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.sgn must 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 3 or Upgrade Cisco VVB Using CLI, on page 4.
2	Switch Version and Verify, on page 4.

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.