



# **Configurar e habilitar a comunicação SSL bidirecional no host Windows**

SnapCenter software

NetApp  
November 06, 2025

# Índice

- Configurar e habilitar a comunicação SSL bidirecional no host Windows . . . . . 1
  - Configurar comunicação SSL bidirecional no host Windows . . . . . 1
    - Configurar o plug-in SnapCenter do Windows para comunicação SSL bidirecional . . . . . 3
- Habilitar comunicação SSL bidirecional no host Windows . . . . . 3
  - Desabilitar comunicação SSL bidirecional . . . . . 4

# Configurar e habilitar a comunicação SSL bidirecional no host Windows

## Configurar comunicação SSL bidirecional no host Windows

Você deve configurar a comunicação SSL bidirecional para proteger a comunicação mútua entre o SnapCenter Server no host Windows e os plug-ins.

### Antes de começar

- Você deve ter gerado o arquivo CSR do certificado CA com o comprimento mínimo de chave suportado de 3072.
- O certificado da CA deve oferecer suporte à autenticação do servidor e à autenticação do cliente.
- Você deve ter um certificado de CA com chave privada e detalhes de impressão digital.
- Você deve ter habilitado a configuração SSL unidirecional.

Para mais detalhes, veja ["Seção Configurar certificado CA."](#)

- Você deve ter habilitado a comunicação SSL bidirecional em todos os hosts de plug-in e no SnapCenter Server.

Ambientes com alguns hosts ou servidores não habilitados para comunicação SSL bidirecional não são suportados.

### Passos

1. Para vincular a porta, execute as seguintes etapas no host do SnapCenter Server para a porta 8146 do servidor web SnapCenter IIS (padrão) e novamente para a porta 8145 do SMCore (padrão) usando comandos do PowerShell.

- a. Remova a vinculação de porta do certificado autoassinado existente do SnapCenter usando o seguinte comando do PowerShell.

```
> netsh http delete sslcert ipport=0.0.0.0:<SMCore port/IIS port>
```

Por exemplo,

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

```
> netsh http delete sslcert ipport=0.0.0.0:8146
```

- b. Vincule o certificado CA recém-adquirido ao servidor SnapCenter e à porta SMCore.

```
> $cert = "<CA_certificate_thumbprint>"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port/IIS port>  
certhash=$cert appid="$guid" clientcertnegotiation=enable  
verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:<SMCore Port/IIS port>
```

Por exemplo,

```
> $cert = "abc123abc123abc123abc123"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0:8146 certhash=$cert appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:8146
```

```
> netsh http show sslcert ipport=0.0.0.0:8145
```

2. Para acessar a permissão para o certificado da CA, adicione o usuário do servidor web IIS padrão do SnapCenter "**IIS AppPool\ SnapCenter**" na lista de permissões de certificado executando as seguintes etapas para acessar o certificado da CA recém-adquirido.
  - a. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo > Adicionar/Remover SnapIn**.
  - b. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
  - c. Na janela do snap-in Certificados, selecione a opção **Conta de computador** e clique em **Concluir**.
  - d. Clique em **Console Root > Certificados – Computador local > Pessoal > Certificados**.
  - e. Selecione o certificado SnapCenter .
  - f. Para iniciar o assistente para adicionar usuário/permissão, clique com o botão direito do mouse no certificado da CA e selecione **Todas as tarefas > Gerenciar chaves privadas**.
  - g. Clique em **Adicionar**, no assistente Selecionar usuários e grupos altere o local para o nome do computador local (o mais alto na hierarquia)
  - h. Adicione o usuário IIS AppPool\ SnapCenter e conceda permissões de controle total.
3. Para **permissão do certificado CA IIS**, adicione a nova entrada de chaves de registro DWORD no SnapCenter Server a partir do seguinte caminho:

No editor de registro do Windows, navegue até o caminho mencionado abaixo,

```
HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
```

4. Crie uma nova entrada de chave de registro DWORD no contexto da configuração do registro SCHANNEL.

```
SendTrustedIssuerList = 0
```

```
ClientAuthTrustMode = 2
```

## Configurar o plug-in SnapCenter do Windows para comunicação SSL bidirecional

Você deve configurar o plug-in SnapCenter do Windows para comunicação SSL bidirecional usando comandos do PowerShell.

### Antes de começar

Certifique-se de que a impressão digital do certificado da CA esteja disponível.

### Passos

1. Para vincular a porta, execute as seguintes ações no host do plug-in do Windows para a porta 8145 do SMCORE (padrão).
  - a. Remova a vinculação de porta do certificado autoassinado existente do SnapCenter usando o seguinte comando do PowerShell.

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

Por exemplo,

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

- b. Vincule o certificado CA recém-adquirido à porta SMCORE.

```
> $cert = "<CA_certificate_thumbprint>"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert  
appid="$guid" clientcertnegotiation=enable  
verifyclientcertrevocation=disable
```

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

Por exemplo,

```
> $cert = "abc123abc123abc123abc123"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:8145
```

## Habilitar comunicação SSL bidirecional no host Windows

Você pode habilitar a comunicação SSL bidirecional para proteger a comunicação mútua entre o SnapCenter Server no host Windows e os plug-ins usando comandos do PowerShell.

### Antes de começar

Execute os comandos para todos os plug-ins e o agente SMCore primeiro e depois para o servidor.

## Passos

1. Para habilitar a comunicação SSL bidirecional, execute os seguintes comandos no SnapCenter Server para os plug-ins, o servidor e para cada um dos agentes para os quais a comunicação SSL bidirecional é necessária.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}  
-HostName <Plugin_HostName>
```

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}  
-HostName localhost
```

```
> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}
```

2. Execute a operação de reciclagem do pool de aplicativos do IIS SnapCenter usando o seguinte comando.

```
> Restart-WebAppPool -Name "SnapCenter"
```

3. Para plug-ins do Windows, reinicie o serviço SMCore executando o seguinte comando do PowerShell:

```
> Restart-Service -Name SnapManagerCoreService
```

## Desabilitar comunicação SSL bidirecional

Você pode desabilitar a comunicação SSL bidirecional usando comandos do PowerShell.

### Sobre esta tarefa

- Execute os comandos para todos os plug-ins e o agente SMCore primeiro e depois para o servidor.
- Quando você desabilita a comunicação SSL bidirecional, o certificado da CA e sua configuração não são removidos.
- Para adicionar um novo host ao SnapCenter Server, você deve desabilitar o SSL bidirecional para todos os hosts de plug-in.
- NLB e F5 não são suportados.

## Passos

1. Para desabilitar a comunicação SSL bidirecional, execute os seguintes comandos no SnapCenter Server para todos os hosts de plug-in e o host SnapCenter .

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}  
-HostName <Agent_HostName>
```

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}  
-HostName localhost
```

```
> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="false"}
```

2. Execute a operação de reciclagem do pool de aplicativos do IIS SnapCenter usando o seguinte comando.

```
> Restart-WebAppPool -Name "SnapCenter"
```

3. Para plug-ins do Windows, reinicie o serviço SMCore executando o seguinte comando do PowerShell:

```
> Restart-Service -Name SnapManagerCoreService
```

## **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 DOCUMENTOS, 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.