Upgrade Overview

- Upgrade Overview, on page 1
- Multistage Upgrades and Maintenance Windows, on page 4
- Unified CCE Contact Center Upgrade Flowcharts, on page 7
- Data Migration Considerations, on page 22
- Enable and Disable TDE on a Database, on page 24
- Silent Upgrade, on page 25
- Unified CCE Upgrade Overview, on page 25

Upgrade Overview

Redundant Central Controller Upgrade Flow

The central controller consists of the Logger, Router, and Administration & Data Server. When upgrading the portion of your Cisco Contact Center, the central controller is upgraded before the other 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 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.

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. After you upgrade the vSphere ESXi and before you upgrade the components, update the properties of each VM to match the appropriate OVA, as follows:

1. Stop the VM.
2. 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.

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:

- AdminClientInstaller—Installs the Administration Client on a system that is not running other components.

  The AdminClientInstaller is delivered on the installation media with the installer.

- 12.0 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, update the JRE installed by the Unified CCE Installer with a later version of the JRE. See Update the Java Runtime Environment (Optional).

  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.

  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.

- 12.0 AdminClientInstaller—Installs the Administration Client on a system that is not running other 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 also requires Microsoft® ODBC Driver 11 for SQL Server® and Visual C++ Redistributable for Visual Studio 2015. 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.

Multistage Upgrades and Maintenance Windows

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 have not yet been upgraded to ensure the overall operation of the contact center. Therefore, it is 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 cannot break any one stage into multiple maintenance windows.

Note

- For co-resident configurations, upgrade Finesse and ECE along with the CUIC/LiveData /IdS server upgrade.

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

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

Stage	Component Group	Components	Notes
1	Queuing and self-service[1]	Cisco Unified Customer Voice Portal (CVP) (Operations Console, Reporting Server, Call Server/VXMLServer, Unified Call Studio)	• Before you upgrade to Unified CVP 12.0, the ES84 or later patch has to be applied to Cisco VVB 11.6 in order to maintain compatibility between Unified CVP 12.0 and Cisco VVB 11.6. • Before you upgrade to Unified CVP 12.5, you must apply the latest ES of CCE 12.0. 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
2	Gateways	- IOS Gateways (If used for ingress access only. If used for Outbound Option Dialer, see Stage 7 .) - IOS VXML Gateways - Cisco Virtualized Voice Browser	
3	Identity Service (IdS)/Single Sign-On(SSO)	IdS Server	- SSO is an optional feature and exchanges authentication and authorization details between the IdS component and IdP provider. For more information, see Unified CCE Contact Center Upgrade Flowcharts, on page 7. - 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
4	Agent and supervisor desktops	Cisco Finesse ECE	- Before you upgrade to Finesse 12.0, apply the latest ES patch on Cisco Unified Intelligence Center 11.6 for the reporting gadgets to continue to work on the new Finesse desktop. - To load any gadget to Finesse, you must first import the certificate to Finesse. **Note** For FinesseVM, 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.

Stage	Component Group	Components	Notes
5	Reporting server	CUIC server	• Cisco Unified Intelligence Center supports TLS 1.2 only. For Cisco Unified Intelligence Center 12.0 to be compatible with releases earlier than Unified CCE Release 11.6(1), run the CLI command **set client tls min-version**. This command allows you to set the minimum TLS version in the client for outbound SSL connections to TLS 1.0 or 1.1. Restart the system for the changes to take effect. • For information about the CLI command to display the current TLS minimum version for client, see Transport Layer Security CLI Commands.
6	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 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**.
7	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.
8	Peripherals	• MR PG (if not collocated with Agent PG on VM), plus VRU 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.

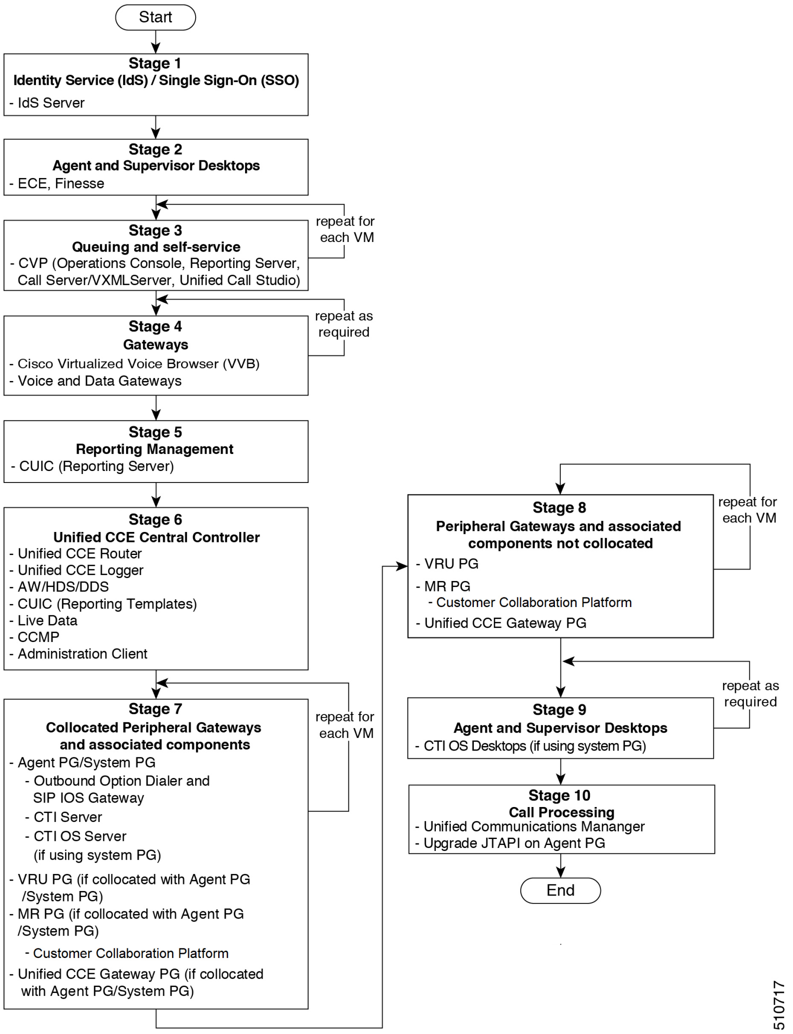
Stage	Component Group	Components	Notes
9	Agent desktop client software	CTI OS (Agent/Supervisor Desktops)	You can have many desktops located in many different sites. You can upgrade CTI OS desktops in multiple maintenance windows; the later upgrade stages are not dependent on the completion of this stage.
10	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. CUCM 12.5 on-box deployment are only supported for M5 and HX M5 servers. 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.

Unified CCE Contact Center 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.

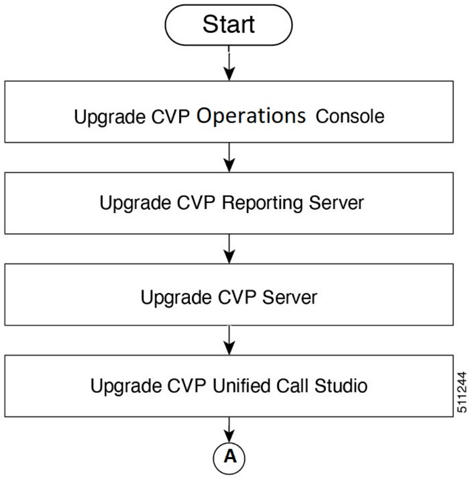
Note After upgrading Finesse, IdS, and CUIC, import IdS certificates on Finesse and CUIC servers.

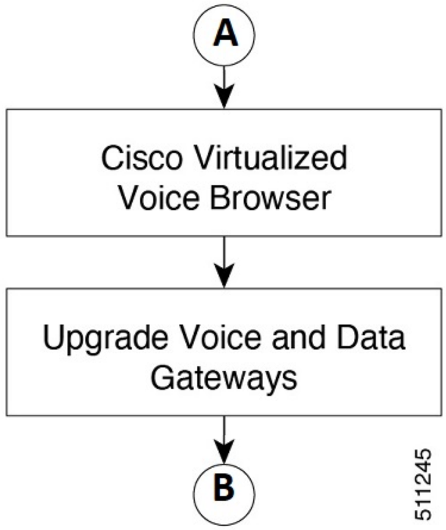

Start
Stage 1
Identity Service (IdS) / Single Sign-On (SSO)
- IdS Server
Stage 2
Agent and Supervisor Desktops
- ECE, Finesse
repeat for each VM
Stage 3
Queuing and self-service
- CVP (Operations Console, Reporting Server, Call Server/VXMLServer, Unified Call Studio)
repeat as required
Stage 4
Gateways
- Cisco Virtualized Voice Browser (VVB)
- Voice and Data Gateways
Stage 5
Reporting Management
- CUIC (Reporting Server)
Stage 6
Unified CCE Central Controller
- Unified CCE Router
- Unified CCE Logger
- AW/HDS/DDS
- CUIC (Reporting Templates)
- Live Data
- CCMP
- Administration Client
repeat for each VM
Stage 7
Collocated Peripheral Gateways and associated components
- Agent PG/System PG
- Outbound Option Dialer and SIP IOS Gateway
- CTI Server
- CTI OS Server (if using system PG)
- VRU PG (if collocated with Agent PG /System PG)
- MR PG (if collocated with Agent PG /System PG)
- Customer Collaboration Platform
- Unified CCE Gateway PG (if collocated with Agent PG/System PG)
repeat for each VM
Stage 8
Peripheral Gateways and associated components not collocated
- VRU PG
- MR PG
- Customer Collaboration Platform
- Unified CCE Gateway PG
repeat as required
Stage 9
Agent and Supervisor Desktops
- CTI OS Desktops (if using system PG)
Stage 10
Call Processing
- Unified Communications Mananger
- Upgrade JTAPI on Agent PG
End
510717

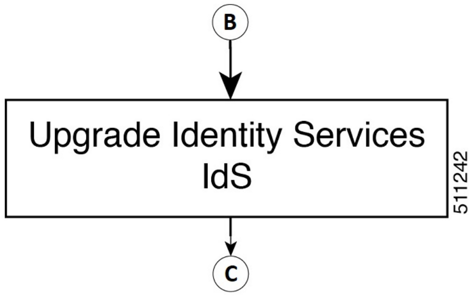
Note

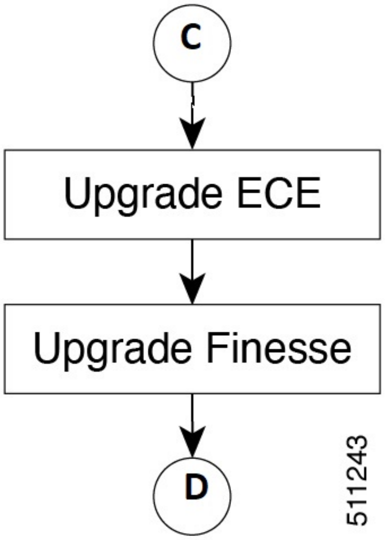
- When you upgrade Unified CVP to Release 12.0, the following considerations apply:
  - If you are upgrading Cisco VVB to Release 12.0, upgrade Unified CVP and Cisco VVB to Release 12.0 in the same maintenance window.
  - If you are upgrading to Unified CVP, Release 12.0 with VVB, Release 11.6(1), you must install VVB, Release 11.6(1) ES84 before you upgrade Unified CVP to Release 12.0.
  - Cisco VVB, Release 11.5(1) is incompatible with Unified CVP, Release 12.0.

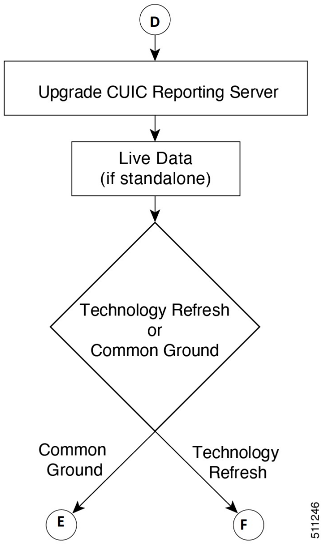
The following diagrams illustrate the stages of the component-level upgrade flows for a Cisco Unified Contact Center Enterprise solution upgrade. Each diagram covers one of the stages. The letter at the end of each flow indicates the start of the next flow that you are required to perform.

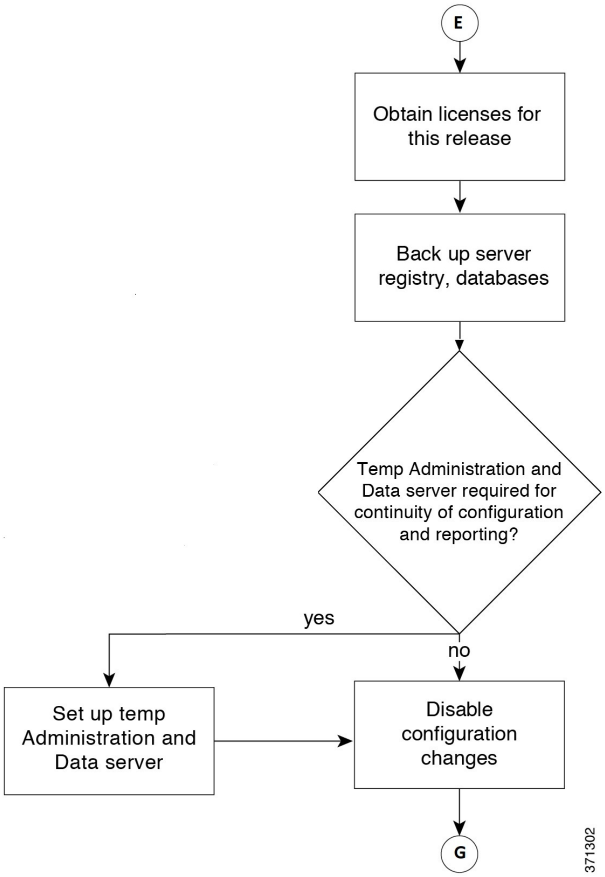

Start
Upgrade CVP Operations Console
Upgrade CVP Reporting Server
Upgrade CVP Server
Upgrade CVP Unified Call Studio
A
511244

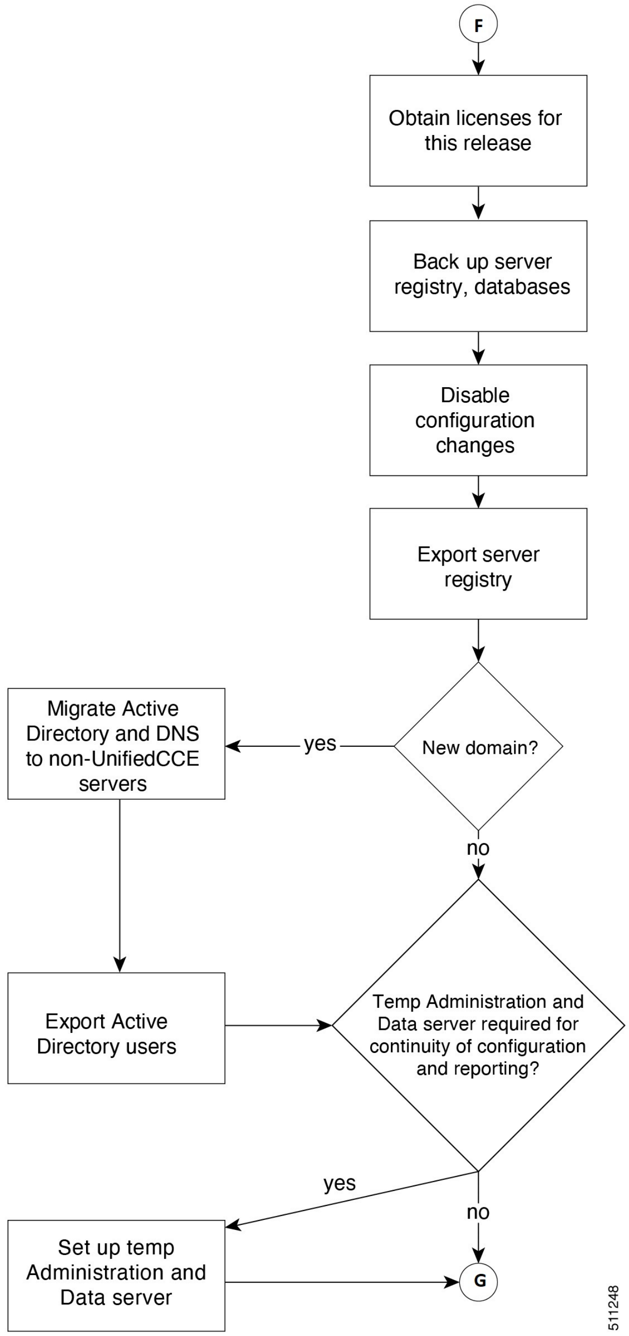

A
Cisco Virtualized Voice Browser
Upgrade Voice and Data Gateways
B
511245

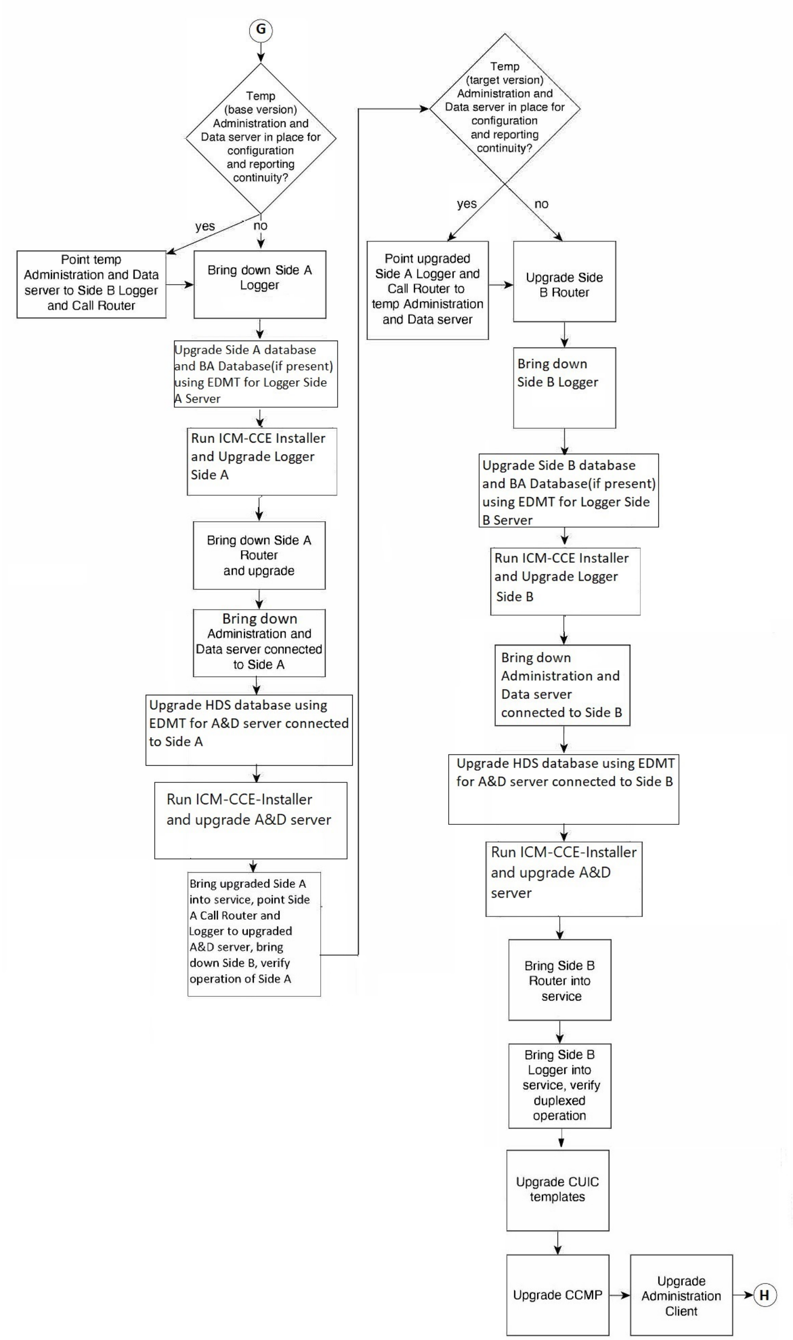

B
Upgrade Identity Services IdS
C
511242

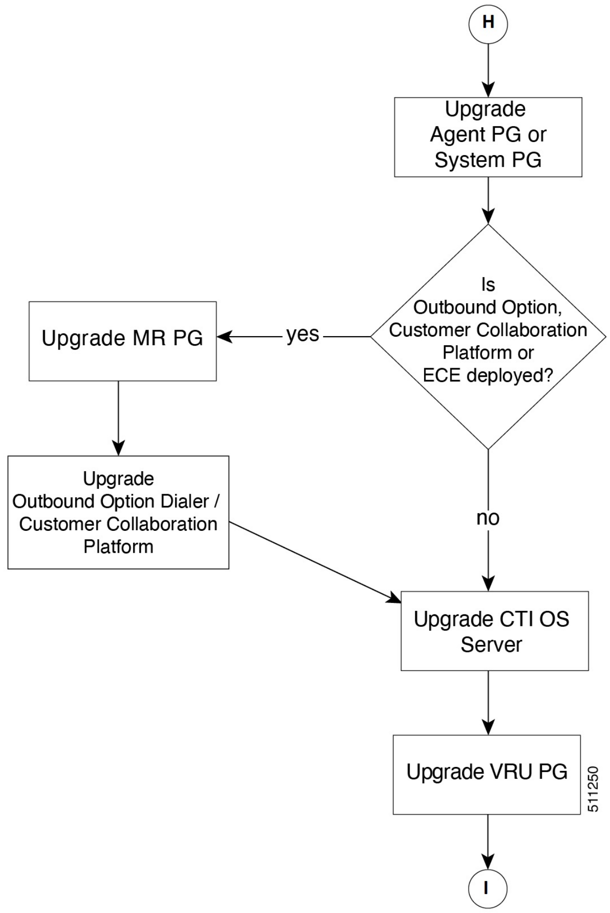

C
Upgrade ECE
Upgrade Finesse
D
511243

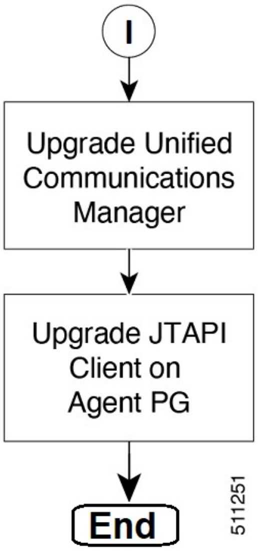

D
Upgrade CUIC Reporting Server
Live Data
(if standalone)
Technology Refresh
or
Common Ground
Common
Ground
Technology
Refresh
E
F
511246

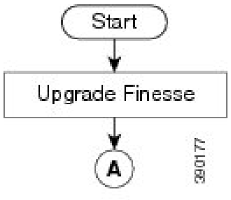

E
Obtain licenses for this release
Back up server registry, databases
Temp Administration and Data server required for continuity of configuration and reporting?
yes
no
Set up temp Administration and Data server
Disable configuration changes
G
371302

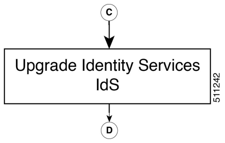

F
Obtain licenses for this release
Back up server registry, databases
Disable configuration changes
Export server registry
New domain?
yes
Migrate Active Directory and DNS to non-UnifiedCCE servers
no
Export Active Directory users
Temp Administration and Data server required for continuity of configuration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

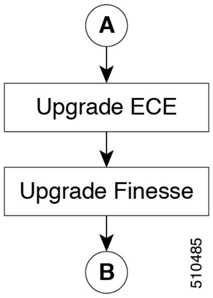

G
Temp (base version) Administration and Data server in place for configuration and reporting continuity?
yes
no
Point temp Administration and Data server to Side B Logger and Call Router
Bring down Side A Logger
Upgrade Side A database and BA Database(if present) using EDMT for Logger Side A Server
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
H

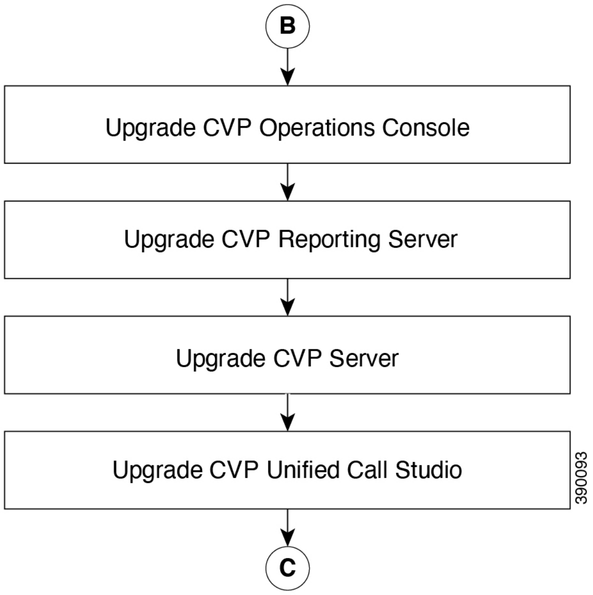

H
Upgrade Agent PG or System PG
Is Outbound Option, Customer Collaboration Platform or ECE deployed?
yes
Upgrade MR PG
Upgrade Outbound Option Dialer / Customer Collaboration Platform
no
Upgrade CTI OS Server
Upgrade VRU PG
511250
I

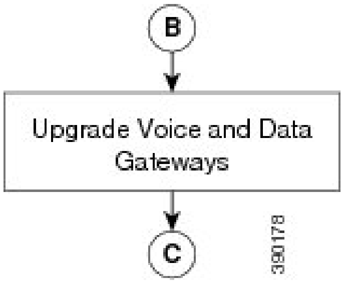

I
Upgrade Unified Communications Manager
Upgrade JTAPI Client on Agent PG
End
511251

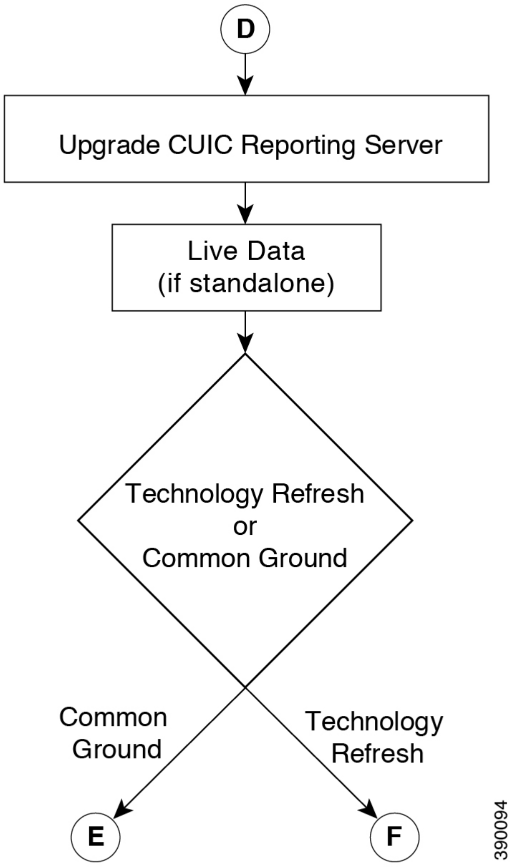

Start
Upgrade Finesse
A
390177

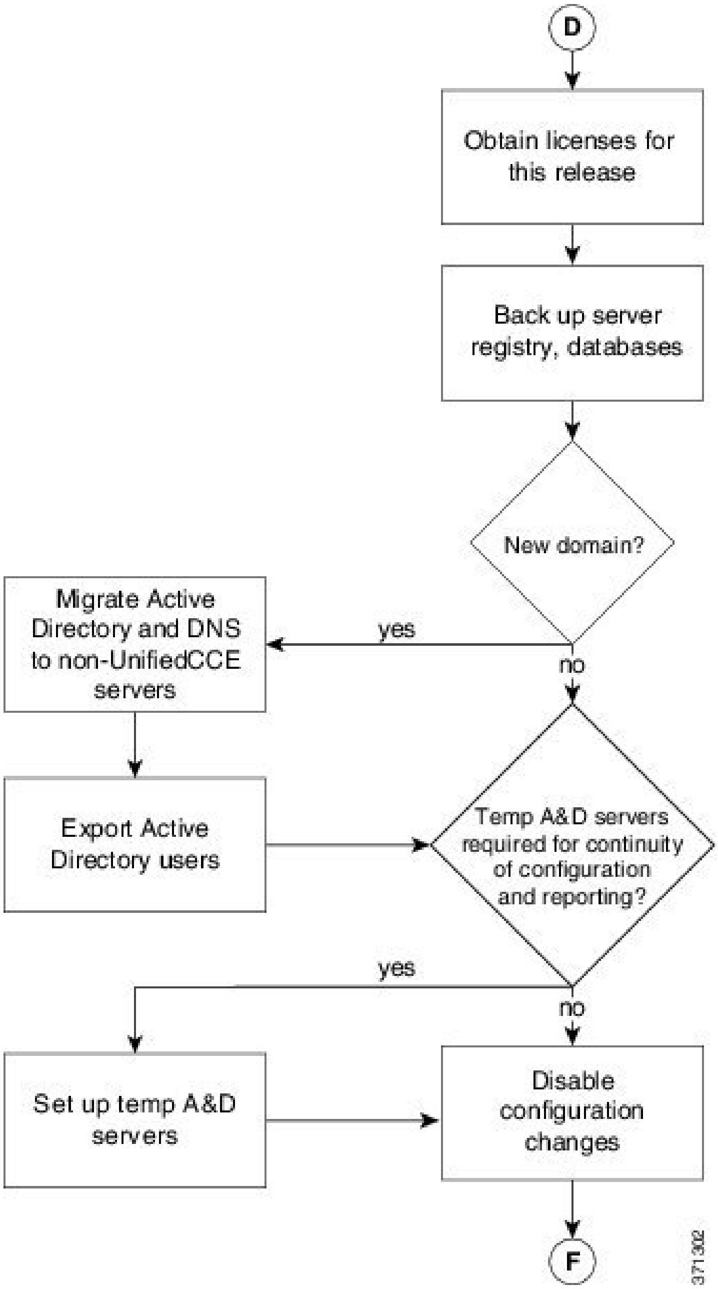

C
Upgrade Identity Services IdS
D
511242

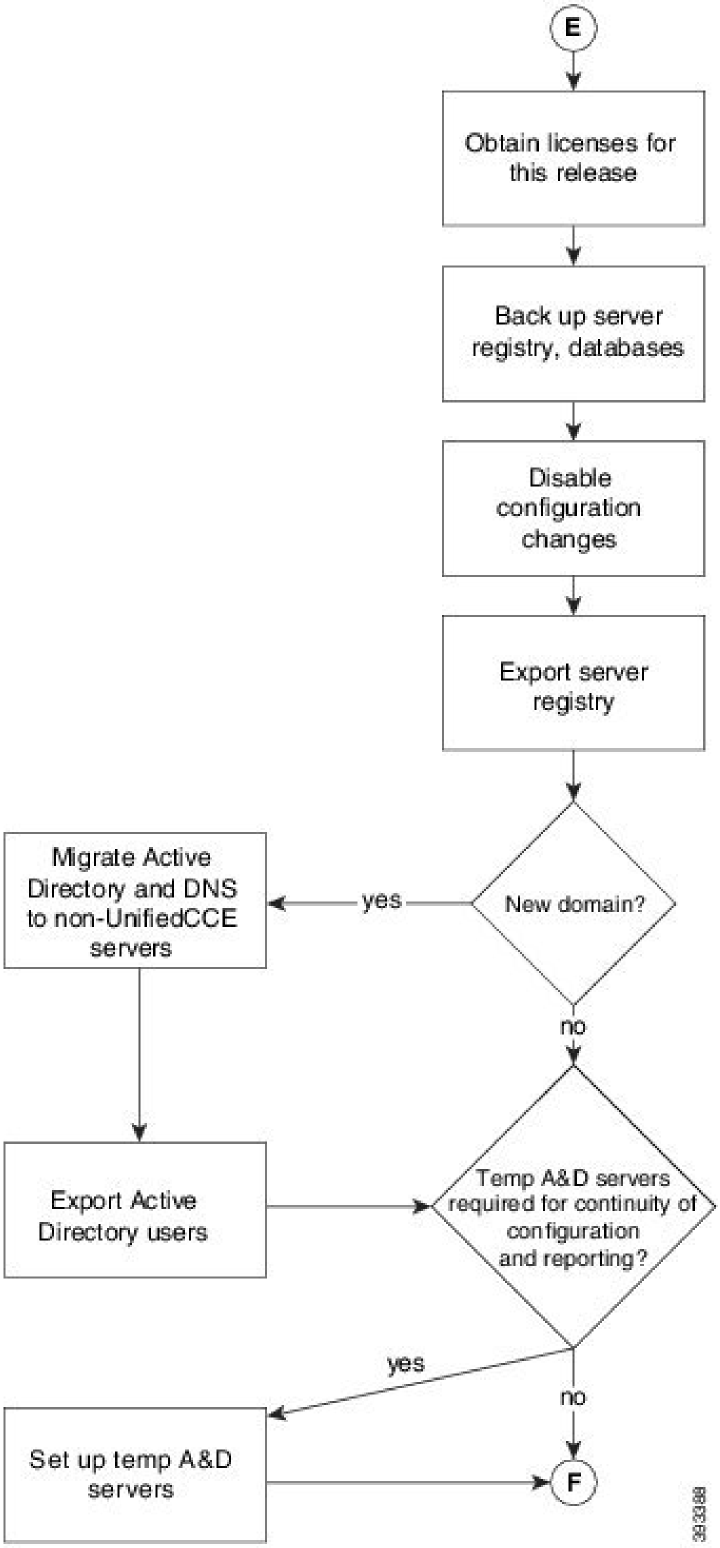

A
Upgrade ECE
Upgrade Finesse
B
510485

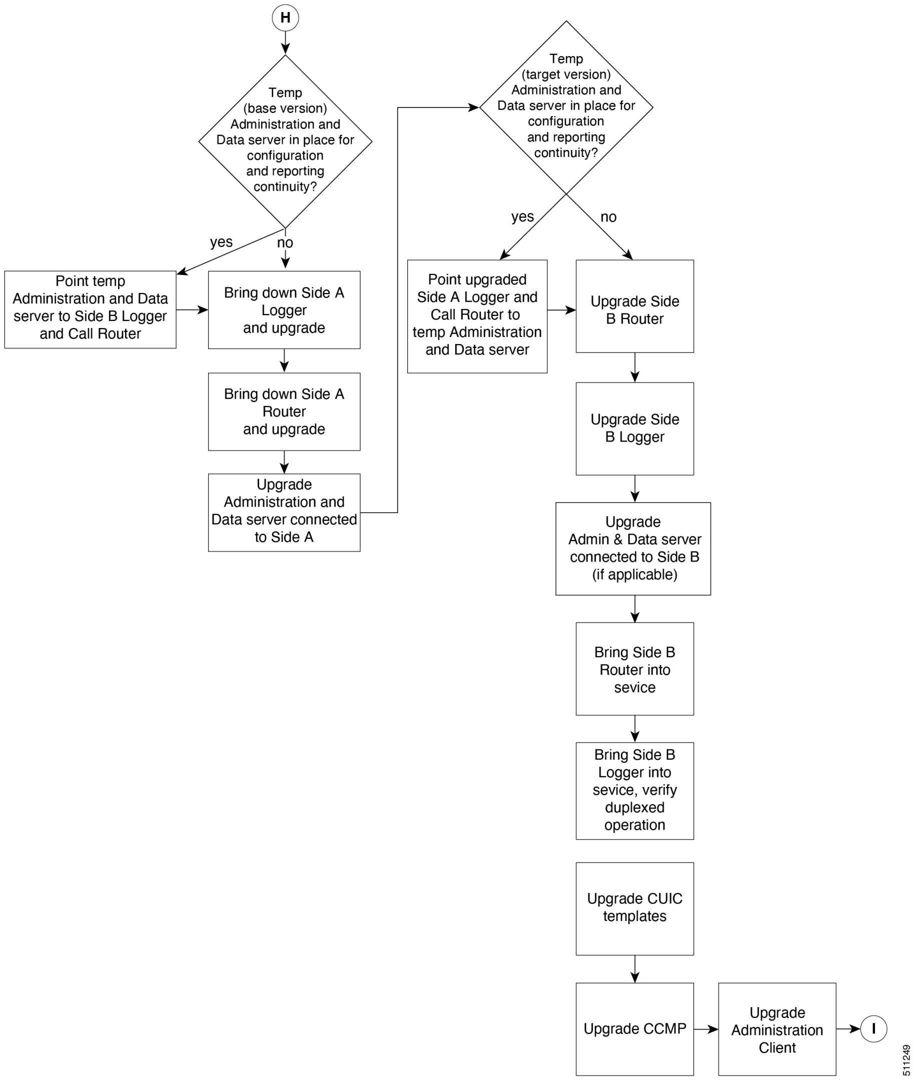

B
Upgrade CVP Operations Console
Upgrade CVP Reporting Server
Upgrade CVP Server
Upgrade CVP Unified Call Studio
C
390093

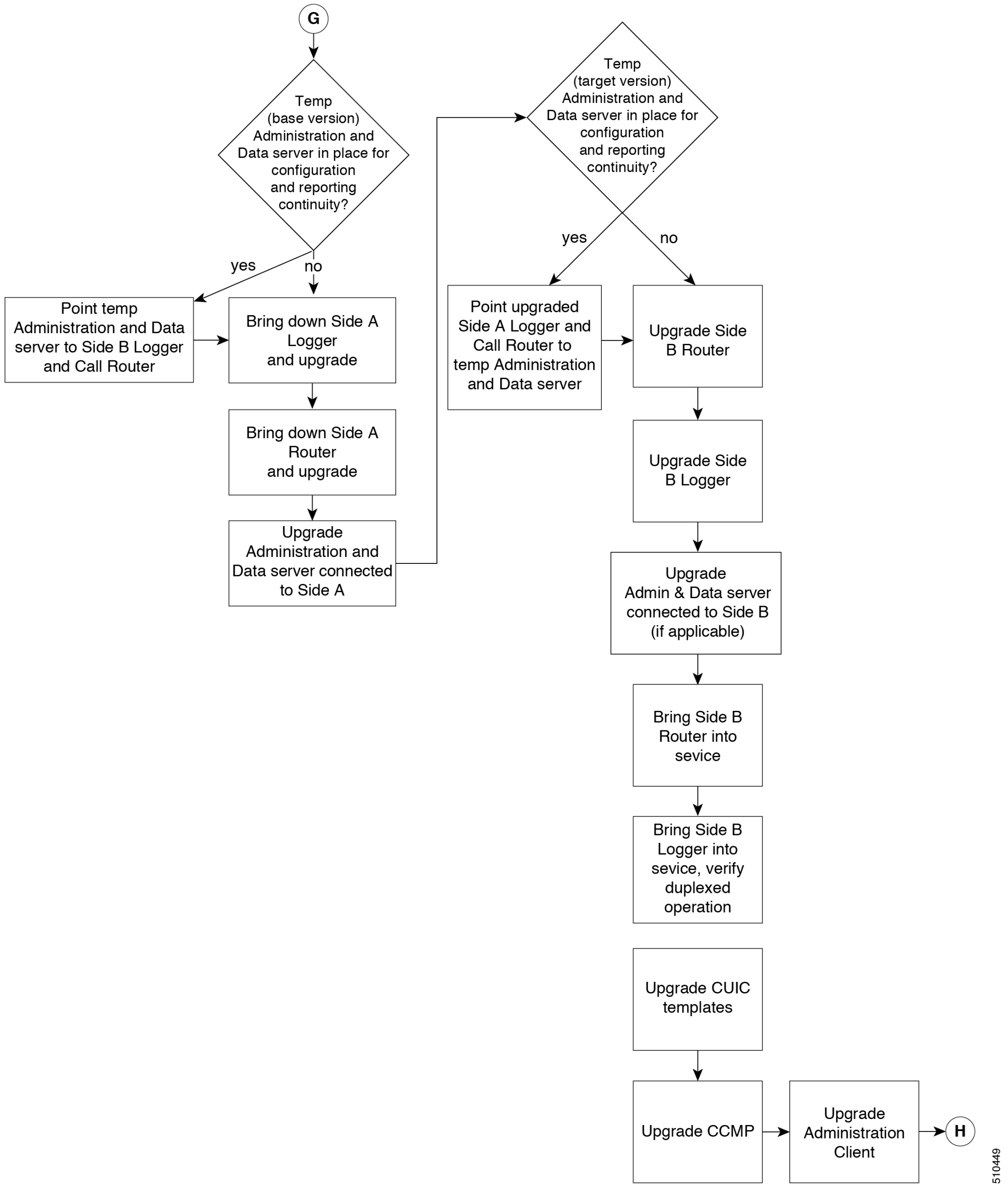

B
Upgrade Voice and Data Gateways
C
390178

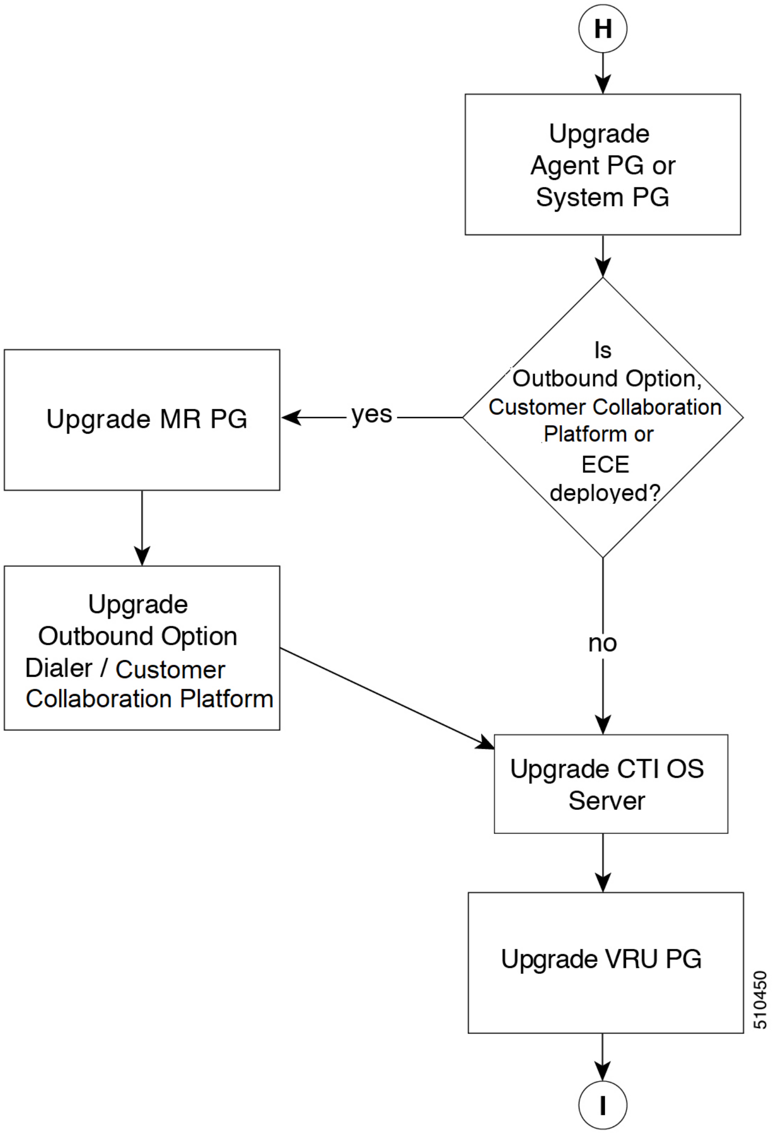

D
Upgrade CUIC Reporting Server
Live Data
(if standalone)
Technology Refresh
or
Common Ground
Common Ground
Technology Refresh
E
F
390094

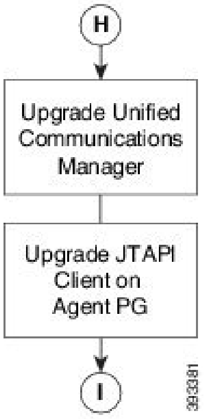

D
Obtain licenses for this release
Back up server registry, databases
New domain?
yes
no
Migrate Active Directory and DNS to non-UnifiedCCE servers
Export Active Directory users
Temp A&D servers required for continuity of configuration and reporting?
yes
no
Set up temp A&D servers
Disable configuration 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 A&D servers required for continuity of configuration and reporting?
yes
no
Set up temp A&D servers
F
393388


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 and upgrade
Bring down Side A Router and upgrade
Upgrade Administration and Data server connected to 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
Upgrade Side B Logger
Upgrade Admin & Data server connected to Side B (if applicable)
Bring Side B Router into sevice
Bring Side B Logger into sevice, verify duplexed operation
Upgrade CUIC templates
Upgrade CCMP
Upgrade Administration Client
I
511249


G
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 and upgrade
Bring down Side A Router and upgrade
Upgrade Administration and Data server connected to 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
Upgrade Side B Logger
Upgrade Admin & Data server connected to Side B (if applicable)
Bring Side B Router into sevice
Bring Side B Logger into sevice, verify duplexed operation
Upgrade CUIC templates
Upgrade CCMP
Upgrade Administration Client
H
510449


H
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
510450
I


H
Upgrade Unified Communications Manager
Upgrade JTAPI Client on Agent PG
I
393381

Data Migration Considerations

The data migration set is identical no matter what migration path you follow.

During the Technology Refresh upgrade, EDMT does the following:

- Backups and restores the data.
- Performs data migration.

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.

For Technology Refresh upgrades, use the fastest possible network (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.

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 24.

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 at .

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 12.0(1) are as follows:

- Unified CCE 11.0(x) to Unified CCE 12.0(1)
- Unified CCE 11.5(x) to Unified CCE 12.0(1)
- Unified CCE 11.6(x) to Unified CCE 12.0(1)

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.