Introduction

Cisco CallManager serves as the software-based call-processing component of the Cisco Communications family of products. A wide range of Cisco Media Convergence Servers provides high-availability server platforms for Cisco CallManager call processing, services, and applications.

The Cisco CallManager system extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications. Additional data, voice, and video services, such as unified messaging, multimedia conferencing, collaborative contact centers, and interactive multimedia response systems, interact through Cisco CallManager open telephony application programming interface (API).

Cisco CallManager provides signaling and call control services to Cisco integrated telephony applications as well as third-party applications. It performs the following primary functions:

- Call processing
- Signaling and device control
- Dial plan administration
- Phone feature administration
- Directory services
- Operations, administration, maintenance, and provisioning (OAM&P)
- Programming interface to external voice-processing applications such as Cisco IP Communicator, Cisco IP Interactive Voice Response (IP IVR), and Cisco CallManager Attendant Console

Additional Information

See the "Related Topics" section on page 1-8.

Key Features and Benefits

The Cisco CallManager system includes a suite of integrated voice applications that perform voice-conferencing and manual attendant console functions. This suite of voice applications means that no need exists for special-purpose voice-processing hardware. Supplementary and enhanced services such as hold, transfer, forward, conference, multiple line appearances, automatic route selection, speed dial, last-number redial, and other features extend to IP phones and gateways. Because Cisco CallManager is a software application, enhancing its capabilities in production environments requires only upgrading software on the server platform, thereby avoiding expensive hardware upgrade costs.

Distribution of Cisco CallManager and all Cisco IP Phones, gateways, and applications across an IP network provides a distributed, virtual telephony network. This architecture improves system availability and scalability. Call admission control ensures that voice quality of service (QoS) is maintained across constricted WAN link and automatically diverts calls to alternate public switched telephone network (PSTN) routes when WAN bandwidth is not available.

A web-browsable interface to the configuration database provides the capability for remote device and system configuration. This interface also provides access to HTML-based online help for users and administrators.

Cisco CallManager release 5.0, designed to work like an appliance, refers to the following functions:

- Cisco CallManager servers can get preinstalled with software to ease customer and partner deployment and automatically search for updates and notify administrators when key security fixes and software upgrades are available for their system.This process comprises Electronic Software Upgrade Notification.
- You can upgrade Cisco CallManager servers while they continue to process calls, so upgrades take place with minimal downtime.
- Cisco CallManager supports the Asian and Middle Eastern markets by providing support for Unicode on higher resolution phone displays.
- Cisco CallManager provides Fault, Configuration, Accounting, Performance, and Security (FCAPS).

Additional Information

See the "Related Topics" section on page 1-8.

Browsing to Cisco CallManager Administration

You access the Cisco CallManager Administration program from a PC that is not the web server or has Cisco CallManager installed. No browser software exists on the server. See the "Web Browsers" section on page 1-2 for more information on browsing to the server.

Additional Information

See the "Related Topics" section on page 1-8.

Web Browsers

Cisco CallManager Administration supports the following Microsoft Windows operating system browsers:

- Microsoft Internet Explorer (IE) 6.0 or higher
- Netscape 7.1 or higher

From any user PC in your network, browse into a server that is running Cisco CallManager Administration and log in with administrative privileges.

Note Simultaneous logon to Cisco CallManager Administration by a large number of users can cause performance to suffer. Try to limit the number of users and administrators that are logged on simultaneously.

Cisco CallManager Administration Logon

Use the following procedure to log on to Cisco CallManager Administration.

Procedure

Use the following procedure to browse into the server and log on to Cisco CallManager Administration.

Step 1 Start your preferred operating system browser.

Step 2 In the address bar of the web browser, enter the following case-sensitive URL:

https://<*CCM-server-name*>:{8443}/ccmadmin/showHome.do

where: <*CCM-server-name*> equals the name or IP address of the server

Note You can optionally specify a port number.

Step 3 A Security Alert dialog box displays. Click the appropriate button.

Step 4 At the Logon window, enter the application user password that you specified during Cisco CallManager installation and click **Submit**.

The Cisco CallManager Administration window displays (see Figure 1-1).

Note For security purposes, Cisco CallManager Administration logs you out after 30 minutes, and you must log back in.

Additional Information

See the "Related Topics" section on page 1-8.

Cisco CallManager Administration Log Off

Procedure

Use the following procedure to log off Cisco CallManager Administration.

Step 1 From the main Cisco CallManager Administration window, click the **Log Off** button that is in the upper, right corner (see Figure 1-1).

Step 2 The Logon window displays.

Additional Information

See the "Related Topics" section on page 1-8.

Hypertext Transfer Protocol Over Secure Sockets Layer (HTTPS)

Hypertext Transfer Protocol over Secure Sockets Layer (SSL), which secures communication between the browser client and the web server (for Microsoft Windows users), uses a certificate and a public key to encrypt the data that is transferred over the internet. HTTPS also ensures that the user login password transports securely via the web. The following Cisco CallManager applications support HTTPS, which ensures the identity of the server: Cisco CallManager Administration, Cisco CallManager Serviceability, the Cisco CallManager User Options, Trace Collection Tool, the Real-Time Monitoring Tool (RTMT), and the XML (AXL) application programming interface.

A self-signed certificate gets generated on the web server at installation (the certificate also gets migrated during upgrades).

Note If you access the web application by using the hostname and install the certificate in the trusted folder and then try to access the application by using the localhost or IP address, the Security Alert dialog box displays to indicate that the name of the security certificate does not match the name of the site.

If you use the localhost, the IP address, or the hostname in the URL to access the application that supports HTTPS, you must save the certificate in the trusted folder for each of type of URL (with the local host, IP address, and so on); otherwise, the Security Alert dialog box displays for each type.

Using Internet Explorer and HTTPS with Cisco CallManager Administration

The following section describes how to save the CA Root certificate in the trusted folder, so the Security Alert dialog box does not display each time that you access the web application. The first time that you (or a user) accesses Cisco CallManager Administration or other Cisco CallManager SSL-enabled virtual directories after the Cisco CallManager 5.0 installation/upgrade from a browser client, a Security Alert dialog box asks whether you trust the server. When the dialog box displays, you must perform one of the following tasks:

- By clicking Yes, you choose to trust the certificate for the current web session only. If you trust the certificate for the current session only, the Security Alert dialog box displays each time that you access the application; that is, until you install the certificate in the trusted folder.
- By clicking View Certificate > Install Certificate, you indicate that you intend to perform certificate installation tasks, so you always trust the certificate. If you install the certificate in the trusted folder, the Security Alert dialog box does not display each time that you access the web application.
- By clicking No, you cancel the action. No authentication occurs, and you cannot access the web application. To access the web application, you must click Yes or install the certificate via the View Certificate > Install Certificate option.

For other tasks that you can perform in the Security Alert dialog box, refer to the *Cisco CallManager Security Guide*.

Procedure

Step 1 Browse to the application on the web server.

Step 2 When the Security Alert dialog box displays, click **View Certificate**.

Step 3 In the Certificate pane, click **Install Certificate**.

Step 4 Click **Next**.

Step 5 Click the **Place all certificates in the following store** radio button; click **Browse**.

Step 6 Browse to **Trusted Root Certification Authorities**.

Step 7 Click **Next**.

Step 8 Click **Finish**.

Step 9 To install the certificate, click **Yes**.

A message states that the import was successful. Click **OK**.

Step 10 In the lower, right corner of the dialog box, click **OK**.

Step 11 To trust the certificate, so you do not receive the dialog box again, click **Yes**.

Note If you use the localhost, the IP address, or the hostname in the URL to access the application that supports HTTPS, you must save the certificate in the trusted folder for each of type of URL (with the local host, IP address, and so on); otherwise, the Security Alert dialog box displays for each type.

Additional Information

See the "Related Topics" section on page 1-8.

Using Netscape and HTTPS with Cisco CallManager Administration

When you use HTTPS with Netscape, you can view the certificate credentials, trust the certificate for one session, trust the certificate until it expires, or not trust the certificate at all.

Tip If you trust the certificate for one session only, you must repeat the following procedure each time that you access the HTTPS-supported application. If you do not trust the certificate, you cannot access the application.

Perform the following procedure to save the certificate to the trusted folder:

Procedure

Step 1 Browse to the application, for example, Cisco CallManager Administration, by using Netscape.

The certificate authority dialog box displays.

Step 2 Click one of the following radio buttons:

- Accept this certificate for this session
- Do not accept this certificate and do not connect
- Accept this certificate forever (until it expires)

Note If you choose Do not accept, the application does not display.

Note To view the certificate credentials before you continue, click **Examine Certificate**. Review the credentials, and click **Close**.

Step 3 Click **OK**.

The Security Warning dialog box displays.

Step 4 Click **OK**.

Additional Information

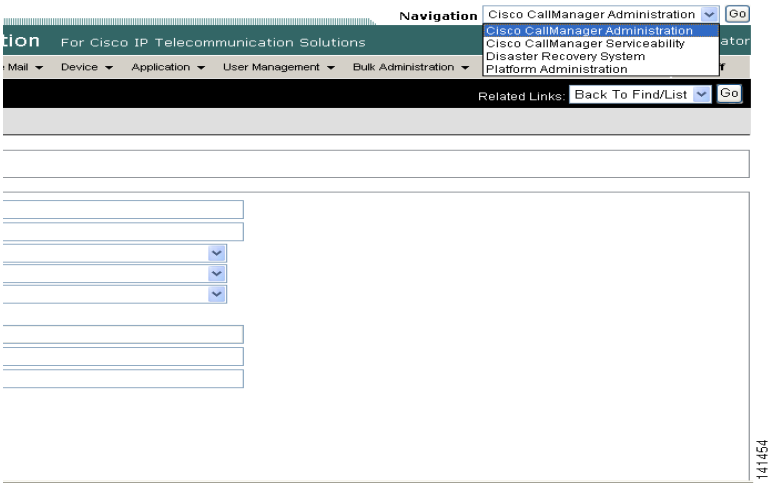
See the "Related Topics" section on page 1-8.

Navigating the Cisco CallManager Administration Application

After you log on, the main Cisco CallManager Administration window displays. The window includes the drop-down list box in the upper, right corner called **Navigation** (see Figure 1-1). To access the applications in the drop-down list box, choose the program that you want and click **Go**. The choices in the drop-down list box include the following Cisco CallManager applications:

- Cisco CallManager Administration—Shows the default when you access Cisco CallManager. Use Cisco CallManager Administration to configure system parameters, route plans, devices, and much more.
- Cisco CallManager Serviceability—Takes you to the main Cisco CallManager Serviceability window that is used to configure trace files and alarms and to activate and deactivate services.
- Disaster Recovery System—Takes you to the Cisco Disaster Recovery System, a program that provides full data backup and restore capabilities for all servers in a Cisco CallManager cluster.
- Platform Administration—Takes you to a logon window, so you can configure and administer the Cisco CallManager platform.

Figure 1-1 Cisco CallManager Administration Navigation



These applications include additional security, so you must enter a userid and password before you can access these programs.

Additional Information

See the "Related Topics" section on page 1-8.

Accessibility

Cisco CallManager Administration and Cisco CallManager User Options provide functionality for users that allows them to access buttons on the window without using a mouse. You can perform the following procedures from any point on the window, so the user does not have to scroll or tab through various fields.

Accessing the Icons in the Window

Many of the windows in Cisco CallManager and Cisco PCA have icons that display at the top of the window; for example, an icon of a disk for Save, an icon that is a plus sign (+) for Add, and so on. To access these icons, perform the following procedure.

1. Press **Alt**, press **1**, then press **Tab**. The cursor will highlight the first icon from the left. To move to the next icon, press **Tab** again.
2. Press **Enter**. The system performs the function of the icon; for example, Add.

Accessing the Buttons in the Window

Many of the windows in Cisco CallManager and Cisco PCA have buttons that display at the bottom of the window; for example, a button for Save, a button for Add, and so on. To access these buttons, perform the following procedure.

1. Press **Alt**, press **2**, and then press **Tab**. The cursor will highlight the first button from the left. To move to the next button, press **Tab** again.
2. Press **Enter**. The function of the button gets performed; for example, Save.

Where to Find More Information

- *Cisco CallManager System Guide*
- *Cisco CallManager Features and Services Guide*
- *Cisco CallManager Serviceability System Guide*
- *Cisco CallManager Serviceability Administration Guide*
- *Cisco CDR Analysis and Reporting Administration Guide*
- *Cisco IP Telephony Solution Reference Network Design Guide*
- *Installing Cisco CallManager Release 5.0(1)*
- *Upgrading Cisco CallManager Release 5.0(1)*
- *Cisco CallManager Security Guide 5.0*
- *Cisco IP Telephony Platform Administration Guide*
- *Cisco IP Telephony Disaster Recovery System Administration Guide*

Related Topics