Criptografia da próxima geração CUCM 11.0 - Criptografia elíptico da curva

Índice

Introdução

Este original descreve a introdução, configuração da criptografia da próxima geração (NGE) do gerente das comunicações unificadas de Cisco (CUCM) 11.0 e mais atrasado, para cumprir a segurança avançada e os requisitos de desempenho

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Princípios da Segurança do Cisco Call Manager
- Gerenciamento certificado do Cisco Call Manager

Componentes Utilizados

A informação neste documento é baseada em Cisco CUCM 11.0, onde os Certificados EDCSA são apoiados somente para o CallManager (o CallManager-EDCSA)

> **Note**: Certificados de Tomcat-EDCSA dos apoios CUCM 11.5 avante também

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Produtos Relacionados

Este original pode igualmente ser usado com estes produtos de software e versões que apoiam Certificados EDCSA:

- Cisco unificou CM IM e presença 11.5
- Cisco Unity Connection 11.5

Informações de Apoio

A criptografia elíptico da curva (ECC) é uma aproximação à criptografia de chave pública baseada na estrutura algébrica de curvas elípticos sobre campos finitos. Um dos benefícios principais em comparação com a criptografia NON-ECC é o mesmo nível de segurança fornecido por chaves do tamanho menor.

Os critérios comuns oferecem a garantia que os recursos de segurança se operam corretamente dentro da solução que está sendo avaliada. Isto é conseguido com as exigências extensivas da documentação dos testes e da reunião.

Aceitado e apoiado por 26 países no mundo inteiro através dos critérios comuns de arranjo de reconhecimento (CCRA)

A liberação 11.0 do gerente das comunicações unificadas de Cisco apoia Certificados elípticos do Digital Signature Algorithm da curva (ECDSA).

Estes Certificados são mais fortes do que os Certificados RSA-baseados e são exigidos para o Produtos que tem os critérios comuns (CC) das certificações. As soluções comerciais do governo dos EUA para o programa classificado dos sistemas (CSfC) exigem a certificação CC e assim, é incluída na liberação 11.0 do gerente das comunicações unificadas de Cisco avante.

Os Certificados ECDSA estão disponíveis junto com os Certificados existentes RSA nestas áreas:

- Gerenciamento certificado
- Função do proxy do Certificate Authority (CAPF)
- Seguimento do Transport Layer Security (TLS)
- Fixe conexões do SORVO
- Gerente da integração de telefonia e computador (CTI)

- HTTP e
- Entropia

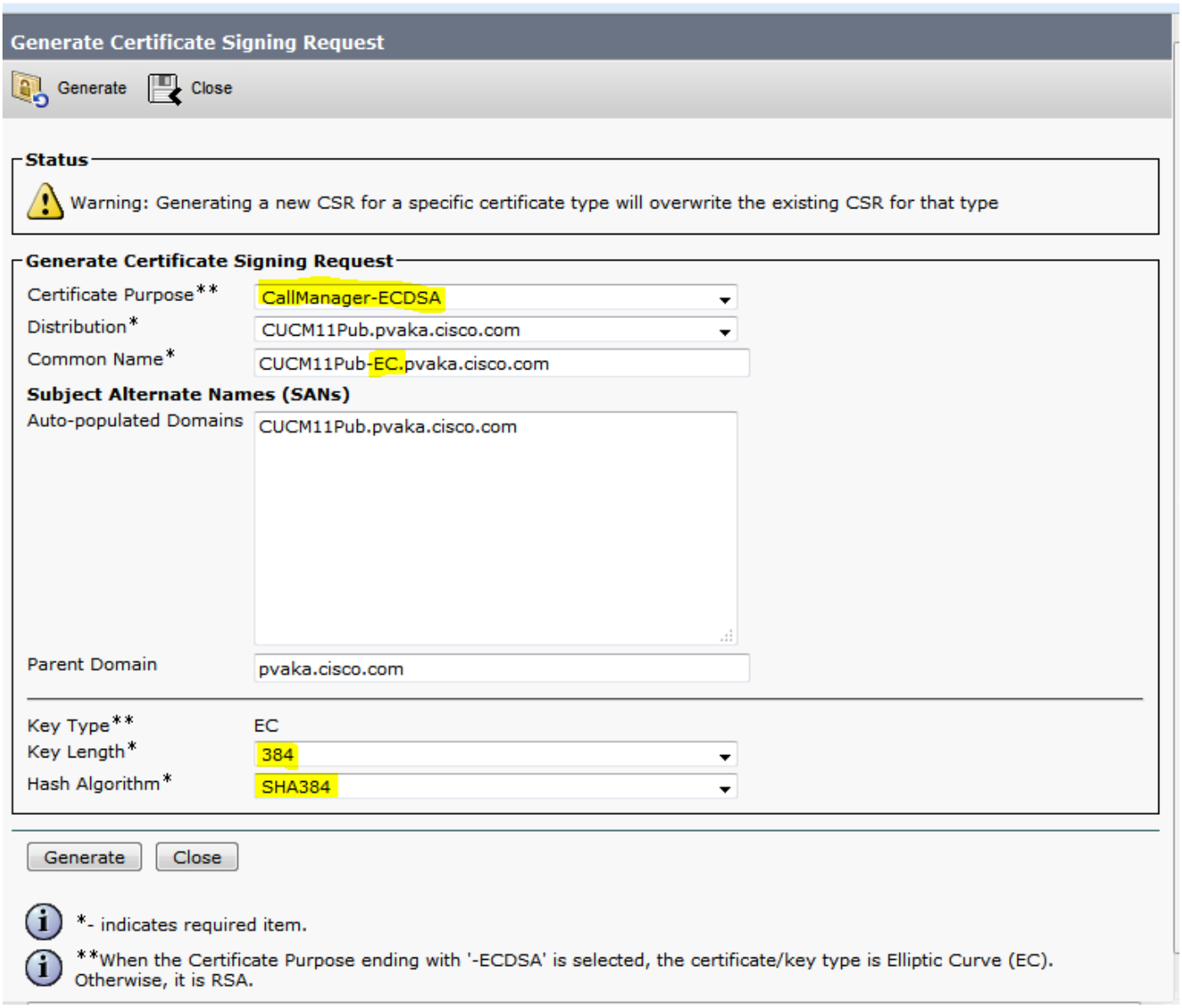
As próximas seções fornecem mais informação detalhada em cada um das áreas 7 acima.

Gerenciamento certificado

Gerando Certificados com criptografia EC

Apoio para o ECC de CUCM 11.0 avante para gerar o certificado do CallManager com criptografia EC

- **CallManager-ECDSA** novo da opção disponível segundo as indicações da imagem.
- Exige a parcela do host do Common Name terminar dentro **– o EC**, para impedir ter o mesmo Common Name que o certificado do **CallManager**.
- Em caso do multi certificado do server SAN, isto deve terminar dentro **– a EC-Senhora**.



- Ambo o pedido do certificado auto-assinado e o CSR pedem o limite as escolhas do algoritmo de hash segundo o tamanho chave EC.

- Para um tamanho chave EC 256 o algoritmo de hash pode ser SHA256, SHA384 ou SHA512. Para um tamanho chave EC 384 o algoritmo de hash pode ser SHA384 ou SHA512. Para um tamanho chave EC 521 a única opção é SHA512.
- O tamanho do chave padrão é 384 e o algoritmo de hashing do padrão é SHA384, que pode ser utilização mudada deixa cair para baixo. As opções disponíveis são baseadas no tamanho chave escolhido.

Configuração de CLI

Uma unidade nova do certificado nomeada **CallManager-ECDSA** foi adicionada para os comandos cli

- ajuste o [unit] CERT REGEN – certificado auto-assinado dos regenerados

```
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)?
```

- ajuste a importação CERT possuem|[unit] da confiança – certificado assinado de CA das importações

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

- ajuste o [unit] gen csr – gerencie o request(CSR) de assinatura do certificado para a unidade especificada

```
admin:set csr gen CallManager-ECDSA

Successfully Generated CSR  for CallManager-ECDSA

admin:
```

- ajuste a exportação maioria|consolide|importação tftp – Quando tftp é o nome da unidade, os Certificados do CallManager-ECDSA obtêm auto-incluídos com os Certificados do CallManager RSA em operações maiorias.

Arquivos CTL e ITL

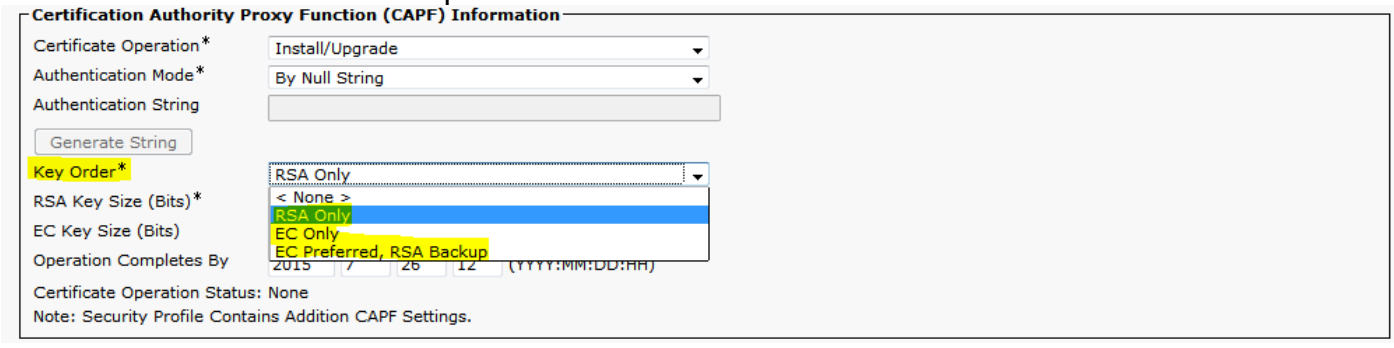
- Os arquivos CTL e ITL têm o presente do **CallManager-ECDSA**.
- O certificado do CallManager-ECDSA tem a função de CCM+TFTP no arquivo ITL e CTL.
- Você pode usar o **ctl da mostra** ou **mostrar** comandos **ITL** ver esta informação segundo as indicações da imagem:

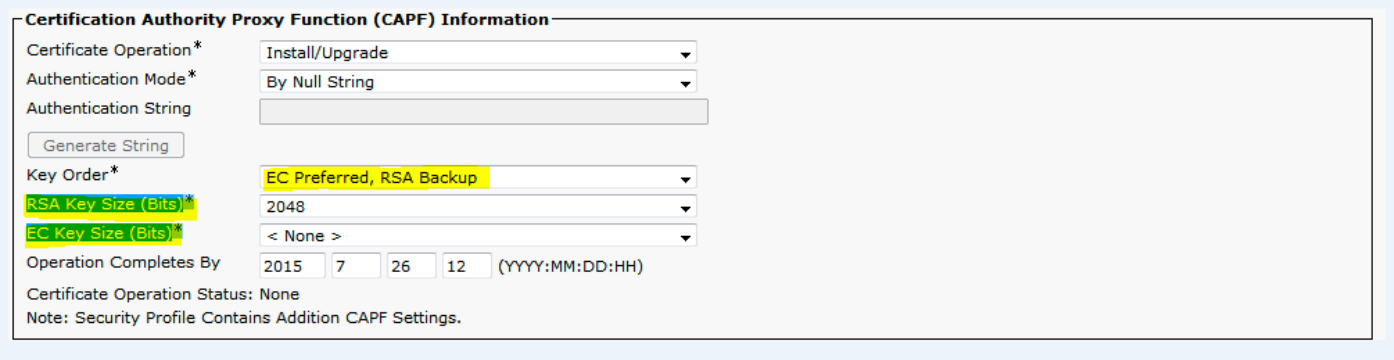
```
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1656
2       DNSNAME         2
3       SUBJECTNAME     65      CN=CUCM11Pub.pvaka.cisco.com;OU=TAC;O=Cisco;L=Sydney;ST=NSW;C=AU
4       FUNCTION        2       CCM+TFTP
5       ISSUERNAME      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 a **atualização do ctl dos utils** para gerar o arquivo CTL.

Função do proxy do Certificate Authority (CAPF)

- A versão 3.0 CAPF em CUCM 11 fornece o apoio para tamanhos chaves EC junto com o RSA.
- As opções adicionais CAPF fornecidas além do que os campos existentes CAPF são ordem chave e tamanho chave EC (bit).
- A opção existente do tamanho chave (bit) foi mudada ao tamanho chave RSA (bit).
- A ordem chave fornece o apoio para o RSA somente, o EC somente e o EC preferido, opções do backup RSA.
- O tamanho chave EC fornece o apoio para tamanhos chaves 384 e 521 de bit 256.
- O tamanho chave RSA fornece o apoio para 512, 1024 e 2048 bit
- Quando chave a ordem de RSA somente é selecionada, simplesmente o tamanho chave RSA pode ser selecionado. Quando o EC somente for selecionado, simplesmente o tamanho chave EC pode ser selecionado. Quando o EC preferido, backup RSA é selecionado, o tamanho chave RSA e EC pode ser selecionado.

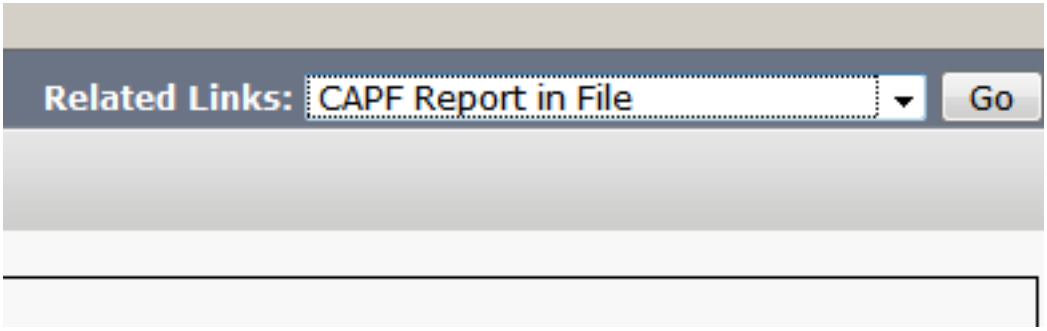




Note: Atualmente, nenhuma versão 3 dos apoios CAPF do valor-limite de Cisco evita assim selecionar a opção EC somente. Contudo, os administradores que querem apoiar mais tarde ECDSA LSC podem configurar seus dispositivos com opção preferida EC do backup RSA. Quando os valores-limite começam a apoiar a versão 3 CAPF para ECDSA LSC, os administradores precisam de reinstalar seu LSC.

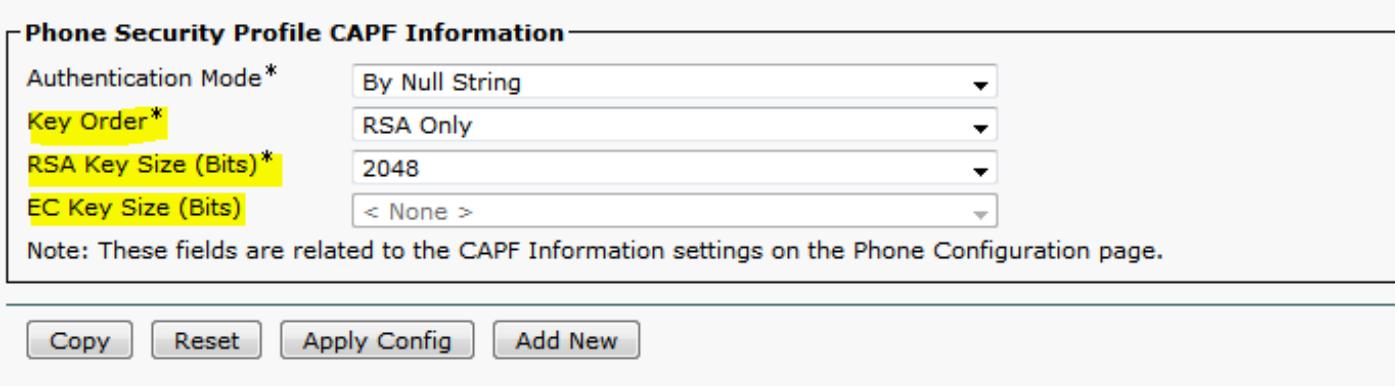
Opções adicionais CAPF para o telefone, o perfil de segurança do telefone, o utilizador final e as páginas de usuário do aplicativo

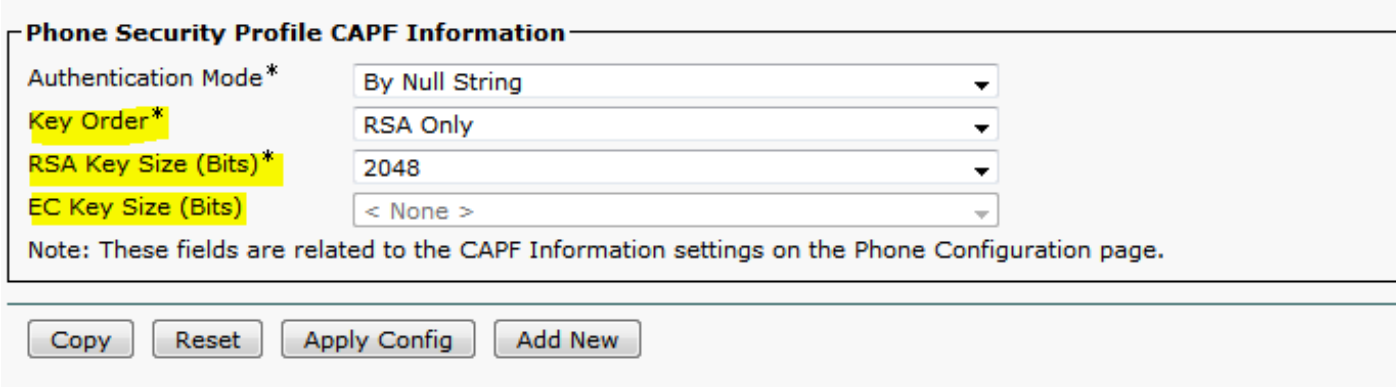
O dispositivo > o telefone > relacionaram os links



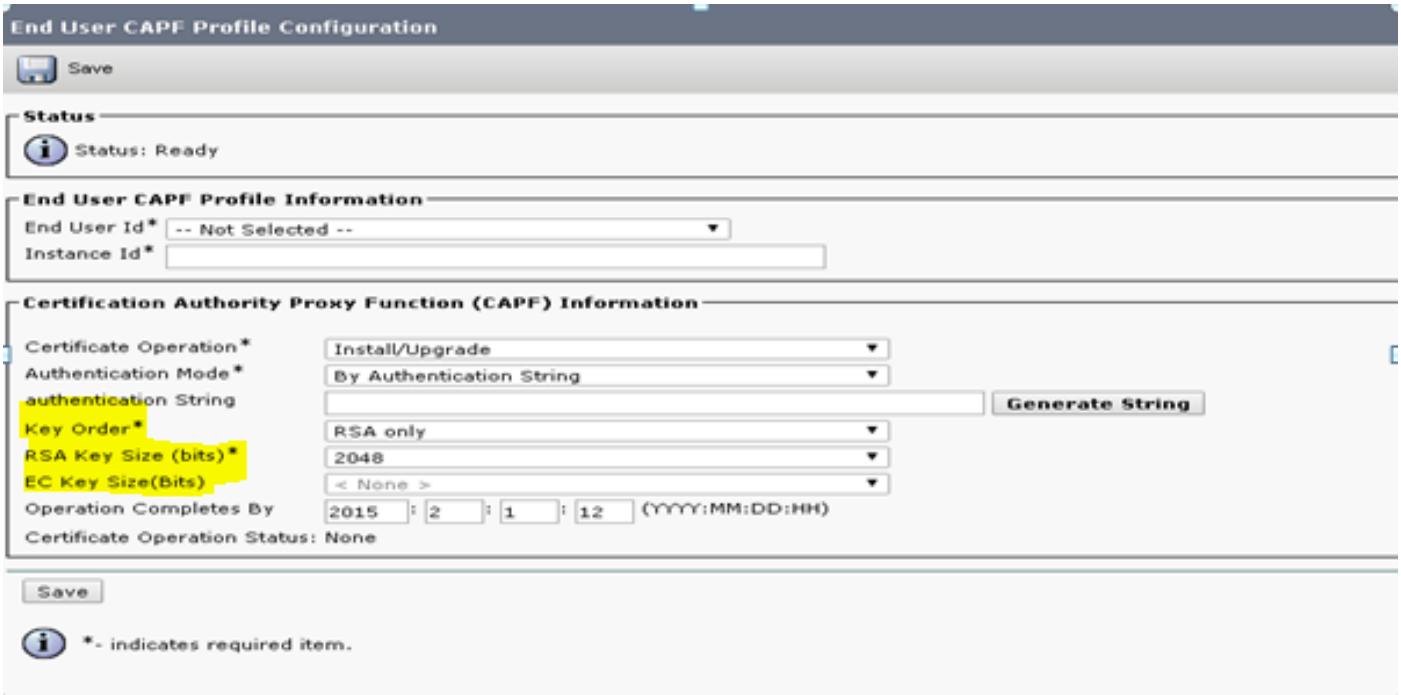
Navegue ao **> segurança do sistema > ao perfil de segurança do telefone**

Gerenciamento de usuário > configurações de usuário > perfil do usuário CAPF do aplicativo



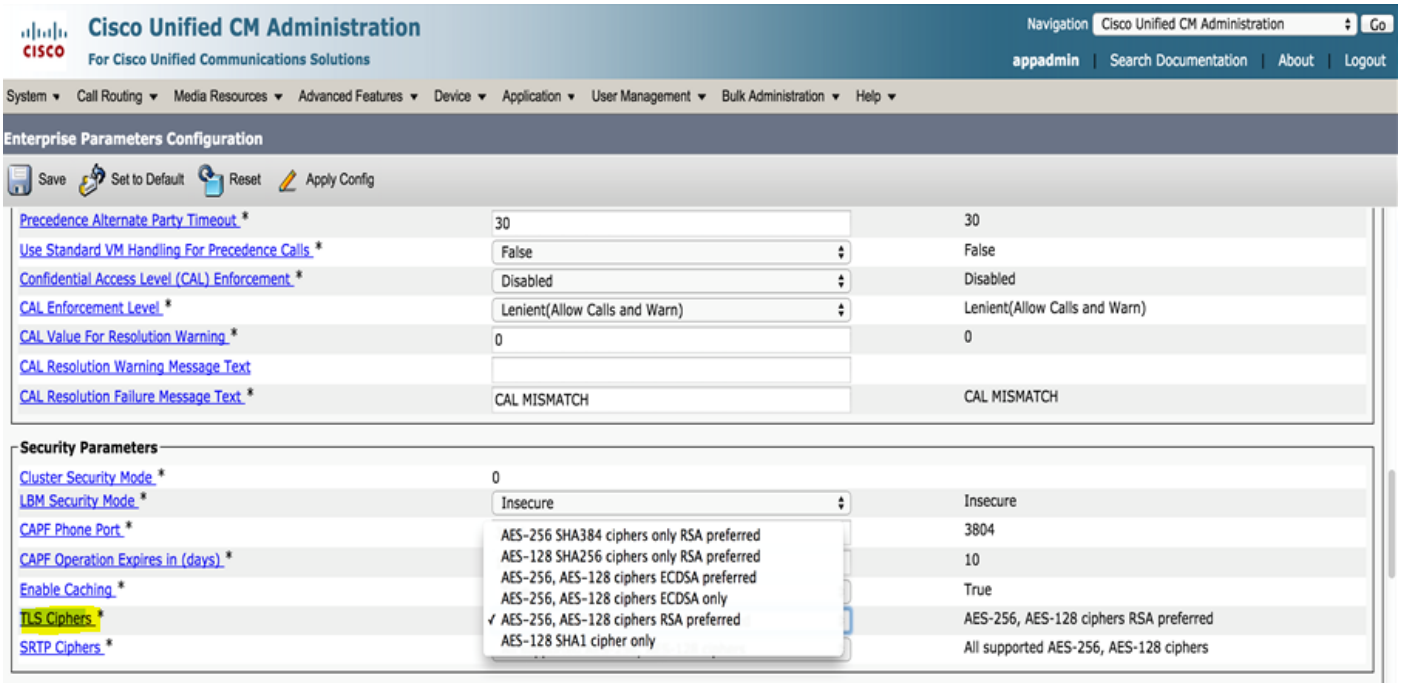


Navegue ao **gerenciamento de usuário > às configurações de usuário > ao perfil do utilizador final CAPF.**



O TLS calcula parâmetros empresariais

- As cifras do parâmetro empresarial TLS foram atualizadas para apoiar cifras ECDSA.
- As cifras do parâmetro empresarial TLS agora ajustam as cifras TLS para a linha do SORVO, tronco do SORVO e fixam o gerenciador de CTI.



Apoio do SORVO ECDSA

- A liberação 11.0 do gerente das comunicações unificadas de Cisco inclui o apoio ECDSA para linhas do SORVO e interfaces de tronco do SORVO.
- A conexão entre o gerente das comunicações unificadas de Cisco e um telefone do valor-limite ou um dispositivo de vídeo é uma linha conexão do SORVO visto que a conexão entre dois gerentes das comunicações unificadas de Cisco é uma conexão de tronco do SORVO.
- Todas as conexões do SORVO apoiam as cifras ECDSA e usam Certificados ECDSA.

A relação segura do SORVO foi atualizada para apoiar estas duas cifras

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

Estas são as encenações quando o SORVO faz conexões TLS (do Transport Layer Security):

- Quando o SORVO atuar como um server TLS

Quando a interface de tronco do SORVO do gerente das comunicações unificadas de Cisco atua como um server TLS para a conexão segura entrante do SORVO, a interface de tronco do SORVO determina se o certificado do CallManager-ECDSA existe no disco. Se o certificado existe no disco, a interface de tronco do SORVO usa o certificado do CallManager-ECDSA se a série selecionada da cifra é

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ou
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

- Quando o SORVO atuar como um cliente TLS

Quando a interface de tronco do SORVO atua como um cliente TLS, a interface de tronco do SORVO envia uma lista de séries pedidas da cifra ao server baseado no campo das cifras TLS (que igualmente inclui o ECDSA calcula a opção) nos parâmetros empresariais CUCM as **cifras TLS**. Esta configuração determina a lista da série da cifra do cliente TLS e as séries apoiadas da cifra por ordem da preferência.

Note: 1. Os dispositivos que usam uma cifra ECDSA para fazer uma conexão a CUCM devem ter o certificado do CallManager-ECDSA em seu arquivo da lista da confiança da identidade (ITL).

Note: 2. As séries da cifra do apoio RSA TLS da interface de tronco do SORVO para conexões dos clientes que não apoiam séries da cifra ECDSA ou quando uma conexão TLS é estabelecida com uma versão anterior de CUCM, isso não apoiam ECDSA.

Apoio seguro do gerenciador de CTI ECDSA

A relação segura do gerenciador de CTI foi atualizada para apoiar estas 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 carga segura da relação do gerenciador de CTI o certificado do CallManager e do CallManager-ECDSA. Isto permite que a relação segura do gerenciador de CTI apoie as cifras novas junto com a cifra existente RSA.
- Similar à relação do SORVO, a opção das cifras do parâmetro empresarial TLS no gerente das comunicações unificadas de Cisco é usada para configurar as cifras TLS que são apoiadas na interface segura do gerenciador de CTI.

Apoio HTTPS para a transferência da configuração

- Para a transferência segura da configuração (por exemplo clientes do Jabber), a liberação 11.0 do gerente das comunicações unificadas de Cisco é aumentada para apoiar o HTTPS além do que as relações HTTP e TFTP que foram usadas nas versões anterior.
- Se for necessário, ambo autenticação mútua do uso do cliente e servidor. Contudo, os clientes que são registrados com ECDSA LSC e configurações de TFTP cifradas são exigidos apresentar seu LSC.
- A relação HTTPS usa o CallManager e os Certificados do CallManager-ECDSA como os certificados de servidor.

Note: 1. Quando você atualiza Certificados do CallManager, do CallManager ECDSA, ou do Tomcat, você deve desativar e reactivate o serviço TFTP.

Note: 2. A porta 6971 é usada para a autenticação dos Certificados do CallManager e do CallManager-ECDSA, usada por telefones.

Note: 3. A porta 6972 é usada para a autenticação dos Certificados de Tomcat, usada pelo

Jabber.

Entropia

A entropia é uma medida da aleatoriedade dos dados e ajuda em determinar o limiar mínimo para critérios comuns das exigências. Para ter a criptografia forte, uma fonte robusta de entropia é exigida. Se um algoritmo de criptografia forte, tal como ECDSA, usa um origem fraca da entropia, a criptografia pode facilmente quebrar-se.

No gerente das comunicações unificadas de Cisco libere 11.0, a fonte da entropia para comunicações unificadas que de Cisco o gerente é melhorado.

O demônio da monitoração da entropia é uma característica incorporado que não exija a configuração. Contudo, você pode desligá-la através do gerente CLI das comunicações unificadas de Cisco.

Use os seguintes comandos CLI controlar o serviço de demônio da monitoração da entropia:

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

- 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
- Suporte Técnico e Documentação - Cisco Systems