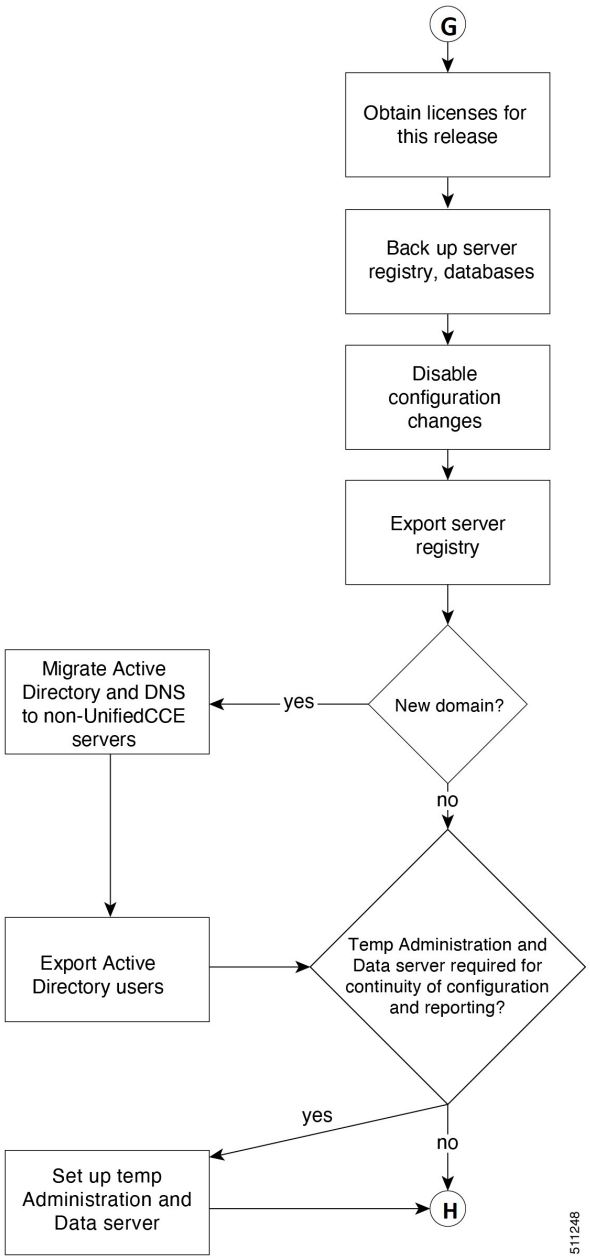

B
Cisco Virtualized Voice Browser
Upgrade Voice and Data Gateways
C
511245

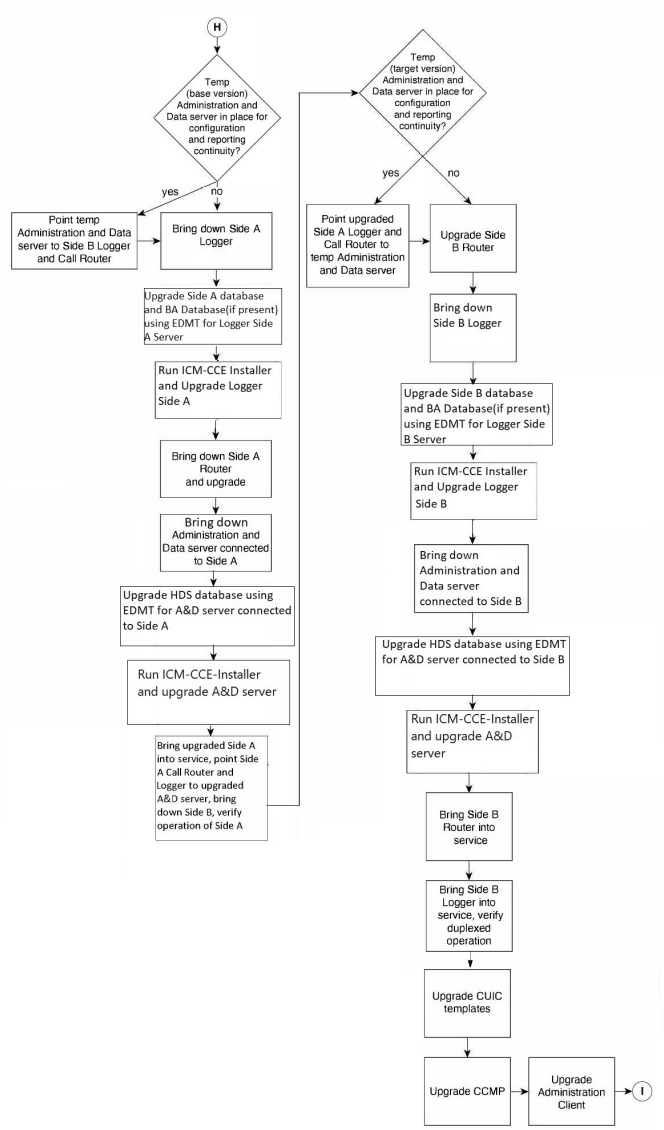

C
Upgrade Identity Services IdS
511242
D

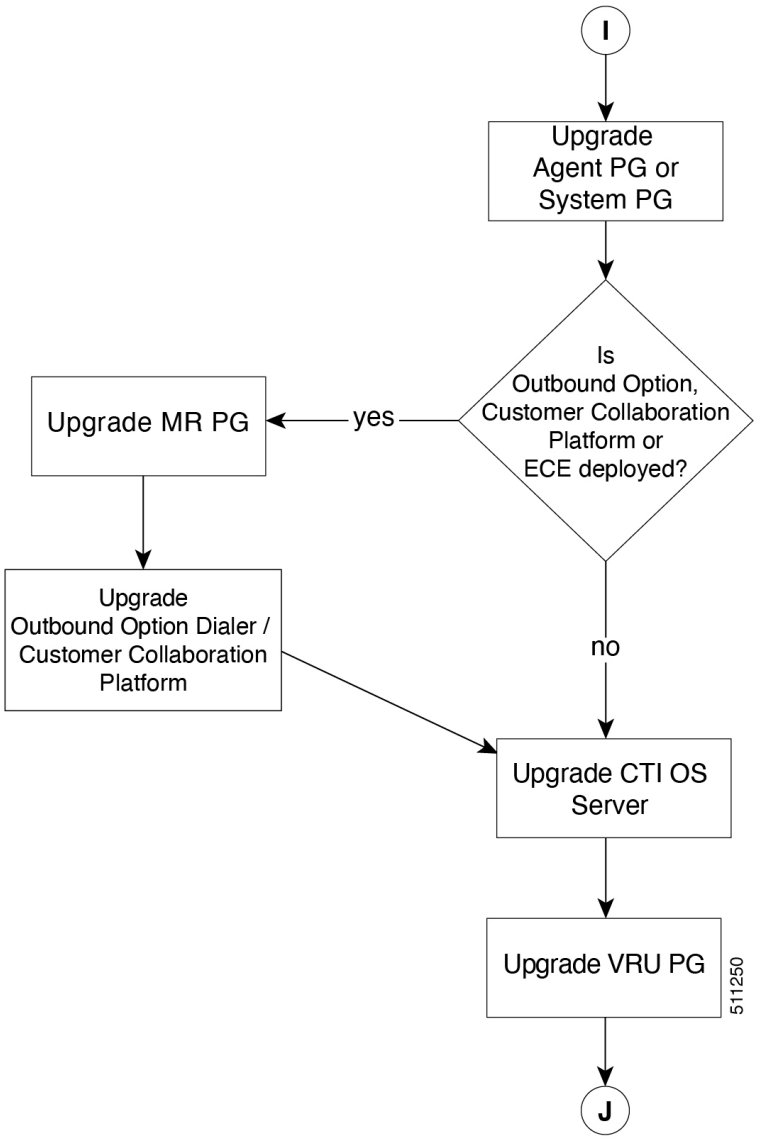

D
Upgrade ECE
Upgrade Finesse
E
511243

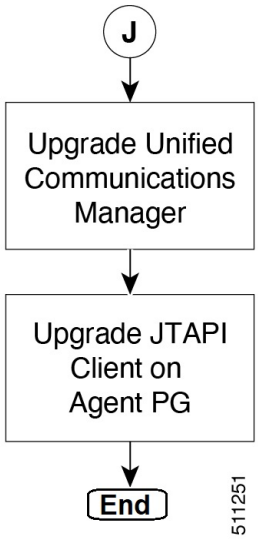

E
Upgrade CUIC Reporting Server
Live Data
(if standalone)
Technology Refresh
or
Common Ground
Common
Ground
Technology
Refresh
F
G
511246


F
Obtain licenses for this release
Back up server registry, databases
Temp Administration and Data server required for continuity of configuration and reporting?
yes
no
Set up temp Administration and Data server
Disable configuration changes
H
371302


G
Obtain licenses for this release
Back up server registry, databases
Disable configuration changes
Export server registry
New domain?
yes
Migrate Active Directory and DNS to non-UnifiedCCE servers
no
Export Active Directory users
Temp Administration and Data server required for continuity of configuration and reporting?
yes
no
Set up temp Administration and Data server
H
511248


H
Temp (base version) Administration and Data server in place for configuration and reporting continuity?
yes
no
Point temp Administration and Data server to Side B Logger and Call Router
Bring down Side A Logger
Upgrade Side A database and BA Database(if present) using EDMT for Logger Side A Server
Run ICM-CCE Installer and Upgrade Logger Side A
Bring down Side A Router and upgrade
Bring down Administration and Data server connected to Side A
Upgrade HDS database using EDMT for A&D server connected to Side A
Run ICM-CCE-Installer and upgrade A&D server
Bring upgraded Side A into service, point Side A Call Router and Logger to upgraded A&D server, bring down Side B, verify operation of Side A
Temp (target version) Administration and Data server in place for configuration and reporting continuity?
yes
no
Point upgraded Side A Logger and Call Router to temp Administration and Data server
Upgrade Side B Router
Bring down Side B Logger
Upgrade Side B database and BA Database(if present) using EDMT for Logger Side B Server
Run ICM-CCE Installer and Upgrade Logger Side B
Bring down Administration and Data server connected to Side B
Upgrade HDS database using EDMT for A&D server connected to Side B
Run ICM-CCE-Installer and upgrade A&D server
Bring Side B Router into service
Bring Side B Logger into service, verify duplexed operation
Upgrade CUIC templates
Upgrade CCMP
Upgrade Administration Client
I


I
Upgrade Agent PG or System PG
Is Outbound Option, Customer Collaboration Platform or ECE deployed?
yes
Upgrade MR PG
Upgrade Outbound Option Dialer / Customer Collaboration Platform
no
Upgrade CTI OS Server
Upgrade VRU PG
J
511250



Data Migration Considerations

Note The EDMT may take a long time to migrate, backup, or restore the data, as the file sizes can be several gigabytes (GB). If the EDMT tool is not responding during data migration or the data migration takes a long time, check the Event logs in the Microsoft Windows Event Viewer tool. The logs may show SQL or BACKUP failure events. These events may occur because of file system errors or hardware errors and failures. Analyze and fix these errors before re-running the EDMT tool.

To reduce data migration time, consider reducing the database size by:

- Removing redundant records, especially call detail records (RCD, RCV, TCD, and TCV tables). However, removing records affects the availability of historical reports; knowledge of the HDS schema is required.
- Purging the Logger database of all data that was already replicated to the HDS (25 GB or less).
- Using more efficient hardware, especially on I/O subsystems:
  - RAID 1 + 0
  - I/O Cache – more is better

Enable the Tempdb log to expand up to 3 GB.

Note When you upgrade to Cisco Unified Contact Center Enterprise, Release , the Do Not Call table that existed before the upgrade is not available. Therefore, you must import the Do Not Call table.

Required Disk Space for Migration

1. Run **EXEC sp_spaceused** command in the SQL Server.
2. Determine the following:
   - DUS (Database Used Size).

     Calculated as:

     Database Used Size (DUS) = (database_size – unallocated space)
   - Required disk space by EDMT for backup of database

     Calculated as:

     Space that is used for backup = 1.2 times of DUS.

Note Note: When the backup and restore drive are same, then required disk space by EDMT is equal to restore database size plus space used for backup.

Note When the backup and restore has to be done through EDMT, and since the database backup contains encrypted data, this process cannot be performed unless the source certificate that encrypted the database is copied to the destination server.

Follow the procedures outlined in the below Microsoft documentation to restore the certificate on destination server.

- https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/move-a-tde-protected-database-to-another-sql-server?view=sql-server-ver15
- https://www.sqlshack.com/restoring-transparent-data-encryption-tde-enabled-databases-on-a-different-server/
- https://www.databasejournal.com/tips/how-to-move-a-tde-encryption-key-to-another-sql-server-instance.html

If you do not want to move the encrypted backup, then disable TDE on the source database, perform the backup and restore through EDMT, and enable TDE on destination database. To enable and disable TDE on the database, see Enable and Disable TDE on a Database, on page 31.

Time Guidelines and Migration Performance Values

For a close estimate of time and space requirements, run EDMT against a copy of your production database on hardware that is similar to your production environment, in a lab environment. For customers who do not have the facility, the following sections provide information that is gathered while performance testing in the labs at Cisco Systems, Inc.

- **Typical database migration performance values**: The following table provides high-level guidelines for the time that is taken to upgrade the Loggers and HDSs based on internal upgrade testing with hardware Cisco UCS C240 M4SX. Actual times may vary based on the parameters previously mentioned.

- **Backup and Restore - Technology Refresh only**: The backup speed depends on the speed of the network, and the speed of the disk sub-system. The faster the network, the sooner the network copy.

Database Used Size (GB)	Backup/Restore Time (hours)	Data Migration Time (minutes)	Total Time (hours)
500 GB	1.5-2 hrs	< 2 mins	2 - 2.5 hrs

Note

- The values in the Database Used Size column are based on the amount of disk space that is used by the source database, and not the size of the disk it resides on.
- The values in the Backup Time and Restore Time columns assumes that the network meets the minimum requirements.

  For more information about the minimum requirements, refer to the *Virtualization for Unified Contact Center Enterprise* at http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html .
- For Technology Refresh upgrades, have the fastest network possible (gigabit through one network switch) between the source and the destination machines. Use of a crossover cable is not supported because it lacks buffer memory and can cause data loss.

Enable and Disable TDE on a Database

To enable Transparent Data Encryption (TDE) on a database, perform the following:

Note These steps are to be performed with sysadmin user permission.

1. Create a server certificate data encryption key.

```
USE master
GO
CREATE CERTIFICATE DEKCert WITH SUBJECT = 'DEK Certificate'
GO
```

2. Create a backup of the server certificate data encryption key.

```
BACKUP CERTIFICATE DEKCert TO FILE = '<SystemDrive>:\DEKCert'
WITH PRIVATE KEY ( FILE = '<SystemDrive>:\temp\DEKCertPrivKey' ,
ENCRYPTION BY PASSWORD = 'C1sco123=' )
GO
```

3. Create database encryption key for the database to configure transparent data encryption. In the following query, *ucce_sideA* is the name of the active database.

```
USE ucce_sideA
GO
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_256
ENCRYPTION BY SERVER CERTIFICATE DEKCert
GO
```

4. Enable database encryption. Run the following query where *ucce_sideA* is the name of the active database.

```
ALTER DATABASE ucce_sideA SET ENCRYPTION ON
```

Note By setting encryption on, a background task starts encrypting all the data pages and the log file. This can take a considerable amount of time, depending on the size of the database. Database maintenance operations should not be performed when this encryption scan is running.

5. To query the status of the database encryption and its percentage completion, query the new sys.dm_database_encryption_keys.

```
SELECT DB_NAME(e.database_id) AS DatabaseName,
e.database_id,
e.encryption_state,
CASE e.encryption_state
WHEN 0 THEN 'No database encryption key present, no encryption'
WHEN 1 THEN 'Unencrypted'
WHEN 2 THEN 'Encryption in progress'
WHEN 3 THEN 'Encrypted'
WHEN 4 THEN 'Key change in progress'
WHEN 5 THEN 'Decryption in progress'
END AS encryption_state_desc,
c.name,
e.percent_complete
FROM sys.dm_database_encryption_keys AS e
LEFT JOIN master.sys.certificates AS c
ON e.encryptor_thumbprint = c.thumbprint
```

To disable TDE on a database, perform the following:

```
USE master;
GO
ALTER DATABASE ucce_sideA SET ENCRYPTION OFF;
GO
-- Remove Encryption Key from Database
USE ucce_sideA;
GO
DROP DATABASE ENCRYPTION KEY;
GO
```

Silent Upgrade

There are situations when silent upgrade can be used in running an installation wizard. You can run a silent installation while performing a fresh install or an upgrade.

For more information, see Silent Installation.

Unified CCE Upgrade Overview

The supported upgrade paths to Unified CCE 12.6(1) are as follows:

- Unified CCE 12.0(1) to Unified CCE 12.5(1) followed by Unified CCE 12.6(1). Use EDMT during this upgrade process.

Note In case of Common Ground upgrade, use 12.5(x) EDMT to upgrade from Unified CCE 12.0(1) to Unified CCE 12.5(1).

- Unified CCE 12.5(1) to Unified CCE 12.6(1). EDMT is not required during this upgrade process. If Windows and SQL platform upgrade is involved during this upgrade process, refer to Technology Refresh Upgrade section for details on using EDMT.

Upgrade Prerequisites

Before you begin

- Make sure that Windows Update is not running in parallel when you begin installation.
- Before you upgrade the Cisco VOS based servers such as the Live Data server, check the **Check and upgrade VMware Tools before each power on** box in the VM's **Options** > **Edit Settings**.

  For more information on VMware Tools upgrade, see the VMware documentation.
- The minimum disk space required to perform the upgrade is 2175 MB.

Custom Truststore to Store Component Certificates

Starting Unified CCE 12.6(x), a new custom truststore is created under the Unified ICM Installation directory `<ICM install directory>\ssl\cacerts` to store all the component certificates. With this new custom truststore, you don't need to export and import the certificates each time Java is updated in the system.

After upgrading from Unified CCE 12.5(x) to Unified CCE 12.6(x), you should export the certificates from the Java truststore to the custom truststore under the Unified ICM Installation directory `<ICM install directory>\ssl\cacerts`.

Export the certificate from the Java truststore:

- Run the command at the command prompt: `cd %JAVA_HOME%\bin`.

Important Use CCE_JAVA_HOME if upgrading from Unified CCE 12.5(1a) or Unified CCE 12.5(1) with ES55 (mandatory OpenJDK ES).

- Export the certificates of all the components imported into the truststore.

  The command to export the certificates is *keytool -export -keystore <JRE path>\lib\security\cacerts -alias <alias of the component> -file <filepath>.cer*
- Enter the truststore password when prompted.

Import the certificate to the custom truststore:

- Run the command at the command prompt: `cd %CCE_JAVA_HOME%\bin`.
- Import the certificates for all the components that you exported from the Java truststore.

The command to import certificates is *keytool -import -keystore <ICM install directory>\ssl\cacerts -file <filepath>.cer -alias <alias>*.

- Enter the truststore password when prompted.
- Enter 'yes' when prompted to trust the certificate.

Upgrade Cloud Connect

Follow the steps to install the ISO file using the Cloud Connect Command line interface (CLI).

You can also install the ISO using the upgrade procedure in the Cisco Unified Operating System Administration web interface. For more information, see *Access Unified OS Administration*.

Before you begin:

Before you begin the upgrade from Cloud Connect 12.5(1) to Cloud Connect 12.6(1), check if the **ucos.keymanagement.v01.cop.sgn** is applied on the base version. The upgrade fails if you don't install the **ucos.keymanagement.v01.cop.sgn**.

Download the ISO file from the software download page for Cloud Connect https://software.cisco.com/download/home/268439622/type/283914286/release/12.6(1) to the SFTP server that can be accessed from the Cloud Connect system.

1. Log in to Cloud Connect CLI and specify the System Administration username and password.
2. Enter the command `utils system upgrade initiate` to initiate the ISO installation.
3. Select **Remote File System** from source list page.
4. Enter the remote path to the directory on the SFTP server where you have downloaded the ISO file.

Note If the ISO file is located on a Linux or UNIX server, you must enter a forward slash (/) at the beginning of the directory path. For example, if the ES file is in the patches directory, enter **/patches**. If the ISO file is located on a Windows server, check with your system administrator for the correct directory path.

5. Enter the SFTP server name or IP address and then enter the credentials.

   It is optional for you to enter the SMTP Host Server name.
6. Select the transfer protocol as SFTP. The system displays the list of ISO files available in the SFTP location.
7. Select the number corresponding to the ISO file that you want to install and press **Enter**.
8. Enter the following options when you are prompted `Switch to new version if the upgrade is successful (yes/no).`
   - Enter **yes** to automatically switch the version.
   - Enter **no** if you need to manually switch the version after all the nodes are upgraded (refer step 10 for more details).

Note Verify if the node is upgraded to Cloud Connect 12.6, after you switch the version successfully (where active version is Cloud Connect 12.6 and inactive version is Cloud Connect 12.5).

9. In cluster setup, first complete the upgrade on the publisher node and perform the upgrade on the subscriber node. After successful upgrades, perform switch version using the command `utils system switch-version` first on the publisher node and later on the subscriber nodes.

Note Verify if the nodes are upgraded to Cloud Connect 12.6, after you switch the version of the publisher node and subscriber nodes successfully (where active version is Cloud Connect 12.6 and inactive version is Cloud Connect 12.5).