Unified Communications Manager 7.X Domain Certificate Configuration Example

Document ID: 111843

Contents

Introduction

This document describes how to set up a domain certificate for Cisco Unified Communications Manager.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Unified Communications Manager version 7.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configuration

This example uses the Microsoft certificate authority (CA) for Unified Communication Manager certificates.

Before You Begin

On a Windows domain controller, install the certificate services as an enterprise root CA. In addition, make sure you install the web enrollment as you will need it to generate the certificates.

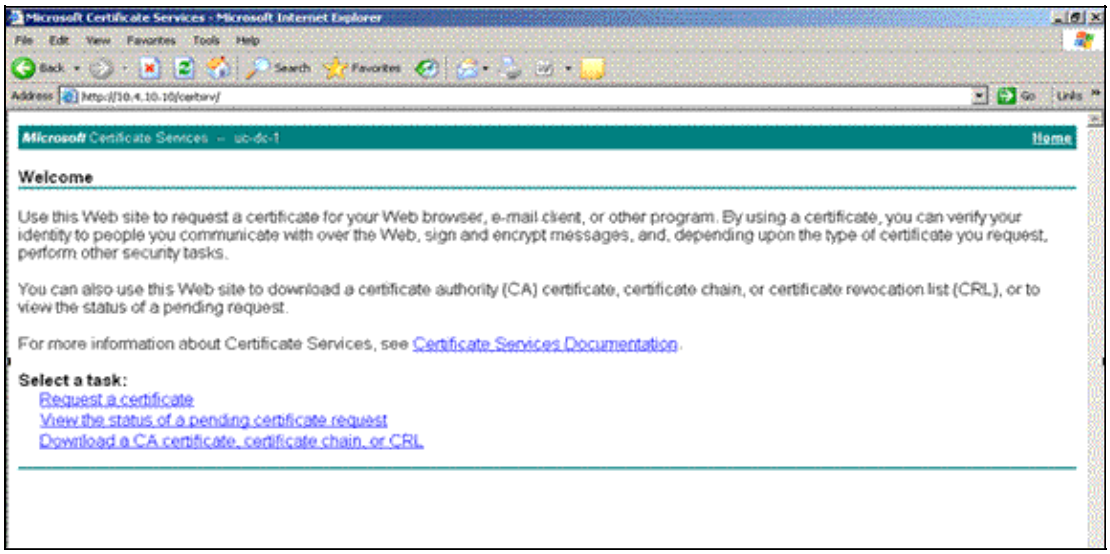
Procedure

1. Download the root certificate from the CA.

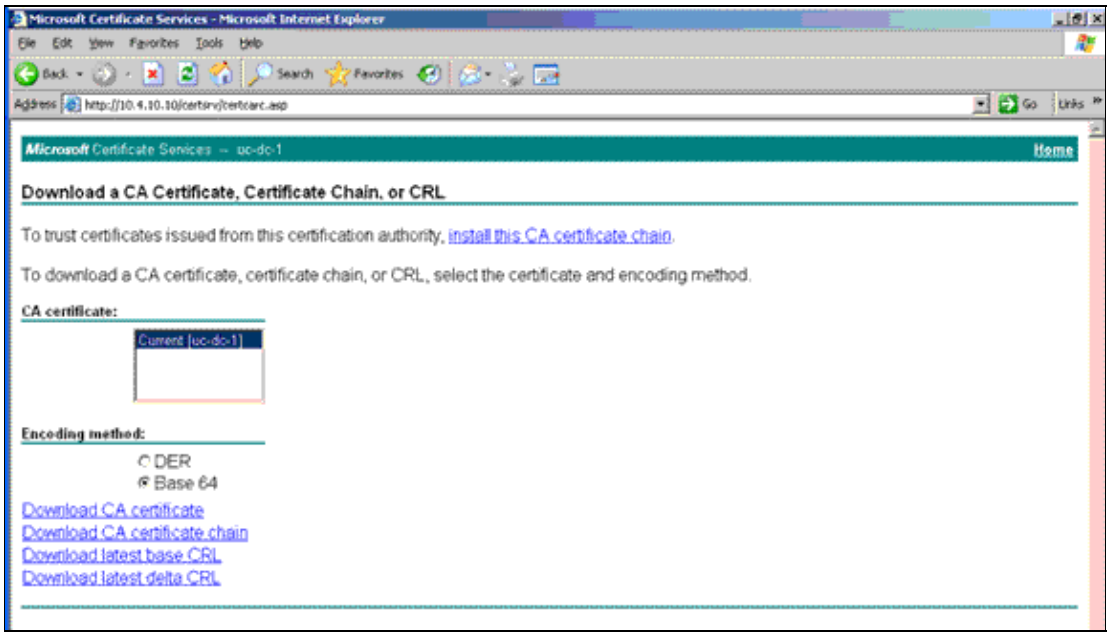
   Note: The certificate must be Active Directory (AD) integrated to generate proper certificates.

   Complete these steps in order to download the root certificate from the CA:

   a. In a web browser, go to http://<*certificate server address*>/certsrv, and click the **Download a CA certificate, certificate chain, or CRL** link.



   b. Click the Base 64 radio button, and then click the **Download CA Certificate** link.



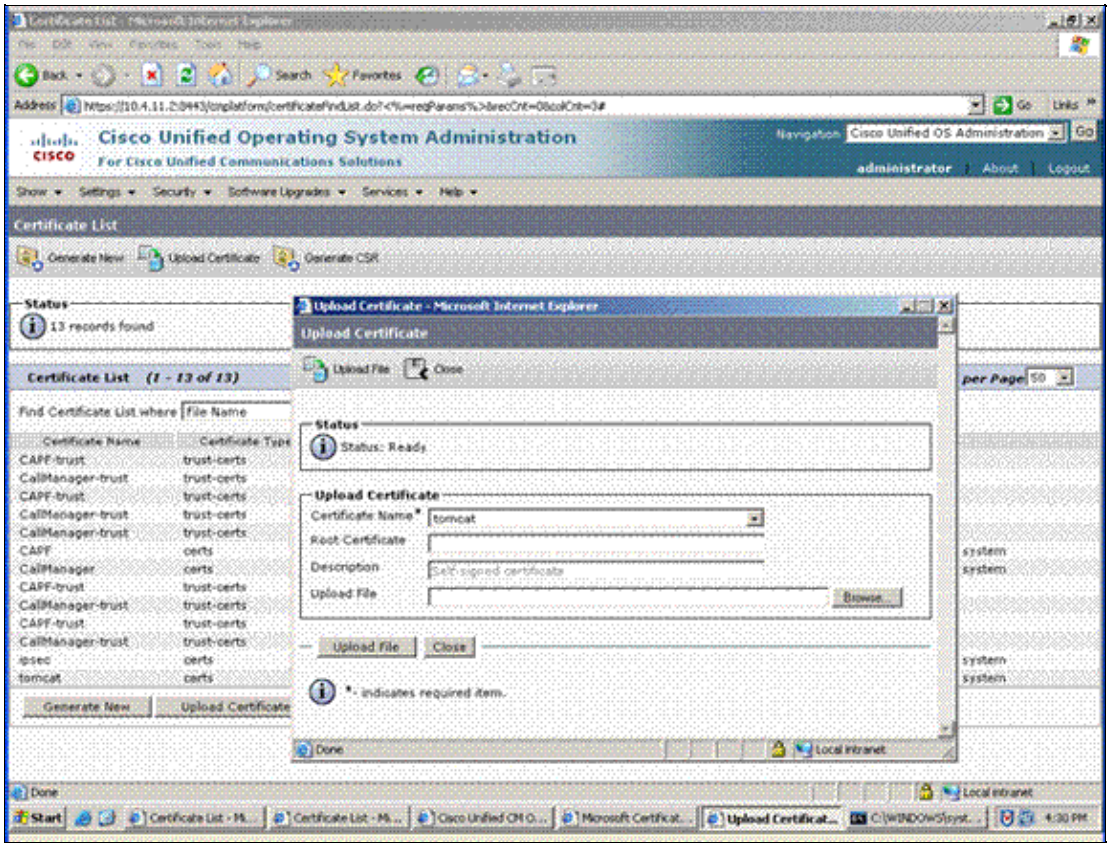
   c. Save the root certificate to your local workstation.

2. Upload the certificate.

   Complete these steps in order to upload the certificate:

   a. On the Unified Operating System Administration page, choose **Security > Certificate Management**, and click **Upload Certificate**.

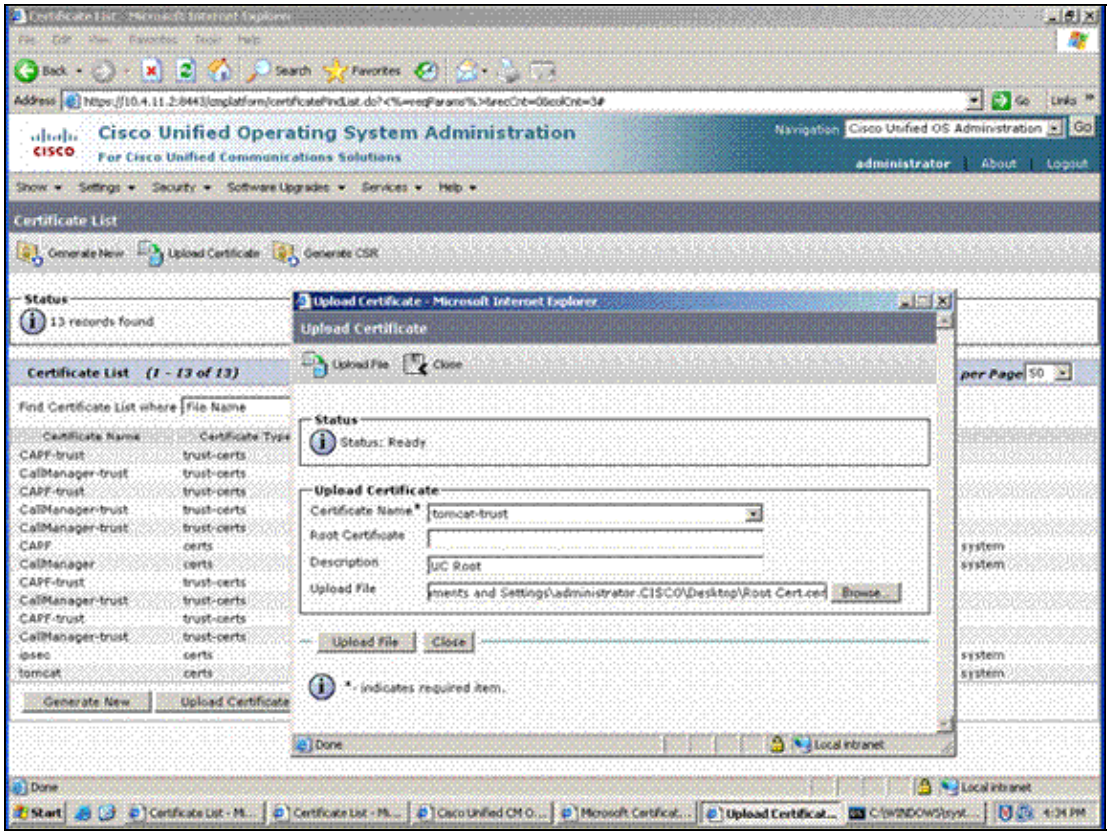
      The Upload Certificate dialog box appears.



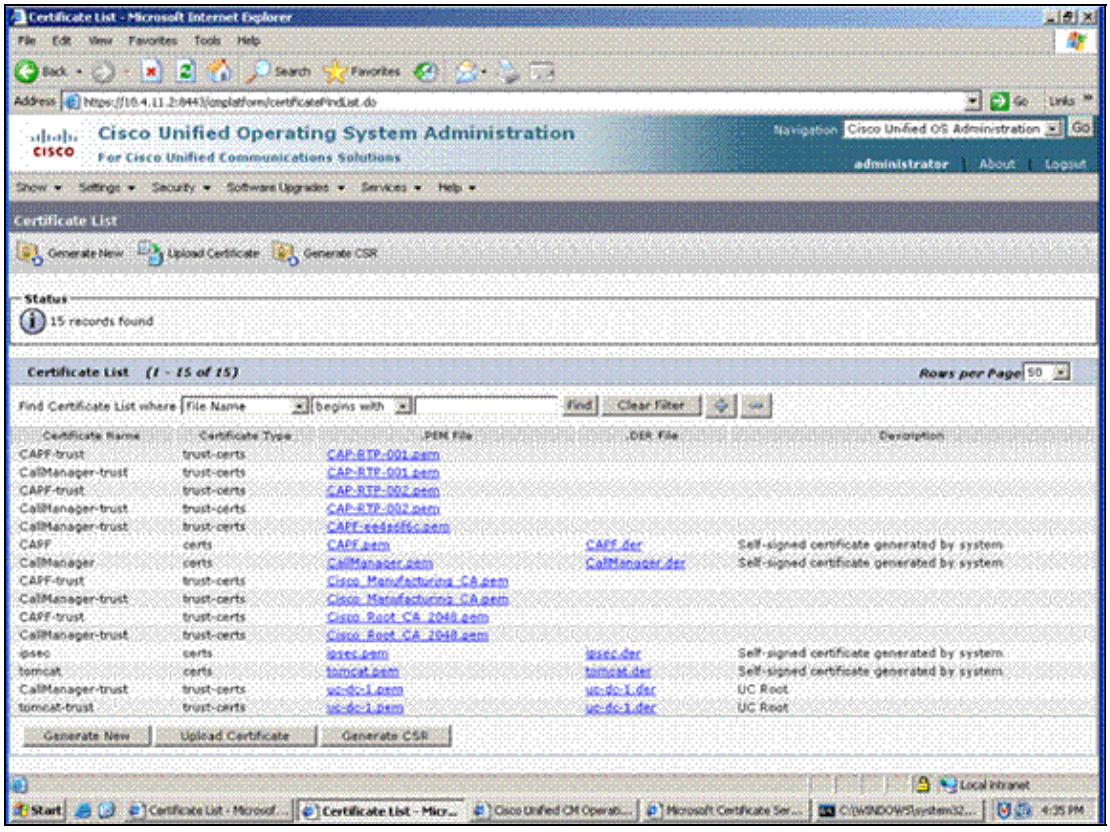
   b. Choose the type of certificate to upload. (The root CA certificate will be uploaded as a *Trust* certificate).

      Note: You must add the root certificate as a trust certificate to each service for which you want to use a CA certificate. This examples uses Tomcat and CallManager.

   c. Add an appropriate description, choose the root certificate to download from the CA, and click **Upload File**.



The CallManager−trust and tomcat−trust certificates are added to the Certificate List.



d. Repeat these steps as needed for IPSec and CAPF.

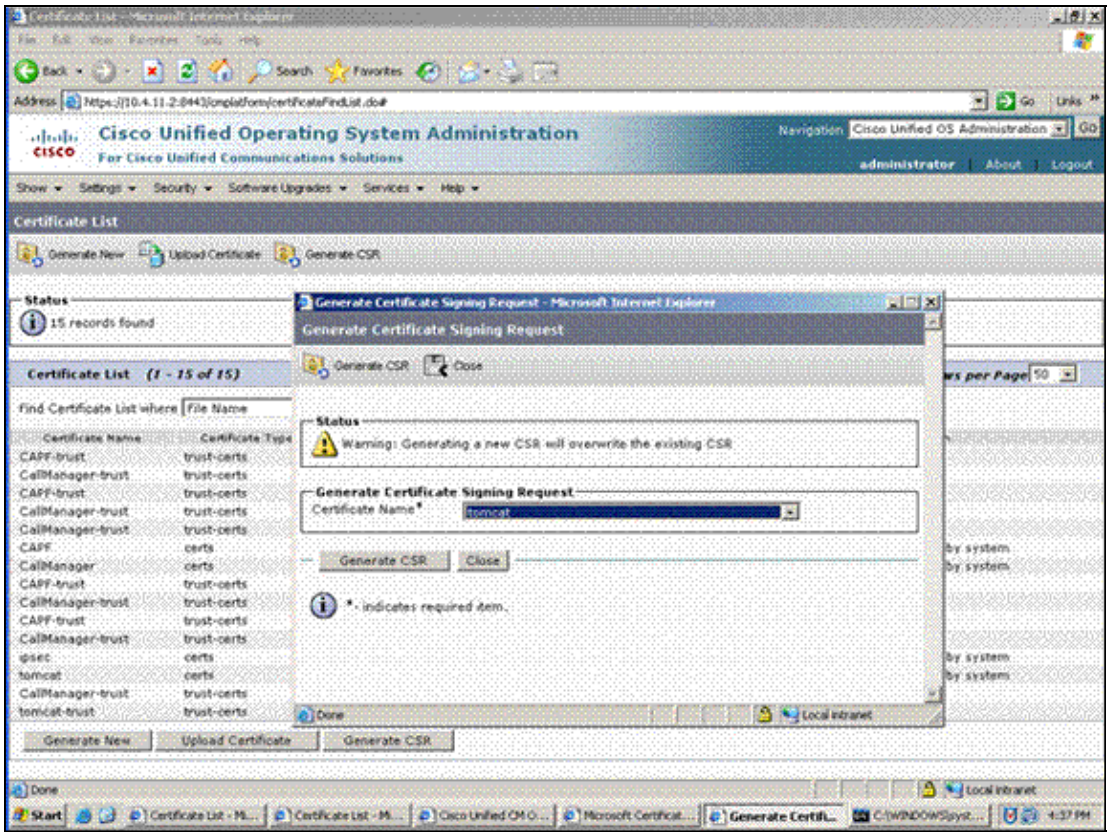
3. Generate a certificate signing request.

Note: This example uses Tomcat and CallManager.

Complete these steps in order to generate certificate signing requests for the types of certificates you want:

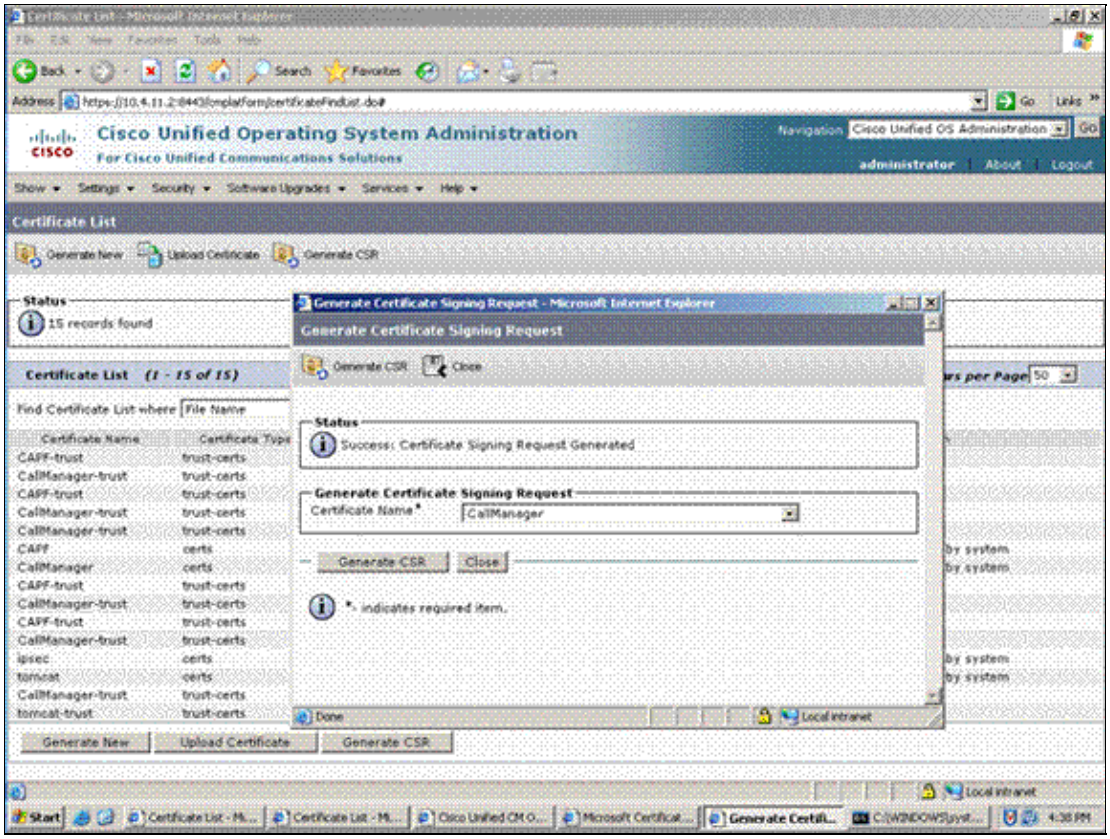
a. Click the **Generate CSR** button.

   The Generate Certificate Signing Request dialog box appears.



b. Choose the service from the Certificate Name drop−down list, and click the **Generate CSR** button.

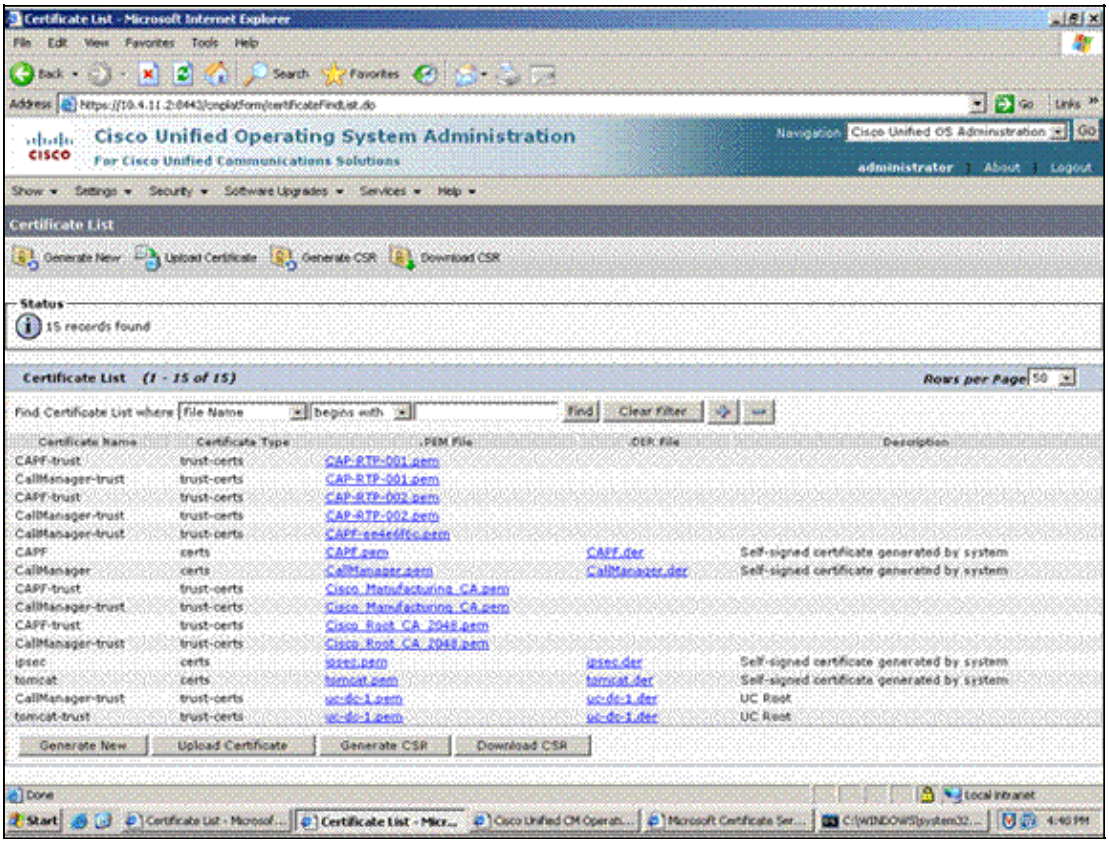
   Once the certificate is generated, the Status message shows "Success: Certificate Signing Request Generated."



c. Repeat these step for the CallManager CSR.

4. Download the CSR.

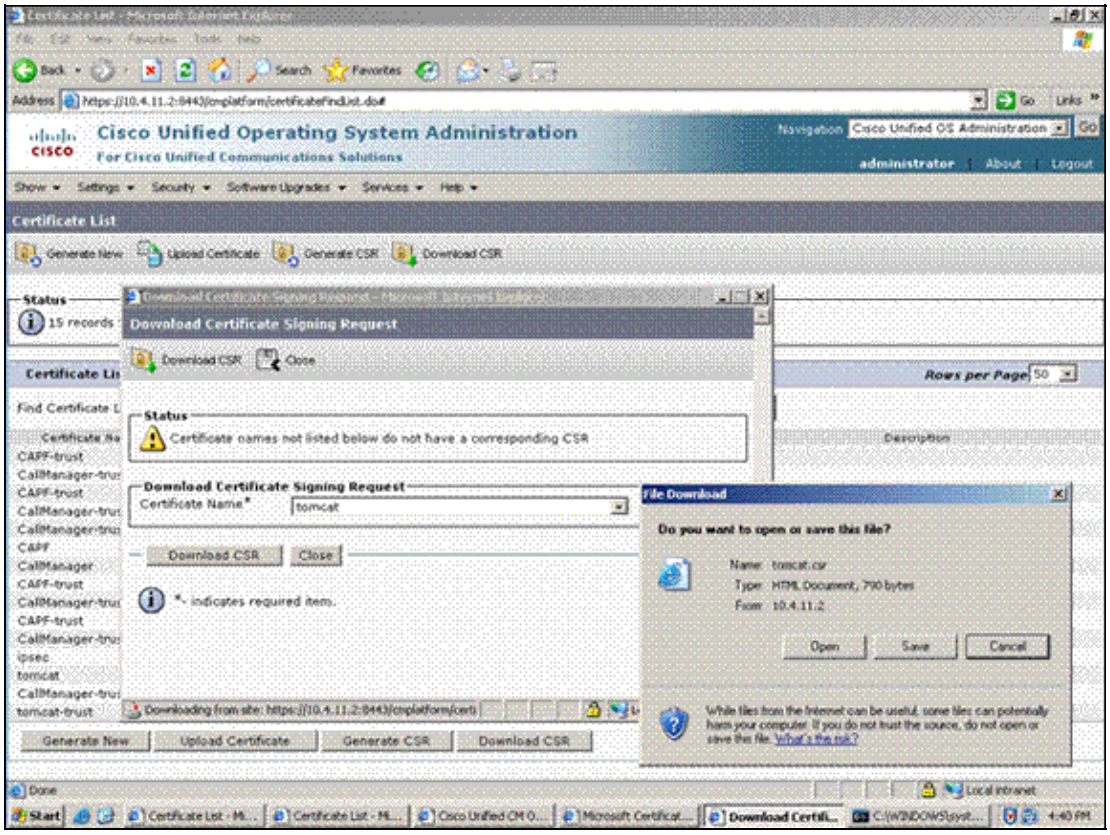
Once you generate the CSRs, the Download CSR button appears on the interface.



Complete these steps in order to download the CSR:

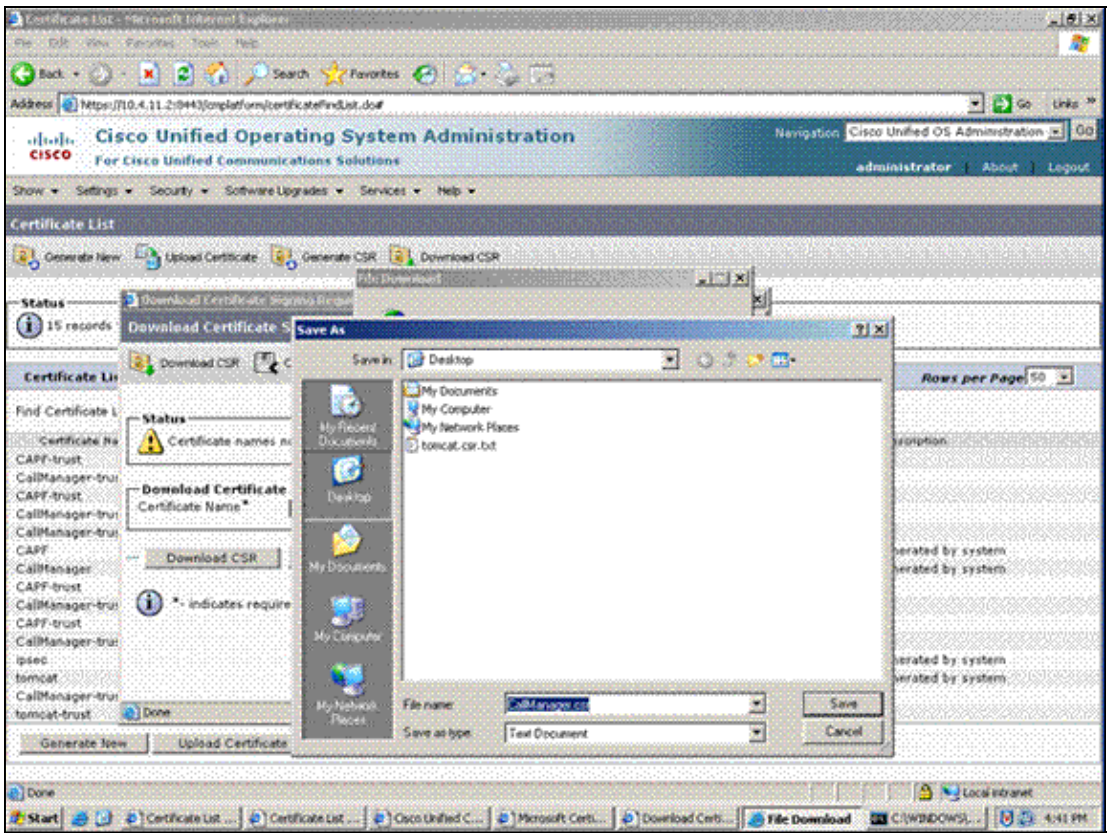
a. Click **Download CSR**.

The Download Certificate Signing Request dialog box appears.



b. Choose the CSR you want to download, and click **Download CSR**.

c. Save this file to your local computer.

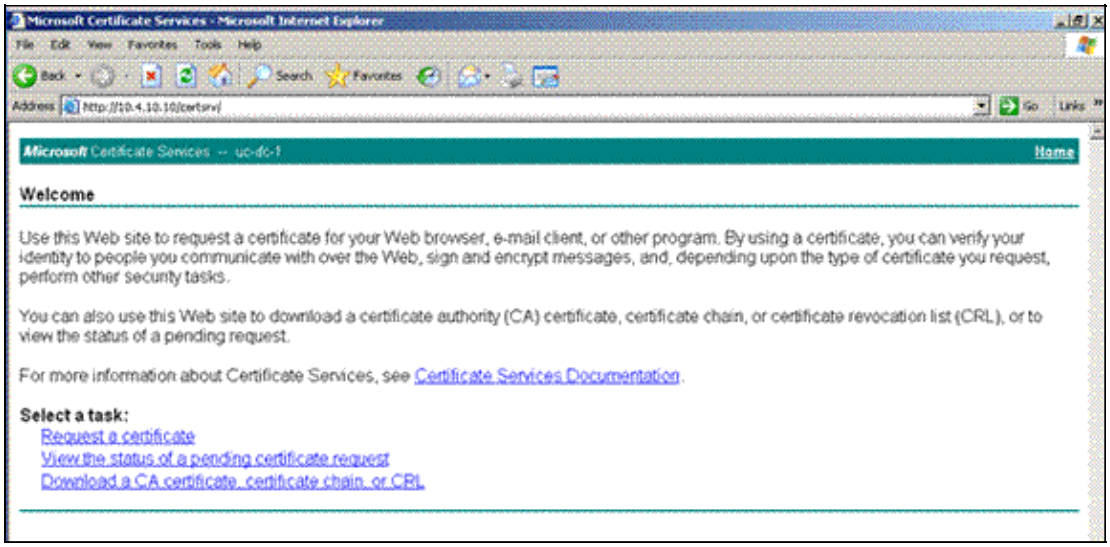


d. Repeat these steps for the CallManager CSR.

5. Request and download the certificates.

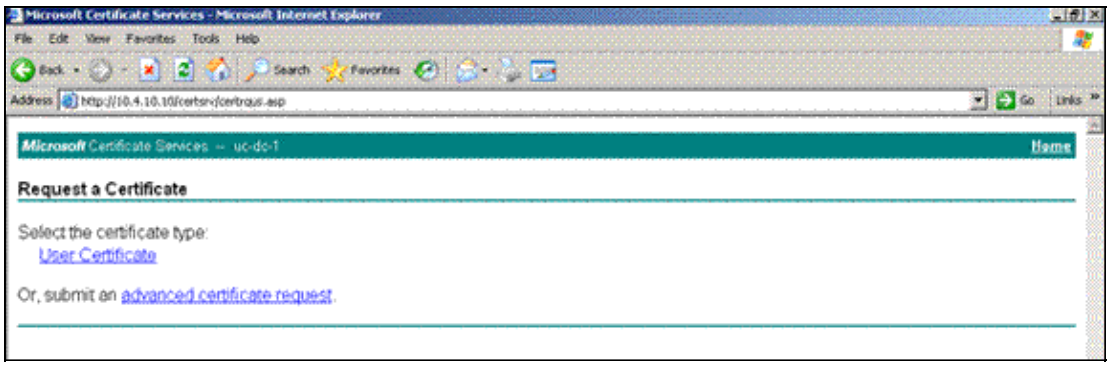
Complete these steps in order to request and download the certificates:

a. Go to http://<*certificate server address*>/certsrv in order to open the Certificates Server web page.



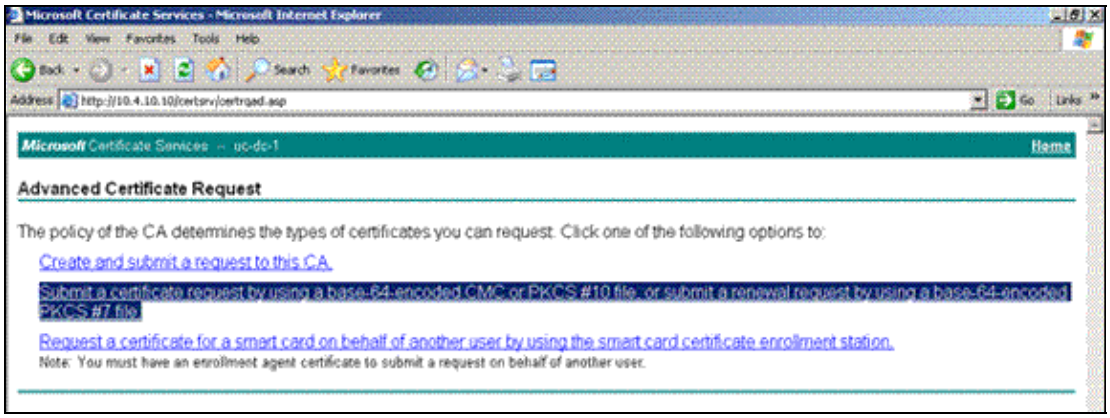
b. Click **Request a certificate**.

The Request a Certificate web page appears.



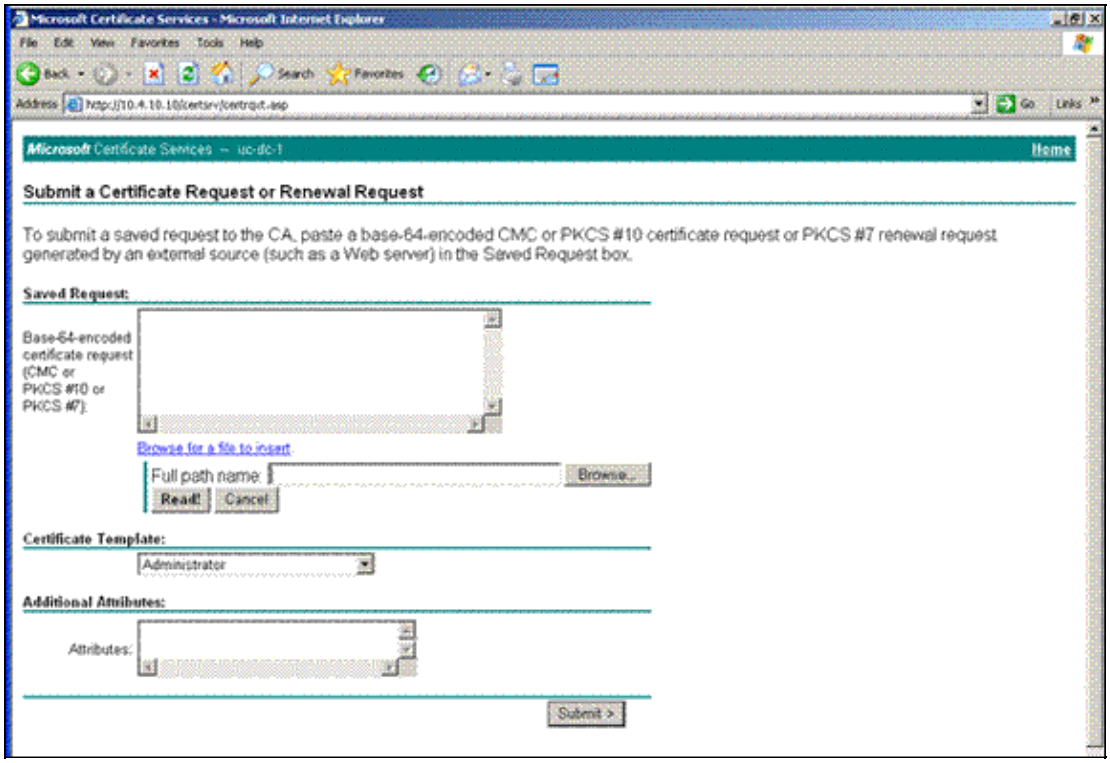
c. Click the **advanced certificate request** link.

The Advanced Certificate Request web page appears.



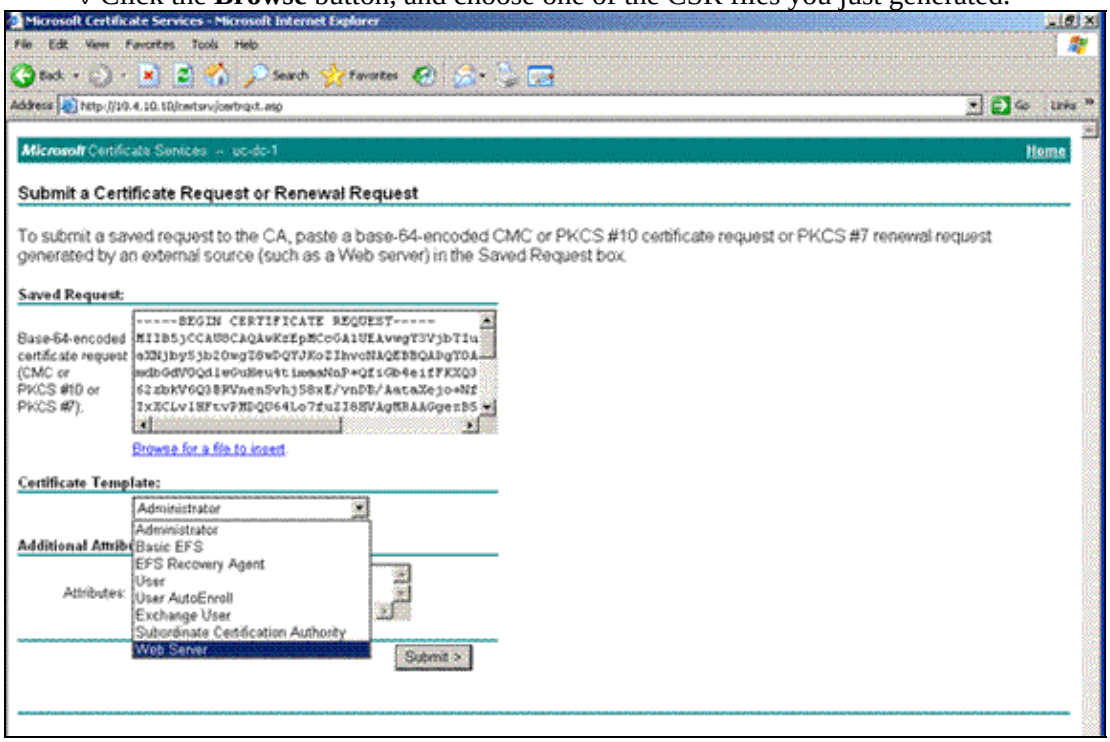
d. Click the **Submit a certificate request by using a base−64−encoded CMC or PKCS #10 file, or submit a renewal request by using a base−64−encoded PKCS #7 file** link.

The Submit a Certificate Request or Renewal Request web page appears.



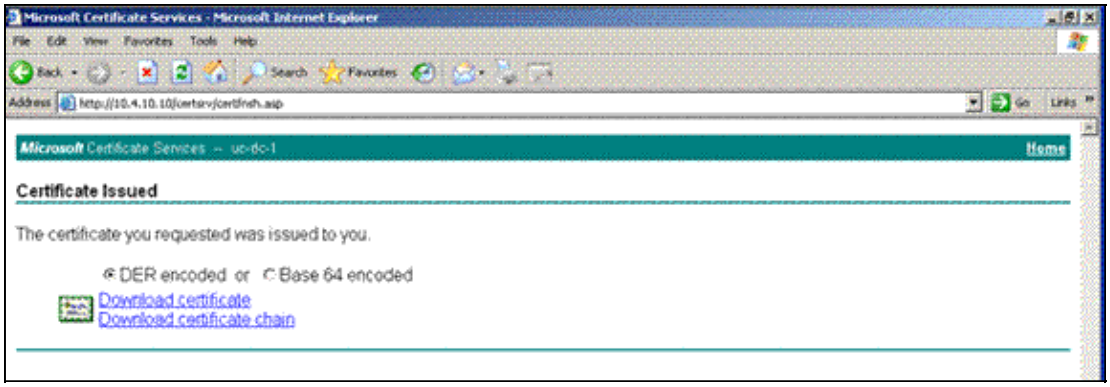
e. Use one of these methods to choose the certificate file:

◊ Paste the CSR file into the Base−64−encoded certificate request field.
◊ Click the **Browse** button, and choose one of the CSR files you just generated.



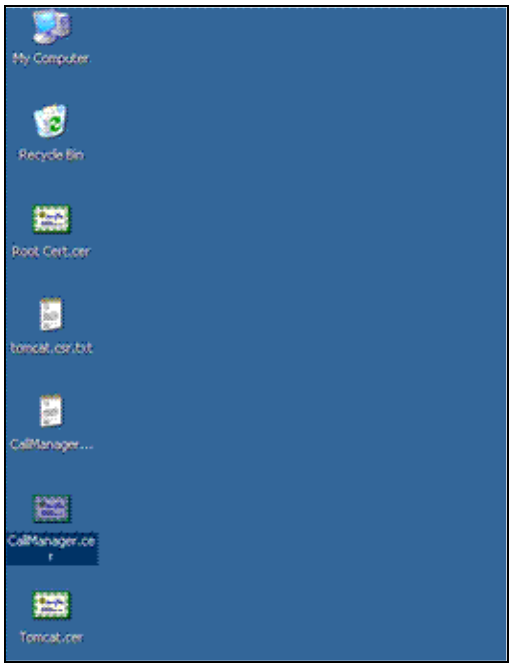
f. In the Certificate Template drop−down list, choose **Web Server**, and click **Submit**.

The Certificate Issued web page appears.



g. On the Certificate Issued web page, click the **DER encoded** radio button, and then click **Download certificate**.
h. Save the file to your local computer.
i. Repeat these steps in order to request and download the other certificates.

Once you complete these steps, all certificates should be stored on your local computer.

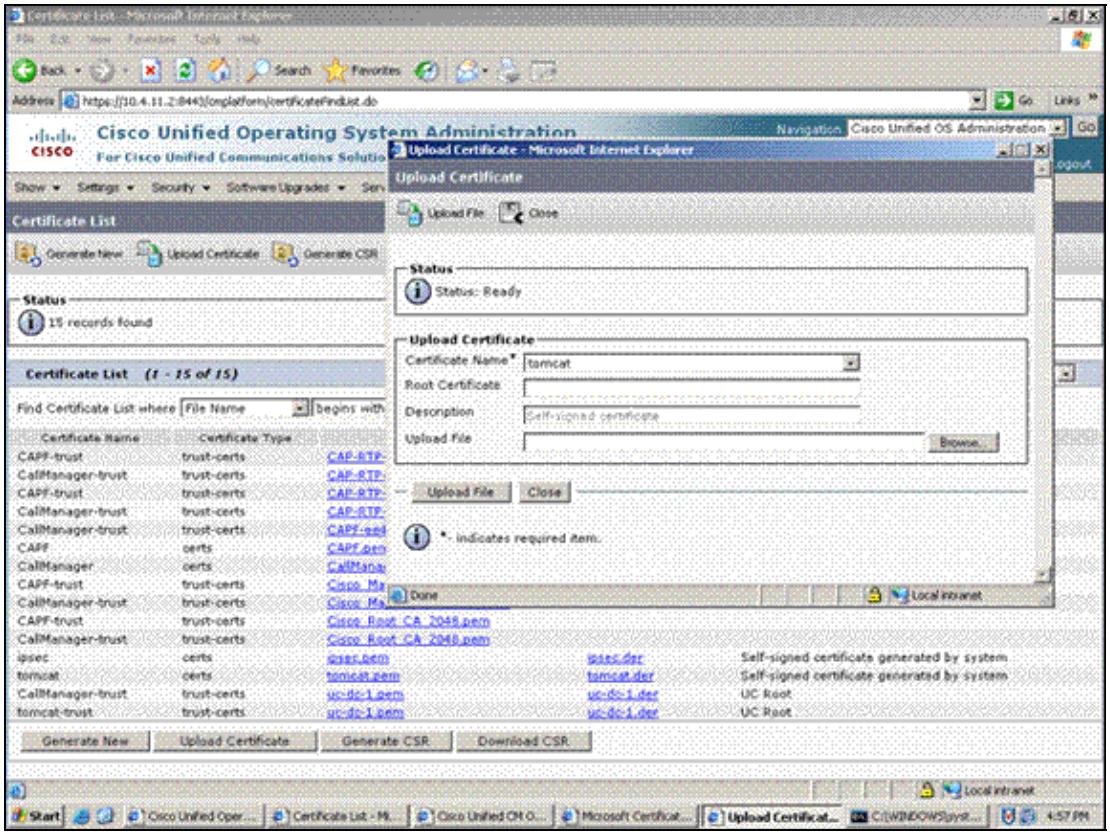


6. Upload the certificate to CallManager.

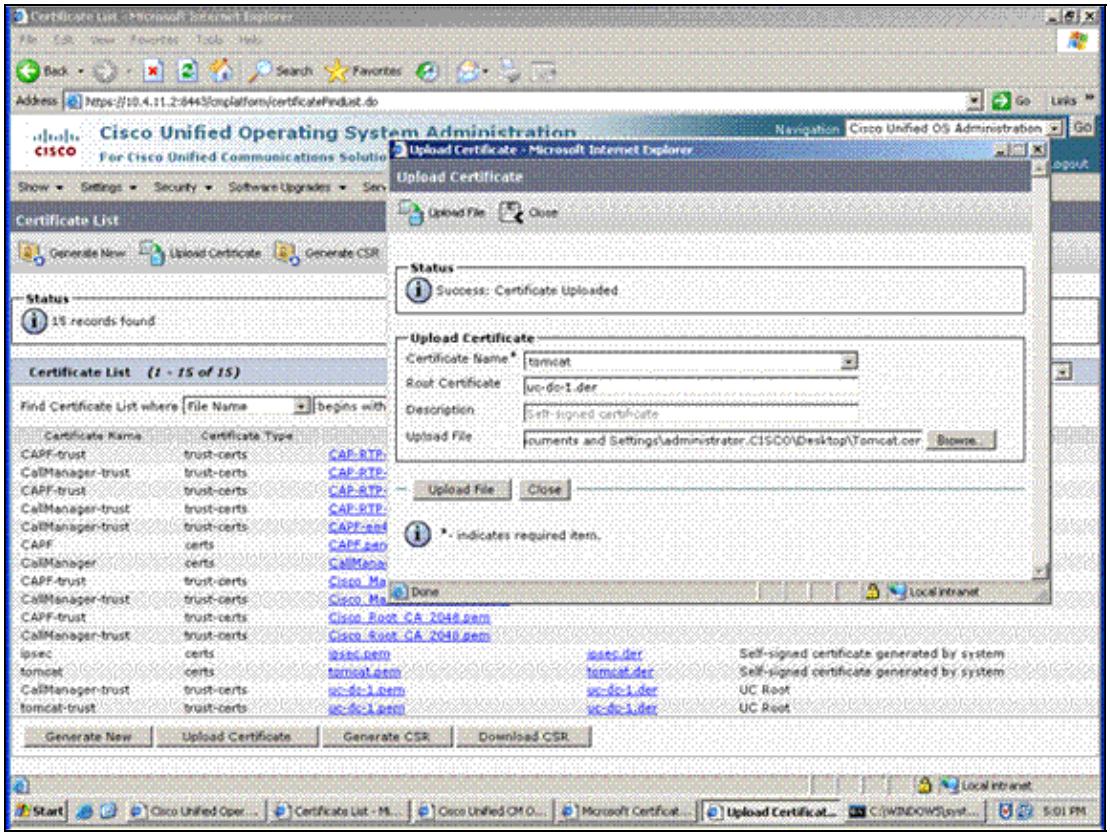
Complete these steps in order to upload the certificate to CallManager:

a. On the Upload Certificate web page, click **Upload Certificate**.

The Upload Certificate web page appears.

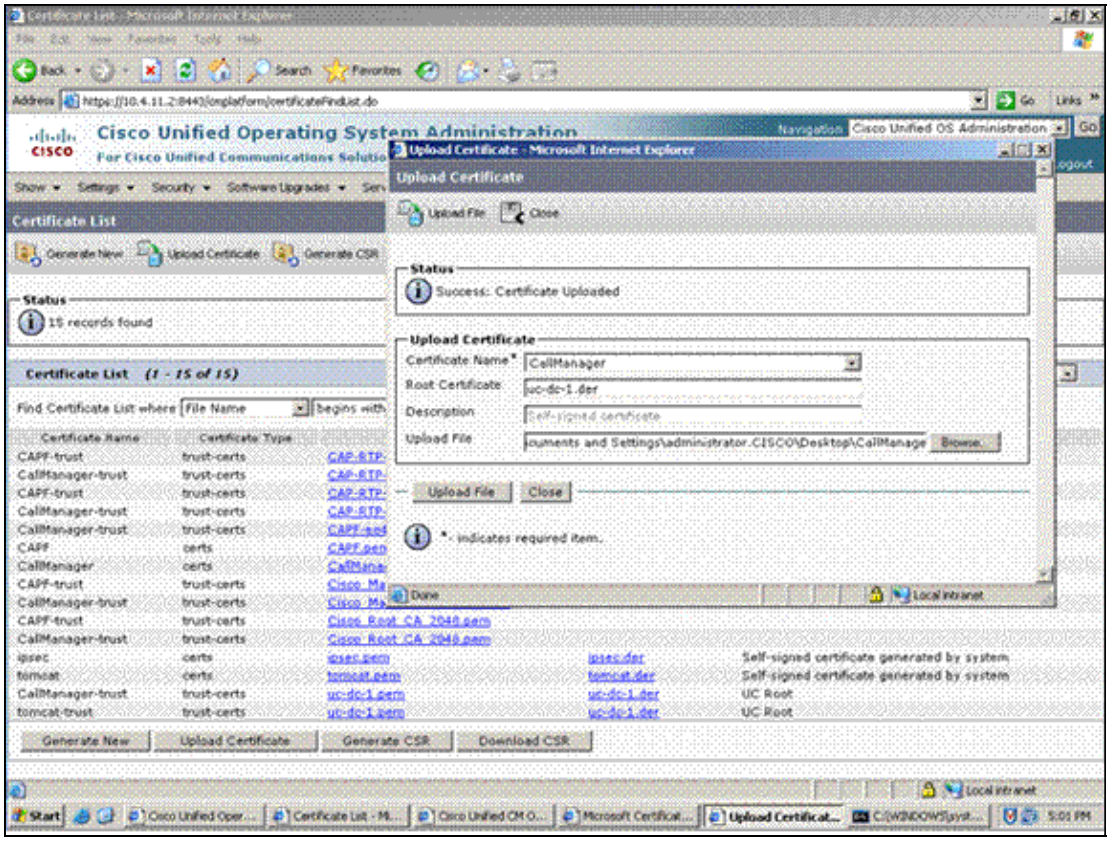


b. Choose the certificate type you want to upload. (This example uploads the Tomcat certificate.)



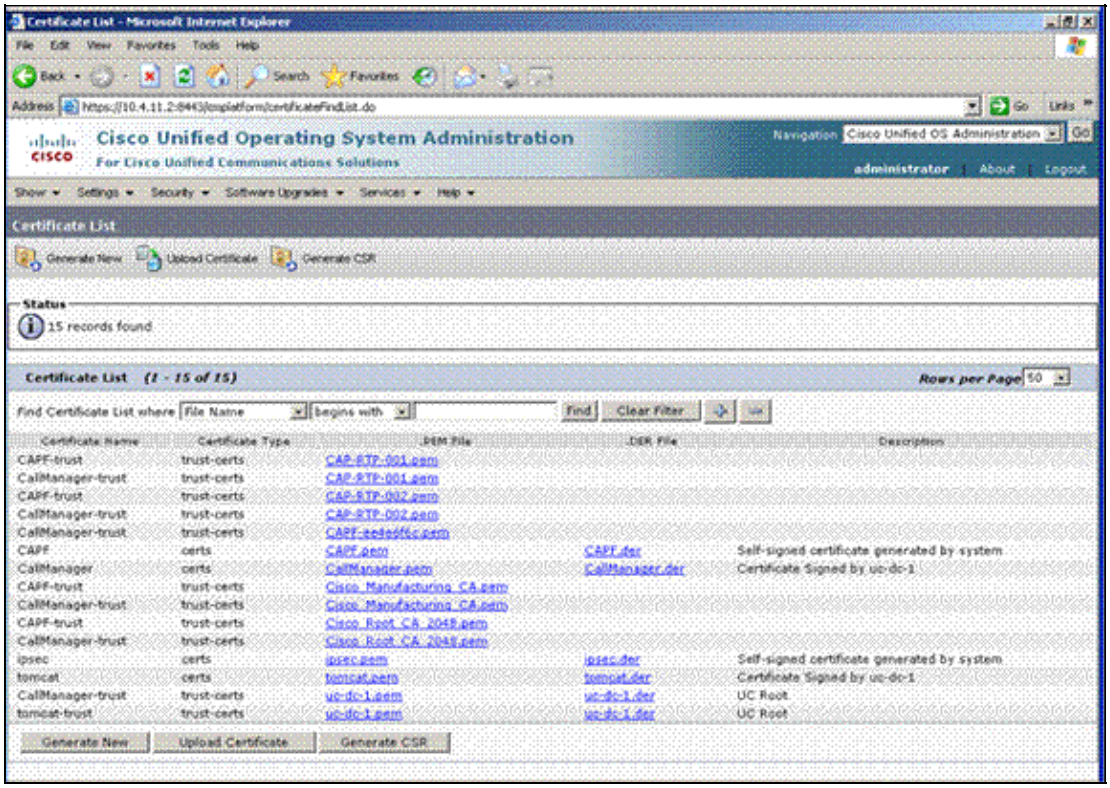
c. In the Root Certificate field, enter the name of the root certificate associated with the Tomcat certificate. (For this example, the root certificate name is *uc−dc−1.der*.)

d. From the Upload File field, choose the Tomcat certificate, and click **Upload File**.



e. Repeat this process for each certificate you want to upload.

Once you complete these steps, the trust certificates are now loaded, and the Tomcat and CallManager Certs are signed by our Microsoft Root CA.



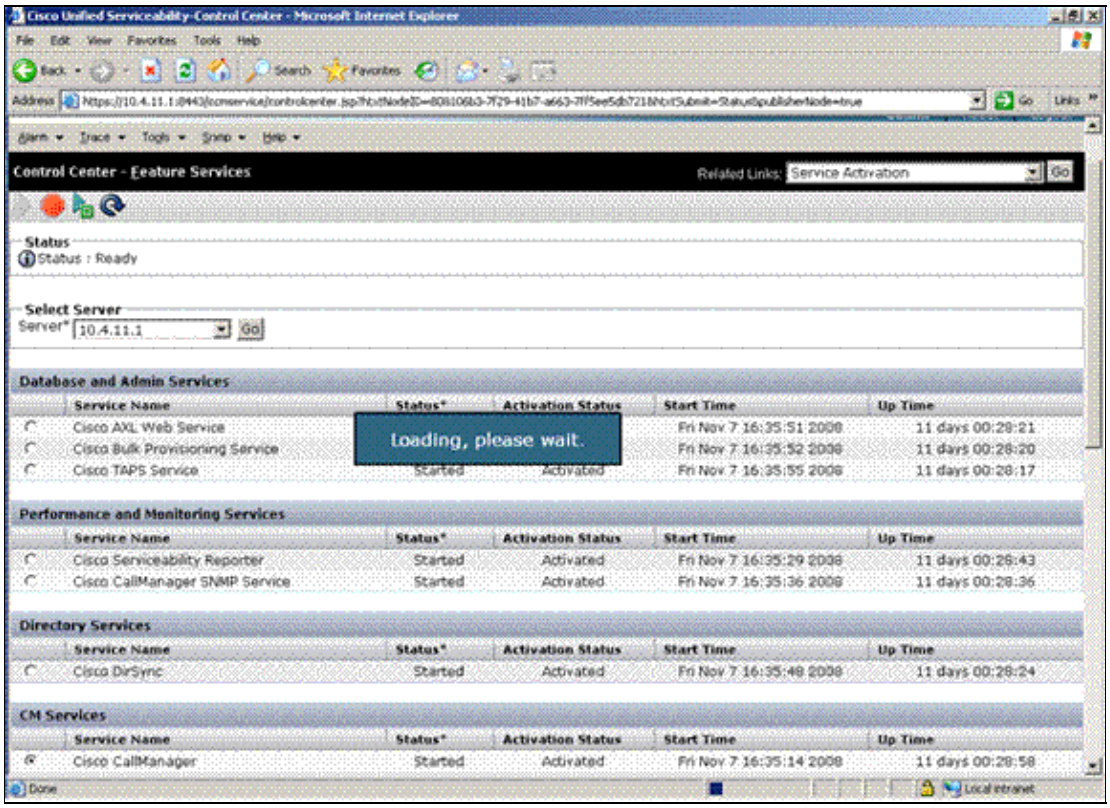
7. Restart the processes.

Once the certificates are loaded, you must restart the processes to force them to use the new

certificates. This examples restarts the CallManager service.

Complete these steps in order to restart the processes.

a. Navigate to the Cisco Unified Serviceability page, and open the Control Center for feature services.



b. From the Console on the CallManager server, log in and type this command in order to restart the Tomcat service:

```
utils service restart Cisco Tomcat
```

This command updates the Tomcat service with the new certificate.

8. Repeat this entire process on all the servers in the cluster.

Verify

There is currently no verification procedure available for this configuration.

Related Information

- **Voice Technology Support**
- **Voice and Unified Communications Product Support**
- **Troubleshooting Cisco IP Telephony**
- **Technical Support & Documentation − Cisco Systems**