CUCM 11.0 次世代 暗号化-楕円曲線暗号解読法

目次

概要

この資料は高められた セキュリティおよび性能要件を満たすために概要を、Cisco Unified Communications Manager（CUCM）からの Next_Generation 暗号化（NGE）の設定 11.0 およびそれ以降、記述したものです

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 Call Manager セキュリティ 基本
- Cisco Call Manager 証明書管理

使用するコンポーネント

この文書に記載されている情報は Cisco CUCM 11.0 に edcsa 認証が CallManager（CallManagerEDCSA）のためにだけサポートされるところで、基づいています

注: CUCM 11.5 前にサポート TomcatEDCSA 認証同様に

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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

この資料も EDCSA 認証をサポートするバージョンおよびこれらのソフトウェア製品と使用することができます:

- Cisco IM および存在 11.5
- Cisco Unity Connection 11.5

背景説明

楕円曲線暗号解読法（ECC）は有限 な フィールド上の楕円曲線の代数構造に基づいて公開キー暗号化へアプローチです。 非 ECC 暗号解読法と比べた主要な 利点の 1 つは小型のキーによって提供される同じセキュリティレベルです。

共通基準は評価されるセキュリティ機能がソリューションの内で正しく動作するという保証を提供します。 これは広範なドキュメント必要条件をテストし、満たすことによって実現します。

共通基準認識配置（CCRA）によって 26 ヶ国につき受け入れられ、世界的にサポートされて

Cisco Unified Communications Manager リリース 11.0 サポート楕円曲線デジタル署名アルゴリズム（ECDSA）認証。

これらの認証が RSA ベースの認証より強く、共通基準（CC）認証がある製品に必要となります。 分類されたシステム（CSfC）プログラムのための米国政府商業ソリューションは CC 認証を必要とし、そう、Cisco Unified Communications Manager リリース 11.0 に前に含まれています。

ECDSA 認証はこれらのエリアで既存の RSA 認証と共に利用できます:

- 証明書管理
- Certificate Authority Proxy Function（CAPF）
- Transport Layer Security （TLS）トレース
- SIP 接続を保護して下さい
- コンピュータ テレフォニー インテグレーション （CTI）マネージャ
- HTTP
- エントロピー

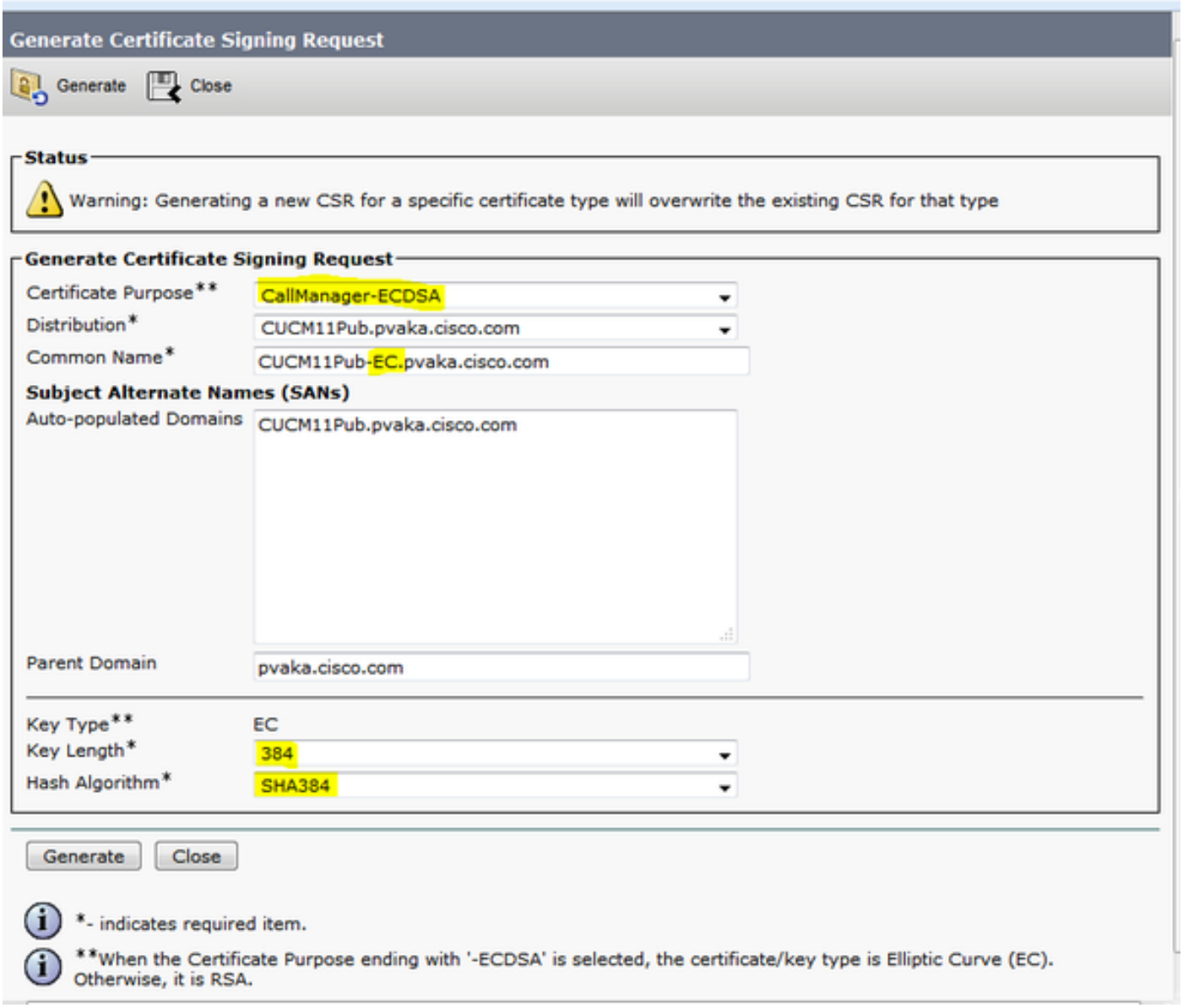
次の セクションは上記の 7 つのエリアのそれぞれで詳細な情報を提供します。

証明書管理

EC 暗号化の認証の生成

EC 暗号化の CallManager 認証を生成する CUCM 11.0 からの ECC のためのサポート前に

- イメージに示すように利用可能 な新しいオプション **CallManagerECDSA**。
- Common Name のホスト部分が終了するように要求しますか。EC、CallManager 認証と同じ Common Name を持っていることを防ぐため。
- マルチ サーバ SAN 認証の場合には、これは終了する必要がありますか。EC ms.



- 自己署名証明書 要求両方ともおよび CSR は EC キーサイズによって限界をハッシュ アルゴリズム選択要求します。
- 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 のどちらである場合もあります。 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 のどれである場合もあります。 EC 521 キーサイズに関しては唯一のオプションは SHA512 です。
- DEFAULT 鍵サイズは 384 であり、デフォルト ハッシュアルゴリズムは廃棄する変更することができる SHA384 です。 利用可能 な オプションは選択されたキーサイズに基づいています。

CLI 設定

CallManagerECDSA と指名される新しい認証 ユニットは CLI コマンドのために追加されました

- 証明書 regen [ユニット]設定 して下さいか。 自己署名証明書を再生します

```
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)?
```

- 証明書インポートを所有します設定 して下さい|信頼[ユニット]か。 輸入高 CA 署名入り認証

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

- CSR ジェネレーション[ユニット]設定 して下さいか。 規定 された ユニットのための認証署名 request (CSR) を生成します

```
admin:set csr gen CallManager-ECDSA

Successfully Generated CSR  for CallManager-ECDSA

admin:
```

- 一定バルク エクスポート|強化して下さい|tftp をインポートして下さいか。 tftp がユニット名前のとき、CallManagerECDSA 認証は一括操作の CallManager RSA 認証と自動含まれている得ます。

CTL および ITL ファイル:

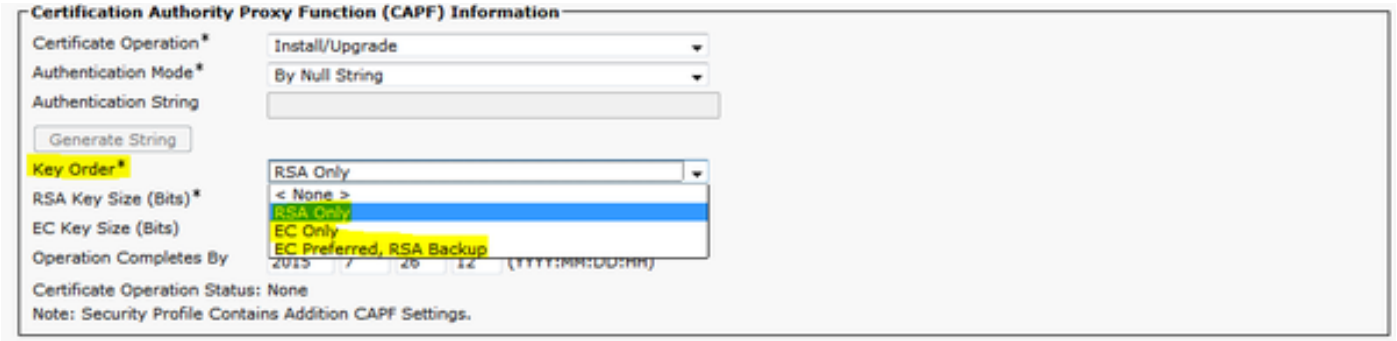
- CTL および ITL 両方ファイルは CallManagerECDSA 提供を過します。
- CallManagerECDSA 認証に ITL および CTL 両方ファイルで CCM+TFTP の機能があります。
- 示すか、ctl をまたは示しますイメージに示すようにこの情報を表示する itl コマンドを使用できます:

```
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.
```

- CTL ファイルを生成するのに **utils ctl アップデートを**使用できます。

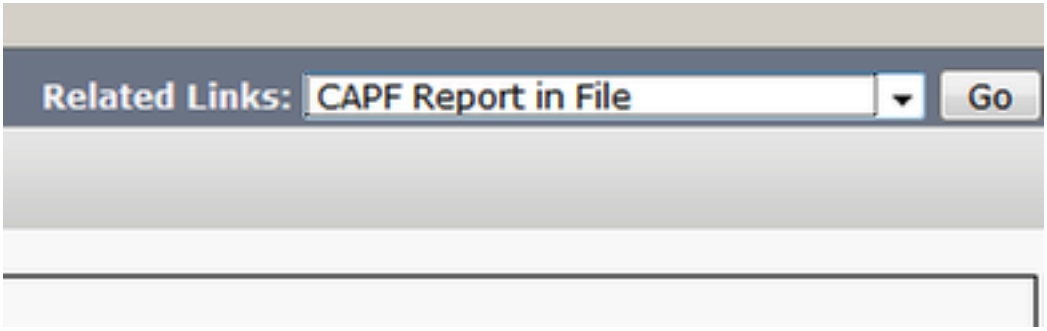
Certificate Authority Proxy Function（CAPF）

- CUCM 11 の CAPF バージョン 3.0 は RSA と共に EC キーサイズにサポートを提供します。
- 既存の CAPF フィールドに加えて提供される追加 CAPF オプションはキー順序および EC キーサイズ（ビット）です。
- 既存のキーサイズ（ビット）オプションは RSA キーサイズ（ビット）に変更されました。
- キー順序は RSA だけ、EC 好まれるおよび EC だけにサポートを RSA バックアップ オプション提供します。
- EC キーサイズは 256、384 のおよび 521 ビットのキーサイズにサポートを提供します。
- RSA キーサイズは 512、1024 のおよび 2048 ビットにサポートを提供します
- キー場合の RSA だけの順序は RSA キーサイズだけが選択することができます、選択されます。 EC だけが選択される時、EC キーサイズだけが選択することができます。 好まれる EC が RSA バックアップ、選択されるとき RSA および EC 両方キーサイズは選択することができます。



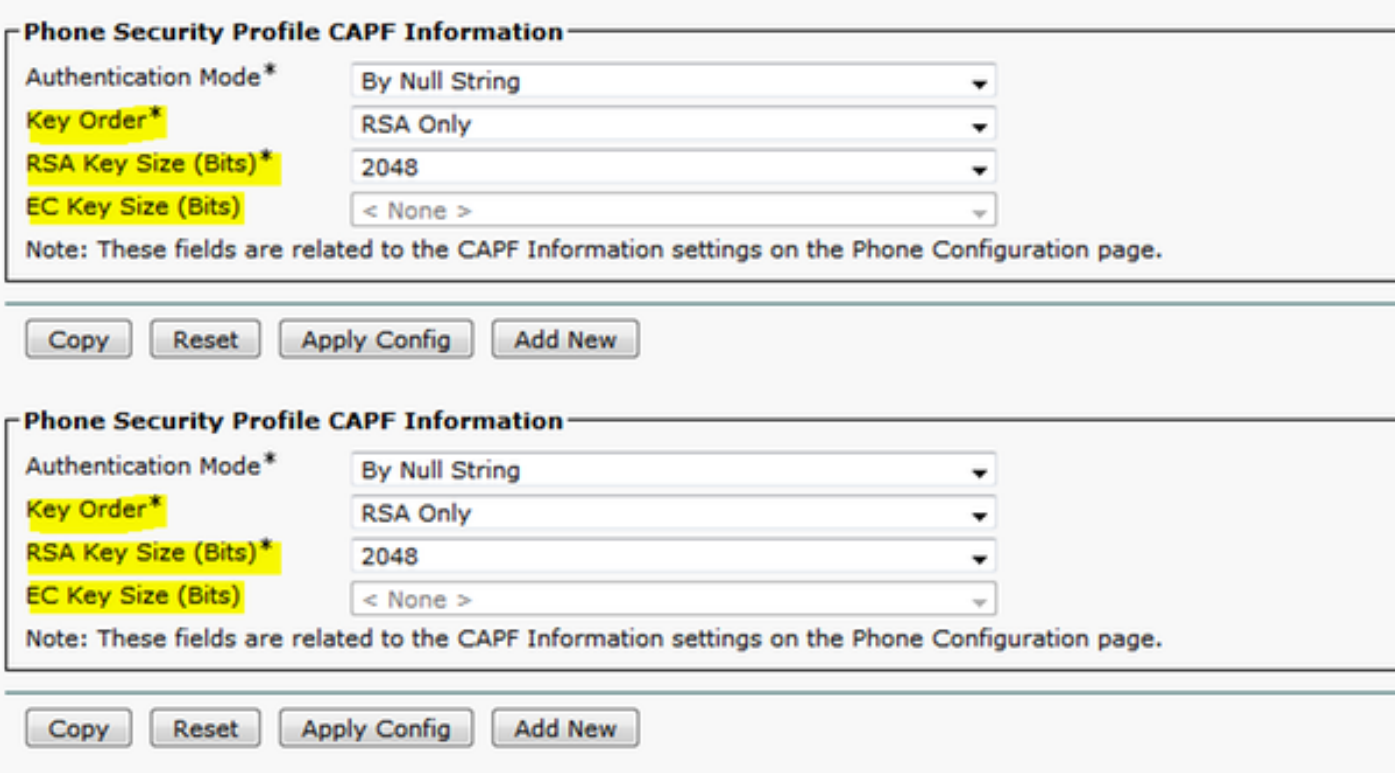
電話、電話セキュリティプロファイル、エンドユーザおよびアプリケーションのユーザー ページのための追加 CAPF オプション

Device > Phone > 関連リンク

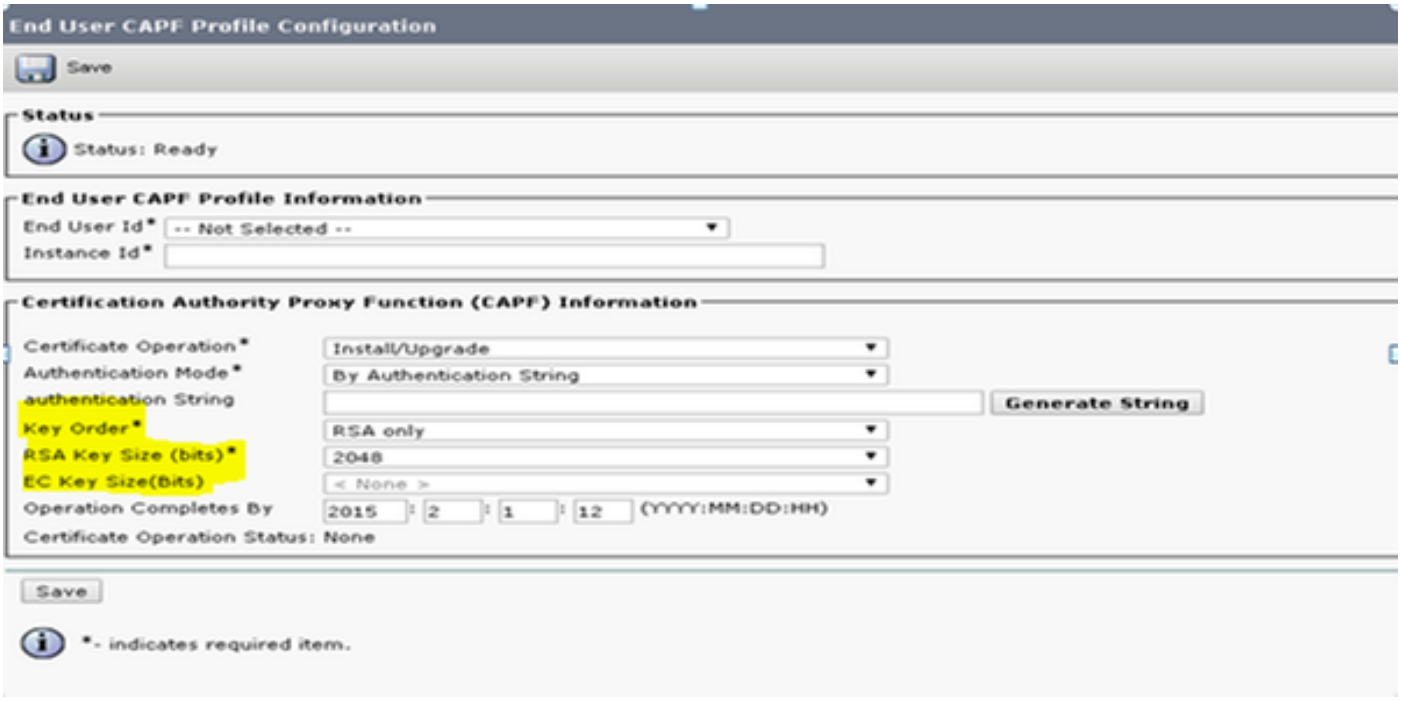


システム > Security > 電話セキュリティプロファイルへのナビゲート

ユーザマネージメント > ユーザ設定 > アプリケーションのユーザー CAPF プロファイル

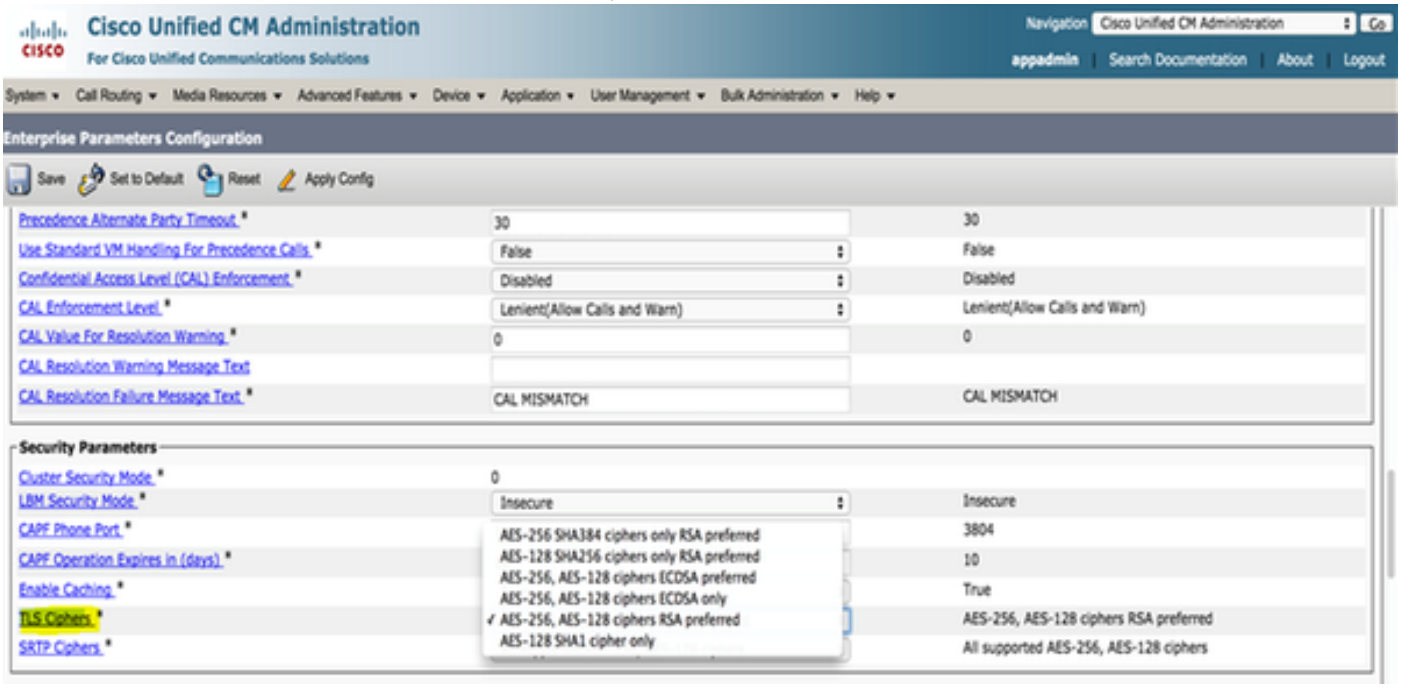


ユーザマネージメント > ユーザ設定 > エンドユーザ CAPF プロファイルへの Navigaet。



TLS はエンタープライズ パラメータを暗号化します

- 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ためにアップデートされました。
- エンタープライズ パラメータ TLS 暗号は今 SIP 行、SIP トランクおよびセキュア CTI マネージャのための TLS 暗号を設定 します。



SIP ECDSA サポート

- Cisco Unified Communications Manager リリース 11.0 は SIP 行および SIP トランクインターフェイスのための ECDSA サポートが含まれています。
- Cisco Unified Communications Manager およびエンドポイント電話またはビデオデバイス間の接続は 2 人の Cisco Unified Communications Manager 間の接続が SIP 中継接続である一方

SIP 行接続です。
- すべての SIP 接続は ECDSA 暗号をサポートし、ECDSA 認証を使用します。

セキュア SIP インターフェイスはこれら二つの暗号をサポートするためにアップデートされました

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

これらは SIP が（Transport Layer Security） TLS 接続をするときシナリオです:

- SIP が TLS サーバとして機能する時

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 接続のための TLS サーバとして機能するとき、SIP トランクインターフェイスはかどうかディスクで存在 する CallManagerECDSA 認証確認しました。 指定暗号スイートがある場合ディスクで存在 する 認証が SIP トランクインターフェイス CallManagerECDSA 認証を使用すれば

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 か
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

- SIP が TLS クライアントとして機能する時

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とき、SIP トランクインターフェイスは **TLS が暗号化する** CUCM エンタープライズ パラメータの TLS 暗号フィールド基づいてサーバに（また ECDSA が暗号化するオプションを含まれている）に要求された暗号スイートのリストを送ります。 この設定はプリファレンスの順で TLS クライアント 暗号スイート リストおよびサポートされた暗号スイートを判別します。

注: 1. CUCM への接続をするのに ECDSA 暗号を使用するデバイスは識別信頼リスト（ITL）ファイルの CallManagerECDSA 認証を備えなければなりません。

注: 2. ECDSA 暗号スイートをサポートしないまたはとき CUCM の以前のバージョンが付いている TLS 接続が確立されるクライアントからの接続のための SIP トランクインターフェイス サポート RSA TLS 暗号スイートは、それ ECDSA をサポートしません。

セキュア CTI マネージャ ECDSA サポート

セキュア CTI マネージャ インターフェイスはこの 4 つの暗号をサポートするためにアップデートされました:

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

- セキュア CTI マネージャ インターフェイス ロード CallManager および CallManagerECDSA 認証両方。 これはセキュア CTI マネージャ インターフェイスが既存の RSA 暗号と共に新し

い暗号をサポートするようにします。
- SIP インターフェイスに類似した、Cisco Unified Communications Manager のエンタープライズ パラメータ TLS 暗号オプションが CTI マネージャ セキュア な インターフェイスでサポートされる TLS 暗号を設定するのに使用されています。

設定ダウンロードのための HTTPS サポート

- 安全な設定ダウンロード (たとえば以前のリリースで使用した HTTP および TFTP インターフェイスに加えて HTTPS をサポートするために Jabber クライアント) に関しては、Cisco Unified Communications Manager リリース 11.0 は高められます。
- 必要であれば、両方クライアント および サーバ 使用 相互認証。 ただし、ECDSA LSCs および TFTP 暗号化されたコンフィギュレーションと登録されるクライアントが LSC を示すために必要となります。
- HTTPS インターフェイスはサーバ証明として CallManager および CallManagerECDSA 認証を両方使用します。

  注: 1. CallManager、CallManager ECDSA、または Tomcat 認証をアップデートするとき、TFTPサービスを無効にし、再稼働して下さい。

  注: 2.ポート 6971 は電話によって使用される CallManager および CallManagerECDSA 認証の認証のために使用されます。

  注: 3.ポート 6972 は Jabber によって使用される Tomcat 認証の認証のために使用されます。

エントロピー

エントロピーはデータの偶発性のメジャーで、必要条件よくある基準ののための最小 しきい値の判別で助けます。 強化暗号化を持つために、エントロピーの強いもとが必要となります。 強化暗号化 アルゴリズムが、ECDSA のような、エントロピーの弱いもとを使用すれば、暗号化は容易に壊すことができます。

Cisco Unified Communications Manager リリース 11.0 では、Cisco Unified Communications Manager におけるエントロピー ソースは改善されます。

エントロピー モニタリング デーモン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 を通してそれを消すことができます。

エントロピー モニタリング デーモン サービスを制御する次の CLI コマンドを使用して下さい:

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

- http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/11_5_1/secugd/CUCM_BK_SEE2CFE1_00_cucm-security-guide-1151/CUCM_BK_SEE2CFE1_00_cucm-security-guide-1151_chapter_011.html#CUCM_RF_C0383C35_00l
- テクニカルサポートとドキュメント - Cisco Systems