

Unified Communications Manager: Delete and Regenerate a Certificate

Document ID: 99815

Contents

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Server Certificate Types

Cisco Unified Communications Operating System Administration

- Delete and Regenerate a Certificate

- Install a Trusted Authority Root Certificate

Troubleshoot

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

- Cisco Unified Communications Manager 7.1: Website Security Certificate Error Webpage

Related Information

Introduction

This document describes how to delete and regenerate different types of server certificates in Cisco Unified Communications Manager 5.x /7.x. 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 Communications Manager 5.x/7.x.

Components Used

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

Server Certificate Types

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

- **HTTPS certificate (tomcat_cert)** This self–signed root certificate is generated during the Cisco Unified Communications Manager installation for the HTTPS server.
- **Cisco Unified Communications Manager node certificate** This self–signed root certificate automatically installs when you install Cisco Unified Communications Manager 5.1 for the Cisco Unified Communications Manager server. Cisco Unified Communications Manager certificates provide server identification, which includes the Cisco Unified Communications Manager 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 Communications Manager installation for IPsec connections with MGCP and H.323 gateways.
- **SRST–enabled gateway certificate** When you configure a secure SRST reference in Cisco Unified Communications Manager Administration, Cisco Unified Communications Manager retrieves the SRST–enabled gateway certificate from the gateway and stores it in the Cisco Unified Communications Manager 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.

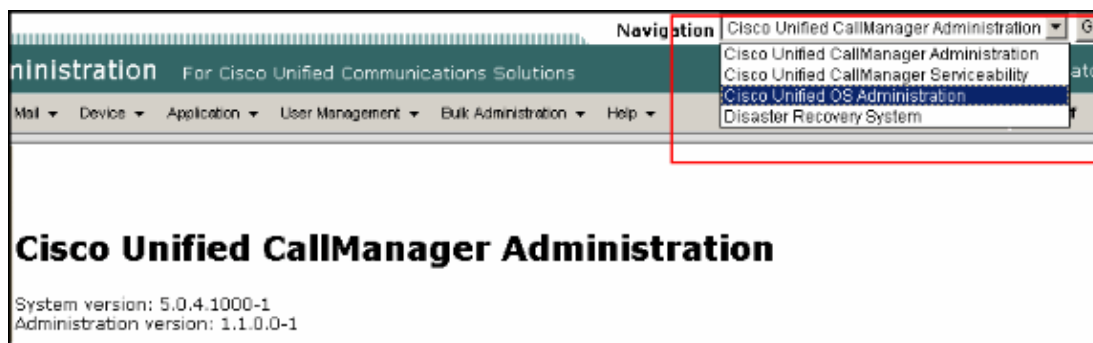
Cisco Unified Communications Operating System Administration

You must delete and regenerate the certificate in Cisco Unified Communications Manager if you encounter this error in the Cisco Unified Communications 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 Communications 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.

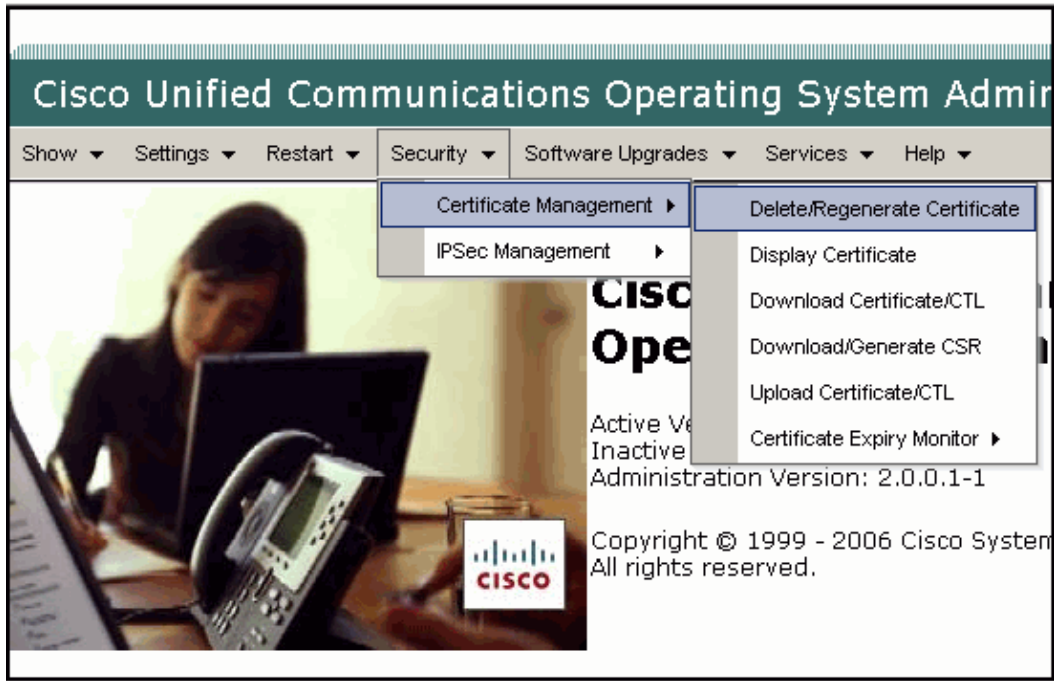
- Delete a Certificate
- Regenerate a Certificate

Delete a Certificate

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

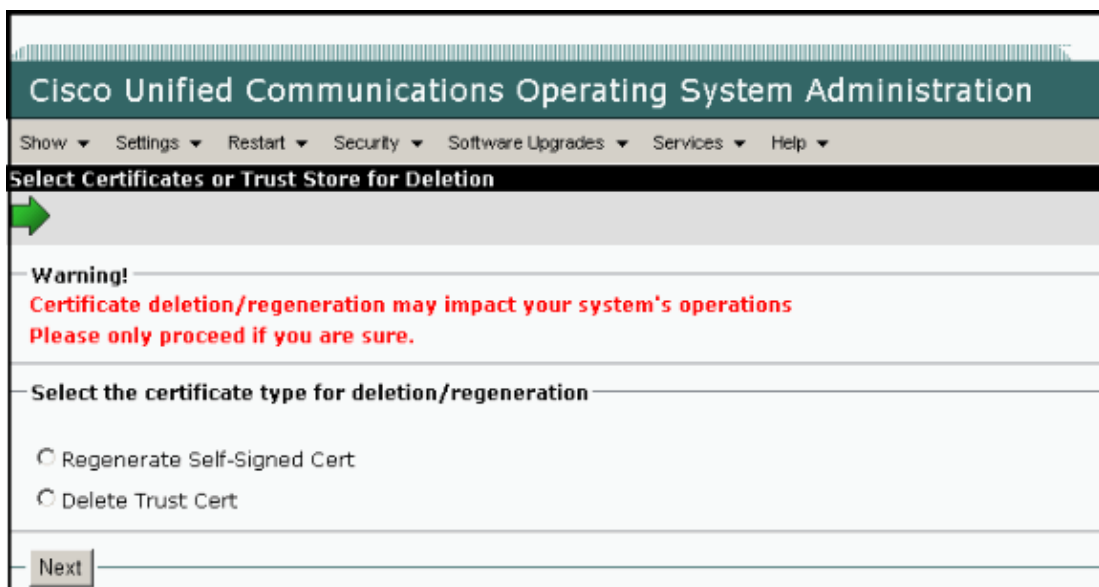
Note: If you delete a certificate, it can affect your system operations.

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**.

Install a Trusted Authority Root Certificate

In order to install a trusted authority root certificate instead of the current certificate in your Cisco Unified Communications Manager, complete these steps:

1. Choose **Start > Administrative Tools > Internet Services Manager (IIS)**.
2. Right-click **Default Web Site**, and click the **Directory Security** tab.
3. Click **Server Certificate** and remove the current certificate.
4. Go back to the same **Server Certificate** button, click **Next**, and select **Process the pending request and install the certificate**.
5. Enter or browse to the location of your IIS SSL certificate, and click **Next**.
6. Read the summary screen to be sure that the correct certificate is processed, and click **Next**.

A confirmation screen appears.

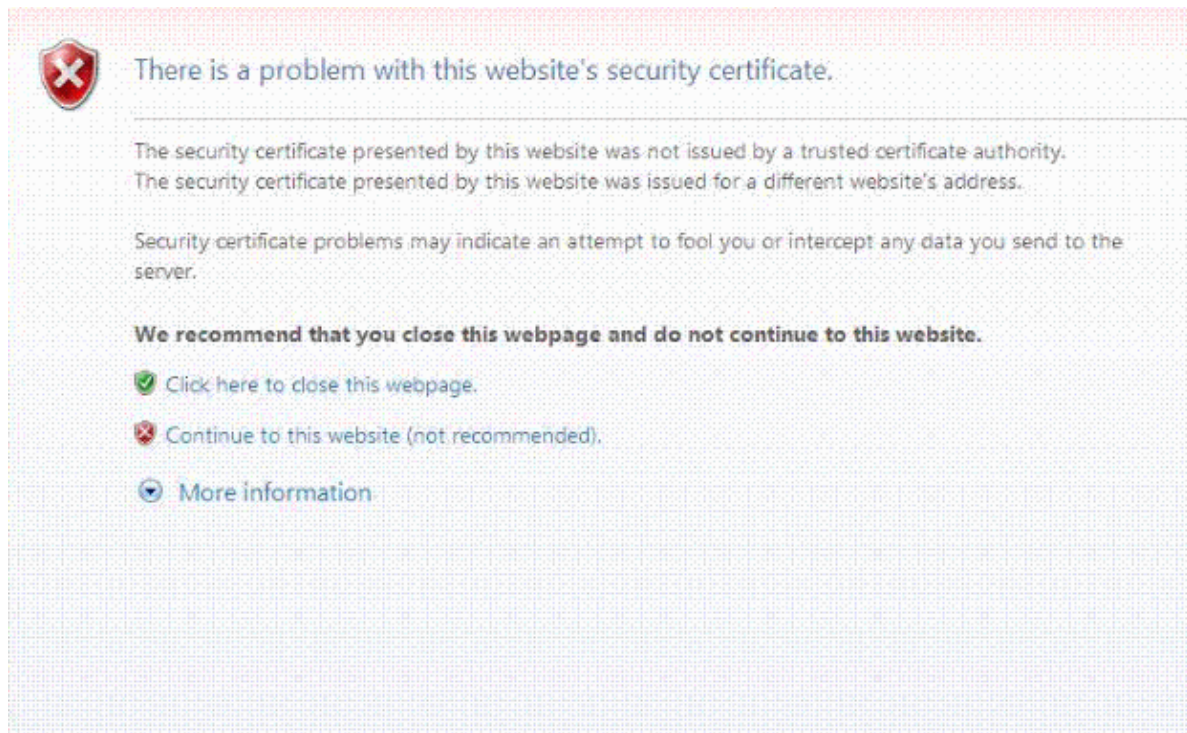
7. When you have read this information, click **Next**.

You now have an IIS SSL server certificate installed.

Troubleshoot

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

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



If you use IE 6.0 or 7.0, complete these nine steps in order to resolve this issue. If you use IE 8.0, complete these nine steps and then continue on to the next set of instructions:

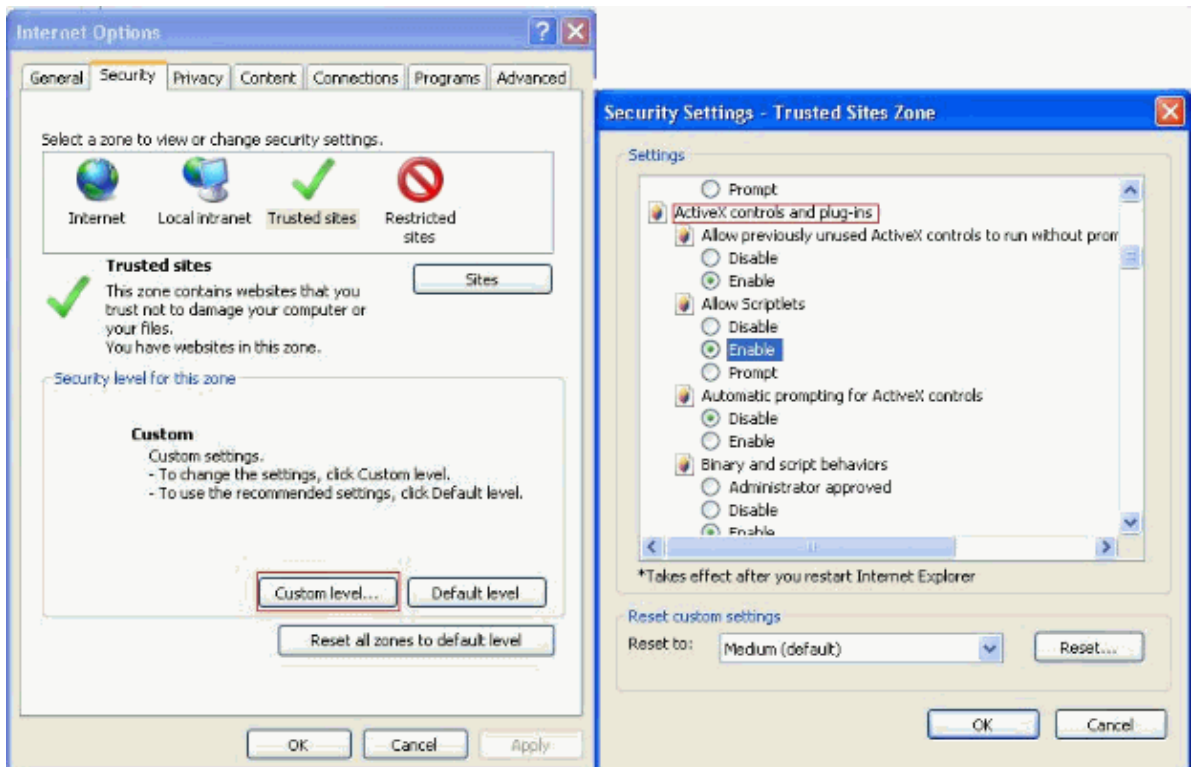
1. In the Security Alert dialog box, click **Continue to this website** and on the address bar, click `Certificate Error`.
2. Choose **View Certificate**.
3. In the Certificate pane, click **Install Certificate**. Click **Next**.
4. Choose **Place all certificates in the following store**, and click **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**.

If you use IE 6 or 7, you are finished. If you use IE 8.0, continue with these steps:

1. In Internet Explorer, choose **Tools > Internet Options**.
2. Click the **Security** tab, and then click **Custom Level**.

The Security Settings – trusted Sites Zone dialog box opens.

3. Scroll down to **Active X controls and plug-ins**, and change the default settings, as shown in figure.



- a. Allow Scriptlets **Enable**
 - b. Automatic prompting for ActiveX controls **Disable**
 - c. Binary and Script behaviours **Enable**
 - d. Display video and animation on a webpage that does not use external media player **Disable**
 - e. Download Signed ActiveX controls **Prompt**
 - f. Download unsigned ActiveX controls **Prompt**
 - g. Initialize and script ActiveX controls not marked as safe for scripting **Prompt**
 - h. Run ActiveX controls and plug-ins **Enable**
 - i. Script ActiveX controls marked safe for scripting **Enable**
4. Click **Ok**.
 5. Click **Yes** when asked Are you sure you want to change the settings for this zone?
 6. Close and re-open the browser.

Note: After you have received the certificate and it is installed within Internet Explorer, you can click **Default level** in IE Internet Options in order to change your security settings back to the default.

Cisco Unified Communications Manager 7.1: Website Security Certificate Error Webpage

Complete these steps in order to resolve the issue:

1. Obtain the root certificate from certificate authority.
2. Upload the root certificate to Cisco Unified Communications Manager as Tomcat-trust, upload any intermediate certificate, and specify Tomcat-trust and the higher level Root certificate as the root.
3. Generate a Tomcat CSR from CCM OS Admin page.
4. Sign the certificate from Certificate Authority.
5. Upload the signed certificate as Tomcat specifying the subject CN of the original Root Cert in the Subject CN. If the Subject CN of the original contains spaces, replace them with _ (underscores).
6. Restart tomcat from the CLI with **utils service restart Cisco Tomcat**.

Related Information

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

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

© 2011 – 2012 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Apr 20, 2010

Document ID: 99815
