Upgrade Unified CVP

You can upgrade to a new version of Unified CVP if the platform of the new and existing version is the same. For example, replacing Unified CVP 11.6(1) with Unified CVP 12.0(1) is an upgrade because both the versions work on the same platform.

If the existing software is to be replaced with a newer version with a change in platform, architecture, or applications, the process is called migration. For example, replacing Unified CVP 10.5(1) with Unified CVP 12.0(1) is a migration because the newer version works on a different platform than the older version. To learn whether replacing the existing version with a new version is an upgrade or a migration, see the Upgrade Path section.

Upgrade of Cisco voice solution components is a multistage process; solution components are grouped in several stages for upgrading. Users must follow the solution level upgrade order mentioned in the *Upgrade* section of the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html for smooth transitioning to higher grade versions.

Note Push the TCL and VXML files to their respective ingress and VXML gateways after the CVP Operations Console is upgraded, but before any other CVP components are upgraded.

Upgrade Path

The following table lists the upgrade paths to replace an existing Unified CVP version with a new one.

Table 1: Unified CVP Upgrade Path

Upgrade Path from Older Release to New Release	Platform Change	Conversion Process	Description
Unified CVP 11.5(1)/11.6(1) to 12.0(1)	Yes	1. Perform an in-place upgrade from Windows Server 2012 to Windows Server 2016. 2. Upgrade to Unified CVP 12.0(1).	Change in platform from 12.0(1) release.

Unified CVP Upgrade Strategies

You can upgrade Unified CVP in a maintenance window. However, when there are a large number of 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.

CVP Units

A CVP unit is a single virtual machine and may comprise VXML Servers and Call Servers. You can upgrade one CVP unit at a time for the Unified CVP deployments that have multiple CVP units. For example, you can upgrade a 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 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 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 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 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 to their respective ingress and VXML gateways after the CVP Operations Console is upgraded, but before any other CVP components are upgraded.

Pre-Upgrade Tasks

Related Topics

Configure Virtual CPU Settings , on page 4
Upgrade Virtual Memory, on page 4
Upgrade Virtual Machine Hardware Version, on page 5
Expand Disk Space of Virtual Machines , on page 5

Upgrade Existing Unified CVP Virtual Machine

The following sections discuss the steps to upgrade the virtual machine hardware by using VMware vSphere Web Client (Thin Client).

Note You must not use VMware vSphere Client (Thick Client) to upgrade the virtual machine hardware.

Configure Virtual CPU Settings

Complete the following procedure to change the virtual hardware resource setting for CPU on Unified CVP virtual machines.

Step 1 Power off the virtual machine.

Step 2 Right-click the virtual machine, choose **Edit Settings**.

Step 3 Click the **Virtual Hardware** tab.

Step 4 Click **CPU**.

Step 5 From the **Cores per Socket** drop-down list, select **1**.

Step 6 In the **Reservation** field, enter the CPU reservation speed (defined in MHz) for Unified CVP virtual machines.

For more information about virtual hardware resource setting for CPU and memory, see *Unified CVP Virtualization Wiki* available at http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-customer-voice-portal.html.

Step 7 Click **OK** to save the settings.

What to do next

Upgrade Virtual Memory

Related Topics

Upgrade Virtual Memory, on page 4

Upgrade Virtual Memory

Complete the following procedure to upgrade the system memory on Unified CVP virtual machines.

Step 1 Ensure that the virtual machine is switched off.

Step 2 Right-click the **Virtual Machine** and select **Edit Settings**.

Step 3 Click the **Virtual Hardware** tab.

Step 4 Click **Memory**.

Step 5 In the **RAM** field, change the RAM value (in MB) of Unified CVP virtual machines as defined in the *Virtualization for Cisco Unified Customer Voice Portal* available at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-customer-voice-portal.html.

Step 6 In the **Reservation** field, enter the RAM value (in MB) corresponding to Unified CVP VMs, as defined in the *Virtualization for Cisco Unified Customer Voice Portal*.

Step 7 Click **OK** to save the settings.

What to do next

Upgrade the Virtual Machine Hardware Version.

Related Topics

Upgrade Virtual Machine Hardware Version, on page 5

Upgrade Virtual Machine Hardware Version

Complete the following procedure to upgrade the virtual machine hardware version on Unified CVP virtual machines.

Step 1 Ensure that the virtual machine is switched off.

Step 2 Right-click the virtual machine and select **Edit Settings**.

Step 3 Click the **Virtual Hardware** tab.

Step 4 Click **Upgrade**.

Step 5 Check the **Schedule VM Compatibility Upgrade** check box.

Step 6 From the **Compatible with (*)** drop-down list, choose one of the following options:

- **ESXi 6.0 update 2 and later**
- **ESXi 6.5 with VMFS5**
- **ESXi 6.5 with VMFS 5**
- **ESXi 6.5 U2 and later updates with VMFS 6**
- **ESXi 6.7 with VMFS 6**

Step 7 Click **OK** to save the settings.

Step 8 Power on the virtual machine.

What to do next

Expand the Virtual Machines Disk Space

Related Topics

Expand Disk Space of Virtual Machines , on page 5

Expand Disk Space of Virtual Machines

Complete the following procedure to expand the virtual machines disk space on Unified CVP virtual machines.

Step 1 Ensure that the virtual machine is switched off.

Step 2 Right-click the virtual machine and choose **Edit Settings**.

Step 3 Click the **Virtual Hardware** tab.

Step 4 In the **Hard disk 1** field, change the disk size value (in GB) of the Unified CVP virtual machines, as defined in the *Virtualization for Cisco Unified Customer Voice Portal* available at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-customer-voice-portal.html.

Step 5 Click **OK**.

Step 6 Power on the virtual machine.

Step 7 Log into your operating system.

Step 8 Right-click **My PC** and select **Manage**.

Step 9 Select **File and Storage Services** > **Disks**.

Step 10 In the Volumes area, right-click **C drive** and select **Extend Volume…**.

Step 11 Change the disk size value (in GB) of the Unified CVP virtual machines as defined in the *Unified CVP Virtualization Wiki*.

Step 12 Click **OK**.

Step 13 Restart the server.

Enable Resource Reservation on Upgraded Virtual Machine

After the virtual machine hardware version is upgraded based on the information provided in the *Virtualization for Cisco Unified Customer Voice Portal*, perform the following steps to enable resource reservation on the respective Unified CVP virtual machines.

For more information on supported virtual machine hardware versions, see available at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-customer-voice-portal.html.

Step 1 Login to vSphere Client and select the Unified CVP virtual machine.

Step 2 Right-click the virtual machine and select the option **Edit Settings** from the popup menu.
The **Virtual Machine Properties** window pops up.

Step 3 Select the **Resources** tab.
The Virtual Hardware Resource Setting that can be customized is shown in the left dialog box. The Resource Allocation for respective virtual hardware is shown in the right.

Step 4 Enable resource reservation for Unified CVP virtual machines.

Note To enable the Virtual Hardware Resource reservation for Unified CVP virtual machines, the setting for CPU and memory must be modified. For information about virtual hardware resource setting for CPU and memory, see *Virtualization for Cisco Unified Customer Voice Portal* available at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-customer-voice-portal.html.

Step 5 After the virtual hardware resource setting for CPU and memory for CVP virtual machines are set, click **OK** to close the VM Properties dialog box.
The CVP virtual machine is reconfigured and the **Resource Reservation** is enabled.

Upgrade Windows Server

Microsoft supports an in-place upgrade of operating system.

Complete the following procedure to upgrade your operating system on all virtual machines for server-based applications.

Before you begin

- As a precautionary measure, follow the steps listed under the Pre-Upgrade Tasks section to preserve the existing version of CVP.
- Upgrading to Windows Server may delete static network configuration (for private and public interfaces) for all Windows virtual machines. Record your static network configurations, including TCP/IP IPv4 information before upgrading. Reconfigure these settings after the upgrade completes.
- Ensure that latest version of VMware Tools software is installed.
- Ensure that ESXi version of the host is ESXi 6.0 update 2 or ESXi 6.5 or later.
- For operating system requirement, see the Compatibility Matrix at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.
- Change the guest operating system to **Microsoft Windows Server 2016**. To do so, right-click the virtual machine, and select **Edit settings** > **Options** > **General Options**. Select the guest operating system as **Microsoft Windows Server 2016**.
- During Windows Server 2016 upgrade, you might be prompted to uninstall anti virus owing to a change in behavior of Windows Server. Re-install the anti-virus after the upgrade.
- Server for NIS Tools is not supported when you upgrade the system to Microsoft Windows Server 2016. Therefore, remove the **Server for NIS Tools** feature from Server Manager before upgrading the system. To do that:
  1. Go to Server Manager and open **Remove Roles and Features Wizard**.
  2. On the **Remove Features** page, expand **Remote Server Administration Tools** > **Role Administration Tools** > **AD DS and AD LDS Tools** > **AD DS Tools**.
  3. Uncheck **Server for NIS Tools [DEPRECATED]** and continue with the wizard.

Step 1 Mount Windows Server ISO image to the virtual machine. Open the file explorer and double-click on the **DVD Drive** to run the Windows Server setup.

Step 2 Select **Download & install updates** to let the installation go on smoothly. Click **Next**.

Step 3 Select **Windows Server Desktop Experience**. Click **Next**.

Step 4 Read the notes and license terms and then click **Accept**.

Step 5 To retain existing Unified CVP configurations, files, services, and all associated settings intact after the inplace upgrade to Windows Sever 2016, select **Keep personal files and apps**. Then click **Next**.

Note If you select **Nothing**, everything (including Unified CVP) in the existing Windows Server 2012 VM will be erased, and the system will be set up as a new Windows Server 2016 VM.

Step 6 In case a Window is displayed with the title **What needs your attention**, click **Confirm** to proceed because existing Unified CVP on Windows Server 2012 has been successfully validated to be working on Windows Server 2016 when such an upgrade process is followed.

Note Once the upgrade begins, the system will restart multiple times without prompting until the upgrade is completed.

Step 7 Use your existing credentials to log in to the system and ensure that Unified CVP-related services are up and running after the completion of Windows Server 2012 platform upgrade to Windows Server 2016.

Related Topics

Configure Virtual CPU Settings , on page 4

Unload Data from Reporting Server Database

Load Data to Reporting Server Database

Configure Reporting Server in Operations Console

Upgrade Unified CVP

Note When you upgrade Cisco Unified CVP Server (VXML Server included), you must also upgrade Unified Call Studio to the same version. Unified Call Studio can work with CVP Server only if both of them have the same version.

Perform the Unified CVP upgrade in the following sequence:

Step 1 Back up any third-party libraries (.class or .jar files) that are found at the following locations (where **APP_NAME** is the name of each deployed voice application):

- `%CVP_HOME%\VXMLServer\common\classes`
- `%CVP_HOME%\VXMLServer\common\lib`
- `%CVP_HOME%\VXMLServer\applications\APP_NAME\java\application\classes`
- `%CVP_HOME%\VXMLServer\applications\APP_NAME\java\application\lib`
- `%CVP_HOME%\VXMLServer\applications\APP_NAME\java\util`

Note By default, %CVP_HOME% is `C:\Cisco\CVP`.

Tomcat is upgraded from 8.0.33 to 9.0.8 in Unified CVP 12.0(1). Back up any third-party .jar files that are required by VXML applications from the `%CVP_HOME%\VXMLServer\Tomcat\common\lib` folder. This common folder is no more available in Tomcat 9.0.8. As a result, after upgrading to Unified CVP 12.0(1), copy the earlier backed up .jar files back to `%CVP_HOME%\VXMLServer\Tomcat\lib` folder.

Step 2 Upgrade Cisco Unified CVP Operations Console (OAMP). For more information, see the Upgrade Operations Console section.

Step 3 (Optional) Upgrade Cisco Unified CVP Reporting Server. For more information, see the Upgrade Reporting Server section.

Step 4 Upgrade Cisco Unified CVP Server. For more information, see the Upgrade CVP Server section.

Step 5 Upgrade Cisco Unified Remote Operations. For more information, see the Upgrade Remote Operations section.

Step 6 Upgrade Cisco Unified Call Studio. For more information, see the Upgrade Call Studio section.

Step 7 Upgrade the previously deployed Unified CVP voice applications.

Upgrade Operations Console

The installed default media files are overwritten with the media format you choose for the Unified CVP upgrade; however, the customized media files are not overwritten during the upgrade. Customized media files, such as custom applications and Whisper Agent-Agent Greeting (WAAG), are retained in the format as they were prior to upgrade.

Note For Unified CVP upgrade, u-law is the default media file format type.

Following sections describe the various scenarios of Operations Console upgrade.

Upgrade Operations Console 11.6(1) in U-law to Operations Console 12.0(1) in U-law

Step 1 Mount the Unified CVP ISO image.

Step 2 Navigate to `C:\CVP\installer_windows` and run setup.exe.

The installer automatically detects the previous installation and guides you through the upgrade process.

Step 3 Restart the server.

Step 4 Navigate to the `C:\Cisco\CVP\conf` location and manually configure the Unified CVP properties file. For more information, see the Manual Configuration of Unified CVP Properties section.

Step 5 Restart the server.

Upgrade Operations Console 11.6(1) in U-law to Operations Console 12.0(1) in A-law

Step 1 Navigate to the `C:\Cisco\CVP\conf` location.

Step 2 Convert the custom media files, such as custom applications and Whisper Agent-Agent Greeting (WAAG), and applications that are in u-law to A-law.

Step 3 In the `cvp_pkgs.properties` file, add the **cvp-pkgs.PromptEncodeFormatALaw = 1** property at line 7 to enable the A-law flag.

Note Ensure that you leave a space before and after the "=" sign.

Step 4 Mount the Unified CVP ISO image, and run setup.exe.

Step 5 Follow the instructions on the screen.

Step 6 Restart the server.

Note

- All the standard packaged media files and applications are installed in A-law format.
- Custom media files, such as custom applications and Whisper Agent-Agent Greeting (WAAG) are retained in the format as they were prior to upgrade.

Step 7 Navigate to the `C:\Cisco\CVP\conf` location and manually configure the Unified CVP properties file. For more information, see the Manual Configuration of Unified CVP Properties section.

Step 8 Restart the server.

Upgrade Operations Console 11.6(1) in A-law to Operations Console 12.0(1) in A-law

Step 1 Navigate to the `C:\Cisco\CVP\conf` location.

Step 2 In the `cvp_pkgs.properties` file, add the **cvp-pkgs.PromptEncodeFormatALaw = 1** property at line 7 to enable the A-law flag.

Note Ensure that you leave a space before and after the "=" sign.

Step 3 Mount the Unified CVP ISO image and run setup.exe.

The installer automatically detects the previous installation, and guides you through the upgrade process.

Step 4 Follow the instructions on the screen.

Step 5 Restart the server.

Note

- All the standard packaged media files and applications are installed in the A-law format.
- Custom media files, such as custom applications and WAAG, are retained in the format as they were prior to upgrade.

Step 6 Navigate to the `C:\Cisco\CVP\conf` location and manually configure the Unified CVP properties file. For more information, see the Manual Configuration of Unified CVP Properties section.

Step 7 Restart the server.

What to do next

Load the IOS scripts into the Cisco IOS memory.

Upgrade Operations Console 11.6(1) in A-law or U-law to Operations Console 12.0(1) in G729

Step 1 Navigate to the `C:\Cisco\CVP\conf` location.

Step 2 In the `cvp_pkgs.properties` file, add the **cvp-pkgs.PromptEncodeFormatG729 = 1** property at line 7 to enable the G729 flag.

Note Ensure that you leave a space before and after the "=" sign.

Step 3 Mount the Unified CVP ISO image and run setup.exe.

Step 4 Follow the instructions on the screen.

Step 5 Restart the server.

Note
- All the standard packaged media files and applications are installed in G729 format.
- Custom media files, such as custom applications and Whisper Agent-Agent Greeting (WAAG) are retained in the format as they were prior to upgrade.

Step 6 Navigate to the `C:\Cisco\CVP\conf` location and manually configure the Unified CVP properties file. For more information, see the Manual Configuration of Unified CVP Properties section.

Step 7 Restart the server.

Upgrade Unified CVP Reporting Server

Before you begin

- Back up the Informix database in another drive.
- Turn off the scheduled purge.
- Ensure that the Unified CVP Reporting Server is not part of any domain and is part of a work group. Add it to the domain after the upgrade, if necessary.

Perform the following steps to upgrade the Unified CVP Reporting Server:

Step 1 Perform Steps 1 to 5 of the Install Unified CVP Reporting Server procedure.

Step 2 From the **Ready to Install the Program** window, select **Unified CVP Reporting Server** component and click **Upgrade**.

Step 3 On the **Authentication** window, enter a password and click **Next**.

Note
- Adhere to the password formation criteria that are listed in the Configuring Secure Passwords section.
- After the upgrade, add the Unified CVP Reporting Server to the domain, if necessary.
- Do not cancel the **cvp_dbadmin user authentication** popup window.

Step 4 Choose to restart the computer right after the upgrade or to restart it later, and click **Finish**.

Step 5 Navigate to the `C:\Cisco\CVP\conf` location and manually configure the Unified CVP properties file. For more information, see the Manual Configuration of Unified CVP Properties section.

Step 6 Restart the server.

Upgrade Unified CVP Server

Before you begin

For A-law implementation in Unified CVP Server, install the latest Unified CVP FCS build.

Note After successful upgrade of Unified CVP server, the **CVP Call Server Service Startup Type** is set to **Automatic** by default.

Upgrade CVP Server 11.6(1) in U-law to CVP Server 12.0(1) in U-law

Perform Steps 1 to 4 of the Upgrade Operations Console in U-law to Operations Console 12.0(1) in U-law procedure.

1. Log into Operations Console of the current version of Unified CVP and click **Bulk Administration** > **File Transfer** > **Scripts and Media**.

2. Load the gateway download transferred files into the Cisco IOS memory for each CVP service using the Cisco IOS **call application voice load <service_name>** CLI command.

3. Restore any backed-up third-party libraries.

4. Upgrade the CVP Server's license.

Upgrade CVP Server 11.6(1) in U-law to CVP Server 12.0(1) in A-law

Perform Steps 1 to 8 of the Upgrade Operations Console 11.6(1) in U-law to Operations Console 12.0(1) in A-law.

Upgrade CVP Server 11.6(1) in A-law to CVP Server 12.0(1) in A-law

Perform Steps 1 to 7 of the Upgrade Operations Console 11.6(1) in A-law to Operations Console 12.0(1) in A-law procedure.

Upgrade CVP Server 11.6(1) in A-law or U-law to CVP Server 12.0(1) in G729

Perform Steps 1 to 7 of the Upgrade Operations Console 11.6(1) in A-law or U-law to Operations Console 12.0(1) in G729 procedure.

Upgrade Remote Operations

Step 1 Mount the Unified CVP ISO image, and run setup.exe.

The installer automatically detects the installation and upgrade of Remote Operations and guides you through the upgrade process.

Step 2 Follow the instructions on the Upgrade screens and click **Upgrade**.

Step 3 Restart the Server.

Upgrade Unified Call Studio

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.

Postupgrade Tasks

After you upgrade the Unified CVP components, synchronize the metadata files using the Sync-up tool. For more information, see Initiate Metadata Synchronization for Unified CVP Rest API.

Note

- If Context Services is enabled, then register the device with Context Services again through OAMP.
- 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.

Note If Context Service is enabled and you have added the certificates in `%CVP_HOME%\conf\security\.keystore`, add them again in `.keystore` on all VXML servers.

Execute the following command to retrieve the password for keytool.

```
more %CVP_HOME%\conf\security.properties.
```

The output of the command is `Security.keystorePW = <Returns the keystore password>`.

Related Topics

Initiate Metadata Synchronization for Unified CVP Rest API
Unified CVP Redeployment

Manual Configuration of Unified CVP Properties

The following table lists the procedure to manually configure the Unified CVP properties files based on the upgrade path.

Table 2: Manual Configuration of Unified CVP Properties

Unified CVP Component	Upgrade Path	Manual Configuration Process
CVP Server	11.0(1) to 12.0(1)	

Unified CVP Component	Upgrade Path	Manual Configuration Process

		1. Upgrade to 11.5(1)/11.6(1).
		2. Navigate to the `C:\Cisco\CVP\conf` location.
		3. Open the cvpwsmconfig.properties file and add the following entry:
		`wsm.job.cleanup.duration=1`
		4. Open the icm.properties file and update the following entry:
		`#Maximum Number Of Calls`
		` ICM.maxCalls=6144`
		`#Use newcall trunk group id for pre-routed calls(Default is`
		` true)`
		`ICM.useNewCallTrunkGroupIDforPreRoutedCall = false`
		5. Open the orm.xml file and replace the existing content with the following content:
		`<?xml version="1.0" encoding="UTF-8"?>`
		`<orm xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"`
		`xsi:noNamespaceSchemaLocation="orm.xsd">`
		` <ormAddresses />`
		`</orm>`
		6. Open the system.properties file and update the following entry:
		`ThreadManager.totalThreads = 500`
		`Infrastructure.threadWeight=4`
		`SIP.threadWeight=50`
		`IVR.threadWeight=1`
		`ICM.threadWeight=1`
		Remove the following entry:
		`CVPServlet.upgradeProperties = true`
		7. Open the vxml.properties file and add the following entry:
		`#ContextService properties`
		`#*******************************************************`
		`VXML.ContextService.maxRetries=1`
		`VXML.ContextService.requestTimeout=1200`
		`VXML.ContextService.labMode=false`
		`VXML.ContextService.executorThreadPoolSize=50`
		`VXML.ContextService.httpMaxConnectionsPerRoute=50`
		`VXML.ContextService.statsLogInterval=1800000`
		`VXML.ContextService.getStatusInterval = 30000`
		`#*******************************************************`
		8. Open the ivr.properties file and update the following entry:
		`# Valid media file extensions list.`
		`IVR.ValidMediaFileExtension=.wav, .au, .vox, .rm`

Unified CVP Component	Upgrade Path	Manual Configuration Process

		9. Open the oamp.properties file and add the following entries in the respective files:
		oamp.properties
		# ---- OAMP Interval for Context Service get Status in seconds (default: 30 seconds) ----
		omgr.contextServiceStatusInterval=30
		# ---- Context Service status timeout value (in seconds) ----
		omgr.csStatusTimeout=180
		# ---- SSL Context to be used
		omgr.sslContextProtocol=TLSv1.2
		10. Open the sip.properties file and add the following entry:
		#whether to send Reinvite to caller after Whipser done
		SIP.ReinviteCallerAfterWhisperDone=true
		#System wide ReasonCode to cause code Mapping
		SIP.System.ReasonCodeToCauseCode=

<table>
<tr><th>Unified CVP Component</th><th>Upgrade Path</th><th>Manual Configuration Process</th></tr>
<tr><td></td><td></td><td>
<b>11.</b> Open the sip.properties file and add the following entry:
<pre>
# Outbound proxy SIP listen (secure) port.
SIP.Proxy.Secure.Port=5061

# Port on which to listen for incoming sip secure requests.
SIP.Incoming.Secure.Port = 5061

# KeyStorePath
SIP.Secure.KeyStorePath =
C:\\Cisco\\CVP\\conf\\security\\.keystore
<b>Note:</b> This file path must be the actual install path.

# KeyStorePassword
SIP.Secure.KeyStorePassword =

# TrustStorePath
SIP.Secure.TrustStorePath =

# TrustStorePassword
SIP.Secure.TrustStorePassword =

#KeyStoreType
SIP.Secure.KeyStoreType = JCEKS

#TrustStoreType
SIP.Secure.TrustStoreType =

# KeyAlgorithm
SIP.Secure.KeyAlgorithm = SunX509

#TrustStoreAlgorithm
SIP.Secure.TrustStoreAlgorithm =

# Incoming secure Protocol
SIP.Incoming.Secure.Transport = TLS

#Outgoing secure Protocol
SIP.Outgoing.Secure.Transport = TLS

#Secure ciphers colon(;) seperated e.g
TLS_RSA_WITH_AES_128_CBC_SHA
SIP.Secure.Ciphers = TLS_RSA_WITH_AES_128_CBC_SHA

#Secure TLS versions flags e.g TLSv1,TLSv1.1,TLSv1.2
SIP.Secure.Tlsv1Enabled = false
SIP.Secure.Tlsv1dot1Enabled = false
SIP.Secure.Tlsv1dot2Enabled = true

#Secure Protocol
SIP.Secure.Protocol = TLS

# Client Certificate is needed or not.
SIP.Secure.UseClientAuth = false

#Whether to use backup IVR Sub System

SIP.UseBackupIVRSS = false

#Calls Max Threshold
</pre>
</td></tr>
</table>

Unified CVP Component	Upgrade Path	Manual Configuration Process

		`SIP.CallsMaxThreshold = -1`
		`Note: This value indicates the maximum number of calls that a Call Server can process. The default value is -1, which denotes the maximum number of licenses (3000). This value can be configured in the range of 0-3000.`
		12. Add the following entries in the respective files:
		`jmx_callserver.conf`
		`com.sun.management.jmxremote.rmi.port = 2097`
		`com.sun.management.jmxremote.ssl.enabled.protocols=TLSv1.2`
		`jmx_oamp.conf`
		`com.sun.management.jmxremote.rmi.port = 10000`
		`com.sun.management.jmxremote.ssl.enabled.protocols=TLSv1.2`
		`jmx_vxml.conf`
		`com.sun.management.jmxremote.rmi.port = 9697`
		`com.sun.management.jmxremote.ssl.enabled.protocols=TLSv1.2`
		`jmx_wsm.conf`
		`com.sun.management.jmxremote.rmi.port = 10003`
		`com.sun.management.jmxremote.ssl.enabled.protocols=TLSv1.2`
		`orm_jmx.properties`
		`com.sun.management.jmxremote.rmi.port=3000`
		`com.sun.management.jmxremote.ssl.enabled.protocols=TLSv1.2`
		13. Open the orm.properties file and add the following entries in the respective files:
		`orm.properties`
		`#Media server root directory.`
		`mediaserver.root.dir =`
		`# ---- SSL Context to be used`
		`orm.sslContextProtocol=TLSv1.2`

<table>
<tr><th>Unified CVP Component</th><th>Upgrade Path</th><th>Manual Configuration Process</th></tr>
<tr><td></td><td></td><td>
<p><b>14.</b> Navigate to the <code>C:\Cisco\CVP</code> location and locate the connector node with attribute SSLCertificateFile="<install_path>\security\wsm.crt" in the file: <code>wsm\Server\Tomcat\conf\server.xml</code> and add the following:</p>
<pre>
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256"
</pre>
<pre>
sslEnabledProtocols="TLSv1.2"
</pre>
<pre>
Example:
<Connector
SSLCertificateFile="C:\Cisco\CVP\conf\security\wsm.crt"
SSLCertificateKeyFile="C:\Cisco\CVP\conf\security\wsm.key"
 SSLEnabled="true"
acceptCount="100"
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256"

clientAuth="false" disableUploadTimeout="true"
enableLookups="true"
executor="tomcatThreadPool" keyAlias="wsm_certificate"
keystoreFile="C:\Cisco\CVP\conf\security\.keystore"
keystorePass="****" keystoreType="JCEKS"
port="8111"
protocol="org.apache.coyote.http11.Http11NioProtocol"
scheme="https" secure="true" sslEnabledProtocols="TLSv1.2"
 sslProtocol="TLS"/>
</pre>
<p><b>15.</b> Locate the connector node with the attribute SSLCertificateFile="<install_path>\security\vxml.crt" in the file: <code>VXMLServer\Tomcat\conf\server.xml</code></p>
<p>and add or update the following:</p>
<pre>
sslEnabledProtocols="TLSv1.2"
</pre>
<p><b>16.</b> Locate the connector node with the attribute SSLCertificateFile="<install_path>\security\vxml.crt" in the file: <code>CallServer\Tomcat\conf\server.xml</code></p>
<p>and add or update the following:</p>
<pre>
sslEnabledProtocols="TLSv1.2"
</pre>
<p><b>17.</b> Navigate to the <code>C:\Cisco\CVP</code> location, and add CauseCode property in the excluded list for Unreachable Table (for example: 47):</p>
<pre>
SIP.System.ExcludedCauseCodeFromUnreachableTable =
</pre>
<p><b>18.</b> Navigate to the <code>C:\Cisco\CVP</code> location, and modify the Unreachable Timer property (default is 180 seconds; max is 180 seconds; min is 10 seconds):</p>
<pre>
SIP.DsUnreachableDestinationTableTimer = 180
</pre>
</td></tr>
</table>

Unified CVP Component	Upgrade Path	Manual Configuration Process

		19. Go to Tomcat's JVM arguments of VXML Server, and replace the following registry entry:
		`Dhttps.client.protocol=TLSv1.2`
		with
		`Djdk.tls.client.protocols=TLSv1.2`

CVP Server	11.5(1)/ 11.6(1) to 12.0(1)	**1.** Open the icm.properties file and update the following:
		`#Use newcall trunk id for pre-routed calls (Default is true)`
		`ICM.useNewCallTrunkGroupIDforPreRoutedCall = false`
		2. Open the ivr.properties file and add the following entry:
		`# Mask the printing of the CED/ECC values in the logs.`
		`IVR.isMaskedEnabled = true`

CVP Server	11.6(1) to 12.0(1)	**1.** Go to the icm.properties file and add the following properties:
		• ICM.enableSecureVRU = false
		• ICM.Secure.UseClientAuth = true
		2. Open the ivr.properties file and add the following entry:
		`# Mask the printing of the CED/ECC values in the logs.`
		`IVR.isMaskedEnabled = true`

WebServices Manager	11.0(1)/ 11.5(1)/ 11.6(1) to 12.0(1)	Open the cvpwsmconfig.properties file and add the following entry: `wsm.job.cleanup.duration=1`

Unified CVP Component	Upgrade Path	Manual Configuration Process
Operations Console	11.0(1) to 12.0(1)	

Unified CVP Component	Upgrade Path	Manual Configuration Process

		1. Upgrade to 11.5(1)/11.6(1).
		2. Navigate to the `C:\Cisco\CVP\conf` location
		3. Open the cvpwsmconfig.properties file and add the following entry:
		`wsm.job.cleanup.duration=1`
		4. Open the icm.properties file and add the following entry:
		`# Maximum Number Of Calls`
		` ICM.maxCalls=6144`
		`#Use newcall trunk group id for pre-routed calls(Default is`
		` true)`
		`ICM.useNewCallTrunkGroupIDforPreRoutedCall = false`
		5. Open the orm.xml file, and replace the existing content with the following content:
		`<?xml version="1.0" encoding="UTF-8"?>`
		`<orm xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"`
		`xsi:noNamespaceSchemaLocation="orm.xsd">`
		` <ormAddresses />`
		`</orm>`
		6. Open the system.properties file and add the following entry:
		`ThreadManager.totalThreads = 500`
		`Infrastructure.threadWeight=4`
		`SIP.threadWeight=50`
		`IVR.threadWeight=1`
		`ICM.threadWeight=1`
		`Remove the following entry:`
		`CVPServlet.upgradeProperties = true`
		7. Open the oamp.properties file and add the following entries in the respective files:
		`oamp.properties`
		`# ---- OAMP Interval for Context Service get Status in`
		`seconds (default: 30 seconds) ----`
		`omgr.contextServiceStatusInterval=30`
		`# ---- Context Service status timeout value (in seconds)`
		`----`
		`omgr.csStatusTimeout=180`
		`# ---- SSL Context to be used`
		`omgr.sslContextProtocol=TLSv1.2`
		8. Navigate to the `C:\Cisco\CVP` location and locate the connector node with attribute SSLCertificateFile="<install_path>\security\wsm.crt" in the file: `wsm\Server\Tomcat\conf\server.xml` and add the following:

Unified CVP Component	Upgrade Path	Manual Configuration Process

		ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
		TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
		TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,
		TLS_RSA_WITH_AES_128_CBC_SHA256"
		sslEnabledProtocols="TLSv1.2"
		Example:
		<Connector
		SSLCertificateFile="C:\Cisco\CVP\conf\security\wsm.crt"
		SSLCertificateKeyFile="C:\Cisco\CVP\conf\security\wsm.key"
		SSLEnabled="true"
		acceptCount="100"
		ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
		TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,
		TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256"
		clientAuth="false" disableUploadTimeout="true"
		enableLookups="true"
		executor="tomcatThreadPool" keyAlias="wsm_certificate"
		keystoreFile="C:\Cisco\CVP\conf\security\.keystore"
		keystorePass="****" keystoreType="JCEKS"
		port="8111"
		protocol="org.apache.coyote.http11.Http11NioProtocol"
		scheme="https" **secure="true" sslEnabledProtocols="TLSv1.2"**
		**sslProtocol="TLS"**/>
		9. Locate the connector node with the attribute SSLCertificateFile="<install_path>\security\vxml.crt" in the file: OPSConsoleServer\Tomcat\conf\server.xml
		and add or update the following:
		sslEnabledProtocols="TLSv1.2"

Unified CVP Component	Upgrade Path	Manual Configuration Process

		10. Navigate to the `C:\Cisco\CVP` location and locate the connector node with attribute SSLCertificateFile="<install_path>\security\wsm.crt" in the file: `wsm\OPSConsoleServer\Tomcat\conf\server.xml` and add the following:
		`ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,`
		`TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,`
		`TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,`
		`TLS_RSA_WITH_AES_128_CBC_SHA256"`
		`sslEnabledProtocols="TLSv1.2"`
		`Example:`
		`<Connector`
		`SSLCertificateFile="C:\Cisco\CVP\conf\security\wsm.crt"`
		`SSLCertificateKeyFile="C:\Cisco\CVP\conf\security\wsm.key"`
		` SSLEnabled="true"`
		`acceptCount="100"`
		`ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,`
		`TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,`
		`TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256"`
		`clientAuth="false" disableUploadTimeout="true"`
		`enableLookups="true"`
		`executor="tomcatThreadPool" keyAlias="wsm_certificate"`
		`keystoreFile="C:\Cisco\CVP\conf\security\.keystore"`
		`keystorePass="****" keystoreType="JCEKS"`
		`port="8111"`
		`protocol="org.apache.coyote.http11.Http11NioProtocol"`
		`scheme="https"` **`secure="true" sslEnabledProtocols="TLSv1.2"`**
		` sslProtocol="TLS"``/>`
		11. Locate the connector node with the attribute SSLCertificateFile="<install_path>\security\vxml.crt" in the file: `OPSConsoleServer\Tomcat\conf\server.xml`
		and add or update the following:
		`sslEnabledProtocols="TLSv1.2"`

Unified CVP Component	Upgrade Path	Manual Configuration Process

		12. Navigate to the `C:\Cisco\CVP` location and locate the connector node with attribute SSLCertificateFile="<install_path>\security\wsm.crt" in the `wsm\OPSConsoleServer\Tomcat\conf\server.xml` file and add the following:
		`ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,`
		`TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,`
		`TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,`
		`TLS_RSA_WITH_AES_128_CBC_SHA256"`
		`sslEnabledProtocols="TLSv1.2"`
		`Example:`
		`<Connector`
		`SSLCertificateFile="C:\Cisco\CVP\conf\security\wsm.crt"`
		`SSLCertificateKeyFile="C:\Cisco\CVP\conf\security\wsm.key"`
		` SSLEnabled="true"`
		`acceptCount="100"`
		`ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,`
		`TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,`
		`TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256"`
		`clientAuth="false" disableUploadTimeout="true"`
		`enableLookups="true"`
		`executor="tomcatThreadPool" keyAlias="wsm_certificate"`
		`keystoreFile="C:\Cisco\CVP\conf\security\.keystore"`
		`keystorePass="****" keystoreType="JCEKS"`
		`port="8111"`
		`protocol="org.apache.coyote.http11.Http11NioProtocol"`
		`scheme="https"` **`secure="true" sslEnabledProtocols="TLSv1.2"`**
		` sslProtocol="TLS"``/>`
		13. Locate the connector node with the attribute SSLCertificateFile="<install_path>\security\vxml.crt" in the `OPSConsoleServer\Tomcat\conf\server.xml` file
		and add or update the following:
		`sslEnabledProtocols="TLSv1.2"`

Unified CVP Component	Upgrade Path	Manual Configuration Process

Operations Console	11.5(1) to 12.0(1)	1. Navigate to the `C:\Cisco\CVP` location and locate the connector node with attribute SSLCertificateFile="<install_path>\security\wsm.crt" in the `wsm\OPSConsoleServer\Tomcat\conf\server.xml` file and add the following:
		`ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,`
		`TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,`
		`TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,`
		`TLS_RSA_WITH_AES_128_CBC_SHA256"`
		`sslEnabledProtocols="TLSv1.2"`
		`Example:`
		`<Connector`
		`SSLCertificateFile="C:\Cisco\CVP\conf\security\wsm.crt"`
		`SSLCertificateKeyFile="C:\Cisco\CVP\conf\security\wsm.key"`
		`SSLEnabled="true"`
		`acceptCount="100"`
		`ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,`
		`TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,`
		`TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256"`
		`clientAuth="false" disableUploadTimeout="true"`
		`enableLookups="true"`
		`executor="tomcatThreadPool" keyAlias="wsm_certificate"`
		`keystoreFile="C:\Cisco\CVP\conf\security\.keystore"`
		`keystorePass="****" keystoreType="JCEKS"`
		`port="8111"`
		`protocol="org.apache.coyote.http11.Http11NioProtocol"`
		`scheme="https" secure="true" sslEnabledProtocols="TLSv1.2"`
		`sslProtocol="TLS"/>`
		2. Locate the connector node with the attribute SSLCertificateFile="<install_path>\security\vxml.crt" in the `OPSConsoleServer\Tomcat\conf\server.xml` file
		and add or update the following:
		`sslEnabledProtocols="TLSv1.2"`

Operations Console	11.6(1) to 12.0(1)	No configuration required.

Unified CVP Component	Upgrade Path	Manual Configuration Process

Reporting Server	11.0(1)/ 11.5(1)/ 11.6(1) to 12.0(1)	**1.** Open the reporting.properties file and add the following entry:
		`#Password of cvp_dbadmin`
		`RPT.DBAdminPassword = ENCRYPTEDPWD`
		`#Time spent by the caller in the first position of the queue. Default is false.`
		`RPT.ewtWithFirstInQueueTime = false`
		`#UseFirstInQueueRetryTime to use retry time of firstpostion in queue (true/false). Default is false.`
		`RPT.UseFirstInQueueRetryTime = false`
		Note The value (ENCRYPTEDPWD) of the new entry must be same as that of the RPT.DBPassword value.