CUCM 11.0 Next Generation Encryption - Elliptic Curve Cryptography

Contents

Introduction

This document describes the configuration of Next Generation Encryption (NGE) from Cisco Unified Communications Manager (CUCM) 11.0 and later to meet the enhanced security and performance requirements.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco CallManager security basics
- Cisco CallManager certificate management

Components Used

The information in this document is based on Cisco CUCM 11.0, where Elliptic Curve Digital Signature Algorithm (ECDSA) certificates are only supported for CallManager (CallManager-ECDSA).

> **Note**: CUCM 11.5 and later supports tomcat-ECDSA certificates as well.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Related Products

This document can also be used with these software products and versions that support ECDSA certificates:

- Cisco Unified CM IM and Presence 11.5
- Cisco Unity Connection 11.5

Background Information

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography is the same level of security provided by keys of smaller size.

Common Criteria (CC) provides assurance that security features operate correctly within the solution being evaluated. This is achieved through testing and meeting extensive documentation requirements.

It is accepted and supported by 26 countries worldwide via Common Criteria Recognition Arrangement (CCRA).

Cisco Unified Communications Manager Release 11.0 supports Elliptic Curve Digital Signature Algorithm (ECDSA) certificates.

These certificates are stronger than the RSA-based certificates and are required for products that have CC certifications. The US government Commercial Solutions for Classified Systems (CSfC) program requires the CC certification and so, it is included in Cisco Unified Communications Manager Release 11.0 and later.

The ECDSA certificates are available along with the existing RSA certificates in these areas:

- Certificate Management
- Certificate Authority Proxy Function (CAPF)
- Transport Layer Security (TLS) Tracing
- Secure Session Initiation Protocol (SIP) Connections
- Computer Telephony Integration (CTI) Manager
- HTTP
- Entropy

The next sections provide more detailed information on each of these seven areas.

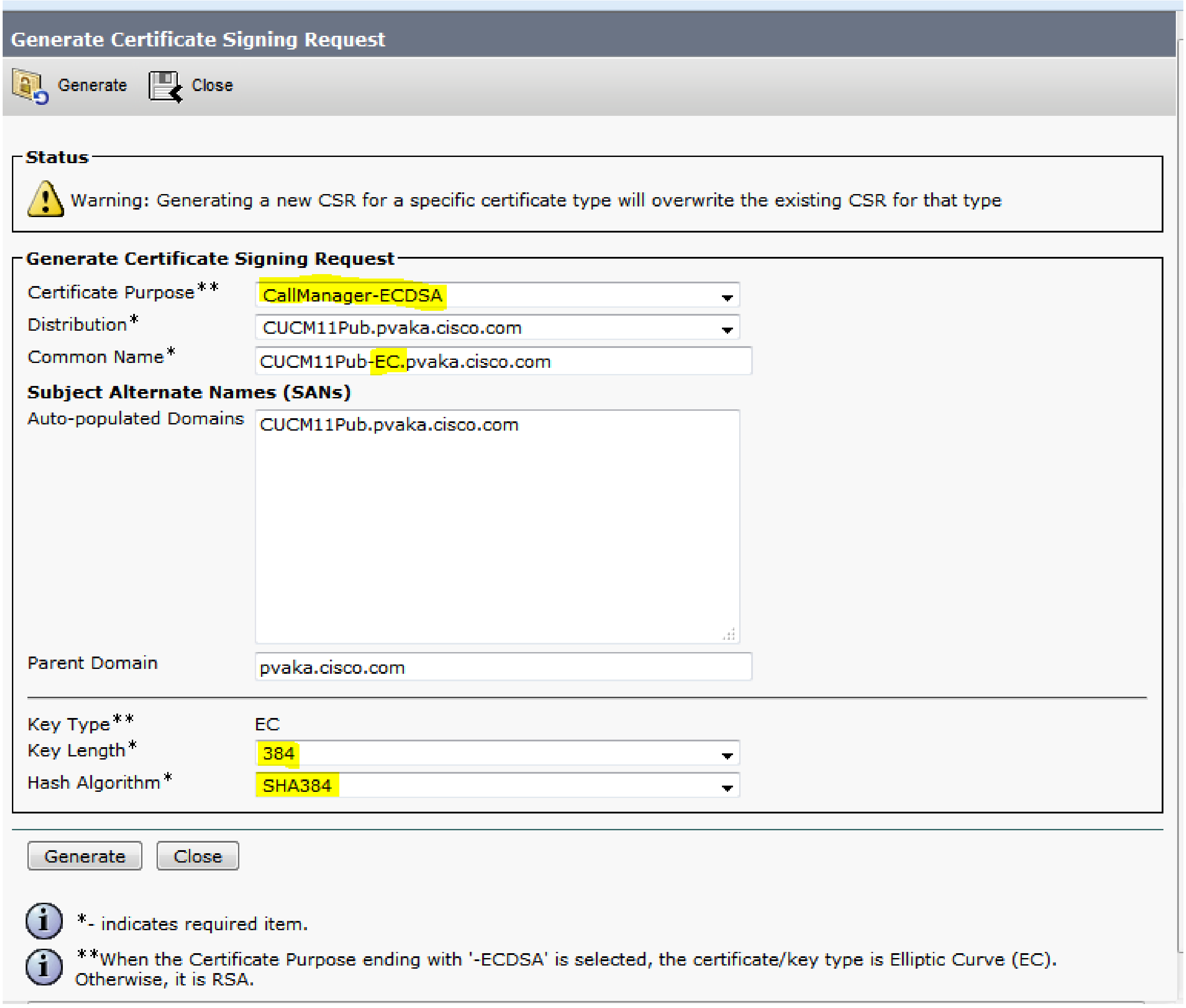
Certificate Management

Generate Certificates with Elliptical Curve Encryption

Support for ECC from CUCM 11.0 and later to generate CallManager certificate with Elliptical

Curve (EC) encryption:

- The new option **CallManager-ECDSA** is available as shown in the image.
- It requires the host portion of the common name to end in **–EC**. This prevents having the same common name as the **CallManager** certificate.
- In case of Multi Server SAN certificate, this must end in **–EC-ms**.



Generate Certificate Signing Request

Status

Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose** CallManager-ECDSA

Distribution* CUCM11Pub.pvaka.cisco.com

Common Name* CUCM11Pub-EC.pvaka.cisco.com

Subject Alternate Names (SANs)

Auto-populated Domains CUCM11Pub.pvaka.cisco.com

Parent Domain pvaka.cisco.com

Key Type** EC

Key Length* 384

Hash Algorithm* SHA384

*- indicates required item.

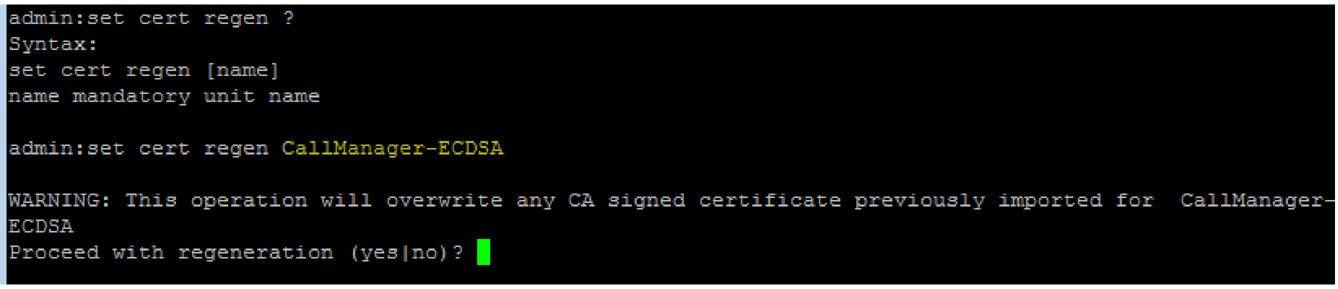
**When the Certificate Purpose ending with '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it is RSA.

- Both the self-signed certificate request and the CSR request limit the hash algorithm choices depending on the EC key size.
- For an EC 256 key size the hash algorithm can be SHA256, SHA384, or SHA512. For an EC 384 key size the hash algorithm can be SHA384 or SHA512. For an EC 521 key size the only option is SHA512.
- The default key size is 384 and default hashing algorithm is SHA384, which can be changed. The options available are based on the chosen key size.

CLI Configuration

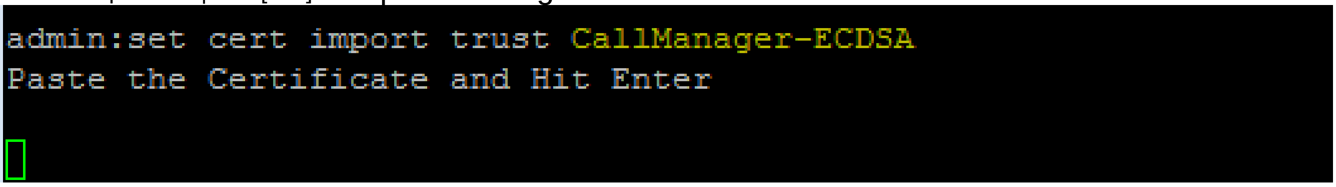
A new certificate unit named **CallManager-ECDSA** has been added for the CLI commands

- set cert regen [unit] – regenerates self-signed certificate



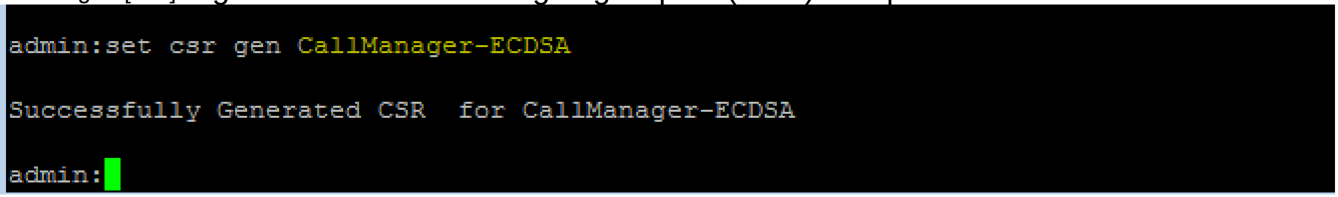
```
admin:set cert regen ?
Syntax:
set cert regen [name]
name mandatory unit name

admin:set cert regen CallManager-ECDSA

WARNING: This operation will overwrite any CA signed certificate previously imported for  CallManager-
ECDSA
Proceed with regeneration (yes|no)?
```

- set cert import own|trust [unit] – imports CA signed certificate



```
admin:set cert import trust CallManager-ECDSA
Paste the Certificate and Hit Enter
```

- set csr gen [unit] – generates certificate signing request(CSR) for specified unit

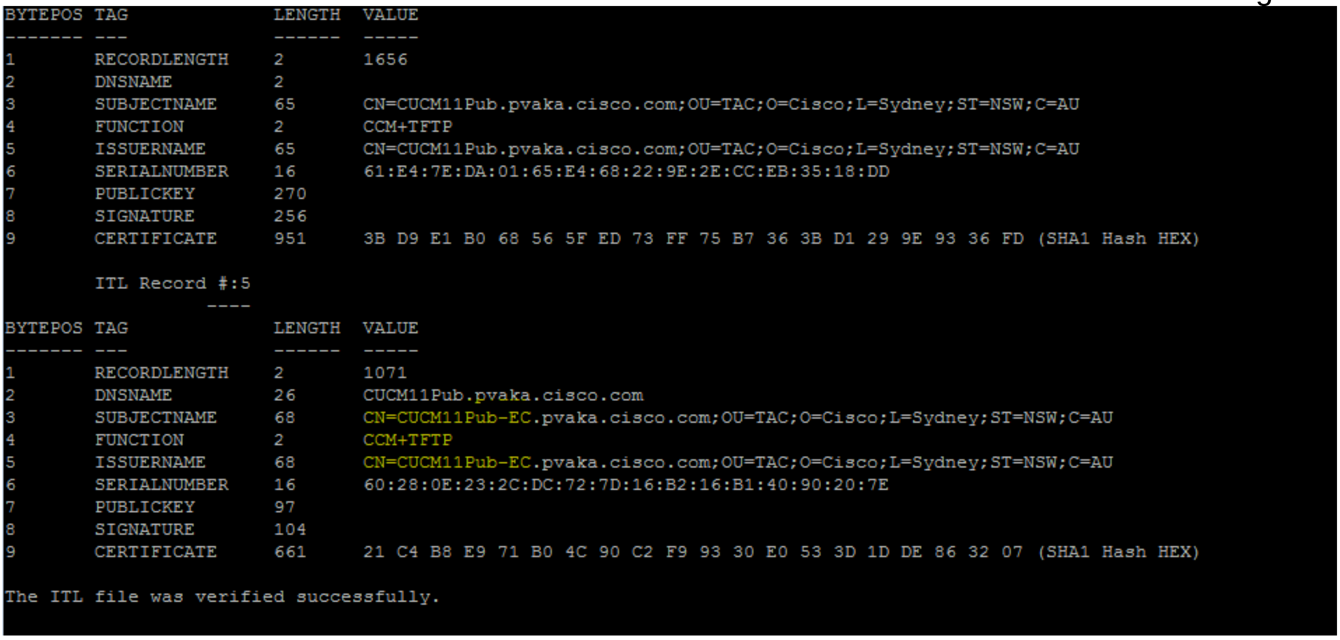


```
admin:set csr gen CallManager-ECDSA

Successfully Generated CSR  for CallManager-ECDSA

admin:
```

- set bulk export|consolidate|import tftp – When tftp is the unit name, CallManager-ECDSA certificates get auto-included with CallManager RSA certificates in bulk operations.

CTL and ITL Files

- Both Certificate Trust List (CTL) and Identify Trust List (ITL) files have **CallManager-ECDSA** present.
- The CallManager-ECDSA certificate have the Function of CCM+TFTP in both the ITL and CTL file.
- You can use the **show ctl** or **show itl** command to view this information as shown in this image:



```
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1656
2       DNSNAME         2
3       SUBJECTNAME     65      CN=CUCM11Pub.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
4       FUNCTION        2       CCM+TFTP
5       ISSUERNAME      65      CN=CUCM11Pub.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
6       SERIALNUMBER    16      61:E4:7E:DA:01:65:E4:68:22:9E:2E:CC:EB:35:18:DD
7       PUBLICKEY       270
8       SIGNATURE       256
9       CERTIFICATE     951     3B D9 E1 B0 68 56 5F ED 73 FF 75 B7 36 3B D1 29 9E 93 36 FD (SHA1 Hash HEX)

        ITL Record #:5
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1071
2       DNSNAME         26      CUCM11Pub.pvaka.cisco.com
3       SUBJECTNAME     68      CN=CUCM11Pub-EC.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
4       FUNCTION        2       CCM+TFTP
5       ISSUERNAME      68      CN=CUCM11Pub-EC.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
6       SERIALNUMBER    16      60:28:0E:23:2C:DC:72:7D:16:B2:16:B1:40:90:20:7E
7       PUBLICKEY       97
8       SIGNATURE       104
9       CERTIFICATE     661     21 C4 B8 E9 71 B0 4C 90 C2 F9 93 30 E0 53 3D 1D DE 86 32 07 (SHA1 Hash HEX)

The ITL file was verified successfully.
```

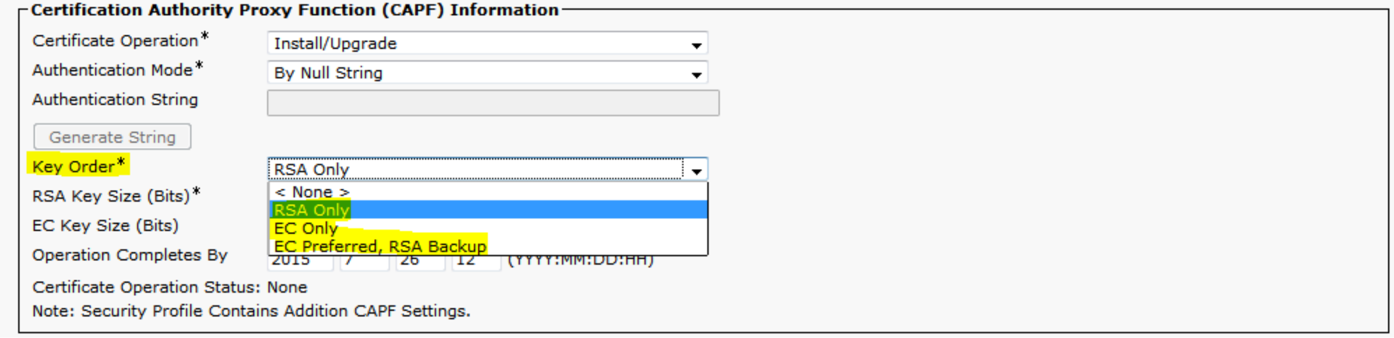
- You can use the **utils ctl update** command to generate the CTL file.

Certificate Authority Proxy Function

- The Certificate Authority Proxy Function (CAPF) Version 3.0 in CUCM 11 provides support for

EC Key Sizes along with RSA.

- The additional CAPF options provided in addition to the existing CAPF fields are Key Order and EC Key Size (bits).
- The existing Key Size (bits) option has been changed to RSA Key Size (bits).
- The Key Order provides support for RSA Only, EC Only and EC Preferred, RSA backup options.
- The EC Key Size provides support for key sizes of 256, 384, and 521 bits.
- The RSA Key Size provides support for 512, 1024, and 2048 bits.
- When Key Order of RSA Only is selected, only RSA Key Size can be selected. When EC only is selected, only EC Key Size can be selected. When EC Preferred, RSA backup is selected, both RSA and EC Key Size can be selected.

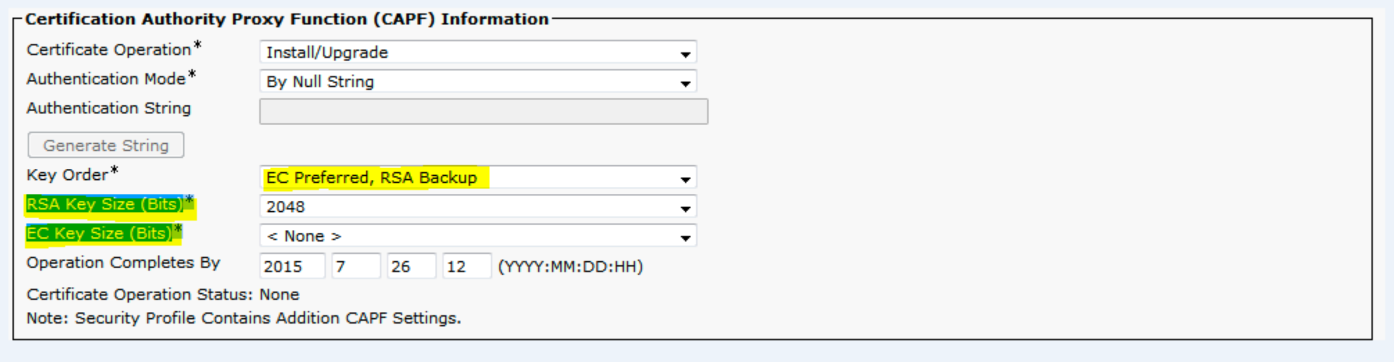


Certification Authority Proxy Function (CAPF) Information

Certificate Operation*	Install/Upgrade
Authentication Mode*	By Null String
Authentication String	
Generate String	
Key Order*	RSA Only
RSA Key Size (Bits)*	< None > RSA Only EC Only EC Preferred, RSA Backup
EC Key Size (Bits)	
Operation Completes By	2015 7 26 12 (YYYY:MM:DD:HH)

Certificate Operation Status: None

Note: Security Profile Contains Addition CAPF Settings.



Certification Authority Proxy Function (CAPF) Information

Certificate Operation*	Install/Upgrade
Authentication Mode*	By Null String
Authentication String	
Generate String	
Key Order*	EC Preferred, RSA Backup
RSA Key Size (Bits)*	2048
EC Key Size (Bits)*	< None >
Operation Completes By	2015 7 26 12 (YYYY:MM:DD:HH)

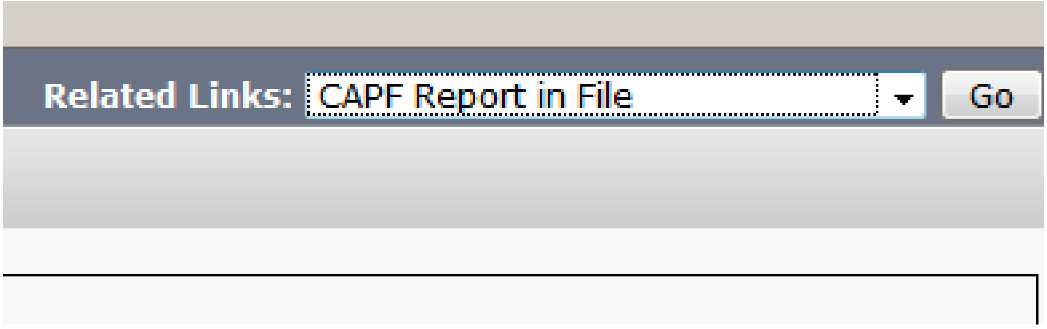
Certificate Operation Status: None

Note: Security Profile Contains Addition CAPF Settings.

Note: Currently no Cisco endpoint supports CAPF Version 3, so do not select the EC Only option. However, administrators who want to support ECDSA Locally Significant Certificates (LSCs) later can configure their devices with the EC Preferred RSA Backup option. When the endpoints begin to support CAPF Version 3 for ECDSA LSCs, the administrators need to reinstall their LSC.

Additional CAPF options for Phone, Phone Security Profile, End User, and Application User Pages are shown here:

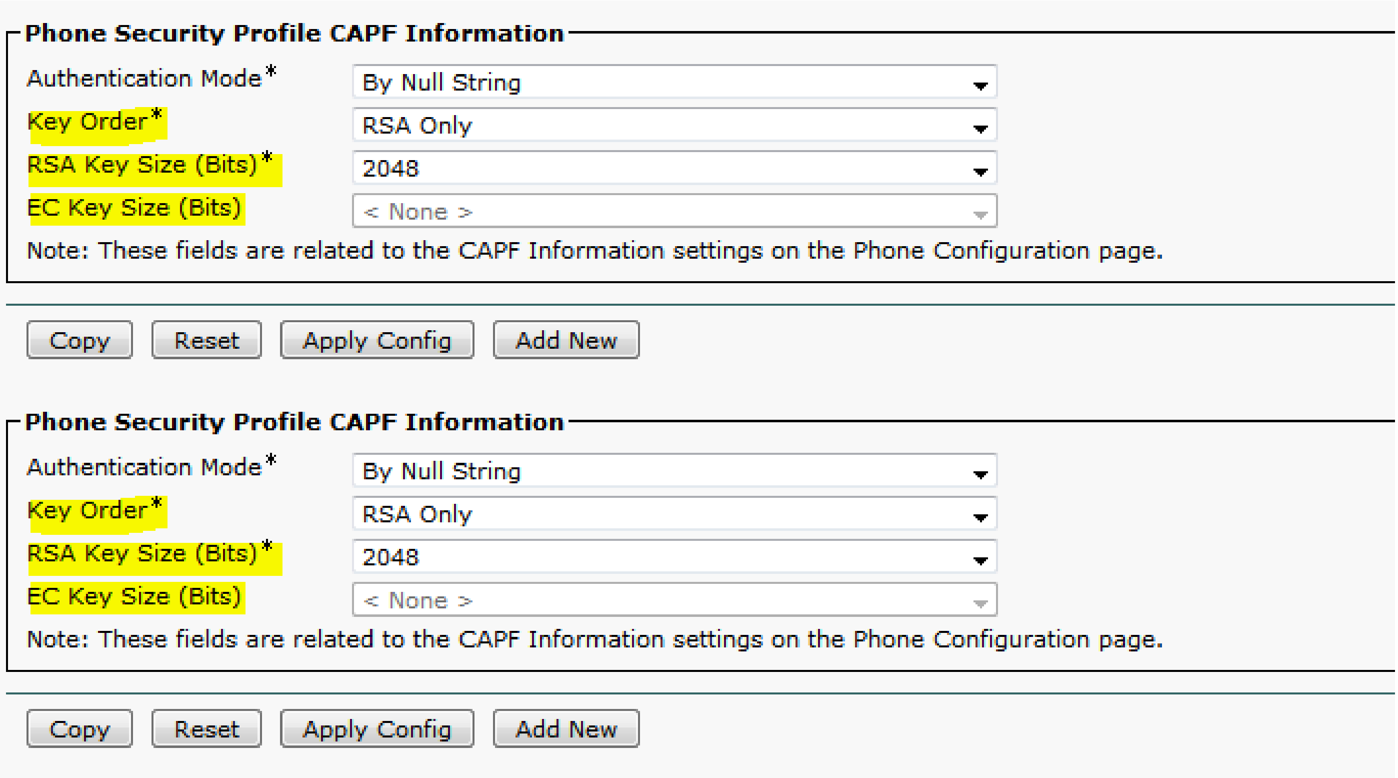
Device > Phone > Related Links



Related Links: CAPF Report in File

Navigate to **System > Security > Phone security profile**

User Management > User Settings > Application User CAPF Profile



Phone Security Profile CAPF Information

Authentication Mode*	By Null String
Key Order*	RSA Only
RSA Key Size (Bits)*	2048
EC Key Size (Bits)	< None >

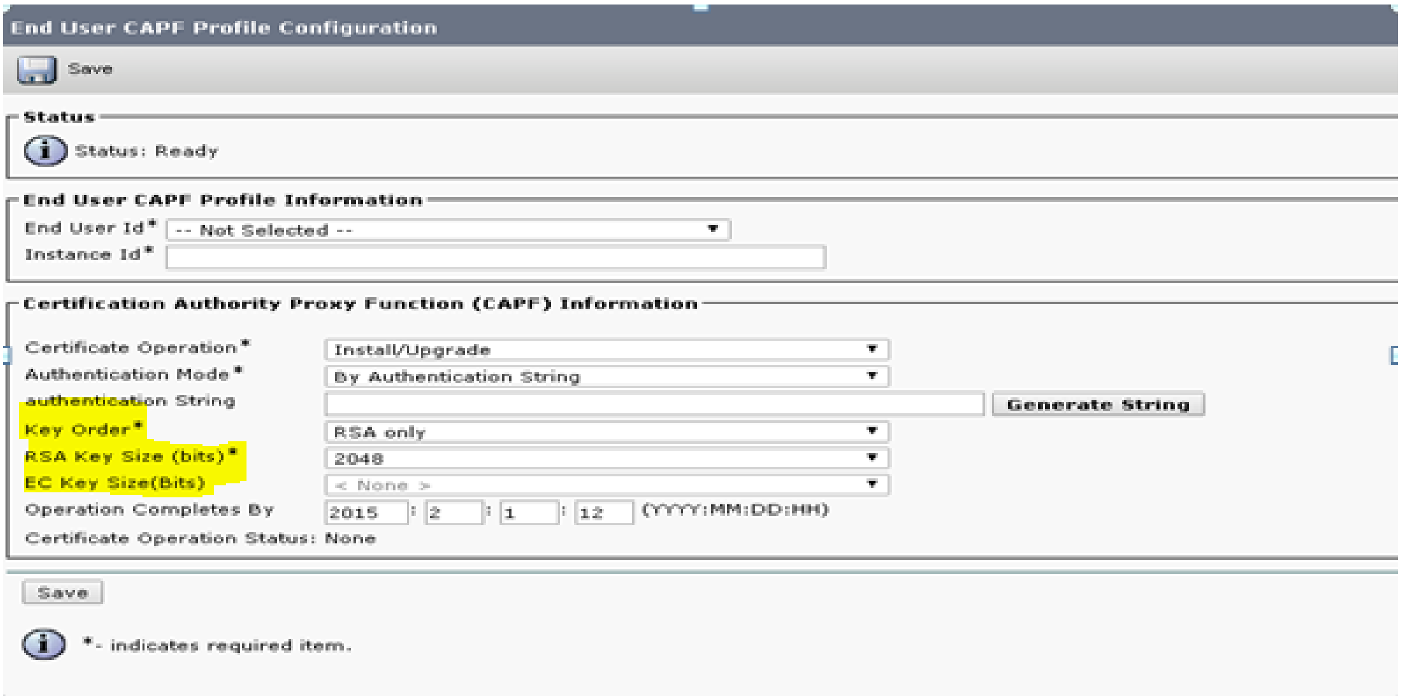
Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Phone Security Profile CAPF Information

Authentication Mode*	By Null String
Key Order*	RSA Only
RSA Key Size (Bits)*	2048
EC Key Size (Bits)	< None >

Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Navigate to **User Management > User Settings > End User CAPF Profile.**



End User CAPF Profile Configuration

Status

Status: Ready

End User CAPF Profile Information

End User Id*	-- Not Selected --
Instance Id*	

Certification Authority Proxy Function (CAPF) Information

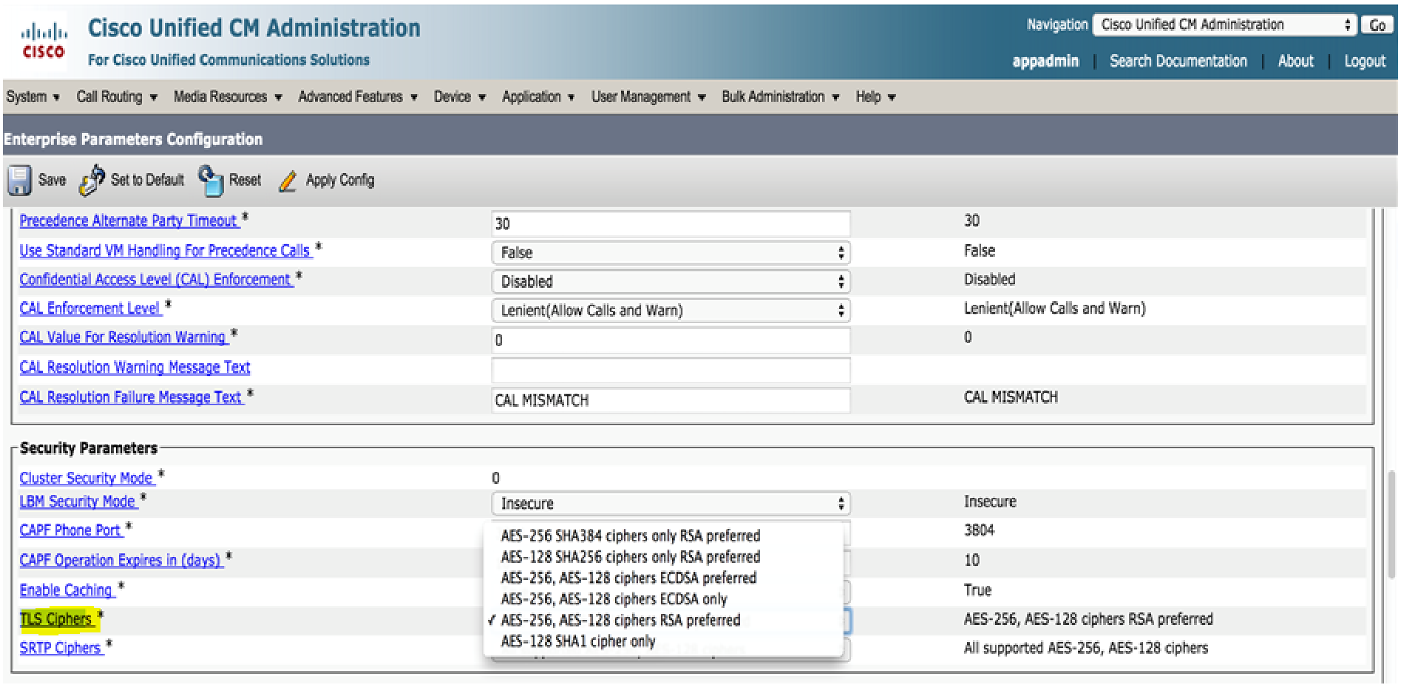
Certificate Operation*	Install/Upgrade
Authentication Mode*	By Authentication String
authentication String	
Key Order*	RSA only
RSA Key Size (bits)*	2048
EC Key Size(Bits)	< None >
Operation Completes By	2015 : 2 : 1 : 12 (YYYY:MM:DD:HH)

Certificate Operation Status: None

*- indicates required item.

TLS Ciphers Enterprise Parameters

- The Enterprise Parameter TLS Ciphers has been updated to support ECDSA Ciphers.
- The Enterprise Parameter TLS Ciphers now sets the TLS Ciphers for SIP Line, SIP Trunk, and Secure CTI Manager.


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation
Cisco Unified CM Administration
Go
appadmin
Search Documentation
About
Logout
System
Call Routing
Media Resources
Advanced Features
Device
Application
User Management
Bulk Administration
Help
Save
Set to Default
Reset
Apply Config
AES-256 SHA384 ciphers only RSA preferred
AES-128 SHA256 ciphers only RSA preferred
AES-256, AES-128 ciphers ECDSA preferred
AES-256, AES-128 ciphers ECDSA only
✓ AES-256, AES-128 ciphers RSA preferred
AES-128 SHA1 cipher only

Enterprise Parameters Configuration

Precedence Alternate Party Timeout *	30	30
Use Standard VM Handling For Precedence Calls *	False	False
Confidential Access Level (CAL) Enforcement *	Disabled	Disabled
CAL Enforcement Level *	Lenient(Allow Calls and Warn)	Lenient(Allow Calls and Warn)
CAL Value For Resolution Warning *	0	0
CAL Resolution Warning Message Text		
CAL Resolution Failure Message Text *	CAL MISMATCH	CAL MISMATCH

Security Parameters

Cluster Security Mode *	0	
LBM Security Mode *	Insecure	Insecure
CAPF Phone Port *		3804
CAPF Operation Expires in (days) *		10
Enable Caching *		True
TLS Ciphers *	AES-256, AES-128 ciphers RSA preferred	AES-256, AES-128 ciphers RSA preferred
SRTP Ciphers *		All supported AES-256, AES-128 ciphers

SIP ECDSA Support

- Cisco Unified Communications Manager Release 11.0 includes ECDSA support for SIP lines and SIP trunk interfaces.
- The connection between Cisco Unified Communications Manager and an endpoint phone or video device is a SIP line connection whereas the connection between two Cisco Unified Communications Managers is a SIP trunk connection.
- All SIP connections support the ECDSA ciphers and use ECDSA certificates.

The Secure SIP interface was updated to support these two ciphers:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

These are the scenarios when SIP makes TLS connections:

- When SIP acts as a TLS server When the SIP trunk interface of Cisco Unified Communications Manager acts as a TLS server for incoming secure SIP connection, the SIP trunk interface determines if the CallManager-ECDSA certificate exists on disk. If the certificate exists on the disk, the SIP trunk interface uses the CallManager-ECDSA certificate if the selected cipher suite isTLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 or TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- When SIP acts as a TLS client When the SIP trunk interface acts as a TLS client, the SIP trunk interface sends a list of requested cipher suites to the server based on the TLS Ciphers field (which also includes the ECDSA ciphers option) in the CUCM Enterprise Parameters **The TLS Ciphers**. This configuration determines the TLS client cipher suite list and the supported cipher suites in order of preference.

  Notes:
  - Devices that use an ECDSA cipher to make a connection to CUCM must have the CallManager-ECDSA certificate in their Identity Trust List (ITL) file.
  - The SIP trunk interface support RSA TLS cipher suites for connections from clients that do not support ECDSA cipher suites or when a TLS connection is established with an earlier

version of CUCM, that do not support ECDSA.

Secure CTI Manager ECDSA Support

The Secure CTI Manager interface was updated to support these four ciphers:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

The Secure CTI Manager interface loads both the CallManager and CallManager-ECDSA certificate. This allows the Secure CTI Manager interface to support the new ciphers along with the existing RSA cipher.

Similar to the SIP interface, the Enterprise Parameter TLS Ciphers option in Cisco Unified Communications Manager is used to configure the TLS ciphers that are supported on the CTI Manager secure interface.

HTTPS Support for Configuration Download

- For secure configuration download (for example, Jabber clients), Cisco Unified Communications Manager Release 11.0 is enhanced to support HTTPS in addition to the HTTP and TFTP interfaces that were used in the earlier releases.
- If required, both client and server use mutual authentication. However, the clients that are enrolled with ECDSA LSCs and Encrypted TFTP configurations are required to present their LSC.
- The HTTPS interface uses both the CallManager and the CallManager-ECDSA certificates as the server certificates.

Notes:
- When you update CallManager, CallManager ECDSA, or Tomcat certificates, you must deactivate and reactivate the TFTP service.
- Port 6971 is used for authentication of the CallManager and CallManager-ECDSA certificates, used by Phones.
- Port 6972 is used for the authentication of the Tomcat certificates, used by Jabber.

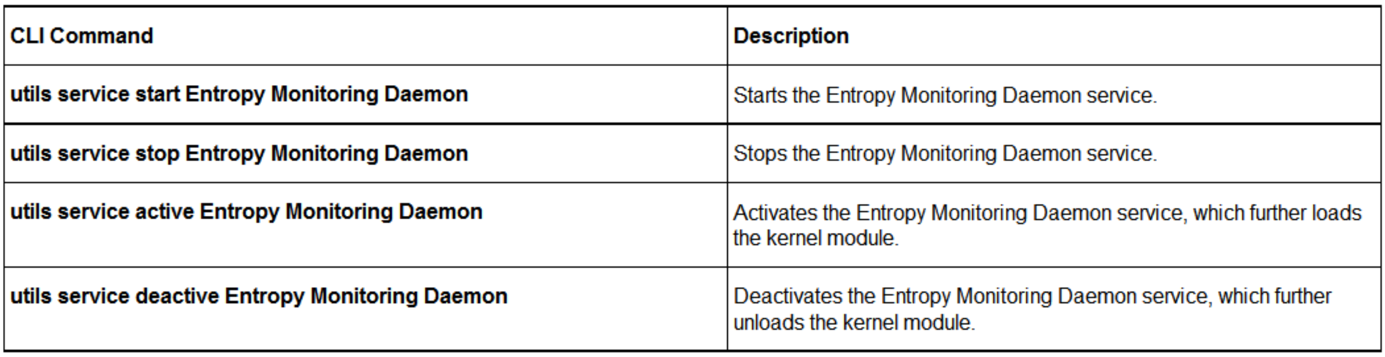
Entropy

Entropy is a measure of randomness of data and helps in determining the minimum threshold for common criteria requirements. To have strong encryption, a robust source of entropy is required. If a strong encryption algorithm, such as ECDSA, uses a weak source of entropy, the encryption can be easily broken.

In Cisco Unified Communications Manager Release 11.0, the entropy source for Cisco Unified Communications Manager is improved.

Entropy Monitoring Daemon is a built-in feature that does not require configuration. However, you can turn it off through the Cisco Unified Communications Manager CLI.

Use these CLI commands in order to control the Entropy Monitoring Daemon service:



CLI Command	Description
utils service start Entropy Monitoring Daemon	Starts the Entropy Monitoring Daemon service.
utils service stop Entropy Monitoring Daemon	Stops the Entropy Monitoring Daemon service.
utils service active Entropy Monitoring Daemon	Activates the Entropy Monitoring Daemon service, which further loads the kernel module.
utils service deactive Entropy Monitoring Daemon	Deactivates the Entropy Monitoring Daemon service, which further unloads the kernel module.

Related Information

- **Security Guide for Cisco Unified Communications Manager, Release 11.5(1)**
- **Technical Support & Documentation - Cisco Systems**