Certificate Setup

This chapter provides information about certificate setup.

About Certificate Setup

Use the Certificate Configuration window to view the certificates on your system. All fields on the Certificate Configuration window are read-only, except Duration in Cache.

Note When a multi-SAN ca-signed certificate is uploaded it is only applied to nodes that are in the cluster at the time the certificate is uploaded to the publisher. Anytime a node is rebuilt or a node is added to the cluster, it is necessary to generate a new multi-SAN Certificate Signing Request (CSR), get it signed by the CA, and upload it to the cluster.

Find Certificate

To find a certificate, perform the following procedure:

Procedure

Step 1 In Unified Communications Manager Administration, choose **System** > **Security** > **Certificate**.

The **Find and List Certificates** 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

a) From the first drop-down list box, choose a search parameter.

b) From the second drop-down list box, choose a search pattern.
c) 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.

Upload Certificate or Certificate Chain

Select and upload a certificate or a cluster-wide certificate to distribute it to all the servers in the selected cluster.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.
The **Certificate List** window appears.

Step 2 Click **Upload Certificate/Certificate chain**.
The **Upload Certificate/Certificate chain** window appears.

Step 3 From the **Certificate Purpose** drop-down box, select a system security certificate, such as **CallManager-ECDSA**.

Step 4 In the **Description** field, enter a name for the certificate.

Step 5 In the **Upload File** field, click **Choose File** to browse for the certificate file that you want to distribute for all the servers in the cluster.

Step 6 Click **Upload**.

Certificate Settings

All fields on the Certificate Management window are read-only, except Duration in Cache.

Table 1: VPN Profile Configuration Settings

Field	Definition
Subject Name (read only)	Displays the subject name for the certificate.
Issuer Name (read only)	Displays the issuer name for the certificate.
Serial Number (read only)	Displays the serial number (MAC address).
IPv4 Address (read only)	Displays the IPv4 address.
IPv6 Address (read only)	Displays the IPv6 address.
Duration in Cache	Enter the time, in hours, that the certificate can persist in the phone cache. A value of zero indicates that the certificate does not get cached. Leave blank to accept the system default value. Maximum: 720 hours
Selected Roles	Displays the roles currently associated with the certificate.
Selected Services	Displays the services currently associated with the certificate.