



# 在 **Windows** 主机上配置并启用双向 **SSL** 通信 SnapCenter software

NetApp  
November 06, 2025

# 目录

在 Windows 主机上配置并启用双向 SSL 通信 .....	1
在 Windows 主机上配置双向 SSL 通信 .....	1
配置 SnapCenter Windows 插件以进行双向 SSL 通信 .....	2
在 Windows 主机上启用双向 SSL 通信 .....	3
禁用双向 SSL 通信 .....	4

# 在 Windows 主机上配置并启用双向 SSL 通信

## 在 Windows 主机上配置双向 SSL 通信

您应该配置双向 SSL 通信以保护 Windows 主机上的SnapCenter服务器与插件之间的相互通信。

开始之前

- 您应该已经生成了具有最小支持密钥长度 3072 的 CA 证书 CSR 文件。
- CA证书应支持服务器认证和客户端认证。
- 您应该拥有一份包含私钥和指纹详细信息的 CA 证书。
- 您应该已经启用单向 SSL 配置。

有关详细信息，请参阅 ["配置CA证书部分。"](#)

- 您必须在所有插件主机和SnapCenter服务器上启用双向 SSL 通信。

不支持某些主机或服务器未启用双向 SSL 通信的环境。

步骤

1. 要绑定端口，请使用 PowerShell 命令在SnapCenter Server 主机上对SnapCenter IIS Web 服务器端口 8146（默认）执行以下步骤，并再次对 SMCore 端口 8145（默认）执行以下步骤。

- a. 使用以下 PowerShell 命令删除现有的SnapCenter自签名证书端口绑定。

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

例如，

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

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

- b. 将新采购的 CA 证书与SnapCenter服务器和 SMCore 端口绑定。

```
> $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>
```

例如，

```
> $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. 要访问 CA 证书的权限，请通过执行以下步骤在证书权限列表中添加 SnapCenter 的默认 IIS Web 服务器用户“**IIS AppPool\ SnapCenter**”来访问新购买的 CA 证书。

- a. 转到 Microsoft 管理控制台 (MMC)，然后单击 文件 > 添加/删除管理单元。
- b. 在“添加或删除管理单元”窗口中，选择“证书”，然后单击“添加”。
- c. 在证书管理单元窗口中，选择“计算机帐户”选项，然后单击“完成”。
- d. 单击 控制台根 > 证书 - 本地计算机 > 个人 > 证书。
- e. 选择 SnapCenter 证书。
- f. 要启动添加用户\权限向导，请右键单击 CA 证书并选择 所有任务 > 管理私钥。
- g. 单击“添加”，在“选择用户和组”向导中将位置更改为本地计算机名称（层次结构中的最顶层）
- h. 添加 IIS AppPool\ SnapCenter 用户，授予完全控制权限。

3. 对于 **CA** 证书 **IIS** 权限，从以下路径在 SnapCenter Server 中添加新的 DWORD 注册表项条目：

在 Windows 注册表编辑器中，遍历下面提到的路径，

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

4. 在 SCHANNEL 注册表配置上下文中创建新的 DWORD 注册表项条目。

```
SendTrustedIssuerList = 0
```

```
ClientAuthTrustMode = 2
```

## 配置 SnapCenter Windows 插件以进行双向 SSL 通信

您应该使用 PowerShell 命令配置 SnapCenter Windows 插件以进行双向 SSL 通信。

开始之前

确保 CA 证书指纹可用。

步骤

1. 要绑定端口，请在 Windows 插件主机上对 SMCORE 端口 8145（默认）执行以下操作。

- a. 使用以下 PowerShell 命令删除现有的SnapCenter自签名证书端口绑定。

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

例如,

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

- b. 将新采购的CA证书与SMCore端口绑定。

```
> $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>
```

例如,

```
> $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
```

## 在 Windows 主机上启用双向 SSL 通信

您可以启用双向 SSL 通信，以使用 PowerShell 命令保护 Windows 主机上的SnapCenter服务器与插件之间的相互通信。

开始之前

首先执行所有插件和 SMCore 代理的命令，然后执行服务器的命令。

步骤

1. 要启用双向 SSL 通信，请在SnapCenter服务器上运行以下命令，用于插件、服务器以及需要双向 SSL 通信的每个代理。

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

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

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

2. 使用以下命令执行 IIS SnapCenter 应用程序池回收操作。 > Restart-WebAppPool -Name "SnapCenter"
3. 对于 Windows 插件，通过运行以下 PowerShell 命令重新启动 SMCORE 服务：

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

## 禁用双向 SSL 通信

您可以使用 PowerShell 命令禁用双向 SSL 通信。

关于此任务

- 首先执行所有插件和 SMCORE 代理的命令，然后执行服务器的命令。
- 当您禁用双向 SSL 通信时，CA 证书及其配置不会被删除。
- 要向 SnapCenter Server 添加新主机，必须禁用所有插件主机的双向 SSL。
- 不支持 NLB 和 F5。

步骤

1. 要禁用双向 SSL 通信，请在 SnapCenter Server 上对所有插件主机和 SnapCenter 主机运行以下命令。

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

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

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

2. 使用以下命令执行 IIS SnapCenter 应用程序池回收操作。 > Restart-WebAppPool -Name "SnapCenter"
3. 对于 Windows 插件，通过运行以下 PowerShell 命令重新启动 SMCORE 服务：

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

## 版权信息

版权所有 © 2025 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

## 商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。