



CHAPTER 2

Using Cisco Unified Serviceability

This chapter comprises the following topics:

- [Accessing Cisco Unified Serviceability, page 2-1](#)
- [Installing the Server Certificate, page 2-2](#)
- [Using the Cisco Unified Serviceability Interface, page 2-6](#)
- [Using Accessibility Features, page 2-8](#)
- [Where to Find More Information, page 2-8](#)

Accessing Cisco Unified Serviceability

You can access the Serviceability application

- by entering **https://<server name or IP address>:8443/ccmservice/** in a browser window and then entering a valid username and password.
- by choosing **Cisco Unified Serviceability** in the Navigation menu in the Cisco Unified Communications Manager Administration console.
- by choosing **Application > Serviceability Webpage** in the Real-Time Monitoring Tool (RTMT) menu and then entering a valid username and password
- by choosing **Cisco Unified Serviceability** in the Navigation menu in Cisco Unity Connection.



Tip

After you log in to Cisco Unified Serviceability, you can access all administrative applications that display in the Navigation menu, except for Cisco Unified OS Administration and Disaster Recovery System, without logging in again. The web pages that you can access within Cisco Unified Serviceability depend on your assigned roles and privileges. Cisco Unified OS Administration and Disaster Recovery System require a separate authentication procedure.

The system uses the Cisco Tomcat service to authenticate users before allowing access to the web application.



Tip

Unified CM and Unified CM BE only: Any user who has the “Standard CCM Admin Users” role assigned can access Cisco Unified Serviceability. For information on how to assign this role to a user, refer to the *Cisco Unified Communications Manager Administration Guide*.

**Tip**

Connection only: Any user who has the System Administrator role or Technician role assigned can access Cisco Unified Serviceability. For information on how to assign this role to a user, refer to the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

If you get a security alert that the site is not trusted, this indicates that the server certificate has not yet downloaded.

To access Cisco Unified Serviceability, perform the following procedure:

Procedure

Step 1 In a supported browser, browse to the server where the Cisco Unified Serviceability service runs.

**Tip**

In the supported browser, enter **https://<server name or IP address>:8443/ccmservice/**, where server name or IP address equals the server where the Cisco Unified Serviceability service runs and 8443 equals the port number for HTTPS.

If you enter **http://<server name or IP address>:8080** in the browser, the system redirects you to use HTTP. HTTP uses the port number, 8080.

Step 2 If the system prompts you about certificates, see the [“Installing the Server Certificate” section on page 2-2](#).

Step 3 Enter a valid username and password; click **Login**.

To clear the username and password, click **Reset**.

Additional Information

See the [“Related Topics” section on page 2-8](#).

Installing the Server Certificate

This section contains information on the following topics:

- [HTTPS Overview for Internet Explorer, page 2-3](#)
- [Installing the Certificate with Internet Explorer 6, page 2-3](#)
- [Installing the Certificate with Internet Explorer 7, page 2-4](#)
- [Installing the Certificate with Netscape, page 2-5](#)

**Note**

For additional information about using HTTPS with Cisco Unified Communications Manager, refer to *Cisco Unified Communications Manager Security Guide*.

Hypertext Transfer Protocol over Secure Sockets Layer (SSL), which secures communication between the browser client and the Tomcat web server, uses a certificate and a public key to encrypt the data that is transferred over the internet. HTTPS, which ensures the identity of the server, supports applications, such as Cisco Unified Serviceability. HTTPS also ensures that the user login password transports securely via the web.

**Note**

Due to the way IE 7 handles certificates, this browser displays an error status after you import the server certificate. This status persists if you reenter the URL or refresh or relaunch the browser and does not indicate an error. Refer to the [“Installing the Certificate with Internet Explorer 7” section on page 2-4](#) for more information.

HTTPS Overview for Internet Explorer

On the first attempt to access Cisco Unified Serviceability, a Security Alert dialog box, which indicates that the server is not trusted because the server certificate does not exist in the trusted folder, displays. When the dialog box displays, 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.

**Note**

The system issues the certificate by using the hostname. If you attempt to access a web application by using the IP address, the Security Alert dialog box displays, even though you installed the certificate.

Additional Information

See the [“Related Topics” section on page 2-8](#).

Installing the Certificate with Internet Explorer 6

Perform the following procedure to save the HTTPS certificate in the trusted folder.

Procedure

- Step 1** Browse to the application on the Tomcat web server.
- Step 2** When the Security Alert dialog box displays, click **View Certificate**. To verify certificate details, click the **Details** tab.
- Step 3** In the Certificate pane, click **Install Certificate**.
- Step 4** When the Certificate Import Wizard displays, 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**; select it and click **OK**.
- Step 7** Click **Next**.
- Step 8** Click **Finish**.
- A Security Warning Box displays the certificate thumbprint for you.
- 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**.

**Tip**

You can verify the certificate was installed successfully by clicking the Certification Path tab in the Certificate pane.

Additional Information

See the [“Related Topics” section on page 2-8](#).

Installing the Certificate with Internet Explorer 7

Internet Explorer 7 adds security features that change the way that the browser handles Cisco certificates for website access. Because Cisco provides a self-signed certificate for the Cisco Unified Communications Manager or Cisco Unity Connection server, Internet Explorer 7 flags the Cisco Unified Communications Manager Administration or Cisco Unity Connection website as untrusted and provides a certificate error, even when the trust store contains the server certificate.

**Note**

Internet Explorer 7, which is a Windows Vista feature, also runs on Windows XP Service Pack 2 (SP2), Windows XP Professional x64 Edition, and Windows Server 2003 Service Pack 1 (SP1). Java Runtime Environment (JRE) must be present to provide Java-related browser support for IE.

Be sure to import the Cisco Unified Communications Manager or Cisco Unity Connection certificate to Internet Explorer 7 to secure access without having to reload the certificate every time that you restart the browser. If you continue to a website that has a certificate warning and the certificate is not in the trust store, Internet Explorer 7 remembers the certificate for the current session only.

After you download the server certificate, Internet Explorer 7 continues to display certificate errors for the website. You can ignore the security warnings when the Trusted Root Certificate Authority trust store for the browser contains the imported certificate.

The following procedure describes how to import the Cisco Unified Communications Manager or Cisco Unity Connection certificate to the root certificate trust store for Internet Explorer 7.

Procedure

- Step 1** Browse to application on the Tomcat server by entering the hostname (server name) or IP address in the browser.

The browser displays a Certificate Error: Navigation Blocked message to indicate that this website is untrusted.

Step 2 To access the server, click **Continue to this website (not recommended)**

The administration window displays, and the browser displays the address bar and Certificate Error status in red.

Step 3 To import the server certificate, click the Certificate Error status box to display the status report. Click the **View Certificates** link in the report.

Step 4 Verify the certificate details.

The Certification Path tab displays “This CA Root certificate is not trusted because it is not in the Trusted Root Certification Authorities store.”

Step 5 Select the General tab in the Certificate window and click **Install Certificate**.

The Certificate Import Wizard launches.

Step 6 To start the Wizard, click **Next**.

The Certificate Store window displays.

Step 7 Verify that the Automatic option, which allows the wizard to select the certificate store for this certificate type, is selected and click **Next**.

Step 8 Verify the setting and click **Finish**.

A security warning displays for the import operation.

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

The Import Wizard displays “The import was successful.”

Step 10 Click **OK**. The next time that you click the View certificates link, the Certification Path tab in the Certificate window displays “This certificate is OK.”

Step 11 To verify that the trust store contains the imported certificate, click **Tools > Internet Options** in the Internet Explorer toolbar and select the Content tab. Click **Certificates** and select the Trusted Root Certifications Authorities tab. Scroll to find the imported certificate in the list.

After importing the certificate, the browser continues to display the address bar and a Certificate Error status in red. The status persists even if you reenter the hostname or IP address or refresh or relaunch the browser.

Additional Information

See the [“Related Topics” section on page 2-8](#).

Installing the Certificate with Netscape

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.

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

**Note**

The address that you use to access Cisco Unified Communications Manager or Cisco Unity Connection must match the name on the certificate or a message will display by default. If you access the web application by using the IP address after you install the certificate in the trusted folder, a security alert indicates that the name of the security certificate does not match the name of the site that you are accessing.

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

Procedure

Step 1 Browse to the application, for example, Cisco Unified Serviceability, 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 Cisco Unified Serviceability 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 2-8](#).

Using the Cisco Unified Serviceability Interface

In addition to performing troubleshooting and service-related tasks in Cisco Unified Serviceability, you can perform the following tasks:

- *Unified CM and Unified CM BE only:* To access Dialed Number Analyzer to test and diagnose a deployed Cisco Unified Communications Manager dial plan configuration, analyze the test results and use the results to tune the dial plan, activate the Cisco Dialed Number Analyzer service by choosing **Tools > Service Activation** and choosing **Tools > Dialed Number Analyzer**. For more information on how to use the Dialed Number Analyzer, refer to the *Cisco Unified Communications Manager Dialed Number Analyzer Guide*.

- *Unified CM and Unified CM BE only:* To access Cisco Unified Communications Manager CDR Analysis and Reporting from **Tools > CDR Analysis and Reporting**, perform the required procedures, as described in the *CDR Analysis and Reporting Administration Guide*.

**Note**

You cannot access the Cisco Unified Communications Manager CDR Analysis and Reporting tool unless you are a member of the Cisco CAR Administrators user group. Refer to the “Configuring the CDR Analysis and Reporting Tool” chapter in the *CDR Analysis and Reporting Administration Guide* for information on how to become a member of the Cisco CAR Administrators user group.

- To display documentation for a single window, choose **Help > This Page** in Cisco Unified Serviceability.
- To display a list of documents that are available with this release (or to access the online help index), choose **Help > Contents** in Cisco Unified Serviceability.
- To verify the version of Cisco Unified Serviceability that runs on the server, choose **Help > About** or click the **About** link in the upper, right corner of the window.
- To go directly to the home page in Cisco Unified Serviceability from a configuration window, choose **Cisco Unified Serviceability** from the Navigation drop-down list box in the upper, right corner of the window.

**Note**

In some scenarios, you cannot access the Cisco Unified Serviceability from Cisco Unified OS Administration. A “Loading, please wait” message displays indefinitely. If the redirect fails, log out from Cisco Unified OS Administration, select Cisco Unified Serviceability from the navigation menu, and log in to Cisco Unified Serviceability.

- To access other application GUIs, choose the appropriate application from the Navigation drop-down list box in the upper, right corner of the window; then, click **Go**.
- To log out of Cisco Unified Serviceability, click the **Logout** link in the upper, right corner of the Cisco Unified Serviceability window.
- In each Cisco Unified Serviceability configuration window, configuration icons display that correspond to the configuration buttons at the bottom of the window; for example, you can either click the Save icon or the Save button to complete the task.

**Tip**

Cisco Unified Serviceability does not support the buttons in your browser. Do not use the browser buttons, for example, the Back button, when you perform configuration tasks.

**Tip**

When a session has been idle for more than 30 minutes, the Cisco Unified Serviceability user interface allows you to make changes before indicating that the session has timed out and redirecting you to the login window. After you log in again, you may have to repeat those changes. This behavior occurs in the Alarm, Trace, Service Activation, Control Center, and SNMP windows. If you know that the session has been idle for more than 30 minutes, log out by using the Logout button before making any changes in the user interface.

Using Accessibility Features

Cisco Unified Serviceability provides functionality for users that allows them to access buttons on the window without using a mouse. These navigation shortcuts assist visually impaired or blind attendants to use the application.

Use [Table 2-1](#) as a guide for navigating the interface by using keyboard shortcuts.

Table 2-1 **Navigation Shortcuts for Cisco Unified Serviceability**

Keystroke	Action
Alt	Moves focus to the browser menu bar.
Enter	Chooses the item with focus (menu option, button, and so on.)
Alt, arrow keys	Moves between browser menus.
Alt+underlined letter	Takes you to the menu; for example, Alt+A moves you to the Alarms menu.
Spacebar	Toggles control; for example, checks and unchecks a check box.
Tab	Moves focus to the next item in the tab order or to next control group.
Shift+Tab	Moves focus to the previous item or group in the tab order.
Arrow keys	Moves among controls within a group.
Home	Moves to the top of the window if more than one screenful of information exists. Also, moves to the beginning of a line of user-entered text.
End	Moves to the end of a line of user-entered text. Moves to the bottom of the window if more than one screenful of information exists.
Page Up	Scrolls up one screen.
Page Down	Scrolls down one screen.

Where to Find More Information

Related Topics

- [Accessing Cisco Unified Serviceability, page 2-1](#)
- [Installing the Server Certificate, page 2-2](#)
- [Using the Cisco Unified Serviceability Interface, page 2-6](#)
- [Using Accessibility Features, page 2-8](#)

Additional Cisco Documentation

- *Unified CM and Unified CM BE only: Cisco Unified Communications Manager Administration Guide*

- *Unified CM and Unified CM BE only: Cisco Unified Communications Manager System Guide*
- *Unified CM and Unified CM BE only: Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide*
- *Unified CM and Unified CM BE only: Cisco Unified Communications Manager Security Guide*
- *Unified CM and Unified CM BE only: CiscoWorks Lan Management Solution user documentation*
- *Cisco Unified Real-Time Monitoring Tool Administration Guide*
- *Unified CM BE and Connection only: Cisco Unity Connection Serviceability Administration Guide*
- *Unified CM BE and Connection only: System Administration Guide for Cisco Unity Connection*

