Configure Basic Security

About Security Configuration

This section provides information about the basic security configuration tasks that you have to perform to set up Cisco Unified Communications Manager.

Security Configuration Tasks

Perform the following tasks to set up the basic security configurations:

Enable Mixed Mode for Cluster

Use this procedure to enable mixed mode in the cluster.

Procedure

Step 1 Log in to the Command Line Interface on the publisher node.

Step 2 Run the **utils ctl set-cluster mixed-mode** CLI command.

Note Make sure that Communications Manager is registered with the Cisco Smart Software Manager or Cisco Smart Software Manager satellite and the Registration Token received from the Smart account or Virtual account has Allow export-controlled functionality enabled while registering with this cluster.

Download Certificates

Use the download certificates task to have a copy of your certificate or upload the certificate when you submit a CSR request.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Specify search criteria and then click **Find**.

Step 3 Choose the required file name and Click **Download**.

Generate a Certificate Signing Request

Generate a Certificate Signing Request (CSR) which is a block of encrypted text that contains certificate application information, public key, organization name, common name, locality, and country. A certificate authority uses this CSR to generate a trusted certificate for your system.

Note If you generate a new CSR, you overwrite any existing CSRs.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Click **Generate CSR**.

Step 3 Configure fields on the **Generate Certificate Signing Request** window. See the online help for more information about the fields and their configuration options.

Step 4 Click **Generate**.

Download a Certificate Signing Request

Download the CSR after you generate it and have it ready to submit to your certificate authority.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.
Step 2 Click **Download CSR**.
Step 3 Choose the certificate name from the **Certificate Purpose** drop-down list.
Step 4 Click **Download CSR**.
Step 5 (Optional) If prompted, click **Save**.

Upload Root Certificate for Third-Party CAs

Upload the CA root certificate to the CAPF-trust store and the Unified Communications Manager trust store to use an external CA to sign LSC certificates.

Note Skip this task if you don't want to use a third-party CA to sign LSCs.

Procedure

Step 1 From Cisco Unified OS Administration choose **Security** > **Certificate Management**.
Step 2 Click **Upload Certificate/Certificate chain**.
Step 3 From the **Certificate Purpose** drop-down list, choose **CAPF-trust**.
Step 4 Enter a **Description** for the certificate. For example, **Certificate for External LSC-Signing CA**.
Step 5 Click **Browse**, navigate to the file, and then click **Open**.
Step 6 Click **Upload**.
Step 7 Repeat this task, uploading certificates to **callmanager-trust** for the **Certificate Purpose**.

TLS Prerequisites

Before you configure the minimum TLS version, make sure that your network devices and applications both support the TLS version. Also, make sure that they are enabled for TLS that you want to configure with Unified Communications Manager and IM and Presence Services. If you have any of the following products deployed, confirm that they meet the minimum TLS requirement. If they do not meet this requirement, upgrade those products:

- Skinny Client Control Protocol (SCCP) Conference Bridge
- Transcoder
- Hardware Media Termination Point (MTP)
- SIP Gateway
- Cisco Prime Collaboration Assurance

- Cisco Prime Collaboration Provisioning
- Cisco Prime Collaboration Deployment
- Cisco Unified Border Element (CUBE)
- Cisco Expressway
- Cisco TelePresence Conductor

You will not be able to upgrade conference bridges, Media Termination Point (MTP), Xcoder, Prime Collaboration Assurance, and Prime Collaboration Provisioning.

Note If you are upgrading from an earlier release of Unified Communications Manager, make sure that all your devices and applications support the higher version of TLS before you configure it. For example, Unified Communications Manager and IM and Presence Services, Release 9.x supports TLS 1.0 only.

Set Minimum TLS Version

By default, Unified Communications Manager supports a minimum TLS version of 1.0. Use this procedure to reset the minimum supported TLS version for Unified Communications Manager and the IM and Presence Service to a higher version, such as 1.1 or 1.2.

Make sure that the devices and applications in your network support the TLS version that you want to configure. For details, see TLS Prerequisites, on page 3.

Procedure

Step 1 Log in to the **Command Line Interface**.

Step 2 To confirm the existing TLS version, run the **show tls min-version** CLI command.

Step 3 Run the **set tls min-version** <*minimum*> CLI command where <*minimum*> represents the TLS version.

For example, run **set tls min-version 1.2** to set the minimum TLS version to 1.2.

Step 4 Perform Step 3 on all Unified Communications Managerand IM and Presence Service Service cluster nodes.

Set TLS Ciphers

You can disable the weaker cipher, by choosing available strongest ciphers for the SIP interface. Use this procedure to configure the ciphers that Unified Communications Manager supports for establishing TLS connections.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 In **Security Parameters**, configure a value for the **TLS Ciphers** enterprise parameter. For help on the available options, refer to the enterprise parameter online help.

Step 3 Click **Save**.