

Como baixar certificados de telefones IP da Cisco

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve o procedimento para recuperar certificados de um telefone IP da Cisco quando o serviço Cisco Authority Proxy Function (CAPF) é executado no editor do Cisco Unified Communications Manager (CUCM).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Certificados SSL no telefone
- administração de CUCM
- Gerenciamento da Interface de Linha de Comando (CLI - Command Line Interface) no CUCM

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Unified Communications Manager (CUCM) versão 11.5.1.11900-26
- Telefone IP Cisco 8811 - sip88xx.12-5-1SR1-4

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O serviço CAPF deve estar ativo no editor do CUCM e o certificado CAPF no Cisco Unified OS Administration deve estar atualizado.

Para telefones IP da Cisco, há duas alternativas de certificados instalados neles:

- MIC (Certificado instalado pelo fabricante)
- MIC e LSC (Certificado localmente significativo)

Os telefones são pré-instalados com o certificado MIC e não podem ser excluídos nem regenerados. Além disso, o MIC não pode ser usado depois que a validade expirar. Os MICs são certificados de chave de 2048 bits assinados pela Autoridade de Certificação da Cisco.

O LSC possui a chave pública para o telefone IP da Cisco, que é assinado pela chave privada CUCM CAPF. Ele não está instalado no telefone por padrão e esse certificado é necessário para que o telefone funcione no modo de segurança

Configurar

Etapa 1. No CUCM, navegue para **Cisco Unified CM Administration > Device > Phone**.

Etapa 2. Localize e selecione o telefone do qual os certificados deseja recuperar.

Etapa 3. Na página de configuração do telefone, navegue até a seção **Certification Authority Proxy Function (CAPF)**.

Etapa 4. Como mostrado na imagem, aplique estes parâmetros:

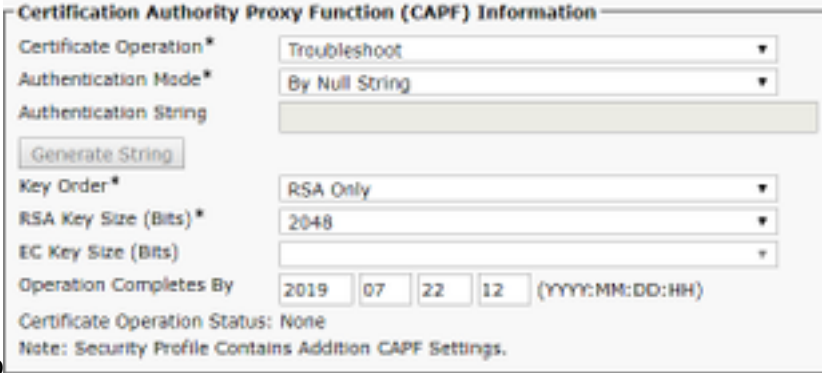
Operação do certificado: Troubleshoot

Modo de autenticação: Por String Nula

Tamanho da chave (bits): 1024

Operação concluída por: Data no

futuro



Certification Authority Proxy Function (CAPF) Information	
Certificate Operation*	Troubleshoot
Authentication Mode*	By Null String
Authentication String	
<input type="button" value="Generate String"/>	
Key Order*	RSA Only
RSA Key Size (Bits)*	2048
EC Key Size (Bits)	
Operation Completes By	2019 07 22 12 (YYYY:MM:DD:HH)
Certificate Operation Status: None	
Note: Security Profile Contains Addition CAPF Settings.	

Etapa 5. Clique em **Salvar e Redefinir** o telefone.

Etapa 6. Depois que o dispositivo estiver registrado no cluster do CUCM, verifique na página de configuração do telefone se a operação de solução de problemas foi concluída conforme

Certification Authority Proxy Function (CAPF) Information

Certificate Operation*	No Pending Operation
Authentication Mode*	By Null String
Authentication String	<input type="text"/>
<input type="button" value="Generate String"/>	
Key Order*	RSA Only
RSA Key Size (Bits)*	2048
EC Key Size (Bits)	<input type="text"/>
Operation Completes By	2019 07 22 12 (YYYY:MM:DD:HH)
Certificate Operation Status: Troubleshoot Success	
Note: Security Profile Contains Addition CAPF Settings.	

mostrado na imagem:

Passo 7. Abra uma sessão SSH para o servidor do Editor do CUCM e execute o comando para listar os certificados associados ao telefone como mostrado na imagem:

lista de arquivos `ativelog /cm/trace/capf/sdi/SEP<MAC_Address>*`

```
admin:file list activelog /cm/trace/capf/sdi/SEP*
SEPF87B204EED99-L1.cer          SEPF87B204EED99-M1.cer
dir count = 0, file count = 2
admin:█
```

Há duas opções para os arquivos a serem listados:

Somente MIC: `SEP<MAC_Address>-M1.cer`

MIC e LSC: `SEP<MAC_Address>-M1.cer` e `SEP<MAC_Address>-L1.cer`

Etapa 8. Para baixar os certificados, execute este comando: `file get activelog /cm/trace/capf/sdi/SEP<MAC_Address>*`

Um servidor Secure File Transfer Protocol (SFTP) é necessário para salvar o arquivo como mostrado na imagem

```
admin:file get activelog /cm/trace/capf/sdi/SEPF87B204EED99-M1.cer
Please wait while the system is gathering files info ...
Get file: /var/log/active/cm/trace/capf/sdi/SEPF87B204EED99-M1.cer
done.
Sub-directories were not traversed.
Number of files affected: 1
Total size in Bytes: 1159
Total size in Kbytes: 1.1318359
Would you like to proceed [y/n]? y
SFTP server IP: 10.1.99.201
SFTP server port [22]:
User ID: alegarc2
Password: *****
Download directory: /

The authenticity of host '10.1.99.201 (10.1.99.201)' can't be established.
RSA key fingerprint is 33:83:bd:c7:8e:4d:1c:5a:b3:be:b2:e2:38:2b:fc:26.
Are you sure you want to continue connecting (yes/no)? yes
```

Informações Relacionadas

- [Certificados de telefone IP](#)