TLS 1.3 for On-Premises Cisco Collaboration Deployments

First Published: November 2024

Contents

Introduction

TLS is a secure transport and session protocol that provides confidentiality and message integrity between a server and a client connection. This protocol uses cryptography and hashing techniques known as a cipher suite.

The primary goal of TLS is to provide a secure channel between two communicating peers.

Specifically, the secure channel should provide the following properties:

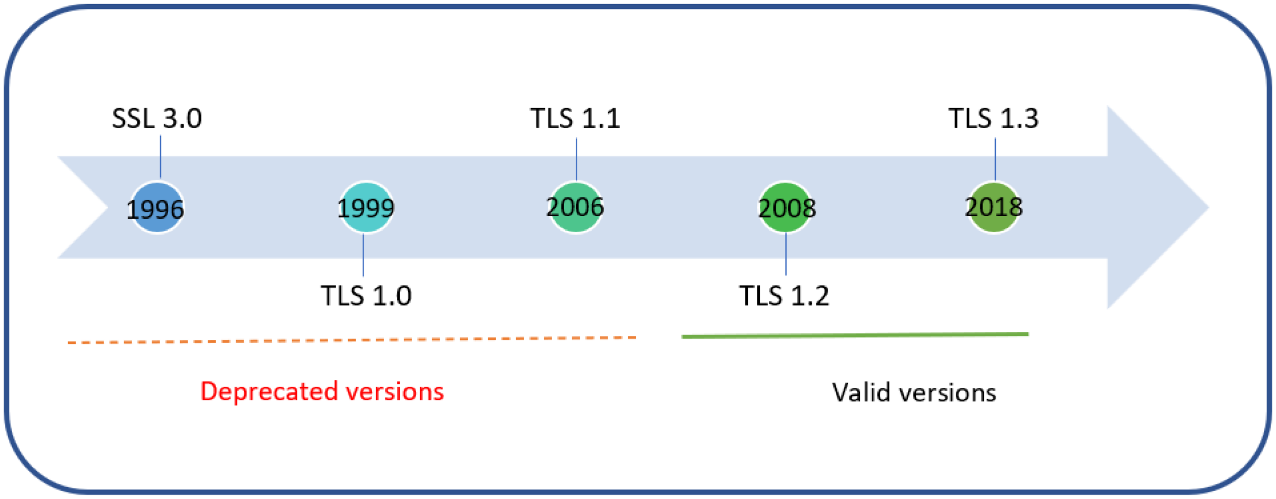
- **Authentication**: The server side of the channel is always authenticated; the client side is optionally authenticated.

— Authentication can happen using asymmetric cryptography (for example, RSA, the Elliptic Curve Digital Signature Algorithm (ECDSA), the Edwards-Curve Digital Signature Algorithm (ECDSA)) or a symmetric pre-shared key (PSK).

- **Confidentiality**: Data sent over the channel after establishment is only visible to the endpoints.

- **Integrity**: Attackers cannot modify data sent over the channel after establishment without detection.

SSL/TLS was established in the mid-1990s. Due to exploiting vulnerabilities, it has undergone several changes over the years.



Transport Layer Security (TLS) and its predecessor, Secure Socket Layer (SSL), are cryptographic protocols providing network communications security. SSL, TLS 1.0, and sometimes TLS 1.1 have security vulnerabilities. Hence, several organizations prefer TLS 1.2 or 1.3.

Why TLS 1.3?

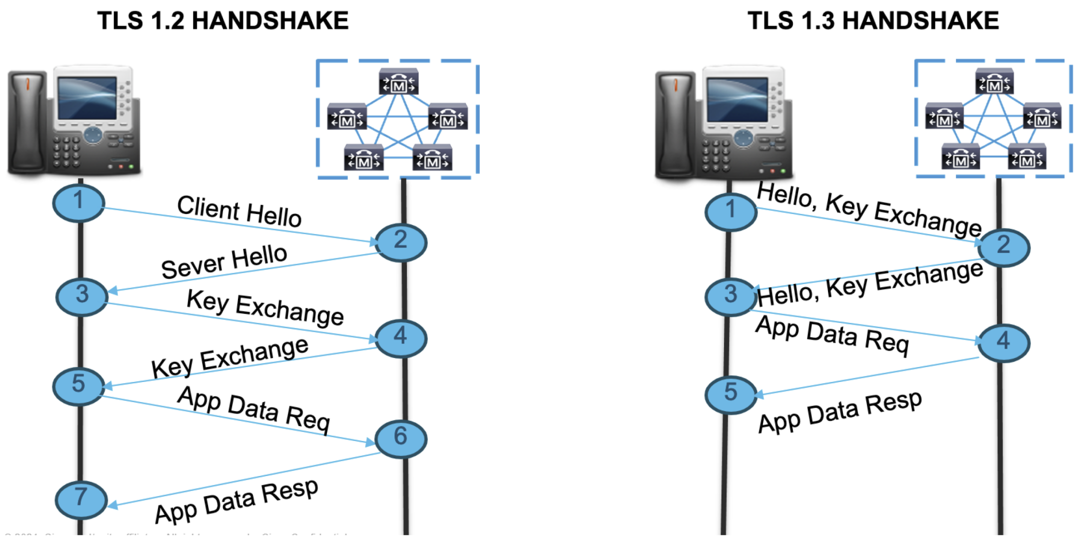
TLS 1.3 is designed to be faster and more secure than its predecessor TLS 1.2. Here are some key differentiating factors:

Simplified handshake process

- TLS 1.2 handshake requires multiple round trips (usually 2) between the client and the server. This causes latency and slower connection time.

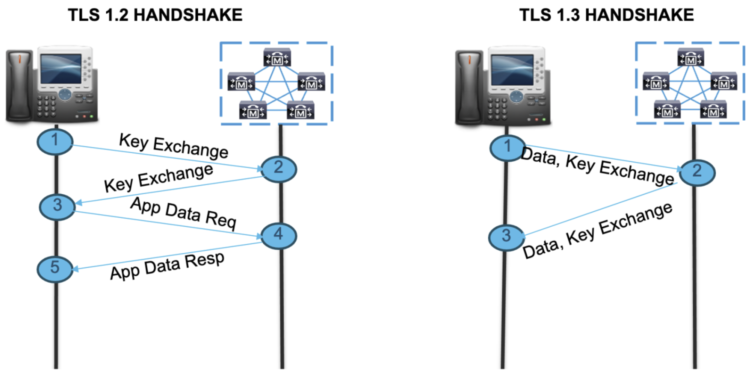
- TLS 1.3 handshake uses only 1 round trip in most cases. It also introduces “0-RTT” (Zero round-trip time), which allows a few connections to resume even without a round trip.

Faster TLS 1.3 Handshake - 1RTT



0 RTT (Zero Round Trip Time)–If the client had connected to a server in a session and the session is currently invalid, TLS 1.3 utilizes parameters agreed upon during the previous session, permitting a zero-round-trip handshake.

TLS 1.3 Supporting 0-RTT



Improved security

- **Removed Weaker Algorithms**: Legacy weaker encryption algorithms (e.g., RSA key exchange) are pruned, and only Authenticated Encryption with Associated Data (AEAD) algorithms are supported
- **Perfect forward secrecy (PFS) enabled by default**: TLS 1.3 uses ephemeral Diffie-Hellman key exchanges to enforce PFS, ensuring the safety of the session keys even when a server's private key is compromised.
- **Simplified Cipher suites**: TLS 1.2 had many cipher suites, some of which were insecure. TLS 1.3 has removed insecure old ciphers and has only AEAD ciphers (Authenticated Encryption with Associated Data). AEAD functions provide a unified encryption and authentication operation. These turn plaintext into authenticated ciphertext and back again.
- **Better Privacy Protections**: All messages in the handshake (after Server Hello) are encrypted. In TLS 1.3, handshake information (such as the server certificate) is encrypted. This hides more information and offers better privacy than TLS 1.2, which often had the entire handshake in plaintext.

Improved performance

- **Reduced Latency**: TLS 1.3 reduces the overall latency during connection time with shorter round-trip time. 0-RTT facilitates faster resumption of previous connections, which is particularly useful for connections over high-latency networks.
- **Streamlined Negotiation**: TLS 1.3 reduces handshake overhead and computational load, making it more efficient. Many unnecessary extensions and features are removed.

Charter to support TLS 1.3

- **Improved security posture***:* TLS version 1.3 is gaining broader use and acceptance, ensuring that Enterprise customers adhere to newer, more secure standards.
- **NIST Recommendations**: NIST recommends transitioning away from earlier versions of TLS protocols and developing plans to support the transition to TLS 1.3 protocol. Support will commence by January 1, 2024. NIST Link.

Transitioning to TLS 1.3

Enabling support for TLS 1.3 is essential to strengthen the security of this solution. Customers are left with a few unviable options without this upgrade:

- **No Encryption**: An option that leaves data highly vulnerable.
- **Older TLS Version**: Older TLS versions lack the robust security features of TLS 1.3, as described in the previous section. Some of these protocol versions do not meet current security standards or policies.

Hence, a comprehensive approach is taken to enable TLS 1.3 on every interface of an on-premise product. For Example

- **VOS Products**: CUCM, IM and Presence, CER, CUC
- **Hard Endpoint**: Cisco IP Phones (Enterprise and MPP), CE Phones, Room Endpoints

- **Soft Endpoints**: Jabber, Webex Teams
- **Edge Products**: Expressway, CUBE
- **Other products**: PCD

Keep these in mind while implementing the migration to minimize the impact.

- Provide a default TLS 1.3 support without requiring additional intervention from an Administrator.
- Retain existing configuration and interconnect after the upgrade.
- Retain existing certificate offering as part of TLS handshake in TLS connection.
- Retain backward compatibility.
- Support for both inbound and outbound connections.
- Simplified configuration.

TLS 1.3 enabled by default

After upgrading the product/component, all transport interfaces (e.g., HTTPS, SIP, etc.) will provide default TLS 1.3 support without any intervention from an Administrator.

Interfaces acting like a TLS Server

Interfaces where products act as TLS servers will accept TLS 1.3 as their highest preferred version.
If the client connecting to these servers does not offer TLS 1.3, the server automatically tries the next maximum version that the Peer offers. The minimum TLS version configured on the product/interface governs this auto fallback.

Interfaces acting like a TLS Client

Product interfaces that act as TLS clients offer TLS 1.3 as their highest preferred TLS version. These will continue to offer all the other TLS base versions over the minimum TLS version configured on the product/interface.

The table below outlines server and client-side TLS compatibility.

		Server TLS protocol			
	Version	Min TLS1.2	Min TLS1.3	Max TLS1.2	Max TLS 1.3
Client TLS protocol	Min TLS1.2	1 ✓ 1.3	✓ 1.3	✓ 1.2	✓ 1.3
	Min TLS1.3	✓ 1.3	✓ 1.3	2 ×	✓ 1.3

	Max TLS1.2	✓ 1.2	✕	✓ 1.2	✓ 1.2
	Max TLS1.3	✓ 1.3	✓ 1.3	✓ 1.2	✓ 1.3

For example,

[1] – The Client supports both TLS 1.2 and 1.3. The server also supports both TLS 1.2 and 1.3. In this scenario, the connection will be negotiated using TLS 1.3.

[2] – Similarly, the connection will not be established if the client offers only TLS 1.3 and the server offers only TLS 1.2.

Retain existing configuration and interconnect after the upgrade

The TLS configuration does not change when a product or component is upgraded. For example, if the Minimum TLS version configured is TLS 1.2, the version remains unchanged after upgrading.

Retain existing certificate offering as part of TLS handshake in TLS connection

The default preference for TLS 1.3 is ECDSA over RSA signature algorithms. It will pick the corresponding certificate based on this preference using ECDSA during negotiations.

After the upgrade, all interfaces will use TLS 1.3 as the preferred protocol version. CUCM and IM & Presence SIP interfaces always offer RSA and ECDSA certificates. Hence, there is a high chance that a successful connection requires an ECDSA certificate.

We have introduced “TLS 1.3 Certificate Preference Order” on CUCM and IM & Presence to maintain backward compatibility for these interfaces. Certificate and cipher preference can be controlled through the below configurations:

TLS 1.2 Ciphers Preference Order – When you select this parameter, Unified Communications Manager and/or IM and Presence Service will select an RSA or EC certificate based on the preference order of TLS 1.2 Ciphers if the client offers both the TLS 1.2 and 1.3 protocols. This option selects a specific certificate needed for TLS 1.3 connections. Connections continue to use the TLS 1.3 cipher and signature algorithm.

TLS 1.3 Signature Algorithm Preference Order – When you select this parameter, Unified Communications Manager and/or IM and Presence will select an RSA or EC certificate based on the preference order of the TLS 1.3 Signature Algorithm if the client offers TLS 1.3 protocol. It is highly recommended that the certificate requirements of the clients (devices) connecting to Unified Communications Manager and/or IM and Presence Service be reviewed, and the necessary certificates in the clients' trust store (including ECDSA) should be updated when using this option.

For clients offering only the TLS 1.3 protocol, Cisco Unified Communication Manager/IM and Presence will select an RSA or EC certificate based on the preference order of the TLS 1.3 Signature Algorithm, regardless of the setting of this parameter. This parameter will have no impact on TLS 1.2 protocol negotiation.

For more details on the enterprise parameter TLS 1.3 Certificate Preference Order, see the CUCM Security guide or online help.

Simplified Configuration

Cluster-wide Min TLS configuration using CLI for CUCM & IM and Presence: Since Release 15SU2, the set minimum TLS CLI command is supported cluster-wide. Any change to the Unified Communications Manager Publisher node is replicated across all other nodes in the cluster.
Users must configure the minimum TLS version on IM and Presence Service on the IM and Presence node separately. Restart all the nodes in the clusters for the changes to take effect.

Configuration needed to support TLS 1.3

The minimum TLS version can be configured using either the CLI or GUI of various products of the on-prem solution. Here, high-level information is provided about each product.

CUCM, IM and Presence, CER, and Unity Connection

From Rel 15SU2, no configuration is required since TLS 1.3 is set as default.

— **In case of fresh installation**

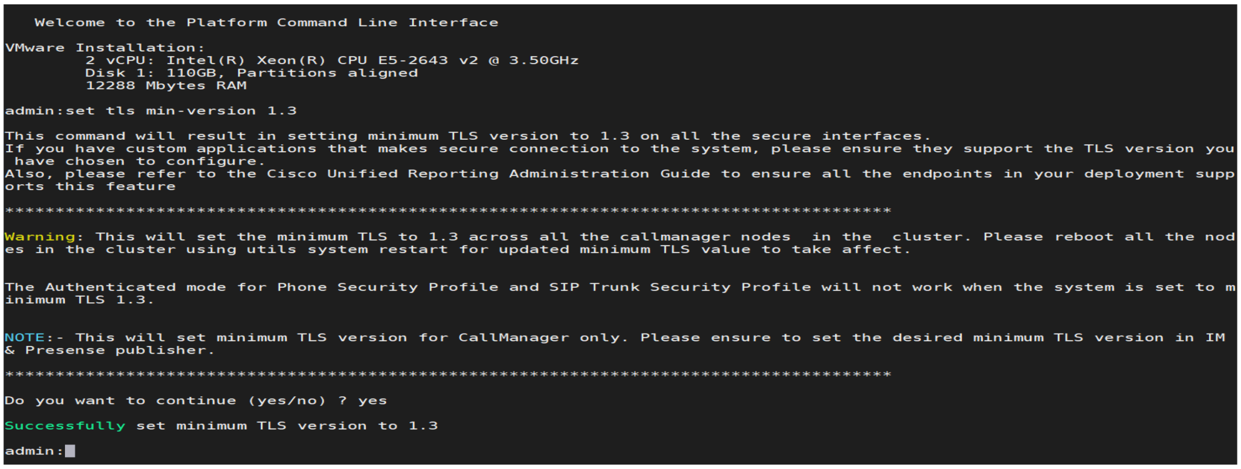
TLS versions 1.0 and 1.1 are disabled as a default setting.

Run the **set tls min-version** command if you want to configure the minimum TLS version as 1.0 or 1.1.

— **For upgrade and/or migration scenarios**, the supported TLS versions are TLS 1.0, 1.1, 1.2, and 1.3. The minimum TLS version is carried forward to the upgraded or migrated version.

Though 15SU2 still supports TLS 1.0 and 1.1, higher TLS versions are recommended to ensure product security.

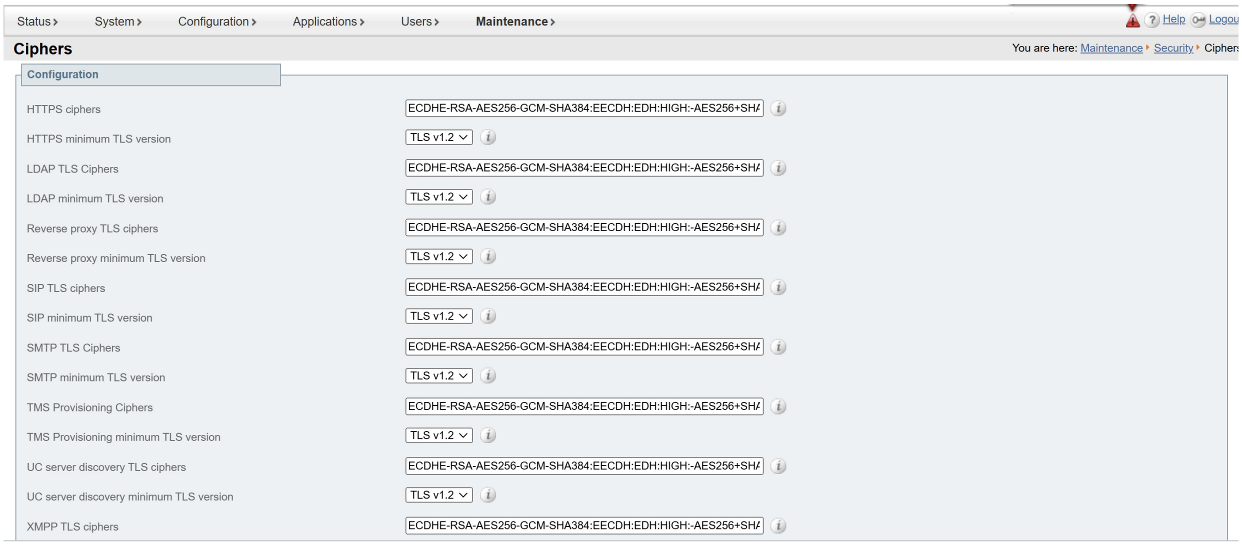
Example configuration of “set tls min-version”



```
   Welcome to the Platform Command Line Interface

VMware Installation:
        2 vCPU: Intel(R) Xeon(R) CPU E5-2643 v2 @ 3.50GHz
        Disk 1: 110GB, Partitions aligned
        12288 Mbytes RAM

admin:set tls min-version 1.3

This command will result in setting minimum TLS version to 1.3 on all the secure interfaces.
If you have custom applications that makes secure connection to the system, please ensure they support the TLS version you
 have chosen to configure.
Also, please refer to the Cisco Unified Reporting Administration Guide to ensure all the endpoints in your deployment supp
orts this feature

****************************************************************************************

Warning: This will set the minimum TLS to 1.3 across all the callmanager nodes  in the  cluster. Please reboot all the nod
es in the cluster using utils system restart for updated minimum TLS value to take affect.


The Authenticated mode for Phone Security Profile and SIP Trunk Security Profile will not work when the system is set to m
inimum TLS 1.3.


NOTE:- This will set minimum TLS version for CallManager only. Please ensure to set the desired minimum TLS version in IM
& Presense publisher.

****************************************************************************************

Do you want to continue (yes/no) ? yes

Successfully set minimum TLS version to 1.3

admin:
```

Expressway

As specified above, the configured TLS protocol version is retained as a default while upgrading from the current version to the TLS 1.3 support version. However, the Administrator can follow the Expressway configuration guide to set the minimum TLS version for each service using the Expressway User Interface.



Ciphers

Configuration

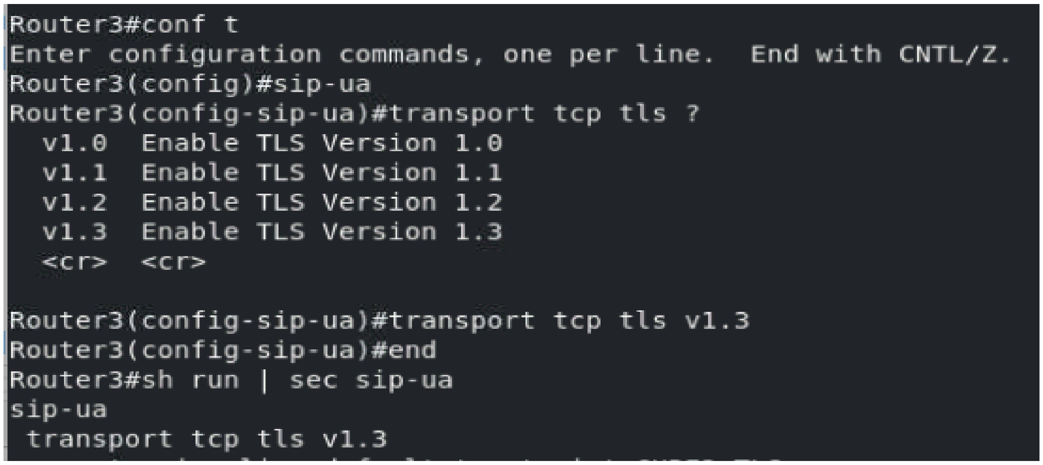
HTTPS ciphers	ECDHE-RSA-AES256-GCM-SHA384:EECDH:EDH:HIGH:-AES256+SHA
HTTPS minimum TLS version	TLS v1.2
LDAP TLS Ciphers	ECDHE-RSA-AES256-GCM-SHA384:EECDH:EDH:HIGH:-AES256+SHA
LDAP minimum TLS version	TLS v1.2
Reverse proxy TLS ciphers	ECDHE-RSA-AES256-GCM-SHA384:EECDH:EDH:HIGH:-AES256+SHA
Reverse proxy minimum TLS version	TLS v1.2
SIP TLS ciphers	ECDHE-RSA-AES256-GCM-SHA384:EECDH:EDH:HIGH:-AES256+SHA
SIP minimum TLS version	TLS v1.2
SMTP TLS Ciphers	ECDHE-RSA-AES256-GCM-SHA384:EECDH:EDH:HIGH:-AES256+SHA
SMTP minimum TLS version	TLS v1.2
TMS Provisioning Ciphers	ECDHE-RSA-AES256-GCM-SHA384:EECDH:EDH:HIGH:-AES256+SHA
TMS Provisioning minimum TLS version	TLS v1.2
UC server discovery TLS ciphers	ECDHE-RSA-AES256-GCM-SHA384:EECDH:EDH:HIGH:-AES256+SHA
UC server discovery minimum TLS version	TLS v1.2
XMPP TLS ciphers	ECDHE-RSA-AES256-GCM-SHA384:EECDH:EDH:HIGH:-AES256+SHA

CUBE

Transport Layer Security (TLS) version 1.3 support is introduced to enhance the security of CUBE flows in Cisco IOS XE 17.14.1a. The configured TLS protocol version is retained as part of the upgrade. However, you can configure the minimum tls protocol version can be configured using “transport tcp tls” under “sip-ua”.

Details can be found here.

Example configuration below:

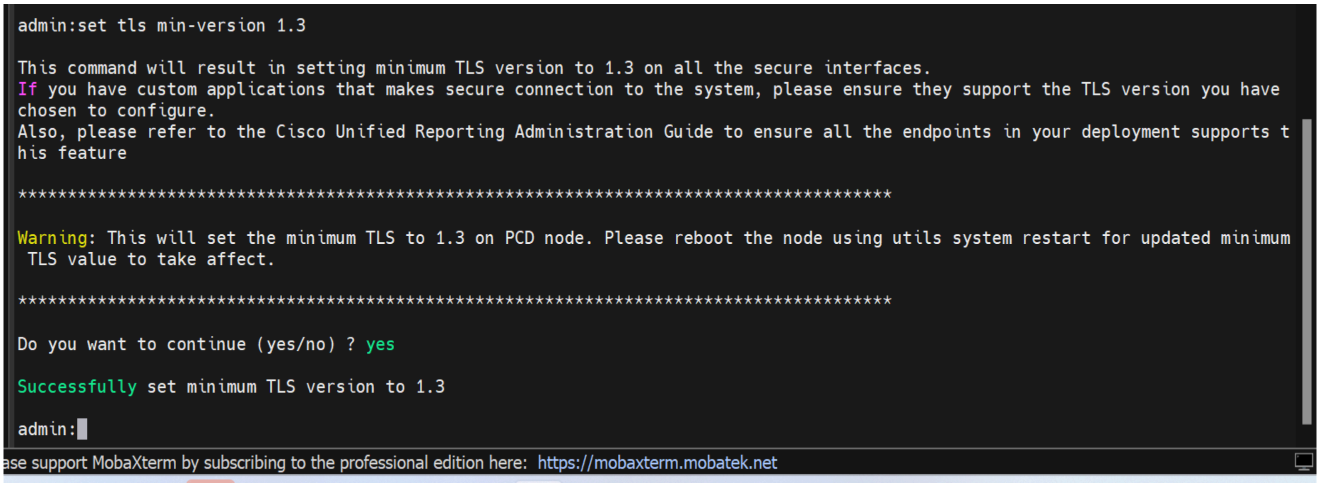


```
Router3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router3(config)#sip-ua
Router3(config-sip-ua)#transport tcp tls ?
  v1.0  Enable TLS Version 1.0
  v1.1  Enable TLS Version 1.1
  v1.2  Enable TLS Version 1.2
  v1.3  Enable TLS Version 1.3
  <cr>  <cr>

Router3(config-sip-ua)#transport tcp tls v1.3
Router3(config-sip-ua)#end
Router3#sh run | sec sip-ua
sip-ua
 transport tcp tls v1.3
```

PCD

PCD also offers TLS 1.3 by default. The minimum TLS version can be configured/modified using “set tls min-version.”

Example configuration of "set tls min-version"



```
admin:set tls min-version 1.3

This command will result in setting minimum TLS version to 1.3 on all the secure interfaces.
If you have custom applications that makes secure connection to the system, please ensure they support the TLS version you have
chosen to configure.
Also, please refer to the Cisco Unified Reporting Administration Guide to ensure all the endpoints in your deployment supports t
his feature

*****************************************************************************************

Warning: This will set the minimum TLS to 1.3 on PCD node. Please reboot the node using utils system restart for updated minimum
 TLS value to take affect.

*****************************************************************************************

Do you want to continue (yes/no) ? yes

Successfully set minimum TLS version to 1.3

admin:
```

ase support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

Limitations/Restrictions with TLS 1.3

CUCM, IM and Presence, CER, and Unity Connection

1. **Common Criteria Mode** - TLS 1.3 is not supported in Common Criteria mode in the 15SU2 version. Products will continue to offer TLS 1.2 as the highest preferred TLS version. This applies to CUCM, IM and Presence, CER, and Unity connections.

2. **Authenticated SIP Trunk and Phone**– Authenticated mode is not supported in TLS 1.3. Hence, devices that use TLS 1.3 can be configured as Encrypted or Non-secure.
   Authenticate mode will continue to work if the phone or trunk uses TLS 1.2 as the maximum supported version. Otherwise, this may lead to registration or call failures. Hence, configure it to use Encrypted mode for an Authenticated device.

3. **MS-SQL integration**– In release 15SU2, the IM and Presence server connection with the external database in MS-SQL does not support a TLS 1.3 connection.

Expressway

Expressway no longer supports certificates signed with SHA1. Before upgrading to Expressway X15.2, replace Expressway server certificates with 256/384/512 signed Certificates.

CUBE

1. ECDSA ciphers are not supported with TLS v1.0.

2. WebSocket-based media forking is not supported by TLS v1.3.

Minimum release requirements

Refer to release 15SU2 compatibility metrics for the minimum release requirement for TLS 1.3 support: Link

Use Cases

Fresh install with 15SU2 CUCM, IM & Presence

Cisco Unified Communications (UC) on-premises solutions offer a suite of collaboration tools designed to enhance communication efficiency and security within an organization. A fresh deployment of these solutions involves setting up various components in the local network, with a strong emphasis on securing communications through Transport Layer Security (TLS) 1.3.

Key Components of Cisco UC On-Premises Deployment

- Unified Communications Manager (CUCM)
- Cisco Unity Connection
- Cisco IM and Presence
- Cisco Expressway
- Cisco Unified Contact Center Express (UCCX)
- Endpoints and Devices

For Greenfield deployment, assess organizational requirements and design a secure network topology. Install and configure servers for CUCM, Unity Connection, IM and Presence, and other components. Ensure network infrastructure supports TLS 1.3 and has the necessary certificates installed.

The default connection support is TLS 1.3. On a fresh install, TLS 1.0 and 1.1 are disabled by default. Though 15SU2 still supports TLS 1.0 and 1.1, it is recommended to use higher TLS versions so that product security is not compromised.

TLS 1.3 uses Signature algorithms to choose between RSA or ECDSA-signed certificates. It evaluates the server's offers before deciding on the certificate type. TLS 1.3 does not have a separate Cipher Management settings page. It relies on the existing Service parameters, HTTP Ciphers, and the TLS Cipher settings.

SIP and other non-HTTP interfaces offer both RSA and ECDSA signature algorithms. Use HTTP Ciphers on the Enterprise Parameters Configuration page to load the RSA, RSA, and ECDSA certificates for HTTP inbound interfaces. The default setting is 'RSA only'.

Ensure that IP phones, video devices, and collaboration tools support TLS 1.3 so that deployment can work with end-to-end TLS 1.3 encryption.

Upgrade use case 1 – Standalone node

- **CUCM, IM and Presence, Unity Connection, CER**

For upgrade and/or migration scenarios, the supported TLS versions are TLS 1.0, 1.1, 1.2, and 1.3. The minimum TLS version is retained from the previous version after upgrade or migration scenarios.

Suppose Unified Communications Manager and IM and Presence Service securely connect to a service or application that does not support TLS 1.3 or later. In that case, they automatically fall back to a lower version based on the minimum TLS version configured to support interoperability.

Most deployments use RSA-signed certificates. A new service parameter, TLS 1.3 Certificate Preference Order, is added to maintain backward compatibility for deployments using RSA-signed certificates. This preference order is defaulted to. If you select the TLS 1.3 Signature Algorithm Preference Order, it falls back to the default TLS 1.3 protocol behavior.

- **Expressway**

If a SHA1-signed certificate is used in Expressway, as a first step, replace it with a SHA2-signed certificate before upgrading to Expressway X15.2. As mentioned, upgrading to Expressway X15.2 TLS 1.3 support is enabled by default. However, the existing minimum version is retained to prevent any functional loss after upgrading to Expressway X15.2

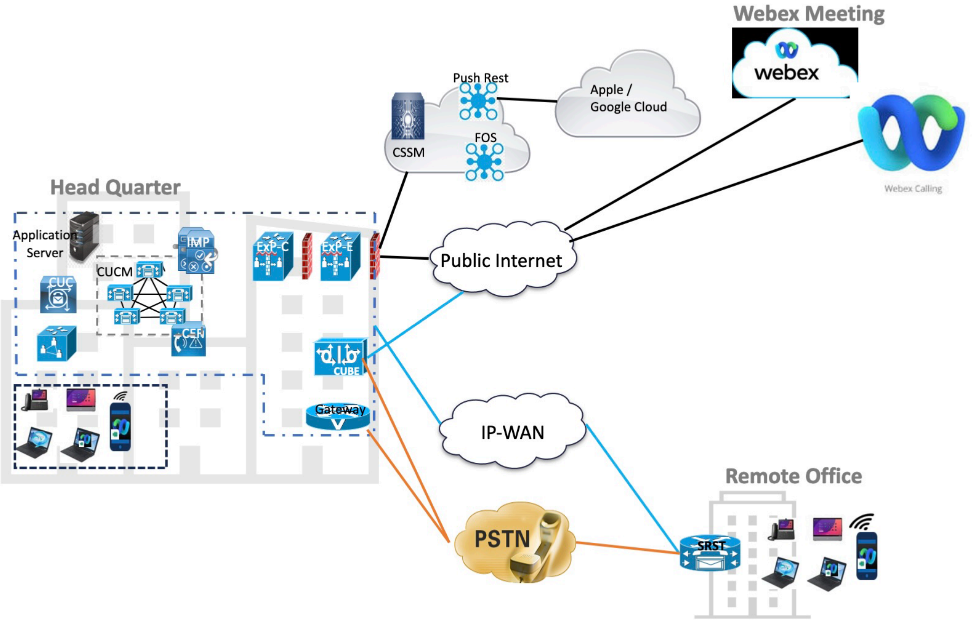
A new CLI is provided to change signature algorithm preference only for TLS connections related to the SIP protocol. For more information, see the Cisco Expressway SHA-1 Certificate Deprecation Rollout and SHA-2 Certificate Transition.

- **CUBE**

For more information, see the CUBE Upgrade Guide.

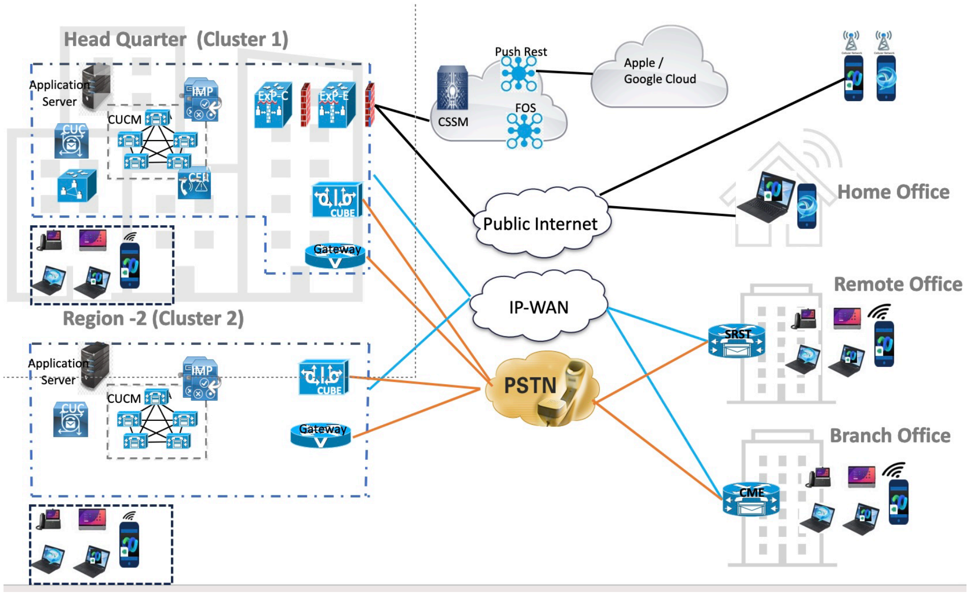
Upgrade use case 2- Single cluster upgrade

In the case of a single cluster upgrade, it's recommended that the edge components like Expressway and CUBE be upgraded. After upgrading these components, the TLS connection between Expressway/ CUBE and other components will continue because of backward compatibility. After that, CER and Unity can be upgraded without impacting any secure connection. After CER and UNITY, CUCM and IMP can be upgraded without impacting any TLS connection.



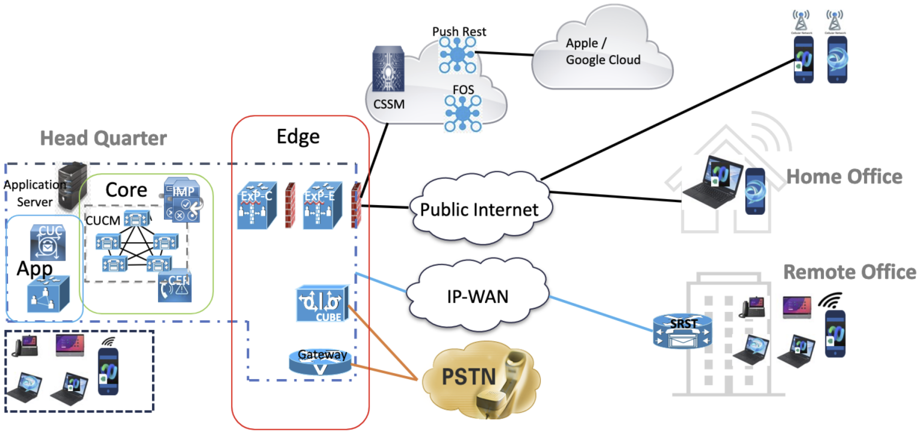
Upgrade use case 3 – Multi-site upgrade

In a multisite environment, upgrading one site would cause other sites to be in older TLS versions. However, because of backward compatibility, this does not break any TLS connection.



Upgrade use case 4 – Hybrid deployment

In this deployment after upgrading the enterprise components, upgraded components would be able to communicate with external cloud components according to their offered protocol version.



Summary

With current Cisco Collaboration products and releases, TLS 1.3 is supported by default. Existing TLS configurations are retained. An interface is provided to configure the minimum TLS version.

Related Documentation

- CUCM Security Guide
- IM and Presence Administrator Guide
- CER Administrator Guide
- CUC Administration Guide
- PCD Administration Guide
- TLS 1.3 Compatibility Matrix
- Expressway Administrator Guide
- Cisco Expressway SHA-1 Certificate Deprecation Rollout and SHA-2 Certificate Transition
- Cisco Unified Border Element Configuration Guide

Documentation Changes

Table 2. Documentation Changes

Date	Change
November 2024	Published the whitepaper for TLS 1.3.

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.

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 and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.