Installation and Upgrade Guide for Cisco Unified Customer Voice Portal, Release 12.6(2)

First Published: 2023-04-28

Last Modified: 2023-04-28

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

Change History

This table lists changes made to this guide. Most recent changes appear at the top.

Change	See	Date
Added system requirements for Windows Defender.	Preinstallation Tasks	June 2023
Added prerequisite to apply ES-02 if VVB is on 12.5(1)_SU before upgrading to 12.6(2).	Preinstallation	May 2023
Initial Release of Document for Release 12.6(2)		April 2023
Added task list for upgrading to Cisco Unified CVP Release 12.6(2).	**Unified CVP Minor Release Upgrade**	
Added **Specific License Reservation** section.	**Unified CVP Licensing**	
Added steps to export system configuration.	**Unified CVP Minor Release Upgrade**	

About this Guide

This document explains how to install and upgrade Cisco Unified Customer Voice Portal (CVP). It is prepared for partners and service providers who will be implementing Unified CVP, who are familiar with Cisco contact center applications, and are experienced regarding the deployment and management of virtual machines.

Audience

This guide is intended for network administrators to install or upgrade the Unified CVP software.

Related Documents

Documentation Guide for Cisco Unified Customer Voice Portal at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-documentation-roadmaps-list.html.

Communications, Services, and Additional Information

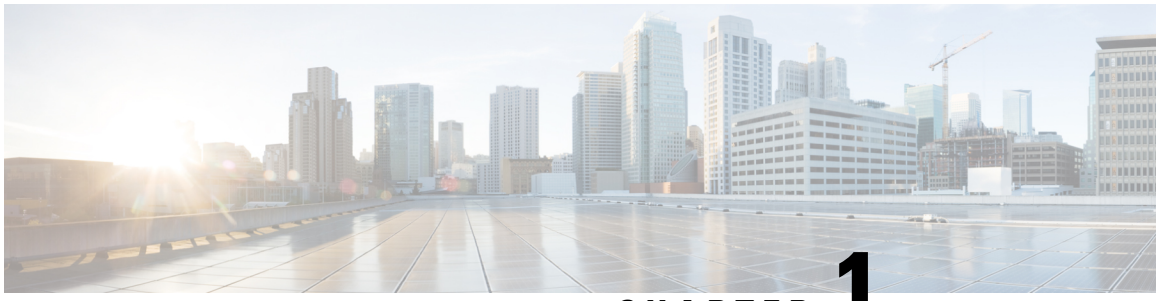
- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Documentation Feedback

Provide your comments about this document to: mailto:contactcenterproducts_docfeedback@cisco.com.



CHAPTER 1

Pre-Installation

The Cisco Unified Customer Voice Portal (CVP), Release 12.6(2) is a patch/minor release (MR). Before installing the 12.6(2) MR, the base Unified CVP 12.5(1) version or base Cisco Unified CVP 12.5(1) with 12.6(1) MR has to be installed.

For more information on installing the base Unified CVP 12.5(1) version, refer to the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal, Release 12.5(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html

For more information on installing the base Unified CVP 12.6(1) MR, refer to the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal, Release 12.6(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html

Download the MR patch from this location: https://software.cisco.com/download/home/270563413/type/280840592/release/12.6(2).

Note If Cisco Virtualized Voice Browser (VVB) is on 12.5(1)_SU, then ES-02 of 12.5(1)_SU is mandatory before installing or upgrading to CVP 12.6(2).

- Pre-Installation Tasks, on page 1

Pre-Installation Tasks

- Close all programs.
- Stop any third-party services and applications that are running on the server.
- Back up `C:\Cisco\CVP` for all Unified CVP components except Operations Console.

Note Unified CVP Server log files are saved in `<CVP_HOME>\logs`; VXML Server log files are saved in `<CVP_HOME>\VXMLServer\logs` and `<CVP_HOME>\VXMLServer\applications\<app_name>\logs`.

- Ensure that the servers are listed as supported hardware and sized appropriately. For information on platform hardware specifications and compatible third party software version requirements, see

https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-technical-reference-list.html.

- Back up the existing Unified CVP installation files onto a different computer for redundancy in case the automatic backup fails.
- Back up the property files of Unified CVP Server, OAMP, and Reporting Server that need modification. Restore them after upgrade is complete.
- This MR encrypts the keystore password, which is required for exchanging certificates. For detailed steps, refer to the *Unified CVP Security* section in the *Configuration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html.

Note Exclude the following folders from on-access scanning configuration of the AV program from all Anti Virus scans:

`c:\Cisco`, `c:\Temp`, `c:\tmp`, `c:\db`, `c:\IFMXDATA`

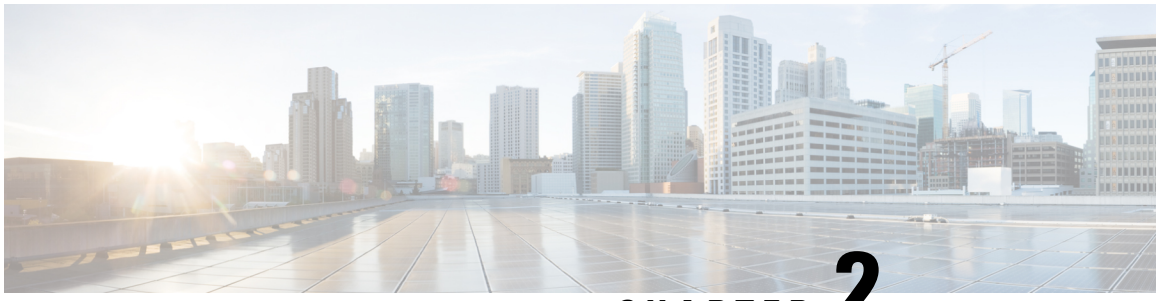
Caution The 12.6(2) release replaces the JRE and Tomcat versions. If you have updated any files in Tomcat (from the `%CVP_HOME%\VXMLServer\Tomcat\webapps\CVP` folder) or JRE configurations (from the `%CVP_HOME%\JRE` folder), ensure that you take a backup of the files before you proceed with the installation. You can restore the backup after the installation is complete.

System Requirements

By default, Windows Defender is enabled on Windows Server. For more information on Windows Defender antivirus compatibility, see https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/windows-defender-antivirus-compatibility.

Unified CVP installation can also take longer than expected due to scanning of files by Windows Defender. Based on your IT policy, do one of the following:

- Disable Windows Defender. For more information, see *Disable Microsoft Defender Antivirus* procedure in Microsoft documentation.
- Add the following path `c:\Cisco`, `c:\Temp`, `c:\tmp`, `c:\db`, `c:\IFMXDATA` to the exclusion list of Windows Defender. For more information, see https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/configure-extension-file-exclusions-windows-defender-antivirus.



CHAPTER 2

Unified CVP Minor Release Upgrade

Unified CVP 12.6(2) MR is an executable file which can be downloaded from CCO. The same executable file can be used to upgrade all Unified CVP components.

Important Before you install Unified CVP MR:

- Refer to the licensing information in the Unified CVP Licensing, on page 19 chapter.
- Ensure that the server chosen for Reporting Server is part of a workgroup.
- Backup all custom audio files present in `<CVP_HOME>/VXMLServer/tomcat/webapps/audio` for Unified CVP upgrade.
- Take a backup of the OAMP config using **Export System Configuration** from the system menu before OAMP upgrade.

To export system configuration from 12.6(1):

1. Export the system configuration files.
2. Unzip the files using the Winrar.
3. Select the contents of the unzipped folder to compress it again.
4. Import the system configuration zip file.

Note After the successful upgrade, the Certificate Authorities (CAs) that are unapproved by Cisco are removed from the platform trust store. However, you can add them back, if necessary.

- For information about the list of CAs that Cisco supports, see the Cisco Trusted External Root Bundle here.
- For information about adding a certificate, see here.

- Upgrade Path, on page 4
- Install Docker to Run Custom Code on Remote Server, on page 4
- Unified CVP Upgrade Strategies, on page 12

Upgrade Path

The following table lists the upgrade paths to replace the existing Unified CVP version with the MR on Windows Server 2016 or Windows Server 2019.

Table 1: Unified CVP Upgrade Path on Windows Server 2016 or Windows Server 2019

Upgrade Path from Older Release to New Release	Platform Change	Conversion Process	Description
Unified CVP 12.5(1) to 12.6(2)	No	Direct upgrade to Unified CVP 12.6(2) through MR.	Platform change is not required because Unified CVP 12.6(2) is supported on Windows Server 2016 and Windows Server 2019.
Unified CVP 12.6(1) to 12.6(2)	No	Direct upgrade to Unified CVP 12.6(2) through MR.	Platform change is not required.

Install Docker to Run Custom Code on Remote Server

Docker streamlines the deployment and administration of custom code on remote servers, enabling you to generate portable and uniform container images that package your applications and their dependencies. Docker provides advantages like scalability, portability, and consistency when executing custom code on remote servers.

Install Docker on Windows Host

Follow this sequence of tasks to install the docker engine on the remote server of the windows host:

Note Setting up this Windows host is a one-time activity and does not need to be repeated for subsequent Docker releases.

Sequence	Task
1	Install Windows Container on Remote Server. See, Install Windows Containers on Remote Server, on page 5

Sequence	Task
2	Install Docker Engine on Remote Server (Windows). See, Install Docker Engine on Remote Server (Windows), on page 5
3	Install Docker Compose Plugin on Remote Server (Windows). See, Install Docker Compose Plugin on Remote Server (Windows), on page 6
4	Install Docker Image on Remote Server (Windows). See, Install Docker Image on Remote Server (Windows), on page 8

Install Windows Containers on Remote Server

Before you begin

- The recommended server version of the host is Windows Server 2022.
- The recommended docker engine version of the host is 25.0.1 (and later) and the docker compose plugin version is 2.26.1 (and later). For more information, refer to the Docker documentation at https://docs.docker.com/engine/release-notes/25.0/.

Procedure

Step 1 In the remote server machine, go to Server Manager and open **Manage** > **Add Roles and Features**.

Step 2 On the **Before You Begin** screen, click **Next**.

Step 3 On the **Select Installation Type** screen, click **Next**.

Step 4 On the **Select Destination Server** screen, click **Next**.

Step 5 On the **Select Server Roles** screen, click **Next**.

Step 6 On the **Select Features** screen, choose the Containers to install on your computer, and click **Next**.

Step 7 On the **Confirm Installation Selections** screen, click **Install**.

Step 8 Click **Close**.

Step 9 Restart the server.

What to do next

Ensure that the container is installed by running the following command in PowerShell as an administrator:

```
Get-WindowsFeature -Name Containers
```

The Install State displays the status as **Installed**.

Install Docker Engine on Remote Server (Windows)

Complete the following procedure to manually install docker engine on the remote server for the windows host.

Before you begin

Refer to the docker documentation at https://docs.docker.com/engine/install/binaries/#install-server-and-client-binaries-on-windows for installing docker on the windows host.

Procedure

Step 1 Download the latest version of the docker binary package file (.zip) from the location: https://download.docker.com/win/static/stable/x86_64.

The recommended version for the docker zip file is 25.0.1 (and later).

Step 2 Run the following commands in the PowerShell application to install and extract the archive to your program files on the windows host:

Note All PowerShell commands in this procedure must be run in Administrator mode.

a. `PS C:\> Expand-Archive  -Path "<Path_to_zip_file>" -DestinationPath $Env:ProgramFiles`

For example:

```
PS C:\> Expand-Archive -Path "C:\docker\docker-25.0.1.zip" -DestinationPath
$Env:ProgramFiles
```

b. `PS C:\> &$Env:ProgramFiles\Docker\dockerd --register-service`

Step 3 Run the following command in the PowerShell application to start the docker service on the windows host:

```
PS C:\> Start-Service docker
```

Verify whether the **Docker Engine Service** is started in Window Services.

Step 4 Verify that Docker Engine is installed and configured on the remote server for the windows host.

Run the following command in PowerShell application to verify the docker engine is installed on the remote server of the windows host:

```
&$Env:ProgramFiles\Docker\docker --version
```

For example, the above command shows the version as `Docker version v25.0.1`.

Install Docker Compose Plugin on Remote Server (Windows)

Complete the following procedure to manually install docker compose plugin on the remote server for the windows host.

Before you begin

Refer to the docker documentation at https://docs.docker.com/compose/install/standalone/ for installing docker compose plugin on the windows host.

Procedure

Step 1 Run the following commands in the PowerShell application on the windows host as Github now uses TLS 1.2:

Note All PowerShell commands in this procedure must be run in Administrator mode.

```
PS C:\> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

Step 2 Run the following commands in the PowerShell application on the windows host to download the latest release of Compose:

The recommended release version for the docker compose plugin zip file is 2.26.1 (and later).

```
PS C:\> Start-BitsTransfer -Source "<Path_To_File_in_Github>" -Destination
$Env:<Destination_Path>
```

For example:

```
PS C:\> Start-BitsTransfer -Source
"https://github.com/docker/compose/releases/download/v2.26.1/docker-compose-windows-x86_64.exe"
 -Destination $Env:ProgramFiles\Docker\docker-compose.exe
```

Step 3 In case of no internet connectivity in the remote server machine, follow the below steps to install docker-compose plugin on the windows host:

a. Download the binary `docker-compose-windows-x86_64.exe` file from the following location: https://github.com/docker/compose/releases/download/v2.26.1/docker-compose-windows-x86_64.exe and copy the file to the `C:\ProgramFiles\Docker` folder.

b. Rename the file `docker-compose-windows-x86_64.exe` to `docker-compose.exe`

c. Run the following command in PowerShell application to install the binary file:
`&$Env:ProgramFiles\Docker\docker-compose.exe`.

Step 4 Verify that Docker Compose plugin is installed and configured on the remote server of the windows host.

Run the following command in PowerShell application to verify the docker engine is installed on the remote server of the windows host:

```
&$Env:ProgramFiles\Docker\docker-compose --version
```

What to do next

After installing Docker Engine, set the system variable `DOCKER_HOME` to the path where Docker is installed.

For example:

- **Variable Name**: `DOCKER_HOME`
- **Variable value**: `C:\Program Files\docker`

After the `DOCKER_HOME` system variable is set, you can run the Docker commands in PowerShell application.

For example:

```
&$Env:DOCKER_HOME\docker images
```

Note For the changes to take effect after adding a system variable, you need to reopen the PowerShell window as an administrator.

Install Docker Image on Remote Server (Windows)

Complete the following procedure to install the docker image on the windows host:

Before you begin

Ensure that you have downloaded the `customapis-windows-docker-<version>.zip` installer zip file.

Procedure

Step 1 Download or copy the `customapis-windows-docker-<version>.zip` installer zip file on the windows host.

Step 2 Create the following directory structure on the host: `C:\Cisco\customapis`.

Step 3 Extract the archive (.zip) to the following location: `C:\Cisco\customapis`, where you need the Installer to be running from.

Step 4 Open the PowerShell application on the windows host to run the launcher script. Refer to the Run the Launcher Script, on page 11 section for more information on using the launcher script.

Note All PowerShell commands in this procedure must be run in Administrator mode from the following location: `C:\Cisco\customapis`.

Step 5 Use the `launcher.bat` file to initiate creation of external mounted folders by providing the `create` parameter by running the following command:

```
PS .\launcher.bat create
```

After you run the command, `external` mount folder gets created at location: `C:\Cisco\customapis`

Step 6 Use the `launcher.bat` file to load the windows docker image and run the container by providing the `load` parameter by running the following command:

```
PS .\launcher.bat load
```

Step 7 Check the status of the container at: `http://<remote_ip_address>:8080/customapis/actuator/health`.

`UP` status means that the container is running.

Step 8 Use the `launcher.bat` file to view the status of the container by providing the `status` parameter by running the following command:

```
PS .\launcher.bat status
```

What to do next

Refer to the chapter "Remote Custom API Server Configuration" of the Configuration Guide fore Unified Customer Voice Portal to run the custom code using remote server on windows host.

Install Docker on Linux Host

Follow this sequence of tasks to install the docker engine on the remote server of the linux host:

Sequence	Task
1	Install Docker Engine on Remote Server (Linux). See, Install Docker Engine on Remote Server (Linux), on page 9
2	Install Docker Compose Plugin on Remote Server (Linux). See, Install Docker Compose Plugin on Remote Server (Linux), on page 10
3	Install Docker Image on Remote Server (Linux). See, Install Docker Image on Remote Server (Linux), on page 10

Install Docker Engine on Remote Server (Linux)

Complete the following procedure to manually install docker engine on the remote server of the Linux host:

Note To install docker engine on CentOS Linux 7 (core), you can refer to the Docker documentation at https://docs.docker.com/engine/install/centos/.

Before you begin

- Ensure that the latest version of CentOS Linux 7 (core) is installed.
- Ensure that the docker engine version of the host is 24.0.2 (and later) and the docker compose plugin version is 2.21.0 (and later). For more information, refer to the Docker documentation at https://docs.docker.com/engine/release-notes/25.0/.

Procedure

Step 1 Download the docker package (.rpm) file for the required docker version that you want to install from the following location: https://download.docker.com/linux/centos/7/x86_64/stable/Packages/.

Step 2 Run the following command to install the docker engine in the relevant path of your download location:

```
$ sudo yum install <Path_to_Docker_Package_File>.rpm
```

```
$ sudo yum install *.rpm
```

Note In case some dependencies are missing during the installation process, you must identify these dependencies and download the necessary .rpm files. Once the required files are downloaded, you must again run the command `sudo yum install *.rpm`.

Step 3 Verify that Docker engine is installed using the following commands:

```
$ docker --version
```

```
$ docker compose version
```

Step 4 Run the following command to start the docker engine:

```
$ sudo systemctl start docker
```

If you want Docker to start automatically after a platform reboot, you can register it with the following command:

```
$ sudo systemctl enable docker
```

Step 5 Verify that the installation of the Docker engine is successful by running the `hello-world` image using the following command:

```
$ sudo docker run hello-world
```

Install Docker Compose Plugin on Remote Server (Linux)

Complete the following procedure to install docker compose plugin on the remote server for the linux host.

Before you begin

Refer to the docker documentation at https://docs.docker.com/compose/install/standalone/ for installing docker-compose on the Linux host.

Procedure

Step 1 Perform Steps 1 to 2 of the Install Docker Engine on Remote Server (Linux) procedure. Refer to the Install Docker Engine on Remote Server (Linux), on page 9 section for more information.

Step 2 Verify that Docker Compose plugin is installed and configured on the remote server of the linux host using the following command.

```
$ docker compose version
```

Install Docker Image on Remote Server (Linux)

Complete the following procedure to install the docker image on the linux host:

Before you begin

Ensure that you have downloaded the `customapis-docker-linux-<version>.zip` installer zip file.

Procedure

Step 1 Download or copy the `customapis-docker-linux-<version>.zip` installer zip on the linux host.

Step 2 Create directory the following structure on the host: `/usr/local/customapis`

Step 3 Run the following command to extract the archive (.zip) to the location: `/usr/local/customapis`, where you need the Installer to be running from:

```
$ unzip customapis-docker-linux-<version>.zip
```

Step 4 Run the following command to provide permission to the `launcher.sh` file:

```
$ chmod +x launcher.sh
```

Note Ensure that you have permissions to directory location: `/usr/local/customapis`

Step 5 Open the Terminal application on the linux host to run the launcher script. Refer to the Run the Launcher Script, on page 11 section for more information on using the launcher script.

Step 6 Use the `launcher.sh` file to initiate creation of external mounted folders by providing the `create` parameter by running the following command:

```
$ ./launcher.sh create
```

After you run the command, `external` mount folder gets created at location: `/usr/local/customapis`

Step 7 Use the `launcher.sh` file to load the windows docker image and run the container by providing the `load` parameter by running the following command:

```
$ ./launcher.sh load
```

Step 8 Check the status of the container at: `http://<remote_ip_address>:8080/customapis/actuator/health`.

`UP` status means that the container is running.

Step 9 Use the `launcher.sh` file to view the status of the container by providing the `load` parameter by running the following command:

```
$ ./launcher.sh status
```

What to do next

Refer to the chapter "Remote Custom API Server Configuration" of the Configuration Guide fore Unified Customer Voice Portal to run the custom code using remote server on windows host.

Run the Launcher Script

A launcher script file helps you execute commands inside the docker container. The launcher script accepts commands, options, and other arguments to modify its behavior.

On the windows host, after downloading the `customapis-docker-windows-<version>.zip` installer, you will find a `launcher.bat` file. To run the launcher script from the `C:/Cisco/customapis` directory, use the following command:

```
launcher.bat <parameter>
```

On the linux host, after downloading the `customapis-docker-linux-<version>.zip` installer, you will find a `launcher.sh` file. To run the launcher script from the `/usr/local/customapis` directory, use the following command:

```
launcher.sh <parameter>
```

Run the launcher script using the following parameters:

Table 2: Parameters to Run the Launcher Script

Parameter	Action
`create`	Creates a directory structure
`load`	Loads the docker image and run the docker container
`run`	Run the docker container
`stop`	Stops the existing docker container
`status`	Displays the status of running docker container

Unified CVP Upgrade Strategies

You can upgrade Unified CVP in a maintenance window. However, when there are a large number of Unified CVP servers to upgrade, it may not be possible to upgrade all of them in one maintenance window. Using the upgrade strategies, you can help large Unified CVP deployments distribute the upgrade process. In addition, you can divide the server upgrades into multiple steps that can be completed over several maintenance windows.

Unified CVP upgrade strategies are described in the following sections.

Unified CVP Units

A Unified CVP unit is a single virtual machine and may comprise VXML Servers and Call Servers. For Unified CVP deployments that have multiple Unified CVP units, ensure that you upgrade one unit at a time. For example, you can upgrade a Unified CVP unit of related servers in a maintenance window. This deployment may be useful for call centers. There may be a need to migrate to Session Initiation Protocol (SIP) to continue call processing and minimize the risks.

Multiphased Approach

Multiphased approach is a strategy to upgrade a subset of Unified CVP Servers and resume call processing. Using the multiphased upgrade approach, you can divide the upgrades in phases over time. If a Unified CVP deployment has multiple Unified CVP units, you can upgrade each unit using the multiphased approach.

Depending on the deployment, choose one of the following multiphased approaches:

- Upgrade all servers of a certain type in a maintenance window.
- Upgrade a subset of a server type in a maintenance window.
- Upgrade a subset of a server type from a Unified CVP unit in a maintenance window.

Use multiphased approach to upgrade the components in the following sequence:

1. Operations Console
2. Unified CVP Reporting Server
3. Unified CVP Server

Note It is not necessary to upgrade all servers in a category in a single maintenance window; however, you must upgrade all Unified CVP components of one type before moving to the next set of components in the Unified CVP deployment or the Unified CVP unit.

Important Considerations for Upgrade

- Upgrade Unified CVP during off-peak hours or during a maintenance window to avoid service interruptions.
- Do not make any configuration changes during the upgrade, because the changes are lost after the upgrade.
- Ensure that a Unified CVP unit remains offline until you upgrade all the components in that unit.
- Upgrade Unified CVP components in a sequence for a successful deployment. A change in upgrade sequence results in loss of call data and error or inability to configure properties that are introduced in the new version.
- Push the TCL and VXML files (from the location `C:\Cisco\CVP\GWDownloads\`) to their respective ingress and VXML gateways after the Unified CVP Operations Console is upgraded, but before any other Unified CVP components are upgraded.

Upgrade Unified CVP Components

Install the Unified CVP 12.6(2) MR on the following components:

- Unified CVP Server
- Operations Console
- Remote Operations
- Unified CVP Reporting Server

Follow the given steps to install the Unified CVP 12.6(2) MR on each of the above components:

Procedure

Step 1 Run (double click) **CVP12.6.2.exe**. A welcome screen is displayed.

Step 2 Click **Next** to proceed.

Step 3 Review and accept the **Software License Agreement**, and click **Next**.

A warning message is displayed to backup all custom audio files. Click **OK** to proceed.

Step 4 Click **Install** to start the MR installation.

Note As soon as the MR set up begins, the following warning may be displayed if any of the 12.5 ESs are installed:

```
Following engineering special(s) installed in the system, are not merged into
CVP12.6(2)
<list of ES installed>

Continuing with the upgrade may result in loss of functionality provided by above
engineering special(s).
Review available engineering special(s) built on CVP12.6(2), for corresponding patches
 that would need to be applied separately.

Do you want to continue the upgrade?
```

Click **Yes** to proceed.

For information on Engineering Special (ES) when upgrading to Cisco Unified Customer Voice Portal to 12.6(2), see *Important Notes*section in the *Cisco Unified Customer Voice Portal* Chapter of the Release Notes for Cisco Contact Center Enterprise Solutions Release.

Step 5 Click **Finish** to complete the MR installation. Reboot the machine after the installation.

Upgrade Unified Call Studio

Procedure

Step 1 Open Call Studio, right-click any existing project in the Navigator view, choose **Export**.

The **Export** wizard opens.

Step 2 Navigate to **General** > **File System**, and click **Next**.

Note From the list displayed by the Export wizard, select multiple projects to export them simultaneously.

Step 3 Browse to the directory where the projects will be exported and click **OK** and then click **Finish**.

Step 4 Uninstall the Call Studio software.

For more information, see the Unified CVP/Call Studio Uninstallation section.

Step 5 Install the Call Studio software.

For more information, see the Install Unified Call Studio section.

After an upgrade, all custom elements need to be recompiled using OpenJDK 1.8.x before using them in Call Studio.

Note The SolarWinds TFTP software and AnyConnect (while a VPN connection is enabled) are the known causes for the Call Studio debugger errors. To resolve the Call Studio debugger errors:

- If you are using SolarWinds, stop SolarWinds TFTP software and run the debugger.
- If you are using AnyConnect, disconnect the VPN connection and run the debugger.

Postupgrade Tasks

After you upgrade the Unified CVP components, synchronize the metadata files using the Sync-up tool.

Initiate metadata synchronization only if you are using CVP Rest API. For more information, see Initiate Metadata Synchronization for Unified CVP Rest API, on page 16.

Important

- After upgrade, restart the **WebServicesManager** service to use system CLI.
- If you are using a VRU connection port other than the default port (5000), then click **Save and Deploy** of Unified CVP Call Server from OAMP.
- If you have added the certificates in *.ormkeystore*, then add them again in *.keystore*.
- Perform the following steps for Smart Licensing to work after upgrading to Unified CVP 12.6(2):
  1. Redeploy all Call Servers and VXML Servers from OAMP.
  2. Restart the services.
- VMWare Tools do not get updated automatically after upgrading to Unified , CVP 12.6(2) on Windows Server 2016/2019 and rebooting the machine.

  Workaround: Perform the following steps to update the VMWare Tools manually:
  1. Right-click on the VM.
  2. Go to **Guest OS** and select **Upgrade VMWare Tools**.
- After you upgrade to Unified CVP 12.6(2), the `WebServiceCredentials` schema gets updated with the encryption method.

  To encrypt the wsm password in OAMP, do the following:
  1. Stop Cisco CVP **OPSConsoleServer** and Cisco CVP **WebServicesManager** services.
  2. Navigate to `C:\Cisco\CVP\bin\`.
  3. Execute the `mgr-init.bat -wsm <wsmadmin password>` command from the command prompt.
  4. Restart the Cisco Unified CVP Operations Console and Cisco CVP WebServicesManager.

  The encryption key, which is a part of OAMP, is absent from the `WebServicesCredentials.xml` files on the CVP Call Server, VXML Server, and Reporting Servers.

  Workaround: To synchronize the `WebServicesCredentials.xml` with the encryption method, it is necessary to redeploy all the Call Servers, VXML Servers, and Reporting Servers.

Initiate Metadata Synchronization for Unified CVP Rest API

In the Unified CVP REST API architecture, information of media files on Media Server and VXML applications on a VXML server is saved on a WSM Server as metadata in Derby database. This metadata information is created, updated, and deleted by the REST API calls. There may be situations where the metadata may go out of sync with files on VXML Servers and Media Servers. Examples are addition and deletion of Unified CVP Servers, deployment of apps and media files by a tool other than the REST API, and Unified CVP Media Server or the VXML server upgraded from a version where the REST API was not supported.

A command line tool “metasynch.cmd” is available at `C:\Cisco\CVP\wsm\CLI` to enable synchronization of metadata with the files on VXML Servers and Media Servers. The tool internally uses the Synch up API to perform the synchronization. It takes three arguments- WSM user name, WSM user password, and server type (MEDIA, VXML or VXML_ STANDALONE). Based on the server type information, all servers of the

respective server type are synchronized. If the server type argument is not provided, metadata is synchronized with all media servers and VXML servers configured in OAMP.

In case of an upgrade, the media files and VXML applications are present in the Media Servers and VXML Servers but corresponding metadata information is not present in the WSM Server. The absence of metadata information limits a user from using the REST API to access, update, and delete existing media files and VXML applications on the Media Server and the VXML Server.

Note Wsmadmin (CLI) users or any other serviceability/readonly role users cannot login or use OAMP/NOAMP/CLI until an Administrator or Super Administrator role user updates their password post an install/upgrade.

Synchronize Metadata Files Using Sync-Up Tool

To invoke **`metasynch.cmd`**, complete the following steps.

Procedure

Step 1 On the Unified CVP OAMP Server, navigate to the `C:\Cisco\CVP\wsm\CLI` location.

Step 2 Run the **metasynch.cmd** file with following arguments:

- **wsm username**
- **wsm password**

Example:

```
metasynch.cmd wsmusername wsmpassword MEDIA
```

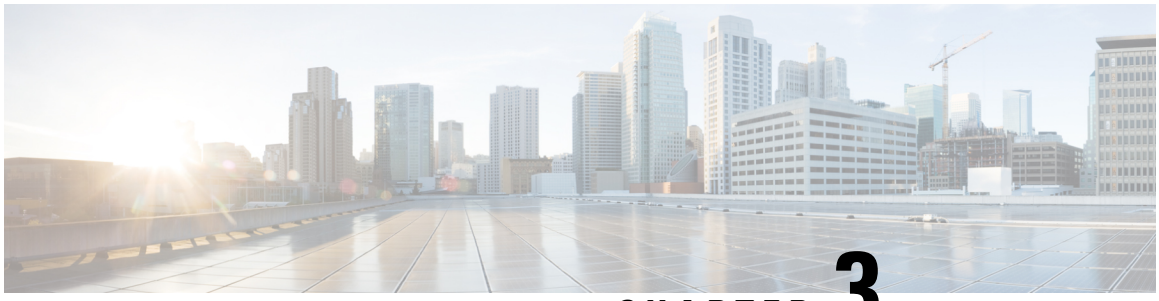
Usage : metasynch [options] username password [servertype]

servertype : MEDIA/VXML/VXML_STANDALONE

options : -help -? print this help message

Note The server type argument should be MEDIA, VXML, or VXML_STANDALONE type. If the server type argument is not provided, the metadata is synched with all the VXML applications on VXML servers and all media files on Media servers. Logs for synch command tool can be found at the following location:

```
C:\Cisco\CVP\wsm\CLI\log\SyncTool.log
```



CHAPTER 3

Unified CVP Licensing

License Plan

Unified CVP now supports Smart Licensing which is a flexible software licensing model that streamlines the way you activate and manage Cisco software licenses across your organization. For detailed feature overview on Smart Licensing, see *Administration Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-maintenance-guides-list.html.

All Unified CVP servers, including Unified CVP server and VoiceXML server, need to register with Cisco SSM. Unified CVP OAMP and CVP Reporting server do not need any licensing registration.

Upgrading from Classic License

After purchasing, the product licenses will be visible in your Smart Account. If you have a classic license, you will need to convert the PAKs to Smart Account. For more information on converting your classic license to Smart Account, see https://software.cisco.com/web/fw/softwareworkspace/smartlicensing/ssmcompiledhelps/c_conversion_settings.html.

Table 3: Unified CVP Components and the Required License

Unified CVP Component	Required License
Unified CVP Call Server/VXML Server	• Self Service Ports • Unified CVP Server license The licenses for the ports on the Unified CVP Call Server and the Unified CVP VXML Server. A Unified CVP VXML Server license is for the number of self-service ports plus queued sessions.
Unified CVP Reporting Server	No License is required for the Unified CVP Reporting Server.

Unified CVP Component	Required License
Unified CVP OAMP Server	No License is required for the Unified CVP OAMP Server.

Note Whenever Unified CVP is installed or upgraded, the Web Service Manager certificate from Unified CVP Call Server/Unified CVP VXML Server needs to be imported into the keystore of the Unified CVP OAMP/PCCE Server.

For information on the detailed steps, see the *Unified CVP Security > Secure Communication between CVP and OAMP Server* section of the *Cisco CVP Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html.

Specific License Reservation

Devices (product instances of Unified CVP) that register with Smart Licensing have to share the license information with Cisco Smart Software Manager (Cisco SSM) at regular intervals. Your deployments that cannot periodically share license utilization data with Cisco SSM or due to regulatory reasons can use the Specific License Reservation feature. Cisco offers license reservation as an on-request configuration for such product instances.

You can reserve licenses (including add-on licenses) for your product instance on Cisco SSM. Specific License Reservation is enabled through the option **License Management** in the Unified CVP NOAMP portal.

Note The reserved licenses require no renewal or reauthorization unless there is a license usage change on the device. License reservation provides limited functionality to certain Smart Licensing features such as transfer of licenses between products, license usage, and asset management.

The Specific License Reservation (SLR) feature does not offer the following benefits that are available as part of the Smart Licensing feature:

- Dynamic movement of license consumption between products
- Real-time license usage visibility and asset management
- Simplified product registration

Before uninstalling Cisco Unified Customer Voice Portal 12.6(2) to base versions 12.6(1) or 12.5(1), always make sure to return the license reservation if registered with SLR.

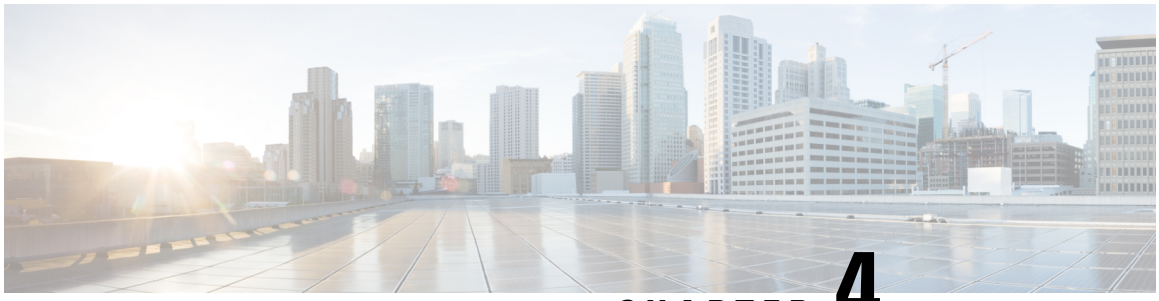
For more information, refer to the *Smart Licensing* section in the *Administration Guide for Cisco Unified Customer Voice Portal 12.6(2)* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html.

Unified CVP Redundant Port

The Redundant Port supports a redundancy model in which one or more failover servers are available to take calls when the primary servers are unavailable.

For example, if a customer has purchased 1500 Self-Service ports, these ports can be used across devices or locations or servers. The customer is entitled to run only 1500 ports simultaneously. The total number of calls that receive queuing or self-service treatment cannot exceed 1500.

Note For all Microapp-based applications (except GS Microapp), when the VXML/IVR ports usage exceeds the system capacity, the call gets disconnected gracefully. The GS Microapp puts the call on hold until license is available.



CHAPTER 4

Unified CVP MR/Call Studio Uninstallation

Uninstall Unified CVP MR/Call Studio From Windows Control Panel

Before you begin

- Shut down all applications and close all open files.
- Close the Unified CVP component and related files.

Procedure

Step 1 Click **Start** > **Control Panel** > **Programs and Features**.

Step 2 Click **Cisco CVP Minor Release CVP12.6(2) / Cisco Unified Call Studio**, and then click **Remove**.

Step 3 Click **Next**.

After uninstallation, the **Uninstall Complete** screen appears. Depending on the components you uninstalled, you may need to reboot your computer.

Note The Unified CVP uninstallation procedure does not clean up all the files and folders, such as log files, media files and folders that are generated postinstallation. Media folders with same names are replaced during the Unified CVP installation process. User-created media files and folders remain unchanged during Unified CVP upgrade. Create all the media folders in `wwwroot` and use the relative paths to simplify the migration process for the future releases of Unified CVP that support A-law, u-law, and G729 files.

Uninstall Unified CVP MR/Call Studio Using Installation Media

Before you begin

- Shut down all applications and close all open files.
- Close Unified CVP component and related files.

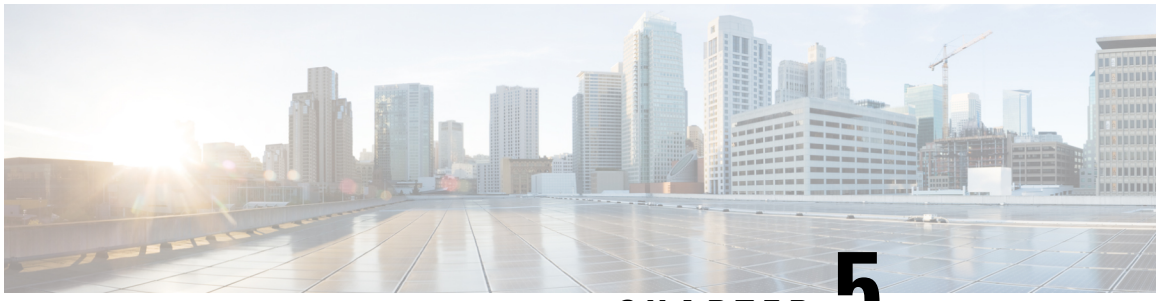
Procedure

Step 1 Run the *CVP12.6.1.exe* file of the Unified CVP software.

Step 2 Select the **Remove** option, and click **Next**.

The **Uninstall Complete** screen appears. Depending on the components you uninstalled, you may need to reboot your computer.

Note The Unified CVP uninstallation procedure does not clean up all the files and folders, such as log files, media files and folders that are generated postinstallation. The media folders with same names get replaced during the Unified CVP installation process. The user created media files and folders remains unchanged during Unified CVP upgrade. It is required to create all the media folders in the `wwwroot` and use the relative paths, as it simplifies the migration process for the future releases of Unified CVP that supports A-law, u-law, and G729 files.



CHAPTER 5

Unified CVP Migration

Migrate Unified CVP to Windows Server 2019

The following table lists the migration paths to replace the existing Unified CVP version with the MR on Windows Server 2019.

Table 4: Unified CVP Migration Path on Windows Server 2019

Migration Path from Older Release to New Release	Platform Change	Conversion Process	Description
Unified CVP 12.5(1) to 12.6(2)	Yes	First install Unified CVP 12.5(1) on Windows Server 2019. Then upgrade to Unified CVP 12.6(2) through MR. **Note** .NET framework must be installed before installing Unified CVP 12.5(1).	Platform change is required.

Note The steps to be followed for installing Windows Server 2019 are the same as the steps for installing Windows Server 2016.

For migration to Windows Server 2019, refer to the *Unified CVP Migration* chapter in the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal, Release 12.5(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html.

Note

- If the installer gives a Windows Server warning regarding the configured guest OS on the virtual machine, ignore it.
- It is recommended to use the OVA file `CVP_12.6_Windows_vmv13_v8.0.ova`. available at https://software.cisco.com/download/home/270563413/type/280840592/release/12.6(1).

  .

For installing Unified CVP 12.5 on Windows Server 2019, refer to the *Unified CVP Installation* section in the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal, Release 12.5(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html.

INDEX

L

U