

# Gerencia o certificado assinado do Certificate Authority (CA) no server do atendimento CVP para o Transport Layer Security do SORVO (o TLS)

## Índice

[Introdução](#)

[Componentes Utilizados](#)

[Configuration Steps](#)

[Verificações](#)

[Referência:](#)

## Introdução

Este original descreve como gerar o certificado assinado de CA para o server do atendimento CVP e como verificar o certificado de servidor do atendimento CVP. Da versão 11.6 CVP, uma comunicação do SORVO TLS é apoiada.

Contribuído por Mingze Yan, engenheiro de TAC da Cisco.

Editado por Sahar Modares, engenheiro de TAC da Cisco.

## [Componentes Utilizados](#)

- Server 11.6 do atendimento CVP

## Configuration Steps

Step1. Senha do achado para o keystore.

Navegue a `c:\Cisco\CVP\conf\security.properties` no server do atendimento CVP a fim encontrar esta senha.

Este arquivo contém a senha para o keystore, que é exigido ao operar o keystore.

Step2. Crie uma variável provisória para evitar incorporam o valor de senha do keystore todas as vezes.

Navegue a `c:\Cisco\CVP\conf\security` e execute este comando:

```
ajuste o kt= c:\Cisco\CVP\jre\bin\keytool.exe - os
```

```
storepass 592(!aT@Hbt{[c)b7n6{Mj6J[0P4C~X2?4!zv~5(@2*12Dm97 - o storetype JCEKS - o keystore .keystore
```

**Note:** Storepass deve ser substituído com sua própria senha do keystore.

Step3. Remova o certificado do server da chamada existente.

Isto é devido à limitação do keysize no server do atendimento que é 2048 bit.

Navegue a **c:\Cisco\CVP\conf\security** para encontrar o certificado existente. Execute este comando suprimir do certificado:

```
%kt% - supressão - aliás callserver_certificate
```

Após o supressão do certificado, este comando pode ser usado a fim verificar todos os Certificados no server CVP:

```
%kt% - lista
```

E a fim confirmar se o certificado de servidor do atendimento foi suprimido, execute este comando:

```
%kt% - lista | callserver do findstr
```

Etapa 4. Gerencia o par de chaves. Você deve usar o par de chaves de 1024 bit.

Navegue a **c:\Cisco\CVP\conf\security** e execute este comando:

```
%kt% - genkeypair - aliás callserver_certificate - v - keysize 1024 - o keyalg RSA
```

Quando você executa este comando, pede esta informação:

**Note:** Você deve usar o hostname do server como o nome e o sobrenome.

**Que é seu nome e sobrenome?**

```
[Unknown]: col115cvpcall02
```

Que é o nome de sua unidade organizacional?

```
[Unknown]: TAC
```

Que é o nome de sua organização?

```
[Unknown]: Cisco
```

Que é o nome de sua cidade ou localidade?

```
[Unknown]: Sydney
```

Que é o nome de sua estado ou província?

```
[Unknown]: NSW
```

Que é o código de país de duas letras para esta unidade?

```
[Unknown]: AU
```

Está CN=col115cvpcall02, OU=TAC, O=Cisco, L=Sydney, ST=NSW, C=AU correto?

```
[não]: sim
```



Step5. Gerencia a solicitação de assinatura de certificado nova (CSR).

Navegue a **c:\Cisco\CVP\conf\security** e execute este comando:

```
%kt% - certreq - aliás callserver_certificate - archive callserver.csr
```

Step6. Assine o CSR por CA interno ou pelo C da terceira.

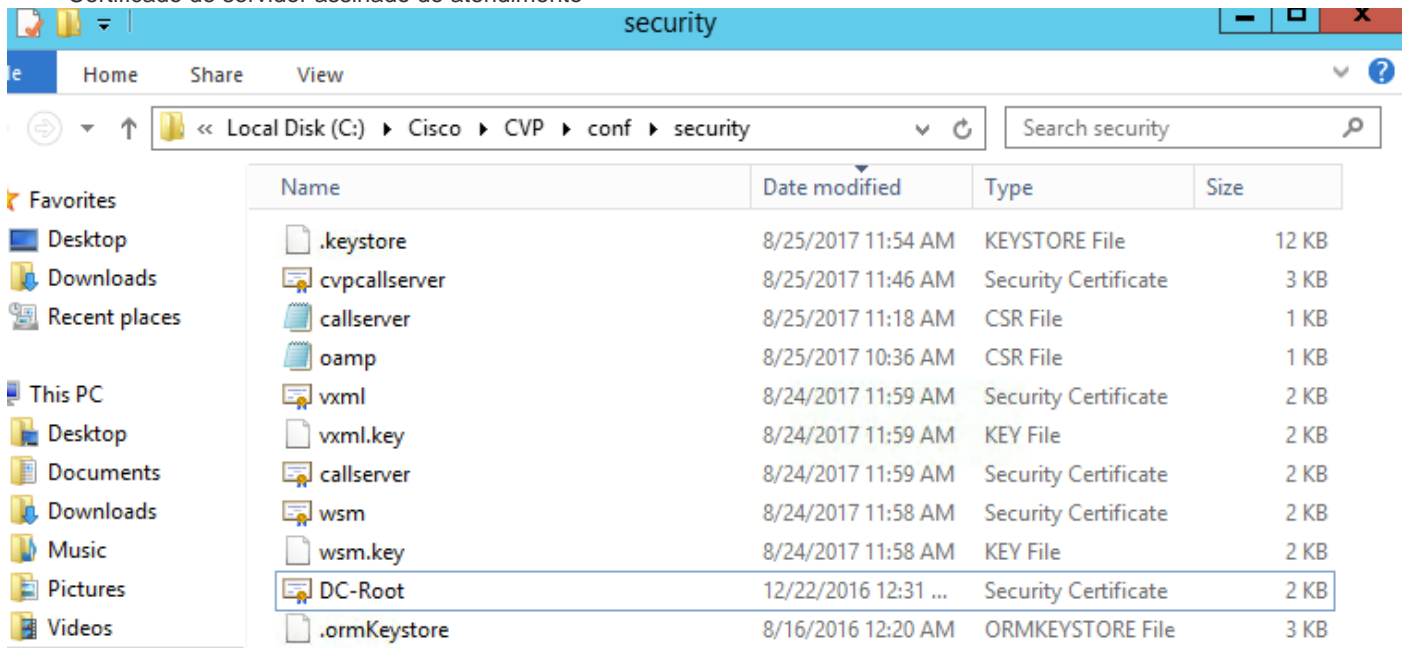
Navegue a **c:\Cisco\CVP\conf\security** a fim encontrar este arquivo CSR:

 callserver	8/25/2017 11:18 AM	CSR File	1 KB
 oamp	8/25/2017 10:36 AM	CSR File	1 KB

Step7. Instale a CA raiz.

Dois Certificados são copiados a c:\Cisco\CVP\conf\security.

- Certificado CA raiz
- Certificado de servidor assinado do atendimento



Execute este comando:

**%kt% - importação - v - trustcacerts - aliás raiz - archive DC-Root.cer**

Neste laboratório, o CERT da CA raiz é DC-Root.cer.

Etapa 8. Instale o certificado de servidor do atendimento que foi assinado por CA.

Navegue a c:\Cisco\CVP\conf\security

Execute este comando:

**%kt% - importação - v - trustcacerts - aliás callserver\_certificate - archive cvpcallserver.cer**

Neste laboratório, o certificado de servidor do atendimento é cvpcallserver.cer.

Etapa 9. Verifique o certificado instalado novo

A fim verificar o certificado instalado novo, navegue a C:\Cisco\CVP\conf\security >

Execute este comando:

**%kt% - lista - v - aliás nome de pseudônimo do callserver\_certificate: callserver\_certificate**

**Note:** O nome de pseudônimo é um valor fixo do sistema. Você deve usar o callserver\_certificate.

Exemplo:

Data de criação: agosto 25, 2017

Tipo da entrada: PrivateKeyEntry

Comprimento de certificate chain: 2

Certificate[1]:

Proprietário: CN=col115cvpcall02, OU=TAC, O=Cisco, L=Sydney, ST=NSW, C=AU

Expedidor: CN=col115-COL115-CA, DC=col115, DC=org, DC=au

Número de série: 610000000e78c717ba3dd3dc2400000000000e

Válido de: Fri o 25 de agosto 11:32:43 AEST 2017 até: Sat o 25 de agosto 11:42:43 AEST 2018

Impressões digitais do certificado:

Após conclusão de todas estas etapas, o certificado assinado de CA para o server do atendimento foi instalado. Este certificado é usado quando a conexão TLS para o SORVO é estabelecida.

## Verificações

Estes dois comandos podem ser usados para alistar todos os Certificados ou somente certificados de servidor do atendimento:

`%kt%` - lista

`%kt%` - lista | callserver do findstr

Este comando pode ser usado para ver detalhes certificados:

Nome de pseudônimo: `callserver_certificate`

`%kt%` - lista - v - aliás `callserver_certificate`

Nome de pseudônimo: `callserver_certificate`

## Referência:

[Manual de configuração para o Portal Cisco Unified Customer Voice, liberação 11.6\(1\)](#)