Configure CA Certificate

SnapCenter Software 4.5

NetApp
July 03, 2026

This PDF was generated from https://docs.netapp.com/us-en/snapcenter-45/protect-scc/reference_generate_CA_certificate_CSR_file.html on July 03, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Configure CA Certificate . . . 1
- Generate CA Certificate CSR file . . . 1
- Import CA certificates . . . 1
- Get the CA certificate thumbprint . . . 2
- Configure CA certificate with Windows host plug-in services . . . 2
- Configure the CA Certificate for the SnapCenter Custom Plug-ins service on Linux host . . . 3
  - Manage password for custom plug-in keystore and alias of the CA signed key pair in use . . . 3
  - Configure root or intermediate certificates to custom plug-in trust-store . . . 4
  - Configure CA signed key pair to custom plug-in trust-store . . . 4
  - Configure certificate revocation list (CRL) for SnapCenter Custom Plug-ins . . . 5
- Configure the CA Certificate for the SnapCenter Custom Plug-ins service on Windows host . . . 5
  - Manage password for custom plug-in keystore and alias of the CA signed key pair in use . . . 6
  - Configure root or intermediate certificates to custom plug-in trust-store . . . 6
  - Configure CA signed key pair to custom plug-in trust-store . . . 7
  - Configure certificate revocation list (CRL) for SnapCenter Custom Plug-ins . . . 7
- Enable CA Certificates for plug-ins . . . 8

Configure CA Certificate

Generate CA Certificate CSR file

You can generate a Certificate Signing Request (CSR) and import the certificate that can be obtained from a Certificate Authority (CA) using the generated CSR. The certificate will have a private key associated with it.

CSR is a block of encoded text that is given to an authorized certificate vendor to procure the signed CA certificate.

For information to generate a CSR, see How to generate CA Certificate CSR file.

If you own the CA certificate for your domain (*.domain.company.com) or your system (machine1.domain.company.com), you can skip generating the CA Certificate CSR file. You can deploy the existing CA certificate with SnapCenter.

For cluster configurations, the cluster name (virtual cluster FQDN), and the respective host names should be mentioned in the CA certificate. The certificate can be updated by filling the Subject Alternative Name (SAN) field before procuring the certificate. For a wild card certificate (*.domain.company.com), the certificate will contain all the hostnames of the domain implicitly.

Import CA certificates

You must import the CA certificates to the SnapCenter Server and the Windows host plug-ins using the Microsoft management console (MMC).

Steps

1. Go to the Microsoft management console (MMC), and then click **File** > **Add/Remove Snapin**.
2. In the **Add or Remove Snap-ins** window, select **Certificates** and then click **Add**.
3. In the **Certificates snap-in** window, select the **Computer account** option, and then click **Finish**.
4. Click **Console Root** > **Certificates – Local Computer** > **Trusted Root Certification Authorities** > **Certificates**.
5. Right-click on the folder “Trusted Root Certification Authorities”, and then select **All Tasks** > **Import** to start the import wizard.
6. Complete the wizard, as follows:

In this wizard window…	Do the following…
Import Private Key	Select the option **Yes**, import the private key, and then click **Next**.
Import File Format	Make no changes; click **Next**.
Security	Specify the new password to be used for the exported certificate, and then click **Next**.

In this wizard window…	Do the following…
Completing the Certificate Import Wizard	Review the summary, and then click **Finish** to start the import.

Importing certificate should be bundled with the private key (supported formats are: *.pfx, *.p12, *.p7b).

7. Repeat Step 5 for the “Personal” folder.

Get the CA certificate thumbprint

A certificate thumbprint is a hexadecimal string that identifies a certificate. A thumbprint is calculated from the content of the certificate using a thumbprint algorithm.

Steps

1. Perform the following on the GUI:
   a. Double-click the certificate.
   b. In the Certificate dialog box, click the **Details** tab.
   c. Scroll through the list of fields and click **Thumbprint**.
   d. Copy the hexadecimal characters from the box.
   e. Remove the spaces between the hexadecimal numbers.

      For example, if the thumbprint is: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", after removing the spaces, it will be: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Perform the following from PowerShell:
   a. Run the following command to list the thumbprint of the installed certificate and identify the recently installed certificate by the subject name.

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Copy the thumbprint.

Configure CA certificate with Windows host plug-in services

You should configure the CA certificate with Windows host plug-in services to activate the installed digital certificate.

Perform the following steps on the SnapCenter Server and all the plug-in hosts where CA certificates are already deployed.

Steps

1. Remove the existing certificate binding with SMCore default port 8145, by running the following command:

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

For example:

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

2. Bind the newly installed certificate with the Windows host plug-in services, by running the following commands:

```
> $cert = "<certificate thumbprint>"

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

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

For example:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert
appid="$guid"
```

Configure the CA Certificate for the SnapCenter Custom Plug-ins service on Linux host

You should manage the password of the custom plug-ins keystore and its certificate, configure the CA certificate, configure root or intermediate certificates to the custom plug-ins trust-store, and configure CA signed key pair to custom plug-ins trust-store with SnapCenter Custom Plug-ins service to activate the installed digital certificate.

Custom plug-ins uses the file 'keystore.jks', which is located at */opt/NetApp/snapcenter/scc/etc* both as its trust-store and key-store.

Manage password for custom plug-in keystore and alias of the CA signed key pair in use

Steps

1. You can retrieve custom plug-in keystore default password from custom plug-in agent property file.

   It is the value corresponding to the key 'KEYSTORE_PASS'.

2. Change the keystore password:

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

3. Change the password for all aliases of private key entries in the keystore to the same password used for the keystore:

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

Update the same for the key KEYSTORE_PASS in *agent.properties* file.

4. Restart the service after changing the password.

> Password for custom plug-in keystore and for all the associated alias password of the private key should be same.

Configure root or intermediate certificates to custom plug-in trust-store

You should configure the root or intermediate certificates without the private key to custom plug-in trust-store.

Steps

1. Navigate to the folder containing the custom plug-in keystore: /opt/NetApp/snapcenter/scc/etc.
2. Locate the file 'keystore.jks'.
3. List the added certificates in the keystore:

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

4. Add a root or intermediate certificate:

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

5. Restart the service after configuring the root or intermediate certificates to custom plug-in trust-store.

> You should add the root CA certificate and then the intermediate CA certificates.

Configure CA signed key pair to custom plug-in trust-store

You should configure the CA signed key pair to the custom plug-in trust-store.

Steps

1. Navigate to the folder containing the custom plug-in keystore /opt/NetApp/snapcenter/scc/etc.
2. Locate the file 'keystore.jks'.
3. List the added certificates in the keystore:

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

4. Add the CA certificate having both private and public key.

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

5. List the added certificates in the keystore.

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

6. Verify that the keystore contains the alias corresponding to the new CA certificate, which was added to the keystore.
7. Change the added private key password for CA certificate to the keystore password.

   Default custom plug-in keystore password is the value of the key KEYSTORE_PASS in agent.properties file.

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

8. If the alias name in the CA certificate is long and contains space or special characters ("*",","), change the alias name to a simple name:

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

9. Configure the alias name from CA certificate in agent.properties file.

   Update this value against the key SCC_CERTIFICATE_ALIAS.

10. Restart the service after configuring the CA signed key pair to custom plug-in trust-store.

Configure certificate revocation list (CRL) for SnapCenter Custom Plug-ins

About this task

- SnapCenter Custom Plug-ins will search for the CRL files in a pre-configured directory.
- Default directory for the CRL files for SnapCenter Custom Plug-ins is ' opt/NetApp/snapcenter/scc/etc/crl'.

Steps

1. You can modify and update the default directory in agent.properties file against the key CRL_PATH.

   You can place more than one CRL file in this directory. The incoming certificates will be verified against each CRL.

Configure the CA Certificate for the SnapCenter Custom Plug-ins service on Windows host

You should manage the password of the custom plug-ins keystore and its certificate, configure the CA certificate, configure root or intermediate certificates to the custom plug-ins trust-store, and configure CA signed key pair to custom plug-ins trust-store with SnapCenter Custom Plug-ins service to activate the installed digital certificate.

Custom plug-ins uses the file *keystore.jks*, which is located at *C:\Program*

Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc both as its trust-store and key-store.

Manage password for custom plug-in keystore and alias of the CA signed key pair in use

Steps

1. You can retrieve custom plug-in keystore default password from custom plug-in agent property file.

   It is the value corresponding to the key *KEYSTORE_PASS*.

2. Change the keystore password:

   keytool -storepasswd -keystore keystore.jks

   > If the "keytool" command is not recognized on the Windows command prompt, replace the keytool command with its complete path.

   C:\Program Files\Java\<jdk_version>\bin\keytool.exe" -storepasswd -keystore keystore.jks

3. Change the password for all aliases of private key entries in the keystore to the same password used for the keystore:

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

   Update the same for the key KEYSTORE_PASS in *agent.properties* file.

4. Restart the service after changing the password.

   > Password for custom plug-in keystore and for all the associated alias password of the private key should be same.

Configure root or intermediate certificates to custom plug-in trust-store

You should configure the root or intermediate certificates without the private key to custom plug-in trust-store.

Steps

1. Navigate to the folder containing the custom plug-in keystore *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Locate the file 'keystore.jks'.
3. List the added certificates in the keystore:

   keytool -list -v -keystore keystore.jks

4. Add a root or intermediate certificate:

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

5. Restart the service after configuring the root or intermediate certificates to custom plug-in trust-store.

> You should add the root CA certificate and then the intermediate CA certificates.

Configure CA signed key pair to custom plug-in trust-store

You should configure the CA signed key pair to the custom plug-in trust-store.

Steps

1. Navigate to the folder containing the custom plug-in keystore *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Locate the file *keystore.jks*.
3. List the added certificates in the keystore:

   keytool -list -v -keystore keystore.jks

4. Add the CA certificate having both private and public key.

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

5. List the added certificates in the keystore.

   keytool -list -v -keystore keystore.jks

6. Verify that the keystore contains the alias corresponding to the new CA certificate, which was added to the keystore.
7. Change the added private key password for CA certificate to the keystore password.

   Default custom plug-in keystore password is the value of the key KEYSTORE_PASS in agent.properties file.

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

8. Configure the alias name from CA certificate in *agent.properties* file.

   Update this value against the key SCC_CERTIFICATE_ALIAS.

9. Restart the service after configuring the CA signed key pair to custom plug-in trust-store.

Configure certificate revocation list (CRL) for SnapCenter Custom Plug-ins

About this task

- To download the latest CRL file for the related CA certificate see How to update certificate revocation list file in SnapCenter CA Certificate.
- SnapCenter Custom Plug-ins will search for the CRL files in a pre-configured directory.
- Default directory for the CRL files for SnapCenter Custom Plug-ins is *'C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\ etc\crl'*.

Steps

1. You can modify and update the default directory in *agent.properties* file against the key CRL_PATH.
2. You can place more than one CRL file in this directory.

   The incoming certificates will be verified against each CRL.

Enable CA Certificates for plug-ins

You should configure the CA certificates and deploy the CA certificates in the SnapCenter Server and the corresponding plug-in hosts. You should enable the CA certificate validation for the plug-ins.

What you will need

- You can enable or disable the CA certificates using the run *Set-SmCertificateSettings* cmdlet.
- You can display the certificate status for the plug-ins using the *Get-SmCertificateSettings*.

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command_name*. Alternatively, you can also refer to the SnapCenter Software Cmdlet Reference Guide.

Steps

1. In the left navigation pane, click **Hosts**.
2. In the Hosts page, click **Managed Hosts**.
3. Select single or multiple plug-in hosts.
4. Click **More options**.
5. Select **Enable Certificate Validation**.

After you finish

The Managed Hosts tab host displays a padlock and the color of the padlock indicates the status of the connection between SnapCenter Server and the plug-in host.

- indicates that the CA certificate is neither enabled nor assigned to the plug-in host.
- indicates that the CA certificate is successfully validated.
- indicates that the CA certificate could not be validated.
- indicates that the connection information could not be retrieved.

> When the status is yellow or green, the data protection operations completes successfully.

Copyright information

Copyright © 2026 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.