



# TLS 1.3 Configuration Overview Guide

First Published: October 2024

## Overview

For security or compliance reasons, administrators can lock down the TLS version of many Cisco Collaboration products to 1.3 and disable TLS 1.0 and TLS 1.1. For an overview, considerations, and implications of enabling TLS 1.3 and disabling TLS 1.0 or 1.1, see the *TLS 1.3 for On-Premises Cisco Collaboration Deployments* available at [Link](#).

This document provides an overview of how to enable TLS 1.3 and disable TLS 1.0 and 1.1 for Cisco Collaboration products. It also provides references to the relevant product documentation.

**Note:** Upgrades to 15SU2 or the version mentioned for each product automatically enable TLS 1.3, and only the set TLS version disables versions lower than the configured version.

## Configuration

The following table outlines how to configure your Cisco Collaboration products for TLS 1.3.

**Prerequisite:** Before configuring your products for TLS 1.3, verify that your product versions can enable TLS 1.3 and disable TLS 1.0 and 1.1. For a list of product versions with this capability, see the [TLS 1.3 Compatibility Matrix for Cisco Collaboration Products](#).

**Note:** You can configure TLS 1.3 and disable TLS 1.0 and 1.1 for the following products in any order.

Table 1. Configure Collaboration Products for TLS 1.3

Product	How to Configure TLS 1.3	References to Product Documentation
Call Control		
Cisco Unified Communications Manager and IM and Presence Service	Use CLI Command: <code>set tls min-version &lt;1.0   1.1   1.2   1.3&gt;</code>	<i>The TLS Setup</i> chapter in the <i>Security Guide for Cisco Unified Communications Manager</i> is available at <a href="https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html">https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html</a>
Cisco Unified Survivable Remote Site Telephony	Use CLI Command: <code>sip-ua transport tcp tls [v1.0   v1.1   v1.2   v1.3]</code>	<i>Cisco Unified SCCP and SIP SRST System Administrator Guide</i> is available at <a href="https://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/products-installation-and-configuration-guides-list.html">https://www.cisco.com/c/en/us/support/unified-communications/unified-survivable-remote-site-telephony/products-installation-and-configuration-guides-list.html</a>
Conferencing		

Cisco Meeting Server	Use CLI Command:  tls <sip   ldap   webadmin> min-tls-version <1.0   1.1   1.2   1.3>	<i>Cisco Meeting Server MMP Command Line Reference Guide</i> is available at <a href="https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html">https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html</a>
Cisco Meeting Management	No command is necessary. TLS 1.1 and 1.0 are disabled.	<i>Cisco Meeting Management Release Notes</i> are available at <a href="https://www.cisco.com/c/en/us/support/conferencing/meeting-management/products-release-notes-list.html">https://www.cisco.com/c/en/us/support/conferencing/meeting-management/products-release-notes-list.html</a>
Enterprise Edge		
Cisco Expressway Series	On the Maintenance > Security > Ciphers page of the product's web UI, you can configure the cipher suite and minimum supported TLS version for each service.	<i>Cisco Expressway Administrator Guide</i> is available at <a href="https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-maintenance-guides-list.html">https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-maintenance-guides-list.html</a>
Cisco Unified Border Element (CUBE)	Use CLI Command:  sip-ua  transport tcp tls <1.0   1.1   1.2   1.3>  For dspfarm configuration, it is  Dspfarm profile <n> conference security  Tls-version <v1.0   v1.1   v1.2   v1.3>	<i>Cisco Unified Border Element Configuration Guide</i> is available at <a href="https://www.cisco.com/c/en/us/support/unified-communications/unified-border-element/products-installation-and-configuration-guides-list.html">https://www.cisco.com/c/en/us/support/unified-communications/unified-border-element/products-installation-and-configuration-guides-list.html</a>
SIP PSTN Gateway	Use CLI Command:  sip-ua  transport tcp tls [v1.0   v1.1   v1.2   v1.3]	<i>Cisco Unified Border Element Configuration Guide</i> is available at <a href="https://www.cisco.com/c/en/us/support/unified-communications/unified-border-element/products-installation-and-configuration-guides-list.html">https://www.cisco.com/c/en/us/support/unified-communications/unified-border-element/products-installation-and-configuration-guides-list.html</a>
Server Applications		
Cisco Emergency Responder	For pre 12.0(1)SU1, install cop file.  For 12.0(1)SU1+, use CLI command:  set tls min-version <1.0   1.1   1.2   1.3>	<i>Cisco Emergency Responder Version Release Notes</i> are available at <a href="https://www.cisco.com/c/en/us/support/unified-communications/emergency-responder/products-release-notes-list.html">https://www.cisco.com/c/en/us/support/unified-communications/emergency-responder/products-release-notes-list.html</a>
Voicemail and Messaging		

Cisco Unity Connection	Use CLI Command:  set tls min-version <1.0   1.1   1.2   1.3>	<i>IP Communications Required by Cisco Unity Connection</i> chapter in the <i>Security Guide for Cisco Unity Connection Guides</i> is available at <a href="https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-user-guide-list.html">https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-user-guide-list.html</a>
Endpoints		
Cisco IP Phone 7800 and 8800 Series	<b>From Cisco Unified CM, set “Disable TLS 1.0 and TLS 1.1 for Web Access”</b> to enabled or disabled.	<p><i>The TLS Setup</i> chapter of the <i>Security Guide for Cisco Unified Communications Manager</i> is available at <a href="https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html">https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html</a></p> <p><i>The Cisco IP Phone Administration</i> chapter in the <i>Cisco IP Phone 7800 Series Administration Guide for Cisco Unified Communications Manager</i> is available at <a href="https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7800-series/products-maintenance-guides-list.html">https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7800-series/products-maintenance-guides-list.html</a></p> <p><i>The Cisco IP Phone Administration</i> chapter in the <i>Cisco IP Phone 8800 Series Administration Guide for Cisco Unified Communications Manager</i> is available at <a href="https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-maintenance-guides-list.html">https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-maintenance-guides-list.html</a></p>
Cisco Video Phone 8875	TLS Client Min Version  TLS Server Min Version	
Cisco Desk Phone 9800 Series	TLS Client Min Version  TLS Server Min Version	
Cisco RoomOS	TLS 1.0 is always disabled. To disable TLS 1.1, go to Setup > Configuration > NetworkServices > ServerMinimumTLSVersion in the endpoint web interface.	
Cisco Webex App		
Cisco Jabber	Not applicable. There is no TLS server interface.	<a href="https://www.cisco.com/c/en/us/products/unified-communications/jabber/index.html">https://www.cisco.com/c/en/us/products/unified-communications/jabber/index.html</a>
Service Management		

Cisco Prime Collaboration (Deployment)	Use CLI Command: set tls min-version <1.0   1.1   1.2   1.3>	The <i>minimum TLS Version Control</i> chapter in the <i>Cisco Prime Collaboration Deployment Administration Guide</i> is available at <a href="https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html">https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html</a>
Communication Gateways		
STC App and Cisco VG Series Gateways	Use CLI Command: stcapp security tls-version v1.3	<i>Configuring Voice Functionality</i> chapter in the <i>Cisco 4000 Series ISRs Software Configuration Guide</i> is available at <a href="https://www.cisco.com/c/en/us/support/routers/4000-series-integrated-services-routers-isr/products-installation-and-configuration-guides-list.html">https://www.cisco.com/c/en/us/support/routers/4000-series-integrated-services-routers-isr/products-installation-and-configuration-guides-list.html</a>
Other		
IOS MTP/CFB	Use CLI Command: dspfarm profile <n> conference security tls-version <v1.0   v1.1   v1.2   v1.3>	The <i>Cisco 4000 Series ISRs Software Configuration Guide</i> is available at <a href="https://www.cisco.com/c/en/us/support/routers/4000-series-integrated-services-routers-isr/products-installation-and-configuration-guides-list.html">https://www.cisco.com/c/en/us/support/routers/4000-series-integrated-services-routers-isr/products-installation-and-configuration-guides-list.html</a>

## Documentation Changes

Table 2. Documentation Changes

Date	Change
October 2024	Updated and Published the guide for TLS 1.3.

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see [What's New in Cisco Product Documentation](#).

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.