Installation and Upgrade Guide for Cisco Unified Customer Voice Portal, Release 12.0(1)

First Published: 2019-01-11

C O N T E N T S

Preface

- Change History, on page vii
- About this Guide, on page viii
- Audience, on page viii
- Related Documents, on page viii
- Communications, Services, and Additional Information, on page viii
- Documentation Feedback, on page ix

Change History

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

Change	See	Date
Initial Release of Document for Release 12.0(1)		

Change	See	Date
Upgrade to Windows Server 2016	Global change	January 2019
Removed instances of ESXi 5.5 update 2	Install Microsoft Windows Server Upgrade Windows Server Upgrade Virtual Machine Hardware Version	
Added notes about Windows Defender	Requirements Upgrade Unified CVP	
Updated Tomcat version and added a note to ensure uninterrupted services in Unified CVP 12.0(1)	Requirements	
Removed license for Call Studio	License Plan	
Added new property files for Unified CVP 12.0(1)	Manual Configuration of Unified CVP Properties	

About this Guide

This document explains how to install and upgrade 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*

- *Solution Design Guide for Cisco Unified Customer Voice Portal*

- *Compatibility Matrix*

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.

Pre-Installation

This chapter provides the tasks that you must perform prior to installing the Unified CVP software.

Important You must stop any third-party services and applications running on the server prior to running the Unified CVP Installer. Some third party services and applications can lock files required by the installer, resulting in an install error.

Unified CVP Components

Table 1: Unified CVP Components

Unified CVP Component	Description
Unified CVP Server	This server consists of: • Unified CVP Call Server • Unified CVP VXML Server • Media Server • SNMP Monitoring service
Operations Console	The Operations Console (OAMP, also known as Operation Administration Maintenance and Provisioning, is a web-based interface that enables you to configure and manage individual components of Unified CVP.
Remote Operations	This component allows remote administration of Unified CVP solution components. It includes Operations and Resource Module (ORM).

Unified CVP Component	Description
Unified CVP Reporting Server	This server provides a historical repository, which can be used for reporting, for a call center. It receives reporting data from one or more Unified CVP Call Servers and Unified CVP VXML Servers, and stores that data in a database. **Note** The IBM Informix database is installed as a part of the Reporting Server. The license of IBM Informix comes bundled as a part of Reporting Server.
Unified Call Studio	This component provides design and syntax for developing call flow for VXML-based execution. Unified Call Studio also supports debugger for application. This helps validate Unified Call Studio application.

Requirements

This section describes the platform and software requirements for Cisco Unified Customer Voice Portal (CVP).

Table 2: Unified CVP Platform and Software Requirements

Unified CVP Component/Task	Platform Requirement
Unified CVP Server	**Note** Refer to the *Cisco Collaboration Virtualization* page at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html.
Unified Operations Console	
Unified Reporting Server	
Unified Call Studio	4GB+ RAM Microsoft Windows 10
Virtualized Platform	Cisco Unified Computing System (UCS) B-Series and C-Series **Note** Access the open virtualization archive (OVA) template at: https://software.cisco.com/download/type.html?mdfid=270563413&flowid=5229.

Note If you are using Unified CVP 12.0 with Cisco VVB 11.5/11.6, then calls may fail as Cisco VVB 11.5/11.6 is not compatible with Tomcat 9.0.8 used in Unified CVP 12.0. To ensure uninterrupted services:

- For Cisco VVB 11.6, install VVB 11.6 ES-84 or upgrade to Cisco VVB 12.0.

- For Cisco VVB 11.5, upgrade to Cisco VVB 12.0.

For information about hardware requirements and compatibility, see the *Unified CCE Solution Compatibility Matrix* available at: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

Unified CVP Server

Category	Requirements
Operating System	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. **Note** To apply the latest Operating System Service Upgrade Release, go to Microsoft upgrade website.
Additional Items	A minimum of 10MB should be available for Unified CVP system media files. Cisco provides .wav files for numbers, days, months, currency types in American English and Latin American Spanish. **Note** Any additional media files will require additional space. By default, the Call Server and the VXML Server are on the same physical machine. For more information, see *Solution Design Guide for Cisco Unified Contact Center Enterprise*, available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html. On Windows platforms, Call Servers require Simple Network Management Protocol and WMI Windows Installer Provider to be installed.
Restriction	Although supported third-party virus scan software can be enabled on the Call Server, full fixed disk virus scans must take place either offline while calls have been diverted to a different system or during a period of low call volume. Do not run a full fixed disk scan while the Call Server is under load.

Unified CVP Operations Console

Category	Requirements
Operating System	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. **Note** To apply the latest Operating System Service Upgrade Release, go to the Microsoft upgrade web site.

[Optional] Unified CVP Reporting Server

Category	Requirements
Operating System	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. **Note** To apply the latest Operating System Service Upgrade Release, go to Microsoft upgrade website.
Restriction	Although supported third-party virus scan software can be enabled on the Reporting Server, full fixed disk virus scans must take place either offline while calls have been diverted to a different system or during a period of low call volume. Do not run a full fixed disk scan while the Reporting Server is under load.

[Optional] Unified Call Studio

Category	Requirements
Supported Hardware	4GB+ RAM required

Configure Secure Passwords

To configure a secure password for Reporting Server users (informix, cvp_dbadmin, cvp_dbuser) and the Operations Console Administrator user, your password must comply with the following rules:

- The password must contain characters only from the ASCII character set:

  - Uppercase and lowercase letters of the English alphabets

  - Numeric characters [0-9]

  - Special characters from this set: !#$&()*+./<?@[\]^_`{}~

- The password length must be 12 characters or more.

- The password must meet the following password complexity:

  - The password must use three of four of the following four types of characters:

    - At least one uppercase letter [A-Z]

    - At least one lowercase letter [a-z]

    - At least one numeric character [0-9]

    - At least one special character from this set: !#$&()*+./<?@[\]^_`{}~

Additional Components

- The characters in the password must not be repeated more than three times consecutively.

- The password must not be "cisco", "ocsic", or any variant obtained by changing the capitalization of letters therein.

Additional Components

You can use the following components that are not part of the Unified CVP software but may be used with Unified CVP for a complete contact center solution.

- Automatic Speech Recognition (ASR) Server/ Text-to-speech (TTS) Server

- Cisco Unified Contact Center Enterprise

- Cisco Unified Communications Manager

- Cisco Unified SIP Proxy

- Ingress Gateway

- Egress Gateway

- Voice XML Gateway

- Cisco Unified Border Element (CUBE)

- Cisco Unified Intelligence Center (CUIC)

- Cisco Virtualized Voice Browser

Unified CVP Installation Modes

Table 3: Unified CVP Installation Modes

Installation Mode	Description
Production	In production mode, you can install only one Unified CVP component on a virtual machine server at a time. If you need to install additional components, you must install these components on a different virtual machine server.
Lab only	Use this mode to install Unified CVP for learning and testing. To use lab only mode, launch the installer from the command line, browse to the setup.exe folder, and enter **setup.exe labonly**. **Note** In lab only mode, the Call Server, OAMP Server, and Reporting Server can be installed together but you cannot selectively uninstall one of them. For example, if you want to remove the Reporting Server you must reinstall Unified CVP.

5

Pre-Installation Tasks

Install Microsoft Windows Server

Complete the following procedure to install Microsoft Windows Server 2016 on all virtual machines for server-based applications.

Before you begin

- Ensure that VMware Tools software is installed. You cannot install VMXNET3 driver without VMware Tools.

- Ensure that ESXi version of the host is ESXi 6.0 update 2 or ESXi 6.5 with VMFS5.

- Ensure that ESXi version of the host is ESXi 6.5 with VMFS 5, ESXi 6.5 U2 and later updates with VMFS 6, or ESXi 6.7 with VMFS 6.

- Ensure that the length of the host name for CVP server is not more than 15 characters.

- Ensure that you have deployed the OVA template for the respective CVP components.

Step 1	Mount Microsoft Windows Server 2016 ISO image to the virtual machine.
Step 2	Power on the virtual machine.
Step 3	Enter the Language, Time and Currency Format, and Keyboard settings. Click **Next**.
Step 4	Click **Install Now**.
Step 5	Select the appropriate version of the windows server with Desktop Experience option that meets your organization's needs, and then click **Next**. Make sure that you have chosen an appropriate edition of Windows server with Desktop Experience.
Step 6	Accept the license terms and click **Next**.
Step 7	Select the **Custom: Install Windows only (advanced)** option for clean installation.
Step 8	Select the hard drive that you want to install the windows server on, and then click on the **New** button to do the partitions.
Step 9	Specify the amount of the drive based on **MB** and then click on the **Apply** button. A warning appears to give the permission to system to create a drive for system files. Click **Cancel**. It is recommended not to change the size of the drive. The installation begins. After the installation is complete, the system restarts without prompting.
Step 10	Enter and confirm the password for the administrator account, and then click **Finish**.

Microsoft Windows Server 2016 is installed. In addition, Internet Explorer 11 is installed automatically. For more information, see *VMware Deployment Checklist*.

Fresh Installation

Fresh Install

Step 1   Obtain the Unified CVP ISO image to install Unified CVP.

Step 2   Obtain the supported virtualization hardware and software that are required for the virtualization of Unified CVP.

Step 3   Identify the components for the required deployment model. For information about hardware requirements compatibility, see the *Unified CCE Solution Compatibility Matrix* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

Step 4   Ensure that the servers are listed as supported hardware and sized appropriately.

Step 5   Verify that the any new server hardware, such as hard drive, is working properly.

Step 6   Stop any third-party services and applications that are running on the server before you run the Unified CVP Installer. Some third-party services and applications can lock files that are required by the installer resulting in an installation error.

Step 7   Obtain licenses for the required CVP components.

Multiple Ethernet Interfaces

The machine that you are using for the Unified CVP Call Server must have only one Ethernet interface enabled. When installing Unified CVP on a machine with two or more Ethernet interfaces, the additional interface(s) must be disabled, even if they are not configured. Refer to Windows documentation for information on enabling/disabling an Ethernet interface.

Multiple Ethernet Interfaces

CHAPTER 2

Unified CVP Installation

Cisco Unified Customer Voice Portal (CVP) ISO image contains the setup files for all the CVP components in the CVP folder.

Only a local administrator must install the Unified CVP software.

Note
- Before you install Unified CVP, refer to the licensing information in the Unified CVP Licensing, on page 63 chapter.
- Ensure that the server chosen for Reporting Server is part of a workgroup.

Install Unified CVP on Virtual Machines

Before you begin

- Disable large receive offload (LRO) for ESXi for virtualization platform for Unified CVP.

- Install and configure the Unified Computing System (UCS).

- Install and boot VMware ESXi.

- Ensure that ESXi is configured and reachable over the network.

- Download the OVA template.

Step 1 Create the Unified CVP virtual machines using the OVA template.

Step 2   Select the CVP components, as required.

Step 3   Install Windows Server.

Step 4   Install the selected CVP components.

Install Unified CVP Server

Fresh installation of Unified CVP includes the following voice prompt encode format types—u-law, A-law, and G729 for media files. Default applications also get installed along with media files. Choose the format type as per requirement.

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

Step 2   Review and accept the license agreement, and click **Next**.

Step 3   On the **Select Package** screen, choose the Unified CVP component to install on your computer, and click **Next**.

Note   Internet Information Server (IIS) is the default Media Server supported by Unified CVP. For details on IIS configuration, see the Microsoft documentation.

Step 4   At the **Voice Prompt Encode Format Type** screen, select one of the following options:

- **U-Law Encoded Wave Format**

- **A-Law Encoded Wave Format**

- **G729 Encoded Wave Format**

Step 5   On the **Choose Destination Location** screen, select the folder where setup will install files. By default, it is `C:\Cisco\CVP.`

Step 6   On the **X.509 Certificate** screen, enter the required information in the form, and click **Next**.

Step 7   Click **Install**.

Note   You cannot cancel the installation when it is in progress.

Step 8   Choose to restart the computer right after the upgrade or to restart it later, and click **Finish**.

Note   After successful installation, the **CVP Call Server Service Startup Type** is set to **Automatic** by default.

What to do next

Install Operations Console

Related Topics

Install Operations Console

Step 1   Perform Steps 1 to 6 of the Install CVP Server procedure.

Step 2   From the **Ready to Install the Program** screen, review the component that you selected, and click **Install**.

Step 3   On the **Ops Console Password** screen, in the **Password** and **Password (for verification)** fields, enter a password and re-enter it for confirmation, and click **Next**.

> **Note**   Adhere to the password formation criteria that are listed on the Operations Console Password screen section.

> **Note**   Operations Console Administrator and Web Services Administrator (wsmadmin) use the Operations Console password.

Step 4   Select one of the options to either restart the computer right after installation or later, and click **Finish**.

What to do next

Install Remote Operations

Related Topics

Install Remote Operations

Step 1   Perform Steps 1 to 4 of the Install Operations Console procedure.

Step 2   Choose to restart the computer right after the upgrade or to restart it later, and click **Finish**.

What to do next

Install Reporting Server

Related Topics

Install Second Drive on Reporting Server Virtual Machine

Step 1   Right-click **My Computer** > **Manage**.

Step 2   In **Storage** section, click **Disk Management**.

Step 3   Select the unformatted partition, which is usually **Disk 1**.

Step 4   Right-click **Online**, and initialize the disk.

Step 5   Click **Format**, and follow the formatting process with NTFS.

Install Unified CVP Reporting Server

IBM Informix database server 12.10 FC3 is installed as part of the Unified CVP Reporting Server.

Before you begin

- Only the actual Local Administrator (should not be renamed) of this system can install CVP Reporting Server.

- Ensure that Unified CVP Reporting Server is not part of any domain and is part of a work group.

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

Step 2   Review and accept the license agreement, and click **Next**.

Step 3   On the **Select Package** screen, select **Reporting Server**, and click **Next**.

   Note   This step takes approximately 30 seconds before moving to the **Choose Destination Location** window.

Step 4   Select the root drive on which you want the Reporting database data and backup data to reside, and click **Next**.

   Note   Choose the E drive or the second drive, whose size is more than 400GB, to store the Reporting database data and to keep the backup of data.

The **Database Size Selection** screen appears, providing the following options:

- **Standard:** Requires a minimum of 250GB of free disk space.

- **Premium:** Requires a minimum of 375GB of free disk space.

Step 5   Choose the appropriate database size for the license that you purchased, and click **Next**.

Step 6   From the **Ready to Install the Program** window, review the component that you have selected, and click **Install**.

Step 7   On the **Reporting Password** window, enter a password and re-enter it for confirmation, and click **Next**.

   Note   • Adhere to the password formation criteria that are listed on the Operations Console Password screen section.

   • The Reporting password requires that the **Minimum Password Age** parameter be set to 0 days for both the local and/or domain security policy and is subject to both the Unified CVP password policy and the password policy enforced by the operating system of the computer on which the Reporting Server resides. For each aspect of the password, the Reporting password must meet the requirement of the more restrictive policy. If you are installing CVP Reporting Server please ensure that your local and/or domain security policy for MINIMUM PASSWORD AGE are set to 0 days for the installation of the CVP Reporting Server component (In Windows, **Control Panel** > **Administrative Tools** > **Local Security Policy** > **Account Policy** > **Password Policy**). If the reporting password you enter is rejected, review the list of password requirements displayed by the installer and consider your operating system's password requirements. You can reconfigure this password repeatedly until an acceptable password is found.

   • After installation, add the Unified CVP Reporting Server to the domain, if necessary.

Step 8   Choose to restart the computer right after installation or to restart it later, and click **Finish**.

Install Unified Call Studio

Step 1   Mount the Unified CVP software (including CVP Studio) installer ISO image, and run setup.exe.

Step 2   On the **Welcome** screen, click **Next**.

> **Note**   If you click **Cancel** here or on the dialog screens that follow before the **Ready to Install the Program** screen, the installation is canceled. The **Exit Setup** dialog box appears.

Step 3   Review **Copyrights to Products** used by Call Studio and click **Next**.

Step 4   Review and accept the license agreement, and click **Next**.

Step 5   On the Choose Destination Location screen, select the folder where setup will install files. By default, it is `C:\Cisco\CallStudio`.

Step 6   On the **InstallShield Wizard Complete** screen, click **Install**.

Step 7   Click **Finish** to exit the wizard.

The Call Studio software is installed on your computer.

CHAPTER 3

Unified CVP Postinstallation

After you install Unified CVP, perform postinstallation tasks to ensure that the all the CVP components are installed successfully. In addition, disable port blocking, address security issues, and apply licenses to the CVP components.

Note   Sometimes after installation, `clean.cvp` file may not be available at `%CVP_HOME%\bin\TAC`. This can happen sporadically but does not impact the functionality of CVP. You can always retrieve this file from the `CVP\Utilities` folder of the CVP iso.

Note
- After installation, go to `C:\Cisco\CVP\conf\orm.properties` file and check if the *orm.oamp.id* parameter has any oamp ID (for example, 495a891e-a64f-4e1b-b80d-26e0dce0e249-2098391835) assigned to it. If so, then delete the ID and restart the **WebServicesManager** service.

- Postinstallation excludes CVP components configuration. For information about CVP component configuration, see the *Configuration Guide for Cisco Unified Customer Voice Portal* available at: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html.

If CVP Server, Operation Console, and Reporting Server have not been installed to the default `C:\Cisco\CVP` path, then update the following files under `<install_path>/conf`:

- **cvpconfigdb.properties:** Update the connection URI so that it matches path of the DB directory `ConnectionUrl=jdbc:derby://localhost:1529/<install_path>/OPSConsoleServer/sql/db`

  Example:
  `ConnectionUrl=jdbc:derby://localhost:1529/C:/Cisco/CVP/OPSConsoleServer/sql/db`

- **cvpwsm.properties:** Update CVP_HOME.default.dir as `CVP_HOME.default.dir = <install_path>`

  Example: `CVP_HOME.default.dir = C:\\Cisco\\CVP`

- **sip.properties:** Update SIP.Secure.KeyStorePath as `SIP.Secure.KeyStorePath= <install_path>\\security\\.keystore`

  Example: `SIP.Secure.KeyStorePath= C:\\Cisco\\CVP\\conf\\security\\.keystore`

This chapter explains the following postinstallation tasks.

Disable Port Blocking

If you have installed Unified CVP Server components on a computer that has antivirus software configured to block ports, exclude Unified CVP processes and Tomcat executables.

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

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

It is the customer's responsibility to deploy the VXML applications after the Antivirus scans. This also applies to the custom `java/jar/class` files deployed in the shared path.

For more information on the Virus Scan guidelines, refer to the following sections of the UCCE documentation:

The Virus Protection section of UCCE Design Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.

The General Antivirus Guidelines section of the Security Guide for Cisco Unified ICM/Contact Center Enterprise at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html

Security

Depending on your choice of Unified CVP deployment, you may need to address certain security considerations. For information about security, see the *Configuration Guide for Cisco Unified Customer Voice Portal* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html.

Note If you are concerned about any vulnerability in Microsoft Visual VC++ 2005 Redistributable, then uninstall it from Control Panel. This will not impact the normal operation of the CVP Reporting Sever.

Initiate Metadata Synchronization for Unified CVP Rest API

In the 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 CVP Servers,

deployment of apps and media files by a tool other than the REST API, and 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.

Synchronize Metadata Files Using Sync-Up Tool

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

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
```

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 4: 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

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

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 23

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 23

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

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, on page 16.

> **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

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 5: 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=`

Unified CVP Component	Upgrade Path	Manual Configuration Process

		11. Open the sip.properties file and add the following entry:
		
		`# 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`
		Note: `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`

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

Unified CVP Component	Upgrade Path	Manual Configuration Process

		14. 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:
		
		`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"/>`
		
		15. Locate the connector node with the attribute SSLCertificateFile="<install_path>\security\vxml.crt" in the file: `VXMLServer\Tomcat\conf\server.xml`
		
		and add or update the following:
		
		`sslEnabledProtocols="TLSv1.2"`
		
		16. Locate the connector node with the attribute SSLCertificateFile="<install_path>\security\vxml.crt" in the file: `CallServer\Tomcat\conf\server.xml`
		
		and add or update the following:
		
		`sslEnabledProtocols="TLSv1.2"`
		
		17. Navigate to the `C:\Cisco\CVP` location, and add CauseCode property in the excluded list for Unreachable Table (for example: 47):
		
		`SIP.System.ExcludedCauseCodeFromUnreachableTable =`
		
		18. Navigate to the `C:\Cisco\CVP` location, and modify the Unreachable Timer property (default is 180 seconds; max is 180 seconds; min is 10 seconds):
		
		`SIP.DsUnreachableDestinationTableTimer = 180`

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.

Unified CVP/Call Studio Uninstallation

Uninstall Unified CVP/Call Studio From Windows Control Panel

Before you begin

• Shut down all applications and close all open files.

• Close the CVP component and related files.

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

Step 2   Click **Cisco Unified Customer Voice Portal / 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 CVP installation process. User-created media files and folders remain unchanged during 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/Call Studio Using Installation Media

Before you begin

• Shut down all applications and close all open files.

• Close CVP component and related files.

Step 1   Run the *setup.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 CVP installation process. The user created media files and folders remains unchanged during 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 6

Unified CVP Migration

If there is a change in platform of a later release of Unified CVP, migration from the existing release to the later release is required. For example, moving from Unified CVP 10.5(1) to Unified CVP 11.6(1) is considered a migration because it involves a change in operating system, platform, or architecture of the later release.

Migration can also involve moving to a new hardware or a software and moving from one database to another database. Migration of database requires converting the data into a common format that can be used as output from the old database and saved into the new database.

Note If you have enabled secure communication, see the *Unified CVP Security* chapter in *Configuration Guide for Cisco Unified Customer Voice Portal* for instructions on uploading certificate for the secure communication.

Premigration Tasks

Before you begin

- Back up the Unified CVP installation files and data onto a different computer for redundancy.

Important You cannot roll back to an earlier version of Unified CVP after you initiate migration. Back up the installation files and data before you begin the migration process.

- Uninstall Cisco Security Agent.

- (Optional) Deploy additional servers if you choose to deploy Reporting Server.

- (Optional) Standalone distributed diagnostics and service network (SDDSN) is no longer required. If you have SDDSN servers, decommission these servers or use them for another purpose.

- Deploy Operations Console. For deployment of Operations Console, see *Configuration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html.

- (Optional) Gatekeepers are not required in SIP implementations. Decommission gatekeepers or in some cases convert them to use as ingress or VXML gateways (or both) if you choose to use SIP for the implementation.

- (Optional) SIP Proxy servers and DNS servers for SIP message routing are optional components for SIP implementation. Add these components to the network if you intend to use them.

> **Note** SIP Proxy servers and DNS servers cannot co-reside with other Unified CVP product components.

- Ensure that the version of Cisco IOS supports the required hardware.

> **Note** If you are using an older gateway or gatekeeper hardware, the version of Cisco IOS that is required in this release may no longer support the required hardware. Hence, you need to purchase new hardware.

- Migrate the operating system. For more information, see the Compatibility Matrix available at https://cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

Migrate Operations Console

To migrate Operations Console, back up and restore the CVP Operations Console configuration. To know whether a change in platform is required, see the *Upgrade Path* section.

Related Topics

Upgrade Path

Back Up Operations Console Configuration

Step 1 Log in to Operations Console.

Step 2 On the Operations Console page, click **System** > **Export System Configuration** > **Export**.

Step 3 Manually copy the sip.properties file.

CVP Operations Console cannot export the sip.properties file.

For more information on Unified CVP Console Configuration, see *Administration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html.

Step 4   Save the `CVP-OpsConsole-Backup.zip` file.

What to do next

- Save the exported configuration and custom files on network storage media or a portable storage media.

- Ensure that you are able to access the shared storage media from the Windows Server Machine.

Restore Operations Console Configuration

Before you begin

- For latest operating system, 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.

- Export the Operations Console configuration from the older version to migrate it to the new version.

Step 1   Stop Cisco CVP WebServicesManager service.

   a) Click **Start** > **All Programs** > **Administrative Tools** > **Services**.

   b) In the list of services names, select Cisco CVP WebServicesManager and click **Stop**.

Step 2   Import the saved Operations Console configuration.

   a) On the Operations Console page, click **System** > **Import System Configuration**.

   b) Click **Browse** and select the filename from the location where you saved the Operations Console configuration files of the previous version.

   c) Click **Import**.

   d) Copy the custom files, license files, and sip.properties files from the location where you saved the Operations Console configuration to their corresponding Unified CVP directories to complete the restore operation.

> **Note**   If you have not restored the backup containing the user-related information from the earlier version of Unified CVP, then skip to Step 5.

Step 3   In the Operations Console page, click **Device management** > **Reporting Server** > **Database Administration**.

Step 4   Delete the Reporting Users that are created in the earlier version of Unified CVP.

> **Note**   Creating the new users that are the same as the existing users does not work.

Step 5   Set the same password for the existing user that you imported from the earlier versions of CVP Operations Console.

   a) Click **Server Manager** > **Configuration** > **Local Users and Groups** > **Users**.

   b) Right-click the existing username and click **Set Password**.

   c) On the **Set Password** screen, click **Proceed**.

   d) Type the old password and confirm the new password.

   e) Click **OK**.

Step 6 Restart Cisco Unified CVP Operations Console and Cisco CVP WebServicesManager.

    a) Click **Start** > **All Programs** > **Administrative Tools** > **Services**.

    b) Select Cisco CVP Operations Console Server.

    c) Click **Restart**.

       The CVP Operations Console Server service starts in the Services window.

    d) Select Cisco CVP WebServicesManager.

    e) Click **Restart**.

       The Cisco CVP WebServicesManager starts in the Services window.

All the existing CVP Operations Console data including the CVP Operations Console login credentials get overwritten by the new data that is imported from the saved CVP Operations Console configuration.

Secure Communication with Operations Console

To secure communication between Operations Console and CVP components, on the Operations Console page, click **Enable Secured Communication with the Operations Console**.

For configuring the security certificate exchange between Operations Console and CVP components, see the *Configuration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/ unified-customer-voice-portal/tsd-products-support-series-home.html.

Migrate Unified CVP Call Server

Before you begin

- Back up existing Unified CVP installation onto a different computer for redundancy.

- If you are migrating your operating system, assign the IP address and hostname of the previous Unified CVP to the later release.

- Install the latest Unified CVP server component.

Step 1 Log in to Operations Console and select **Device Management** > **Unified CVP Call Server**.

Step 2 Select the Unified CVP Call server with the chosen IP address and the hostname.

Step 3 Click **Edit**.

Step 4 Click **Save and Deploy** to deploy the configuration to Unified CVP Call Server.

Step 5 Click **System** > **SIP Server Groups**.

On the SIP Server Groups screen, verify that the data is populated from the previous OAMP configuration importing step.

Step 6   Click **Save and Deploy** and confirm that the operation has completed successfully.

Step 7   Select **System** > **Dialed Number Pattern**.

In the **Dialed Number Pattern** screen, verify that the data is populated from the previous OAMP configuration importing step.

Step 8   Click **Deploy**.

Step 9   Select **Device Management** > **Media Server**.

Step 10   From the **Default Media Server** drop-down list, choose the appropriate media server.

Step 11   Click **Set**.

Step 12   Click **Deploy**.

Step 13   From the Media Server that is installed on the computer, select **Internet Information Services** > **Sites**.

- To add a new group to the list, click **Add** and select **Everyone**.
- To give full control to group **Everyone**, check the **Full Control** check box.

Step 14   From the FTP site, click **Restart** to restart the FTP server.

> **Note**   If you want to configure Unified CVP Call Server as Media Server and use the agent greeting recording, then you must enable FTP on the Media Server. If Microsoft FTP Service is not enabled in Windows Services Control Panel, then set it to Automatic and start the service.

Migrate Unified CVP VXML Server

Before you begin

- Ensure that the Unified CVP VXML Server and Unified Call Studio are of the same version so that Unified Call Studio can work with the Unified CVP VXML Server.

- Ensure that you have licenses for all Unified CVP components.

> **Note**   If you do not apply licenses to the migrated components, the software runs in evaluation mode.

- Back up any custom audio files from `%CATALINA_HOME%/webapps/CVP/audio`.

- Back up third-party libraries, such as .class or .jar files, at:

```
%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
```

where APP_NAME is the name of deployed voice application.

- Install Unified CVP Server. See Install Unified CVP Server, on page 10.

Step 1   Log in to Operations Console and select **Device Management** > **Unified CVP VXML Server**.

Step 2   Select the Unified CVP VXML Server with the chosen IP address and the hostname.

Step 3   Click **Edit** and select the Unified CVP VXML Server configuration for editing.

Step 4   Click **Save and Deploy** to deploy the configuration to the new Unified CVP VXML Server.

Step 5   (Optional) If you need a secure connection between the Operations Console and Unified CVP VXML Server, configure SSL certificates.

Step 6   Upload the license file to the new Unified CVP VXML Server using Operations Console.

Step 7   Restore the audio files to the `%CATALINA_HOME%\webapps\CVP\audio folder`.

Step 8   Restart Cisco CVP VXML Server and VXMLServer service.

What to do next

To configure the Unified CVP VXML Server using Operations Console, see *Configuration Guide for Cisco Unified Customer Voice Portal*.

Migrate Unified Call Studio

Before you begin

- Back up all audio files.

> **Note**   Audio files are deployed to `%CATALINA_HOME%\webapps\CVP\audio` are deleted. %CATALINA_HOME% implies the Tomcat installation directory.

- Launch the Call Studio application.

- Ensure that you have licenses for all Unified CVP components.

> **Note**   If you do not apply licenses to migrated components, then the software runs in the evaluation mode.

- In the **Navigator** view, right-click the project, and click **Export**.

> **Note**   Export Unified Call Studio projects to offline media, if they are not stored in version-control systems. You can export multiple projects simultaneously by unchecking them from the list that Export wizard displays.

Step 1   Select the **Existing Cisco Unified CVP Project into Workspace** option to import the projects.

The import process upgrades the projects to the format of the new release, if necessary.

Note If you check out applications from a source repository rather than importing from the file system, you can still import the applications to Call Studio project to start the conversion process. In addition, for the first check-in after importing, all files in each project are considered modified and you need to update them in the repository.

Step 2 Recompile any custom components that were compiled in the earlier versions of Java.

Review the list of Java changes that may affect backward compatibility and make any required updates. You can locate the compatibility page at http://www.oracle.com/technetwork/java/javase/downloads/index.html.

Step 3 Deploy all projects, including the newly recompiled components from the previous step, to the appropriate Cisco Unified CVP VXML Servers.

Use Operations Console for bulk transfer of the project to multiple Unified CVP VXML Servers in one step.

Migrate Unified CVP Reporting Server

Before you begin

Retain the call data during migration by unloading the existing databases of Unified CVP.

Step 1 Unload data from Reporting Server Database.

Step 2 Uninstall Reporting Server.

Step 3 Upgrade Microsoft Windows Server.

Step 4 Install Reporting Server.

Step 5 Load data to Reporting Server Database.

Step 6 Configure Unified CVP Reporting Server in Operations Console.

Related Topics

Prepare Unified CVP Reporting Server

Step 1 Install Unified CVP Reporting Server on Windows Server.

Note Ensure that the Unified CVP Reporting database is active.

Start the Informix IDS - CVP service in Windows Service Manager.

Step 2 From the command prompt, run **dbaccess**, and then select a database.

Step 3 Select the following databases and press **Return**.

- callback

- ciscoadmin

- cvp_data

Unload Data from Reporting Server Database

Step 1   Log in as cvp_dbadmin user to Unified CVP.

Step 2   Stop **Cisco CVP Call Server** service from Windows Service Manager.

Note   Ensure that enough disk space is available to unload data. To check the disk space (in MB), run the query:

```
select sum(tabsize(tabname)) from systables where tabid>99
```

-OR- go to **OAMP** > **Unified CVP Reporting Server** > **Database Administration** > **Database details.**

Step 3   Access the Unified CVP installation file.

Step 4   From the command prompt, change the directory to the migration folder.

Note   You can also copy the migration folder to the local disk and run the unload script directly.

Step 5   Locate the `migrate_unload.bat` file.

Step 6   By default, the data is exported to `c:\migration`. Ensure that this path exists. If you want to change the default path, then update the path in *unl.sql*:

```
create procedure unld(path char(128) default "c:\migration\") RETURNING char(128)
```

Step 7   Run the following command to unload the Reporting Server database:

```
migrate_unload.bat
```

After running the script, a set of .unl files is created under the path provided. The .unl files are exported to `c:\migration`. This folder must have full access permission for cvp_dbadmin user.

Step 8   Copy the exported migration folder to the Unified CVP database Reporting Server.

Note   Reduce the retention period for data and execute a purge to reduce the data to migrate.

Step 9   Start **Cisco CVP Call Server** service from Windows Service Manager.

Load Data to Reporting Server Database

Step 1   Open the Unified CVP installation file.

Step 2   Stop **Cisco CVP Call Server** service from Windows Service Manager.

Step 3   Go to **CVP** > **Migration**.

Step 4 Copy the migration folder to the local disk and run the load script directly. From the command prompt, change the directory to the migration folder.

Step 5 On the local disk, locate the .unl files that you want to load into the Unified CVP database and copy them into the migration folder.

Step 6 Run the following command as an administrator to load the Unified CVP database: `migrate_load.bat`

> **Note** If the .unl files are located in `c:\migration`, you must run the script load as `migrate_load.bat`.

This script loads all the three Unified CVP Reporting databases with the previous call data to the Unified CVP Reporting database.

> **Note** The load runs at a rate of about 1.5GB/hour.

Step 7 Start **Cisco CVP Call Server** service from Windows Service Manager.

Configure Reporting Server in Operations Console

Step 1 Import the Operations Console configuration and redeploy the Unified CVP Reporting Server to retain the same IP address as that of Unified CVP.

Step 2 If the IP address of the server is changed, then delete the previous instance of the server and add the new Unified CVP Reporting Server to Operations Console, and then deploy the server.

Upgrade VM Network Adapter from E1000 to VMXNet 3

Before you upgrade the operating system of the virtual machine from Windows Server 2008 R2 SP1, upgrade the VM network adapters to VMXNet3. Unified CVP 11.6(1) requires VMXNet3 network adapters. If you upgrade the operating system to Windows Server 2012 R2 Standard Edition without upgrading to VMXNet3, the static IP configuration on the ethernet adapter resets to automatic after the Windows upgrade.

Step 1 Record the network settings, including the IP addresses, dubnet masks, default gateway, DNS, persistent static routes, and MAC address of the network adapter.

> **Important** You need these values to re-create the configurations on the new virtual machine network adapter. For more information, see .

Step 2 Stop the Unified CVP Server. The CVP Server cannot be active during reconfiguration of the network adapter.

Step 3 Add the VMXNet 3 network adapter:
  a) Select **Edit Settings** from the VM context menu.
  b) Click **Add** on the **Hardware** tab.
  c) Select **Ethernet Adapter** in the **Device Type** page and click **Next**.
  d) Select **VMXNet 3** from the **Adapter Type** drop-down list and click **Next**.
  e) Select the network port group from the **Network label** drop-down list and click **Finish**.

Step 4   Apply the network settings that you recorded in Step 1 from the E1000 network adapter to the VMXNet 3 network adapter.

Step 5   Enable the VMXNet 3 network adapter.

Step 6   Remove the E1000 network adapter:

    a)   Select **Edit Settings** from the VM context menu.

    b)   Select the **E1000 network adapter** on the **Hardware** tab.

    c)   Click **Remove** and then click **Finish**.

Step 7   Remove the E1000 network adapter from VMs for CallServer/VXMLServer, Operations Console and Reporting Servers:

    a)   Select **Edit Settings** from the VM context menu.

    b)   Select the **E1000 network adapter** on the **Hardware** tab.

    c)   Click **Remove** and then click **Finish**.

Step 8   Use **traceroute** to test the network connectivity.

Step 9   Re-enable the Unified CVP services.

Related Topics

Save MAC Address of Virtual Machine Network Adapter

Complete the following procedure to preserve the MAC address of the virtual machine network adapter.

Step 1   Right-click the Unified CVP virtual machine and click **Edit Settings**.

Step 2   On the **Hardware** tab, select the Network adapter used by the virtual machine to connect to the network.

Step 3   Record the value that is in the MAC address field.

Step 4   Save the MAC address.

Step 5   From the **Hardware Settings** tab, click **Add Hardware**.

Step 6   From the **Adapter Type** drop-down list, change the adapter type to **VMXNET3**.

Step 7   Under the **MAC Address** field, select **Manual**.

Step 8   In the **MAC Address** field, enter the MAC address you recorded.

Step 9   Click **OK**.

Step 10   Restart the virtual machine.

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

Unified CVP Redeployment

You can redeploy an existing Unified CVP component from Operations Console.

Redeploy Operations Console

Related Topics

Redeploy Unified CVP Server

Related Topics

Redeploy Unified CVP Reporting Server

Step 1 Reinstall the Unified CVP Reporting Server.

Step 2 Save and deploy the Unified CVP Reporting Server in Operations Console.

Step 3 Update the Unified CVP Reporting Server license.

Step 4 Restart the Unified CVP Reporting Server.

Step 5 Redeploy courtesy callback system-level configuration, if applicable.

Step 6 Redeploy SNMP configuration, if applicable.

Redeploy Unified Call Studio

See the Migrate Unified Call Studio section.

Related Topics

Unified CVP Licensing

License Plan

Unified CVP licenses consist of Unified CVP Server licenses, Unified CVP Port licenses, Unified CVP Call Director licenses, and Redundant Port licenses. Each Unified CVP component license is tied to its IP address.

Order licenses for each server, such as Unified CVP server, VoiceXML server, or redundant server. These servers host the Unified CVP software, with the exception of Unified CVP Reporting Server and Operations Console Server.

Table 6: Unified CVP Components and the Required License

CVP Component	Required License
Unified CVP Call Server/VXML Server	• Self Service Ports • 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 • Standard (Dual Processor) • Premium (Quad Processor)	No License is required for the CVP Reporting Server.
Unified CVP OAMP Server	No License is required for the CVP OAMP Server.

Unified CVP supports FlexLM licensing for Call Server, Reporting Server, VXML Server, and Call Studio. The supported license features of Unified CVP are listed in the following table.

Table 7: Unified CVP Supported License Features

Supported License Feature	Description
CVP_SOFTWARE	The basic feature license that is required for Unified CVP.
CVPPorts and SelfServicePorts	The licenses for the ports on the Unified CVP Call Server and the Unified CVP VXML Server. The Unified CVP Call Server license is for the number of SIP sessions on the Call Server. A single Unified CVP Call Server license supports up to 3000 sessions. A Unified CVP VXML Server license is for the number of self-service ports plus queued sessions.
RPT	The license for the Unified CVP Reporting Server.

Note

- Unified CVP licenses for all Unified CVP components are aggregated in the `cvp.license` file, which is located at `%CVP_HOME%\conf\license`. When you deploy a license through Operations Console, the license is appended to the `cvp.license` file. If there are multiple valid Unified CVP component licenses within the license file, the port licenses are additive. For example, if a Unified CVP license file has 200 VXML ports and you apply a license for an additional 100 VXML ports, then the VXML server adds licenses for both the ports, creating 300 licensed ports.

- If the Unified CVP Reporting Server is not licensed, it begins counting messages when you turn it on. When a message is written to the database, Unified CVP Reporting Server checks the local date. After the database writes reach 10000 in a day, an alarm is sent and messages are no longer written to the database. The number 10000 comprises the sum of both inserts and updates that can be written to the database. After a change in the local date, database writes and count resume.

- Unified CVP Call Servers and Unified CVP Reporting Servers do not support additive licenses.

- Unified CVP no longer reports the license usage. Instead, it reports the port usage based on the maximum number of ports available in the `cvp.license` file. This change affects all reports, the Operations Console Statistics page, and the diagnostic portal license information requests. Alerts are issued at the 90%, 94%, and 97% thresholds of licensing usage as with previous releases.

- To update or transfer new license file(s) before the temporary license expires, you must first delete the existing license file (cvp.license) present in %CVP_HOME%\conf\license. Apply the relevant valid licenses through OAMP, and restart the affected services.

For information on Transfer License Files Using Bulk Administration File Transfer(BAFT), see *Administration 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.

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.

Both the primary and the redundant Unified CVP servers use the Unified CVP Server software licenses and the Unified CVP Port licenses. The failover server ensures that there is no loss of service in case of a failure of one or more primary servers. Before you purchase CVP Primary and Redundant Port licenses you must appropriately size and design the port distribution based on the supported redundancy models.

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 orders made after September 22, 2014, each Unified CVP port is bundled with one redundant port license. Existing customers can order additional redundant port licenses to make the count equal to the number of primary port licenses. Customers must also order a server license for each additional redundant server.

Unified CVP Reporting Server License

The Unified CVP Reporting Server license provides the reporting repository for Unified CVP data. The license includes a relational database that uses Crystal reports to query data and examples to build reports. The license includes only the reporting repository and does not include the presentation server. The Reporting Server license includes the IBM Informix license. Previously, two versions of options of CVP Reporting Server were available: the standard version and premium version. The standard version supports a dual-processor server with a smaller database for basic reporting. The premium version supports a larger database on a four-way processor.

Note Sale of the standard reporting server was discontinued as of September 22, 2014, but existing standard reporting servers will be supported until their End-of-Life (EOL).

Evaluation License

Unified CVP installation comes bundled with an evaluation license. This license supports 30 ports on all Call Servers and 10,000 Reporting Server database writes and updates and is active for 30 days. After the evaluation license expires, the server logs a message to the application server console and startup log to indicate that you need to activate the license. Purchase a license for each component during or after the evaluation period for continued functionality.

Note • A license is considered inactive if it is missing, invalid, or expired.

• The Call Server and VXML Server evaluation licenses support 3000 ports. The licenses are useful for simple testing or evaluation purposes. Although the evaluation license expires 30 days after installation, a production server must always have a license applied to support the desired number of concurrent sessions.

• An expired license needs to be deleted before updating or transferring the new license file.

Generate a License

Before you begin

Access the product authorization key (PAK) that you received with the Unified CVP software.

⚠️

Attention This procedure only applies when you are performing a fresh install of Packaged CCE. If you are upgrading from Unified CVP Release 11.x to 12.0, use the Unified CVP 11.0 license.

Step 1 Sign in to the Product License Registration Portal at https://tools.cisco.com/SWIFT/LicensingUI/Home.

Step 2 Click **Continue to Product License Registration**.

Step 3 In the **Get New Licenses** field, enter your PAK.

You can enter up to 10 PAKs, separated by commas.

Step 4 Click **Fulfill**.

Step 5 Select your features and enter the quantity.

Step 6 In the **Serial Number** field, enter the following:

• For a Unified CVP Server or Unified CVP Reporting Server, enter the IP address.

Step 7 Click **Next**.

Step 8 Accept the terms of the License Agreement, enter your Recipient Information, and click **Submit**.

Your request is processed.

Step 9 Click **Download** to download your license.
Your license is also sent to you by email.

What to do next

Ensure that the license file is named as `cvp.license`.

Copy the license file to `C:\Cisco\CVP\conf\license`. Shut down gracefully and then restart each of the Call Server components for the new license to take effect.

Apply and Upgrade Call Server/VXML Server/Reporting Server License

Step 1 From the **Device Management** menu, select a Unified CVP component.

The **Find, Add, Delete, Edit** window lists the Unified CVP components that are added to the network map.

Step 2   Click the Unified CVP component link, and then click **Edit**.

Step 3   From the toolbar, click **File Transfer** > **Licenses**.

     The **File Transfer** page appears listing the host name and IP address for the selected Unified CVP component.

Step 4   From **Select From Available License Files**, select the license file, and then click **Select**.

     Note   If the license file is not listed in the **Select From Available License Files** text box, click **Select a License File from Your Local PC** and enter the filename in the text box. Alternatively, click **Browse** to search the license file on the local file system.

Step 5   To transfer the license file to the selected Unified CVP component, click **Transfer**.

Step 6   Select and restart the Unified CVP component through the Operations Console.

     For more information, see *Operations Console Online Help for Cisco Unified Customer Voice Portal.*

What to do next

- Verify that VXML Server is operational and that the license is applied by running the `status.bat` or `status` administrative script. Run this script at `%CVP_HOME%\VXMLServer\admin` and review the output.

- On the Operations Console, verify that Reporting Server is operational. For more details, see *Operations Console Online Help for Cisco Unified Customer Voice Portal*.

- For upgrade information, see *Solutions Ordering Guide*.

- For more information about Unified CVP licensing, see *Configuration Guide for Cisco Unified Customer Voice Portal* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html.

Microapps Licensing

Beginning with Release 11.5(1), the IVR service that was part of the Call Server is now part of the VXML Server. The Voice Browser sends a request to the VXML Server to service its requests. Whenever the VXML Server receives a request from Voice Browser, it consumes one license. Microapps, during the execution on VXML Server, consumes an IVR port.

I N D E X