



# TLS 1.2 for On-Premises Cisco Collaboration Deployments

First Published: October 5, 2017

Last Updated: April 20, 2018

## Introduction

Transport Layer Security (TLS) and its predecessor, Secure Socket Layer (SSL), are cryptographic protocols that provide communications security over a network. However, SSL, TLS 1.0, and sometimes TLS 1.1 may not provide the level of security required by an organization. Many organizations may require TLS 1.2.

This white paper provides information on TLS 1.2 support and on the ability to disable lower versions of TLS for on-premises Cisco Collaboration deployments. It also discusses the implications when disabling TLS 1.0 and 1.1. However, it does not discuss cipher suites support with TLS 1.2.

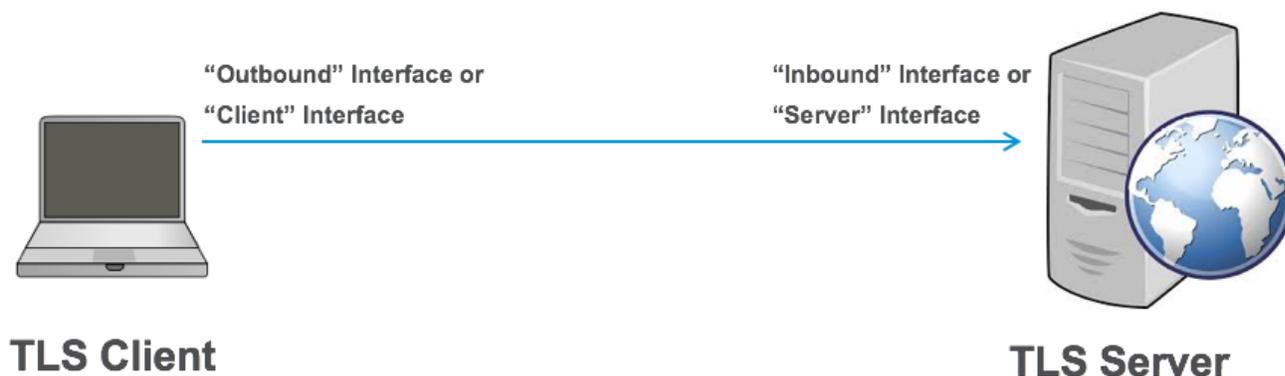
This document also complements the:

- *TLS 1.2 Compatibility Matrix for Cisco Collaboration Products:*  
[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/uc\\_system/unified/communications/system/Compatibility/TLS/TLS1-2-Compatibility-Matrix.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compatibility/TLS/TLS1-2-Compatibility-Matrix.html)
- *TLS 1.2 Configuration Overview Guide:*  
[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/uc\\_system/TLS/TLS-1-2-Configuration-Overview-Guide.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/TLS/TLS-1-2-Configuration-Overview-Guide.html)

## Terminology – TLS Client and Server Interfaces

In a TLS connection, the device that initiates the TLS request is known as the TLS client and its interface is known as the outbound interface or client interface. On the other side of the connection, the device that receives the TLS request is known as the TLS server and its interface is known as the inbound interface or server interface. Figure 1 provides an illustration of this terminology.

Figure 1: TLS Client and TLS Server



In a collaboration solution, endpoints or phones are considered clients. Applications such as Cisco Unified Communications Manager (Unified CM) are considered servers based on their main function within the Cisco Collaboration deployment. However, from a TLS connection standpoint, the definition of a client and server is different. A device can have both client interfaces and server interfaces. For example, an endpoint has an interface for call signaling (SIP or SCCP) that could be encrypted and acts as a TLS client to Unified CM. An endpoint also has a web interface for the endpoint internal web server that could be encrypted (HTTPS), causing the endpoint to act as a TLS server. Figure 2 provides an example of the TLS server interface and TLS client interfaces on an endpoint. Similarly, Unified CM has TLS client interfaces such as the secure LDAP interface and has TLS server interfaces such as the web interface. Unified CM's SIP interface also acts as both TLS client and TLS server interfaces. Figure 3 shows some of the Unified CM interfaces.

Figure 2: Example of TLS Server and TLS Client Interfaces with Endpoint

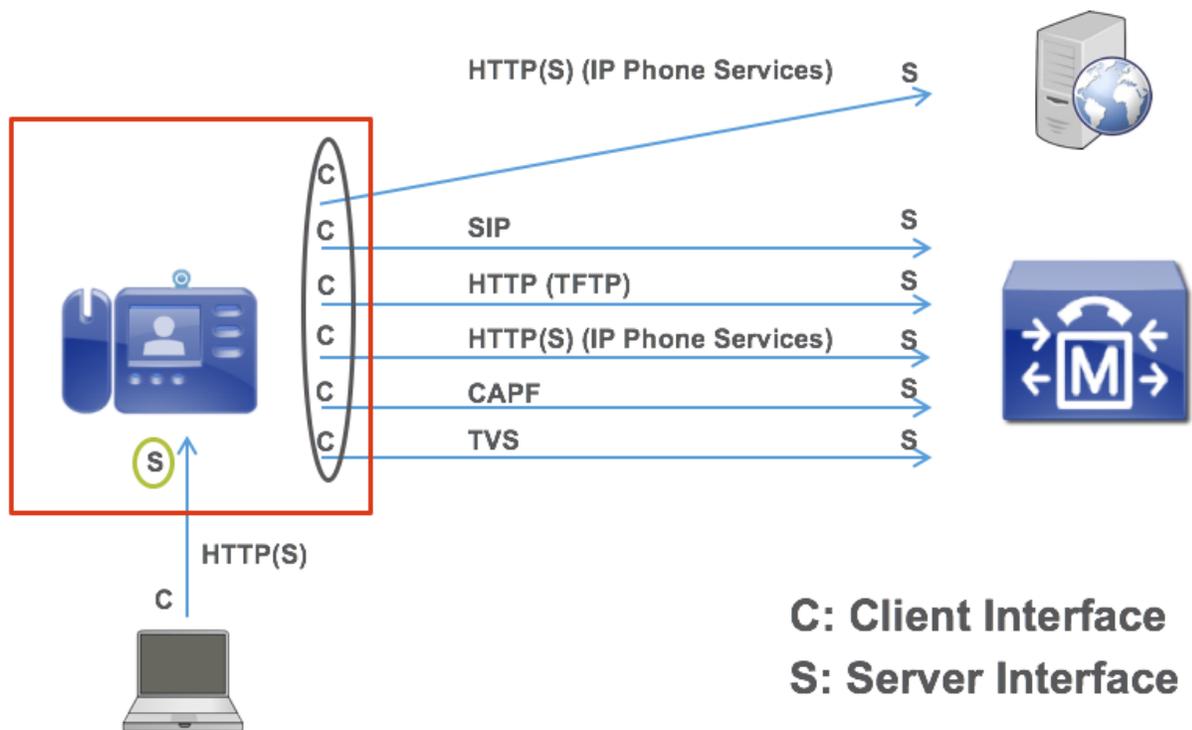
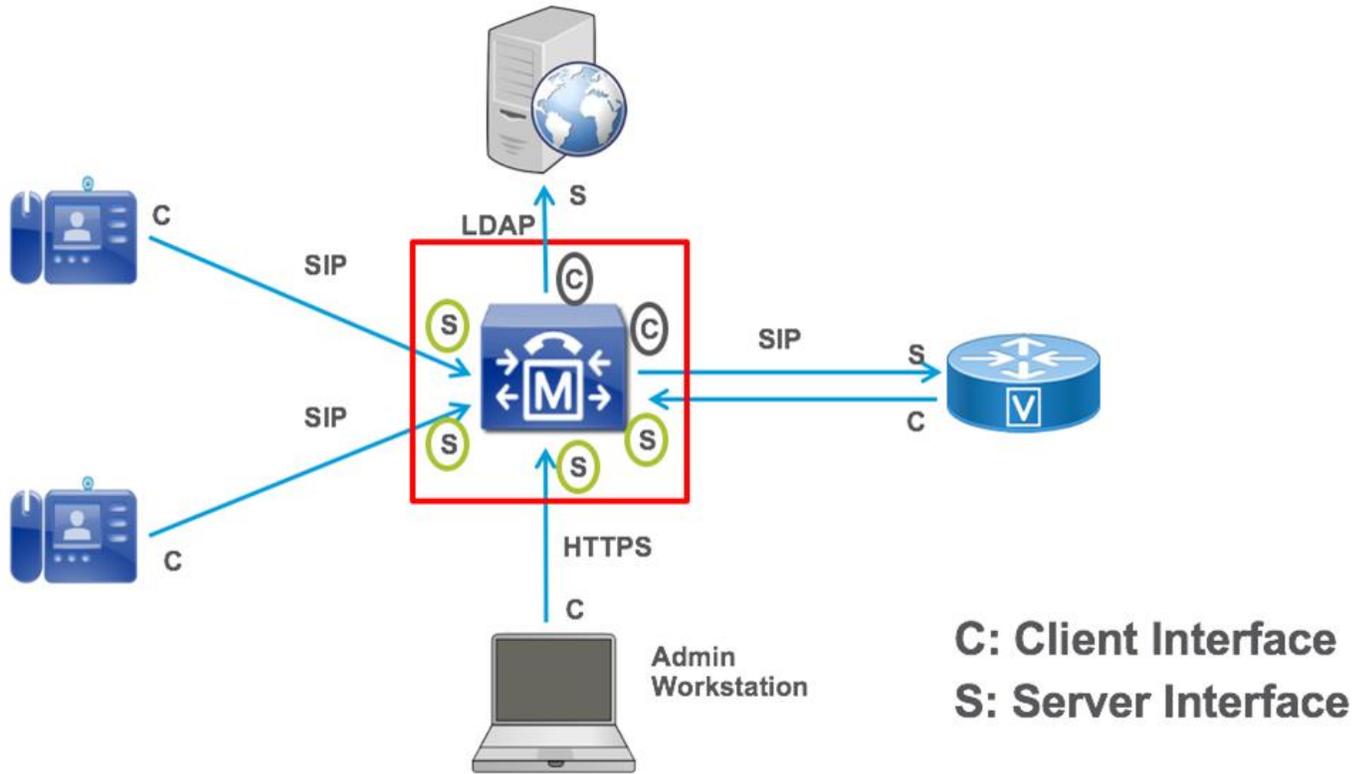


Figure 3: Example of TLS Server and TLS Client Interfaces with Unified CM



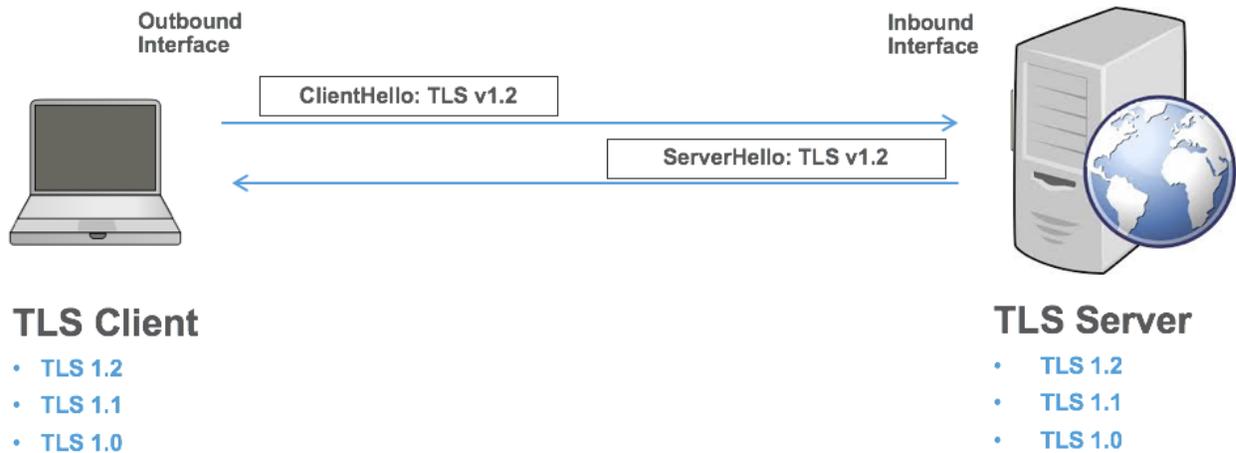
## TLS Version Negotiation Defaults to TLS 1.2

If a TLS client and TLS server both support TLS 1.2, then by default TLS version 1.2 is negotiated, even if they also support TLS 1.0 and TLS 1.1.

A TLS handshake initiates a TLS connection. At the beginning of the TLS handshake, the TLS client sends a ClientHello that includes the TLS version. If the TLS client supports TLS 1.0, 1.1, and 1.2, by default it first sends the ClientHello with a TLS version set to 1.2. If the TLS server also supports TLS 1.2, then it replies with a ServerHello with the TLS version set to 1.2. The TLS version negotiation is complete at this point, even if the client or server also supports TLS 1.0/1.1.

However, if there was an issue with the first TLS 1.2 handshake, the TLS client would indicate TLS 1.0 or 1.1 in subsequent ClientHello messages. A normal TLS negotiation is illustrated in Figure 3.

Figure 3: TLS 1.2 Negotiated When TLS Client and Server Support Both TLS 1.2 and Prior TLS Versions



Most of the components in Cisco Collaboration Systems Release 12.0 support TLS 1.2. For a list of Cisco Collaboration products that support TLS 1.2, refer to the *TLS 1.2 Compatibility Matrix for Cisco Collaboration Products* at [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/uc\\_system/unified/communications/system/Compatibility/TLS/TLS1-2-Compatibility-Matrix.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compatibility/TLS/TLS1-2-Compatibility-Matrix.html).

Note: SSL has been removed from most of the Cisco Collaboration products and from all products listed in the *TLS 1.2 Compatibility Matrix for Cisco Collaboration Products*.

## Disabling TLS 1.0/1.1

TLS version 1.2 should always be negotiated between devices that support TLS 1.2, even if they also support TLS 1.0 and TLS 1.1. However, there could be Man-in-the-Middle (MitM) attacks that attempt to alter the TLS handshake and negotiate a lower version of TLS or even SSL. To prevent this from happening, disable TLS 1.0 (and TLS 1.1), thus forcing all TLS communications to be restricted to just TLS 1.2 (and TLS 1.1). The *TLS 1.2 Compatibility Matrix for Cisco Collaboration Products* indicates the minimum versions of Cisco Collaboration products that can disable TLS version 1.0 and 1.1.

Disabling TLS 1.0/1.1 on TLS connections could be done in theory either on the client interfaces or the server interfaces, it does not need to be done on both interface types. With Cisco Collaboration products, it is done on the server interface. When an administrator disables TLS 1.0/1.1, the TLS server interfaces do not allow TLS 1.0/1.1 anymore. In some cases, in addition to TLS server interfaces, disabling TLS 1.0/1.1 could also apply to TLS client interfaces, for example with the LDAP client interface or the SIP client interface in Unified CM.

Figure 4 shows the typical implementation where the configuration to disable TLS 1.0 and 1.1 applies to the server interface and where the version for the TLS connection is therefore restricted to 1.2. This is what the *TLS 1.2 Compatibility Matrix for Cisco Collaboration Products* tracks. It considers that a product can disable TLS version 1.0/1.1 if all the TLS server interfaces of that product can disable TLS version 1.0 and 1.1. The client interfaces may still allow TLS 1.0 and 1.1. **The matrix doesn't track the ability to disable TLS 1.0/1.1 on the client interfaces.**

Figure 4: Configuration to Disable TLS 1.0/1.1 Applies to Server Interface



Disabling TLS 1.0/1.1 might result in compatibility issues if some components do not support TLS 1.2. Before you disable TLS 1.0/1.1, verify that all the products in your deployments support TLS 1.2 and consider the limitations described in the following section.

## Limitations When Disabling TLS 1.0/1.1

When you disable a version (or versions) of TLS on a product, ensure that there is still a common version of TLS that can be negotiated with the other products that are connecting to it. For example, if you disable TLS 1.0 and TLS 1.1 on Unified CM, ensure that all the products connecting to Unified CM through a TLS connection support TLS 1.2. If not, there may be interoperability issues.

For a list of products supporting TLS 1.2, refer to the *TLS 1.2 Compatibility Matrix for Cisco Collaboration Products*.

The following sections describe some of the key limitations of disabling TLS 1.0/1.1.

### Limitations When Disabling TLS 1.0/1.1 on Unified CM

When you disable TLS 1.0/1.1 on a Unified CM node, it sets the minimum version of TLS and applies this version to all server interfaces in the Unified CM node such as the HTTPS web server interface, the SIP server interface, and the Certificate Trust List (CTL) provider server interface. It also applies the version to some client interfaces such as the SIP client interface and the LDAP client interface. **The following limitations apply when you configure Unified CM's minimum TLS version to TLS 1.1 or 1.2.**

- Certificate Trust List Client
  - The main limitation with Unified CM is with the Certificate Trust List (CTL) Client. The CTL Client that is used with the USB eTokens to enable Unified CM mixed-mode does not support TLS 1.2, even with Unified CM 12.0.
    - Workaround: Enable TLS 1.0 temporarily on Unified CM when enabling mixed-mode or when updating the CTL file.
    - Workaround: Migrate to the Tokenless CTL (CLI-based).

### Limitations When Disabling TLS 1.0/1.1

- Cisco IP Phone Address Book Synchronizer  
Cisco IP Phone Address Book Synchronizer enables users to synchronize their Microsoft Windows Address Book with the Cisco Personal Address Book. This client only supports TLS 1.0.
  - Workaround: There is no workaround.
- Interconnectivity with Unified CM clusters running an older release  
Releases before Unified CM 10.5(2) do not support TLS 1.2. Therefore, interconnecting with those older clusters may be limited if restricting the TLS version on your local Unified CM cluster. For example, secure SIP trunks, secure Location Bandwidth Management (LBM), Intercluster Lookup Service (ILS), and remote cluster discovery service used with Extension Mobility Cross Cluster (EMCC) may not be functional.
  - Workaround: Unified CM 10.5(2) introduced TLS 1.2 support for many interfaces including SIP, but for TLS 1.2 support on all Unified CM interfaces, deploy Unified CM 11.5(1)SU3 or later.
- Interconnectivity with older products through SIP trunks  
Disabling TLS 1.0/1.1 applies to SIP server interfaces and SIP client interfaces.
  - Workaround: Ensure that the products that your Unified CM nodes connect to through a SIP trunk also support TLS 1.2. For example, if Cisco Unified Border Element (CUBE) is deployed, ensure it is running a release that supports TLS 1.2.
- Interoperability with older phones
  - This limitation is discussed in the following section.

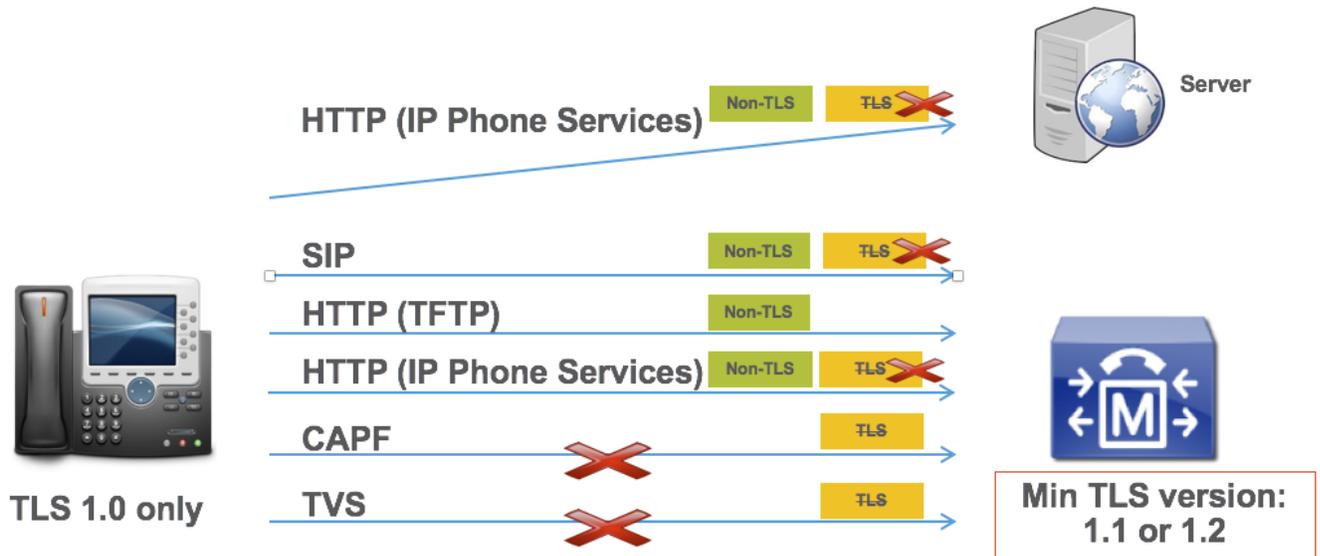
### Limitations of Older Phones

Disabling TLS 1.0/1.1 in Unified CM can also have significant implications on older phones, such as the Cisco Unified IP Phone 8961, Cisco Unified IP Phone 9900, 7900, 6900, 3900 Series, and Cisco IP Communicator.

Those older phones do not support TLS 1.1 and TLS 1.2. Therefore, if Unified CM is configured with the minimum TLS version set to 1.1 or 1.2, the TLS connections won't be able to establish. With SIP and HTTP for IP Phone Services, a workaround is to use non-encrypted connections instead, but doing this may be a security issue. Other Unified CM interfaces like Trust Verification Service (TVS) and Certificate Authority Proxy Function (CAPF) only allow TLS, and non-encrypted connections are not available, therefore the corresponding services will not be available at all with the older phones.

See figure 5 for an example of those connections when setting the minimum TLS version on Unified CM to 1.1 or 1.2. Some connections may still be possible if they can be non-encrypted. Some other connections that only support TLS will break.

Figure 5: Connections with Older Phones When TLS 1.1 or 1.2 Is Unified CM Minimum Version



The following sections provide more details about these limitations and the possible workarounds.

### SIP Interface

When a phone is configured in authenticated or encrypted mode, it registers to Unified CM through a TLS connection (encrypted SIP or encrypted SCCP). If the SIP interface of the phone does not support TLS 1.2 and Unified CM is configured with the minimum TLS version set to 1.2, then this connection cannot be established. Moreover, when configured in that mode, for security reasons, the phone does not attempt to register through a non-TLS connection. **Therefore, the endpoint won't be able to register and won't be able to place or receive calls.**

Workaround: Configure phones in nonsecure mode.

### HTTPS Web Server Interface for IP Phone Services

The phone client interface that connects to Unified CM web services for IP Phone services does not support TLS 1.2 on older phones. Therefore, an IP Phone service will not work if the phone attempts to use HTTPS to connect to the IP Phone Service. If a phone does not support HTTPS for that IP Phone Services interface (for example 7940/7960), then it **disregards the secure URLs that are configured, it doesn't use HTTPS, it just uses the nonsecure URLs.** IP Phone Services will work in this particular case. But if a phone supports HTTPS, for security reasons, it will only attempt to use HTTPS (it will not try to fallback to HTTP) if a secure URL is configured or if the default configuration is used for built-in Cisco IP Phone Services (such as Application:Cisco/CorporateDirectory). With TLS 1.2 not being supported on older phones, IP Phone services will not be available at all. This limitation applies to most of the older phones discussed here (for example 7941/7961 or newer 7900 models, 6900, 9900, 8961 models).

Workaround: Use nonsecure URLs (HTTP instead of HTTPS) for all the phones in your deployment. However, HTTP is not recommended as it is not secure and may be a concern especially when sensitive data is transmitted (for example, user id and PIN with Extension Mobility). For default Cisco IP Phone services (such as Application:Cisco/CorporateDirectory), using specific URLs has drawbacks. With default configuration of those default Cisco IP Phone services, the phone uses the Unified CM nodes configured in the CM group and follows the same preference order as it does for call processing. If the primary Unified CM call processing subscriber fails, the phone will fail over to the secondary call processing subscriber. However, by configuring a URL, a single server is specified, and there is no resiliency for the IP Phone service anymore. Another drawback is that the load may not be well distributed

when configuring a URL. If the same server is configured for all IP Phone services, the performance of that server can be affected.

To alleviate some of those issues, you could configure only the older phones with a nonsecure URL (HTTP), and configure newer phones supporting TLS 1.2 to use the normal configuration (secure URLs and default configuration with default Cisco IP Phone services). However, there are provisioning challenges when configuring HTTP for older phones and HTTPS for newer phones. You would need to add separate IP Phone services, some based on HTTP, some based on HTTPS, and then associate the phones to the appropriate IP Phone Services. You may also need to remove some secure URLs from the Unified CM enterprise parameters page and then add them back for the new phones only.

### Trust Verification Service Interface

**Trust Verification Service (TVS) is the main component of Unified CM's Security by Default architecture.** TVS can validate certificates on behalf of the phones or provide certificates to the phones. For example, TVS enables the endpoints to connect to IP Phone Services securely (through HTTPS). With Unified CM releases before 12.0, TVS was also used by endpoints to trust Unified CM when renewing the CallManager certificate or migrating between Unified CM clusters. From Unified CM 12.0 onward, TVS is typically not used in those scenarios since the tokenless CTL and ITL files are signed by the ITLrecovery key.

Older endpoints do not support TLS 1.2 on this interface. Since TLS is the only option with TVS (non-encrypted connection not allowed), older endpoints are not able to connect to the Unified CM TVS service if Unified CM is configured with the minimum TLS version set to 1.1 or 1.2. The implications are:

- Older endpoints cannot use secure URLs (HTTPS) for IP Phone services, even with external IP Phone Services (not hosted by Unified CM).
  - Workaround: Use nonsecure URLs (HTTP), but this is not recommended as it may be a security issue. There may also be provisioning challenges.
- With Unified CM 11.5(1)SU3 and subsequent SUs, renewing the CallManager certificate results in older phones not trusting Unified CM because the phones are not able to verify the CTL and ITL files signed by the new CallManager key. This is not an issue with Unified CM releases 12.0 and later since the tokenless CTL and ITL files are signed by the ITLrecovery key.
  - Workaround: Temporarily set the Prepare Cluster for Rollback to pre 8.0 enterprise parameter to True.
  - Workaround: Temporarily allow TLS 1.0 in Unified CM.
  - Workaround: Upgrade to Unified CM 12.0 or later.
- With Unified CM 11.5(1)SU3 and subsequent SUs, if mixed-mode is not enabled or if it is enabled with the CLI (tokenless CTL), Extension Mobility Cross Cluster (EMCC) does not work with older phones. Moreover, phone migrations from one Unified CM cluster to another Unified CM cluster require the deletion of the CTL/ITL file on each phone.
  - Workaround: Enable Unified CM mixed-mode with USB eTokens and use the same eTokens across all Unified CM clusters.
  - Workaround: Upgrade to Unified CM 12.0 or later.
- With Unified CM 11.5(1)SU3 and subsequent SUs, with Proxy TFTP server deployed, the older phones are not able to validate static files signed by the Proxy TFTP server, such as ringlist files, background images, or locales.
  - Workaround: Upgrade Unified CM home clusters to Unified CM 12.0 or later.

### Certificate Authority Proxy Function Interface

Unified CM's Certificate Authority Proxy Function (CAPF) service allows certificate-related operations such as issuing or updating Locally Significant Certificate (LSC) on endpoints or getting the endpoint certificates and public keys that are needed to support encrypted TFTP configuration files.

Older endpoints do not support TLS 1.2 on this interface. Since TLS is the only option with CAPF (non-encrypted connection not allowed), then older endpoints are not able to connect to the Unified CM CAPF service if Unified CM is configured with the minimum TLS version set to 1.2. The implications are:

- LSC certificates cannot be installed on older phones. Therefore, services based on LSC certificates are not available. For example, 802.1x authentication and Phone VPN cannot be based on LSC certificates.
  - Workaround: Services based on LSC certificates would have to be based on other authentication mechanisms such as MIC certificates or end-user credentials.
- Encrypted TFTP configuration files is not possible, even with MIC certificates.
  - Workaround: Use non-encrypted TFTP configuration files, but this may be a security concern especially when credentials are configured in the Unified CM Administration phone page.

### Summary of Older Phone Limitations and Workarounds

When Unified CM's minimum TLS version is set to 1.1 or 1.2, older phones such as the Cisco Unified IP Phone 8961, Cisco Unified IP Phone 9900, 7900, 6900, 3900 Series, and Cisco IP Communicator are not fully functional and have important limitations. The following table summarizes the main limitations and provides some workarounds. The recommendation is however to upgrade those older phones to newer phones such as the Cisco IP Phone 7800 or 8800.

Table 1: Summary of Older Phone Limitations and Workarounds When Unified CM Minimum TLS Version Is 1.1 or 1.2

Feature	Limitation	Workaround
SIP Interface		
Encrypted mode or Authenticated mode	Older phones in Encrypted mode or Authenticated mode are not functional; they cannot register to Unified CM.	Configure those phones in nonsecure mode.
HTTPS Web Server Interface for IP Phone Services		
IP Phone Services using secure URLs (HTTPS)	Older phones cannot connect to IP Phone Services using secure URLs (HTTPS).	Use nonsecure URLs (HTTP), but this is not recommended as it may be a security issue. There may also be provisioning challenges.
Trust Verification Service Interface		

CallManager certificate renewal	<p>With Unified CM release 11.5(1)SU3 and subsequent SUs, older phones lose trust when CallManager certificates are renewed.</p> <p>This is not an issue with Unified CM 12.0 and later.</p>	<p>Temporarily set the Prepare Cluster for Rollback to pre 8.0 enterprise parameter to True.</p> <p>OR</p> <p>Temporarily allow TLS 1.0 in Unified CM.</p> <p>OR</p> <p>Upgrade to Unified CM 12.0 release or later.</p>
Extension Mobility Cross Cluster (EMCC)	<p>EMCC is not supported with older phones and Unified CM release 11.5(1)SU3 and subsequent SUs, if mixed-mode is not enabled or if it is enabled with the CLI (tokenless CTL).</p>	<p>Enable Unified CM mixed-mode with USB eTokens and use the same eTokens across all Unified CM clusters.</p> <p>OR</p> <p>Upgrade to Unified CM 12.0 release or later.</p>
Proxy TFTP Server	<p>With Unified CM 11.5(1)SU3 and subsequent SUs, with Proxy TFTP server deployed, the older phones are not able to validate static files signed by the Proxy TFTP server, such as ringlist files, background images, or locales.</p>	<p>Upgrade Unified CM home clusters to Unified CM 12.0 release or later.</p>
Certificate Authority Proxy Function Interface		
Locally Significant Certificates (LSC)	<p>LSC cannot be installed or updated on older phones. As a result, 802.1x and phone VPN authentications based on LSC are not available.</p>	<p>Use other authentication mechanisms such as MIC certificates or end-user credentials.</p>
Encrypted Trivial File Transfer Protocol (TFTP) configuration files	<p>TFTP configuration files cannot be encrypted with older phones.</p>	<p>Use non-encrypted TFTP configuration files and avoid configuration credentials on the Unified CM Administration phone page.</p>

## Disabling TLS 1.0/1.1 Configuration Example

The configuration to disable TLS 1.0 and TLS 1.1 depends on the product. This example shows how to disable TLS versions for Unified CM with IM and Presence Service and products based on the same platform, such as Cisco Unity Connection, Cisco Emergency Responder (Emergency Responder), and Cisco Prime Collaboration Deployment.

**Note:** For configuration information for other products, refer to the related product documentation.

Summary

By default, the minimum version of TLS is set to 1.0 for Unified CM with IM and Presence Service, Cisco Unity Connection, Emergency Responder, or Cisco Prime Collaboration Deployment. Setting the minimum TLS version to 1.1 disables TLS 1.0. Setting the minimum TLS version to 1.2 disables TLS 1.0 and TLS 1.1.

To disable TLS 1.0 and TLS 1.1, log in to the Command Line Interface and run the `set tls min-version 1.2` CLI command.

Figure 6 shows an example of how to configure the minimum version of TLS on a Unified CM with IM and Presence Service node. After the configuration, the node reboots. This configuration applies only to the local node, so if you want to disable TLS 1.0/1.1 for all the nodes in a cluster, apply this configuration on all cluster nodes.

Figure 6: Configuring TLS 1.2 as Minimum Version on Unified CM with IM and Presence Service

```

[admin:set tls min-version 1.2

This command will result in setting minimum TLS version to 1.2 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 this feature
*****

Warning: This will set the minimum TLS to 1.2 and the server will reboot.
*****

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

Successfully set minimum TLS version to 1.2

The system will reboot in a few minutes.
    
```

To verify the minimum TLS version currently configured on Unified CM and IM and Presence Service, Cisco Unity Connection, Emergency Responder, or Cisco Prime Collaboration Deployment, run the `show tls min-version` CLI command.

Figure 7: Verifying the Configured Minimum TLS Version of Unified CM with IM and Presence Service

```

admin:show tls min-version
Configured TLS minimum version: 1.2
    
```

## Summary

With current Cisco Collaboration products and current releases, SSL is disabled and TLS 1.2 should be negotiated by default. To prevent attacks on TLS version downgrades, disable TLS 1.0 and TLS 1.1. Before disabling TLS 1.0 and TLS 1.1, ensure the other products that are involved in the relevant TLS connections support TLS 1.2. If you have older phones, they may not be fully functional and may have important limitations. The recommendation is to upgrade to newer phones such as the Cisco IP Phone 7800 or 8800 Series.

## Related Documentation

- For a list of Cisco Collaboration products that support TLS 1.2 and can disable TLS 1.0 and TLS 1.1, see the *TLS 1.2 Compatibility Matrix for Cisco Collaboration Products* at [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/uc\\_system/unified/communications/system/Compatibility/TLS/TLS1-2-Compatibility-Matrix.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compatibility/TLS/TLS1-2-Compatibility-Matrix.html). This matrix is also available from the Compatibility Information page available at <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-device-support-tables-list.html>.
- For an overview on how to enable TLS 1.2 and disable TLS 1.0 and 1.1 for Cisco Collaboration products, see the *TLS 1.2 Configuration Overview Guide*, at

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/uc\\_system/TLS/TLS-1-2-Configuration-Overview-Guide.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/TLS/TLS-1-2-Configuration-Overview-Guide.html).

- For information on disabling TLS 1.0/ 1.1, or on configuring a minimum version of TLS on the server interface, refer to the product support documentation at <https://www.cisco.com/>.
- For security information about Unified CM, see the *Security Guide for Cisco Unified Communications Manager* available at <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>.
- For security information about Cisco Unity Connection, see the *Security Guide for Cisco Unity Connection* available at <https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html>.
- For the compatible product software release versions for Cisco Collaboration Systems Releases, see the *Cisco Collaboration Systems Release Compatibility Matrix* at [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/uc\\_system/unified/communications/system/Compatibility/CSR-Compatibility-Matrix.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compatibility/CSR-Compatibility-Matrix.html).

## Documentation Changes

Table 2. Documentation Changes

Date	Change
April 20, 2018	Added link to <a href="#">TLS 1.2 Configuration Overview Guide</a> .

## 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](#).

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the [What's New in Cisco Product Documentation RSS feed](#). The RSS feeds are a free service.

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. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.