



# **Configurar certificado CA**

## **SnapCenter software**

NetApp  
November 06, 2025

This PDF was generated from [https://docs.netapp.com/pt-br/snapcenter-61/protect-nsp/generate\\_CA\\_certificate\\_CSR\\_file.html](https://docs.netapp.com/pt-br/snapcenter-61/protect-nsp/generate_CA_certificate_CSR_file.html) on November 06, 2025. Always check docs.netapp.com for the latest.

# Índice

Configurar certificado CA .....	1
Gerar arquivo CSR de certificado CA .....	1
Importar certificados de CA .....	1
Obtenha a impressão digital do certificado CA .....	2
Configurar certificado CA com serviços de plug-in de host do Windows .....	2
Configurar o certificado CA para o serviço de plug-ins suportados pela NetApp no host Linux .....	3
Gerenciar senha para keystore de plug-in e alias do par de chaves assinadas pela CA em uso .....	3
Configurar certificados raiz ou intermediários para plug-in trust-store .....	4
Configurar o par de chaves assinadas pela CA para plug-in trust-store .....	4
Configurar lista de revogação de certificados (CRL) para plug-ins .....	5
Configurar o certificado CA para o serviço de plug-ins suportados pela NetApp no host Windows .....	6
Gerenciar senha para keystore de plug-in e alias do par de chaves assinadas pela CA em uso .....	6
Configurar certificados raiz ou intermediários para plug-in trust-store .....	6
Configurar o par de chaves assinadas pela CA para plug-in trust-store .....	7
Configurar lista de revogação de certificados (CRL) para plug-ins SnapCenter .....	7
Habilitar certificados CA para plug-ins .....	8

# Configurar certificado CA

## Gerar arquivo CSR de certificado CA

Você pode gerar uma Solicitação de Assinatura de Certificado (CSR) e importar o certificado que pode ser obtido de uma Autoridade de Certificação (CA) usando o CSR gerado. O certificado terá uma chave privada associada a ele.

CSR é um bloco de texto codificado que é fornecido a um fornecedor de certificado autorizado para obter o certificado de CA assinado.



O comprimento mínimo da chave RSA do certificado CA deve ser de 3072 bits.

Para obter informações sobre como gerar um CSR, consulte ["Como gerar um arquivo CSR de certificado CA"](#).



Se você possui o certificado CA para seu domínio (\*.domain.company.com) ou seu sistema (machine1.domain.company.com), você pode pular a geração do arquivo CSR do certificado CA. Você pode implantar o certificado CA existente com o SnapCenter.

Para configurações de cluster, o nome do cluster (FQDN do cluster virtual) e os respectivos nomes de host devem ser mencionados no certificado da CA. O certificado pode ser atualizado preenchendo o campo Nome Alternativo do Assunto (SAN) antes de adquirir o certificado. Para um certificado curinga (\*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

## Importar certificados de CA

Você deve importar os certificados de CA para o SnapCenter Server e os plug-ins do host do Windows usando o console de gerenciamento da Microsoft (MMC).

### Passos

1. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo > Adicionar/Remover Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
3. Na janela do snap-in Certificados, selecione a opção **Conta de computador** e clique em **Concluir**.
4. Clique em **Console Root > Certificados – Computador local > Autoridades de certificação raiz confiáveis > Certificados**.
5. Clique com o botão direito do mouse na pasta “Autoridades de Certificação Raiz Confiáveis” e selecione **Todas as Tarefas > Importar** para iniciar o assistente de importação.
6. Conclua o assistente da seguinte forma:

Nesta janela do assistente...	Faça o seguinte...
Importar chave privada	Selecione a opção <b>Sim</b> , importe a chave privada e clique em <b>Avançar</b> .

Nesta janela do assistente...	Faça o seguinte...
Formato de arquivo de importação	Não faça alterações; clique em <b>Avançar</b> .
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em <b>Avançar</b> .
Concluindo o Assistente de Importação de Certificados	Revise o resumo e clique em <b>Concluir</b> para iniciar a importação.



O certificado de importação deve ser agrupado com a chave privada (os formatos suportados são: \*.pfx, \*.p12 e \*.p7b).

7. Repita a Etapa 5 para a pasta "Pessoal".

## Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma sequência hexadecimal que identifica um certificado. Uma impressão digital é calculada a partir do conteúdo do certificado usando um algoritmo de impressão digital.

### Passos

1. Execute o seguinte na GUI:
  - a. Clique duas vezes no certificado.
  - b. Na caixa de diálogo Certificado, clique na guia **Detalhes**.
  - c. Percorra a lista de campos e clique em **Impressão digital**.
  - d. Copie os caracteres hexadecimais da caixa.
  - e. Remova os espaços entre os números hexadecimais.

Por exemplo, se a impressão digital for: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", após remover os espaços, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Execute o seguinte no PowerShell:
  - a. Execute o seguinte comando para listar a impressão digital do certificado instalado e identificar o certificado instalado recentemente pelo nome do assunto.
 

```
Get-ChildItem -Path Cert:\LocalMachine\My
```
  - b. Copie a impressão digital.

## Configurar certificado CA com serviços de plug-in de host do Windows

Você deve configurar o certificado CA com os serviços de plug-in do host do Windows para ativar o certificado digital instalado.

Execute as seguintes etapas no SnapCenter Server e em todos os hosts de plug-in onde os certificados CA já estão implantados.

### Passos

1. Remova a vinculação de certificado existente com a porta padrão 8145 do SMCore, executando o seguinte comando:

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

Por exemplo:

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. Vincule o certificado recém-instalado aos serviços de plug-in do host do Windows, executando os seguintes comandos:
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert appid="$guid"
```

Por exemplo:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert appid="$guid"
```

## Configurar o certificado CA para o serviço de plug-ins suportados pela NetApp no host Linux

Você deve gerenciar a senha do keystore do plug-in e seu certificado, configurar o certificado da CA, configurar certificados raiz ou intermediários para o trust-store do plug-in e configurar o par de chaves assinadas pela CA para o trust-store do plug-in com o serviço de plug-ins do SnapCenter para ativar o certificado digital instalado.

Os plug-ins usam o arquivo 'keystore.jks', que está localizado em `/opt/NetApp/snapcenter/scc/etc` como seu armazenamento confiável e armazenamento de chaves.

### Gerenciar senha para keystore de plug-in e alias do par de chaves assinadas pela CA em uso

#### Passos

1. Você pode recuperar a senha padrão do keystore do plug-in a partir do arquivo de propriedades do agente do plug-in.

É o valor correspondente à chave 'KEYSTORE\_PASS'.

2. Alterar a senha do keystore:

```
keytool -storepasswd -keystore keystore.jks
```

. Altere a senha de todos os aliases de entradas de chave privada no keystore para a mesma senha usada para o keystore:

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Atualize o mesmo para a chave KEYSTORE\_PASS no arquivo *agent.properties*.

3. Reinicie o serviço após alterar a senha.



A senha para o keystore do plug-in e para todas as senhas de alias associadas da chave privada deve ser a mesma.

## Configurar certificados raiz ou intermediários para plug-in trust-store

Você deve configurar os certificados raiz ou intermediários sem a chave privada para conectar o trust-store.

### Passos

1. Navegue até a pasta que contém o keystore do plug-in: /opt/ NetApp/snapcenter/scc/etc.
2. Localize o arquivo 'keystore.jks'.
3. Listar os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Adicione um certificado raiz ou intermediário:

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks
```

. Reinicie o serviço após configurar os certificados raiz ou intermediários para conectar o trust-store.



Você deve adicionar o certificado da CA raiz e depois os certificados da CA intermediária.

## Configurar o par de chaves assinadas pela CA para plug-in trust-store

Você deve configurar o par de chaves assinadas pela CA para o trust-store do plug-in.

### Passos

1. Navegue até a pasta que contém o keystore do plug-in /opt/ NetApp/snapcenter/scc/etc.
2. Localize o arquivo 'keystore.jks'.

3. Listar os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Adicione o certificado da CA com chave privada e pública.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Listar os certificados adicionados no keystore.

```
keytool -list -v -keystore keystore.jks
```

6. Verifique se o keystore contém o alias correspondente ao novo certificado CA, que foi adicionado ao keystore.

7. Altere a senha da chave privada adicionada para o certificado CA para a senha do keystore.

A senha padrão do keystore do plug-in é o valor da chave KEYSTORE\_PASS no arquivo agent.properties.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks
```

. Se o nome do alias no certificado da CA for longo e contiver espaços ou caracteres especiais ("\*", ",", "), altere o nome do alias para um nome simples:

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

. Configure o nome do alias do certificado CA no arquivo agent.properties.

Atualize este valor em relação à chave SCC\_CERTIFICATE\_ALIAS.

8. Reinicie o serviço após configurar o par de chaves assinadas pela CA para plug-in trust-store.

## Configurar lista de revogação de certificados (CRL) para plug-ins

### Sobre esta tarefa

- Os plug-ins do SnapCenter procurarão os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL dos plug-ins do SnapCenter é 'opt/NetApp/snapcenter/scc/etc/crl'.

### Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo agent.properties em relação à chave CRL\_PATH.

Você pode colocar mais de um arquivo CRL neste diretório. Os certificados recebidos serão verificados em relação a cada CRL.

# Configurar o certificado CA para o serviço de plug-ins suportados pela NetApp no host Windows

Você deve gerenciar a senha do keystore do plug-in e seu certificado, configurar o certificado da CA, configurar certificados raiz ou intermediários para o trust-store do plug-in e configurar o par de chaves assinadas pela CA para o trust-store do plug-in com o serviço de plug-ins do SnapCenter para ativar o certificado digital instalado.

Os plug-ins usam o arquivo *keystore.jks*, que está localizado em *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc* como seu armazenamento confiável e armazenamento de chaves.

## Gerenciar senha para keystore de plug-in e alias do par de chaves assinadas pela CA em uso

### Passos

1. Você pode recuperar a senha padrão do keystore do plug-in a partir do arquivo de propriedades do agente do plug-in.

É o valor correspondente à chave *KEYSTORE\_PASS*.

2. Alterar a senha do keystore:

```
keytool -storepasswd -keystore keystore.jks
```



Se o comando "keytool" não for reconhecido no prompt de comando do Windows, substitua o comando keytool pelo seu caminho completo.

```
C:\Arquivos de Programas\Java\<versão_jdk>\bin\keytool.exe" -storepasswd -keystore keystore.jks
```

3. Altere a senha de todos os aliases de entradas de chave privada no keystore para a mesma senha usada para o keystore:

```
keytool -keypasswd -alias "nome_do_alias_no_certificado" -keystore keystore.jks
```

Atualize o mesmo para a chave *KEYSTORE\_PASS* no arquivo *agent.properties*.

4. Reinicie o serviço após alterar a senha.



A senha para o keystore do plug-in e para todas as senhas de alias associadas da chave privada deve ser a mesma.

## Configurar certificados raiz ou intermediários para plug-in trust-store

Você deve configurar os certificados raiz ou intermediários sem a chave privada para conectar o trust-store.

### Passos

1. Navegue até a pasta que contém o keystore do plug-in *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localize o arquivo 'keystore.jks'.



3. Listar os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Adicione um certificado raiz ou intermediário:

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. Reinicie o serviço após configurar os certificados raiz ou intermediários para conectar o trust-store.



Você deve adicionar o certificado da CA raiz e depois os certificados da CA intermediária.

## Configurar o par de chaves assinadas pela CA para plug-in trust-store

Você deve configurar o par de chaves assinadas pela CA para o trust-store do plug-in.

### Passos

1. Navegue até a pasta que contém o keystore do plug-in `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc`

2. Localize o arquivo `keystore.jks`.

3. Listar os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Adicione o certificado da CA com chave privada e pública.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Listar os certificados adicionados no keystore.

```
keytool -list -v -keystore keystore.jks
```

6. Verifique se o keystore contém o alias correspondente ao novo certificado CA, que foi adicionado ao keystore.

7. Altere a senha da chave privada adicionada para o certificado CA para a senha do keystore.

A senha padrão do keystore do plug-in é o valor da chave `KEYSTORE_PASS` no arquivo `agent.properties`.

```
keytool -keypasswd -alias "nome_do_alias_no_certificado_da_CA" -keystore keystore.jks
```

8. Configure o nome do alias do certificado CA no arquivo `agent.properties`.

Atualize este valor em relação à chave `SCC_CERTIFICATE_ALIAS`.

9. Reinicie o serviço após configurar o par de chaves assinadas pela CA para plug-in trust-store.

## Configurar lista de revogação de certificados (CRL) para plug-ins SnapCenter

### Sobre esta tarefa

- Para baixar o arquivo CRL mais recente para o certificado CA relacionado, consulte ["Como atualizar o arquivo de lista de revogação de certificados no SnapCenter CA Certificate"](#) .

- Os plug-ins do SnapCenter procurarão os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL dos plug-ins do SnapCenter é 'C:\Arquivos de Programas\NetApp\ SnapCenter\ Snapcenter Plug-in Creator\ etc\crl'.

### Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo *agent.properties* em relação à chave CRL\_PATH.
2. Você pode colocar mais de um arquivo CRL neste diretório.

Os certificados recebidos serão verificados em relação a cada CRL.

## Habilitar certificados CA para plug-ins

Você deve configurar os certificados CA e implantá-los no SnapCenter Server e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

### Antes de começar

- Você pode habilitar ou desabilitar os certificados da CA usando o cmdlet run *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando *Get-SmCertificateSettings*.





As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command\_name*. Alternativamente, você também pode consultar o ["Guia de referência do cmdlet do software SnapCenter"](#).

### Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Hosts gerenciados**.
3. Selecione hosts de plug-in únicos ou múltiplos.
4. Clique em **Mais opções**.
5. Selecione **Ativar validação de certificado**.

### Depois que você terminar

A guia Hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o SnapCenter Server e o host do plug-in.

- \*  \* indica que o certificado CA não está habilitado nem atribuído ao host do plug-in.
- \*  \* indica que o certificado CA foi validado com sucesso.
- \*  \* indica que o certificado CA não pôde ser validado.
- \*  \* indica que as informações de conexão não puderam ser recuperadas.



Quando o status é amarelo ou verde, as operações de proteção de dados foram concluídas com sucesso.

## **Informações sobre direitos autorais**

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTE; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

## **Informações sobre marcas comerciais**

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.