Security Overview

Implementing security mechanisms in the Unified Communications Manager system prevents identity theft of the phones and the Unified Communications Manager server, data tampering, and call-signaling/media-stream tampering.

The CiscoIP telephony network establishes and maintains authenticated communication streams, digitally signs files before transferring the file to the phone, and encrypts media streams and call signaling between Cisco Unified IP Phones.

Terms and Acronyms

The definitions in the following table apply when you configure authentication, encryption, and other security features for your CiscoIPtelephony network:

Table 1: Terminology

Term	Definition
Access Control List (ACL)	List that defines rights and permissions to access system functions and resources. See Method List.

Term	Definition
Authentication	Process that verifies the identity of the communicating entity.
Authorization	Process that specifies whether an authenticated user, service, or application has the necessary permissions to perform a requested action; in Unified Communications Manager, the security process that restricts certain trunk-side SIP requests to authorized users.
Authorization Header	A SIP user agent response to a challenge.
Certificate	A message that contains the certificate holder name, the public key, and the digital signature of the certificate authority that is issuing the certificate.
Certificate Authority (CA)	Trusted entity that issues certificates: Cisco or a third-party entity.
Certificate Authority Proxy Function (CAPF)	Process by which supported devices can request locally significant certificates by using Unified Communications Manager Administration.
Certificate Trust List (CTL)	A file, which is created either with the CLI command set **utils cli** or with the CTL Client and signed by the Cisco Site Administrator Security Token (security token), that contains a list of certificates for servers that the phone is to trust.
Challenge	In digest authentication, a request to a SIP user agent to authenticate its identity.
Cisco Site Administrator Security Token (security token; etoken)	A portable hardware security module that contains a private key and an X.509v3 certificate that the Cisco Certificate Authority signs; used for file authentication, it may be used to sign the CTL file. Hardware security tokens are required for only the CTL Client. The CLI command set **utils ctl** does not require hardware security tokens.
Device Authentication	Process that validates the identity of the device and ensures that the entity is what it claims to be before a connection is made.
Digest Authentication	A form of device authentication where an MD5 hash of a shared password (among other things) gets used to establish the identity of a SIP user agent.
Digest User	User name that is included in an authorization request that phones that are running SIP or SIP trunks send.
Digital Signature	Value that is generated by hashing the message and then encrypting the message with the private key of the signer; the recipient decrypts the message and the hash with the signer public key, produces another hash with the same hash function, then compares the two hashes to ensure that the messages match and the content is intact.
DSP	Digital signaling processor.
DSP Farm	A network resource for IP telephony conferencing that is provided by DSPs on a H.323 or MGCP gateway.

Term	Definition
Encryption	Process of translating data into ciphertext, which ensures the confidentiality of the information and that only the intended recipient can read the data. Requires an encryption algorithm and encryption key.
File Authentication	Process that validates digitally signed files that the phone downloads. The phone validates the signature to make sure that file tampering did not occur after the file creation.
H.323	An internet standard that defines a common set of codecs, call setup and negotiating procedures, and basic data transport methods.
hash	A number, usually in hexadecimal, that is generated from a string of text by using a hash function, which creates a small digital “fingerprint” for the data.
Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)	An IETF-defined protocol that ensures (at a minimum) the identity of the HTTPS server; by using encryption, ensures the confidentiality of the information that is exchanged between the Tomcat server and the browser client.
Image Authentication	Process whereby a phone validates the integrity and source of a binary image prior to loading it on the phone.
Integrity	Process that ensures that data tampering did not occur between entities.
IPSec	Transport that provides secure H.225, H.245, and RAS signaling channels for end-to-end security.
Locally Significant Certificate (LSC)	A digital X.509v3 certificate that CAPF issues; installed on the phone or JTAPI/TAPI/CTI application.
Manufacture Installed Certificate (MIC)	A digital X.509v3 certificate that is signed by the Cisco Certificate Authority and installed in supported phones by Cisco Manufacturing; used as the authentication mechanism to CAPF when LSCs are installed in phones.
Man-in-the-Middle Attacks	Process that allows an attacker to observe and modify the information flow between Unified Communications Manager and the phone.
Multipoint Control Unit (MCU)	A flexible system to connect multiple H.323 endpoints and allow multiple users to participate in IP-based video conferences.
MD5	A hash function that is used with encryption.
Media Encryption	Process whereby the confidentiality of the media is protected with cryptographic procedures. Media encryption uses Secure Real-Time Protocol (SRTP) as defined in IETFRFC3711.
Message/Data Tampering	Event when an attacker attempts to alter messages in transit, including ending a call prematurely.

Term	Definition
Method List	Tool to restrict certain categories of messages that can come in on a SIP trunk during the authorization process; defines which SIP nonINVITE methods are allowed for a trunk-side application or device. Also method ACL.
Mixed Mode	Unified Communications Manager security mode that you configure to allow devices with secure/nonsecure profiles and RTP/ SRTP media to connect to Unified Communications Manager.
Nonce	A unique, random number that the server generates for each digest authentication request; used to generate an MD5 hash.
Nonsecure Mode	Unified Communications Manager security mode that you configure to allow devices with nonsecure profiles and RTP media to connect to Unified Communications Manager.
Nonsecure Call	Call in which at least one device is not authenticated or encrypted.
Nonsecure Device	Device that uses UDP or TCP signaling and nonsecure media.
PKI	Public key infrastructure, which comprises the set of elements that is needed for public key encryption, including secure public key distribution, certificates, and certificate authorities.
Public / Private key	Keys that are used in encryption. Public keys are widely available, but private keys are held by their respective owners. Asymmetrical encryption combines both types.
Replay Attack	Event when an attacker captures information that identifies a phone or proxy server and replays information while pretending to be the actual device; for example, by impersonating the proxy server private key.
RTP	Real-Time Transport Protocol
Simple Certificate Enrollment Protocol (SCEP)	A protocol that is used to communicate with a certificate authority that issues X.509 certificates.
Secure Call	Call in which all devices are authenticated, signaling is encrypted, and the media (voice stream) is encrypted.
Signaling Authentication	TLS process that validates that no tampering occurred to signaling packets during transmission.
Signaling Encryption	Process that uses cryptographic methods to protect the confidentiality of all signaling messages that are sent between the device and the Unified Communications Manager server.
SIP Realm	A string (name) that Unified Communications Manager uses to respond to a challenge.
SRTP	Secure Real-Time Transport Protocol that secures voice conversation in the network and provides protection against replay attacks.

Term	Definition
SSL	A cryptographic protocol that secures data communications such as e-mail on the Internet; equivalent to TLS, its successor.
Transport Layer Security (TLS)	A cryptographic protocol that secures data communications such as e-mail on the Internet; functionally equivalent to SSL.
Trust List	Certificate list without digital signatures.
Trust Store	A repository of X.509 certificates that an application, such as Unified Communications Manager, explicitly trusts.
X.509	An ITU-T cryptographic standard for importing PKI certificates, which includes certificate formats.

System Requirements

The following system requirements exist for authentication or encryption:

- The Administrator password can differ on every server in a cluster.
- The username and password that are used at the Cisco CTL client (to log in to the Unified Communications Manager server) must match the Unified Communications Manager Administration username and password (the username and password that are used to log in to Unified Communications Manager Administration).
- Before you configure voicemail ports for security, verify that you installed a version of Cisco Unity or Cisco Unity Connection system that supports this Unified Communications Manager release.

Related Topics

CAPF System Interactions and Requirements

Features List

Unified Communications Manager system uses a multilayered approach to call security, from the transport layer to the application layer.

Transport layer security includes TLS and IPSec for signaling authentication and encryption to control and prevent access to the voice domain. SRTP adds media authentication and encryption to secure privacy and confidentiality for voice conversation and other media.

The following table provides a summary of the authentication and encryption features that Unified Communications Manager can implement during an SCCP call session, depending on the features that are supported and configured.

Table 2: SCCP Call Security Features

Security Feature	Line Side	Trunk Side
Transport/Connection/Integrity	Secure TLS port	IPSec associations

Security Feature	Line Side	Trunk Side
Device Authentication	TLS certificate exchange w/Unified Communications Manager and/or CAPF	IPSec certificate exchange or preshared key
Signaling Authentication/Encryption	TLS Mode: authenticated or encrypted	IPSec [authentication header, encryption (ESP), or both]
Media Encryption	SRTP	SRTP
Authorization	Presence requests	Presence requests
Note Supported features on a device vary by device type.		

The following table provides a summary of the authentication and encryption features that Unified Communications Manager can implement during a SIP call session, depending on the features that are supported and configured.

Table 3: SIP Call Security Features

Security Feature	Line Side	Trunk Side
Transport/Connection/Integrity	Secure TLS port	Secure TLS port
Device Authentication	TLS certificate exchange w/Unified Communications Manager and/or CAPF	IPSec certificate exchange or preshared key
Digest Authentication	Each SIP device uses unique digest user credentials.	SIP trunk user agents use unique digest credentials.
Signaling Authentication/Encryption	TLS Mode: authenticated or encrypted (except Cisco Unified IP Phones 7942/7962).	TLS Mode: authenticated or encrypted mode
Media Encryption	SRTP	SRTP
Authorization	Presence requests	Presence requests Method list
Note Supported features on a device vary by device type.		

Security Icons

Unified Communications Manager provides security status for a call, according to security levels that are configured for the Unified Communications Manager server(s) and devices that are participating in the call.

Phones that support security icons display the call security level.

- The phone displays a shield icon for calls with a signaling security level of authenticated. A shield identifies a secured connection between CiscoIP devices, which means that the devices have authenticated or encrypted signaling.
- The phone displays a lock icon for calls with encrypted media, which means that the devices are using encrypted signaling and encrypted media.

Note Some phone models display only the lock icon.

The security status of a call can change for point-to-point, intracluster, intercluster, and multihop calls. SCCP line, SIP line, and H.323 signaling support notification of call security status changes to participating endpoints. Refer to topics related to security icons and encryption for restrictions that are associated with security icons.

The audio and video portions of the call provide basis for the call security status. Consider the call secure only if both the audio and video portions are secure. The following table describes the rules that determine whether a security icon displays, and which icon appears.

Table 4: Security Icon Display Rules

Media and Device Types In the Call	Phones That Display Both Shield and Lock Icons	Phones That Display Only the Lock Icon
Secure audio only	Lock	Lock
Secure audio with unsecure video	Shield	None
Secure audio with secure video	Lock	Lock
Authenticated device with nonsecure audio only	Shield	None
Authenticated device with nonsecure audio and video	Shield	None
Unauthenticated device with nonsecure audio only	None	None
Unauthenticated device with nonsecure audio and video	None	None

Note The "Override BFCP Application Encryption Status When Designating Call Security Status" service parameter displays the lock icon when parameter value is True and audio is secure. This condition ignores the security statuses of all other media channels. The default parameter value is False.

For conference and barge calls, the security icon displays the security status for the conference.

Related Topics

Secure Conference Icons

Interactions and Restrictions

This section contains interaction and restriction information.

See the related topics for information about interactions and restrictions that are associated with the secure conference feature.

Related Topics

Interactions, on page 8
Restrictions, on page 9
Secure Conference Resources Setup

Interactions

This section provides information on the Interaction of Cisco Security features with Unified Communications Manager applications.

Presence

Configure presence groups to restrict presence requests sent to authorized users. You can add presence group authorization for phones and trunks that are running SIP.

Refer to Feature Configuration Guide for Cisco Unified Communications Manager for more information about configuring presence groups.

Configure Unified Communications Manager to allow and accept presence requests on SIP trunk. If required, Configure Unified Communications Manager to accept and authenticate incoming presence requests from remote devices or applications.

SIP Trunk

Configure SIP Trunk Security Profile to accept incoming, out of dialog, REFER requests to use SIP-initiated transfer features and other advanced transfer features on SIP trunks. For Example, Web Transfer and Click to Dial.

Configure SIP Trunk Security Profile to accept Unsolicited Notification SIP requests to report events (MWI support) and to reduce per-call MTP allocations (from a voice-messaging server).

Configure SIP Trunk Security Profile to accept SIP requests which replaces header in REFERS and INVITES. The Unified Communications Manager can now transfer an external call for a SIP trunk to an external device or party.

Extension Mobility

For Extension Mobility, SIP digest credentials change when a user logs in and out as different end users have different credentials.

Computer Telephony Integration (CTI)

Cisco Unified Communications Manager Assistant supports a secure connection to CTI (transport layer security connection) when you configure a CAPF profile (one for each Cisco Unified Communications Manager Assistant node).

CTI TLS support requires you to configure a unique InstanceID (IID) for every application instance, when multiple instances of a CTI/JTAPI/TAPI application are running. The IID secures the signaling and media communication streams between CTI Manager and JTAPI/TSP/CTI applications.

When the device security mode equals authenticated or encrypted, the Cisco Unity-CM TSP connects to Unified Communications Manager through the Unified Communications Manager TLS port. When the security mode equals nonsecure, the Cisco Unity TSP connects to Unified Communications Manager through the CTI Manager port.

Restrictions

This section describes restrictions that apply to Cisco security features.

Related Topics

Authentication and Encryption, on page 9
Barge and Encryption, on page 9
Cluster and Device Security Modes, on page 12
Digest Authentication and Encryption, on page 12
Media Resources and Encryption, on page 10
Packet Capturing and Encryption, on page 12
Phone Support and Encryption, on page 10
Phone Support and Encrypted Setup Files, on page 11
Security Icons, on page 6
Wideband Codecs and Encryption, on page 10

Authentication and Encryption

Consider the following restrictions before you install and configure authentication and encryption features:

- You cannot implement signaling or media encryption without device authentication. To install device authentication, enable the Cisco CTL Provider service and install and configure the Cisco CTL client.
- Cisco does not support Network Address Translation (NAT) with Unified Communications Manager if you configure mixed mode.

  You can enable UDP in the firewall to allow media stream firewall traversal. Enabling UDP 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.

Barge and Encryption

The following restrictions apply to barge and encryption:

- Due to bandwidth requirements, Cisco IP Phones 7942 and 7962 do not support barge from an encrypted device on an active encrypted call. The barge attempt will fail. A tone plays on the initiator phone to indicate that the barge failed.
- Encrypted Cisco IP Phones that are running release 8.2 or earlier can only barge an active call as authenticated or nonsecure participants.
- If a caller barges a secure SCCP call, the system uses an internal tone-playing mechanism at the target device, and the status remains secure.
- If a caller barges a secure SIP call, the system provides tone-on-hold, and Unified Communications Manager classifies the call as nonsecure during the tone.

Note Nonsecure or authenticated Cisco IP Phones that are running release 8.3 or later can barge encrypted calls. The security icon indicates the security status for the conference.

Related Topics

Secure Conference Icons

Wideband Codecs and Encryption

The following information applies for Cisco Unified IP Phones 7962 or 7942 that are configured for encryption and associated with a wideband codec region. This only applies to Cisco Unified IP Phones 7962 or 7942 that are configured for TLS/SRTP.

To establish an encrypted call, Unified Communications Manager ignores the wideband codec and chooses another supported codec from the codec list that the phone presents. If the other devices in the call are not configured for encryption, Unified Communications Manager may establish the authenticated/nonsecure call by using the wideband codec.

Media Resources and Encryption

Unified Communications Manager supports authenticated and encrypted calls between secure Cisco Unified IP Phones (SCCP or SIP), secure CTI devices/route points, secure Cisco MGCP IOS gateways, secure SIP trunks, secure H.323 gateways, secure conference bridges, and secure H.323/H.245/H.225 trunks where no media resources are used. Unified Communications Manager does not provide media encryption in the following cases:

- Calls that involve transcoders
- Call that involve media termination points

Note MTP encryption is not supported only with the non-passthrough MTP.

Phone Support and Encryption

The following Cisco Unified IP Phones that are running SCCP support encryption: 6901, 6911, 6921, 6941, 6945, 6961,7906G, 7911G, 7925G, 7925G-EX, 7926G, 7931G, 7941G, 7941G-GE, 7942G, 7945G, 7961G, 7961G-GE, 7962G, 7965G, 7975G, 8941, 8945, and 9961.

The following Cisco Unified IP Phones that are running SIP support encryption: 6901, 6911, 6921, 6941, 6945, 6961, 7811, 7821, 7841, 7861, 7832, 7906G, 7911G, 7941G, 7941G-GE, 7942G, 7961G, 7961G-GE,7962G, 7965G, 7975G, 8811, 8821, 8821-EX, 8832, 8841, 8845, 8851, 8851NR, 8865, 8865NR, 8941, 8945, 8961, 9971, and 9971.

For more information, see the *System Configuration Guide for Cisco Unified Communications Manager* that support encryption and this version of Unified Communications Manager.

Warning To obtain the full benefit of security features, Cisco recommends that you upgrade Cisco IP Phones to firmware release 8.3 or later, which supports the encryption features in this Unified Communications Manager release. Encrypted phones that run earlier releases do not fully support these new features. These phones can participate in secure conference and barge calls only as authenticated or nonsecure participants.

Cisco IP Phones that are running on firmware release 8.3 with an earlier release of Unified Communications Manager will display their connection security status, not the conference security status, during a conference or barge call, and do not support secure conference features like conference list.

Phone Support and Encrypted Setup Files

Not all phones support encrypted configuration files. Some phones support encrypted configuration files but do not validate file signatures. All phones that support encrypted configuration files require firmware that is compatible with Unified Communications Manager Release 5.0 or later to receive full encrypted configuration files.

Related Topics

Phone Model Support

Security Icons and Encryption

The following restrictions apply to security icons and encryption:

- The encryption lock icon may not display on the phone when you perform tasks such as transferring or putting a call on hold; the status changes from encrypted to nonsecure if the media streams that are associated with these tasks, such as MOH, are not encrypted.
- Unified Communications Manager does not display the shield icon for calls that are transiting H.323 trunks.
- For calls that involve the PSTN, the security icon shows the security status for only the IP domain portion of the call.
- A SIP trunk will report encrypted or not-authenticated security status when using the TLS transport type. When SRTP is negotiated, the security status will get encrypted; otherwise it will remain not-authenticated. This will allow Unified Communications Manager call control to determine the overall security level of a call that involves a SIP trunk.

  A SIP trunk will report authenticated status over the trunk if a party is authenticated during events such as a meet-me conference or a cbarge. (The SIP trunk will still be using TLS/SRTP.)
- For Secure Monitoring and Recording, a SIP trunk will utilize the existing Call Info header mechanism for transmitting the security icon status over the SIP trunk, as currently used by the SIP line. This enables the SIP trunk peer to monitor the overall security status of a call.
- Some phone models display only the lock icon, not the shield icon.

Related Topics

Secure Conference Icons

Cluster and Device Security Modes

Note Device security mode configures the security capability for a Cisco IP Phone or SIP trunk. Cluster security mode configures the security capability for your standalone server or a cluster.

When the cluster security mode equals nonsecure, the device security mode equals nonsecure in the phone configuration file. In these circumstances, the phone makes nonsecure connections with the SRST-enabled gateway and Unified Communications Manager, even if the device security mode specifies authenticated or encrypted. Security-related settings other than device security mode, such as the SRST Allowed check box, also get ignored. The security configuration does not get deleted in Unified Communications Manager Administration, but security does not get provided.

The phone attempts a secure connection to the SRST-enabled gateway only when the cluster security mode equals mixed, the device security mode in the phone configuration file is set to authenticated or encrypted, the SRST Allowed? check box is checked in the Trunk Configuration window, and a valid SRST certificate exists in the phone configuration file.

Digest Authentication and Encryption

Unified Communications Manager defines a SIP call as having two or more separate call legs. For a standard, two-party call between two SIP devices, two separate call legs exist: one leg between the originating SIP user agent and Unified Communications Manager (the originating call leg) and the other leg between Unified Communications Manager and destination SIP user agent (the terminating call leg). Each call leg represents a separate dialog. Because digest authentication is a point-to-point process, digest authentication on each call leg stays independent of the other call legs. SRTP capabilities can change for each call leg, depending on the capabilities that are negotiated between the user agents.

Packet Capturing and Encryption

When SRTP encryption is implemented, third-party sniffing tools do not work. Authorized administrators with appropriate authentication can initiate packet capturing with a configuration change in Unified Communications Manager Administration (for devices that support packet capturing). See the *Troubleshooting Guide for Cisco Unified Communications Manager* that supports this release for information about configuring packet capturing in Unified Communications Manager.

Best Practices

We recommend the following best practices while configuring security for Unified Communications Manager:

- Always install and configure security in a secure lab environment before you deploy to a wide-scale network.
- Use IPSec for gateways and other application servers at remote locations.

Warning If you fail to use IPSec, the session encryption keys get transmitted in cleartext.

- To prevent toll fraud, configure conference enhancements. For more information, see System Configuration Guide for Cisco Unified Communications Manager.

  To restrict external call transfers, perform configuration tasks. For more information, see Feature Configuration Guide for Cisco Unified Communications Manager.

Related Topics

Media Encryption with Barge Setup, on page 14
Reset Devices, Servers, Clusters, and Services, on page 14

Device Resets, Server and Cluster Reboots, and Service Restarts

This section describes when you need to reset the devices, to reboot the server/cluster, or to restart services in Cisco Unified Serviceability.

Consider the following guidelines:

- Reset a single device after you apply a different security profile in Cisco Unified Communications Manager Administration.
- Reset the devices if you perform phone-hardening tasks.
- Reset the devices after you change the cluster security mode from mixed to nonsecure mode (or vice versa).
- Restart all devices after you configure the Cisco CTL client or update the CTL file.
- Reset the devices after you update CAPF enterprise parameters.
- Restart the Cisco CTL Provider service after you update ports for the TLS connection.
- Restart the Cisco CallManager service after you change the cluster security mode from mixed to nonsecure mode (or vice versa).
- Restart the Cisco Certificate Authority Proxy Function service after you update associated CAPF service parameters.
- Restart all Cisco CallManager and Cisco TFTP services in Cisco Unified Serviceability after you configure the Cisco CTL Client or update the CTL file. Perform this task on all servers that run these services in the cluster.
- Restart all Cisco CallManager and Cisco TFTP services after you start or stop the CTL Provider service.
- Reset dependent devices after you configure secure SRST references.
- If you set the Smart Card service to Started and Automatic, reboot the PC where you installed the Cisco CTL client.
- Restart the Cisco IP Manager Assistant service, Cisco Web Dialer Web Service, and the Cisco Extended Functions service after you configure the security-related service parameters that are associated with the Application User CAPF Profile.

To restart the Cisco CallManager service, refer to *Cisco Unified Serviceability Administration Guide*.

To reset a single device after you update the phone configuration, see topics related to applying the phone security profile.

Related Topics

Apply Security Profiles to Phone

Reset Devices, Servers, Clusters, and Services

This section provides information on when to reset devices, servers, clusters, and services in Cisco Unified Serviceability.

To reset all devices in a cluster, perform the following procedure:

Procedure

Step 1 From Unified Communications Manager, choose **System** > **CiscoUnifiedCM**.

Step 2 Click **Find**.

A list of configured Unified Communications Manager servers appears.

Step 3 Choose the Unified Communications Manager on which you want to reset devices.

Step 4 Click **Reset**.

Step 5 Perform Step 2 and Step 4 for each server in the cluster.

Related Topics

Device Resets, Server and Cluster Reboots, and Service Restarts, on page 13

Media Encryption with Barge Setup

Configure barge for Cisco Unified IP Phones 7962 and 7942 for encryption and perform the following tasks in Cisco Unified Communications Manager Administration.

- Update the Cluster Security Mode parameter in the CTL client.
- Update the Builtin Bridge Enable parameter in the **Service Parameter** window.

On completion of the tasks, the following message appears.

Attention If you configure encryption for Cisco Unified IP Phone models 7962 and 7942, the encrypted devices can't accept a barge request when they are participating in an encrypted call. The barge attempt fails when the call is encrypted.

Cisco Unified IP Phones 7962 and 7942 configured with an encrypted security profile doesn't display the message in the **Phone Configuration** window. You choose **Default** for the Built In Bridge setting or the default setting equals Default. The same restriction applies for either selection.

Tip Reset the dependent CiscoIP devices for changes to take effect.

Related Topics

Barge and Encryption, on page 9

CTL Client, SSL, CAPF, and Security Token Installation

To obtain authentication support, you can use one of the following options:

1. Install the Cisco CTL client, from Unified Communications Manager Administration. For the Cisco CTL client option, you must obtain at least two security tokens.
2. Use the CLI command set **utils ctl**, which does not require security tokens. For more information about this option, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

Media and signaling encryption capabilities automatically install when you install Unified Communications Manager.

Unified Communications Manager automatically installs Secure Sockets Layer (SSL) for Unified Communications Manager virtual directories.

Cisco Certificate Authority Proxy Function (CAPF) installs automatically as a part of Unified Communications Manager Administration.

TLS and IPSec

Transport security handles the coding, packing, and sending of data. Unified Communications Manager provides the following secure transport protocols:

- Transport Layer Security (TLS) provides secure and reliable data transfer between two systems or devices, by using secure ports and certificate exchange. TLS secures and controls connections among Unified Communications Manager-controlled systems, devices, and processes to prevent access to the voice domain. Unified Communications Manager uses TLS to secure SCCP calls to phones that are running SCCP and SIP calls to phones or trunks that are running SIP.
- IP Security (IPSec) provides secure and reliable data transfer between Unified Communications Manager and gateways. IPSec implements signaling authentication and encryption to CiscoIOS MGCP and H.323 gateways.

You can add secure RTP (SRTP) to TLS and IPSec transport services for the next level of security on devices that support SRTP. SRTP authenticates and encrypts the media stream (voice packets) to ensure that voice conversations that originate at or terminate to CiscoUnifiedIPPhones and either TDM or analog voice gateway ports are protected from eavesdroppers who may have gained access to the voice domain. SRTP adds protection against replay attacks.

Cisco Unified Communications Manager 9.0 and later provides TLS/SRTP support for dual-mode smart phones. TLS establishes the same secure and reliable data transfer mode for mobile phones as for IP phones, and SRTP encrypts voice conversations.

Certificates

Certificates secure client and server identities. After root certificates are installed, certificates get added to the root trust stores to secure connections between users and hosts, including devices and application users.

Administrators can view the fingerprint of server certificates, regenerate self-signed certificates, and delete trust certificates at the Cisco Unified Communications Operating System GUI.

Administrators can also regenerate and view self-signed certificates at the command line interface (CLI).

For information on updating the CallManager trust store and managing certificates, refer to the *Administration Guide for Cisco Unified Communications Manager* that supports this Unified Communications Manager release.

Note

- Unified Communications Manager supports only PEM (.pem) and DER (.der) formatted certificates.
- The maximum supported size of certificate for DER or PEM is 4096 bits.

Note When you upload two certificates, ensure that they have same common name and same validity period but different serial numbers and signature algorithms.

For example, root CA with `27:20:41:0c:5b:08:69:80:42:62:4f:13:bd:16:06:6a`serial number and SHA1 algorithm exists in Cisco Unified Communications Manager tomcat-trust. When you attempt to upload the certificate with `7b:35:33:71:0b:7c:08:b2:47:b3:aa:f9:5c:0d:ca:e4` serial number and SHA256 algorithm, the certificate management happens in the following way:

1. The validity of incoming certificate is verified.
2. The certificate with same common name is searched in the Tomcat trust folder.
3. The serial numbers of the certificate existing in the Tomcat trust folder and the incoming certificate that you are uploading is checked. If the serial numbers are different, the validity start date of both the certificates is verified. If the validity start time stamp of incoming certificate is later than the validity start time stamp of the existing certificate, the existing certificate replaces the newer incoming certificate in the Tomcat trust folder. Else, the new incoming certificate is not uploaded.

Both SHA1 and SHA256 algorithms have same subject name or common name, which implies that they belong to the same entity. The Unified Communications Manager framework does not support both these algorithms on the Unified Communications Manager server simultaneously. Only one certificate that belongs to any entity is supported in a particular trust folder, irrespective of the signature algorithm.

Related Topics

Phone Certificate Types, on page 16
Server Certificate Types, on page 18
Support for Certificates from External CAs, on page 19

Phone Certificate Types

A phone certificate is a unique identifier which authenticates phones. It's crucial for security against IP attacks.

Phone Certificates are as follows:

Table 5:

Phone Certificates	Description
Manufacture Installed Certificate (MIC)	MICs are signed by Cisco Manufacturing CA and we automatically install this certificate in supported Cisco Unified IP Phone. MICs authenticate with CiscoCertificate Authority Proxy Function (CAPF) for Locally Significant Certificates (LSC) installation or download an encrypted configuration file. Cannot use after expiry, as administrators can't modify, delete, or revoke the certificates.
Locally Significant Certificates (LSC)	Cisco Unified IP Phones require an LSC to operate in secure mode and is used for authentication and encryption. They are signed by CAPF, Online or Offline CA and takes precedence over MIC. After you perform the necessary tasks that are associated with CAPF, this certificate gets installed on supported phones. The LSC secures the connection between Unified Communications Manager and the phone after you configure the device security mode for authentication or encryption.

Tip We recommend that you use only MICs for LSC installation. We support LSCs to authenticate the TLS connection with Unified Communications Manager. When phone configurations use MICs for TLS authentication or for any other purpose, we assume no liability as MIC root certificates get easily compromised.

Upgrade Cisco Unified IP Phones 6900, 7900, 8900, and 9900 series to use LSCs for a TLS connection to Unified Communications Manager. Remove MIC root certificates from the Unified Communications Manager trust store to avoid possible future compatibility issues.

Note Phone models that use MICs for TLS connection to Unified Communications Manager may not be able to register.

Administrators should remove the following MIC root certificates from the Unified Communications Manager trust store:

- CAP-RTP-001
- CAP-RTP-002
- Cisco_Manufacturing_CA
- Cisco_Root_CA_2048
- Cisco_Manufacturing_CA_SHA2
- Cisco_Root_CA_M2
- ACT2_SUDI_CA

MIC root certificates that stay in the CAPF trust store get used for certificate upgrades. For information on updating the Unified Communications Manager trust store and managing certificates, see Administration Guide for Cisco Unified Communications Manager.

Note The Secure Onboarding feature doesn't work if you remove the Cisco Manufacturing certificates from the CallManger-trust store, because it can't validate the Manufacture Installed Certificates (MICs) from phones.

Related Topics

Set Up Authentication and Encryption, on page 33

Server Certificate Types

Server Certificates are basically to identify a server. The server certificates serve the rationale of encrypting and decrypting the content.

Self-signed (own) certificate types in Unified Communications Manager servers are as follows:

Unified Communications Manager imports the following certificate types to the Unified Communications Manager trust store:

Table 6: Certificate Type and Description

Certificate Type	Description
Cisco Unity server or Cisco Unity Connection certificate	Cisco Unity and Cisco Unity Connection use this self-signed root certificate to sign the Cisco Unity SCCP and Cisco Unity Connection SCCP device certificates. For Cisco Unity, the Cisco Unity Telephony Integration Manager (UTIM) manages this certificate. For Cisco Unity Connection, Cisco Unity Connection Administration manages this certificate.
Cisco Unity and Cisco Unity Connection SCCP device certificates	Cisco Unity and Cisco Unity Connection SCCP devices use this signed certificate to establish a TLS connection with Unified Communications Manager.
SIP Proxy server certificate	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.

Note The certificate name represents a hash of the certificate subject name, which is based on the voice-mail server name. Every device (or port) gets issued a certificate that is rooted at the root certificate.

The following additional trust store exists:

- Common trust store for Tomcat and web applications
- IPSec-trust
- CAPF-trust
- Userlicensing-trust
- TVS-trust

- Phone-SAST-trust
- Phone-CTL-trust

For more information about CA trust certificates for Cisco Unity Connection, see the Administration Guide for Cisco Unified Communications Manager. These trust-certificates secure connections to Exchange or Meeting Place Express for fetching e-mails, calendar information, or contacts.

Support for Certificates from External CAs

Unified Communications Manager supports integration with third-party certificate authorities (CAs) by using a PKCS#10 certificate signing request (CSR) mechanism, which is accessible at the Unified Communications Manager GUI.

Customers who currently use third-party CAs should use the CSR mechanism to issue certificates for:

- Unified Communications Manager
- CAPF
- IPSec
- Tomcat
- TVS

Note Multiserver (SAN) CA-signed certificates only applies to nodes in the cluster when the certificate gets uploaded to the Publisher. Generate a new multiserver certificate. Upload it to the cluster every time you add a new node or build it again.

If you run your system in mixed mode, some endpoints may not accept CA certificates with a key size of 4096 or longer. To use CA certificates in mixed mode, choose one of the following options:

- Use certificates with a certificate key size less than 4096.
- Use self-signed certificates.

Note This release of Unified Communications Manager doesn't provide SCEP interface support.

Note Be sure to run the CTL client after you upload a third-party, CA-signed certificate to the platform to update the CTL file.

Restart the appropriate services for the update after running the CTL client.

For example:

- Restart TFTP services and Unified Communications Manager services when you update the Unified Communications Manager certificate.

- Restart CAPF when you update the CAPF certificate.

After uploading the Unified Communications Manager or CAPF certificates, you might observe the phones reset automatically to update their ITL File.

For information on generating Certificate Signing Requests (CSRs) at the platform, see Administration Guide for Cisco Unified Communications Manager.

Related Topics

Cisco CTL Client Setup
Default Security Setup

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.

Related Topics

Authorization, on page 24
Device Authentication, on page 20
Digest Authentication, on page 22
File Authentication, on page 21
Image Authentication, on page 20
Signaling Authentication, on page 22

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.

Related Topics

Certificate Authority Proxy Function
Cisco CTL Client Setup
Phone Model Support

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.

Related Topics

Cisco CTL Client Setup
Phone Model Support

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.

Related Topics

Cisco CTL Client Setup

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.

Related Topics

Digest Authentication for SIP Phones Setup
Encrypted Phone Configuration File Setup
Digest Authentication Setup for SIP Trunks

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.

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:

Related Topics

Configuration File Encryption, on page 31
Media Encryption, on page 26
Signaling Encryption, on page 25

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.

Related Topics

Secure Conference Resources Setup

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.

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 7: 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.

Related Topics

TFTP Encrypted Configuration Files Overview
Phone Model Support

Encrypted iX Channel

Unified Communications Manager supports an encrypted iX channel. The iX channel provides a reliable channel for multiplexing application media between SIP phones in a video conference. Encrypted iX Channel uses DTLS to add security to your deployment and ensures that the application media is sent over the iX Channel is private and cannot be viewed by intermediate parties who attempt to intercept media.

IOS MTP and RSVP agents in pass through mode also support encrypted iX Channel.

Configuration

To enable an encrypted iX Channel on Unified Communications Manager, you must:

- Check the **Allow iX Application Media** check box in the SIP Profile Configuration that is used by any intermediate SIP trunks. This setting turns on the iX channel negotiation.
- Configure the **Secure Call Icon Display Policy** service parameter to enable a secure lock icon. By default, the setting is **All media except BFCP and iX transports must be encrypted**.

Encryption Modes

There are two types of Session Description Protocol (SDP) offers thatUnified Communications Manager supports for iX Channel encryption for encrypted phones. This encryption type is driven by what the endpoints support and is not a configurable item in the Unified Communications Manager.

- **Best Effort Encryption**—The SDP offer is for an encrypted iX Channel, but falls back to a non-encrypted iX Channel if the SIP peers do not support it. This approach can be used if encryption is not mandatory in the solution.

  For example, encryption is mandatory within the cloud, and not in a single enterprise.

  Best-Effort iX Encryption

  m=application 12345 **UDP/UDT/IX ***

  a=setup:actpass

  a=fingerprint: SHA-1 <key>

- **Forced Encryption**—The SDP offer is for an encrypted iX Channel only. This offer is rejected if the SIP peers do not support iX Channel encryption. This approach can be used in deployments where encryption is mandatory between endpoints.

  For example, encryption is mandatory between the two SIP devices.

  Forced iX Encryption

  m=application 12345 **UDP/DTLS/UDT/IX ***

  a=setup:actpass

  a=fingerprint: SHA-1 <key>

By default, all Cisco IP Phones are set to offer Best Effort iX Encryption. However, you can reset this to Forced Encryption by setting the **Encryption Mode** to **On** within the Product-Specific Configuration of Cisco TelePresence endpoints, or by reconfiguring settings on the Cisco Meeting Server.

Non-Encrypted Modes

Unified Communications Managerenables negotiation of secure active control messages in media path from endpoints in a meeting when the endpoint may not be deployed in a fully secure mode. For example, if the endpoint is Off-Net and is registered with Unified CM in Mobile and Remote Access mode.

Prerequisite

Before you start using this feature, make sure that:

- System adheres to the export compliance requirement
- SIP trunk to the conference bridge is secure

Unified CM can negotiate the DTLS information in secure active control messages for non-secure endpoints or softphones and receive messages in the following ways:

- **Best Effort Encryption iX** to On-Premise registered endpoints or softphones
- **Forced iX Encryption** to Off-Premise registered endpoints or softphones

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

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.

Related Topics

Activate Certificate Authority Proxy Function Service
Activate Cisco CTL Provider Service
Apply Security Profiles to Phone
Apply SIP Trunk Security Profile
Authorization, on page 24
Cisco CTL Client Installation
CTL Client, SSL, CAPF, and Security Token Installation, on page 15
Digest Authentication for SIP Phones Setup
Digest Authentication Setup for SIP Trunks
TFTP Encrypted Configuration Files Tips
Encrypted Phone Configuration File Setup
Encryption Setup for Gateways and Trunks
Enter Phone Authentication String
IPsec Setup Within Network Infrastructures
Phone Hardening
Phone Security Profile Setup Prerequisites
Reset Devices, Servers, Clusters, and Services, on page 14
Secure Conference Resources Setup
Secure Survivable Remote Site Telephony (SRST) Reference
Set Up CAPF
Cisco CTL Client Setup
Upgrade Cisco CTL Client and Migrate Cisco CTL File
Set Up Digest Authentication Enterprise Parameters
Phone Security Profile Setup
Set up Secure Ports
SIP Trunk Security Profile Setup
System Requirements, on page 5
Voice-Messaging Ports Security Setup

Cipher Management

Cipher management is an optional feature that enables you to control the set of security ciphers that is allowed for every TLS and SSH connection. Cipher management allows you to disable weaker ciphers and thus enable a minimum level of security.

The **Cipher Management** page has no default values. Instead, the Cipher Management feature takes effect only when you configure the allowed ciphers. Certain weak ciphers are never allowed, even if they are configured on the **Cipher Management** page.

You can configure ciphers on the following TLS and SSH interfaces:

- **All TLS**—The ciphers that are assigned in this field are applicable to all server and client connections that support the TLS protocol on Unified Communications Manager and IM and Presence Service.

- **HTTPS TLS**—The ciphers that are assigned in this field are applicable to all Cisco Tomcat connections on ports 443 and 8443 that support the TLS protocol on Unified Communications Manager and IM and Presence Service.

Note If you assign ciphers on **HTTPS TLS** and **All TLS** fields, the ciphers that are configured on **HTTPS TLS** override **All TLS** ciphers.

- **SIP TLS**—The ciphers that are assigned in this field are applicable to all encrypted connections to or from the SIP TLS interfaces that support the TLS protocol on Unified Communications Manager. It is not applicable for SCCP or CTI devices.

  SIP interface in authenticated mode only supports NULL-SHA ciphers.

  If you configure ciphers in the SIP interface or All interface, authenticated mode is no longer supported.

  If you assign ciphers in **SIP TLS** and **All TLS** fields, then the ciphers you configured on SIP TLS override the All TLS ciphers.

- **SSH Ciphers**—The ciphers that are assigned in this field are applicable to SSH connections on Unified Communications Manager and IM and Presence Service.
- **SSH Key Exchange**—The Key Exchange algorithms that are assigned in this field are applicable to the SSH interface on Unified Communications Manager and IM and Presence Service.

Curve Negotiation

Following are the points for negotiating the curves:

- ECDSA ciphers are negotiated with different EC curves based on the key size of the ECDSA certificate.
- The RSA ciphers are negotiated with all the EC curves irrespective of key size of the certificate.
- The key size of a ECDSA certificate must be same as the curve size for the TLS negotiation to happen.

Example:

The 384 key certificate and ECDSA ciphers are negotiated, when the client offers P-384 EC curve.

Curve negotiation is based on the client preference for both RSA and ECDSA ciphers.

When the certificate size is 384 bits and client offerings are P-521, P-384, P-256 EC curves then TLS negotiation happen with the P-521 curve. Since curve offered by the client is P-521 at the first and P- 384 curve is also available on the list. When the certificate size is 384 bits and client offerings are P-521, P-256 EC curves then TLS negotiation will not happen because the P-384 curve is not offered by the client.

The following are the supported ciphers for EC curves:

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
```

```
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
```

Recommended Ciphers

By default, Unified Communications Manager and IM and Presence Service already uses a set of ciphers (see TLS and SSH Ciphers section below) that supports secure integration with most other products, including third-party products. Therefore, it is usually not required to make changes. If Cipher suite mismatches are causing TLS Handshake failures, Unified Communications Manager Cipher Management can be used to add additional ciphers to the list of supported Ciphers.

Cipher Management can also be used if customers want to be more restrictive and prevent certain Cipher suites from being negotiated during TLS handshake. After configuring the ciphers, restart the affected services or reboot the server for the changes to take effect.

Warning Configuring hmac-sha2-512 in SSH MAC interface affects the DRS and CDR functionality.

Configuring ciphers aes128-gcm@openssh.com, aes256-gcm@openssh.com in "SSH Cipher's" field or configuring only ecdh-sha2-nistp256 algorithm in "SSH KEX" will break the DRS and CDR functionalities.

We support the following cipher strings for the TLS and SSH interface configuration:

TLS

```
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:
ECDHE-RSA-AES256-SHA:AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:
ECDHE-RSA-AES128-SHA:AES128-GCM-SHA256:AES128-SHA256:AES128-SHA
```

SSH Ciphers

```
aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,
aes256-gcm@openssh.com
```

SSH MAC

```
hmac-sha2-512,hmac-sha2-256,hmac-sha1
```

SSH KEX for FIPS

```
ecdh-sha2-nistp521, ecdh-sha2-nistp384, ecdh-sha2-nistp256,
diffie-hellman-group14-sha1, diffie-hellman-group16-sha512, diffie-hellman-group14-sha256
```

SSH KEX for Non-FIPS

```
ecdh-sha2-nistp521, ecdh-sha2-nistp384, ecdh-sha2-nistp256,
diffie-hellman-group14-sha1, diffie-hellman-group16-sha512, diffie-hellman-group14-sha256
```

Configure Cipher String

- Make sure you enter the cipher string in OpenSSL cipher string format in **All TLS**, **SIP TLS**, and **HTTPS TLS** fields.
- Make sure that you also enter the ciphers or algorithms in OpenSSH format in **SSH Ciphers**,algorithms in **SSH MAC**, and **SSH Key Exchange** fields.
- Review Recommended Ciphers, on page 38.

To configure the cipher string on different secure interfaces, see the Cipher Restrictions section.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Cipher Management**.
The Cipher Management page appears.

Step 2 To configure the cipher string in **All TLS**, **SIP TLS**, or **HTTPS TLS** field, enter the cipher string in OpenSSL cipher string format in the **Cipher String** field.

Step 3 If you don't configure the cipher string in the following fields:

- **All TLS or HTTPS TLS** field—the HTTPS TLS interface port (8443) takes configuration from the **Enterprise parameters** (HTTPS ciphers) page.
- **All TLS or SIP TLS** field—the SIP interface port (5061) takes configuration from the **Enterprise parameters** (TLS ciphers) page in encrypted mode and NULL-SHA ciphers in authenticated mode.

Note If you don't configure the cipher string in the **HTTPS TLS** or **SIP TLS** field, the system takes the configuration from the **All TLS** field by default.

For more information about OpenSSL cipher string format, see https://www.openssl.org/docs/man1.0.2/apps/ciphers.html.

Step 4 To configure the cipher string in the **SSH Ciphers** field, enter the cipher string in OpenSSH cipher string format in the **Cipher String** field.

For more information about OpenSSH cipher string format for SSH Ciphers, see https://www.ssh.com/manuals/server-admin/44/Ciphers_and_MACs.html.

If you don't configure any cipher string in the **SSH Ciphers** field, the following ciphers are applicable to all SSH connections by default:

In FIPS mode:

```
aes128-ctr, aes192-ctr, aes256-ctr,
aes128-gcm@openssh.com, aes256-gcm@openssh.com
```

In non-FIPS mode:

```
aes128-ctr, aes192-ctr, aes256-ctr,
aes128-gcm@openssh.com, aes256-gcm@openssh.com
```

Step 5 To configure the key exchange algorithm in the **SSH Key Exchange** field, enter the algorithm string in OpenSSH string format in the **Algorithm String** field.

For more information about OpenSSH algorithm string format for SSH Key Exchange, see the https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html.

If you don't configure any key exchange algorithm in the **SSH Key Exchange** field, the following key exchange algorithms are applicable to all SSH connections by default:

In FIPS mode:

```
diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,
diffie-hellman-group-exchange-sha1,diffie-hellman-group-exchange-sha256,
ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
```

In non-FIPS mode:

```
diffie-hellman-group1-sha1, diffie-hellman-group14-sha1,
diffie-hellman-group-exchange-sha1,diffie-hellman-group-exchange-sha256,
ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
```

Step 6 To configure MAC algorithm in the **SSH MAC** field, enter the algorithm string in OpenSSH string format in the **Algorithm String** field.

For more information about OpenSSH algorithm string format for SSH MAC, see https://www.ssh.com/manuals/server-admin/44/Ciphers_and_MACs.html.

If you don't configure any MAC algorithm in the **SSH MAC** field, the following MAC algorithms are applicable to all SSH connections by default:

In FIPS mode:

```
hmac-sha1
```

In non-FIPS mode:

```
hmac-sha1
```

Step 7 Click **Save**.

Note You can't edit **Cipher Expansion String** and **Algorithm Expansion String** fields.

The system validates the ciphers in the **All TLS**, **SIP TLS**, **HTTPS TLS** , and **SSH Ciphers** fields and auto populates ciphers in the **Cipher Expansion String** field.

If you enter invalid ciphers in the **Cipher String** field, the **Cipher Expansion String** field doesn't auto populate and the following error message appears:

```
You have entered an invalid Cipher String.
```

The system validates the algorithms in the **SSH Key Exchange** and **SSH MAC** fields, and auto populates the algorithms in the **Algorithm Expansion String** field.

If you enter invalid algorithms in the **Algorithm String** field, the **Algorithm Expansion String** field doesn't auto populate and the following error messge appears:

```
You have entered an invalid Algorithm String.
```

Note The ciphers or algorithms auto populated in **Cipher Expansion String** and **Algorithm Expansion String** fields are not the effective ciphers or algorithms. The system chooses the ciphers or algorithms from the **Cipher Expansion String** or **Algorithm Expansion String** field.

If you have configured ciphers in the corresponding fields, you have to either reboot or restart the respective services.

Table 8: Configured Ciphers and their corresponding Actions

Configured Cipher Fields	Action
All TLS	Reboot all nodes in the cluster for the cipher string to take effect.
HTTPS TLS	Restart the Cisco Tomcat service on all nodes for the cipher string to take effect.
SIP TLS	Restart Unified Communications Manager on all nodes for the cipher string to take effect.
SSH Ciphers	Reboot all nodes in the cluster for the cipher string to take effect.
SSH Key Exchange or **SSH MAC**	Reboot all nodes in the cluster for the algorithm string to take effect.

Note You can enable ciphers by entering them in the **Cipher String** fields of the **Cipher Management** page. If you don't enter them, all default ciphers supported by the application are enabled. However, you can also disable certain weak ciphers by not entering them in the **Cipher String** fields of the **Cipher Management** page.

Cipher Limitations

Although the **Cipher Management** configuration page allows you to configure any number of ciphers, each application has a list of ciphers it supports on its interfaces. For example, **All TLS** interfaces may show ECDHE or DHE or ECDSA-based ciphers, but an application such as Unified Communications Manager may not support these ciphers because EC curves or DHE algorithms are not enabled for this application's interfaces. For more information, see the "Application Ciphers Support" section below for a list of ciphers supported by individual application interfaces.

Note Cisco Cloud Onboarding is not part of the Cipher Management suite and will use all the default ciphers that are supported in the server. However, this limitation has been fixed from 12.5(1) SU6 release onwards.

Validation in GUI

The ciphers on **Cipher Management** page are validated according to the OpenSSL guidelines. For example, if a cipher configured is ALL:BAD:!MD5, the cipher string will be considered as valid even though "BAD" is not a recognized cipher suite. OpenSSL considers this as a valid string. If AES128_SHA is configured

instead of AES128-SHA (using an underscore instead of a hyphen) however, OpenSSL identifies this as an invalid cipher suite.

Authenticated Mode (NULL Ciphers)

If NULL ciphers are in use by an application interface, you can revoke the support for NULL ciphers by configuring any cipher list in **All TLS** or **SIP TLS** fields on **Cipher Management** page.

Examples of application interfaces that use NULL ciphers are:

- **All TLS Interface:** Unified Communications Manager SIP Proxy in IM and Presence through the **TLS Context Configuration** page.
- **SIP TLS Interface:** Unified Communications Manager through SIP or SCCP, when any **Device Security Profile** is set to **Authenticated** mode.

Don't configure ciphers for either of these two interfaces if NULL ciphers must be used.

Override Functionality

The settings on the **Cipher Management** page overrides the default settings for each application and any other location where ciphers have been configured. This means that if no ciphers are configured on the **Cipher Management** page, then the original functionality on all interfaces will be retained.

For example, if the **Enterprise Parameter** "**TLS Ciphers**" is configured with "*ALL Supported Ciphers*" and the **Cipher Management** page is configured with ciphers "*AES256-GCM-SHA384:AES256-SHA256*" on **All TLS** interfaces, all application SIP interfaces will support only the "*AES256-GCM-SHA384:AES256-SHA256*" ciphers and ignores the **Enterprise Parameter** value.

Application Ciphers Support

The following table lists the application interfaces and the all corresponding ciphers and algorithms that are supported on TLS and SSH interfaces.

Table 9: Unified Communications Manager Cipher Support for TLS Ciphers

Application / Process	Protocol	Port	Supported Ciphers
Cisco CallManager	TCP / TLS	2443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: AES256-GCM-SHA384: AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256: AES128-SHA256:AES128-SHA: CAMELLIA128-SHA

Application / Process	Protocol	Port	Supported Ciphers
DRS	TCP / TLS	4040	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-CAMELLIA128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA
Cisco Tomcat	TCP / TLS	8443 / 443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: DHE-RSA-AES256-GCM-SHA384: DHE-RSA-AES256-SHA256: DHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-AES128-GCM-SHA256: DHE-RSA-AES128-SHA256: DHE-RSA-AES128-SHA: DHE-RSA-CAMELLIA128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: EDH-RSA-DES-CBC3-SHA: DES-CBC3-SHA ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-ECDSA-DES-CBC3-SHA
Cisco CallManager	TCP / TLS	5061	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-RSA-AES256-SHA ECDHE-ECDSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256 ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-ECDSA-DES-CBC3-SHA

Application / Process	Protocol	Port	Supported Ciphers
Cisco CTL Provider	TCP / TLS	2444	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA:
Cisco Certificate Authority Proxy Function	TCP / TLS	3804	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA:
CTIManager	TCP / TLS	2749	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA
Cisco Trust Verification Service	TCP / TLS	2445	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA
Cisco Intercluster Lookup Service	TCP / TLS	7501	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA:AES256-GCM-SHA384: AES256-SHA256:AES256-SHA: CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA:
Secure Configuration download (HAPROXY)	TCP / TLS	6971, 6972	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-CAMELLIA128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-ECDSA-DES-CBC3-SHA:

Application / Process	Protocol	Port	Supported Ciphers
Authenticated Contact Search	TCP / TLS	9443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-CAMELLIA128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-ECDSA-DES-CBC3-SHA:

Table 10: Unified Communications Manager IM & Presence Cipher Support for TLS Ciphers

Application / Process	Protocol	Port	Supported Ciphers
Cisco SIP Proxy	TCP / TLS	5061	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: ECDHE-ECDSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256: AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: DES-CBC3-SHA

Application / Process	Protocol	Port	Supported Ciphers
Cisco SIP Proxy	TCP / TLS	5062	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: ECDHE-ECDSA-AES256-SHA: AES256-GCM-SHA384: AES256-SHA256:AES256-SHA: CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: DES-CBC3-SHA
Cisco SIP Proxy	TCP / TLS	8083	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: ECDHE-ECDSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: DES-CBC3-SHA

Application / Process	Protocol	Port	Supported Ciphers
Cisco Tomcat	TCP / TLS	8443, 443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: DHE-RSA-AES256-GCM-SHA384: DHE-RSA-AES256-SHA256: DHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-AES128-GCM-SHA256: DHE-RSA-AES128-SHA256: DHE-RSA-AES128-SHA: DHE-RSA-CAMELLIA128-SHA: AES128-GCM-SHA256: AES128-SHA256:AES128-SHA: CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: EDH-RSA-DES-CBC3-SHA: DES-CBC3-SHA ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-ECDSA-DES-CBC3-SHA
Cisco XCP XMPP Federation Connection Manager	TCP /TLS	5269	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: ECDHE-ECDSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: DES-CBC3-SHA

Application / Process	Protocol	Port	Supported Ciphers
Cisco XCP Client Connection Manager	TCP / TLS	5222	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: ECDHE-ECDSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: DES-CBC3-SHA

Table 11: Cipher Support for SSH Ciphers

Service	Ciphers/Algorithms
SSH Server	• Ciphers aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com • MAC algorithms: hmac-sha2-256 hmac-sha1 • Kex algorithms: ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1

Service	Ciphers/Algorithms

SSH Client	• Ciphers:
	`aes128-ctr`
	`aes192-ctr`
	`aes256-ctr`
	`aes128-gcm@openssh.com`
	`aes256-gcm@openssh.com`
	• MAC algorithms:
	`hmac-sha2-256`
	`hmac-sha1`
	• Kex algorithms:
	`ecdh-sha2-nistp521`
	`ecdh-sha2-nistp384`
	`ecdh-sha2-nistp256`
	`diffie-hellman-group14-sha1`
	`diffie-hellman-group1-sha1`
	`diffie-hellman-group-exchange-sha256`
	`diffie-hellman-group-exchange-sha1`

DRS Client	• Ciphers:
	`aes256-ctr`
	`aes256-cbc`
	`aes128-ctr`
	`aes128-cbc`
	`3des-cbc`
	`blowfish-cbc`
	• MAC algorithms:
	`hmac-md5`
	`hmac-sha2-256`
	`hmac-sha1`
	`hmac-sha1-96`
	`hmac-md5-96`
	• Kex algorithms:
	`diffie-hellman-group1-sha1`
	`diffie-hellman-group14-sha1`
	`diffie-hellman-group-exchange-sha1`

Service	Ciphers/Algorithms

SFTP client	• Ciphers:
	`aes128-ctr`
	`aes192-ctr`
	`aes256-ctr`
	• MAC algorithms:
	`hmac-sha2-256`
	`hmac-sha1`
	• Kex algorithms:
	`ecdh-sha2-nistp521`
	`ecdh-sha2-nistp384`
	`diffie-hellman-group14-sha1`
	`diffie-hellman-group1-sha1`
	`diffie-hellman-group-exchange-sha256`
	`diffie-hellman-group-exchange-sha1`

End Users (Linux OS)	`SHA-256 - Hashing (salted)`
DRS Backups / RTMT SFTPs	`AES-128 - Encryption`
Application Users	`AES-256 - Encryption`

Cipher Restrictions

The **Cipher Management** page allows configuration of ciphers supported by OpenSSL or OpenSSH. However, some of the ciphers are disabled internally based on Cisco's security standards to avoid accidental exposure of critical data.

When you configure ciphers on the **Cipher Management** page, the following ciphers are essentially disabled.

TLS Disabled Ciphers

```
EDH-RSA-DES-CBC-SHA:EDH-DSS-DES-CBC-SHA:ADH-DES-CBC-SHA:
DES-CBC-SHA:KRB5-DES-CBC-SHA:KRB5-DES-CBC-MD5:EXP-EDH-RSA-DES-CBC-SHA:
EXP-EDH-DSS-DES-CBC-SHA:EXP-ADH-DES-CBC-SHA:EXP-DES-CBC-SHA:EXP-RC2-CBC-MD5:
EXP-KRB5-RC2-CBC-SHA:EXP-KRB5-DES-CBC-SHA:EXP-KRB5-RC2-CBC-MD5:EXP-KRB5-DES-CBC-MD5:
EXP-ADH-RC4-MD5:EXP-RC4-MD5:EXP-KRB5-RC4-SHA:EXP-KRB5-RC4-MD5:ADH-AES256-GCM-SHA384:
ADH-AES256-SHA256:ADH-AES256-SHA:ADH-CAMELLIA256-SHA:ADH-AES128-GCM-SHA256:ADH-AES128-SHA256:
ADH-AES128-SHA:ADH-SEED-SHA:ADH-CAMELLIA128-SHA:ADH-DES-CBC3-SHA:ADH-RC4-MD5:
AECDH-AES256-SHA:AECDH-AES128-SHA:AECDH-DES-CBC3-SHA:AECDH-RC4-SHA:AECDH-NULL-SHA:
DES-CBC3-MD5:IDEA-CBC-MD5:RC2-CBC-MD5:RC4-MD5:ECDHE-RSA-RC4-SHA:ECDHE-ECDSA-RC4-SHA:
ECDH-RSA-RC4-SHA:ECDH-ECDSA-RC4-SHA:RC4-SHA:RC4-MD5:PSK-RC4-SHA:KRB5-RC4-SHA:
KRB5-RC4-MD5:IDEA-CBC-SHA:KRB5-IDEA-CBC-SHA:KRB5-IDEA-CBC-MD5:DHE-RSA-SEED-SHA:
DHE-DSS-SEED-SHA:SEED-SHA:KRB5-DES-CBC3-MD5:NULL-MD5:PSK-AES256-CBC-SHA:
PSK-AES128-CBC-SHA:PSK-3DES-EDE-CBC-SHA:ECDHE-RSA-NULL-SHA:ECDHE-ECDSA-NULL-SHA:
ECDH-RSA-NULL-SHA:ECDH-ECDSA-NULL-SHA:NULL-SHA256:NULL-SHA
```

SSH Disabled Ciphers

```
3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se
```

SSH Disabled KEX Algorithms

```
curve25519-sha256@libssh.org,gss-gex-sha1-,gss-group1-sha1-,gss-group14-sha1-
```

SSH Disabled MAC Algorithms

```
hmac-sha1-etm@openssh.com,hmac-sha2-256-etm@openssh.com
```

Where to Find More Information

Related Cisco Documentation

Refer to the following documents for further information about related CiscoIP telephony applications and products:

- *System Configuration Guide for Cisco Unified Communications Manager*
- *Administration Guide for Cisco Unified Communications Manager*
- *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*
- *Cisco Unified Communications Manager Integration Guide for Cisco Unity*
- *Cisco Unified Communications Manager Integration Guide for Cisco Unity Connection*
- *Cisco Unified Survivable Remote Site Telephony (SRST) Administration Guide* that supports the SRST-enabled gateway.
- *Administration Guide for Cisco Unified Communications Manager*
- *Cisco Unified Communications Manager Bulk Administration Guide*
- *Troubleshooting Guide for Cisco Unified Communications Manager*
- *Cisco IP Phone Administration Guide* that support your phone model