Criptografia de última geração CUCM 11.0 - Criptografia de curva elíptica

Contents

Introduction

Este documento descreve a configuração da Next Generation Encryption (NGE) do Cisco Unified Communications Manager (CUCM) 11.0 e posterior para atender aos requisitos avançados de segurança e desempenho.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Princípios básicos de segurança do Cisco CallManager
- Gerenciamento de certificado do Cisco CallManager

Componentes Utilizados

As informações neste documento são baseadas no Cisco CUCM 11.0, em que os certificados Elliptic Curve Digital Signature Algorithm (ECDSA) só são suportados para o CallManager (CallManager-ECDSA).

> **Note**: O CUCM 11.5 e posterior também suporta certificados tomcat-ECDSA.

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.

Produtos Relacionados

Este documento também pode ser usado com estes produtos de software e versões que suportam certificados ECDSA:

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

Informações de Apoio

A criptografia da curva elíptica (ECC) é uma abordagem à criptografia de chave pública baseada na estrutura algébrica das curvas elípticas em campos finitos. Um dos principais benefícios em comparação à criptografia não-ECC é o mesmo nível de segurança fornecido por chaves de tamanho menor.

Common Criteria (CC) oferece garantia de que os recursos de segurança operam corretamente na solução que está sendo avaliada. Isso é obtido por meio de testes e do cumprimento de requisitos abrangentes de documentação.

Éaceite e apoiado por 26 países em todo o mundo através do Common Criteria Recognition Agreement (CCRA).

O Cisco Unified Communications Manager versão 11.0 suporta certificados Elliptic Curve Digital Signature Algorithm (ECDSA).

Esses certificados são mais fortes que os certificados baseados em RSA e são necessários para produtos que possuem certificações CC. O programa de soluções comerciais para sistemas classificados (CSfC) do governo dos EUA requer a certificação CC e, portanto, está incluído no Cisco Unified Communications Manager Release 11.0 e posterior.

Os certificados ECDSA estão disponíveis junto com os certificados RSA existentes nessas áreas:

- Gerenciamento de certificado
- Função de proxy da autoridade de certificação (CAPF)
- Rastreamento TLS (Transport Layer Security)
- Conexões Secure Session Initiation Protocol (SIP)
- Gerente de integração de telefonia/computador (CTI)
- HTTP
- Entropia

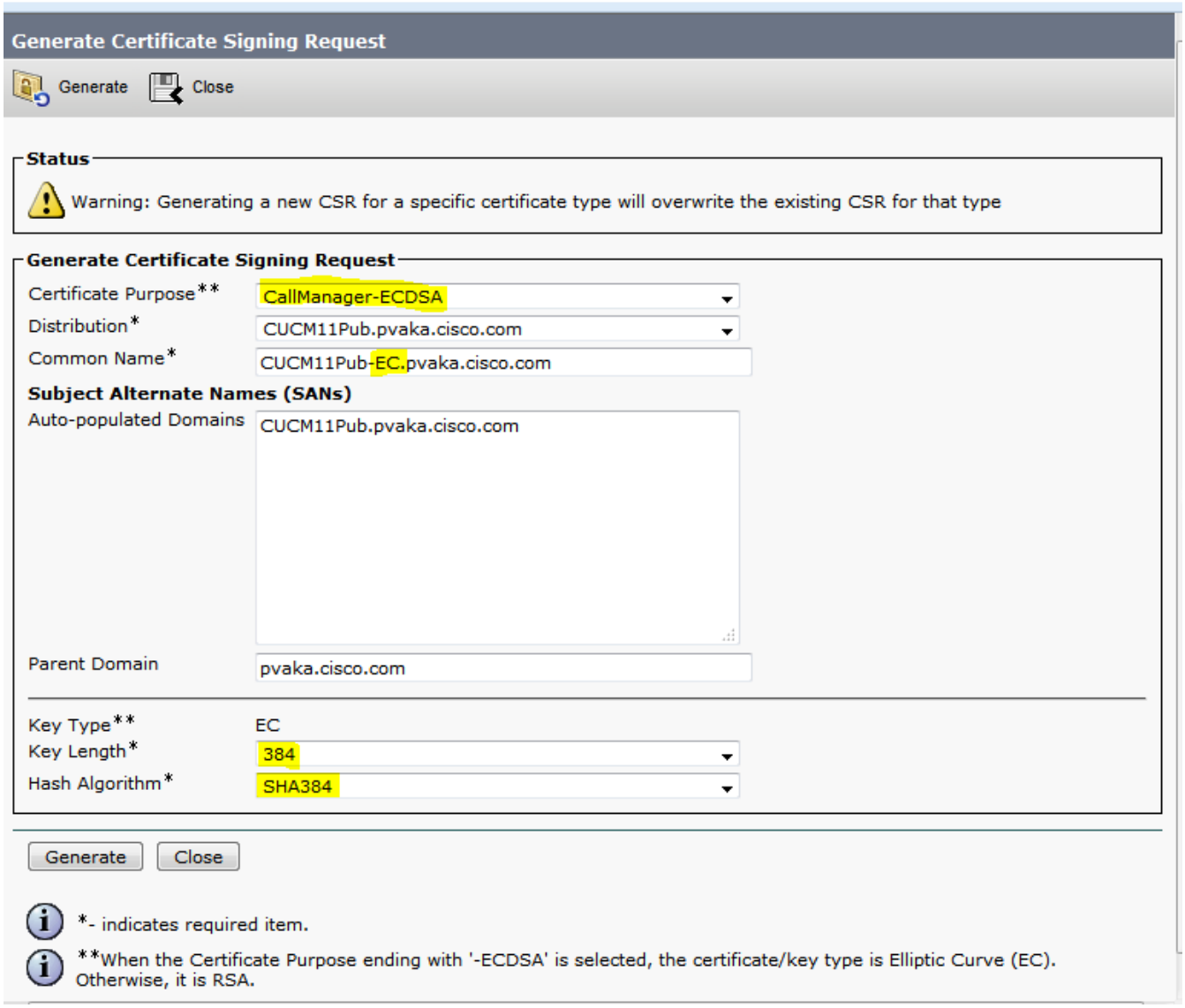
As próximas seções fornecem informações mais detalhadas sobre cada uma dessas sete áreas.

Gerenciamento de certificado

Gerar certificados com criptografia de curva elíptica

Suporte para ECC do CUCM 11.0 e posterior para gerar certificado do CallManager com criptografia de Curva Elíptica (EC):

- A nova opção **CallManager-ECDSA** está disponível como mostrado na imagem.
- Requer que a parte do host do nome comum termine em **-EC**. Isso evita ter o mesmo nome comum do certificado **CallManager**.
- No caso do certificado SAN de vários servidores, ele deve terminar em **-EC-ms**.



- Tanto a solicitação de certificado autoassinado quanto a solicitação CSR limitam as opções de algoritmo de hash dependendo do tamanho da chave EC.
- Para um tamanho de chave EC 256, o algoritmo de hash pode ser SHA256, SHA384 ou SHA512. Para um tamanho de chave EC 384, o algoritmo de hash pode ser SHA384 ou SHA512. Para um tamanho de chave EC 521, a única opção é SHA512.
- O tamanho da chave padrão é 384 e o algoritmo de hash padrão é SHA384, que pode ser alterado. As opções disponíveis baseiam-se no tamanho da chave escolhida.

Configuração de CLI

Uma nova unidade de certificado chamada **CallManager-ECDSA** foi adicionada para os comandos CLI

- set cert regen [unit] - regenera certificado autoassinado

```
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] - importa o certificado assinado da AC

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

- set csr gen [unit] - gera solicitação de assinatura de certificado (CSR) para a **unidade** especificada

```
admin:set csr gen CallManager-ECDSA

Successfully Generated CSR  for CallManager-ECDSA

admin:
```

- set bulk export|consolidate|import tftp - Quando tftp é o nome da unidade, os certificados CallManager-ECDSA são incluídos automaticamente nos certificados RSA do CallManager em operações em massa.

Arquivos CTL e ITL

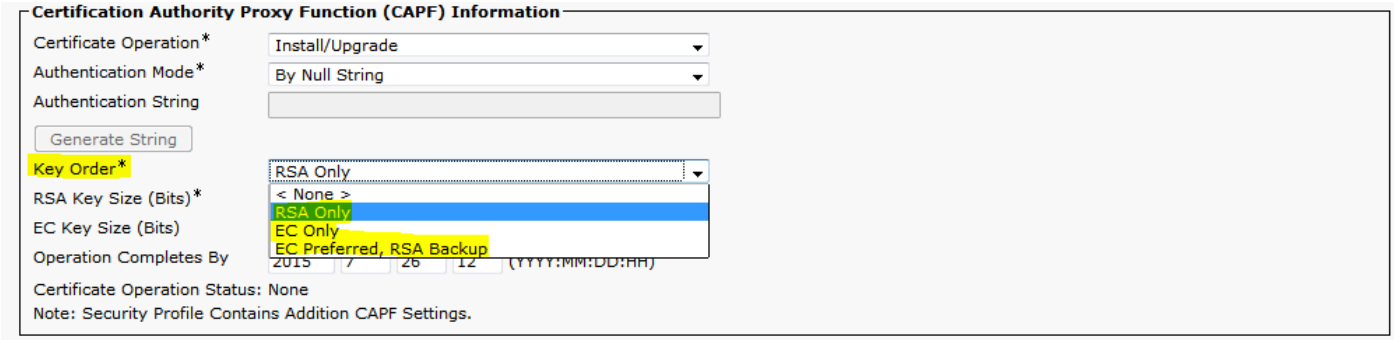
- Tanto os arquivos da lista de confiança de certificado (CTL) como da lista de confiança de identificação (ITL) têm o **CallManager-ECDSA** presente.
- O certificado CallManager-ECDSA tem a Função CCM+TFTP nos arquivos ITL e CTL.
- Você pode usar o comando **show ctl** or **show itl** para exibir essas informações como mostrado nesta imagem:

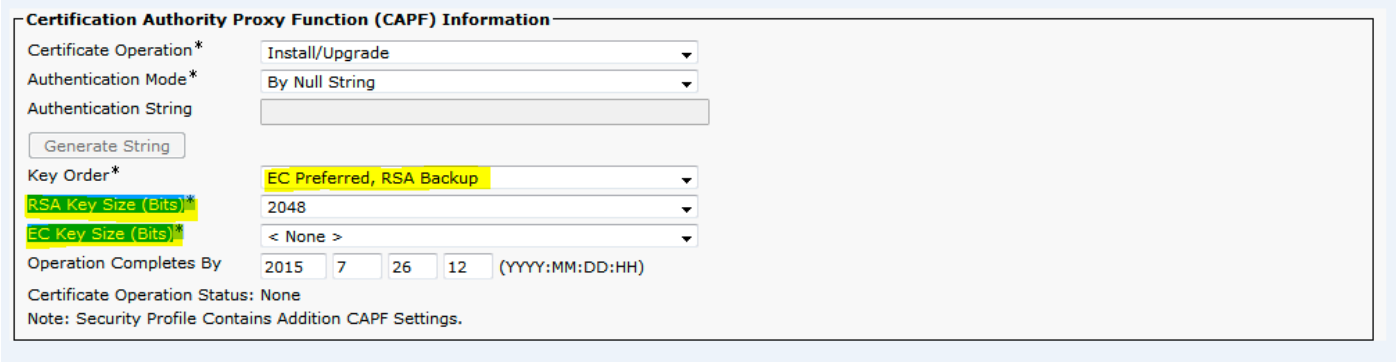
```
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1656
2       DNSNAME         2
3       SUBJECTNAME     65      CN=CUCM11Pub.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
4       FUNCTION        2       CCM+TFTP
5       ISSUERNAME 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

- Você pode usar o comando **utils ctl update** para gerar o arquivo CTL.

Função de Proxy da Autoridade de Certificação

- A versão 3.0 do CAPF (Certificate Authority Proxy Function) no CUCM 11 oferece suporte para Tamanhos de chave EC junto com RSA.
- As opções CAPF adicionais fornecidas além dos campos CAPF existentes são: Ordem principal e Tamanho da chave EC (bits).
- A opção Key Size (bits) existente foi alterada para RSA Key Size (bits).
- O pedido principal fornece suporte para as opções de backup RSA apenas RSA, EC apenas e EC preferido, RSA.
- O tamanho da chave EC oferece suporte para tamanhos de chave de 256, 384 e 521 bits.
- O tamanho da chave RSA oferece suporte para 512, 1024 e 2048 bits.
- Quando a opção Key Order of RSA Only (Ordem principal somente RSA) é selecionada, somente o RSA Key Size (Tamanho da chave RSA) pode ser selecionado. Quando EC apenas é selecionado, somente EC Key Size (Tamanho da chave EC) pode ser selecionado. Quando EC preferido, o backup RSA é selecionado, RSA e EC Key Size podem ser selecionados.

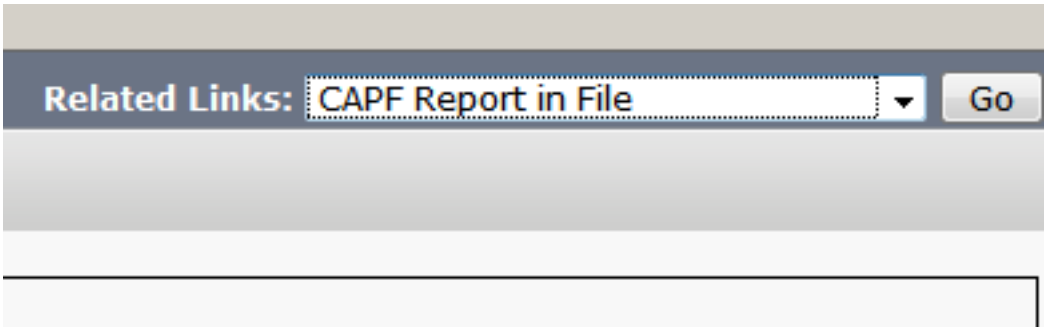




> **Note**: No momento, nenhum endpoint da Cisco oferece suporte ao CAPF Versão 3, portanto, não selecione a opção EC Only (Somente EC). No entanto, os administradores que desejam oferecer suporte a certificados localmente significativos (LSCs) ECDSA posteriormente podem configurar seus dispositivos com a opção EC Preferred RSA Backup. Quando os endpoints começam a oferecer suporte à versão 3 do CAPF para LSCs ECDSA, os administradores precisam reinstalar seu LSC.

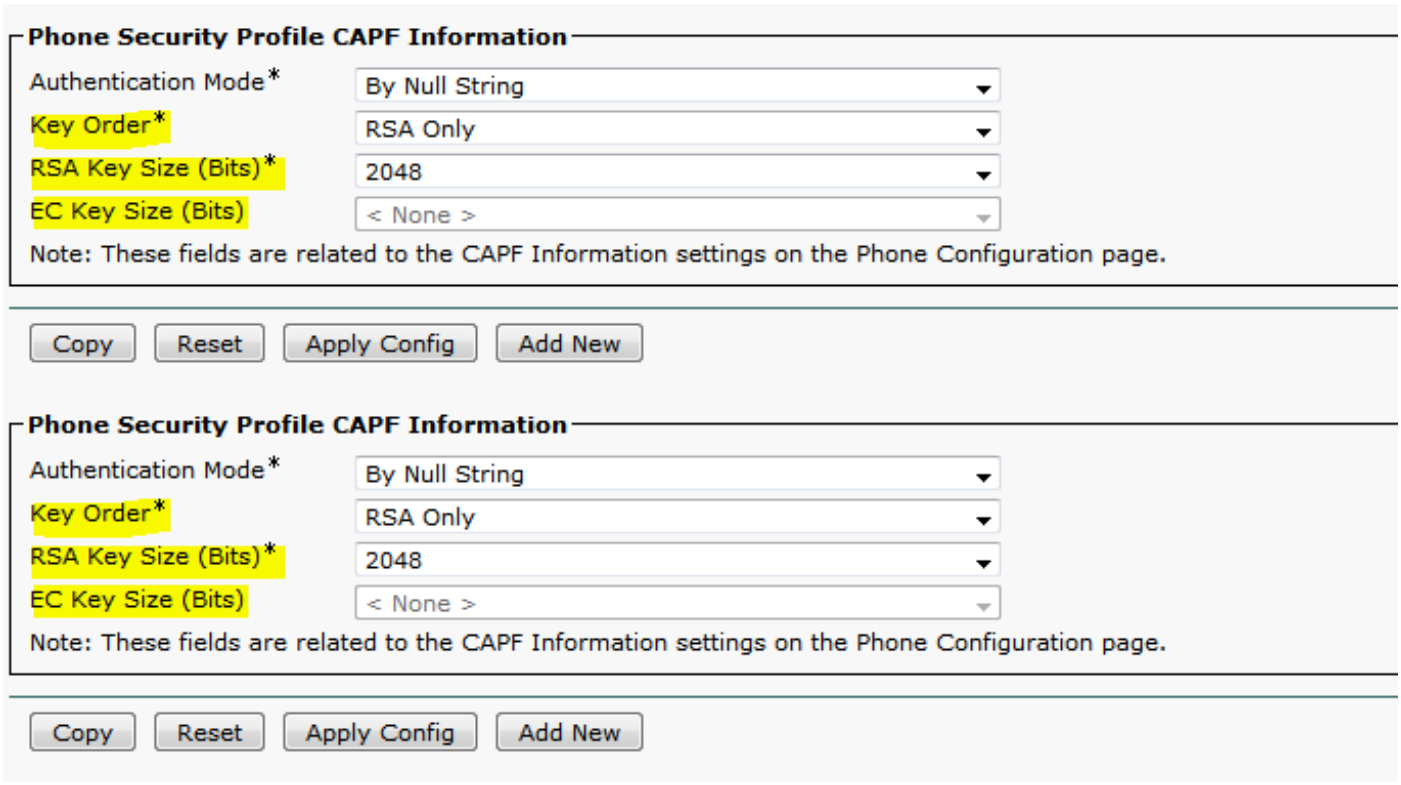
As opções CAPF adicionais para telefone, perfil de segurança do telefone, usuário final e páginas de usuário do aplicativo são mostradas aqui:

Dispositivo > Telefone > Links Relacionados

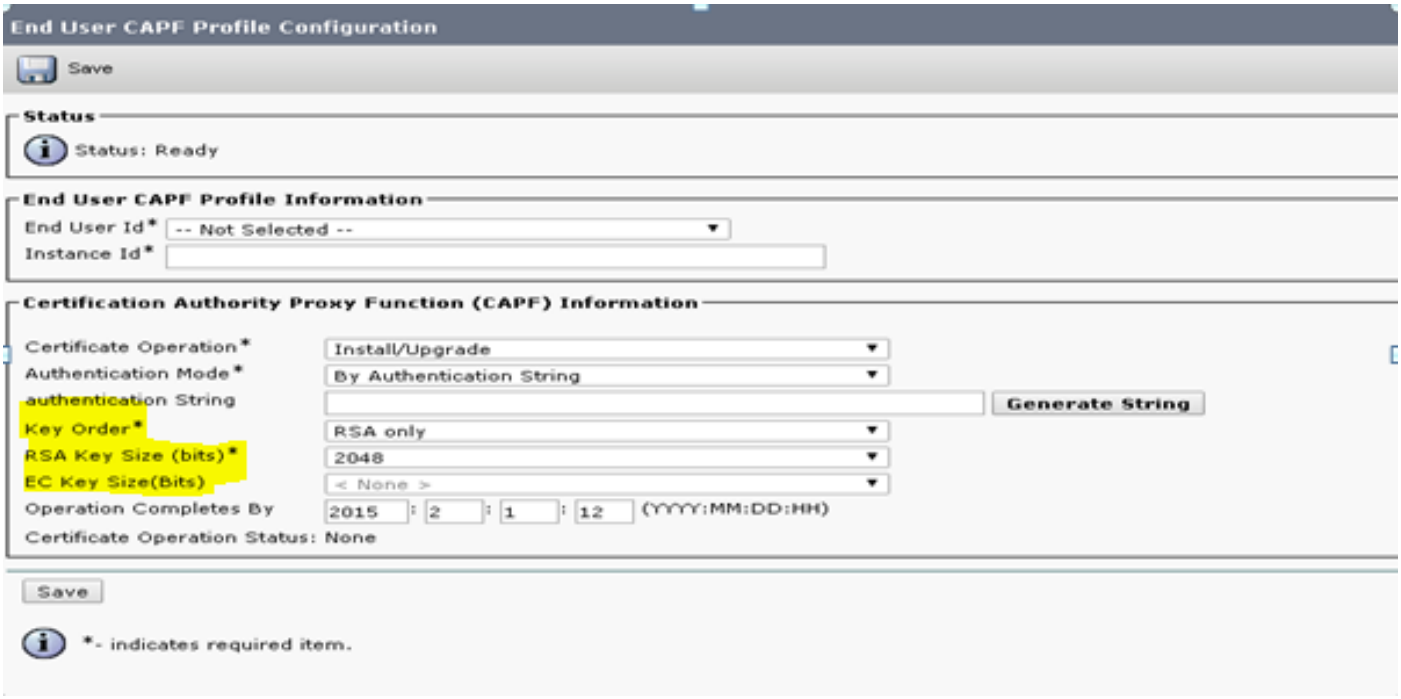


Navegue até **Sistema > Segurança > Perfil de segurança do telefone**

Gerenciamento de usuário > Configurações do usuário > Perfil CAPF do usuário do aplicativo

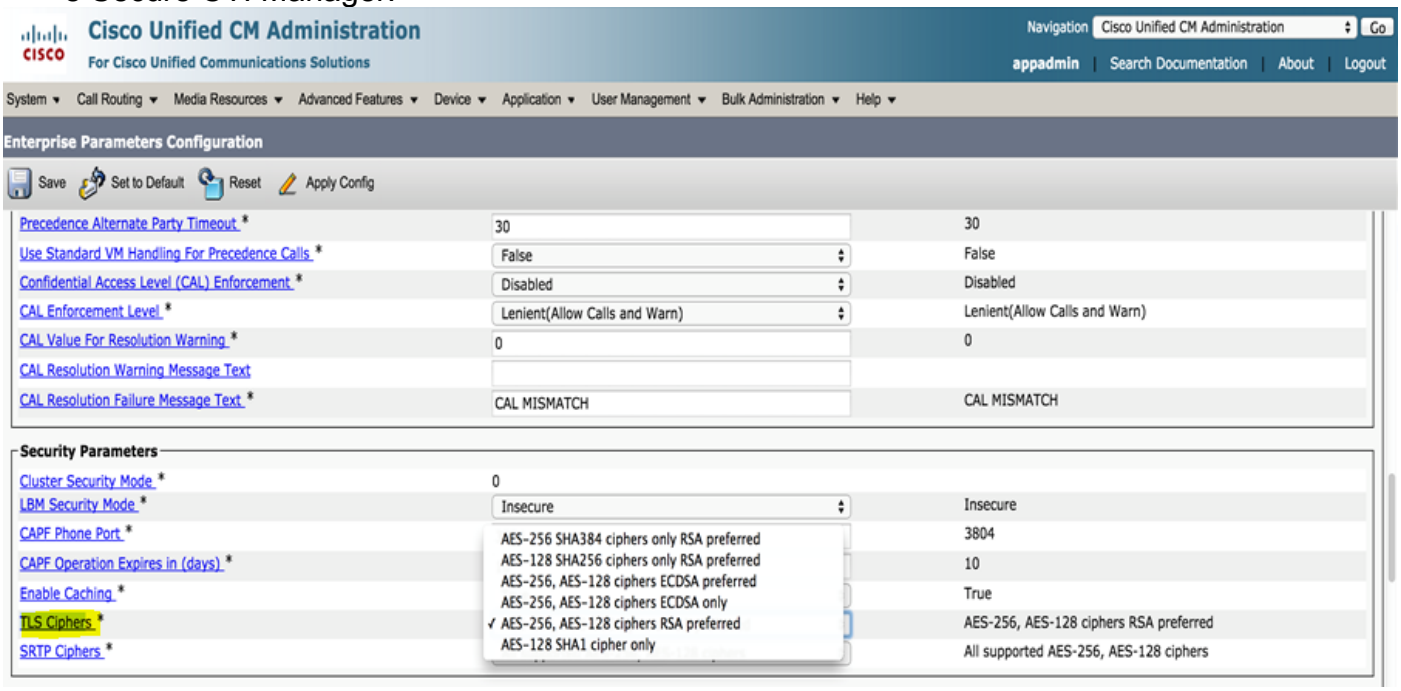


Navegue até **User Management > User Settings > End User CAPF Profile.**



Parâmetros corporativos de cifras TLS

- O parâmetro Enterprise TLS Ciphers foi atualizado para suportar ECDSA Ciphers.
- O parâmetro empresarial TLS Ciphers agora define os TLS Ciphers para SIP Line, SIP Trunk e Secure CTI Manager.



Suporte a SIP ECDSA

- O Cisco Unified Communications Manager versão 11.0 inclui suporte ECDSA para linhas SIP e interfaces de tronco SIP.
- A conexão entre o Cisco Unified Communications Manager e um telefone ou dispositivo de vídeo de endpoint é uma conexão de linha SIP, enquanto a conexão entre dois Cisco Unified Communications Managers é uma conexão de tronco SIP.

- Todas as conexões SIP suportam cifras ECDSA e usam certificados ECDSA.

A interface SIP segura foi atualizada para suportar estes dois cifras:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

Estes são os cenários em que o SIP faz conexões TLS:

- Quando o SIP atua como um servidor TLS Quando a interface de tronco SIP do Cisco Unified Communications Manager atua como um servidor TLS para conexão SIP segura de entrada, a interface de tronco SIP determina se o certificado CallManager-ECDSA existe no disco. Se o certificado existir no disco, a interface de tronco SIP usa o certificado CallManager-ECDSA se o conjunto de cifras selecionado forTLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ou TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- Quando o SIP atua como um cliente TLS Quando a interface de tronco SIP atua como um cliente TLS, a interface de tronco SIP envia uma lista de suítes de cifras solicitadas ao servidor com base no campo TLS Ciphers (que também inclui a opção de cifras ECDSA) nos Parâmetros do CUCM Enterprise **The TLS Ciphers**. Essa configuração determina a lista de pacotes de cifras do cliente TLS e os conjuntos de cifras suportados na ordem de preferência.

  Notas:
  - Os dispositivos que usam uma cifra ECDSA para fazer uma conexão com o CUCM devem ter o certificado CallManager-ECDSA em seu arquivo de Lista de Confiança de Identidade (ITL).
  - A interface de tronco SIP suporta as suítes de cifras RSA TLS para conexões de clientes que não suportam pacotes de cifras ECDSA ou quando uma conexão TLS é estabelecida com uma versão anterior do CUCM, que não suportam ECDSA.

Suporte ECDSA do Secure CTI Manager

A interface do Secure CTI Manager foi atualizada para suportar estes quatro cifras:

- 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

A interface do Secure CTI Manager carrega o certificado do CallManager e do CallManager-ECDSA. Isso permite que a interface do Secure CTI Manager ofereça suporte aos novos cifras juntamente com a cifra RSA existente.

Semelhante à interface SIP, a opção Enterprise Parameter TLS Ciphers no Cisco Unified Communications Manager é usada para configurar as cifras TLS suportadas na interface segura do CTI Manager.

Suporte HTTPS para download de configuração

- Para download de configuração segura (por exemplo, clientes Jabber), o Cisco Unified Communications Manager Release 11.0 é aprimorado para suportar HTTPS além das interfaces HTTP e TFTP que foram usadas nas versões anteriores.

- Se necessário, o cliente e o servidor usam autenticação mútua. No entanto, os clientes que estão inscritos com as configurações de ECDSA LSCs e de Encrypted TFTP são necessários para apresentar seu LSC.
- A interface HTTPS usa os certificados CallManager e CallManager-ECDSA como certificados de servidor.

Notas:
- Ao atualizar os certificados CallManager, CallManager ECDSA ou Tomcat, você deve desativar e reativar o serviço TFTP.
- A porta 6971 é usada para autenticação dos certificados CallManager e CallManager-ECDSA, usados por telefones.
- A porta 6972 é usada para a autenticação dos certificados Tomcat, usados pelo Jabber.

Entropia

A entropia é uma medida de aleatoriedade de dados e ajuda a determinar o limite mínimo para requisitos de critérios comuns. Para ter criptografia forte, é necessária uma fonte robusta de entropia. Se um algoritmo de criptografia forte, como o ECDSA, usar uma fonte fraca de entropia, a criptografia pode ser facilmente quebrada.

No Cisco Unified Communications Manager versão 11.0, a fonte de entropia do Cisco Unified Communications Manager é aprimorada.

Entropy Monitoring Daemon é um recurso interno que não exige configuração. Entretanto, você pode desligá-lo por meio da CLI do Cisco Unified Communications Manager.

Use estes comandos CLI para controlar o serviço Entropy Monitoring Daemon:

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.

Informações Relacionadas

- Guia de segurança do Cisco Unified Communications Manager, versão 11.5(1)
- Suporte Técnico e Documentação - Cisco Systems