Default Security

Default Security Overview

The Default Security features provides a basic level of security for supported Cisco Unified IP Phone without any extra configuration requirement.

This feature provides the following default security for supported IP Phones:

- Default Authentication of TFTP
- Optional Encryption
- Certificate Verifications

Default Security uses the following components to provide basic security in non secure environments:

- Identity Trust List (ITL)—this file is created only after TFTP service is activated at cluster installation and is used by Cisco Unified IP Phone to establish trust.
- Trust Verification Service—This service runs on all Unified Communications Manager nodes and authenticates certificates for Cisco Unified IP Phone. The TVS certificate, along with a few other key certificates, is bundled in the ITL file.

Initial Trust List

The Initial Trust List (ITL) file is used for the initial security, so that the endpoints can trust Unified Communications Manager. ITL does not need any security features to be enabled explicitly. The ITL file is automatically created when the TFTP service is activated and the cluster is installed. The Unified Communications Manager's TFTP server’s private key is used to sign the ITL file.

When the Unified Communications Manager cluster or server is in non-secure mode, the ITL file is downloaded on every supported Cisco Unified IP Phone. You can view the contents of an ITL file using the CLI command **admin:show itl**.

Cisco Unified IP Phone need the ITL file to perform the following tasks:

- Communicate securely to CAPF, a prerequisite to support the configuration file encryption.
- Authenticate the configuration file signature
- Authenticate application servers, such as EM services, directory, and MIDlet during HTTPS establishment using TVS.

If the Cisco IP Phone does not have an existing CTL file, it trusts the first ITL file automatically. The TVS must be able to return the certificate corresponding to the signer.

If the Cisco IP Phone has an existing CTL file, it uses the CTL file to authenticate the ITL file signature.

Note The SHA-1or MD5 algorithm value changes only when there is a change in the Initial Trust List (ITL) file value. You can use the checksum value of the ITL files to identify the difference between the ITL file of Cisco IP Phone and Unified Communications Manager cluster. The checksum value of the ITL file changes only when you modify the ITL file.

The Initial Trust List (ITL) file has the same format as the CTL file. However, it is a smaller and leaner version.

The following attributes apply to the ITL file:

- The system builds the ITL file automatically when the TFTP service is activated and you install the cluster. The ITL file is updated automatically if the content is modified.
- The ITL file does not require eTokens. It uses a soft eToken (the private key associated with TFTP server's CallManager certificate).
- The Cisco Unified IP Phone download the ITL file during a reset, restart, or after downloading the CTL file.

The ITL file contains the following certificates:

- ITLRecovery Certificate—This certificate signs the ITL File.
- The CallManager certificate of the TFTP server—This certificate allows you to authenticate the ITL file signature and the phone configuration file signature.
- All the TVS certificates available on the cluster—These certificates allow the phone to communicate to TVS securely and to request certificates authentication.
- The CAPF certificate—These certificates support configuration file encryption. The CAPF certificate isn't required in the ITL File (TVS can authenticate it), however, it simplifies the connection to CAPF.

The ITL file contains a record for each certificate. Each record contains:

- A certificate
- Pre-extracted certificate fields for easy lookup by the Cisco IP Phone
- Certificate role (TFTP, CUCM, TFTP+CCM, CAPF, TVS, SAST)

The TFTP server's CallManager certificate is present in two ITL records with two different roles:

- TFTP or the TFTP and CCM role—To authenticate configuration file signature.
- SAST role—To authenticate the ITL file signature.

Certificate Management Changes for ITLRecovery Certificate

- The validity of ITLRecovery has been extended from 5 years to 20 years to ensure that the ITLRecovery certificate remains same for a longer period.

Note The validity of ITLRecovery certificates continues to be 5 years if you upgrade Unified Communications Manager. While upgrading Unified Communications Manager, the certificates get copied to the later release. However, when you regenerate an ITLRecovery certificate or when you do a fresh install of Unified Communications Manager, the validity of ITLRecovery gets extended to 20 years.

- Before you regenerate an ITLRecovery certificate, a warning message appears on both the CLI and the GUI. This warning message displays that if you use a tokenless CTL and if you regenerate the CallManager certificate, ensure that the CTL file has the updated CallManager certificate and that certificate is updated to endpoints.

Interactions and Restrictions

If a Unified Communications Manager cluster has more than 39 certificates, then the ITL file size on Cisco IP Phone exceeds 64 kilobytes. Increase in the ITL file size affects the ITL to load properly on the phone causing the phone registration to fail with Unified Communications Manager.

Trust Verification Service

There are large number of phones in a network and Cisco Unified IP Phone have limited memory. Hence, Unified Communications Manager acts as a remote trust store through TVS and so that a certificate trust store doesn't have to be placed on each phone. The Cisco Unified IP Phones contact TVS server for verification, because it cannot verify a signature or certificate through CTL or ITL files. Thus, having a central trust store is easier to manage than having the trust store on all the Cisco Unified IP Phones.

TVS enables Cisco Unified IP Phone to authenticate application servers, such as EM services, directory, and MIDlet, during HTTPS establishment.

TVS provides the following features:

- Scalability—Cisco Unified IP Phone resources are not impacted by the number of certificates to trust.
- Flexibility—Addition or removal of trust certificates are automatically reflected in the system.
- Security by Default—Non-media and signaling security features are part of the default installation and don't require user intervention.

Note When you enable secure signaling and media, create a CTL file and then set the cluster to mixed mode. To create a CTL file and set the cluster to mixed mode, use the CLI command **utils ctl set-cluster mixed-mode**.

The following are the basic concepts that describe TVS:

- TVS runs on the Unified Communications Manager server and authenticates certificates on behalf of the Cisco IP Phone.

- Cisco Unified IP Phone only needs to trust TVS, instead of downloading all the trusted certificates.
- The ITL file is generated automatically without user intervention. The ITL file is downloaded by Cisco Unified IP Phone and trust flows from there.

Authentication, Integrity, and Authorization

Integrity and authentication protect against the following threats:

- TFTP file manipulation (integrity)
- Modification of call-processing signaling between the phone and Unified Communications Manager (authentication)
- Man-in-the-middle attacks (authentication), as defined in *Acronyms* section.
- Phone and server identity theft (authentication)
- Replay attack (digest authentication)

Authorization specifies what an authenticated user, service, or application can do. You can implement multiple authentication and authorization methods in a single session.

Image Authentication

This process prevents tampering with the binary image, the firmware load, prior to loading it on the phone. Tampering with the image causes the phone to fail the authentication process and reject the image. Image authentication occurs through signed binary files that automatically install when you install Unified Communications Manager. Likewise, firmware updates that you download from the web also provide signed binary images.

Device Authentication

This process validates the identity of the communicating device and ensures that the entity is who it claims to be.

Device authentication occurs between the Unified Communications Manager server and supported Cisco Unified IP Phones, SIP trunks, or JTAPI/TAPI/CTI applications (when supported). An authenticated connection occurs between these entities only when each entity accepts the certificate of the other entity. Mutual authentication describes this process of mutual certificate exchange.

Device authentication relies on the creation of the CiscoCTL file (for authenticating Unified Communications Manager server node and applications), and the Certificate Authority Proxy Function (for authenticating phones and JTAPI/TAPI/CTI applications).

Tip A SIP user agent that connects via a SIP trunk authenticates to Unified Communications Manager if the CallManager trust store contains the SIP user agent certificate and if the SIP user agent contains the Unified Communications Manager certificate in its trust store. For information on updating the CallManager trust store, refer to the *Administration Guide for Cisco Unified Communications Manager* that supports this Unified Communications Manager release.

File Authentication

This process validates digitally signed files that the phone downloads; for example, the configuration, ring list, locale, and CTL files. The phone validates the signature to verify that file tampering did not occur after the file creation. For a list of devices that are supported, see “Phone Model Support”.

If you configure the cluster for mixed mode, the TFTP server signs static files, such as ring list, localized, default.cnf.xml, and ring list wav files, in.sgn format. The TFTP server signs files in <device name>.cnf.xml format every time that the TFTP server verifies that a data change occurred for the file.

The TFTP server writes the signed files to disk if caching is disabled. If the TFTP server verifies that a saved file has changed, the TFTP server re-signs the file. The new file on the disk overwrites the saved file that gets deleted. Before the phone can download the new file, the administrator must restart affected devices in Unified Communications Manager.

After the phone receives the files from the TFTP server, the phone verifies the integrity of the files by validating the signature on the file. For the phone to establish an authenticated connection, ensure that the following criteria are met:

- A certificate must exist in the phone.
- The CTL file must exist on the phone, and the Unified Communications Manager entry and certificate must exist in the file.
- You configured the device for authentication or encryption.

Signaling Authentication

This process, also known as signaling integrity, uses the TLS protocol to validate that no tampering occurred to signaling packets during transmission.

Signaling authentication relies on the creation of the Certificate Trust List (CTL)file.

Digest Authentication

This process for SIP trunks and phones allows Unified Communications Manager to challenge the identity of a device that is connecting to Unified Communications Manager. When challenged, the device presents its digest credentials, similar to a username and password, to Unified Communications Manager for verification. If the credentials that are presented match those that are configured in the database for that device, digest authentication succeeds, and Unified Communications Manager processes the SIP request.

Note Be aware that the cluster security mode has no effect on digest authentication.

Note If you enable digest authentication for a device, the device requires a unique digest user ID and password to register.

You configure SIP digest credentials in the Unified Communications Manager database for a phone user or application user.

- For applications, you specify digest credentials in the Application User Configuration window.

- For phones that are running SIP, you specify the digest authentication credentials in the End User window. To associate the credentials with the phone after you configure the user, you choose a Digest User, the end user, in the Phone Configuration window. After you reset the phone, the credentials exist in the phone configuration file that the TFTPserver offers to the phone. See topics related to encrypted phone configuration file setup to ensure digest credentials do not get sent in the clear in TFTP downloads.
- For challenges received on SIP trunks, you configure a SIP realm, which specifies the realm username (device or application user) and digest credentials.

When you enable digest authentication for an external phone or trunk that is running SIP and configure digest credentials, Unified Communications Manager calculates a credentials checksum that includes a hash of the username, password, and the realm. The system uses a nonce value, which is a random number, to calculate the MD5 hash. Unified Communications Manager encrypts the values and stores the username and the checksum in the database.

To initiate a challenge, Unified Communications Manager uses a SIP 401 (Unauthorized) message, which includes the nonce and the realm in the header. You configure the nonce validity time in the SIP device security profile for the phone or trunk. The nonce validity time specifies the number of minutes that a nonce value stays valid. When the time interval expires, Unified Communications Manager rejects the external device and generates a new number.

Note Unified Communications Manager acts as a user agent server (UAS) for SIP calls that are originated by line-side phones or devices that are reached through the SIP trunk, as a user agent client (UAC) for SIP calls that it originates to the SIP trunk, or a back-to-back user agent (B2BUA) for line-to-line or trunk-to-trunk connections. In most environments, Unified Communications Manager acts primarily as B2BUA connecting SCCP and SIP endpoints. (A SIP user agent represents a device or application that originates a SIP message.)

Tip Digest authentication does not provide integrity or confidentiality. To ensure integrity and confidentiality for the device, configure the TLS protocol for the device, if the device supports TLS. If the device supports encryption, configure the device security mode as encrypted. If the device supports encrypted phone configuration files, configure encryption for the files.

Digest Authentication for Phones

When you enable digest authentication for a phone, Unified Communications Manager challenges all requests for phones that are running SIP except keepalive messages. Unified Communications Manager does not respond to challenges from line-side phones.

After receiving a response, Unified Communications Manager validates the checksum for the username that is stored in the database against the credentials in the response header.

Phones that are running SIP exist in the Unified Communications Manager realm, which is defined in Unified Communications Manager Administration at installation. You configure the SIP Realm for challenges to phones with the service parameter SIP Station Realm. Each digest user can have one set of digest credentials per realm.

Tip If you enable digest authentication for an end user but do not configure the digest credentials, the phone will fail registration. If the cluster mode is nonsecure and you enable digest authentication and configure digest credentials, the digest credentials get sent to the phone, and Unified Communications Manager still initiates challenges.

Digest Authentication for Trunks

When you enable digest authentication for a trunk, Unified Communications Manager challenges SIP trunk requests from SIP devices and applications that connect through a SIP trunk. The system uses the Cluster ID enterprise parameter in the challenge message. SIP user agents that connect through the SIP trunk respond with the unique digest credentials that you configured for the device or application in Unified Communications Manager.

When Unified Communications Manager initiates a SIP trunk request, a SIP user agent that connects through the SIP trunk can challenge the identity of Unified Communications Manager. For these incoming challenges, you configure a SIP Realm to provide the requested credentials for the user. When Unified Communications Manager receives a SIP 401(Unauthorized) or SIP 407 (Proxy Authentication Required) message, Unified Communications Manager looks up the encrypted password for the realm that connects though the trunk and for the username that the challenge message specifies. Unified Communications Manager decrypts the password, calculates the digest, and presents it in the response message.

Tip The realm represents the domain that connects through the SIP trunk, such as xyz.com, which helps to identify the source of the request.

To configure the SIP Realm, see topics related to digest authentication for SIP trunks. You must configure a SIP Realm and username and password in Unified Communications Manager for each SIP trunk user agent that can challenge Unified Communications Manager. Each user agent can have one set of digest credentials per realm.

Authorization

Unified Communications Manager uses the authorization process to restrict certain categories of messages from phones that are running SIP, from SIP trunks, and from SIP application requests on SIP trunks.

- For SIP INVITE messages and in-dialog messages, and for phones that are running SIP, Unified Communications Manager provides authorization through calling search spaces and partitions.
- For SIP SUBSCRIBE requests from phones, Unified Communications Manager provides authorization for user access to presence groups.
- For SIP trunks, Unified Communications Manager provides authorization of presence subscriptions and certain non-INVITE SIP messages; for example, out-of-dial REFER, unsolicited notification, and any SIP request with the replaces header. You specify authorization in the SIP Trunk Security Profile Configuration window when you check the allowed SIP requests in the window.

To enable authorization for SIP trunk applications, check the Enable Application Level Authorization and the Digest Authentication check box in the SIP Trunk Security Profile window; then, check the allowed SIP request check boxes in the Application User Configuration window.

If you enable both SIP trunk authorization and application level authorization, authorization occurs for the SIP trunk first and then for the SIP application user. For the trunk, Unified Communications Manager downloads the trunk Access Control List (ACL) information and caches it. The ACL information gets applied to the incoming SIP request. If the ACL does not allow the SIP request, the call fails with a 403 Forbidden message.

If the ACL allows the SIP request, Unified Communications Manager checks whether digest authentication is enabled in the SIP Trunk Security Profile. If digest authentication is not enabled and application-level authorization is not enabled, Unified Communications Manager processes the request. If digest authentication is enabled, Unified Communications Manager verifies that the authentication header exists in the incoming request and then uses digest authentication to identify the source application. If the header does not exist, Unified Communications Manager challenges the device with a 401 message.

Before an application-level ACL gets applied, Unified Communications Manager authenticates the SIP trunk user agent through digest authentication. Therefore, you must enable digest authentication in the SIP Trunk Security Profile before application-level authorization can occur.

NMAP Scan Operation

You can run a Network Mapper (NMAP) scan program on any Windows or Linux platform to perform vulnerability scans. NMAP represents a free and open source utility for network exploration or security auditing.

Note NMAP DP scan can take up to 18 hours to complete.

Syntax

nmap -n -vv -sU -p <*port_range*> <*ccm_ip_address*>

where:

-*n*: No DNS resolution. Tells NMAP to never do reverse DNS resolution on the active IP addresses that it finds. Because DNS can be slow even with the NMAP built-in parallel stub resolver, this option can slash scanning times.

-*v*: Increases the verbosity level, which causes NMAP to print more information about the scan in progress. The system shows open ports as they are found and provides completion time estimates when NMAP estimates that a scan will take more than a few minutes. Use this option twice or more for even greater verbosity.

-*sU*: Specifies a UDP port scan.

-*p*: Specifies which ports to scan and overrides the default. Be aware that individual port numbers are acceptable, as are ranges that are separated by a hyphen (for example 1-1023).

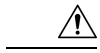
ccm_ip_address: IP address of Cisco Unified Communications Manager

Autoregistration

The system supports autoregistration in both mixed mode and nonsecure mode. The default configuration file will also be signed. Cisco IP Phones that do not support Security by Default will be served a nonsigned default configuration file.

Migrate IP Phones Between Clusters with Cisco Unified Communications Manager and ITL Files

Unified Communications Manager 8.0(1) and later introduced the new Security By Default feature and the use of Initial Trust List (ITL) files. With this new feature, you must be careful when moving phones between different Unified CM clusters and ensure that you follow the proper steps for migration.



Caution Failure to follow the proper steps may lead to a situation where thousands of phones must manually have their ITL files deleted.

Cisco IP Phones that support the new ITL file must download this special file from their Unified CM TFTP server. Once an ITL file is installed on a phone, all future configuration files and ITL file updates must be signed by one of the following items:

- The TFTP server certificate that is currently installed on the phone or
- A TFTP certificate that can be validated TVS services on one of the clusters. You can find the certificates of TVS services within the cluster listed in the ITL file.

With this new security functionality in mind, three problems can occur when moving a phone from one cluster to another cluster:

1. The ITL file of the new cluster is not signed by the current ITL file signer, so the phone cannot accept the new ITL file or configuration files.
2. The TVS servers listed in the existing ITL of the phone may not be reachable when the phones are moved to the new cluster.
3. Even if the TVS servers are reachable for certificate verification, the old cluster servers may not have the new server certificates.

If one or more of these three problems are encountered, one possible solution is to delete the ITL file manually from all phones being moved between clusters. However, this is not a desirable solution since it requires massive effort as the number of phones increases.

The most preferred option is to make use of the Cisco Unified CM Enterprise Parameter Prepare Cluster for Rollback to pre-8.0. Once this parameter is set to True, the phones download a special ITL file that contains empty TVS and TFTP certificate sections.

When a phone has an empty ITL file, the phone accepts any unsigned configuration file (for migrations to Unified CM pre-8.x clusters), and also accepts any new ITL file (for migrations to different Unified CM 8.x clusters).

The empty ITL file can be verified on the phone by checking **Settings** > **Security** > **Trust List** > **ITL**. Empty entries appear where the old TVS and TFTP servers used to be.

The phones must have access to the old Unified CM servers only as long as it takes them to download the new empty ITL files.

If you plan to keep the old cluster online, disable the Prepare Cluster for Rollback to pre-8.0 Enterprise Parameter to restore Security By Default.

Encryption

Tip Encryption capability installs automatically when you install Unified Communications Manager on a server.

This section describes the types of encryption that Unified Communications Manager supports:

Secure End Users Login Credentials

From Unified Communications Manager Release 12.5(1), all end users login credentials are hashed with SHA2 to provide enhanced security. Earlier than Unified Communications Manager Release 12.5(1), all end users login credentials were hashed with SHA1 only. Unified Communications Manager Release 12.5(1) also includes the "UCM Users with the Out-Of-Date Credential Algorithm" report. This report is available in the Cisco Unified Reporting page. This report helps the administrator to list all the end users whose passwords or PINs are hashed with SHA1.

All end users passwords or PINs that are hashed with SHA1 are migrated to SHA2 automatically upon their first successful login. The end users with SHA1 hashed (out of date) credentials can update their PINs or passwords using one of the following ways:

- Update the PIN by logging into Extension Mobility or Directory access on the phone.
- Update the password by logging into Cisco Jabber, Cisco Unified Communications Self Care Portal, or Cisco Unified CM Administration.

For more information on how to generate the report, see the *Cisco Unified CM Administration Online Help*.

Signaling Encryption

Signaling encryption ensures that all SIP and SCCP signaling messages that are sent between the device and the Unified Communications Manager server are encrypted.

Signaling encryption ensures that the information that pertains to the parties, DTMF digits that are entered by the parties, call status, media encryption keys, and so on, are protected against unintended or unauthorized access.

Cisco does not support Network Address Translation (NAT) with Unified Communications Manager if you configure the cluster for mixed mode; NAT does not work with signaling encryption.

You can enable UDP ALG in the firewall to allow media stream firewall traversal. Enabling the UDP ALG allows the media source on the trusted side of the firewall to open a bidirectional media flow through the firewall by sending the media packet through the firewall.

Tip Hardware DSP resources cannot initiate this type of connection and, therefore, must exist outside the firewall.

Signaling encryption does not support NAT traversal. Instead of using NAT, consider using LAN extension VPNs.

Media Encryption

Media encryption, which uses Secure Real-Time Protocol (SRTP), ensures that only the intended recipient can interpret the media streams between supported devices. Media encryption includes creating a media master key pair for the devices, delivering the keys to the devices, and securing the delivery of the keys while the keys are in transport. Unified Communications Manager supports SRTP primarily for IOS gateways and Unified Communications Manager H.323 trunks on gatekeeper-controlled and non-gatekeeper-controlled trunks as well as on SIP trunks.

Note Cisco Unified Communications Manager handles media encryption keys differently for different devices and protocols. All phones that are running SCCP get their media encryption keys from Unified Communications Manager, which secures the media encryption key downloads to phones with TLS encrypted signaling channels. Phones that are running SIP generate and store their own media encryption keys. Media encryption keys that are derived by Unified Communications Manager system securely get sent via encrypted signaling paths to gateways over IPSec-protected links for H.323 and MGCP or encrypted TLS links for SCCP and SIP.

Devices must state upon negotiation if it can use SRTP. CUCM does not support SRTP if the device uses cached previous negotiations SDP with different devices within the same call.

If the devices support SRTP, the system uses a SRTP connection. If at least one device does not support SRTP, the system uses an RTP connection. SRTP-to-RTP fallback may occur for transfers from a secure device to a non-secure device, transcoding, music on hold, and so on.

For most security-supported devices, authentication and signaling encryption serve as the minimum requirements for media encryption; that is, if the devices do not support signaling encryption and authentication, media encryption cannot occur. CiscoIOS gateways and trunks support media encryption without authentication. For CiscoIOS gateways and trunks, you must configure IPSec when you enable the SRTP capability (media encryption).

Warning Before you configure SRTP or signaling encryption for gateways and trunks, Ciscostrongly recommends that you configure IPSec because CiscoIOS MGCP gateways, H.323 gateways, and H.323/H.245/H.225 trunks rely on IPSec configuration to ensure that security-related information does not get sent in the clear. Unified Communications Manager does not verify that you configured IPSec correctly. If you do not configure IPSec correctly, security-related information may get exposed.

SIP trunks rely on TLS to ensure that security-related information does not get sent in the clear.

The following example demonstrates media encryption for SCCP and MGCP calls.

1. Device A and Device B, which support media encryption and authentication, register with Unified Communications Manager.
2. When Device A places a call to Device B, Unified Communications Manager requests two sets of media session master values from the key manager function.
3. Both devices receive the two sets: one set for the media stream, Device A—Device B, and the other set for the media stream, Device B—Device A.
4. Using the first set of master values, Device A derives the keys that encrypt and authenticate the media stream, Device A—Device B.

5. Using the second set of master values, Device A derives the keys that authenticate and decrypt the media stream, Device B—Device A.
6. Device B uses these sets in the inverse operational sequence.
7. After the devices receive the keys, the devices perform the required key derivation, and SRTP packet processing occurs.

Note Phones that are running SIP and H.323 trunks/gateways generate their own cryptographic parameters and send them to Unified Communications Manager.

For media encryption with conference calls, refer to topics related to secure conference resources.

AES 256 Encryption Support for TLS and SIP SRTP

Cisco Collaboration Solutions use Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP) for signaling and media encryption. Currently, Advanced Encryption Standard (AES) with a 128-bit encryption key is used as the encryption cipher. AES also uses Hash-based Message Authentication Code Secure Hash Algorithm-1 (HMAC-SHA-1) as the authentication method. These algorithms cannot effectively scale to meet the required changing security and performance needs. To meet escalating security and performance requirements, the algorithms and protocols for encryption, authentication, digital signatures, and key exchange in Next-Generation Encryption (NGE) are developed. Also, AES 256 encryption support is provided instead of AES 128 for TLS and Session Initiation Protocol (SIP) SRTP that supports NGE.

The AES 256 encryption support for TLS and SIP SRTP is enhanced to focus on AES 256 cipher support in signaling and media encryption. This feature is useful for the applications that run on Unified Communications Manager to initiate and support TLS 1.2 connections with the AES-256 based ciphers that conform to SHA-2 (Secure Hash Algorithm) standards and is Federal Information Processing Standards (FIPS) compliant.

This feature has the following requirements:

- The connection that the SIP trunk and SIP line initiates.
- The ciphers that Unified Communications Manager supports for SRTP calls over SIP line and SIP trunk.

Note With this release, TLS 1.2 is supported on some interfaces like SIP, but is not supported on all interfaces. It is recommended that you leave TLS 1.0 and 1.1 enabled in your Collaboration deployment.

AES 256 and SHA-2 Support in TLS

The Transport Layer Security (TLS) protocol provides authentication, data integrity, and confidentiality for communications between two applications. TLS 1.2 is based on Secure Sockets Layer (SSL) protocol version 3.0, although the two protocols are not compatible with each other. TLS operates in a client/server mode where one side acts as a server and the other side acts as a client. SSL is positioned as a protocol layer between the Transmission Control Protocol (TCP) layer and the application to form a secure connection between clients and servers so that they can communicate securely over a network. To operate, TLS requires TCP as the reliable transport layer protocol.

In Unified Communications Manager, AES 256 and SHA-2 (Secure Hash Algorithm-2) support in TLS 1.2 is an enhancement to handle the connection that is initiated by the SIP Trunk and the SIP line. The supported ciphers, which are AES 256 and SHA-2 compliant, are listed as follows:

- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256—The cipher string is ECDH-RSA-AES128-GCM-SHA256.
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384—The cipher string is ECDH-RSA-AES256-GCM-SHA384.

where:

- TLS is Transport Layer Security
- ECDH is Elliptic curve Diffie–Hellman, which is an algorithm
- RSA is Rivest Shamir Adleman, which is an algorithm
- AES is Advanced Encryption Standards
- GCM is Galois/Counter Mode

In addition to the newly-supported ciphers, Unified Communications Manager continues to support TLS_RSA_WITH_AES_128_CBC_SHA. The cipher string of this cipher is AES128-SHA.

Note

- The Unified Communications Manager certificates are based on RSA.
- In Unified Communications Manager, Cisco Endpoints (phones) do not support the above mentioned new ciphers for TLS 1.2.
- With AES 256 and SHA-2 (Secure Hash Algorithm-2) support in TLS 1.2 enhancement in Unified Communications Manager, the default key size for Certificate Authority Proxy Function (CAPF) is increased to 2048 bits.

AES 256 Support in SRTP SIP Call Signaling

Secure Real-time Transport Protocol (SRTP) defines the methods of providing confidentiality and data integrity for both Real-time Transport Protocol (RTP) voice and video media and their corresponding Real-time Transport Control Protocol (RTCP) streams. SRTP implements this method through the use of encryption and message authentication headers. In SRTP, encryption applies to the payload of the RTP packet only, and not to the RTP header. However, message authentication applies to both the RTP header and the RTP payload. Also, SRTP indirectly provides protection against replay attacks because message authentication applies to the RTP sequence number within the header. SRTP uses Advanced Encryption Standards (AES) with a 128-bit encryption key as the encryption cipher. It also uses Hash-based Message Authentication Code Secure Hash Algorithm-1 (HMAC-SHA-1) as the authentication method.

Unified Communications Manager supports crypto ciphers for the SRTP calls over SIP line and SIP trunk. These crypto ciphers are AEAD_AES_256_GCM and AEAD_AES_128_GCM, where AEAD is Authenticated-Encryption with Associated-Data, and GCM is Galois/Counter Mode. These ciphers are based on GCM. If these ciphers are present in the Session Description Protocol (SDP), they are treated with higher priority as compared to the AES 128 and SHA-1 based ciphers. Cisco Endpoints (phones) do not support these new ciphers that you add for Unified Communications Manager for SRTP.

In addition to the newly supported ciphers, Unified Communications Manager continues to support the following ciphers:

- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32
- F8_128_HMAC_SHA1_80

AES 256 encryption is supported in the following calls:

- SIP line to SIP line call signaling
- SIP line to SIP trunk signaling
- SIP trunk to SIP trunk signaling

Cisco Unified Communications Manager Requirements

- Support for TLS Version 1.2 on the SIP trunk and SIP line connections is available.
- Cipher support—TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (cipher string ECDHE-RSA-AES256-GCM-SHA384) and TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (cipher string ECDHE-RSA-AES128-GCM-SHA256)—is available when the TLS 1.2 connection is made. These ciphers are based on GCM and conform to SHA-2 category.
- Unified Communications Manager initiates TLS1.2 with the TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 and TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ciphers. If the peer does not support TLS1.2, then Unified Communications Manager will fall back to TLS 1.0 with the existing AES128-SHA cipher.
- The SRTP calls over SIP line and SIP trunk support the GCM-based AEAD_AES_256_GCM and AEAD_AES_128_GCM ciphers.

Interactions and Restrictions

- Unified Communications Manager requirements apply to SIP line and SIP trunk, and basic SIP to SIP calls only.
- The device types that are based on non-SIP protocols will continue to support the existing behavior with the TLS versions with the supported ciphers. Skinny Call Control Protocol (SCCP) also supports TLS 1.2 with the earlier supported ciphers.
- SIP to non-SIP calls will continue to use AES 128 and SHA-1 based ciphers.

AES 80-Bit Authentication Support

Unified Communications Manager supports Advanced Encryption Standard (AES) with a 128-bit encryption key and an 80-bit authentication tag used as the encryption cipher on Music On Hold (MOH), Interactive Voice Response (IVR), and Annunciator. By default, the phones that support the 80-bit authentication tag play the MOH, IVR, and Annunciator using the AES_CM_128_HMAC_SHA1_80 crypto ciphers.

When a phone securely connects with IP Voice Media Streaming (IPVMS), precedence is given to the AES_CM_128_HMAC_SHA1_80 crypto cipher. If the phone does not support 80-bit authentication, it reverts

to the AES_CM_128_HMAC_SHA1_32 cipher. If a phone does not support 80-bit or 32-bit authentication tag, the negotiation occurs over Real-Time Transport Protocol (RTP).

Note The SCCP phone supports only 32-bit authentication tag. Hence, negotiation between the phone and IPVMS happens only over the AES_CM_128_HMAC_SHA1_32 cipher.

If Phone A supports AES_CM_128_HMAC_SHA1_80 and Phone B supports the AES_CM_128_HMAC_SHA1_32 crypto cipher, and when User A (Phone A) dials User B (Phone B) and the call is placed on hold by User B, then Phone A connects to MOH. The negotiation between Phone A and MOH occurs through AES_CM_128_HMAC_SHA1_80 cipher because Phone A supports only the 80-bit authentication tag.

If User B (Phone B) dials User A (Phone A) and the call is placed on hold by User A, the negotiation between Phone B and MOH occurs through the AES_CM_128_HMAC_SHA1_32 cipher because Phone B supports only the 32-bit authentication tag.

If a phone supports 80-bit authentication tag, the negotiation between a phone and an IVR or Annunciator occurs through AES_CM_128_HMAC_SHA1_80.

The following table shows the supported crypto ciphers on the phones and their negotiation cipher.

Table 1: Phones Capabilities vs. Negotiated Cipher

Phones Capabilities	Negotiated Cipher
AES_CM_128_HMAC_SHA1_32 and AES_CM_128_HMAC_SHA1_80	AES_CM_128_HMAC_SHA1_80
AES_CM_128_HMAC_SHA1_32	AES_CM_128_HMAC_SHA1_32
AES_CM_128_HMAC_SHA1_80	AES_CM_128_HMAC_SHA1_80
Other than AES_CM_128_HMAC_SHA1_32 and AES_CM_128_HMAC_SHA1_80	Revert to RTP.

Self-encrypting Drive

Unified Communications Manager supports self-encrypting drives (SED). This is also called Full Disk Encryption (FDE). FDE is a cryptographic method that is used to encrypt all the data that is available on the hard drive. The data includes files, operating system, and software programs. The hardware available on the disk encrypts all the incoming data and decrypts all the outgoing data.

When the drive is locked, an encryption key is created and stored internally. All data that is stored on this derive is encrypted using that key and stored in the encrypted form. The FDE comprises a key ID and a security key.

For more information, see Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Configuration File Encryption

Unified Communications Manager pushes confidential data such as digest credentials and administrator passwords to phones in configuration file downloads from the TFTP server.

Unified Communications Manager uses reversible encryption to secure these credentials in the database. To secure this data during the download process, Cisco recommends that you configure encrypted configuration files for all Cisco IP Phones that support this option. When this option is enabled, only the device configuration file gets encrypted for download.

Note In some circumstances, you may choose to download confidential data to phones in the clear; for example, to troubleshoot the phone.

Unified Communications Manager encodes and stores encryption keys in the database. The TFTP server encrypts and decrypts configuration files by using symmetric encryption keys:

- If the phone has PKI capabilities, Unified Communications Manager can use the phone public key to encrypt the phone configuration file.
- If the phone does not have PKI capabilities, you must configure a unique symmetric key in Unified Communications Manager and in the phone.

You enable encrypted configuration file settings in the Phone Security Profile window in Unified Communications Manager Administration, which you then apply to a phone in the Phone Configuration window.

Default Security Administration Tasks

The following are the default security administration tasks:

Procedure

	Command or Action	Purpose
Step 1	Update ITL File for Cisco Unified IP Phones	Validates TFTP configuration files.
Step 2	Obtain Cisco Unified IP Phone Support List	Obtain the Cisco Unified IP Phone Support List using Cisco Unified Reporting page.
Step 3	Roll Back Cluster to a Pre-8.0 Release	Prepare the cluster for rollback.
Step 4	Perform Bulk Reset of ITL File, on page 19	Perform the bulk reset of ITL file.
Step 5	Reset CTL Localkey	Perform a reset of the Cisco Trust List (CTL) file with the CLI command
Step 6	View the Validity Period of ITLRecovery Certificate	View the validity period of ITLRecovery Certificate.
Step 7	Set Up Authentication and Encryption	Implement authentication and encryption for a new install.

Update ITL File for Cisco Unified IP Phones

A centralized TFTP with Unified Communication Manager using Security By Default with ITL files installed on the phones does not validate TFTP configuration files.

Perform the following procedure before any phones from the remote clusters are added to the centralized TFTP deployment.

Procedure

Step 1 On the Central TFTP server, enable the Enterprise Parameter **Prepare cluster for pre CM-8.0 rollback**.

Step 2 Restart TVS and TFTP.

Step 3 Reset all phones to verify that they download the new ITL file that disables ITL signature verification.

Step 4 Configure Enterprise Parameter Secure https URLs to use HTTP instead of HTTPS.

Note Unified Communications Manager Release 10.5 and later automatically resets phones after you enable the **Prepare cluster for pre CM-8.0 rollback** Enterprise Parameter. For Central TFTP server's Unified Communications Manager version and how to enable this parameter, see "Roll Back Cluster to a Pre-8.0 Release" section in the Security Guide for Cisco Unified Communications Manager.

Obtain Cisco Unified IP Phone Support List

Use the Cisco Unified Reporting tool to generate a list of Cisco endpoints that support Security By Default.

Procedure

Step 1 From Cisco Unified Reporting, choose **System Reports**.

Step 2 From the **System Reports** list, choose **Unified CM Phone Feature List**.

Step 3 From the **Product** drop-down list, choose **Security By Default**.

Step 4 Click **Submit**.
A report is generated with the list of supported features for the particular phone.

Roll Back Cluster to a Pre-8.0 Release

Before you roll back a cluster to a pre-8.0 release of Unified Communications Manager, you must prepare the cluster for rollback using the Prepare Cluster for Rollback to pre-8.0 enterprise parameter.

To prepare the cluster for rollback, follow this procedure on each server in the cluster.

Procedure

Step 1 From Unified Communications Manager, choose **System** > **Enterprise Parameters Configuration**.

The **Enterprise Parameters Configuration** window displays.

Set the Prepare Cluster for Rollback to pre-8.0 enterprise parameter to **True**.

Note Enable this parameter only if you are preparing to rollback your cluster to a pre-8.0 release of Unified Communications Manager. Phone services that use https (for example, extension mobility) will not work while this parameter is enabled. However, users will be able to continue making and receiving basic phone calls while this parameter is enabled.

Step 2 Wait ten minutes for the Cisco IP Phones to automatically restart and register with Unified Communications Manager.

Step 3 Revert each server in the cluster to the previous release.

For more information about reverting a cluster to a previous version, see *Administration Guide for Cisco Unified Communications Manager* .

Step 4 Wait until the cluster finishes switching to the previous version.

Step 5 If you are running one of the following releases in mixed mode, you must run the CTL client:

- Unified Communications Manager Release 7.1(2)
  - All regular releases of 7.1(2)
  - All ES releases of 712 prior to 007.001(002.32016.001)
- Unified Communications Manager Release 7.1(3)
  - All regular releases of 713 prior to 007.001(003.21900.003) = 7.1(3a)su1a
  - All ES releases of 713 prior to 007.001(003.21005.001)

Note For more information about running the CTL client, see the “Configuring the CTL Client” chapter.

Step 6 If “Prepare Cluster for Rollback to pre 8.0” is set to True in Enterprise Parameters then the following change must be made for Corporate Directories to work:

Under **Device > Device Settings > Phone Services > Corporate Directory** you must change the Service URL from Application:Cisco/CorporateDirectory to http://<ipaddr>:8080/ccmcip/xmldirectoryinput.jsp.

Step 7 If “Prepare Cluster for Rollback to pre 8.0” is set to True in Enterprise Parameters then the following change must be made for Personal Directories to work:

Under **Device > Device Settings > Phone Services > Personal Directory** you must change the Service URL from Application:Cisco/PersonalDirectory to 'http://<ipaddr>>:8080/ccmpd/pdCheckLogin.do?name=undefined.

Switch Back to Release 8.6 or Later After Revert

If you decide to switch back to the release 8.6 or later partition after you revert the cluster to Release 7.x, follow this procedure.

Procedure

Step 1 Follow the procedure for switching the cluster back to the inactive partition. For more information, see the *Administration Guide for Cisco Unified Communications Manager* .

Step 2 If you were running one of the following releases in mixed mode, you must run the CTL client:

Unified Communications Manager Release 7.1(2)

- All regular releases of 7.1(2)
- All ES releases of 712 prior to 007.001(002.32016.001)
- Unified Communications Manager Release 7.1(3)
  - All regular releases of 713 prior to 007.001(003.21900.003) = 7.1(3a)su1a
  - All ES releases of 713 prior to 007.001(003.21005.001)

Note For more information about running the CTL client, see the "Configuring the CTL Client" chapter.

Step 3 From Unified Communications Manager Administration, choose **System** > **Enterprise Parameters Configuration**.

The **Enterprise Parameters Configuration** window displays.

Set the Prepare Cluster for Rollback to pre-8.6 enterprise parameter to **False**.

Step 4 Wait ten minutes for the Cisco Unified IP Phones to automatically restart and register with Unified Communications Manager.

Perform Bulk Reset of ITL File

Make sure you perform this procedure only from the Unified Communications Manager publisher.

The bulk reset of the ITL file is performed, when phones no longer trust the ITL file signer and also cannot authenticate the ITL file provided by the TFTP service locally or using TVS.

To perform a bulk reset, use the CLI command **utils itl reset**. This command generates a new ITL recovery file and re-establishes the trust between phones and the TFTP service on CUCM.

Tip When you install Unified Communications Manager, use the CLI command **file get tftp** *ITLRecovery.p12*to export the ITL Recovery pair and then perform a backup through DR. You will also be prompted to enter the SFTP server (where the key is exported) and password.

Procedure

Step 1 Perform any one of the following steps:

- Run **utils itl reset localkey**.
- Run **utils itl reset remotekey**.

Note For **utils itl reset localkey**, the local key resides on the publisher. When issuing this command, the ITL file is signed temporarily by the CallManager key while the ITL Recovery key is resetting.

Step 2 Run **show itl** to verify that the reset was successful.

Step 3 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 4 Click **Reset**.

The devices restart. They are ready to download the ITL file that is signed by the CallManager key and accept configuration files.

Step 5 Restart the TFTP service and restart all devices.

Note Restarting the TFTP service causes the ITL File to be signed by the ITLRecovery Key and rolling back the changes in Step 1.

The devices download the ITL file that is signed with the ITLRecovery Key and register correctly to Unified Communications Manager again.

Reset CTL Localkey

When devices on a Unified Communications Manager cluster are locked and lose their trusted status, perform a reset of the Cisco Trust List (CTL) file with the CLI command **utils ctl reset localkey**. This command generates a new CTL file.

Procedure

Step 1 Run **utils ctl reset localkey**

Note For **utils ctl reset localkey**, the local key resides on the publisher. When issuing this command, the CTL file is temporarily signed by the CallManager key.

Step 2 Run **show ctl** to verify that the reset was successful.

Step 3 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.
The **Enterprise Parameters Configuration** page appears.

Step 4 Click **Reset**.

The devices restart. They are ready to download the CTL file that is signed by the CallManager key and accept configuration files.

Step 5 Run the **utils ctl update CTLFile** and restart the necessary services rolling back the changes in Step 1.

The devices restart. They are ready to download the CTL file that is signed by the ITLRecovery key and accept configuration files.

The devices download the CTL file that is signed using the required keys and register correctly to Unified Communications Manager again.

View the Validity Period of ITLRecovery Certificate

The ITLRecovery certificate has a long validity period with phones. You can navigate to the **Certificate File Data** pane to view the validity period or any other ITLRecovery certificate details.

Procedure

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

Step 2 Enter the required search parameters to find the certificate and view its configuration details. The list of certificates that match the criteria appears in the **Certificate List** page.

Step 3 Click the **ITLRecovery** link to view the validity period.

The ITLRecovery certificate details appear in the **Certificate File Data** pane.

The validity period is 20 years from the current year.

Set Up Authentication and Encryption

Important This procedure applies to the CTL Client encryption option. You may also set up encryption by using the **utils ctl** CLI command set. For more information about this option, see the *Command Line Interface Guide for Cisco Unified Communications Solutions.*

The following procedure provides all the tasks that you must perform to implement authentication and encryption. See the related topics for chapter references which contain tasks that you must perform for the specified security feature.

- To implement authentication and encryption for a new install, refer to the following table.
- To add a node to a secure cluster, see *Installing Cisco Unified Communications Manager*, which describes how to add a node and how to configure security for the new node.

Procedure

Step 1 Activate the Cisco CTL Provider service in Cisco Unified Serviceability

Be sure to activate the Cisco CTL Provider service on each Unified Communications Manager server in the cluster.

Tip If you activated this service prior to a Unified Communications Manager upgrade, you do not need to activate the service again. The service automatically activates after the upgrade.

Step 2 Activate the Cisco Certificate Authority Proxy service in Cisco Unified Serviceability to install, upgrade, troubleshoot, or delete locally significant certificates.

Activate the Cisco Certificate Authority Proxy service on the first node only.

Timesaver Performing this task before you install and configure the Cisco CTL client ensures that you do not have to update the CTL file to use CAPF.

Step 3 If you do not want to use the default port settings, configure ports for the TLS connection.

Tip If you configured these settings prior to a Unified Communications Manager upgrade, the settings migrate automatically during the upgrade.

Step 4 If using the Cisco CTL client for encryption, obtain at least two security tokens and the passwords, hostnames/IP addresses, and port numbers for the servers that you will configure for the Cisco CTL client.

Note You do not need hardware security tokens for the **utils ctl** CLI option.

Step 5 Install the Cisco CTL client.

Tip To update the Cisco CTL file after an upgrade to this Unified Communications Manager release, you must install the plug-in that is available in this Cisco Unified Communications Manager Administration release.

Step 6 Configure the Cisco CTL client.

Tip If you created the Cisco CTL file prior to a Unified Communications Manager upgrade, the Cisco CTL file migrates automatically during the upgrade. To update the Cisco CTL file after an upgrade to this Unified Communications Manager release, you must install and configure the latest version of the Cisco CTL client.

Note Cisco's CTL client is no longer supported from Release 14. We recommend you use the CLI command to switch the Unified Communications Manager server to Mixed Mode instead of the Cisco CTL plugin.

Step 7 Configure the phone security profiles.

Perform the following tasks when you configure the profiles:

a) Configure the device security mode.

Tip The device security mode migrates automatically during the Unified Communications Manager upgrade. If you want to configure encryption for devices that only supported authentication in a prior release, you must choose a security profile for encryption in the **Phone Configuration** window.

b) Configure CAPF settings (for some phones that are running SCCP and SIP).

Additional CAPF settings display in the Phone Configuration window.

c) If you plan to use digest authentication for phones that are running SIP, check the Enable Digest Authentication check box.
d) To enable encrypted configuration files (for some phones that are running SCCP and SIP), check the Encrypted Confide check box.
e) To exclude digest credentials in configuration file downloads, check the Exclude Digest Credential in Configuration File check box.

Step 8 Apply the phone security profiles to the phones.

The following steps are optional:

Step 9 (Optional) Verify that the locally significant certificates are installed on supported Cisco Unified IP Phones .

Step 10 (Optional) Configure digest authentication for phones that are running SIP.

Step 11 (Optional) Perform phone-hardening tasks.

Tip If you configured phone-hardening settings prior to a Unified Communications Manager upgrade, the device configuration settings migrate automatically during the upgrade.

Step 12 (Optional) Configure conference bridge resources for security.

Step 13 (Optional) Configure voice mail ports for security.

For more information, see the applicable Cisco Unity or Cisco Unity Connection integration guide for this Unified Communications Manager release.

Step 14 (Optional) Configure security settings for SRST references.

Tip If you configured secure SRST references in a previous Unified Communications Manager release, the configuration automatically migrates during the Unified Communications Manager upgrade.

Step 15 (Optional) Configure IPSec.

For more information, see the *Administration Guide for Cisco Unified Communications Manager* .

Step 16 (Optional) Configure the SIP trunk security profile.

If you plan to use digest authentication, check the Enable Digest Authentication check box in the profile.

For trunk-level authorization, check the authorization check boxes for the allowed SIP requests.

If you want application-level authorization to occur after trunk-level authorization, check the Enable Application Level Authorization check box.

You cannot check application-level authorization unless digest authentication is checked.

Step 17 (Optional) Apply the SIP trunk security profile to the trunk.

Step 18 (Optional) Configure digest authentication for the trunk.

Step 19 (Optional) If you checked the Enable Application Level Authorization check box in the SIP trunk security profile, configure the allowed SIP requests by checking the authorization check boxes in the Application User Configuration window.

Step 20 (Optional) Reset all phones.

Step 21 (Optional) Reboot all servers.