# Installation and Upgrade Guide for Cisco Virtualized Voice Browser, Release 12.6(2)

**First Published:** 2023-04-28

**Last Modified:** 2023-08-24

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

# CONTENTS

PREFACE

CHAPTER 1

CHAPTER 2

# Preface

## Change History

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

| Change | See | Date |
|---|---|---|
| Added note that before upgrading from 12.5(1) ES-02 to be applied. | Cisco VVB Upgrade | May 2023 |
| **Initial Release of Document for Release 12.6(2)** | | April 2023 |
| Added task list for upgrading from Cisco VVB, Release 12.6(1) to Cisco VVB, Release 12.6(2) | Cisco VVB Upgrade | |

## About This Guide

This document explains how to install Cisco Virtualized Voice Browser (Cisco VVB) in a Contact Center deployment. Review all the installation instructions carefully before you install Cisco VVB.

## Audience

This guide is intended for administrators who install and upgrade Cisco VVB.

# Related Documents

Cisco VVB provides the following documentation:

- *Solution Design Guide for Cisco Unified Customer Voice Portal*
- *Configuration Guide for Cisco Unified Customer Voice Portal*
- *Solution Port Utilization Guide for Cisco Virtualized Voice Browser*
- *Operations Guide for Cisco Virtualized Voice Browser*
- *Developer Guide for Cisco Virtualized Voice Browser*

# Communications, Services, and Additional Information

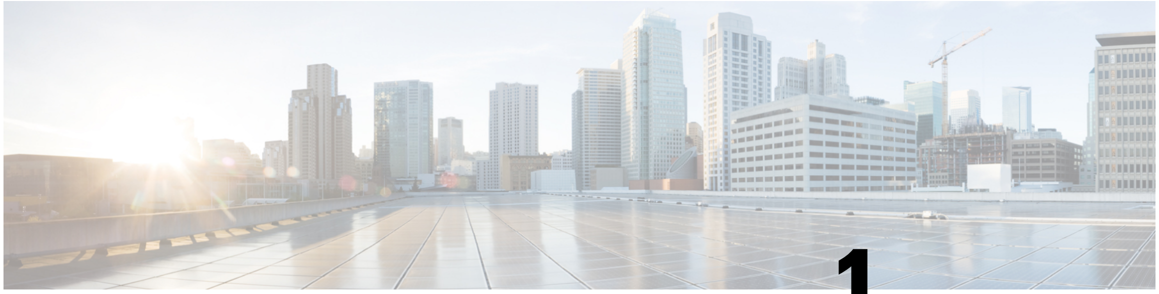
- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class 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

To provide comments about this document, send an email to contactcenterproducts_docfeedback@cisco.com



CHAPTER 1

# Cisco VVB Installation

**Note** Cisco VVB does not support clustering. Therefore, you may ignore any message on the Cisco VVB Admin UI/CLI that refers to **cluster**, **publisher**, **subscriber**, etc.

## System Requirements

**Note** Cisco Virtualized Voice Browser (Cisco VVB) supports installation on virtualized servers. For more information on system requirements and Open Virtualization Archive (OVA), see the *Virtualization for Cisco Virtualized Voice Browser* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-virtualized-voice-browser.html.

### Supported Browsers

See *Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

# Create a Virtual Machine from the OVA

**Step 1** Select the host in the vSphere client.

**Step 2** Choose **File** > **Deploy OVF Template**.

**Step 3** Browse to the location on your local drive where you stored the OVA.

**Note** For Cisco VVB OVA, an End User License Agreement displays. Click **Agree** and then click **Next**.

**Step 4** On the **Select a name and folder** page, enter a name for the virtual machine and then choose the location for the virtual machine.

The name can contain up to 32 characters. Invalid characters are space and special characters.

**Step 5** Click **Next**.

**Step 6** On the **Select a compute resource** page, select the destination compute resource. Click **Next.**

**Step 7** On the **Review details** page, verify the OVF template details.

**Step 8** On the **Configuration** page, select the applicable configuration from the available list. Click **Next**.

**Step 9** On the **Select storage** page, ensure that the virtual disk format is **Thick provision Lazy Zeroed** and then choose a datastore on which you want to deploy the new virtual machine. Click **Next.**

**Step 10** On the Network Mapping page, select the appropriate network from the **Destination** drop-down list.

**Step 11** On the **Ready to complete** page, click **Finish** to create the VM.

**Note** Do not make any changes to the VM configurations once the VMs are created.

# Configure DNS Server

This procedure is for Windows DNS server.

**Note** If the deployment uses host files in addition to DNS, use FQDNs in the host file. Live Data requires FQDNs in order to work properly.

**Note** If the deployment uses host files in addition to DNS, use FQDNs in the host file. Live Data and single sign-on (SSO) require FQDNs in order to work properly.

# Mount ISO Files

**Upload ISO image to data store:**

1. Select the host in the vSphere client and click **Configuration**. Then click **Storage** in the left panel.
2. Select the datastore that will hold the ISO file.
3. Right click and select **Browse datastore**.
4. Click the **Upload** icon and select **Upload file**.
5. Browse to the location on your local drive where you saved the ISO file, and upload the ISO to the datastore.

**Mount the ISO image:**

1. Right-click the VM in the vSphere client and select **Edit virtual machine settings**.
2. Click **Hardware** and select **CD|DVD Drive 1**.
3. Check **Connect at power on** (Device status panel upper right).
4. Click the **Datastore ISO File** radio button and then click **Browse**.
5. Navigate to the data store where you uploaded the file.
6. Select the ISO file and click **OK**.

# Install Cisco VVB

### Before you begin

Perform the following tasks before installation:

- Ensure the Network Time Protocol (NTP) and DNS servers are running (mandatory for VMware deployments).
- Download the Cisco VVB ISO image and OVA template.
- Deploy virtual machine using the OVA template.
- For Virtual Agent Voice (VAV) feature, ensure that Cloud Connect is installed and registered with VVB and InService. For more information on Cloud Connect, see the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide.

**Step 1** Mount the ISO image on the virtual machine.

**Step 2** The installer checks the integrity of the ISO image before beginning the installation. Click **Yes** to perform a media check.

- If the media integrity check fails, the ISO might be corrupted. Download another ISO image and reinstall.
- If the media integrity check is successful, click **OK** to proceed with the installation.

**Step 3** Follow the instructions on the screen to complete the installation. Enter the basic configuration information as described in Server Configuration Information for Installation, on page 4.

**Important**

- When the **Apply Patch** window appears, click **No** to begin the basic installation. Installation may take 2-3 hours to complete.
- When installation is in progress, the window becomes blank but the **Ctrl+Alt+Delete** option is enabled. In such a scenario, do not press **Ctrl+Alt+Delete** because this stops the installation and reboots the system.

## Server Configuration Information for Installation

**Note**

- You can use the configuration table for saving your entries either on a printed paper or online.
- Ensure the hostname and passwords that you enter while running the installation program are case-sensitive.
- Per security guidelines, limit the validity of the generated or the requested SSL certificates to 2-3 years or shorter.
- While establishing TLS connection, a hostname verifier parameter is used (`strict_hostname_verifier`), which can be set using CLI command. The default value of `strict_hostname_verifier` is **true**. If you are upgrading, it is enabled by default.

***Table 1: Configuration Table***

| Parameter | Your Entry |
|---|---|
| **Time Zone** | |
| **NIC Duplex**<br>**Note** This parameter is not displayed if automatic negotiation is used. | |
| **NIC Speed**<br>**Note** This parameter is not displayed if automatic negotiation is used. | |
| **MTU Size**<br>**Note** Maximum Transmission Unit (MTU) value of the server. | |
| **Hostname**<br>**Tip** Ensure that the hostname is assigned on the DNS server. The hostname must contain only alphanumeric characters or hyphen. It cannot be "localhost" or an IP address. | |

| Parameter | Your Entry |
|---|---|
| **IP Address** | |
| **IP Mask** | |
| **Gateway Address** | |
| **[Optional] Primary DNS** | |
| **[Optional] Secondary DNS** (optional) | |
| **[Optional] Domain** | |
| **Administrator ID**<br>**Note** You *cannot* change the original administrator account user ID.<br>**Caution** Do not create administrator IDs (for CLI access or Operating System administration) that start with “vvb” or “VVB” because such IDs conflict with system account names that are used internally within the Cisco Virtualized Voice Browser server. | |
| **Administrator Password**<br>**Note** This field specifies the password for the administrator account, which you can use for secure shell access to the CLI and for logging into Cisco Unified Communications Operating System Administration. Ensure that the password is at least six characters long; it can contain alphanumeric characters, hyphens, and underscores.<br>You can change the password after installation. | |
| **Unit**<br>**Note** The value you enter is used to generate a Certificate Signing Request. | |
| **Location** | |
| **State**<br>**Note** The value you enter is used to generate a Certificate Signing Request. | |
| **Country**<br>**Note** The value that you enter is used to generate a Certificate Signing Request and self-signed certificates. | |

| Parameter | Your Entry |
|---|---|
| **NTP Server**<br>**Note** Enter the hostname or IP address of one or more Network Time Protocol (NTP) servers with which you want to synchronize.<br>You can enter up to 5 NTP servers.<br>You can change the NTP server after installation. | |
| **Security Password**<br>**Note** This password is used to reset your application password. The password must contain at least six alphanumeric characters. It can contain hyphens and underscores, but it must start with an alphanumeric character.<br>You can change the password after installation by using the following CLI command:<br>**set password user security** | |
| **SMTP Location**<br>**Note** You must populate this field if you plan to use e-mail notification. | |
| **Application User Name**<br>**Note** Use the Application User Name to log in to the Administration Web Portal. | |
| **Application User Password**<br>**Note** Use the Application User password as the default password for the application. Ensure that the password is at least six characters long; it can contain alphanumeric characters, hyphens, and underscores.<br>You can change the password after installation. | |

**Note** If you are testing with the self-signed TLS certificates that are generated as a part of the installation, ensure that you map the CN/SANs on the certificate to the corresponding IP through DNS or hosts file entries.

# Post Installation

**Note** Use single instance of Web browser to complete the post-installation steps.

**Step 1** After the initial installation, open the VVB user interface on a web browser and log in as the configured administrator.

**Step 2** Wait for all the components to be activated, and then click **Next**.

**Step 3** Configure system parameters, and then click **Next**.
You can view the status of the VVB setup.

**Step 4** Close the Web browser and log in again to use VVB.

# Unattended Installation

Unattended installation performs installation silently using a configuration file that includes all the input parameters. Use Cisco Unified Communications Answer File Generator to generate answer files for unattended installations of Cisco VVB.

The Answer File Generator supports the following features:

- Allows simultaneous generation and saving of answer files for unattended installation.
- Provides syntactical validation of data entries.
- Provides online help and documentation.

**Step 1** Go to https://www.cisco.com/web/cuc_afg/index.html (Cisco Unified Communications Answer File Generator web page).

**Step 2** Select the following options:

a) **Primary Node Installed On** as **Virtual Machine**
b) **Product** as **Cisco Virtualized Voice Browser**
c) **Version** as **12.6.2**

**Step 3** Enter the remaining information on Answer File Generator web page and click to generate a configuration file.

a) Click the **Proceed to Download Answer Files** button to download the file.
b) Follow the Download Instructions on the page and click the **Download File** button.

**Step 4** Save the `platformConfig.xml` file on your local system.

## Perform Unattended Installation Using Answer File

**Step 1** Create a floppy drive image adding the Answer file.

**Step 2** Mount the floppy drive image in VM under the **Floppy Drive 1**.

**Step 3** Select the **Connect at power-on** option in Floppy Drive 1.

**Step 4** After you start the VM, the Cisco VVB ISO boots the system and runs `platformConfig.xml` automatically.

# Access Cisco VVB Administration Web Interface

The web pages of the Cisco VVB Administration web interface allow you to configure and manage the Cisco VVB system and its subsystems.

Use the following procedure to navigate to the server and log in to Cisco VVB Administration web interface.

**Step 1** Open the Cisco VVB Administration Authentication page from a web browser on any computer on your network and enter the case-sensitive URL in the following format:

```
https://<servername>/appadmin/main
```

Replace <*servername*> with the hostname or IP address of the required Cisco VVB server.

A Security Alert dialog box is displayed.

**Note** Ensure to enter the complete URL to access the VVB Appadmin page.

**Step 2** On the Cisco Virtualized Voice Browser Administration web page, enter your Cisco VVB username and password.

**Note** If you are accessing Cisco VVB for the first time, enter the Application User credentials that you specified during installation of the Cisco VVB.

**Step 3** Click **Login**.

# Access Cisco VVB Serviceability Web Page

Cisco VVB Serviceability is used to view alarm and trace definitions for Cisco VVB services (start, stop, and monitor Cisco VVB Engine activity) and to activate and deactivate services.

**Step 1** Log in to **Cisco Virtualized Voice Browser Administration** web page.

**Step 2** From the Navigation drop-down list, select **Cisco VVB Serviceability** and click **GO**.
**Cisco VVB Serviceability** web page is displayed.

CHAPTER 2

# Cisco VVB Upgrade

## Cisco VVB Upgrade Types

### Before You Begin

- Ensure that there are no hostname/IP address entries beyond the system entries. If you do, then back up these hostname/IP address entries by running **show vvb host-to-ip** command. You can delete the hostname/IP address by running **utils vvb delete host-to-ip** command.

**Note** Add the hostname/IP address entries after upgrade and switch version are successful by running **utils vvb add host-to-ip** command.

- Check the VVB OVA HDD profile using the CLI command: **show hardware**
- Ensure that you change the CPU resource allocation as mentioned in the *Virtualization for Cisco Virtualized Voice Browser* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-virtualized-voice-browser.html.

Upgrade files are available as ISO images.

**Important** From Release 11.6, VVB is available in two release ISO types: the VVB export restricted software image and the VVB export unrestricted software image. The export unrestricted image does not support SRTP voice media. An upgrade from one release ISO type to the other is not possible.

You can upgrade Cisco VVB from:

- Cisco OS Administration web interface
- Command Line Interface (CLI)

You can apply the ISO images from:

- Local DVD
- FTP/SFTP server

For information about supported upgrades, see *Compatibility Matrix for Cisco VVB* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

**Note** Local DVD option is not available for upgrading Cisco VVB on KVM.

To apply ES, follow the same procedure as Cisco VVB upgrade.

Before upgrading from 12.5(1)_SU to 12.6(2), ES-02 must be applied. For ES-02 information, see Virtualized Voice Browser Engineering Specials for Release 12.5(1)_SU.

| Upgrade Path | Procedure | Description |
|---|---|---|
| 12.5(1) to 12.6(2) | Before upgrading from 12.5(1) to 12.6(2), the release key cop file ucos.keymanagement.v01.cop.sgnmust be applied | There is service interruption during the upgrade and subsequent server restart. |
| 12.6(1) to 12.6(2) | Before upgrading from 12.6(1) to 12.6(2), the release key cop file `ucos.keymanagement.v02.cop.sgn`. must be applied | There is service interruption during the upgrade and subsequent server restart. |

# Important Information

- You may experience a delay of approximately 30 minutes for the services to start during the first restart of the Cisco VVB system post the switch version. This is due to the application of Security policies post upgrade. This delay will not appear in subsequent restarts.
- It takes approximately 2 hours to upgrade.
- Cisco VVB versions include a feature in the VMware Installation information line to indicate whether the disk partitions are aligned. If the disk partitions are aligned, the VMware installation information line will indicate `Partitions aligned`. After upgrading, if the VMware installation information line indicates `ERROR-UNSUPPORTED: Partitions unaligned`, it means Cisco cannot provide support for performance issues.
- While establishing TLS connection, a hostname verifier parameter is used (`strict_hostname_verifier`), which can be set using CLI command. The default value of `strict_hostname_verifier` is **true**. If you are upgrading, it is enabled by default.

# Preupgrade Tasks

**Step 1** Ensure that you have the Secure File Transfer Protocol (SFTP) server product.

**Step 2** Obtain the appropriate ISO file from https://software.cisco.com/download/home.

**Step 3** Get an ISO image of the upgrade file and follow the steps:

a) Copy the ISO image on an FTP/SFTP server on which your server has access.

**Step 4** Download and install `ucos.keymanagement.cop.sgn` file from https://software.cisco.com/download/home/268439622/type/286325642/release/.

**Step 5** For Virtual Agent Voice (VAV) feature, ensure that Cloud Connect is installed and registered with VVB and InService. For more information on Cloud Connect, see the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide.

# Cisco VVB Upgrade

The following table lists the tasks to be performed in order to upgrade from Cisco VVB, Release 12.6(1) to Cisco VVB, Release 12.6(2).

| Sequence | Task |
|---|---|
| 1 | Upgrade Cisco VVB Using Web Interface, on page 11 or Upgrade Cisco VVB Using CLI, on page 12. |
| 2 | Switch Version and Verify, on page 12. |

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

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

## Upgrade Cisco VVB Using Web Interface

You can upgrade Cisco VVB either from a local DVD or from a FTP/SFTP server.

**Step 1** Log in to **Cisco OS Administration** using administrator username and password.

**Step 2** Choose **Software Upgrades** > **Install/Upgrade**.

**Step 3** Choose source as either **DVD/CD** or **Remote Filesystem** from the **Source** list.

**Step 4** Enter the path of the upgrade file in the **Directory** field. For **Remote Filesystem**, enter a forward slash (/) followed by the directory path.

**Step 5** If you chose **Remote Filesystem**, follow the instructions on the screen; otherwise, skip to **Step 6**.

**Step 6** Click **Next** to see the list of upgrades that are available.

**Step 7** Choose the appropriate upgrade file, and click **Next**.

**Step 8** Enter relevant information in the **Email Destination** and **SMTP server** fields to use the Email Notification feature.

**Step 9** Click **Next** to initiate the upgrade process.

**Note** Perform switch version in the same maintenance window to avoid additional downtime.

## Upgrade Cisco VVB Using CLI

**Step 1** Log in to Cisco Unified Communications OS Platform CLI using administrator username and password.

**Step 2** Enter the command **show version active** and check the current version.

**Step 3** Enter the command **utils system upgrade status** and check whether the node is ready for upgrade.

**Step 4** Enter the command **utils system upgrade initiate** to initiate the upgrade process.

**Step 5** Choose the source where the upgrade file is placed.

**Step 6** Follow the instructions on the screen.

Your entries are validated and the list of available files is displayed.

**Step 7** Select the ISO image you want to apply from the available list, and confirm the installation when you are prompted.

**Step 8** Enter the command **show version active** and check the upgrade version.

**Note** Perform switch version in the same maintenance window to avoid additional downtime.

# Switch Version and Verify

This procedure provides information to switch versions, verify active versions and status of services either by using the web interface or using the CLI.

**Step 1** To perform switch version, you can either use web interface or CLI.

- Follow the steps for web interface:

  **a.** Log in to **Cisco Unified OS Administration** using administrator username and password.

  **b.** Choose **Settings** > **Version** to check the versions.

  **c.** Click **Switch Versions**, and click **OK** to start the switch version process.

  **d.** Choose **Settings** > **Version** to check the active version.

**Note** The time taken for switching version depends on the size of records in the database.

- Follow the steps for CLI:

  **a.** Log in to Cisco Unified Communications OS Platform CLI using administrator username and password.

  **b.** Enter the command **show version active** to check the active version.

  **c.** Enter the command **show version inactive** to check the inactive version.

  **d.** Enter the command **utils system switch-version** to start the switch version process.

  **e.** Enter the command **show version active** to check the active version.

  **Note** The time taken for switching version depends on the size of records in the database.

**Note** If switch version is unsuccessful, you can restore the database by following these steps:

**a.** Log in to Cisco Unified Communications OS Platform CLI using administrator username and password.

**b.** Enter the command **utils vvb switch-version db-check** to check if the database is corrupt.

**c.** Enter the command **utils vvb switch-version db-recover** to restore the database.

**Step 2** To verify the active and inactive versions of Cisco VVB, you can use either the web interface or the CLI.

- Follow the steps for web interface:

  **a.** Log in to **Cisco Unified OS Administration** using administrator username and password.

  **b.** Choose **Settings** > **Version** to check the current active and inactive versions.

- Follow the steps for CLI:

  **a.** Log in to Cisco Unified Communications OS Platform CLI using administrator username and password.

  **b.** Enter the command **show version active** to check the active version.

  **c.** Enter the command **show version inactive** to check the inactive version.

**Step 3** To verify the status of services, you can use either the web interface or the CLI.

- Follow the steps for web interface:

  **a.** Log in to **Cisco VVB Serviceability** using administrator username and password.

  **b.** Choose **Tools** > **Control Center - Network Services** and verify that all the services are running.

- Follow the steps for CLI:

  **a.** Log in to Cisco Unified Communications OS Platform CLI using administrator username and password.

  **b.** Enter the command **utils service list** to verify that all the services are running.

# Postupgrade Tasks

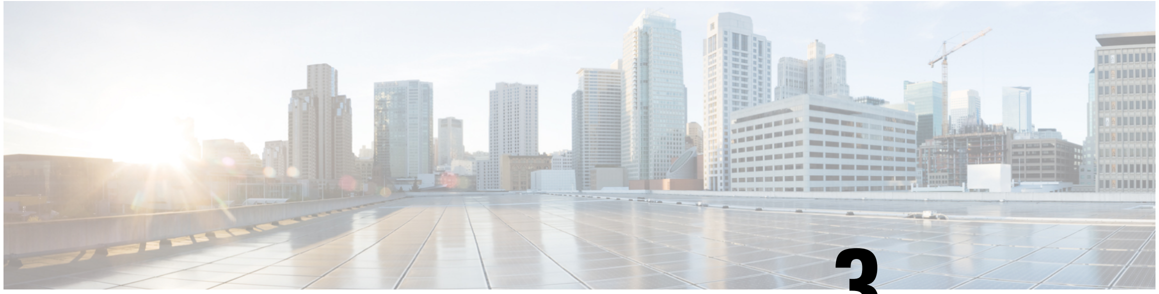
You must update the VMWare Tools after you complete and upgrade. There are options for updating the VMware Tools:

- Configure the tools to use the **Automatic Tools Upgrade** option.
- Configure the tool to automatically check the tools version during a VM power on and upgrade the tools

For more information about how to configure the options, see the VMware documentation here.

# Disaster Recovery Service

Disaster Recovery Service and CLI commands from Cisco Voice Operating System (VOS) are not supported in Cisco VVB. Ignore the warning message alert on the Cisco Unified OS Administration login page.



CHAPTER 3

# Cisco VVB Installation on KVM

## Install Cisco VVB on KVM

### Before you begin

- Download Cisco VVB OVA template from CCO. Read the OVA's readme file before you create a virtual machine using the OVA.
- For hardware requirements, see https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-virtualized-voice-browser.html.

**Step 1** Copy the OVA image from FTP/TFTP server to the router by running:

**copy ftp harddisk**

**Example:**

```
router# copy ftp harddisk:
Address or name of remote host [10.10.10.10]?
Source filename [ag2.xml]? VVB_12_x_y_ISR4K.ova
Destination filename [VVB_12_x_y_ISR4K.ova]?
Accessing ftp://10.10.10.10/VVB_12_x_y_ISR4K.ova...
Loading VVB_12_x_y_ISR4K.ova !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - -1055619072/4096 bytes]
```

**Step 2** Install the package by running:

**virtual-service install name <name> package <uri:.ova>**

**Note** The package name is case-sensitive.

**Example:**

```
router# virtual-service install name vvb package harddisk:VV
router# virtual-service install name vvb package harddisk:VVB-12-x-y-ISR4K.ova
Installing package 'harddisk:/VVB-12-x-y-ISR4K.ova' for virtual-service 'vvb'.
Once the install has finished, the VM may be activated.
Use 'show virtual-service list' for progress.
```

```
router# show virtual-service list
System busy installing virtual-service 'vvb'. The request may take several minutes...
Installation and Upgrade Guide for Cisco Virtualized Voice Browser
Virtual Service List:
Name   Status   Package Name
 ------------------------------------------------------------------------------
vvb    Installing   VVB-12-x-y-ISR4K.ova

router#show virtual-service list
Virtual Service List:


Name                    Status             Package Name
------------------------------------------------------------------------------
vvb                     Installed          VVB-12-x-y-ISR4K.ova
```

**Step 3** Configure VirtualPortGroup Interface by running:

**interface VirtualPortGroup <interface number>**

**ip unnumbered <interface type> <interface number>**

**Example:**

```
router# config t
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)# interface VirtualPortGroup1
router(config-if)# ip unnumbered GigabitEthernet0/0/0
router(config-if)# end
router# show ip int brief | sec VirtualPortGroup1
VirtualPortGroup1      10.10.10.58    YES unset  up        up
```

**Note**

- The virtual-service name is case-sensitive and must match the name given in Step 2.
- The IP address of the router/VirtualPortGroup Interface and the guest/VM must be on the same subnet.
- This VirtualPortGroup1 interface acts as the default gateway for the VM.

**Step 4** Configure the service by running:

**virtual-service <name>**

**Example:**

```
1. Get into the virtual-service config mode by running:
conf t
<enter>

2. Assign VirtualPortGroup Interface as gateway to connect to guest virtual-service/VM
router# config t
router(config)# virtual-service vvb
router(config-virt-serv)# vnic gateway VirtualPortGroup1
router(config-virt-serv-vnic)# guest ip address 10.10.10.59
router(config-virt-serv-vnic)#
router(config-virt-serv-vnic)#!!! 10.00.00.000 will be the IP of the VM!!!
router(config-virt-serv-vnic)# exit
vnic gateway VirtualPortGroup <interface number><enter>
```

**Note**

- The virtual-service name is case-sensitive and must match the name given in Step 2.
- The IP address of the router/VirtualPortGroup Interface and the guest/VM must be on the same subnet.

**Step 5** Add the static IP route for the guest VM instance by running:

**ip route <VM IP address> <subnet mask> <VirtualPortGroup Interface>**

**Example:**

```
router# config t
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)# ip route 10.10.10.10 255.255.255.0 VirtualPortGroup1
router(config)#!!!! 10.10.10.10 will be Guest/VM  IP !!!!!!!
```

**Note** This is to make sure that the assigned VirtualPortGroup interface is the gateway for only this specific IP address in the network.

**Step 6** Activate the service by running:

**activate**

**Example:**

```
router# config t
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)# virtual-service vvb
router(config-virt-serv)# activate
% Activating virtual-service 'vvb', this might take a few minutes. Use 'show virtual-service list'
for progress.
router(config-virt-serv)# end
router# show virtual-service list
System busy activating virtual-service 'vvb'. The request may take several minutes...
Virtual Service List:
Name                    Status             Package Name
------------------------------------------------------------------------------
vvb                     Activating         VVB_12_x_y_ISR4K.ova

router# show virtual-service list
Virtual Service List:
Name                    Status             Package Name
------------------------------------------------------------------------------
vvb                     Activated          VVB_12_x_y_ISR4K.ova
```

**Note** The virtual-service name is case-sensitive and must match the name given in Step 2.

**Step 7** Connect to the virtual service console by running:

**virtual-service connect name <name> console**

**Example:**

```
router# virtual-service connect name vvb console
Connected to appliance. Exit using ^c^c^c
Cisco Virtualized Voice Browser <12.x.y>
vvbkvm login:
```

```
Default credentials: administrator/C1sco123=
```

**Note** This may take 2-3 minutes to connect to the console.

**Step 8** Change the hostname and the IP address by running:

**set network hostname**

**Example:**

```
Host name Change:

Login to administrator
admin:set network hostname
ctrl-c: To quit the input.
         ***   W A R N I N G   ***
Do not close this window without first canceling the command.
This command will automatically restart system services.
The command should not be issued during normal operating
hours.
=======================================================
 Note: Please verify that the new hostname is a unique
       name across the cluster and, if DNS services are
       utilized, any DNS configuration is completed
       before proceeding.
=======================================================
Security Warning : This operation will regenerate
       all UCCX Certificates including any third party
       signed Certificates that have been uploaded.
Enter the hostname: vvbkvm
Would you like to change the network ip address at this time [yes]: yes
Warning: Do not close this window until command finishes.
ctrl-c: To quit the input.



           ***   W A R N I N G   ***
=======================================================
 Note: Please verify that the new ip address is unique
       across the cluster.
=======================================================

Enter the ip address:: 10.78.0.00
Enter the ip subnet mask:: 255.255.255.0
Enter the ip address of the gateway:: 10.78.0.1
Hostname: vvbkvm
IP Address:     10.78.0.00
Subnet Mask: 255.255.255.0
Gateway:        10.78.0.1
Do you want to continue [yes/no]? yes
calling 1 of 8 component notification script: acluster_healthcheck.sh
calling 2 of 8 component notification script: adpuccx_IP_HostName_change.sh
calling 3 of 8 component notification script: ahostname_callback.sh
Info(0): Processnode query returned using kvmvvb:
name
======
kvmvvb
updating server table from:'kvmvvb', to: 'vvbkvm'
Rows: 1
updating database, please wait 90 seconds
updating database, please wait 60 seconds
updating database, please wait 30 seconds
```

```
calling 4 of 8 component notification script: drf_notify_hostname_change.py
calling 5 of 8 component notification script: hosts_mgr.sh
calling 6 of 8 component notification script: idsLocalPrefsUpdateFile.sh
Going to trigger /usr/bin/python /usr/local/cm/lib/dblupdatefiles-plugin.py -f=vvbkvm,kvmvvb
calling 7 of 8 component notification script: regenerate_all_certs.sh
calling 8 of 8 component notification script: update_idsenv.sh
System services will restart in 1 minute
admin: utils system restart
```

**Note**

- Changing the hostname fails if the hostname includes any of these wildcard characters: “.”, “_” , “@”, “!”,”#”, “$”, “%”
- Engine takes around 5 minutes to be in service after the server comes back up.
- API and configuration services take around 10 minutes to be in service.

**Step 9** Validate Cisco VVB services.

a) Log in to VVB administrator using appadmin credentials.
b) Go to Cisco VVB serviceability.
c) Check if the services are up and running.

CHAPTER 4

# Cisco VVB Uninstallation on KVM

# Cisco VVB Uninstallation on KVM

## Uninstall Cisco VVB on KVM

**Step 1** Deactivate virtual-service from the virtual-service config mode by running:

**no activate**

**Example:**

```
router# configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#
router(config)# virtual-service vvb
router(config-virt-serv)# no activate
router(config-virt-serv)# ^Z
router# show virtual-service list
Virtual Service List:

Name                    Status             Package Name
------------------------------------------------------------------------------


vvb                Deactivating            VVB_12_5_1_ISR4K.ova
Name                    Status             Package Name
------------------------------------------------------------------------------


vvb                Deactivated             VVB_12_5_1_ISR4K.ova
```

**Note** This can take around 5-10 minutes.

**Step 2** In the privileged EXEC mode, run:

**virtual-service uninstall name <name>**

**Example:**

```
router# virtual-service uninstall name vvb
```

**Note** The virtual-service name is case-sensitive and must match the name given in Step 2 of the preceding procedure.

**Step 3** To verify the VVB instance was successfully deactivated/uninstalled, run:

a) **show log**

**Example:**

```
router# show log

------------------------------------------------------------------------------
show log
*Aug  1 08:51:48.845: %VIRT_SERVICE-5-ACTIVATION_STATE: Successfully deactivated virtual service
 vvb
*Aug  1 08:52:45.418: %VIRT_SERVICE-5-INSTALL_STATE: Successfully uninstalled virtual service vvb
```

b) **show virtual-service list**

**Example:**

```
router# show virtual-service list
Virtual Service List:
```

**Note** The output of the command must be empty.