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 **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.	

Parameter	Your Entry
IP Address	
IP Mask	
Gateway Address	
[Optional] Primary DNS	
[Optional] Secondary DNS (optional)	
[Optional] Domain	
Administrator ID **Note** You *cannot* change the original administrator account user ID. **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 **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. You can change the password after installation.	
Unit **Note** The value you enter is used to generate a Certificate Signing Request.	
Location	
State **Note** The value you enter is used to generate a Certificate Signing Request.	
Country **Note** The value that you enter is used to generate a Certificate Signing Request and self-signed certificates.	

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