Verschlüsselung der nächsten Generation mit CUCM 11.0 - elliptische Kurven-Kryptografie

Inhalt

Einführung

In diesem Dokument wird die Konfiguration von NGE (Next Generation Encryption) aus Cisco Unified Communications Manager (CUCM) 11.0 und höher beschrieben, um die erweiterten Sicherheits- und Leistungsanforderungen zu erfüllen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Sicherheitsgrundlagen für Cisco CallManager
- Zertifikatsverwaltung von Cisco CallManager

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco CUCM 11.0, wobei ECDSA-Zertifikate (Elliptic Curve Digital Signature Algorithm) nur für CallManager (CallManager-ECDSA) unterstützt werden.

> **Hinweis**: CUCM 11.5 und höher unterstützt auch ECDSA-Zertifikate.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Dieses Dokument kann auch mit folgenden Softwareprodukten und Versionen verwendet werden, die ECDSA-Zertifikate unterstützen:

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

Hintergrundinformationen

Elliptic Curve Kryptography (ECC) ist ein Ansatz für Public-Key-Verschlüsselung, der auf der algebraischen Struktur elliptischer Kurven über endliche Felder basiert. Einer der Hauptvorteile im Vergleich zur Nicht-ECC-Verschlüsselung ist die gleiche Sicherheitsstufe, die auch Schlüssel mit geringerer Größe bieten.

Common Criteria (CC) garantiert, dass die Sicherheitsfunktionen innerhalb der zu evaluierenden Lösung ordnungsgemäß funktionieren. Dies wird durch Tests und die Erfüllung umfassender Dokumentationsanforderungen erreicht.

Es wird von 26 Ländern weltweit über das Common Criteria Recognition Arrangement (CCRA) akzeptiert und unterstützt.

Cisco Unified Communications Manager Release 11.0 unterstützt ECDSA-Zertifikate (Elliptic Curve Digital Signature Algorithm).

Diese Zertifikate sind höher als die RSA-basierten Zertifikate und werden für Produkte mit CC-Zertifizierungen benötigt. Für das US Government Commercial Solutions for Classified Systems (CSfC)-Programm ist die CC-Zertifizierung erforderlich. Daher ist es in Cisco Unified Communications Manager Version 11.0 und höher enthalten.

Die ECDSA-Zertifikate sind zusammen mit den bestehenden RSA-Zertifikaten in folgenden Bereichen erhältlich:

- Zertifikatsverwaltung
- CAPF (Certificate Authority Proxy Function)
- TLS-Ablaufverfolgung (Transport Layer Security)
- SIP-Verbindungen (Secure Session Initiation Protocol)
- CTI-Manager (Computer Telefony Integration)
- HTTP
- Entropie

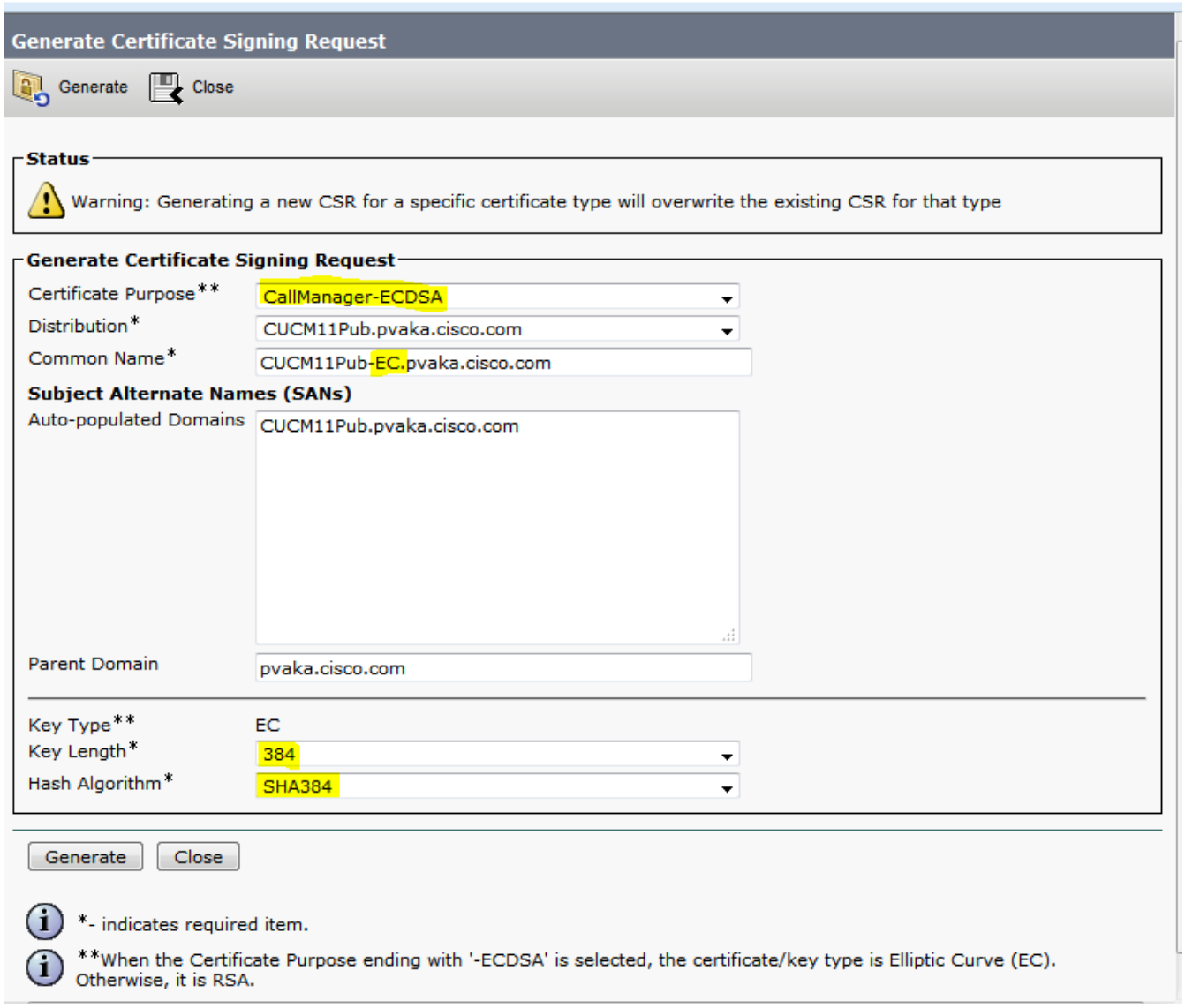
Die folgenden Abschnitte enthalten detailliertere Informationen zu jedem dieser sieben Bereiche.

Zertifikatsverwaltung

Generieren von Zertifikaten mit elliptischer Curve-Verschlüsselung

Unterstützung für ECC ab CUCM 11.0 zum Generieren des CallManager-Zertifikats mit Elliptical Curve (EC)-Verschlüsselung:

- Die neue Option **CallManager-ECDSA** ist wie im Bild gezeigt verfügbar.
- Der Hostteil des gemeinsamen Namens muss in **-EC** enden. Dadurch wird verhindert, dass der gleiche gebräuchliche Name wie das **CallManager-**Zertifikat vorhanden ist.
- Im Fall eines Multi-Server-SAN-Zertifikats muss dieses in **-EC-ms** enden.



- Sowohl die selbstsignierte Zertifikatsanforderung als auch die CSR-Anfrage beschränken die Auswahl des Hash-Algorithmus in Abhängigkeit von der EC-Schlüssellänge.
- Bei einer EC 256-Schlüsselgröße kann der Hash-Algorithmus SHA256, SHA384 oder SHA512 lauten. Bei einer EC 384-Schlüsselgröße kann der Hash-Algorithmus SHA384 oder SHA512 lauten. Bei einer EC 521-Schlüsselgröße ist SHA512 die einzige Option.
- Die Standardschlüsselgröße ist 384, der Standard-Hashing-Algorithmus SHA384, der geändert werden kann. Die verfügbaren Optionen basieren auf der gewählten Schlüssellänge.

CLI-Konfiguration

Eine neue Zertifikateinheit mit dem Namen **CallManager-ECDSA** wurde für die CLI-Befehle hinzugefügt.

- set cert regen [unit] - selbst signiertes Zertifikat neu erstellt.

```
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] - signiertes Einfuhrzertifikat der Zertifizierungsstelle

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

- set csr gen [unit] - generiert einen Zertifikatssignierungsantrag (Certificate Signing Request, CSR) für die angegebene **Einheit**

```
admin:set csr gen CallManager-ECDSA

Successfully Generated CSR  for CallManager-ECDSA

admin:
```

- set bulk export|consolidate|import tftp - Wenn tftp der Gerätename ist, werden CallManager-ECDSA-Zertifikate automatisch in CallManager-RSA-Zertifikate in Massenoperationen eingeschlossen.

CTL- und ITL-Dateien

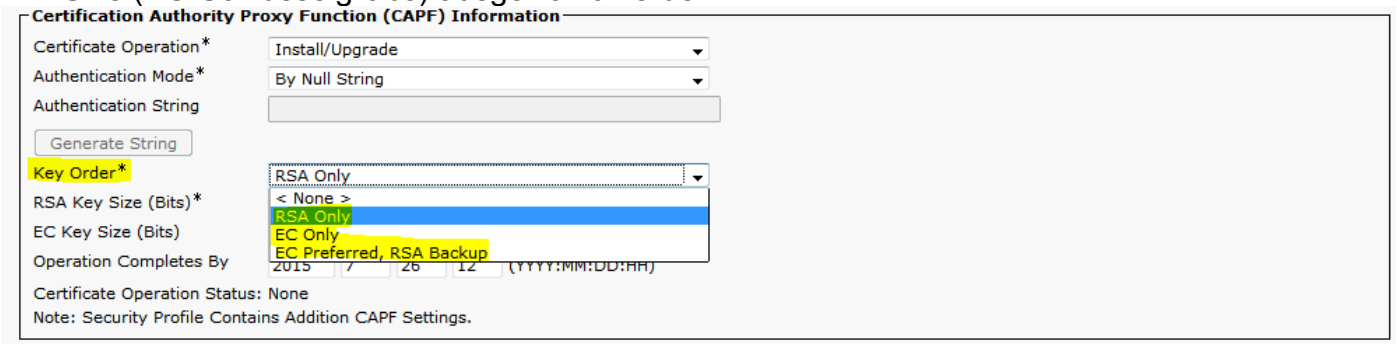
- Sowohl CTL- (Certificate Trust List) als auch ITL-Dateien (Identify Trust List) enthalten **CallManager-ECDSA**.
- Das CallManager-ECDSA-Zertifikat hat die Funktion von CCM+TFTP sowohl in der ITL- als auch in der CTL-Datei.
- Sie können **show ctl** oder **show itl** um diese Informationen anzuzeigen, wie in diesem Bild gezeigt:

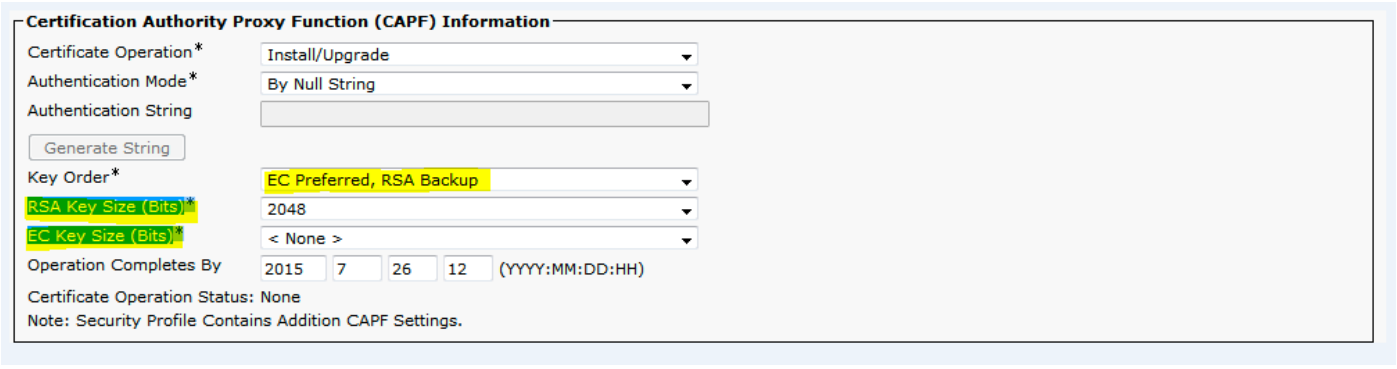
```
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1656
2       DNSNAME         2
3       SUBJECTNAME     65      CN=CUCM11Pub.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
4       FUNCTION        2       CCM+TFTP
5       ISSUERNAME      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.
```

- Sie können den Befehl **utils ctl update** zum Generieren der CTL-Datei verwenden.

Proxy-Funktion der Zertifizierungsstelle

- Die CAPF-Version 3.0 (Certificate Authority Proxy Function) des CUCM 11 unterstützt EC Key-Größen zusammen mit RSA.
- Die zusätzlichen CAPF-Optionen, die zusätzlich zu den vorhandenen CAPF-Feldern bereitgestellt werden, sind Key Order (Schlüsselbestellung) und EC Key Size (Bit) (EC-Schlüsselgröße).
- Die vorhandene Option Key Size (bits) wurde in RSA Key Size (bits) geändert.
- Die Key-Order-Bestellung bietet Unterstützung für RSA Only-, EC Only- und EC Preferred-, RSA-Sicherungsoptionen.
- Die EC Key Size unterstützt Schlüsselgrößen von 256, 384 und 521 Bit.
- Die RSA-Schlüsselgröße unterstützt 512, 1024 und 2048 Bit.
- Wenn die Schlüsselreihenfolge von RSA Only (Nur RSA-Schlüssel) ausgewählt ist, kann nur die RSA-Schlüsselgröße ausgewählt werden. Wenn nur EC (EC) ausgewählt ist, kann nur EC Key Size (EC-Schlüsselgröße) ausgewählt werden. Wenn "EC Preferred" (EC Bevorzugt), "RSA backup" (RSA-Sicherung) ausgewählt ist, können sowohl die RSA- als auch die EC Key Size (EC-Schlüsselgröße) ausgewählt werden.

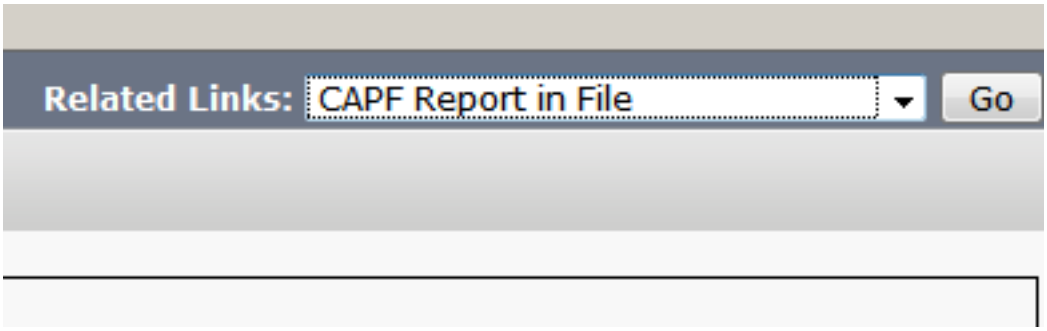




> **Hinweis**: Derzeit unterstützt kein Cisco Endgerät CAPF Version 3. Wählen Sie daher nicht die Option Nur EC aus. Administratoren, die zu einem späteren Zeitpunkt ECDSA Locally Significant Certificates (LSCs) unterstützen möchten, können ihre Geräte jedoch mit der Option "EC Preferred RSA Backup" (Von EC bevorzugte RSA-Sicherung) konfigurieren. Wenn die Endgeräte CAPF Version 3 für ECDSA LSCs unterstützen, müssen die Administratoren ihr LSC neu installieren.

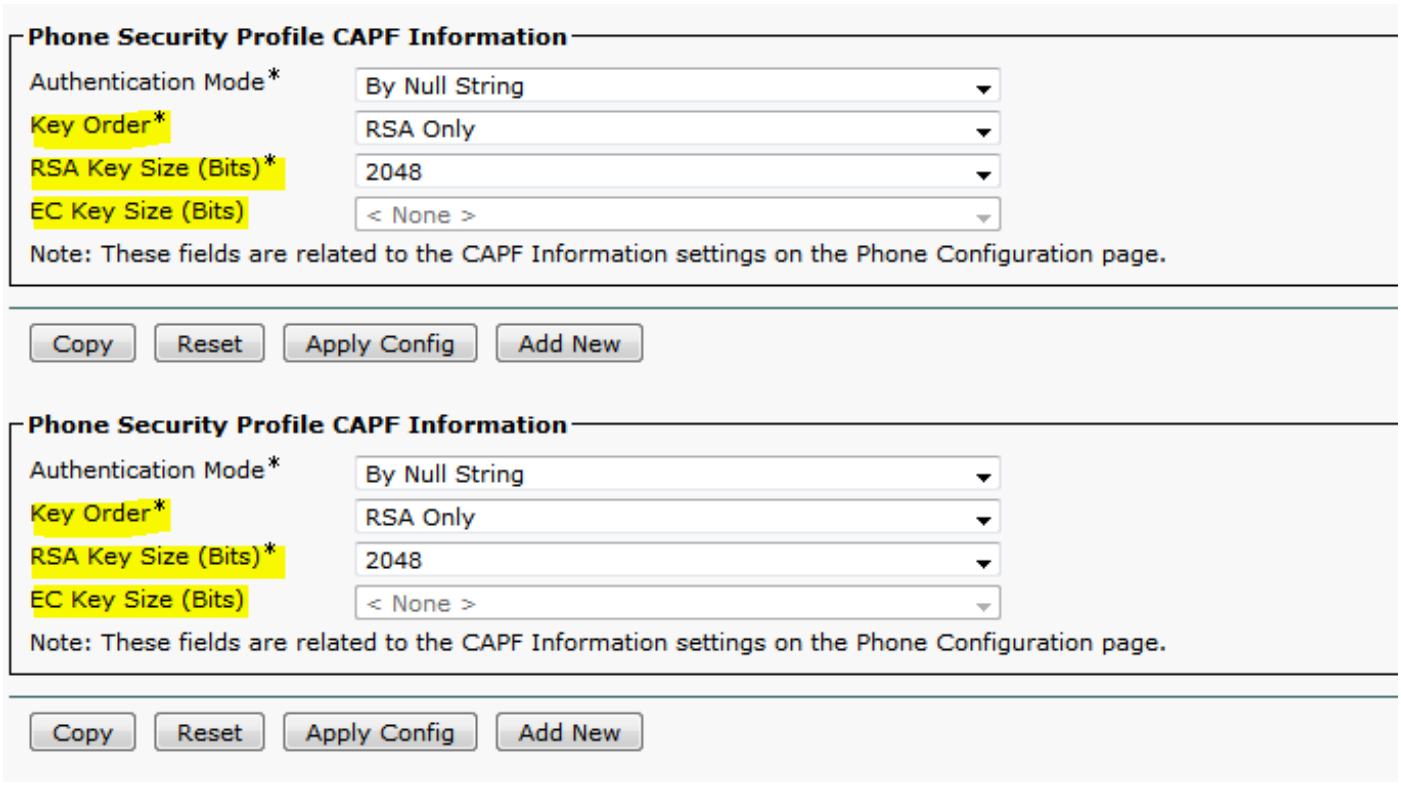
Zusätzliche CAPF-Optionen für Telefon-, Telefon-Sicherheitsprofil-, Endbenutzer- und Anwendungsbenutzerseiten sind hier aufgeführt:

Gerät > Telefon > Verwandte Links

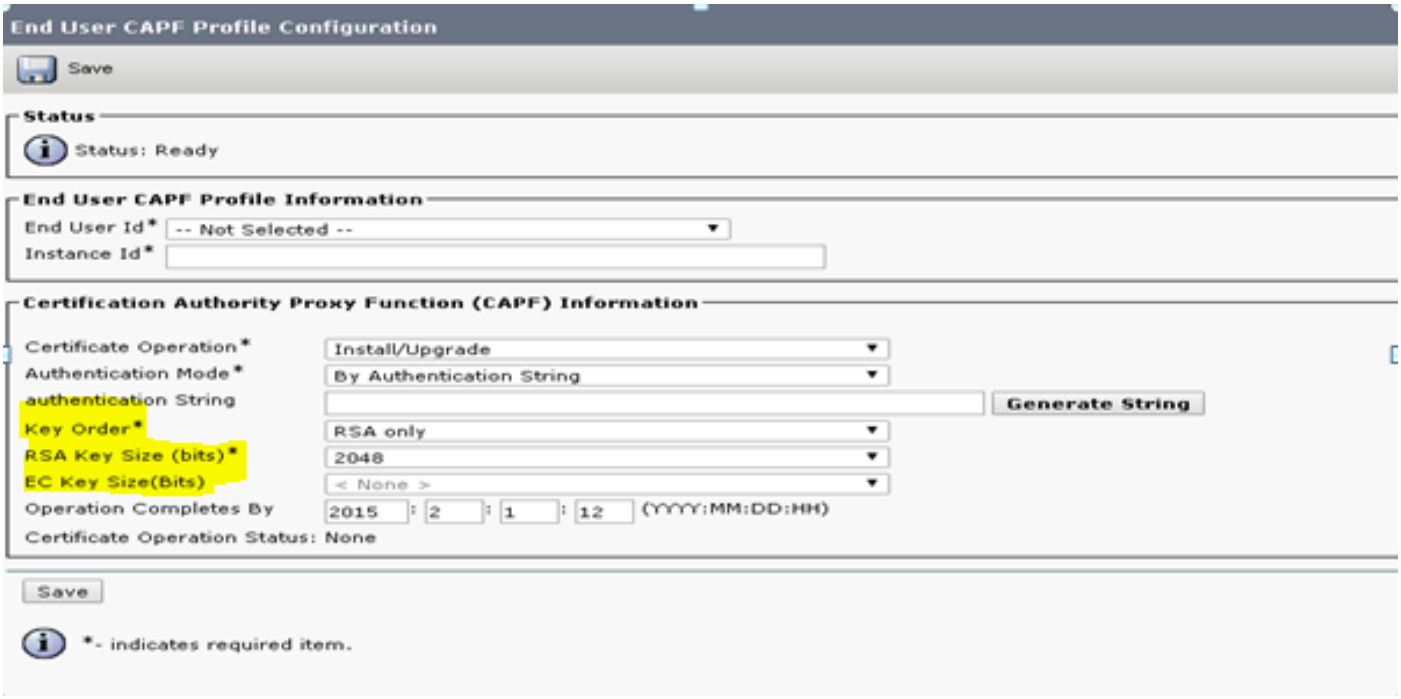


Navigieren Sie zu **System > Security > Phone Security Profile.**

Benutzerverwaltung > Benutzereinstellungen > CAPF-Profil für Anwendungsbenutzer

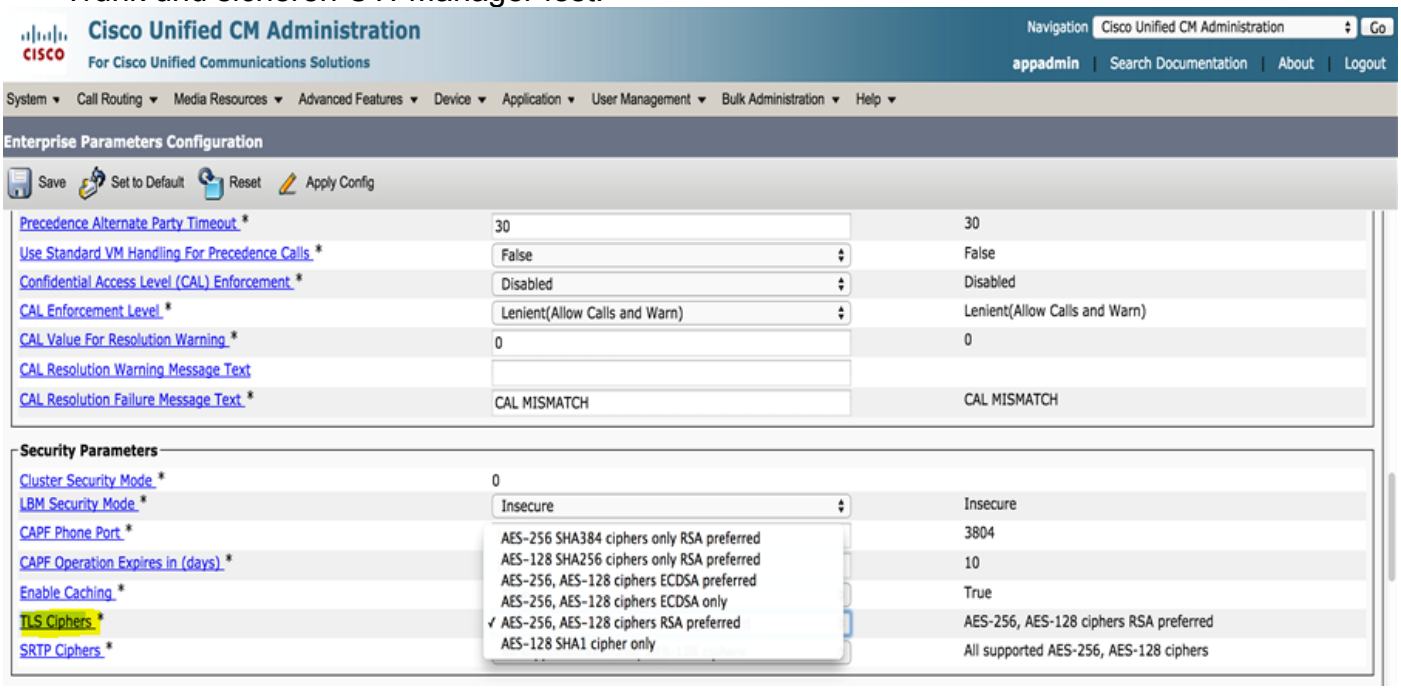


Navigieren Sie zu **User Management > User Settings > End User CAPF Profile.**



Enterprise-Parameter für TLS-Ciphers

- Die TLS-Chiffren für Enterprise-Parameter wurden aktualisiert, um ECDSA-Chiffers zu unterstützen.
- Die TLS-Ciphers für Enterprise-Parameter legen nun die TLS-Chiffren für SIP-Leitung, SIP-Trunk und sicheren CTI-Manager fest.



SIP ECDSA-Unterstützung

- Cisco Unified Communications Manager Version 11.0 bietet ECDSA-Unterstützung für SIP-Leitungen und SIP-Trunk-Schnittstellen.
- Die Verbindung zwischen Cisco Unified Communications Manager und einem Endpunkt-Telefon oder Videogerät ist eine SIP-Leitungsverbindung, während es sich bei der Verbindung

zwischen zwei Cisco Unified Communications Manager um eine SIP-Trunk-Verbindung handelt.
- Alle SIP-Verbindungen unterstützen die ECDSA-Chiffren und verwenden ECDSA-Zertifikate.

Die Secure SIP-Schnittstelle wurde aktualisiert, um die folgenden beiden Verschlüsselungszeichen zu unterstützen:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

Dies sind die Szenarien, in denen SIP TLS-Verbindungen herstellt:

- Wenn SIP als TLS-Server fungiert Wenn die SIP-Trunk-Schnittstelle von Cisco Unified Communications Manager als TLS-Server für eingehende, sichere SIP-Verbindungen fungiert, bestimmt die SIP-Trunk-Schnittstelle, ob das CallManager-ECDSA-Zertifikat auf der Festplatte vorhanden ist. Wenn das Zertifikat auf der Festplatte vorhanden ist, verwendet die SIP-Trunk-Schnittstelle das CallManager-ECDSA-Zertifikat, wenn die ausgewählte VerschlüsselungssuiteTLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 oder TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- Wenn SIP als TLS-Client fungiert Wenn die SIP-Trunk-Schnittstelle als TLS-Client fungiert, sendet die SIP-Trunk-Schnittstelle basierend auf dem Feld "TLS Ciphers" (TLS Ciphers) in den CUCM-Enterprise-Parametern **Die TLS-Ciphers** eine Liste der angeforderten Verschlüsselungssuiten an den Server. Diese Konfiguration legt die bevorzugte Reihenfolge für die Liste der TLS-Client-Chiffren-Suites und die unterstützten Verschlüsselungssuiten fest.

  Hinweise:
  - Geräte, die eine ECDSA-Verschlüsselung für die Verbindung mit dem CUCM verwenden, müssen das CallManager-ECDSA-Zertifikat in ihrer ITL-Datei (Identity Trust List) haben.
  - Die SIP-Trunk-Schnittstelle unterstützt RSA TLS-Verschlüsselungssuiten für Verbindungen von Clients, die keine ECDSA-Verschlüsselungssuiten unterstützen, oder wenn eine TLS-Verbindung mit einer früheren Version von CUCM hergestellt wurde, die ECDSA nicht unterstützt.

ECDSA-Support für Secure CTI Manager

Die Secure CTI Manager-Schnittstelle wurde aktualisiert, um diese vier Verschlüsselungscodes zu unterstützen:

- 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

Die Schnittstelle Secure CTI Manager lädt sowohl das CallManager- als auch das CallManager-ECDSA-Zertifikat. Dadurch kann die Schnittstelle Secure CTI Manager die neuen Chiffren zusammen mit der vorhandenen RSA-Chiffre unterstützen.

Ähnlich wie die SIP-Schnittstelle wird die Option TLS-Chiffren für Enterprise-Parameter in Cisco Unified Communications Manager zum Konfigurieren der TLS-Chiffren verwendet, die von der sicheren CTI Manager-Schnittstelle unterstützt werden.

HTTPS-Unterstützung für Konfigurationsdownload

- Für das sichere Herunterladen von Konfigurationen (z. B. Jabber-Clients) wurde Cisco Unified Communications Manager Version 11.0 um HTTPS erweitert, zusätzlich zu den HTTP- und TFTP-Schnittstellen, die in früheren Versionen verwendet wurden.
- Bei Bedarf verwenden Client und Server gegenseitige Authentifizierung. Die Clients, die bei ECDSA LSCs und verschlüsselten TFTP-Konfigurationen registriert sind, müssen jedoch ihr LSC vorlegen.
- Die HTTPS-Schnittstelle verwendet sowohl das CallManager- als auch das CallManager-ECDSA-Zertifikat als Serverzertifikat.

Hinweise:
- Wenn Sie CallManager-, CallManager ECDSA- oder Tomcat-Zertifikate aktualisieren, müssen Sie den TFTP-Dienst deaktivieren und erneut aktivieren.
- Port 6971 wird zur Authentifizierung der von Telefonen verwendeten CallManager- und CallManager-ECDSA-Zertifikate verwendet.
- Port 6972 wird für die Authentifizierung der Tomcat-Zertifikate verwendet, die von Jabber verwendet werden.

Entropie

Entropie ist ein Maß für die Randomie der Daten und hilft bei der Bestimmung des Mindestschwellenwerts für gemeinsame Kriterienanforderungen. Um eine starke Verschlüsselung zu erreichen, ist eine robuste Entropie erforderlich. Wenn ein starker Verschlüsselungsalgorithmus wie ECDSA eine schwache Entropie verwendet, kann die Verschlüsselung leicht unterbrochen werden.

In Cisco Unified Communications Manager Version 11.0 wird die Entropie-Quelle für Cisco Unified Communications Manager verbessert.

Entropy Monitoring Daemon ist eine integrierte Funktion, die keine Konfiguration erfordert. Sie können die Funktion jedoch über die CLI von Cisco Unified Communications Manager deaktivieren.

Verwenden Sie die folgenden CLI-Befehle, um den Daemon-Dienst für die Entropy-Überwachung zu steuern:

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.

Zugehörige Informationen

- Sicherheitsleitfaden für Cisco Unified Communications Manager, Version 11.5(1)
- Technischer Support und Dokumentation - Cisco Systems