



Cisco VVB Installation

- [System Requirements](#), on page 1
- [Create a Virtual Machine from the OVA](#), on page 1
- [Configure DNS Server](#), on page 2
- [Mount and Unmount ISO Files](#), on page 2
- [Install Cisco VVB](#), on page 3
- [Post Installation](#), on page 6
- [Unattended Installation](#), on page 7
- [Access Cisco VVB Administration Web Interface](#), on page 8
- [Access Cisco VVB Serviceability Web Page](#), on page 9

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

Before you begin

Download Cisco VVB OVA template from CCO.

Procedure

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. Click **Open** to select the file. Click **Next**.

Step 4 Click **Next** at the OVF Template Details page.

Note For Cisco Unified CVP ova, an End User License Agreement displays. Click **Agree** and then click **Next**.

Step 5 Enter the virtual machine name. Click **Next**.

Step 6 On the Deployment Configuration page, use the drop-down to select the appropriate configuration. Then click **Next**.

Step 7 Choose a datastore on which to deploy the new virtual machine. Then click **Next**.

Step 8 On the Disk Format page, keep the default virtual disk format: **Thick provisioned Lazy Zeroed format**. Click **Next**.

Step 9 At the Successfully Completed message, click **Close**.

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

Configure DNS Server



Note This is an optional configuration step.

This procedure is for Windows DNS server.

Mount and Unmount 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**.

Unmount 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. Uncheck **Connect at power on** (Device status panel, upper right).

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.

Procedure

- 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.
-

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.

Table 1: Configuration Table

Parameter	Your Entry
Time Zone	
NIC Duplex Note This parameter is not displayed if automatic negotiation is used.	
NIC Speed Note This parameter is not displayed if automatic negotiation is used.	
MTU Size Note Maximum Transmission Unit (MTU) value of the server.	
Hostname 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.	
IP Address	
IP Mask	
Gateway Address	
[Optional] Primary DNS	
[Optional] Secondary DNS (optional)	
[Optional] Domain	

Parameter	Your Entry
<p>Administrator ID</p> <p>Note You <i>cannot</i> change the original administrator account user ID.</p> <p>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.</p>	
<p>Administrator Password</p> <p>Note This field specifies the password for the administrator account, which you use for secure shell access to the CLI, for logging in to Cisco Unified Communications Operating System Administration, and for logging in to the Disaster Recovery System. Ensure that the password is at least six characters long; it can contain alphanumeric characters, hyphens, and underscores. You can change the password after installation.</p>	
<p>Unit</p> <p>Note The value you enter is used to generate a Certificate Signing Request.</p>	
<p>Location</p>	
<p>State</p> <p>Note The value you enter is used to generate a Certificate Signing Request.</p>	
<p>Country</p> <p>Note The value that you enter is used to generate a Certificate Signing Request and self-signed certificates.</p>	
<p>NTP Server</p> <p>Note Enter the hostname or IP address of one or more Network Time Protocol (NTP) servers with which you want to synchronize. You can enter up to 5 NTP servers. You can change the NTP server after installation.</p>	

Parameter	Your Entry
<p>Security Password</p> <p>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.</p> <p>You can change the password after installation by using the following CLI command:</p> <p>set password user security</p>	
<p>SMTP Location</p> <p>Note You must populate this field if you plan to use e-mail notification.</p>	
<p>Application User Name</p> <p>Note Use the Application User Name to log in to the Administration Web Portal.</p>	
<p>Application User Password</p> <p>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.</p> <p>You can change the password after installation.</p>	

Post Installation



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

Procedure

- 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.

Procedure

- 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**
- 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

Procedure

- Step 1** Create a floppy drive image adding the Answer file.
- a) Create the answer file (`platformConfig.xml`) using https://www.cisco.com/web/cuc_afg/index.html.
 - b) Fill out the required information on the Answer File Generate page.
 - c) Click the **Generate Answer Files & License MAC** button.
 - d) From the popup window, click **Proceed to Download Answer Files** and click **Download File**.
- Note** Ensure that you have enabled popup windows option on your browser.
- e) Copy the contents as a text file.

- f) Right-click the popup window and select **View Page Source**.
A window is displayed with xml format of the file.
- g) Copy the contents and paste into a text editor. Save the file as *platformConfig.xml*.
- h) Download the **WinImage** program. Use this program to create the FLP image that can be mounted.
- i) Run WinImage and drag the file into the program.
The program pops up a **Format Selection** window. Click **OK** and click **Yes** to inject the file into the program.
- j) Save the file as *Virtual floppy image.flp* format. The file must have the name *platformConfig.flp*.
- k) You can now mount this file on your VM. Access the VM via console access using vSphere.
- l) Click the floppy disk icon and select **Connect to floppy on local disk**. This is your local PC. You can upload to the datastore as well.

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 executes *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.

Procedure

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
```

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

A Security Alert dialog box is displayed.

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.

Procedure

- 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.
-

