



Introduction

Cisco CallManager serves as the software-based call-processing component of the Cisco IP Telephony Solutions for the Enterprise, part of Cisco AVVID (Architecture for Voice, Video and Integrated Data). The Cisco IP Telephony Applications Server provides a high-availability server platform 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 SoftPhone, Cisco IP Interactive Voice Response (IP IVR), Cisco Personal Assistant, and Cisco CallManager Attendant Console

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 only requires 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.

Browsing to Cisco CallManager Administration

Cisco recommends that you access the Cisco CallManager Administration program from a PC that is not on the same machine as the Web Server or Cisco CallManager program.

Web Browsers

**Caution**

A web browser as a resource-intensive application may consume large amounts of system memory and CPU cycles. When the web browser takes resources away from Cisco CallManager, it adversely affects call processing. Possible consequences of using the browser on the same machine as the Web Server and Cisco CallManager include delayed dial tone and dropped calls.

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

- Netscape Communicator 4.X
- Microsoft Internet Explorer 5 or 6

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 web page performance to suffer. Try to limit the number of users and administrators that are logged on simultaneously.

Procedure

Use the following procedure to browse into the server.

-
- Step 1** Start your preferred Microsoft Windows operating system browser.
- Step 2** In the address bar of the web browser, enter the following URL:
`http://<CCM-server-name>/CCMAdmin/main.asp`
where: <CCM-server-name> equals the name or IP address of the server
- Step 3** Log in with your assigned administrative privileges.
-

Java Runtime Environment

Cisco CallManager requires that a Java Runtime Environment (JRE) be installed and configured on the local PC that is browsing into Cisco CallManager Administration. In addition, the browser security must have Java enabled.

To obtain the JRE for the local PC, go to the C:\utils\JRE directory, copy the J2RE_Client.zip file onto the local PC, unzip the file, and run the executable.



Note

To obtain the JRE in the preceding directory, you must be running Microsoft OS version 2000.2.6 or later on the Cisco CallManager server.

When using Microsoft Internet Explore, a window displays asking for the userid and password. When SUN JRE is used in IE, there will be a second login window prompt for user name and password from JRE. Click the remember password button to always use that password; however, security may become an issue because the password would always be available. If you do not set remember password, you will have to enter the password every time this window displays.

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 IIS server, 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 IP Phone User Option Pages, the Bulk Administration Tool (BAT), TAPS, Cisco CDR Analysis and Reporting (CAR), Trace Collection Tool, and the Real Time Monitoring Tool.

When you install/upgrade Cisco CallManager, the HTTPS self-signed certificate, https-cert.cer, automatically installs on the IIS default website that hosts the Cisco CallManager virtual directories, which include CCMAAdmin, CCMService, CCMUser, AST, BAT, RTMTReports, CCMTraceAnalysis, PktCap, ART, and CCMServiceTraceCollectionTool. The HTTPS certificate gets stored in the C:\Program Files\Cisco\Certificates directory. If you prefer to do so, you can install a server authentication certificate from a certificate authority and use it instead of the HTTPS self-signed certificate. To use the certificate authority

certificate after the Cisco CallManager installation/upgrade, you must delete the self-signed certificate, as described in the *Cisco CallManager Security Guide*. Then, you install the server authentication certificate that is provided by the certificate authority, as described in the certificate authority documentation.

**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 4.1 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 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 options.

For other tasks that you can perform in the Security Alert dialog box, refer to the *Cisco CallManager Security Guide 4.1*:

Procedure

- Step 1 Browse to the application on the IIS 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.

Related Topics

- [Using Internet Explorer and HTTPS with Cisco CallManager Administration, page 1-5](#)
- [Hypertext Transfer Protocol over Secure Sockets Layer \(HTTPS\), page 1-4](#)
- *Cisco CallManager Security Guide*

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** Access the application, for example, Cisco CallManager Administration, through Netscape.
- Step 2** After the New Site Certificate window displays, click **Next**.
- Step 3** After the next New Site Certificate window displays, click **Next**.

**Tip**

To view the certificate credentials before you click **Next**, click **More Info**. Review the credentials, and click **OK**.; then, click **Next** in the New Site Certificate window.

- Step 4** 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)
- Step 5** Click **Next**.
- Step 6** If you clicked the Do not accept this certificate... radio button, go to [Step 8](#).
- Step 7** If you want Netscape to warn you before sending information to other sites, check the **Warn me before I send information to this site** check box; then, click **Next**.
- Step 8** Click **Finish**.
-

Related Topics

- [Hypertext Transfer Protocol over Secure Sockets Layer \(HTTPS\), page 1-4](#)
- [Using Netscape and HTTPS with Cisco CallManager Administration, page 1-7](#)
- *Cisco CallManager Security Guide*

Where to Find More Information

- *Cisco CallManager System Guide*
- *Cisco IP Telephony Solution Reference Network Design Guide*
- *Installing Cisco CallManager*
- *Upgrading Cisco CallManager*
- *Cisco CallManager Security Guide 4.1*