CUCM 11.0 Next Generation Encryption - Elliptic Curve Cryptography

목차

소개

이 문서에서는 향상된 보안 및 성능 요구 사항을 충족하기 위해 Cisco CUCM(Unified Communications Manager) 11.0 이상에서 NGE(Next Generation Encryption)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco CallManager 보안 기본 사항
- Cisco CallManager 인증서 관리

사용되는 구성 요소

이 문서의 정보는 Cisco CUCM 11.0을 기반으로 합니다. 여기서 ECDSA(Elliptic Curve Digital Signature Algorithm) 인증서는 CallManager(CallManager-ECDSA)에만 지원됩니다.

> **참고:**CUCM 11.5 이상에서는 tomcat-ECDSA 인증서도 지원합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

관련 제품

이 문서는 ECDSA 인증서를 지원하는 소프트웨어 제품 및 버전과 함께 사용할 수도 있습니다.

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

배경 정보

ECC(Elliptic Curve Cryptography)는 유한 필드를 넘는 타원 곡선의 대수적 구조를 기반으로 공개 키 암호화에 대한 접근 방식입니다.비 ECC 암호화와 비교했을 때 얻을 수 있는 주요 이점 중 하나는 더 작은 크기의 키에 의해 제공되는 보안 수준과 동일합니다.

CC(Common Criteria)는 평가 중인 솔루션 내에서 보안 기능이 올바르게 작동함을 보장합니다.이는 광범위한 문서 요구 사항을 충족하고 테스트를 통해 달성됩니다.

CCRA(Common Criteria Recognition Arrangement)를 통해 전 세계 26개 국가에서 이를 수용하고 지원합니다.

Cisco Unified Communications Manager 릴리스 11.0은 ECDSA(Elliptic Curve Digital Signature Algorithm) 인증서를 지원합니다.

이러한 인증서는 RSA 기반 인증서보다 강력하며 CC 인증을 보유한 제품에 필요합니다.미국 정부 CSfC(Commercial Solutions for Classified Systems) 프로그램은 CC 인증이 필요하므로 Cisco Unified Communications Manager 릴리스 11.0 이상에 포함되어 있습니다.

ECDSA 인증서는 다음 영역에서 기존 RSA 인증서와 함께 사용할 수 있습니다.

- 인증서 관리
- CAPF(Certificate Authority Proxy Function)
- TLS(Transport Layer Security) 추적
- SIP(Secure Session Initiation Protocol) 연결
- CTI(Computer Telephony Integration) 관리자
- HTTP
- 엔트로피

다음 섹션에서는 이러한 7개 영역 각각에 대한 자세한 정보를 제공합니다.

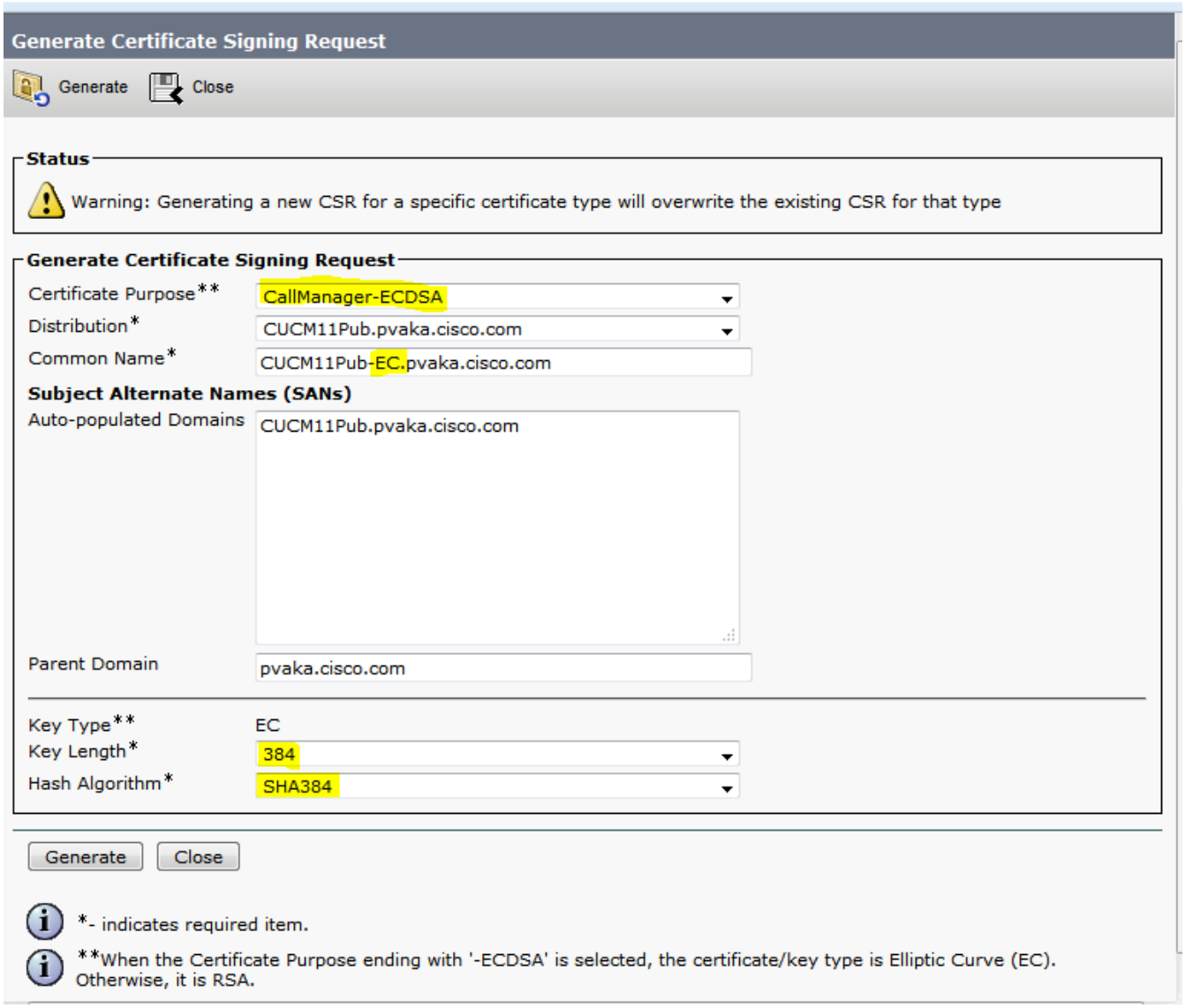
인증서 관리

타원 곡선 암호화를 사용하여 인증서 생성

CUCM 11.0 이상에서 ECC를 지원하여 EC(Elliptical Curve) 암호화를 사용하여 CallManager 인증서를 생성합니다.

- 새 옵션 **CallManager-ECDSA**는 이미지에 표시된 대로 사용할 수 있습니다.

- EC에서 종료하려면 공용 이름의 호스트 부분이 **필요합니다**.이렇게 하면 CallManager 인증서와 동일한 공용 이름**을** 가질 수 없습니다.
- 다중 서버 SAN 인증서의 경우 **-EC-ms로 끝나야 합니다**.



- 자체 서명 인증서 요청과 CSR 요청 모두 EC 키 크기에 따라 해시 알고리즘 선택을 제한합니다.
- EC 256 키 크기의 경우 해시 알고리즘은 SHA256, SHA384 또는 SHA512가 될 수 있습니다. EC 384 키 크기의 경우 해시 알고리즘은 SHA384 또는 SHA512가 될 수 있습니다. EC 521 키 크기의 경우 옵션만 SHA512가 됩니다.
- 기본 키 크기는 384이고 기본 해싱 알고리즘은 변경할 수 있는 SHA384입니다.사용 가능한 옵션은 선택한 키 크기에 따라 달라집니다.

CLI 컨피그레이션

CLI 명령에 **대해 CallManager-ECDSA**라는 새 인증서 단위가 추가되었습니다.

- set cert regen [unit] - 자체 서명 인증서 재생성

```
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] - CA 서명 인증서 가져오기

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

- set csr gen [unit] - 지정된 **유닛**에 대한 CSR(certificate signing request)을 생성합니다.

```
admin:set csr gen CallManager-ECDSA

Successfully Generated CSR  for CallManager-ECDSA

admin:
```

- set bulk export|consolidate|import tftp - tftp가 장치 이름인 경우 CallManager-ECDSA 인증서는 대량 작업에서 CallManager RSA 인증서에 자동으로 포함됩니다.

CTL 및 ITL 파일

- CTL(Certificate Trust List) 및 ITL(Identify Trust List) 파일 모두 **CallManager-ECDSA가** 있습니다.
- CallManager-ECDSA 인증서는 ITL 및 CTL 파일에서 CCM+TFTP 기능을 갖습니다.
- 사용 가능한 **show ctl** 또는 **show itl** 이 이미지에 표시된 대로 이 정보를 볼 수 있습니다.

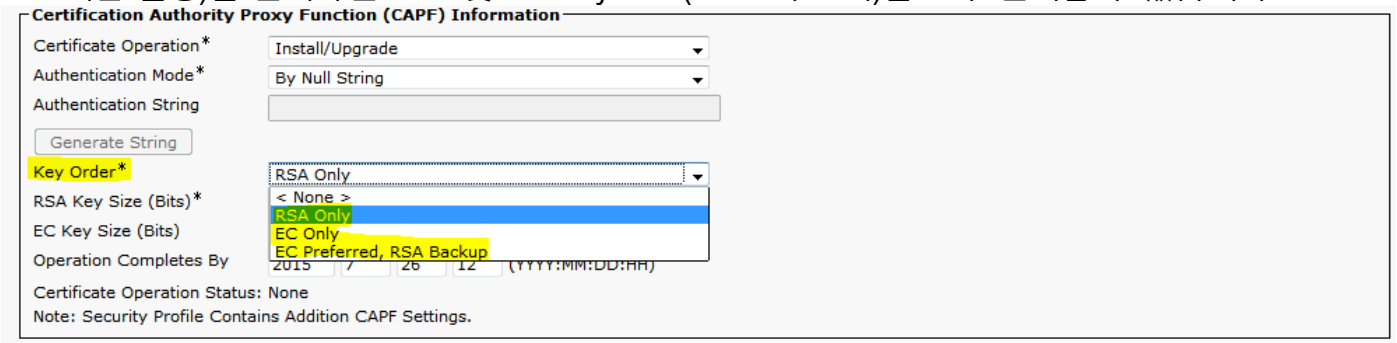
```
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1656
2       DNSNAME         2
3       SUBJECTNAME     65      CN=CUCM11Pub.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
4       FUNCTION        2       CCM+TFTP
5       ISSUERNAME 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

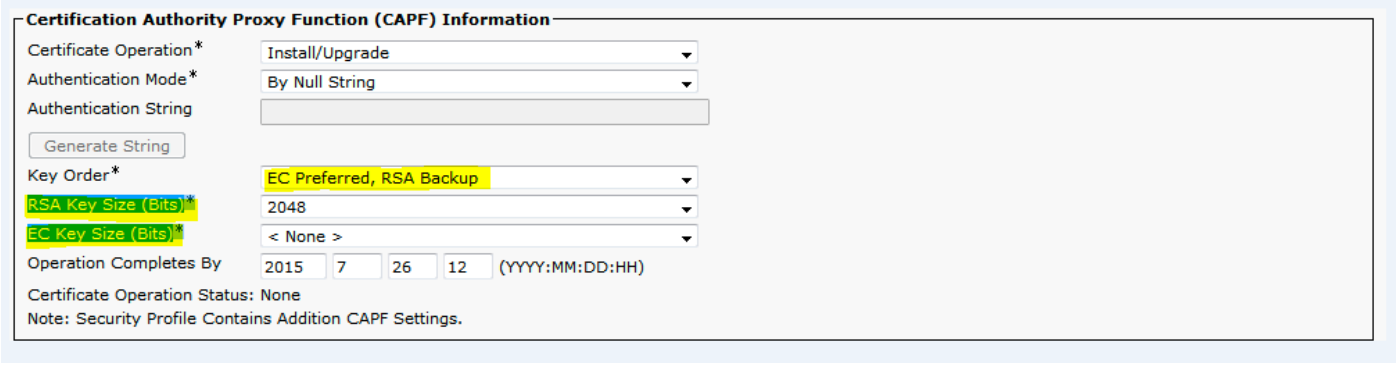
- utils ctl **update** 명령을 사용하여 CTL 파일을 생성할 수 있습니다.

인증 기관 프록시 기능

- CUCM 11의 CAPF(Certificate Authority Proxy Function) 버전 3.0은 RSA와 함께 EC 키 크기를 지원합니다.

- 기존 CAPF 필드 외에 제공되는 추가 CAPF 옵션은 Key Order(키 순서) 및 EC Key Size(비트)입니다.
- 기존 키 크기(비트) 옵션이 RSA 키 크기(비트)로 변경되었습니다.
- Key Order(키 주문)에서는 RSA 전용, EC 전용 및 EC Preferred(RSA 백업 옵션)를 지원합니다.
- EC Key Size는 256, 384 및 521비트의 키 크기를 지원합니다.
- RSA 키 크기는 512, 1024 및 2048비트를 지원합니다.
- Key Order of RSA Only(RSA 전용 키 순서)를 선택하면 RSA Key Size(RSA 키 크기)만 선택할 수 있습니다.EC만 선택하면 EC Key Size(EC 키 크기)만 선택할 수 있습니다.EC Preferred(EC 기본 설정)를 선택하면 RSA 및 EC Key Size(RSA 키 크기)를 모두 선택할 수 있습니다.

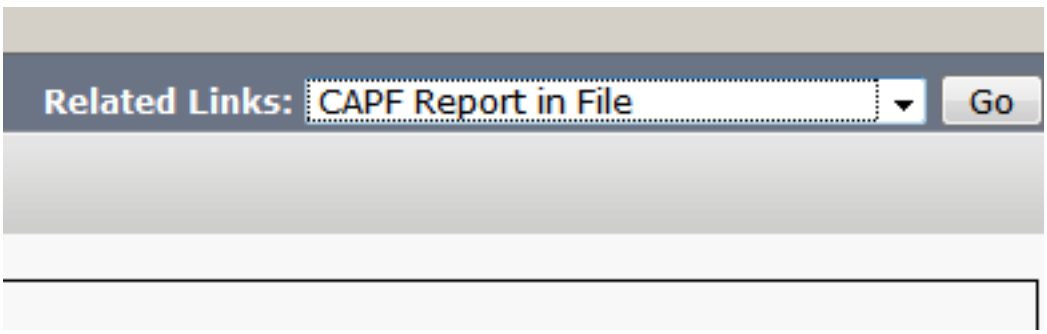




참고:현재 Cisco 엔드포인트는 CAPF 버전 3을 지원하지 않으므로 EC Only 옵션을 선택하지 마십시오.그러나 나중에 ECDSA LSC(Locally Significant Certificates)를 지원하려는 관리자는 EC Preferred RSA Backup 옵션을 사용하여 디바이스를 구성할 수 있습니다.엔드포인트가 ECDSA LSC에 대해 CAPF 버전 3을 지원하기 시작하면 관리자가 LSC를 다시 설치해야 합니다.

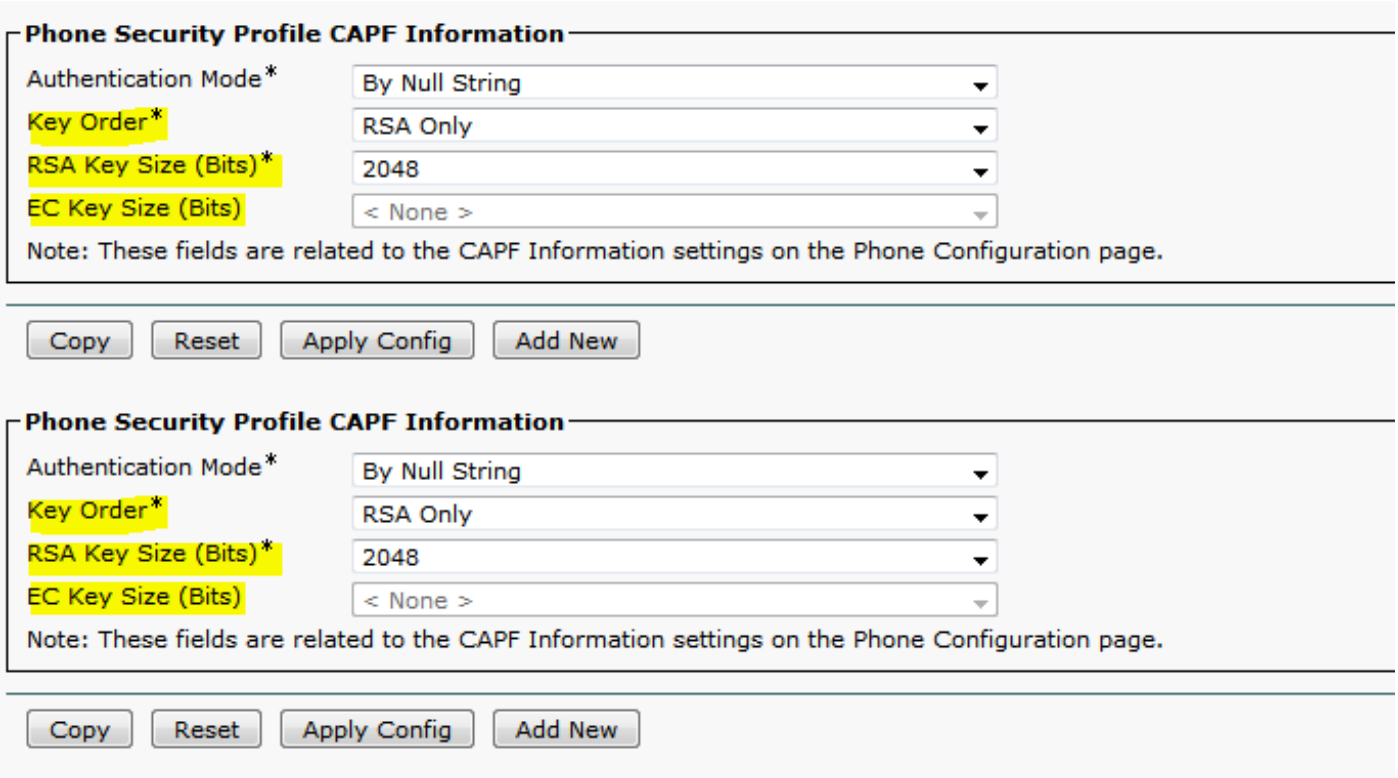
전화, 전화 보안 프로필, 최종 사용자 및 애플리케이션 사용자 페이지에 대한 추가 CAPF 옵션은 다음과 같습니다.

디바이스 > 전화 > 관련 링크

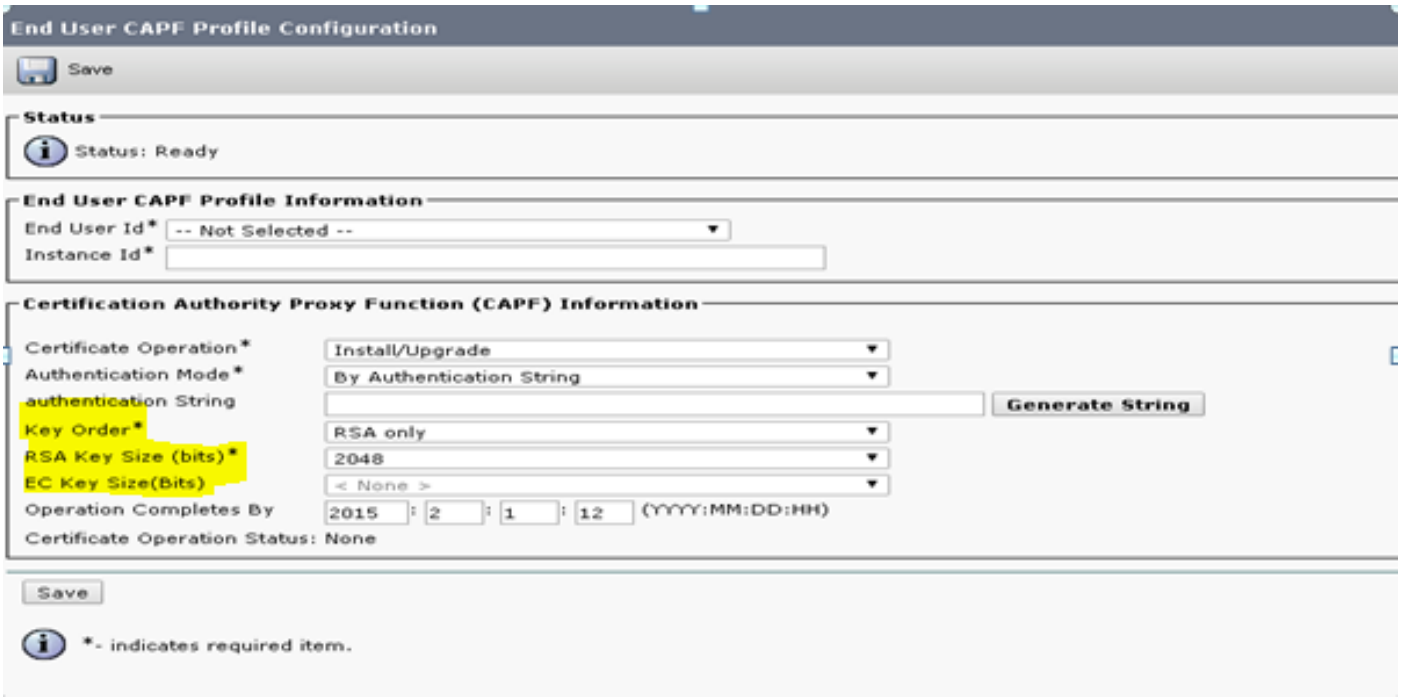


System(**시스템) > Security(보안) > Phone security profile(전화기 보안 프로파일)으로 이동합니다.**

사용자 관리 > 사용자 설정 > 애플리케이션 사용자 CAPF 프로파일

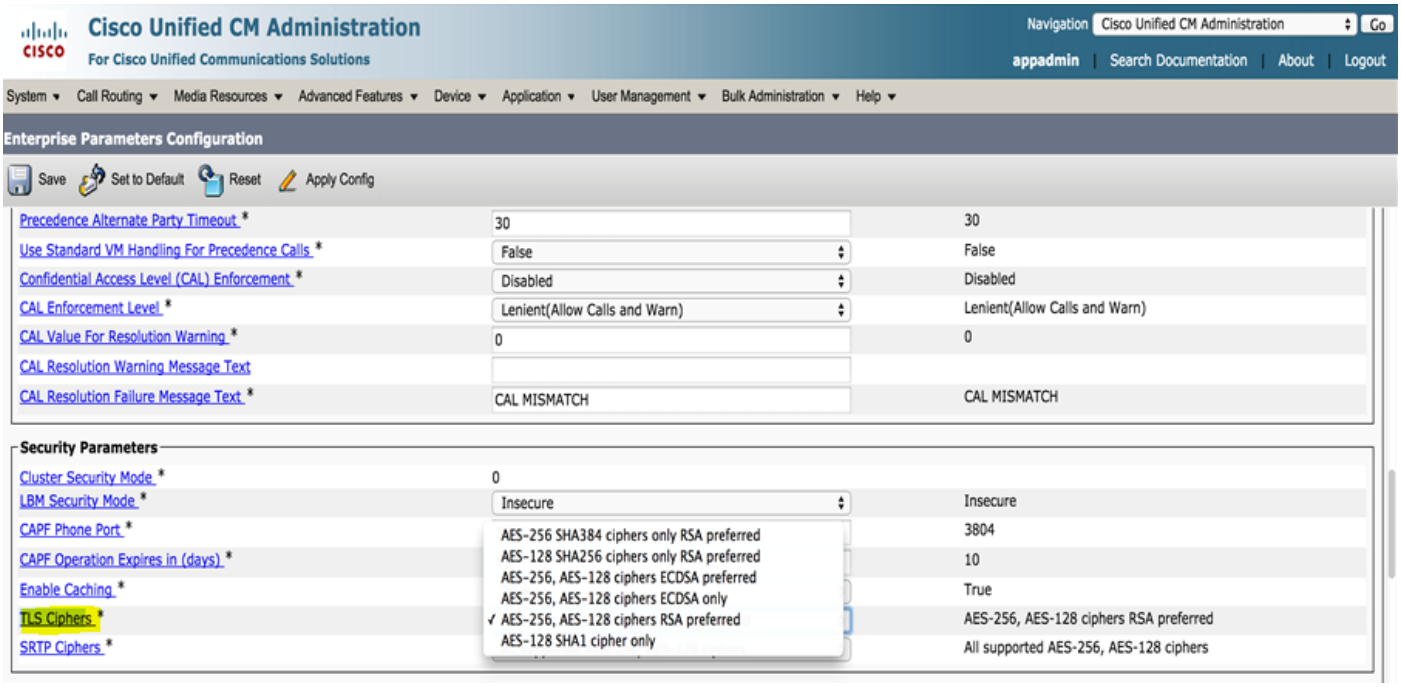


User **Management(사용자 관리) > User Settings(사용자 설정) > End User CAPF Profile(최종 사용자 CAPF 프로파일)**로 이동합니다.



TLS 암호 엔터프라이즈 매개변수

- 엔터프라이즈 매개 변수 TLS 암호가 ECDSA 암호를 지원하도록 업데이트되었습니다.
- Enterprise Parameter TLS Ciphers는 이제 SIP Line, SIP Trunk 및 Secure CTI Manager용 TLS 암호를 설정합니다.



SIP ECDSA 지원

- Cisco Unified Communications Manager Release 11.0에는 SIP 회선 및 SIP 트렁크 인터페이스에 대한 ECDSA 지원이 포함됩니다.
- Cisco Unified Communications Manager와 엔드포인트 전화기 또는 비디오 디바이스 간의 연결은 SIP 회선 연결인 반면, 두 Cisco Unified Communications Manager 간의 연결은 SIP 트렁크 연결입니다.
- 모든 SIP 연결은 ECDSA 암호를 지원하고 ECDSA 인증서를 사용합니다.

Secure SIP 인터페이스는 다음 두 암호를 지원하도록 업데이트되었습니다.

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

다음은 SIP가 TLS 연결을 만드는 시나리오입니다.

- SIP가 TLS 서버 역할을 하는 경우 Cisco Unified Communications Manager의 SIP 트렁크 인터페이스가 수신 보안 SIP 연결을 위한 TLS 서버 역할을 하는 경우 SIP 트렁크 인터페이스는 CallManager-ECDSA 인증서가 디스크에 있는지 여부를 결정합니다.인증서가 디스크에 있는 경우 선택한 암호 그룹이TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 또는 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- SIP가 TLS 클라이언트로 작동하는 경우 SIP 트렁크 인터페이스가 TLS 클라이언트 역할을 하는 경우 SIP 트렁크 인터페이스는 CUCM Enterprise Parameters The TLS Ciphers의 TLS Ciphers 필드(ECDSA 암호 옵션도 포함)를 기반으로 요청된 암호 그룹 목록**을** 서버로 **전송합니다**.이 컨피그레이션은 TLS 클라이언트 암호 그룹 목록 및 지원되는 암호 그룹을 기본 설정 순서대로 결정합니다.

참고:
- ECDSA 암호를 사용하여 CUCM에 연결하는 디바이스에는 ITL(Identity Trust List) 파일에 CallManager-ECDSA 인증서가 있어야 합니다.
- SIP 트렁크 인터페이스는 ECDSA 암호 그룹을 지원하지 않는 클라이언트 또는 ECDSA를 지원하지 않는 이전 버전의 CUCM으로 TLS 연결이 설정된 경우 RSA TLS 암호 그룹을 지원합니다.

Secure CTI Manager ECDSA 지원

Secure CTI Manager 인터페이스는 다음 네 가지 암호를 지원하도록 업데이트되었습니다.

- 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

Secure CTI Manager 인터페이스는 CallManager 및 CallManager-ECDSA 인증서를 모두 로드합니다.이렇게 하면 Secure CTI Manager 인터페이스가 기존 RSA 암호와 함께 새 암호를 지원할 수 있습니다.

SIP 인터페이스와 마찬가지로 Cisco Unified Communications Manager의 Enterprise Parameter TLS Ciphers 옵션을 사용하여 CTI Manager 보안 인터페이스에서 지원되는 TLS 암호를 구성합니다.

구성 다운로드를 위한 HTTPS 지원

- 보안 컨피그레이션 다운로드(예: Jabber 클라이언트)를 위해 Cisco Unified Communications Manager Release 11.0은 이전 릴리스에서 사용된 HTTP 및 TFTP 인터페이스 외에도 HTTPS를 지원하도록 개선되었습니다.
- 필요한 경우 클라이언트와 서버 모두 상호 인증을 사용합니다.그러나 ECDSA LSC 및 암호화된 TFTP 컨피그레이션과 함께 등록된 클라이언트는 LSC를 제공해야 합니다.
- HTTPS 인터페이스는 CallManager 및 CallManager-ECDSA 인증서를 모두 서버 인증서로 사용합니다.

  참고:
  - CallManager, CallManager ECDSA 또는 Tomcat 인증서를 업데이트할 때 TFTP 서비스를 비활성화하고 다시 활성화해야 합니다.
  - 포트 6971은 전화기에서 사용되는 CallManager 및 CallManager-ECDSA 인증서의 인증에 사용됩니다.
  - 포트 6972는 Jabber에서 사용하는 Tomcat 인증서의 인증에 사용됩니다.

엔트로피

엔트로피는 데이터의 임의 측정이며 공통 기준 요구 사항에 대한 최소 임계값을 결정하는 데 도움이 됩니다.강력한 암호화를 위해서는 강력한 엔트로피 소스가 필요합니다.ECDSA와 같은 강력한 암호화 알고리즘이 낮은 엔트로피 소스를 사용하는 경우, 암호화가 쉽게 손상될 수 있습니다.

Cisco Unified Communications Manager 릴리스 11.0에서는 Cisco Unified Communications Manager의 엔트로피 소스가 개선되었습니다.

Entropy Monitoring Daemon은 구성이 필요하지 않은 기본 제공 기능입니다.그러나 Cisco Unified Communications Manager CLI를 통해 해제할 수 있습니다.

다음과 같은 CLI 명령을 사용하여 엔트로피 모니터링 데몬 서비스를 제어합니다.

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.

관련 정보

- Cisco Unified Communications Manager 릴리스 11.5(1)용 보안 설명서
- 기술 지원 및 문서 – Cisco Systems