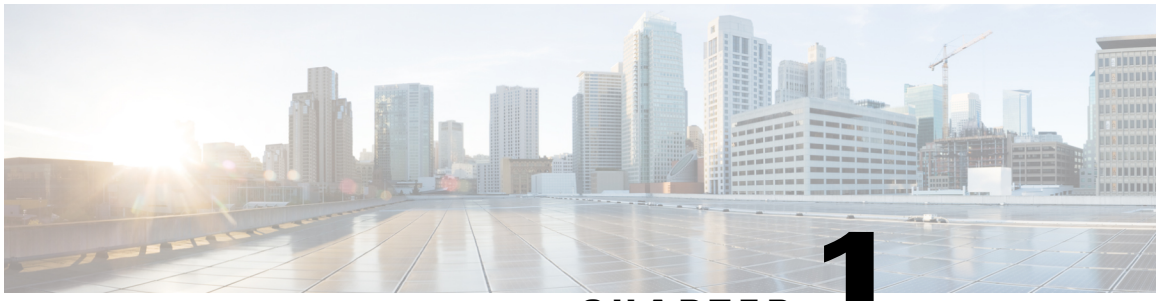
Cisco Unified Communications Operating System Administration Guide for Cisco Virtualized Voice Browser, Release 11.5(1)

First Published: August 10, 2016

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



CHAPTER 1

Introduction

Cisco Virutalized 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

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

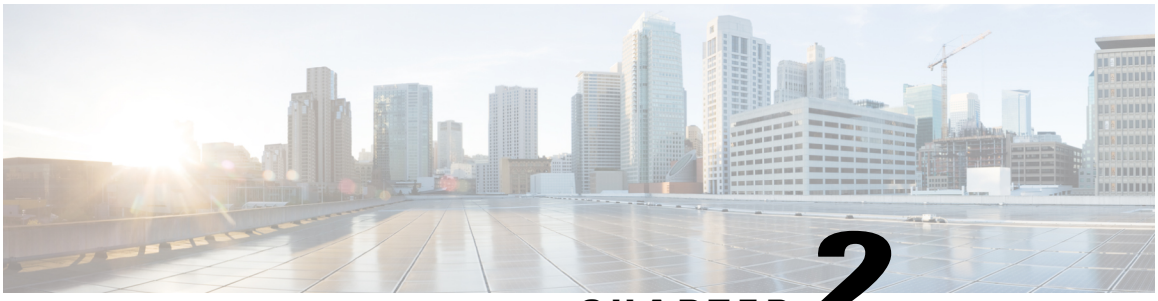
The application provides the following operating system utilities:

- 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*.



CHAPTER 2

Cisco Unified Communications Operating System Administration

This chapter describes the procedure for accessing the Cisco Unified Communications Operating System Administration. This chapter also provides procedures for resetting a lost password.

Login to Cisco Unified Communications Operating System

To access and login to Cisco Unified Communications Operating System from Cisco VVB, follow this procedure:

Note Do not use the browser controls (for example, the Back button) while you are using Cisco Unified Communications Operating System Administration.

Procedure

Step 1 Log in to Cisco VVB Application Administration web interface.

Step 2 From the Navigation menu in the upper-right corner of the Cisco VVB Application Administration web interface, choose **Cisco Unified OS Administration** and click **Go**.
The Cisco Unified Communications Operating System Administration Logon web page appears.

Note You can also access Cisco Unified Communications Operating System Administration directly by entering the following URL:

```
https://<serverIP>/cmplatform
```

Step 3 Enter your platform user credentials as configured during installation of Cisco VVB.

Note The platform username and password get established during installation or created by using the command line interface.

Step 4 Click **Submit**.

The Cisco Unified Communications Operating System Administration window appears.

Reset Administrator or Security Password

If you lose the administrator password or security password, use the following procedure to reset the passwords.

Caution Failure to reboot the server (node) causes system service problem and problems with the Cisco Unified Communications Manager Administration windows on the subscriber servers.

Note During this procedure, you must remove and then insert a valid CD or DVD in the disk drive to prove that you have physical access to the system.

Before You Begin

To perform the password reset process, you must be connected to the system through the system console, that is, you must have a keyboard and monitor connected to the server. You cannot reset a password when connected to the system through a secure shell session.

Procedure

Step 1 Log in to the system with the following username and password:
a) Username: **pwrecovery**
b) Password: **pwreset**
The **Welcome to platform password reset** window appears.

Step 2 Press any key to continue.

Step 3 If you have a CD or DVD in the disk drive, remove it now.

Step 4 Press any key to continue.
The system tests to ensure that you have removed the CD or DVD from the disk drive.

Step 5 Insert a valid CD or DVD into the disk drive. For this test, you must use a data CD, not a music CD. The system tests to ensure that you inserted the disk.

Step 6 After the system verifies that you have inserted the disk, you are prompted to enter one of the following options to continue:

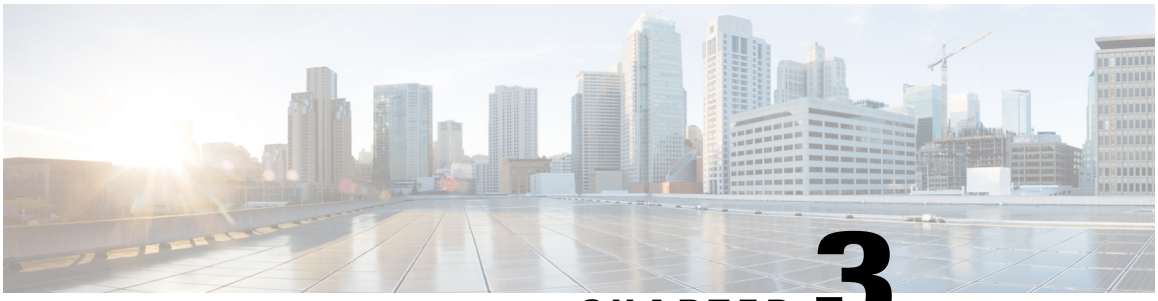
- Enter **a** to reset the administrator password.
- Enter **s** to reset the security password.
- Enter **q** to quit.

Step 7 Enter a new password of the type that you chose.

Step 8 Reenter the new password.

The password must contain at least 6 characters. The system checks the new password for strength. If the password does not pass the strength check, you are prompted to enter a new password.

Step 9 After the system verifies the strength of the new password, the password is reset, and you are prompted to press any key to exit the password reset utility.



CHAPTER 3

Status and Configuration

View Hardware Status

To view the hardware status, follow this procedure:

Procedure

From the Cisco Unified Communications Operating System Administration window, navigate to **Show** > **Hardware**.
The following table contains descriptions of the fields on the **Hardware status** window.

Table 1: Hardware Status Field Descriptions

Field	Description
Platform Type	Displays the model identity of the platform server.
Serial Number	Displays the serial number of the platform server.
Virtual Hardware	Displays the status of the virtual hardware configured.
Virtual Support	Displays the status of the virtual support available.
Processor Speed	Displays the processor speed.

Field	Description
CPU Type	Displays the type of processor in the platform server.
Memory	Displays the total amount of memory in MB.
Object ID	Displays the object ID.
OS Version	Displays the operating system version.
RAID Details	Displays details about the RAID drive, including controller information, logical drive information, and physical device information.

Display Network Status

The network status information that appears depends on if Network Fault Tolerance is enabled. When Network Fault Tolerance is enabled, Ethernet port 1 automatically takes over network communications if Ethernet port 0 fails. If Network Fault Tolerance is enabled, network status information appears for the network ports Ethernet 0, Ethernet 1, and Bond 0. If Network Fault Tolerance is not enabled, status information appears only for Ethernet 0.

To view the network status, follow this procedure:

Procedure

From the Cisco Unified Communications Operating System Administration window, navigate to **Show** > **Network**.
The following table contains descriptions of the fields on the **Network Settings** window.

Table 2: Network Settings Field Descriptions

Field	Description
Ethernet Details	
DHCP	Disabled for Cisco VVB.
Status	Indicates whether the port is Up or Down for Ethernet ports 0 and 1.
IP Address	Shows the IP address of Ethernet port 0 [and Ethernet port 1 if Network Fault Tolerance (NFT) is enabled].
IP Mask	Shows the IP mask of Ethernet port 0 (and Ethernet port 1 if NFT is enabled).
Link Detected	Indicates whether an active link exists.
Queue Length	Displays the length of the queue.

Field	Description
MTU	Displays the maximum transmission unit.
MAC Address	Displays the hardware address of the port.
Receive Statistics (RX)	Displays information on received bytes, packets, and errors, as well as dropped, overrun and multicast statistics.
Transmit Statistics (TX)	Displays information on transmitted bytes, packets, and errors, as well as dropped, carrier, and collision statistics.
DNS Details	
Primary	Displays the IP address of the primary domain name server.
Secondary	Displays the IP address of the secondary domain name server.
Options	Displays the configured DNS options.
Domain	Displays the domain of the server.
Gateway	Displays the IP address of the network gateway on Ethernet port 0.

Verify Installed Software

To view the software versions and installed software options, follow this procedure:

Procedure

From the Cisco Unified Communications Operating System Administration window, navigate to **Show** > **Software**.
The following table contains descriptions of the fields in the **Software Packages** window.

Table 3: Software Packages Field Descriptions

Field	Description
Partition Versions	Displays the software version that is running on the active and inactive partitions.
Installed Software Options	
Active Version Installed Software Options	Displays the versions of installed software options, including Cisco Options Package (COP) patch files that are installed on the active version.

Field	Description
Inactive Version Installed Software Options	Displays the versions of installed software options, including COP patch files that are installed on the inactive version.

View System Status

To view the system status, follow this procedure:

Procedure

From the Cisco Unified Communications Operating System Administration window, navigate to **Show** > **System**.
See the following table for descriptions of the fields on the **System Status** window.

Table 4: System Status Field Descriptions

Field	Description
Host Name	Displays the name of the Cisco MCS host where Cisco Unified Communications Operating System is installed.
Date	Displays the date and time based on the continent and region that were specified during operating system installation.
Time Zone	Displays the time zone that was chosen during installation.
Locale	Displays the language that was chosen during operating system installation.
Product Version	Displays the operating system version.
Platform Version	Displays the platform version.
License MAC	Displays the license MAC.
Uptime	Displays system uptime information.
CPU	Displays the percentage of CPU capacity that is idle, the percentage that is running system processes, and the percentage that is running user processes.
Memory	Displays information about memory usage, including the amount of total memory, free memory, used memory, cached memory, shared memory, and buffers in KBytes.
Disk/active	Displays the amount of total, free, and used disk space on the active disk.
Disk/inactive	Displays the amount of total, free, and used disk space on the inactive disk.

Field	Description
Disk/logging	Displays the amount of total, free, and disk space that is used for disk logging.

Display Registered Ports

You can use the **IP Preferences** window to display a list of registered ports that the system can use. The **IP Preferences** window contains the following information:

- Application
- Protocol
- Port Number
- Type
- Translated Port
- Status
- Description

To access the **IP Preferences** window, follow this procedure.

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, choose **Show** > **IP Preferences**.
The **IP Preferences** window appears. Records from an active (prior) query may also appear in the window.

Step 2 To find all records in the database, ensure the dialog box is empty and go to Step 4.

Step 3 To filter or search records, do the following:

a) From the first drop-down list box, select a search parameter.
b) From the second drop-down list box, select a search pattern.
c) Specify the appropriate search text, if applicable.

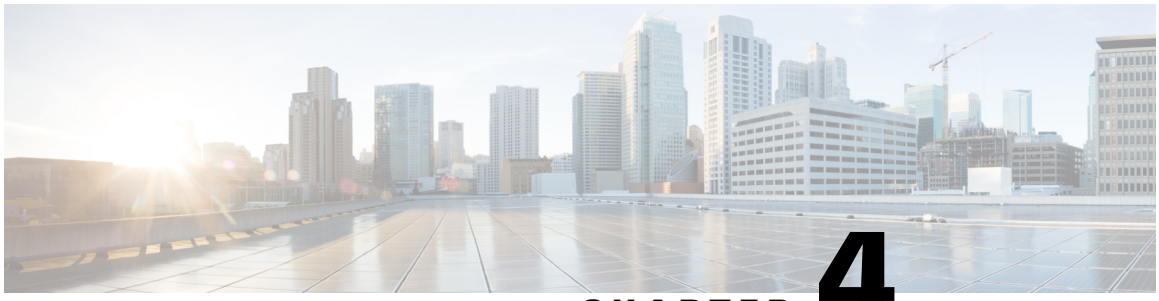
Note To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the **Clear Filter** button to remove all added search criteria.

Step 4 Click **Find**.
All matching records appear. You can change the number of items that appear on each page by choosing a different value from the Rows per Page drop-down list box.

The following table contains descriptions of the IP Preferences fields.

Table 5: IP Preferences Field Descriptions

Field	Description
Application	Name of the application using (listening on) the port.
Protocol	Protocol used on this port (TCP, UDP).
Port Number	Numeric port number.
Type	Type of traffic allowed on this port: • Public—All traffic allowed • Translated—All traffic allowed but forwarded to a different port • Private—Traffic only allowed from a defined set of remote servers, for example, other nodes in the cluster
Translated Port	Traffic destined for this port is forwarded to the port listed in the Port Number column. This field applies to Translated type ports only.
Status	Status of port usage: • Enabled—In use by the application and opened by the firewall • Disabled—Blocked by the firewall and not in use
Description	Brief description of how the port is used.



CHAPTER 4

Settings

IP and Port Settings

Use the IP Settings option to view and change IP and port setting for the Ethernet connection on the subsequent node and configure the IP address of the publisher.

This section contains the following topics:

Note Update the values in the fields only if you are changing the IP address. Host name change is not supported in Cisco VVB.

Change IP Settings

Use the **IP Settings** window to change or view the related Ethernet IP addresses, as well as the IP address for the network gateway.

All Ethernet settings apply to ethernet interface Eth0 or Eth1. You cannot configure any settings for Eth1. The Maximum Transmission Unit (MTU) on Eth0 defaults to 1500.

For detailed instructions about changing the IP address of servers in a cluster, see the *Unified CVP Configuration Guide*, available here:

http://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html

View Publisher IP Settings

You can view the IP address of the first node or publisher for the node on the subsequent node.

Note Update the values in the fields only if you are changing the IP address. For detailed instructions about changing the IP address of servers in a cluster, see the *Unified CVP Configuration Guide*.

To view the publisher IP settings, follow this procedure:

Procedure

From the Cisco Unified Communications Operating System Administration window, navigate to **Settings** > **IP** > **Publisher**.
The **Publisher Settings** window appears.

Note You can view the publisher IP address only on the subsequent node of the cluster, not on the publisher itself.

Configure NTP Servers

Ensure that external NTP servers are stratum 9 or higher (1-9). To add, delete, or modify an external NTP server, follow this procedure:

Note You can only configure the NTP server settings on the first node or publisher.

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Settings** > **NTP Servers**.
The **NTP Server Settings** window appears.

Step 2 Add, delete, or modify an NTP server:

Note To avoid potential compatibility, accuracy, and network jitter problems, the external NTP servers that you specify for the primary node must be NTP v4 (version 4). If you are using IPv6 addressing, external NTP servers must be NTP v4.

- To delete an NTP server, select the check box in front of the appropriate server, and then click **Delete**.
- To add an NTP server, click **Add**, enter the hostname or IP address, and then click **Save**.
- To modify an NTP server, click the IP address, modify the hostname or IP address, and then click **Save**.

Note Any change that you make to the NTP servers can take up to 5 minutes to complete. Whenever you make any change to the NTP servers, you must refresh the window to view the correct status.

Step 3 To refresh the **NTP Server Settings** window and view the correct status, choose **Settings** > **NTP**. After deleting, modifying, or adding the NTP server, you must restart the other node in the cluster for the changes to take effect.

Set SMTP settings

Use the **SMTP Settings** window to view or set the SMTP hostname and determine if the SMTP host is active.

Tip If you want the system to send you e-mail, you must configure an SMTP host.

To access the SMTP settings, follow this procedure:

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Settings** > **SMTP**.
The **SMTP Settings** window appears.

Step 2 Enter or modify the SMTP hostname or IP address.

Step 3 Click **Save**.

Set Time

To manually configure the time, follow this procedure:

Note The time cannot be set if NTP is currently enabled. Before you can manually configure the server time, you must delete any NTP servers that you configured.

Caution If you enter a time that is before the time when Cisco VVB was installed on the server, the digital certificates that the server uses for security become invalid, causing the webserver (Tomcat) to stop working. If this happens, you must regenerate the certificates.

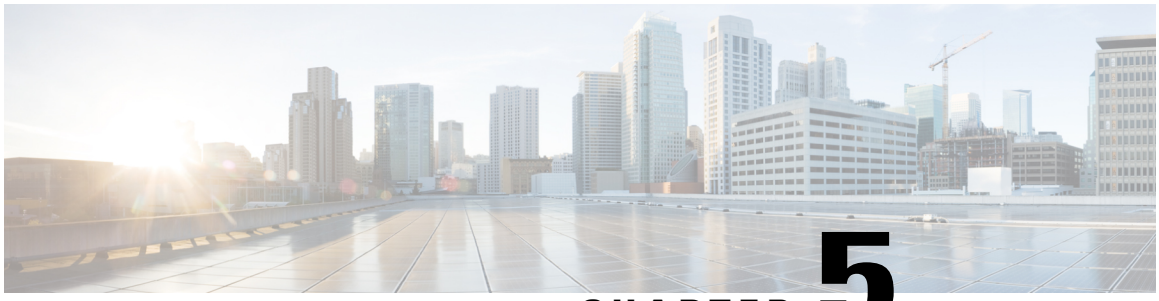
Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Settings** > **Time**.

Step 2 Enter the date and time for the system.

Step 3 Click **Save**.

Step 4 On a Cisco VVB server, if you changed the date or if you changed the time by more than two minutes, use the CLI command **utils system restart** to restart the server.



CHAPTER 5

System Restart

Switch Versions and Restart

You can use this option both when you are upgrading to a newer software version, and when you need to fall back to an earlier software version. To shut down the system that is running on the active disk partition and then automatically restart the system by using the software version on the inactive partition, follow this procedure:

Caution This procedure causes the system to restart and become temporarily out of service.

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Settings** > **Version**.
The **Version Settings** window appears, showing the software version on both the active and inactive partitions.

Step 2 Click **Switch Versions** to switch versions and restart. Click **Cancel** to stop the operation.
If you click **Switch Versions**, the system restarts, and the partition that is inactive becomes active.

Restart Current Version

To restart the system on the current partition without switching versions, follow this procedure:

Caution This procedure causes the system to restart and become temporarily out of service.

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Settings** > **Version**.
The **Version Settings** window appears, showing the software version on both the active and inactive partitions.

Step 2 Click **Restart** to restart the system, or click **Cancel** to stop the operation.
If you click **Restart**, the system restarts on the current partition without switching versions.

Shut Down System

Caution Do not press the power button on the server to shut down the server or to reboot the server. If you do, you may accidentally corrupt the file system, which may prevent you from future server reboots.

Caution This procedure causes the system to shut down.

Procedure

Step 1 If you are shutting down the system from the command line interface, go to step 4. Otherwise, go to Step 2.

Step 2 From the Cisco Unified Communications Operating System Administration window, navigate to **Settings** > **Version**.
The **Version Settings** window appears, showing the software version on both the active and inactive partitions.

Step 3 Click **Shutdown** to shut down the system, or click **Cancel** to stop the operation.
If you click **Shutdown**, the system halts all processes and shuts down.

Note The hardware may require several minutes to power down.

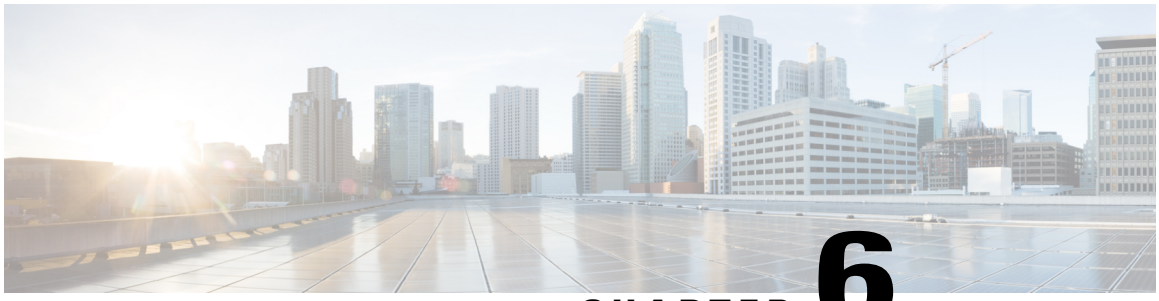
Step 4 Enter the command **utils system shutdown** or the command **utils system restart**.
For more information about CLI commands, see the *Operations Guide for Cisco Virtualized Voice Browser* , located at http://www.cisco.com/c/en/us/support/customer-collaboration/virtualized-voice-browser/tsd-products-support-maintain-and-operate.html.

What to Do Next

When the user initiates a switch version, system restart, or system shutdown from the Cisco Unified OS Administration web interface, the operation fails in the following scenarios:

- If the system detects that a switch version is in progress.
- If the system detects that a previous switch version was abruptly terminated.

Note A switch version operation is abruptly terminated if a power reset or hard reboot is done on the Cisco VVB system when it is in progress.



CHAPTER 6

Security

This chapter describes Certificate Management and IPSec Management and provides procedures for managing system security.

Set Internet Explorer Security Settings

To download certificates from the server, ensure your Internet Explorer security settings are configured as follows:

Procedure

Step 1 Start Internet Explorer.

Step 2 Navigate to **Tools** > **Internet Option**.

Step 3 Click the **Advanced** tab.

Step 4 Scroll down to the Security section on the **Advanced** tab.

Step 5 If necessary, clear the **Do not save encrypted pages to disk** check box.

Step 6 Click **OK**.

Certificate Management menu

Note To access the Security menu items, you must log in to Cisco Unified Communications Operating System Administration using your administrator password.

Display Certificates

To display existing certificates, follow this procedure:

Procedure

Step 1 Navigate to **Security** > **Certificate Management**.
The **Certificate List** window appears.

Step 2 You can use the Find controls to filter the certificate list.

Step 3 To view details of a certificate or trust store, click its file name.
The **Certificate Configuration** window shows information about the certificate.

Step 4 To return to the **Certificate List** window, select **Back To Find/List** in the Related Links list; then, click **Go**.

Download Certificate

To download a certificate from the Cisco Unified Communications Operating System to your PC, follow this procedure:

Procedure

Step 1 Navigate to **Security** > **Certificate Management**.
The **Certificate List** window appears.

Step 2 You can use the Find controls to filter the certificate list.

Step 3 Click the file name of the certificate.
The **Certificate Configuration** window appears.

Step 4 Click **Download**.

Step 5 In the **File Download** dialog box, click **Save**.

Delete Certificate

To delete a trusted certificate, follow this procedure:

Caution Deleting a certificate can affect your system operations. Any existing CSR for the certificate that you choose from the Certificate list is deleted from the system. You must generate a new CSR.

Procedure

Step 1 Navigate to **Security** > **Certificate Management**.
The **Certificate List** window appears.

Step 2 You can use the **Find** controls to filter the certificate list.

Step 3 Click the file name of the certificate.
The **Certificate Configuration** window appears.

Step 4 Click **Delete**.

Regenerate Certificate, on page 25

Regenerate Certificate

To regenerate a certificate, follow this procedure:

Caution Regenerating a certificate can affect your system operations.

Procedure

Step 1 Navigate to **Security** > **Certificate Management**.
The **Certificate List** window appears.

Step 2 Click **Generate New**.
The **Generate Certificate** dialog box opens.

Step 3 Choose a certificate name from the **Certificate Name** list.
The following table contains descriptions of the certificate names that appear:

Name	Description
tomcat	This self-signed root certificate is generated during installation for the HTTPS server.
ipsec	This self-signed root certificate is generated during installation for IPSec connections with MGCP and H.323 gateways.

Step 4 Click **Generate New**.

What to Do Next

After you regenerate certificates in Cisco Unified Communications Operating System, you must perform a backup so that the latest backup contains the regenerated certificates. For information on performing a backup, see the *Cisco Unified Contact Center Express Disaster Recovery System Administration Guide* .

Upload Certificate to Server

Caution Uploading a new certificate can affect your system operations. After you upload a new certificate, you must restart the Cisco VVB server (in the case of high availability deployments, restart both nodes).

Note The system does not distribute trust certificates to other cluster node automatically. If you must have the same certificate on more than one node, you must upload the certificate to each node individually.

Upload Certificate or Certificate Chain

Procedure

Step 1 Navigate to **Security** > **Certificate Management**.
The **Certificate List** window appears.

Step 2 Click **Upload Certificate/Certificate Chain**.
The **Upload Certificate/Certificate Chain** dialog box opens.

Step 3 Select the certificate name from the **Certificate Name** list.

Step 4 Select the file to upload by performing one of the following steps:

- In the **Upload File** text box, enter the path to the file, or
- Click the **Browse** button and navigate to the file; then, click **Open**.
  Cisco VVB supports Privacy Enhanced Mail (PEM) Base64 encoded format of X.509 certificate (only one PEM certificate in a file), Distinguished Encoding Rules (DER) format of X509 Certificate and DER format of PKCS#7 (Public-Key Cryptography Standards) Certificate Chain. The system does not support PEM format of PKCS#7 Certificate Chain.

Step 5 Click the **Upload File** button to upload the file to the server.

Obtain Third-Party CA Certificates

Cisco Unified Communications Operating System supports certificates that a third-party Certificate Authority (CA) issues with PKCS # 10 Certificate Signing Request (CSR). The following table provides an overview of this process, with references to additional documentation:

Procedure

Step 1 Generate a CSR on the server.
See Generate Certificate Signing Request, on page 27.

Step 2 Download the CSR to your PC.
See Download Certificate Signing Request, on page 27.

Step 3 Use the CSR to obtain an application certificate from a CA.
Get information about obtaining application certificates from your CA. See Application Certificates, on page 28 for additional notes.

Step 4 Obtain the CA root certificate.
Get information about obtaining a root certificate from your CA. See Application Certificates, on page 28 for additional notes.

Step 5 Upload the CA root certificate to the server.
See Upload Certificate or Certificate Chain, on page 26.

Step 6 Upload the application certificate to the server.
See Upload Certificate or Certificate Chain, on page 26.

Step 7 Restart the services that are affected by the new certificate.
For all certificate types, restart the corresponding service (for example, restart the Tomcat service if you updated the Tomcat certificate). See the Cisco VVB Serviceability Administration Guide for information about restarting services.

Generate Certificate Signing Request

To generate a Certificate Signing Request (CSR), follow these steps:

Procedure

Step 1 Navigate to **Security** > **Certificate Management**.
The **Certificate List** window appears.

Step 2 Click **Generate CSR**.
The **Generate Certificate Signing Request** dialog box opens.

Step 3 Select the certificate name from the **Certificate Name** list.

Note For the current release of the Cisco Unified Operating System, the Directory option no longer appears in the list of Certificate Names.

Step 4 Click **Generate CSR**.

Download Certificate Signing Request

To download a Certificate Signing Request, follow this procedure:

Procedure

Step 1 Navigate to **Security** > **Certificate Management**.
The **Certificate List** window appears.

Step 2 Click **Download CSR**.
The **Download Certificate Signing Request** dialog box opens.

Step 3 Select the certificate name from the **Certificate Name** list.

Step 4 Click **Download CSR**.

Step 5 In the **File Download** dialog box, click **Save**.

Application Certificates

To use an application certificate that a third-party CA issues, you must obtain both the signed application certificate and the CA root certificate from the CA. Collect information about obtaining these certificates from your CA. The process varies among CAs.

Cisco Unified Communications Operating System generates certificates in DER and PEM encoding formats and generates CSRs in PEM encoding format. It accepts certificates in DER and PEM encoding formats.

For all certificate types, obtain and upload a CA root certificate and an application certificate on each node.

The CSRs for Tomcat and IPSec use the following extensions:

```
X509v3 Key Usage:
Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication, IPSec End
System
```

1. Upload the CA root certificate of the CA that signed an application certificate. If a subordinate CA signs an application certificate, you must upload the CA root certificate of the subordinate CA, not the root CA.
2. You upload CA root certificates and application certificates by using the same Upload Certificate dialog box. When you upload a CA root certificate, choose the certificate name with the format *certificate type*-**trust**.
3. When you upload an application certificate, choose the certificate name that only includes the certificate type. For example, choose **tomcat-trust** when you upload a Tomcat CA root certificate; choose **tomcat** when you upload a Tomcat application certificate.

Monitor Certificate Expiration Dates

The system can automatically send you an e-mail when a certificate is close to its expiration date. To view and configure the Certificate Expiration Monitor, follow this procedure:

Procedure

Step 1 Navigate to **Security** > **Certificate Monitor**.

The **Certificate Monitor** window appears.

Step 2 Enter the required configuration information.
See the table below for a description of the Certificate Monitor Expiration fields.

Step 3 To save your changes, click **Save**.

Table 6: Certificate Monitor Field Descriptions

Field	Description
Notification Start Time	Enter the number of days before the certificate expires that you want to be notified.
Notification Frequency	Enter the frequency for notification, either in hours or days.
Enable Email Notification	Select the check box to enable e-mail notification.
Email IDs	Enter the e-mail address to which you want notifications sent. **Note** For the system to send notifications, you must configure an SMTP host.

IPSec Management

The following topics describe the functions that you can perform with the IPSec menu:

- Set Up New IPSec Policy, on page 29
- Manage IPSec Policies, on page 31

Note IPSec does not automatically get set up between nodes in the cluster during installation.

Set Up New IPSec Policy

Any changes that you make to an IPSec policy during a system upgrade are lost, so do not modify or create IPSec policies during an upgrade.

Caution IPSec, especially with encryption, affects the performance of your system.

Procedure

Step 1 Navigate to **Security** > **IPSEC Configuration**.

The **IPSEC Policy List** window appears.

Step 2 Click **Add New**.
The **IPSEC Policy Configuration** window appears.

Step 3 Enter the appropriate information on the **IPSEC Policy Configuration** window. See the table below for descriptions of the fields on this window.

Step 4 Click **Save** to set up the new IPSec policy.

Table 7: IPSec Policy and Association Field Descriptions

Field	Description
Policy Group Name	Specifies the name of the IPSec policy group. The name can contain only letters, digits, and hyphens.
Policy Name	Specifies the name of the IPSec policy. The name can contain only letters, digits, and hyphens.
Authentication Method	Specifies the authentication method.
Preshared Key	Specifies the preshared key if you selected Pre-shared Key in the Authentication Name field. **Note** Pre-shared IPSec keys can contain alphanumeric characters and hyphens only, not white spaces or any other characters. If you are migrating from a Windows-based version of Cisco VVB, you may need to change the name of your pre-shared IPSec keys, so they are compatible with current versions of Cisco VVB.
Peer Type	Specifies whether the peer is the same type or different.
Certificate Name	If you choose Different for the Peer Type, enter the new certificate name.
Destination Address	Specifies the IP address or FQDN of the destination.
Destination Port	Specifies the port number at the destination.
Source Address	Specifies the IP address or FQDN of the source.
Source Port	Specifies the port number at the source.
Mode	Specifies Transport mode.
Remote Port	Specifies the port number to use at the destination.
Protocol	Specifies the protocol: • TCP • UDP • Any

Field	Description
Encryption Algorithm	From the drop-down list, choose the encryption algorithm. Choices include • DES • 3DES
Hash Algorithm	Specifies the hash algorithm: • SHA1—Hash algorithm that is used in phase 1 IKE negotiation • MD5—Hash algorithm that is used in phase 1 IKE negotiation
ESP Algorithm	From the drop-down list, choose the ESP algorithm. Choices include • NULL_ENC • DES • 3DES • BLOWFISH • RIJNDAEL
Phase One Life Time	Specifies the lifetime for phase One, IKE negotiation, in seconds.
Phase One DH	From the drop-down list, choose the phase One DH value. Choices include: 2, 1, and 5.
Phase Two Life Time	Specifies the lifetime for phase Two, IKE negotiation, in seconds.
Phase Two DH	From the drop-down list, choose the phase Two DH value. Choices include: 2, 1, and 5.
Enable Policy	Check the check box to enable the policy.

Manage IPSec Policies

To display, enable or disable, or delete an existing IPSec policy, follow this procedure:

Note Because any changes that you make to an IPSec policy during a system upgrade are lost, do not modify or create IPSec policies during an upgrade.

Caution IPSec, especially with encryption, will affect the performance of your system.

Caution Any changes that you make to the existing IPSec policies can impact your normal system operations.

Procedure

Step 1 Navigate to **Security** > **IPSEC Configuration**.

Note To access the Security menu items, you must log in to Cisco Unified Communications Operating System Administration again by using your Administrator password.

The **IPSEC Policy List** window appears.

Step 2 To display, enable, or disable a policy, follow these steps:

a) Click the policy name.
The **IPSEC Policy Configuration** window appears.
b) To enable or disable the policy, click the **Enable Policy** check box.
c) Click **Save**.

Step 3 To delete one or more policies, follow these steps:

a) Check the check box next to the policies that you want to delete.
You can click **Select All** to select all policies or **Clear All** to clear all the check boxes.
b) Click **Delete Selected**.

Bulk Certificate Management

Note The **Security** > **Bulk Certificate Management** menu option is not applicable for Cisco VVB.

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.

To use **Bulk Certificate Management** to export certificates, use the following procedure:

1. Navigate to **Security > Bulk Certificate Management**.
   The Bulk Certificate Management window displays.
2. Enter the appropriate information on the **Bulk Certificate Management** window.
3. To save the values you entered, click **Save**.
4. To export certificates, click **Export**.
   The **Bulk Certificate Export** popup window displays.
5. From the drop-down menu, choose the type of certificate you want to export:

- Tomcat
- TFTP
- Capf
- All

6 Click **Export**.

The system exports and stores the certificates you chose on the central SFTP server.

You can also use the **Bulk Certificate Management** window to import certificates that you have exported from other clusters. However, before the **Import** button displays, you must complete the following activities:

- Export the certificates from at least two clusters to the SFTP server.
- Consolidate the exported certificates.

Single Sign On

Note The **Security** > **Single Sign On** menu option is not applicable for Cisco VVB.

Note SSO is not supported for Application User accounts.

To configure **OpenAM SSO**, click **Cisco Unified OS Administration > Security > Single Sign On** and follow the below procedure:

1 Enter the following URL of the Open Access Manager (OpenAM) server: http://opensso.sample.com:443/opensso.

2 Enter the relative path where the policy agent should be deployed. The relative path must be alphanumeric.

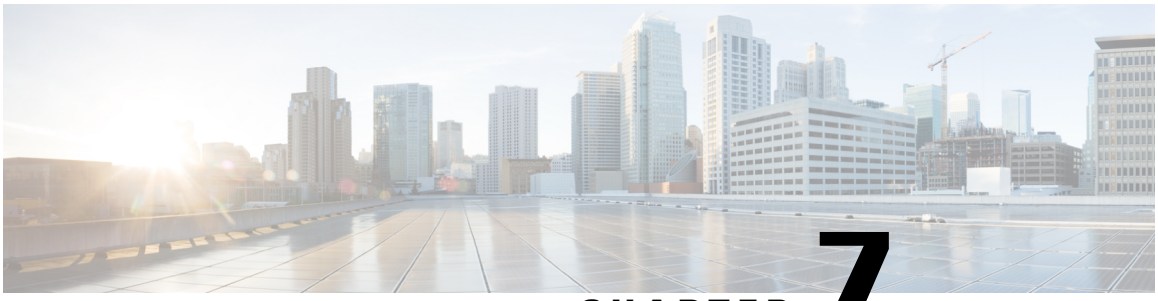
3 Enter the name of the profile that is configured for this policy agent.

4 Enter the password of the profile name.

5 Enter the login Module instance name that is configured for Windows Desktop SSO.

6 Click **Save**.

7 Click **OK** on the confirmation dialog box to restart Tomcat.



CHAPTER 7

Software Upgrades

You can use the **Install/Upgrade** option to upgrade the Cisco VVB software and install Cisco VVB COP patch files.

Note For more information regarding the supported versions of Cisco VVB and Unified CM, see *Cisco Solutions Compatibility Matrix*.

Caution When you upgrade Cisco VVB the system restarts as part of the upgrade process. Therefore, you may want to perform the upgrade during maintenance window to avoid service interruptions.

Cisco VVB Upgrade and Roll Back

For Upgrade and Rollback instructions, see *Installation and Upgrade Guide for Cisco Virtualized Voice Browser* available here:

http://www.cisco.com/c/en/us/support/customer-collaboration/virtualized-voice-browser/tsd-products-support-install-and-upgrade.html

TFTP File Management

Note The **Software Upgrades** > **TFTP File Management** menu option is not applicable for Cisco VVB.

Set Up Customized Logon Message

You can upload a text file that contains a customized logon message that appears in Cisco Unified Communications Operating System Administration, Disaster Recovery System, and the command-line interface.

To upload a customized logon message, follow this procedure:

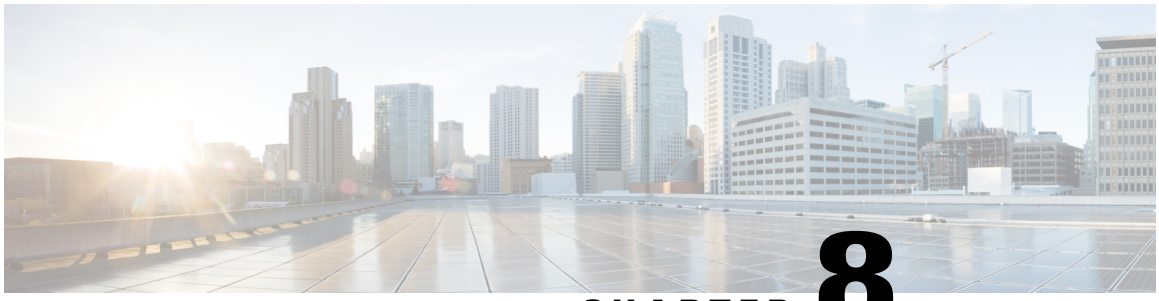
Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Software Upgrades** > **Customized Logon Message**.
The **Customized Logon Message** window appears.

Step 2 To choose the text file that you want to upload, click **Browse**.

Step 3 Click **Upload File**. You cannot upload a file that is larger than 10kB.
The customized logon message appears.

Step 4 To revert to the default log-on message, click **Delete**.
Your customized logon message is deleted, and the system displays the default logon message.



CHAPTER 8

Utility Functions

This chapter describes the utility functions that are available on the operating system: pinging another system and setting up remote support.

Ping

Use the **Ping Utility** window to ping another server in the network.

To ping another system, follow this procedure:

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Services** > **Ping**.
The **Ping Remote** window appears.

Step 2 Enter the IP address or network name for the system that you want to ping.

Step 3 Enter the ping interval in seconds.

Step 4 Enter the packet size.

Step 5 Enter the ping count (the number of times that you want to ping the system).

Note When you specify multiple pings, the ping command does not display the ping date and time immediately. Be aware that the Ping command displays the data after it completes the number of pings that you specified.

Step 6 Choose whether you want to validate IPSec.

Step 7 Click **Ping**.
The **Ping Remote** window displays the ping statistics.

Remote Account Support

From the **Remote Access Configuration** window, you can set up a remote account that Cisco support personnel can use to access the system for a specified time.

The remote support process works like this:

1. The customer sets up a remote support account. This account includes a time limit on how long Cisco personnel can access it. This time limit can be configured to various values.
2. When the remote support account is set up, a pass phrase gets generated.
3. The customer calls Cisco support and provides the remote support account name and pass phrase.
4. Cisco support enters the pass phrase into a decoder program that generates a password from the pass phrase.
5. Cisco support logs into the remote support account on the customer system by using the decoded password.
6. When the account time limit expires, Cisco support can no longer access the remote support account.

To set up remote support, follow this procedure:

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Services** > **Remote Support**.
The **Remote Access Configuration** window appears.

Step 2 Enter an account name for the remote account in the **Account Name** field.
The account name must comprise at least six-characters that are all lowercase, alphabetic characters.

Caution Avoid creating remote account names starting with “vvb” or “VVB” because such user names may conflict with system account names used internally within Cisco VVB server.

Step 3 Enter the account duration, in days, in the **Account Duration** field.
The default account duration specifies 30 days.

Step 4 Click **Save**.
The fields in the following table appears in the Remote Access Account Information area:

Table 8: Remote Access Account Information Fields and Descriptions

Field	Description
Account name	Displays the name of the remote support account.
Expiration	Displays the date and time when access to the remote account expires.
Passphrase	Displays the generated pass phrase.
Decode version	Indicates the version of the decoder in use.

Step 5 To access the system by using the generated pass phrase, contact your Cisco personnel.

Step 6 To delete the remote access support account, click **Delete**.

INDEX

P

R

S

T

V