CUCM 11.0次世代暗号化：楕円曲線暗号化

内容

概要

このドキュメントでは、拡張されたセキュリティおよびパフォーマンス要件を満たすために、Cisco Unified Communications Manager(CUCM)11.0以降からのNext Generation Encryption(NGE)の設定について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco CallManagerセキュリティの基本
- Cisco CallManager証明書管理

使用するコンポーネント

このドキュメントの情報はCisco CUCM 11.0に基づいています。Cisco CUCM 11.0では、楕円曲線デジタル署名アルゴム(ECDSA)証明書は、CallManager(CallManager-ECDSA)でのみサポートされています。

> **注：**CUCM 11.5以降では、tomcat-ECDSA証明書もサポートされています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

関連製品

このドキュメントは、ECDSA証明書をサポートする次のソフトウェア製品およびバージョンでも使用できます。

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

背景説明

楕円曲線暗号(ECC)は、有限分野上の楕円曲線の代数構造に基づいて、公開キー暗号化を行うアプローチの一つで、これを実現します。非ECC暗号化と比較した主な利点の1つは、小さいサイズのキーによって提供されるセキュリティの同じレベルです。

Common Criteria(CC)は、評価対象のソリューション内でセキュリティ機能が正しく動作することを保証します。これは、テストを行い、広範なドキュメント要件を満たすことで実現されます。

Common Criteria Recognition Arrangement(CCRA)を通じて、世界26ヵ国で承認およびサポートされています。

Cisco Unified Communications Managerリリース11.0は、楕円曲線デジタル署名アルゴリズム(ECDSA)証明書をサポートしています。

これらの証明書はRSAベースの証明書よりも強力であり、CC認定を持つ製品に必要です。米国政府のCommercial Solutions for Classified Systems(CSfC)プログラムにはCC認定が必要なため、Cisco Unified Communications Managerリリース11.0以降に含まれています。

ECDSA証明書は、次の領域の既存のRSA証明書とともに使用できます。

- 証明書の管理
- Certificate Authority Proxy Function（CAPF）
- Transport Layer Security(TLS)トレース
- Secure Session Initiation Protocol(SIP)接続
- Computer Telephony Integration(CTI)Manager
- HTTP
- エントロピー

次のセクションでは、これら7つの各エリアについて詳しく説明します。

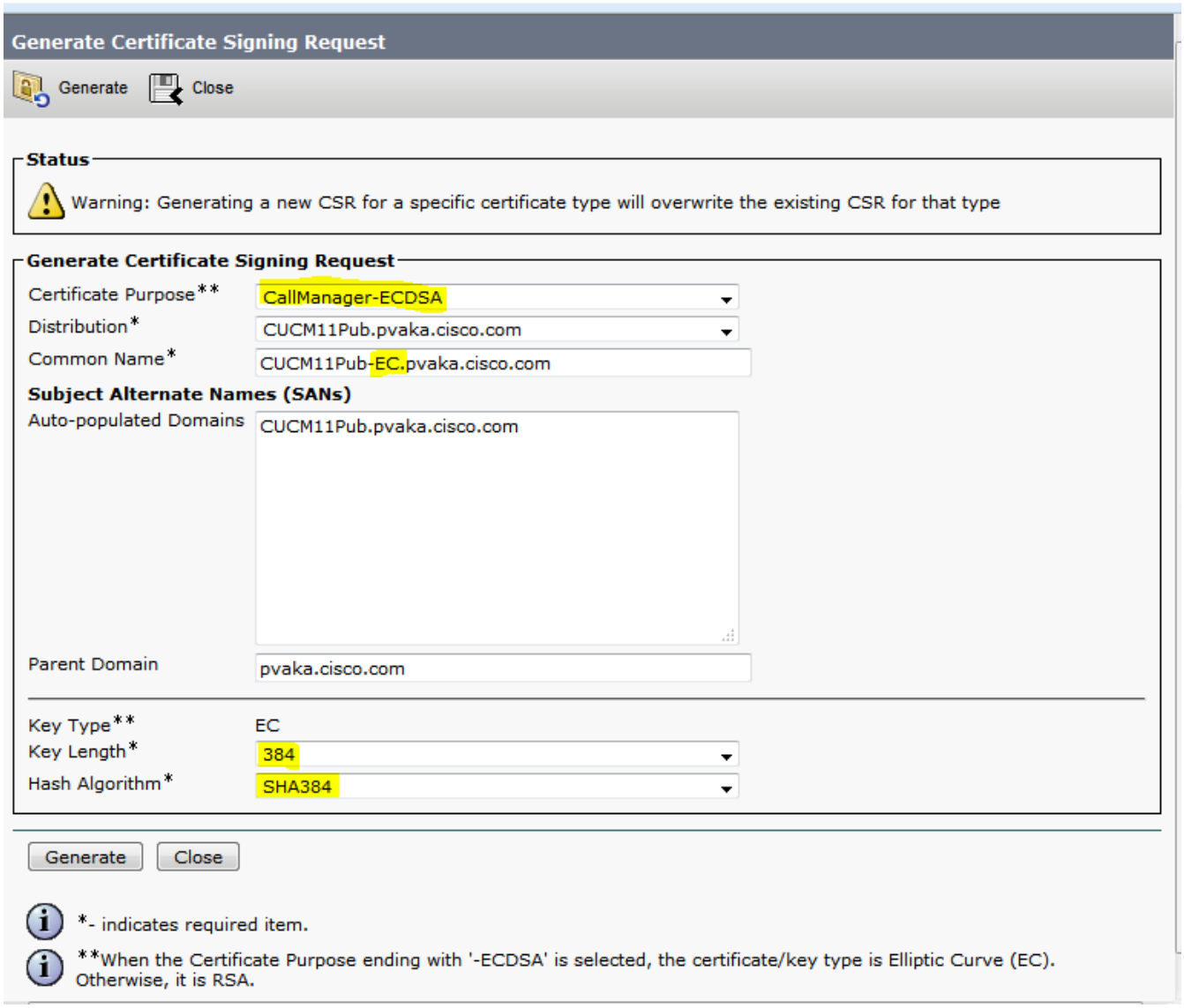
証明書の管理

楕円曲線暗号化による証明書の生成

楕円曲線(EC)暗号化を使用したCallManager証明書を生成するためのCUCM 11.0以降からの

ECCのサポート：

- 図に示すように、新**しいオプションCallManager-ECDSA**を使用できます。
- このコマンドを実行するには、共通名のホスト部分がIn-ECで終わる必要**があります**。これにより、CallManager証明書と同じ共通名を持つ**ことができ**ません。
- マルチサーバSAN証明書の場合は、EC-msで終わる必要**があります**。



- 自己署名証明書の要求とCSRの要求の両方で、ECキーサイズに応じてハッシュアルゴリズムの選択が制限されます。
- EC 256キーサイズの場合、ハッシュアルゴリズムはSHA256、SHA384、またはSHA512になります。EC 384キーサイズの場合、ハッシュアルゴリズムはSHA384またはSHA512になります唯一のオプションはSHA512です。
- デフォルトのキーサイズは384で、デフォルトのハッシュアルゴリズムはSHA384です。これは変更可能です。使用できるオプションは、選択したキーサイズに基づいています。

CLI での設定

CLIコマンドに**CallManager-ECDSA**という名前の新しい証明書ユニットが追加されました

- set cert regen [unit] – 自己署名証明書を再生成します

```
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署名付き証明書をインポートします

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

- set csr gen [unit] – 指定されたユニットの証明書署名要求(CSR)を生成します

```
admin:set csr gen CallManager-ECDSA

Successfully Generated CSR  for CallManager-ECDSA

admin:
```

- set bulk export|consolidate|import tftp - tftpがユニット名の場合、CallManager-ECDSA証明書は一括操作でCallManager RSA証明書に自動組み込まれます。

CTLファイルとITLファイル

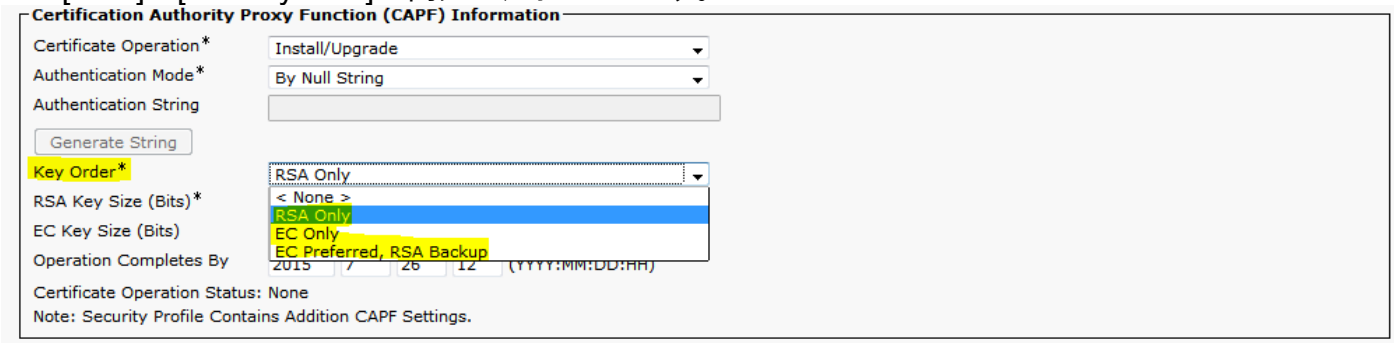
- 証明書信頼リスト(CTL)ファイルと信頼リスト(ITL)ファイルの両方に**CallManager-ECDSAが存在します。**
- CallManager-ECDSA証明書は、ITLファイルとCTLファイルの両方でCCM+TFTPの機能を備えています。
- コントローラ GUI または CLI を使用して **show ctl** または **show itl** コマンドを使用して、次の図に示すように、この情報を表示します。

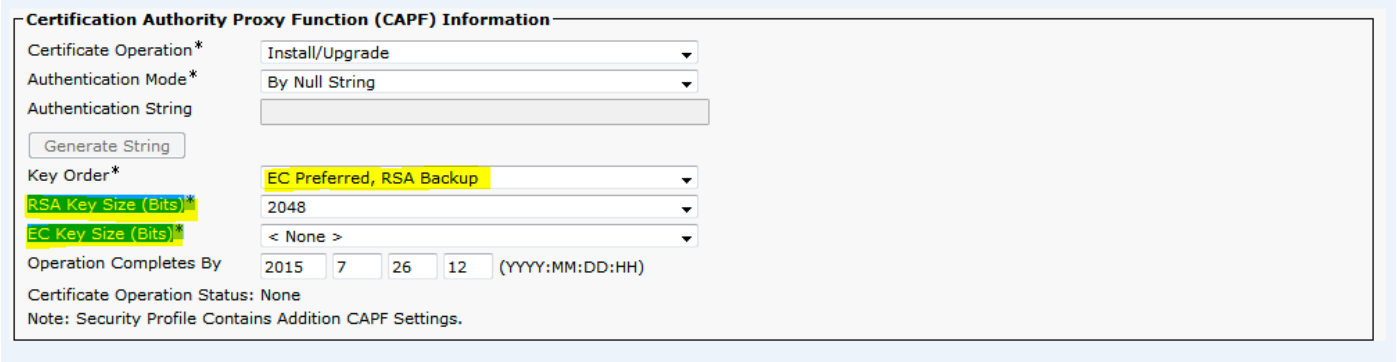
```
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1656
2       DNSNAME         2
3       SUBJECTNAME     65      CN=CUCM11Pub.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
4       FUNCTION        2       CCM+TFTP
5       ISSUERNAME      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コマンドを使用**してCTL**ファイルを生成できます。

認証局プロキシ機能

- CUCM 11のCertificate Authority Proxy Function(CAPF)バージョン3.0では、RSAとともにECキーサイズがサポートされています。
- 既存のCAPFフィールドに加えて提供される追加のCAPFオプションは、Key Order（キー順序）とEC Key Size（ビット）です。
- 既存のキーサイズ（ビット）オプションがRSAキーサイズ（ビット）に変更されました。
- [Key Order]では、RSA Only、EC Only、およびEC Preferred、RSAバックアップオプションがサポートされます。
- ECキーサイズは、256、384、および521ビットのキーサイズをサポートします。
- RSAキーサイズは、512、1024、および2048ビットをサポートします。
- [Key Order of RSA Only]を選択すると、[RSA Key Size]のみを選択できます。[ECのみ]を選択すると、[ECキーサイズ]のみを選択できます。[EC Preferred]で[RSA backup]を選択すると、[RSA]と[EC Key Size]の両方を選択できます。

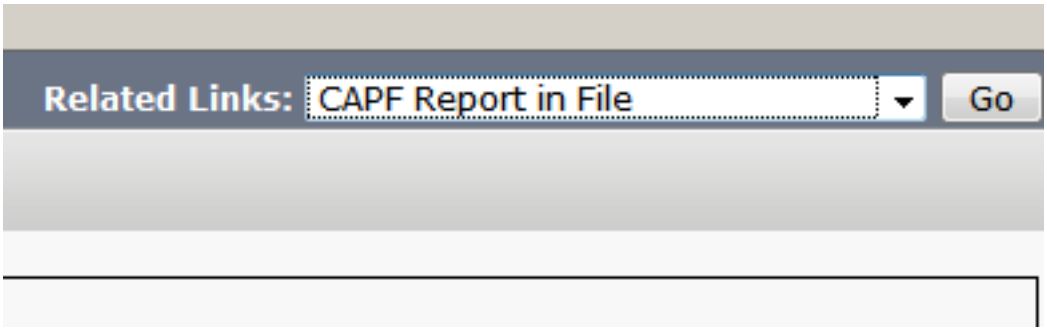




注：現在、CAPFバージョン3をサポートするシスコエンドポイントはないため、EC Onlyオプションは選択しないでください。ただし、後でECDSA Locally Significant Certificates(LSC)をサポートする必要がある管理者は、EC Preferred RSA Backupオプションを使用してデバイスを設定できます。エンドポイントがECDSA LSCのCAPFバージョン3をサポートし始めると、管理者はLSCを再インストールする必要があります。

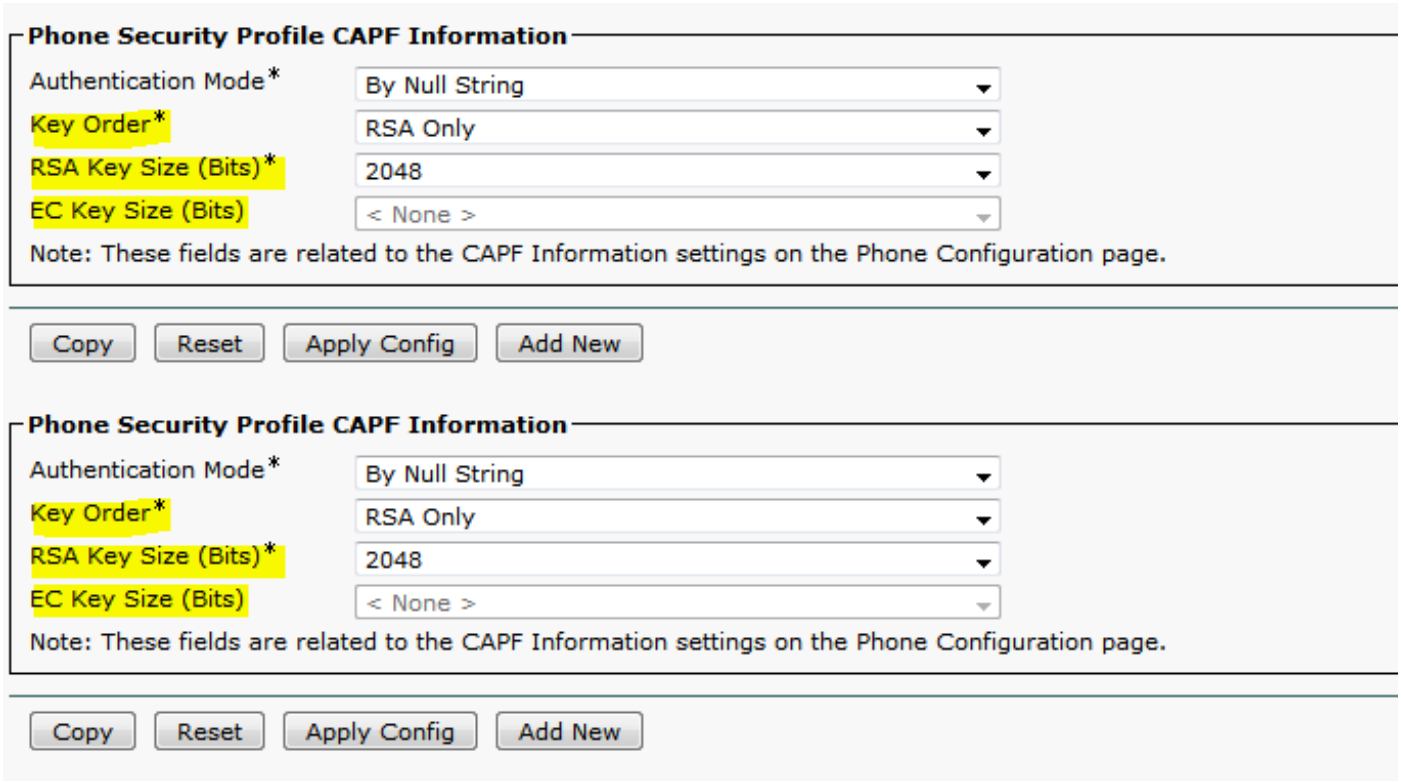
電話機、電話セキュリティプロファイル、エンドユーザ、およびアプリケーションユーザページのその他のCAPFオプションを次に示します。

[Device] > [Phone] > [Related Links]

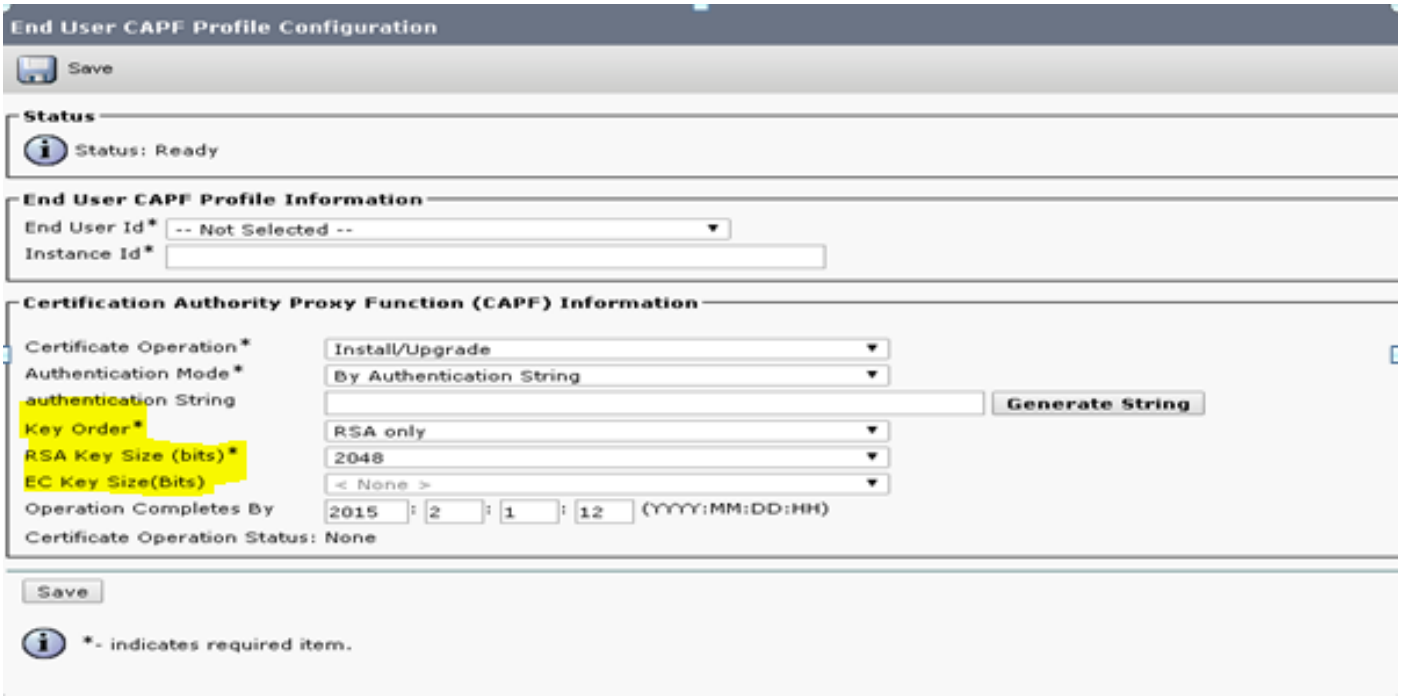


[システム(System)] > [セキュリティ(Security)] > [電話セキュリティプロファイル(Phone security profile)]に移動します

[User Management] > [User Settings] > [Application User CAPF Profile]

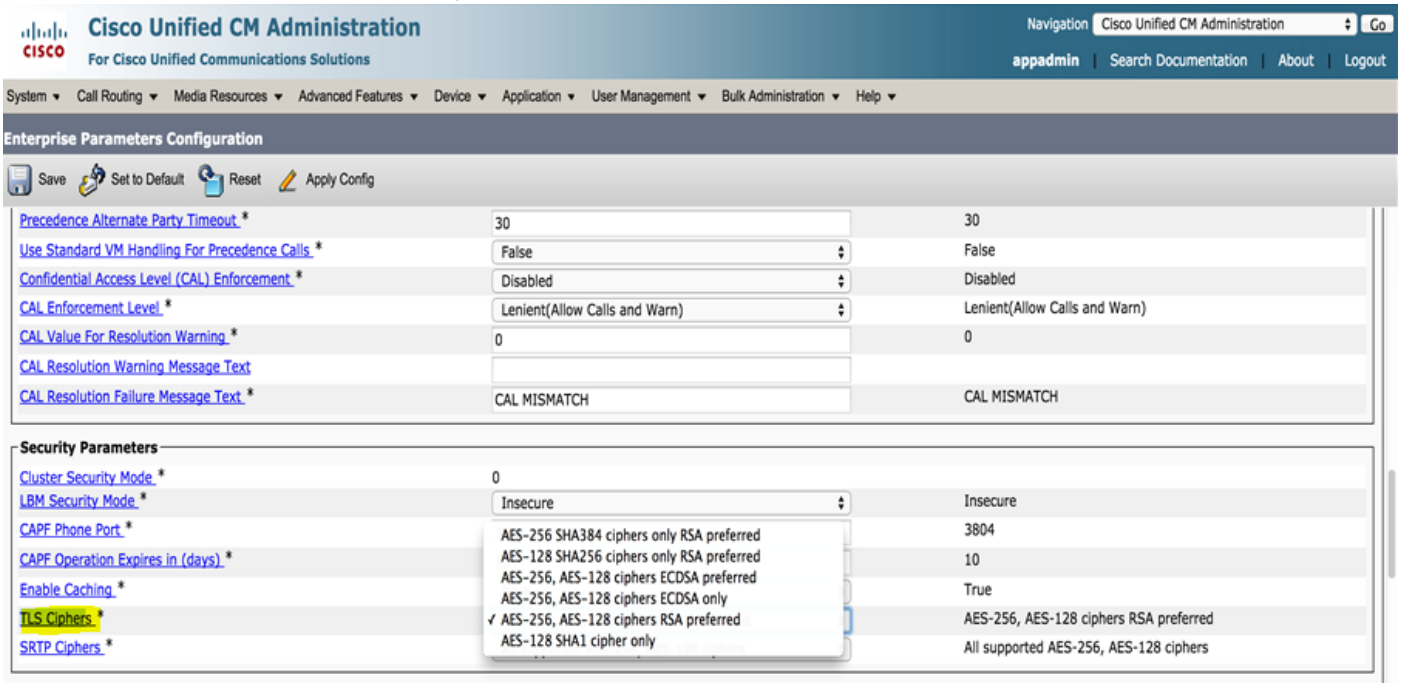


[User Management] > [User Settings] > [End User CAPF Profile]に移動します。



TLS暗号エンタープライズパラメータ

- エンタープライズパラメータTLS暗号は、ECDSA暗号をサポートするように更新されています。
- エンタープライズパラメータTLS暗号は、SIP回線、SIPトランク、およびセキュアCTIマネージャのTLS暗号を設定します。



SIP ECDSAのサポート

- Cisco Unified Communications Managerリリース11.0には、SIP回線およびSIPトランクインターフェイスのECDSAサポートが含まれています。
- Cisco Unified Communications Managerとエンドポイントの電話機またはビデオデバイスの間の接続はSIP回線接続であるのに対し、2つのCisco Unified Communications Manager間の

接続はSIPトランク接続です。
- すべてのSIP接続はECDSA暗号をサポートし、ECDSA証明書を使用します。

セキュアSIPインターフェイスは、次の2つの暗号をサポートするように更新されました。

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

SIPがTLS接続を行うシナリオは次のとおりです。

- SIPがTLSサーバとして機能するとき Cisco Unified Communications ManagerのSIPトランクインターフェイスが着信セキュアSIP接続のTLSサーバとして機能する場合、SIPトランクインターフェイスはCallManager-ECDSA証明書がディスク上に存在するかどうかを判断します。証明書がディスクに存在する場合、選択した暗号スイートがTLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256またはTLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- SIPがTLSクライアントとして機能するとき SIPトランクインターフェイスがTLSクライアントとして機能する場合、SIPトランクインターフェイスは、CUCM Enterprise Parameters **The TLS CiphersのTLS Ciphersフィールド（ECDSA ciphersオプションも含む）に基づいて、要求された暗号スイートのリストをサーバ送信します**。この設定は、TLSクライアント暗号スイートリストとサポートされる暗号スイートを優先順に決定します。

  注：
  - CUCMへの接続にECDSA暗号を使用するデバイスは、Identity Trust List(ITL)ファイルにCallManager-ECDSA証明書を含める必要があります。
  - SIPトランクインターフェイスは、ECDSA暗号スイートをサポートしていないクライアントからの接続、またはECDSAをサポートしていない以前のバージョンのCUCMでTLS接続が確立された場合のRSA TLS暗号スイートをサポートします。

Secure CTI Manager ECDSAのサポート

Secure CTI Managerインターフェイスは、次の4つの暗号をサポートするように更新されました。

- 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インターフェイスは、CallManager証明書とCallManager-ECDSA証明書の両方をロードします。これにより、Secure CTI Managerインターフェイスは、既存のRSA暗号とともに新しい暗号をサポートできます。

SIPインターフェイスと同様に、Cisco Unified Communications Managerの[エンタープライズパラメータTLS暗号(Enterprise Parameter TLS Ciphers)]オプションを使用して、CTI Managerセキュアインターフェイスでサポートされているの暗号を設定します。

設定のダウンロードのためのHTTPSサポート

- セキュアな設定のダウンロード（Jabberクライアントなど）のために、Cisco Unified Communications Managerリリース11.0は、以前のリリースで使用されていたHTTPおよび

TFTPインターフェイスに加えて、HTTPSをサポートするように拡張されています。
- 必要に応じて、クライアントとサーバの両方が相互認証を使用します。ただし、LSCを提示するには、ECDSA LSCおよび暗号化TFTP設定に登録されているクライアントが必要です。
- HTTPSインターフェイスは、CallManager証明書とCallManager-ECDSA証明書の両方をサーバ証明書として使用します。

注：
- CallManager、CallManager ECDSA、またはTomcat証明書を更新する場合は、TFTPサービスを非アクティブにして再アクティブ化する必要があります。
– ポート6971は、電話機で使用されるCallManager証明書およびCallManager-ECDSA証明書の認証に使用されます。
– ポート6972は、Jabberで使用されるTomcat証明書の認証に使用されます。

エントロピー

エントロピーはデータのランダム性を示す尺度であり、一般的な基準要件の最小しきい値を決定するのに役立ちます。強力な暗号化を実現するには、堅牢なエントロピー源が必要です。ECDSAなどの強力な暗号化アルゴリズムがエントロピーの弱いソースを使用している場合、暗号化を簡単に解除できます。

Cisco Unified Communications Managerリリース11.0では、Cisco Unified Communications Managerのエントロピーソースが改善されています。

Entropy Monitoring Daemonは、設定を必要としない組み込み機能です。ただし、Cisco Unified Communications Manager CLIを使用してオフにできます。

Entropy Monitoring Daemonサービスを制御するには、次のCLIコマンドを使用します。

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.

関連情報

- Cisco Unified Communications Managerセキュリティガイド、リリース11.5(1)
- テクニカル サポートとドキュメント – Cisco Systems