Getting Started

- Sign In to Adminstrative Interfaces, on page 1
- Reset the Administrator or Security Password, on page 1
- Shut Down or Restart the System, on page 2

Sign In to Adminstrative Interfaces

Use this procedure to sign in to any of the administrative interfaces in your system.

Procedure

Step 1 Open the Unified Communications Manager interface in your web browser.

Step 2 Choose the administration interface from the **Navigation** drop-down list.

Step 3 Click **Go**.

Step 4 Enter your username and password.

Step 5 Click **Login**.

Reset the Administrator or Security Password

If you lose the administrator password and cannot access your system, use this procedure to reset the password.

Note For password changes on IM and Presence nodes, stop the Cisco Presence Engine service in all IM and Presence nodes before resetting the administrator password. After the password reset, restart the Cisco Presence Engine service in all the nodes. Make sure that you perform this task during maintenance because you may face presence issues when the PE is stopped.

Before you begin

- You require physical access to the node on which you perform this procedure.

- At any point, when you are requested to insert CD or DVD media, you must mount the ISO file through the vSphere client for the VMWare server. See "Adding DVD or CD Drives to a Virtual Machine" https://www.vmware.com/support/ws5/doc/ws_disk_add_cd_dvd.html for guidance.
- The security password on all nodes in a cluster must match. Change the security password on all machines, or the cluster nodes will not communicate.

Procedure

Step 1 Sign in to the CLI on the publisher node with the following username and password:

a) Username: **pwrecovery**

b) Password: **pwreset**

Step 2 Press any key to continue.

Step 3 If you have a valid CD/DVD in the disk drive or you mounted an ISO file, remove it from the VMWare client.

Step 4 Press any key to continue.

Step 5 Insert a valid CD or DVD into the drive or mount the ISO file.

Note
For this test, you must use a disk or ISO file that is data only.

Step 6 After the system verifies the last step, 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.

Note
You must reset each node in a cluster after you change its security password. Failure to reboot the nodes causes system service problems and problems with the administration windows on the subscriber nodes.

Step 7 Enter the new password, and then reenter it to confirm.

The administrator credentials must start with an alphabetic character, be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores.

Step 8 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.

If you want to set up a different administrator password, use the CLI command **set password**. For more information, see the *Command Line Interface Reference Guide for CiscoUnified Solutions* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Shut Down or Restart the System

Use this procedure if you need to shut down or restart your system, for example, after you make a configuration change.

Before you begin

If the server is forced to shutdown and restart from your virtual machine, the file system may become corrupted. Avoid a forced shutdown; instead, wait for the server to shutdown properly after this procedure or after you run **utils system shutdown** from the CLI.

Note If you force shutdown or restart the virtual machine from VMware administration tools (vCenter or Embedded Host Client):

- From 12.5(1)SU4 or later, the Unified Communications Manager and IM and Presence Service will gracefully shutdown/restart and this will be displayed in the system-history.log
- From 12.5(1)SU3 or older, this will be an ungraceful shutdown/restart, and the filesystem may become corrupted. The ungraceful shutdown will be displayed in the system-history.log. You are instead recommended to gracefully shutdown/restart via utils system shutdown CLI command (this will be displayed in the system-history.log as a graceful shutdown/restart).

Caution Unified Communications Manager and IM and Presence Service identifies an ungraceful shutdown/restart. A rebuild of such systems is highly recommended to ensure that there are no negative impacts such as corruption of configuration data or the filesystem itself. The administrator is notified on GUI and CLI login and a SyslogSeverityMatchFound alert is triggered until the system is rebuilt or upgraded. For more information on rebuild instruction, see Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Settings** > **Version**.

Step 2 Perform one of the following actions:

- Click **Shutdown** to stop all processes and shut down the system.
- Click **Restart** to stop all processes and restart the system.