



Configure and enable two-way SSL communication on Windows host

SnapCenter Software 6.0

NetApp
July 23, 2024

This PDF was generated from https://docs.netapp.com/us-en/snapcenter/install/task_configure_two_way_ssl.html on July 23, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- Configure and enable two-way SSL communication on Windows host 1
- Configure two-way SSL communication on Windows host 1
- Enable two-way SSL communication on Windows host 3

Configure and enable two-way SSL communication on Windows host

Configure two-way SSL communication on Windows host

You should configure the two-way SSL communication to secure the mutual communication between SnapCenter Server on Windows host and the plug-ins.

Before you begin

- You should have generated the CA Certificate CSR file with the minimum supported key length of 3072.
- The CA certificate should support server authentication and client authentication.
- You should have a CA certificate with private key and thumbprint details.
- You should have enabled the one-way SSL configuration.

For more details, see [Configure CA certificate section](#).

- You must have enabled two-way SSL communication on all the plug-in hosts and the SnapCenter Server.

Environment with some hosts or server not enabled for two-way SSL communication is not supported.

Steps

1. To bind the port, perform the following steps on SnapCenter Server host for SnapCenter IIS web server port 8146 (default) and once again for SMCORE port 8145 (default) using PowerShell commands.
 - a. Remove the existing SnapCenter self-signed certificate port binding using the following PowerShell command.

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

For example,

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

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

- b. Bind the newly procured CA certificate with the SnapCenter server and SMCORE port.

```
> $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>
```

For example,

```
> $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. To access permission to the CA certificate, add the SnapCenter's default IIS web server user "**IIS AppPool\SnapCenter**" in the certificate permission list by performing the following steps to access the newly procured CA certificate.
 - a. Go to the Microsoft management console (MMC), and then click **File > Add/Remove SnapIn**.
 - b. In the Add or Remove Snap-ins window, select **Certificates** and then click **Add**.
 - c. In the Certificates snap-in window, select the **Computer account** option, and then click **Finish**.
 - d. Click **Console Root > Certificates – Local Computer > Personal > Certificates**.
 - e. Select the SnapCenter certificate.
 - f. To start the add user\permission wizard, right-click on the CA certificate and select **All Tasks > Manage private keys**.
 - g. Click on **Add**, on Select users and groups wizard change the location to local computer name (top most in the hierarchy)
 - h. Add the IIS AppPool\SnapCenter user, give full control permissions.
3. For **CA certificate IIS permission**, add the new DWORD registry keys entry in SnapCenter Server from the following path:

In the windows registry editor, traverse to the below mentioned path,

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

4. Create new DWORD registry key entry under the context of SCHANNEL registry configuration.

```
SendTrustedIssuerList = 0
```

```
ClientAuthTrustMode = 2
```

Configure SnapCenter Windows plug-in for Two-way SSL communication

You should configure SnapCenter Windows plug-in for two-way SSL communication using PowerShell commands.

Before you begin

Ensure that the CA certificate thumbprint is available.

Steps

1. To bind the port, perform the following actions on Windows plug-in host for SMCore port 8145 (default).

- a. Remove the existing SnapCenter self-signed certificate port binding using the following PowerShell command.

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

For example,

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

- b. Bind the newly procured CA certificate with the SMCore port.

```
> $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>
```

For example,

```
> $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
```

Enable two-way SSL communication on Windows host

You can enable two-way SSL communication to secure the mutual communication between SnapCenter Server on Windows host and the plug-ins using PowerShell commands.

Before you begin

Execute the commands for all the plug-ins and the SMCore agent first and then for server.

Steps

1. To enable the two-way SSL communication, run the following commands on the SnapCenter Server for the plug-ins, server, and for each of the agents for which the two-way SSL communication is required.

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

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

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

2. Perform the IIS SnapCenter Application pool recycle operation by using the following command. >
`Restart-WebAppPool -Name "SnapCenter"`

3. For Windows plug-ins, restart the SMCORE service by running the following PowerShell command:

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

Disable two-way SSL Communication

You can disable the two-way SSL communication using PowerShell commands.

About this task

- Execute the commands for all the plug-ins and the SMCORE agent first and then for server.
- When you disable the two-way SSL communication, the CA certificate and its configuration are not removed.
- To add a new host to SnapCenter Server, you must disable the two-way SSL for all plug-in hosts.
- NLB and F5 are not supported.

Steps

1. To disable the two-way SSL communication, run the following commands on SnapCenter Server for all the plug-in hosts and the SnapCenter host.

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

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

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

2. Perform the IIS SnapCenter Application pool recycle operation by using the following command. >
`Restart-WebAppPool -Name "SnapCenter"`

3. For Windows plug-ins, restart the SMCORE service by running the following PowerShell command:

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

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.