



Introduction

Cisco Virtualized Voice Browser (Cisco VVB) manages VoiceXML applications for departments, branches, or small to medium-size companies planning to deploy an entry-level or mid-market IVR solution.

Cisco Unified Operating System Administration web interface in Cisco VVB allows you to configure and manage the Cisco Unified Communications Operating System.

- [Overview, page 1](#)
- [Browser Requirements, page 2](#)
- [Operating System Component Status, page 2](#)
- [Operating System Settings, page 2](#)
- [Operating System Security Options, page 3](#)
- [Application Software Upgrades, page 3](#)
- [Services, page 3](#)
- [Command Line Interface, page 4](#)

Overview

For Cisco VVB, you can perform many common system administration functions through the Cisco Unified Communications Operating System. Administration tasks include the following examples:

- Check software and hardware status.
- Check and update IP addresses.
- Ping other network devices.
- Manage NTP servers.
- Upgrade system software and options.
- Manage server security, including IPSec and certificates
- Manage remote support accounts
- Restart the system.

The following sections describe each operating system function in more detail.

Browser Requirements

For supported web browsers, see *Solution Compatibility Matrix*.

**Note**

If you are using Microsoft Internet Explorer or Mozilla Firefox browser, verify that the popup blocker is disabled.

Ensure the URL of the Cisco Unified Communications Operating System server (`https://serverIP`) is included in the browser “Trusted Site Zone” or the “Local Intranet Site Zone” for all product features to work correctly.

Operating System Component Status

From the **Show** menu, you can check the status of various operating system components, including:

- Cluster and node
- Hardware
- Network
- System
- Installed software and options
- IP Preferences

Operating System Settings

From the **Settings** menu, you can view and update the following operating system settings:

- IP—Updates the IP addresses that were entered when the application was installed.
- NTP Server settings—Configures the IP addresses of an external NTP server; add or delete an NTP server.
- SMTP settings—Configures the SMTP host that the operating system uses to send e-mail notifications.

From the **Settings > Version** window, you can choose from the following options for restarting or shutting down the system:

- Switch Versions—Switches the active and inactive disk partitions and restarts the system. You normally choose this option after the inactive partition has been updated and you want to start running a newer software version.
- Current Version—Restarts the system without switching partitions.
- Shutdown System—Stops all running software and shuts down the server.

**Note**

This command does not power down the server. To power down the server, press the power button.

Operating System Security Options

Use the operating system security options to manage security certificates and Secure Internet Protocol (IPSec). From the **Security** menu, you can choose the following security options:

Certificate Management	Manages certificates and Certificate Signing Requests (CSR). You can display, upload, download, delete, and regenerate certificates. Through Certificate Management, you can also monitor the expiration dates of the certificates on the server.
Certificate Monitor	Monitors the certificate expiration. The system can automatically send you an e-mail message when a certificate is close to its expiration date.
Certificate Revocation	The Online Certificate Status Protocol (OCSP) is used to obtain the revocation status of the certificate.
IPSEC Management	Displays or updates existing IPSEC policies; sets up new IPSEC policies and associations.
Bulk Certificate Management	To support the Extension Mobility Cross Cluster (EMCC) feature, the system allows you to execute a bulk import and export operation to and from a common SFTP server that has been configured by the cluster administrator.
Single Sign On	Manages the Single Sign On configurations of specific applications.

Application Software Upgrades

Use the software upgrade options to upgrade the application software or apply patch files.

From the **Install/Upgrade** menu option, you can upgrade system software from either a local disc or a remote server. The upgraded software is installed on the inactive partition, and you can then restart the system and switch partitions, so the system starts running on the newer software version.

**Note**

You must perform all software installations and upgrades by using the software upgrades features that are included in the Cisco Unified Communications Operating System GUI and command line interface. The system can upload and process only software that Cisco Systems approved. You cannot install or use third-party or Windows-based software applications that you may have been using with a previous version of Cisco VVB.

Services

The application provides the following operating system utilities:

- Ping—Checks connectivity with other network devices.
- Remote Support—Configures an account that Cisco support personnel can use to access the system. This account automatically expires after the number of days that you specify.

Command Line Interface

You can access a command-line interface from the console or through a secure shell connection to the server.

For more information, see the "Command line interface" section of the *Cisco Virtualized Voice Browser Operations Guide*.