



Cisco Unified Mobility Advantage Server Security Profile Setup

This chapter provides information about Cisco Unified Mobility Advantage server security profile setup.

- [About Cisco Unified Mobility Advantage Server Security Profile Setup, on page 1](#)
- [Find Cisco Unified Mobility Advantage Server Security Profile, on page 2](#)
- [Set Up Cisco Unified Mobility Advantage Server Security Profile, on page 2](#)
- [Cisco Unified Mobility Advantage Server Security Profile Settings, on page 3](#)
- [Cisco Unified Mobility Advantage Server Security Profile Client Application, on page 4](#)
- [Delete Cisco Unified Mobility Advantage Server Security Profile, on page 4](#)
- [Where to Find More Information About Cisco Unified Mobility Advantage Server Security Profile, on page 5](#)

About Cisco Unified Mobility Advantage Server Security Profile Setup

Unified Communications Manager Administration groups security-related settings to allow you to assign a single security profile to multiple Mobile Communicator clients. Security-related settings include device security mode, incoming transport type, and X.509 subject name. Configuring a Cisco Unified Mobility Advantage server security profile in Unified Communications Manager Administration automatically applies this profile to all configured Mobile Communicator clients on that Unified Communications Manager.

Only the security features that the Cisco Unified Mobility Advantage server supports display in the security profile settings window.



Note You cannot configure Cisco Unified Mobility Advantage servers in Unified Communications Manager Assistant Administration. For information on setting up a security profile for a Cisco Unified Mobility Advantage server, refer to your Cisco Unified Mobility Advantage documentation. Make sure that the Cisco Unified Mobility Advantage Security Profile you configure on Unified Communications Manager matches the security profile on the Cisco Unified Mobility Advantage servers. For information on configuring a Cisco Unity Cisco Unified Mobility Advantage server security profile, see the *Cisco Unified Communications Manager Security Guide*.

Find Cisco Unified Mobility Advantage Server Security Profile

To find a Cisco Unified Mobility Advantage server security profile, perform the following procedure:

Procedure

- Step 1** In Unified Communications Manager Administration, choose **System > Security Profile > CUMA Server Security Profile**.
- The Find and List CUMA Server Security Profile window displays. Records from an active (prior) query may also display in the window.
- Step 2** To find all records in the database, ensure the dialog box is empty; go to [Step 3, on page 2](#).
- To filter or search records
- From the first drop-down list box, choose a search parameter.
 - From the second drop-down list box, choose a search pattern.
 - 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 3** Click **Find**.
- All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.
- Step 4** From the list of records that display, click the link for the record that you want to view.
- Note** To reverse the sort order, click the up or down arrow, if available, in the list header.
- The window displays the item that you choose.
-

Set Up Cisco Unified Mobility Advantage Server Security Profile

To add, update, or copy a security profile, perform the following procedure:

Procedure

- Step 1** In Unified Communications Manager Administration, choose **System > Security Profile > CUMA Server Security Profile**.
- Step 2** Perform one of the following tasks:

- a) To add a new profile, click **Add New** in the **Find** window and continue with [Cisco Unified Mobility Advantage Server Security Profile Setup, on page 1](#).
- b) To copy an existing security profile, locate the appropriate profile and click the **Copy** button next to the security profile that you want to copy, and continue with [Cisco Unified Mobility Advantage Server Security Profile Setup, on page 1](#).
- c) To update an existing profile, locate the appropriate security profile and continue with [Cisco Unified Mobility Advantage Server Security Profile Setup, on page 1](#).

When you click **Add New**, the configuration window displays with the default settings for each field. When you click **Copy**, the configuration window displays with the copied settings.

Step 3 Enter the appropriate settings as described in [Table 1: Security Profile Settings, on page 3](#)

Step 4 Click **Save**.

Cisco Unified Mobility Advantage Server Security Profile Settings

The following table describes the settings for the Cisco Unified Mobility Advantage Server security profiles.

Table 1: Security Profile Settings

| Setting | Description |
|----------------------|---|
| Name | Enter a name for the security profile. Tip Include the device model in the security profile name to help you find the correct profile when you are searching for or updating a profile. |
| Description | Enter a description for the security profile. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>). |
| Device Security Mode | From the drop-down list box, choose one of the following options: <ul style="list-style-type: none"> • Non Secure—No security features except image authentication exist for the Cisco Unified Mobility Advantage server. A TCP connection opens to Unified Communications Manager. • Authenticated—Unified Communications Manager provides integrity and authentication for the Cisco Unified Mobility Advantage server. A TLS connection that uses NULL/SHA opens for signaling. • Encrypted—Unified Communications Manager provides integrity, authentication, and encryption for the Cisco Unified Mobility Advantage server. A TLS connection that uses AES128/SHA opens for signaling, and SRTP carries the media for all mobile calls. |

| Setting | Description |
|--|--|
| Transport Type | <p>When Device Security Mode is Non Secure, choose the following option from the drop-down list box:</p> <ul style="list-style-type: none"> • TCP—Choose the Transmission Control Protocol to ensure that packets get received in the same order as the order in which they are sent. This protocol ensures that no packets get dropped, but the protocol does not provide any security. <p>When Device Security Mode is Authenticated or Encrypted, TLS specifies the Transport Type. TLS provides signaling integrity, device authentication, and signaling encryption (encrypted mode only).</p> |
| Secure Certificate Subject or Subject Alternate Name | <p>(Required for Authenticated or Encrypted Device Security Mode setting.) This field applies if you configured TLS as the transport type.</p> <p>Secure Certificate Subject or Subject Alternate Name is an ITU Telecommunication Standardization Sector standard for Public Key Infrastructure in cryptography. The subject name corresponds to the source connection TLS certificate.</p> <p>If multiple Secure Certificate Subject or Subject Alternate Name exists, enter one of the following characters to separate the names: space, comma, semicolon, or a colon.</p> <p>You can enter up to 4096 characters in this field.</p> |

Cisco Unified Mobility Advantage Server Security Profile Client Application

No “Device Security Profile” field exists on the device configuration window for a Mobile Communicator client, which means that you do not have to manually apply the Cisco Unified Mobility Advantage Server Security profile to a client.

Configuring a Cisco Unified Mobility Advantage server security profile in Unified Communications Manager Administration automatically applies this profile to all configured Mobile Communicator clients on that Unified Communications Manager.

Delete Cisco Unified Mobility Advantage Server Security Profile

This section describes how to delete a Cisco Unified Mobility Advantage server security profile from the Unified Communications Manager database.

Procedure

-
- Step 1** Find the security profile to delete.
- Step 2** To delete a security profile, perform the following task:

- a) In the **Find and List** window, check the check box next to the appropriate security profile; then, click **Delete Selected**.

Step 3 When prompted to confirm the delete operation, click **OK** to delete or **Cancel** to cancel the delete operation.

Where to Find More Information About Cisco Unified Mobility Advantage Server Security Profile

