TLS Setup

TLS Overview

Transport Layer Security (TLS) provides secure and reliable signaling and data transfer between two systems or devices, by using secure ports and certificate exchange. TLS secures and controls connections among Unified Communications Manager-controlled systems, devices, and processes to prevent access to the voice domain.

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.

TLS Configuration Task Flow

Complete the following tasks to configure Unified Communications Manager for TLS connections.

Procedure

	Command or Action	Purpose
Step 1	Set Minimum TLS Version, on page 3.	By default, Unified Communications Manager supports a minimum TLS version of 1.0. If your security needs require a higher version of TLS, reconfigure the system to use TLS 1.1 or 1.2.
Step 2	(Optional) Set TLS Ciphers, on page 3.	Configure the TLS cipher options that Unified Communications Manager supports.
Step 3	Configure TLS in a SIP Trunk Security Profile, on page 3.	Assign TLS connections to a SIP Trunk. Trunks that use this profile use TLS for signaling. You can also use the secure trunk to add TLS connections to devices, such as conference bridges.
Step 4	Add Secure Profile to a SIP Trunk, on page 4.	Assign a TLS-enabled SIP trunk security profile to a SIP trunk to allow the trunk to support TLS. You can use the secure trunk to connect resources, such as conference bridges.
Step 5	Configure TLS in a Phone Security Profile, on page 4.	Assign TLS connections to a phone security profile. Phones that use this profile use TLS for signaling.
Step 6	Add Secure Phone Profile to a Phone, on page 5.	Assign the TLS-enabled profile that you created to a phone.
Step 7	Add Secure Phone Profile to a Universal Device Template, on page 6.	Assign a TLS-enabled phone security profile to a universal device template. If you have the LDAP directory synchronization configured with this template, you can provision phones with security through the LDAP sync.

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 1.

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**.

Note All TLS Ciphers will be negotiated based on client cipher preference

Configure TLS in a SIP Trunk Security Profile

Use this procedure to assign TLS connections to a SIP Trunk Security Profile. Trunks that use this profile use TLS for signaling.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Security** > **SIP Trunk Security Profile**.

Step 2 Perform one of the following steps:

- Click **Add New** to create a new SIP trunk security profile.
- Click **Find** to search and select an existing profile.

Step 3 In the **Name** field, enter a name for the profile.

Step 4 Configure the **Device Security Mode** field value to **Encrypted** or **Authenticated**.

Step 5 Configure both the **Incoming Transport Type** and **Outgoing Transport Type** field values to **TLS**.

Step 6 Complete the remaining fields of the **SIP Trunk Security Profile** window. For help on the fields and their configuration, see the online help.

Step 7 Click **Save**.

Add Secure Profile to a SIP Trunk

Use this procedure to assign a TLS-enabled SIP trunk security profile to a SIP trunk. You can use this trunk to create a secure connection to resources, such as conference bridges.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Trunk**.

Step 2 Click **Find** to search and select an existing trunk.

Step 3 For the **Device Name** field, enter a device name for the trunk.

Step 4 From the **Device Pool** drop-down list, choose a device pool.

Step 5 From the **SIP Profile** drop-down list, choose a SIP Profile.

Step 6 From the **SIP Trunk Security Profile** drop-down list, choose the TLS-enabled SIP Trunk Profile that you created in the previous task.

Step 7 In the **Destination** area, enter the destination IP address. You can enter up to 16 destination addresses. To enter additional destinations, click the (+) button.

Step 8 Complete the remaining fields in the **Trunk Configuration** window. For help with the fields and their configuration, see the online help.

Step 9 Click **Save**.

Note If you are connecting the trunk to a secure device, you must upload a certificate for the secure device to Unified Communications Manager. For certificate details, see the **Certificates** section.

Configure TLS in a Phone Security Profile

Use this procedure to assign TLS connections to a Phone Security Profile. Phones that use this profile use TLS for signaling.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Security** > **Phone Security Profile**.

Step 2 Perform one of the following steps:

- Click **Add New** to create a new profile.
- Click **Find** to search and select an existing profile.

Step 3 If you are creating a new profile, select a phone model and protocol, and click **Next**.

Note If you want to use a universal device template and LDAP sync to provision security through the LDAP sync, select **Universal Device Template** as the **Phone Security Profile Type**.

Step 4 Enter a name for the profile.

Step 5 From the **Device Security Mode** drop-down list, select either **Encrypted** or **Authenticated**.

Step 6 (For SIP phones only) From the Transport Type, select **TLS**.

Step 7 Complete the remaining fields of the **Phone Security Profile Configuration** window. For help with the fields and their configuration, see the online help.

Step 8 Click **Save**.

Add Secure Phone Profile to a Phone

Use this procedure to assign the TLS-enabled phone security profile to a phone.

Note To assign a secure profile to a large number of phones at once, use the Bulk Administration Tool to reassign the security profile for them.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Perform one of the following steps:

- Click **Add New** to create a new phone.
- Click **Find** to search and select an existing phone.

Step 3 Select the phone type and protocol and click **Next**.

Step 4 From the **Device Security Profile** drop-down list, assign the secure profile that you created to the phone.

Step 5 Assign values for the following mandatory fields:

- MAC address
- Device Pool
- SIP Profile
- Owner User ID
- Phone Button Template

Step 6 Complete the remaining fields of the **Phone Configuration** window. For help with the fields and their configuration, see the online help.

Step 7 Click **Save**.

Add Secure Phone Profile to a Universal Device Template

Use this procedure to assign a TLS-enabled phone security profile to a universal device template. If you have LDAP directory sync configured, you can include this universal device template in the LDAP sync through a feature group template and user profile. When the sync occurs, the secure profile is provisioned to the phones.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Universal Device Template**.

Step 2 Perform one of the following steps:

- Click **Add New** to create a new template.
- Click **Find** to search and select an existing template.

Step 3 For the **Name** field, enter a name for the template.

Step 4 From the **Device Pool** drop-down list, select a device pool.

Step 5 From the **Device Security Profile** drop-down list, select the TLS-enabled security profile that you created.

Note The Phone Security Profile must have been created with **Universal Device Template** as the device type.

Step 6 Select a **SIP Profile**.

Step 7 Select a **Phone Button Template**.

Step 8 Complete the remaining fields of the **Universal Device Template Configuration** window. For help with the fields and their configuration, see the online help.

Step 9 Click **Save**.
Include the Universal Device template in an LDAP directory synchronization. For details on how to set up an LDAP Directory sync, see the “Configure End Users” part of the System Configuration Guide for Cisco Unified Communications Manager.

TLS Interactions and Restrictions

This chapter provides information about the TLS Interactions and Restrictions.

TLS Interactions

Table 1: TLS Interactions

Feature	Interaction
Common Criteria mode	You can enable Common Criteria mode along with configuration of minimum TLS version. If you do so, the applications continue to comply with Common Criteria requirements and disable TLS 1.0 secure connections at application level. When the common criteria mode is enabled, you can configure the minimum TLS version as either 1.1 or 1.2 for the applications. For details on Common Criteria mode, see the Compliance to Common Criteria topic of the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

TLS Restrictions

The following table highlights issues that you may run into when implementing Transport Layer Security (TLS) version 1.2 on legacy phones, such as 79xx, 69xx, 89xx, 99xx, 39xx, and IP Communicator. To verify whether your phone supports secure mode in this release, see the Phone Feature List Report in Cisco Unified Reporting. The feature restrictions on legacy phones and the workaround to implement the feature is listed in the following table:

Note The workarounds are designed to get the impacted feature functioning in your system. However, they do not guarantee TLS 1.2 compliance for that feature.

Table 2: Transport Layer Security Version 1.2 Restrictions

Feature	Restriction
Legacy phones in Encrypted Mode	Legacy phones in Encrypted Mode do not work. There is no workaround.
Legacy phones in Authenticated Mode	Legacy phones in Authenticated Mode do not work. There is no workaround.
IP Phone services using secure URLs based on HTTPS.	IP Phone services using secure URLs based on HTTPS do not work. Workaround to use IP Phone services: Use HTTP for all underlying service options. For example, corporate directory and personal directory. However, HTTP is not recommended as HTTP is not as secure if you need to enter sensitive data for features, such as Extension Mobility. The drawbacks of using HTTP include: • Provisioning challenges when configuring HTTP for legacy phones and HTTPS for supported phones. • No resiliency for IP Phone services. • Performance of the server handling IP phone services can be affected.

Feature	Restriction
Extension Mobility Cross Cluster (EMCC) on legacy phones	EMCC is not supported with TLS 1.2 on legacy phones. Workaround: Complete the following tasks to enable EMCC: **1.** Enable EMCC over HTTP instead of HTTPS. **2.** Turn on mixed-mode on all Unified Communications Manager clusters. **3.** Use the same USB eTokens for all Unified Communications Manager clusters.
Locally Significant Certificates (LSC) on legacy phones	LSC is not supported with TLS 1.2 on legacy phones. As a result, 802.1x and phone VPN authentication based on LSC are not available. Workaround for 802.1x: Authentication based on MIC or password with EAP-MD5 on older phones. However, those are not recommended. Workaround for VPN: Use phone VPN authentication based on end-user username and password.
Encrypted Trivial File Transfer Protocol (TFTP) configuration files	Encrypted Trivial File Transfer Protocol (TFTP) configuration files are not supported with TLS 1.2 on legacy phones even with Manufacturer Installed Certificate (MIC). There is no workaround.
CallManager certificate renewal causes legacy phones to lose trust	Legacy phones lose trust when CallManager certificate is renewed. For example, a phone cannot get new configurations after renewing the certificate. This is applicable only in Unified Communications Manager 11.5.1 Workaround: To prevent legacy phones from losing trust, complete the following steps: **1.** Before you enable the CallManager certificate, set the **Cluster For Roll Back to Pre 8.0** enterprise parameter to **True**. By default, this setting disables the security. **2.** Temporarily allow TLS 1.0 (multiple Unified Communications Manager reboots).
Connections to non-supported versions of Cisco Unified Communications Manager	TLS 1.2 connections to older versions of Unified Communications Manager that do not support the higher TLS version do not work. For example, a TLS 1.2 SIP trunk connection to Unified Communications Manager Release 9.x does not work because that release does not support TLS 1.2. You can use one of the following workarounds: • Workaround to enable connections: Use nonsecure trunks, although this is not a recommended option. • Workaround to enable connections while using TLS 1.2: Upgrade the non-supported version to a release that does support TLS 1.2.

Feature	Restriction
Certificate Trust List (CTL) Client	CTL client does not support TLS 1.2. You can use one of the following workarounds: • Temporarily allow TLS 1.0 when using the CTL client and then move the Cluster to Common Criteria mode. Configure Minimum TLS to 1.1 or 1.2 • Migrate to the Tokenless CTL by using the CLI Command **utils ctl set-cluster mixed-mode** in Common Criteria mode. Configure Minimum TLS to 1.1 or 1.2
Address Book Synchronizer	There is no workaround.

Cisco Unified Communications Manager Ports Affected by Transport Layer Security Version 1.2

The following table lists the Unified Communications Manager Ports Affected By TLS Version 1.2

Table 3: Cisco Unified Communications Manager Ports Affected by Transport Layer Security Version 1.2

Application	Protocol	Destination / Listener	Cisco Unified Communications Manager Operating in Normal mode			Cisco Unified Communications Manager Operating in Common Criteria Mode		
			Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2	Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2
Tomcat	HTTPS	443	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS v1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
SCCP - SEC - SIG	Signalling Connection Control Part (SCCP)	2443	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
CTL-SERV	Proprietary	2444	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
Computer Telephony Integration (CTI)	Quick Buffer Encoding (QBE)	2749	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
CAPF-SERV	Transmission Control Protocol (TCP)	3804	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2

Application	Protocol	Destination / Listener	Cisco Unified Communications Manager Operating in Normal mode			Cisco Unified Communications Manager Operating in Common Criteria Mode		
			Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2	Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2
Intercluster Lookup Service (ILS)	Not applicable	7501	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
Administrative XML (AXL)	Simple Object Access Protocol (SOAP)	8443	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
High Available-Proxy (HA-Proxy)	TCP	9443	TLS 1.2	TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.2	TLS 1.2
SIP-SIG	Session Initiation Protocol (SIP)	5061 (configurable with trunk)	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
HA Proxy	TCP	6971, 6972	TLS 1.2	TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
Cisco Tomcat	HTTPS	8080, 8443	8443: TLS 1.0, TLS 1.1, TLS 1.2	8443: TLS 1.1, TLS 1.2	8443: TLS 1.2	TLS 1.1	8443: TLS 1.1, TLS 1.2	8443: TLS 1.2
Trust Verification Service (TVS)	Proprietary	2445	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2

Instant Messaging and Presence Ports Affected by Transport Layer Security Version 1.2

The following table lists the IM and Presence Service Ports Affected By Transport Layer Security Version 1.2:

Table 4: Instant Messaging & Presence Ports Affected by Transport Layer Security Version 1.2

Destination/Listener	Instant Messaging & Presence Operating in Normal mode			Instant Messaging & Presence Operating in Common Criteria mode		
	Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2	Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2
443	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
5061	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
5062	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
7335	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
8083	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
8443	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2