

CallManager 5.x: Delete and Regenerate a Certificate

Document ID: 99815

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Server Certificate Types

Cisco Unified Communications Operating System Administration

- Delete and Regenerate a Certificate

Troubleshoot

- Error: There is a problem with this website's security certificate

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document describes how to delete and regenerate different types of server certificates in Cisco Unified Communication Manager 5.x (CallManager). Certificates secure client and server identities. After root certificates are installed, certificates are added to the root trust stores in order to secure connections between users and hosts, which includes devices and application users.

Prerequisites

Requirements

Cisco recommends that you have knowledge of Cisco Unified Communication Manager 5.x.

Components Used

The information in this document is based on Cisco Unified Communication Manager 5.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 Cisco Technical Tips Conventions for more information on document conventions.

Server Certificate Types

Cisco uses these self-signed (own) certificate types in Cisco Unified CallManager servers:

- HTTPS certificate (tomcat_cert) This self-signed root certificate is generated during the Cisco Unified CallManager installation for the HTTPS server.

- Cisco Unified CallManager node certificate This self–signed root certificate automatically installs when you install Cisco Unified CallManager 5.1 for the Cisco Unified CallManager server. Cisco Unified CallManager certificates provide server identification, which includes the Cisco Unified CallManager server name and the Global Unique Identifier (GUID).
- CAPF certificate The system copies this root certificate to all servers in the cluster after you complete the Cisco CTL client configuration.
- IPsec certificate (ipsec_cert) This self–signed root certificate is generated during Cisco Unified CallManager installation for IPsec connections with MGCP and H.323 gateways.
- SRST–enabled gateway certificate When you configure a secure SRST reference in Cisco Unified CallManager Administration, Cisco Unified CallManager retrieves the SRST–enabled gateway certificate from the gateway and stores it in the Cisco Unified CallManager database. After you reset the devices, the certificate is added to the phone configuration file. Because the certificate is stored in the database, this certificate is not integrated into the certificate management tool.

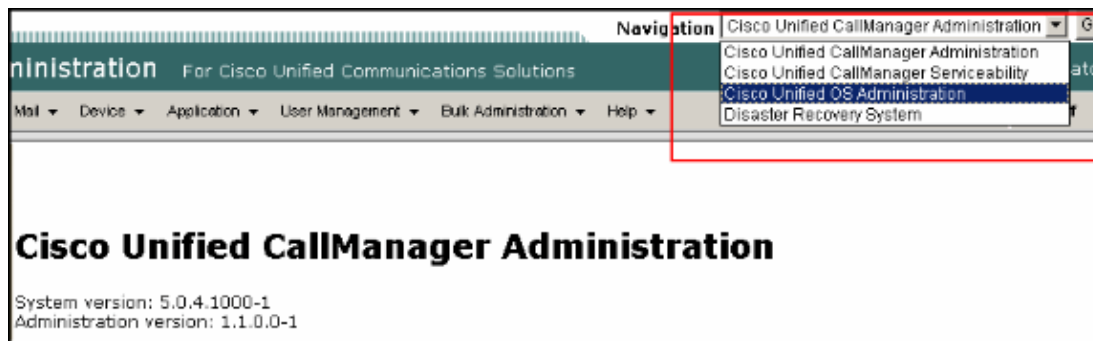
Cisco Unified Communications Operating System Administration

You must delete and regenerate the certificate in Cisco Unified Communication Manager if you encounter this error in the Cisco Unified Communication Manager server:

The security certificate presented by this website was not issued by a trusted certificate authority. Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

In order to delete and regenerate a certificate in Cisco Unified Communication Manager 5.x you need to login into Cisco Unified Communications Operating System Administration.

Choose **Cisco Unified OS Administration** from the **Navigation** drop–down menu from the right hand side of the Administration page, and click **Go**.



Delete and Regenerate a Certificate

Log into the Cisco Unified Communications Operating System Administration with your Administrator password which is provided during the installation of the server.

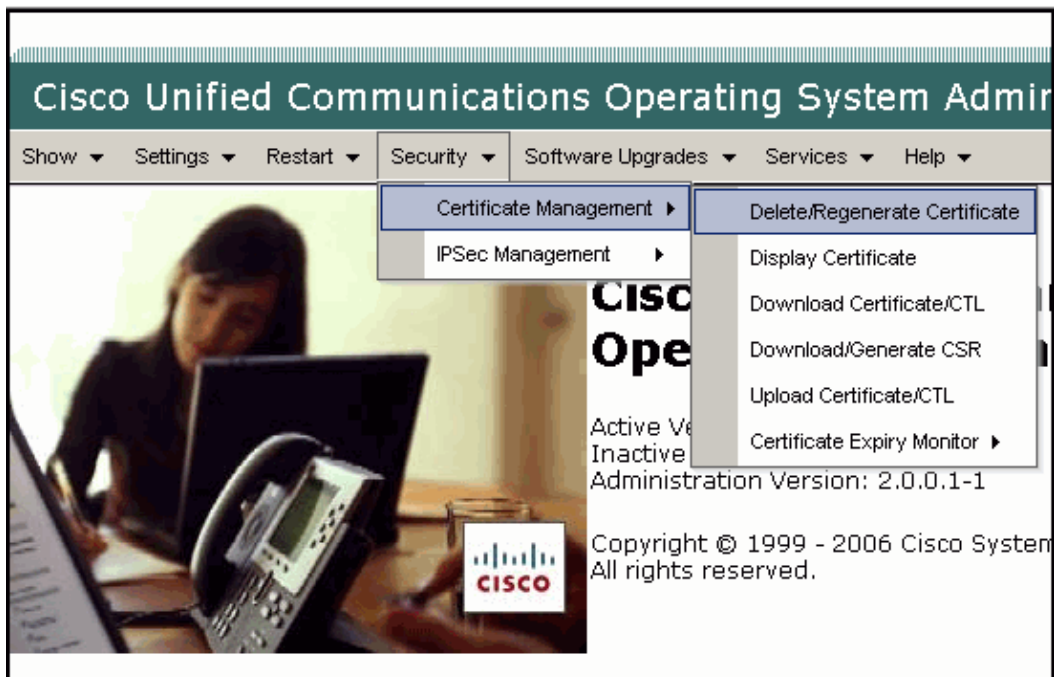
- Delete a Certificate
- Regenerate a Certificate

Delete a Certificate

In order to delete a trusted certificate, complete these steps:

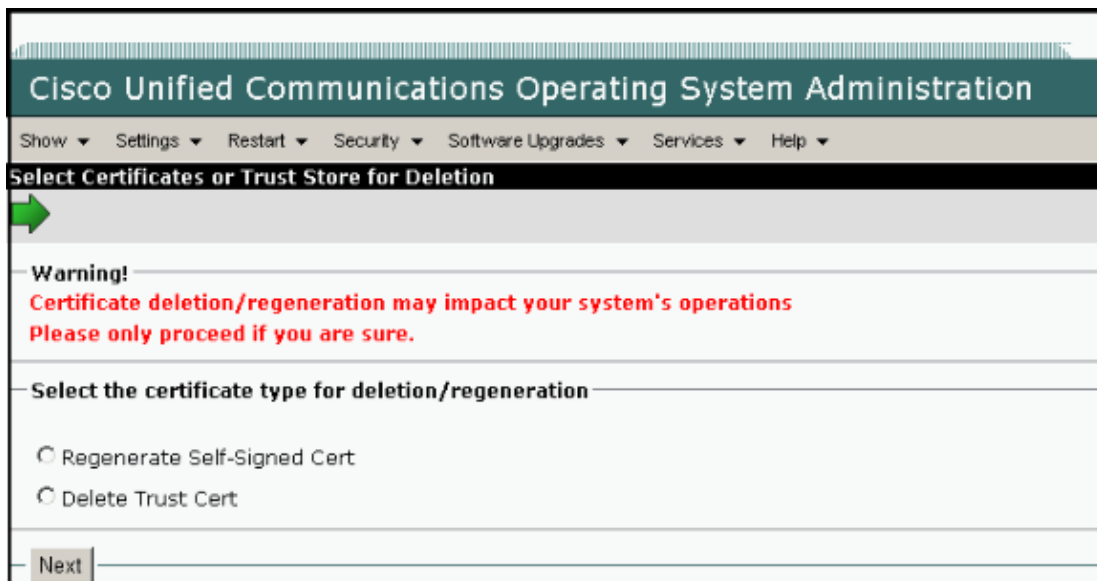
Note: If you delete a certificate, it can affect your system operations.

1. Choose **Security>Certificate Management>Delete/Regenerate Cert.**



2. Check the **Delete Trust Cert** check box, and click **Next**.

The Display Certificates or Trust Units For Delete/Regenerate window appears.



3. Check the check box for the existing **certificate type** that you want to delete, and click **Next**.

The Delete Certificates or Trust Store window appears.

4. Check the Existing Certificate Name check box for the certificate that you want to delete, and click **Delete**.

Regenerate a Certificate

In order to regenerate a certificate, complete these steps:

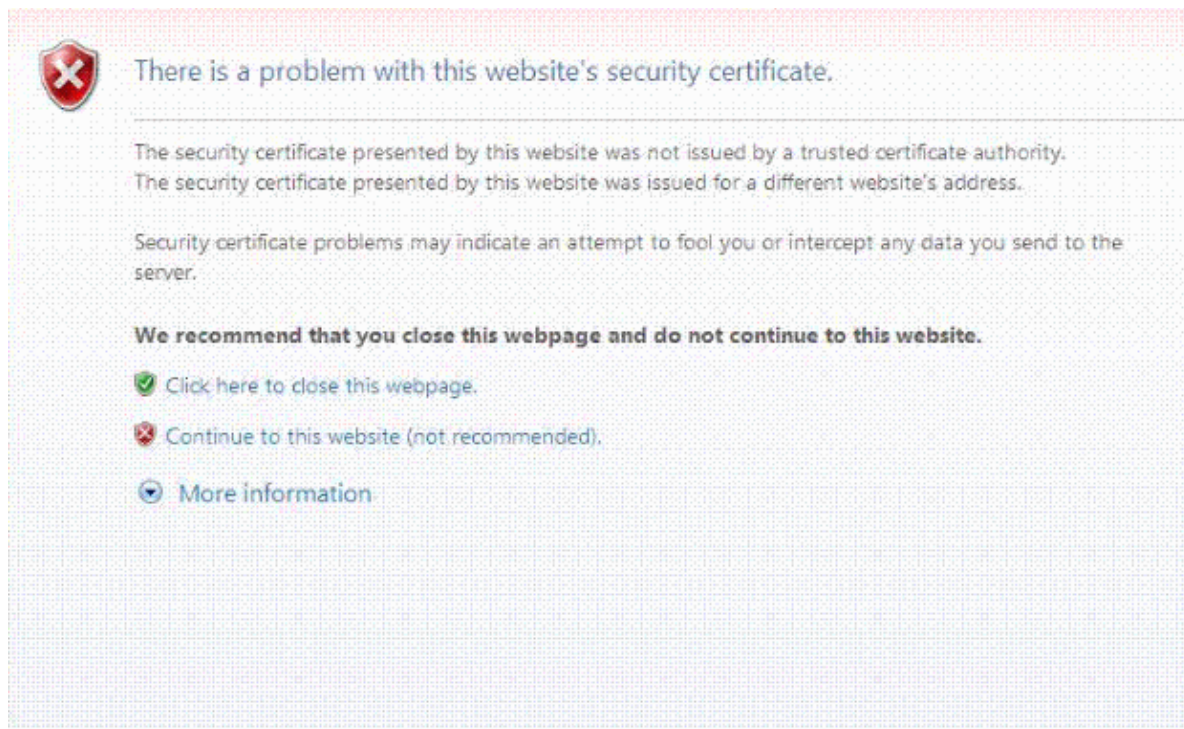
1. Choose **Security > Certificate Management > Delete/Regenerate Cert.**

- The Select Certificates or Trust Store for Deletion window appears.
2. Check the **Regenerate Self-Signed Cert** check box, and click **Next**.
 3. Check the appropriate Existing Certificates Types check box for the certificate that you want to regenerate, and click **Next**.
 4. Check the appropriate Existing Certificate check box, and click **Regenerate**.

Troubleshoot

Error: There is a problem with this website's security certificate

When you navigate through the Cisco CallManager 5.0 Administration pages, the There is a problem with this website's security certificate error messages appears.



In order to resolve this issue, complete these steps:

1. In the Security Alert dialog box, click **Continue to this website** and on the address bar, click **Certificate Error**.
2. Choose **View Certificate**.
3. In the Certificate pane, click **Install Certificate**. Click **Next**.
4. Choose **Place all certificates in the following store** and click **Browse**.
5. Browse to **Trusted Root Certification Authorities**.
6. Click **Next**, and then click **Finish**.
7. In order to install the certificate, click **Yes**. A message states that the import is successful. Click **OK**.
8. In the lower, right corner of the dialog box, click **OK**.
9. In order to trust the certificate so you do not receive the dialog box again, click **Yes**.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Voice

Service Providers: Voice over IP

Voice & Video: Voice over IP

Voice & Video: IP Telephony

Voice & Video: IP Phone Services for End Users

Voice & Video: Unified Communications

Voice & Video: IP Phone Services for Developers

Voice & Video: General

Related Information

- **Voice Technology Support**
- **Voice and Unified Communications Product Support**
- **Recommended Reading: Troubleshooting Cisco IP Telephony**
- **Technical Support & Documentation – Cisco Systems**

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 24, 2007

Document ID: 99815
