



# **Install SnapCenter Plug-in for Microsoft Exchange Server**

**SnapCenter Software 4.9**

NetApp  
March 20, 2024

This PDF was generated from [https://docs.netapp.com/us-en/snapcenter-49/protect-sce/concept\\_install\\_snapcenter\\_plug\\_in\\_for\\_microsoft\\_exchange\\_server.html](https://docs.netapp.com/us-en/snapcenter-49/protect-sce/concept_install_snapcenter_plug_in_for_microsoft_exchange_server.html) on March 20, 2024. Always check docs.netapp.com for the latest.

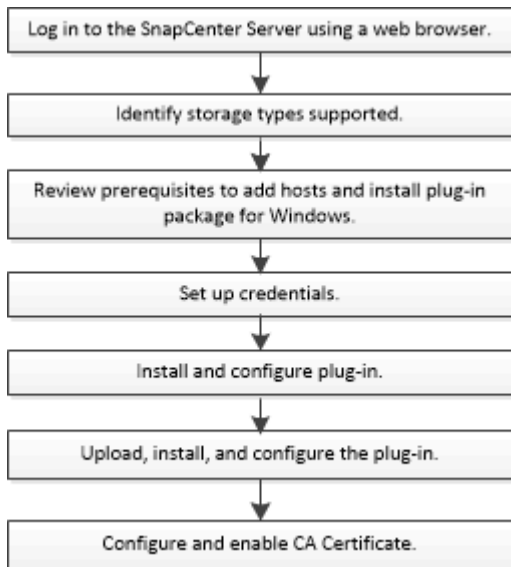
# Table of Contents

- Install SnapCenter Plug-in for Microsoft Exchange Server ..... 1
  - Installation workflow of SnapCenter Plug-in for Microsoft Exchange Server ..... 1
  - Prerequisites to add hosts and install SnapCenter Plug-in for Microsoft Exchange Server ..... 1
  - Set up credentials for SnapCenter Plug-in for Windows ..... 5
  - Configure gMSA on Windows Server 2012 or later ..... 6
  - Add hosts and install Plug-in for Exchange ..... 8
  - Install Plug-in for Exchange from the SnapCenter Server host using PowerShell cmdlets ..... 12
  - Install the SnapCenter Plug-in for Exchange silently from the command line ..... 13
  - Monitor SnapCenter plug-in package installation status ..... 14
  - Configure CA Certificate ..... 15
  - Configure SnapManager 7.x for Exchange and SnapCenter to coexist ..... 18

# Install SnapCenter Plug-in for Microsoft Exchange Server

## Installation workflow of SnapCenter Plug-in for Microsoft Exchange Server

You should install and set up SnapCenter Plug-in for Microsoft Exchange Server if you want to protect Exchange databases.



## Prerequisites to add hosts and install SnapCenter Plug-in for Microsoft Exchange Server

Before you add a host and install the plug-in packages, you must complete all the requirements.

- If you are using iSCSI, the iSCSI service must be running.
- You must have a domain user with local administrator privileges with local login permissions on the remote host.
- You must be using Microsoft Exchange Server 2013, 2016, or 2019 for standalone and Database Availability Group configurations.
- When installing a plug-in on a Windows host, if you specify a credential that is not built-in or if the user belongs to a local workgroup user, you must disable UAC on the host.
- If you manage cluster nodes in SnapCenter, you must have a user with administrative privileges to all the nodes in the cluster.
- You must have a user with administrative permissions on the Exchange Server.
- If SnapManager for Microsoft Exchange Server and SnapDrive for Windows are already installed, you must unregister the VSS Hardware Provider used by SnapDrive for Windows before you install Plug-in for Exchange on the same Exchange Server to ensure successful data protection using SnapCenter.
- If SnapManager for Microsoft Exchange Server and Plug-in for Exchange are installed on the same server,

you must suspend or delete from the Windows scheduler all schedules created by SnapManager for Microsoft Exchange Server.

- The host must be resolvable to the fully qualified domain name (FQDN) from the server. If the hosts file is modified to make it resolvable and if both the short name and the FQDN are specified in the hosts file, create an entry in the SnapCenter hosts file in the following format: `<ip_address> <host_fqdn> <host_name>`.
- Ensure the following ports are not blocked in the firewall, otherwise the add host operation fails. To resolve this issue, you must configure the dynamic port range. For more information, see [Microsoft documentation](#).
  - Port range 50000 - 51000 for Windows 2016 and Exchange 2016
  - Port range 6000 - 6500 for Windows 2012 R2 and Exchange 2013
  - Port range 49152 - 65536 for Windows 2019


To identify the port range, execute the following commands:



- netsh int ipv4 show dynamicport tcp
- netsh int ipv4 show dynamicport udp
- netsh int ipv6 show dynamicport tcp
- netsh int ipv6 show dynamicport udp

## Host requirements to install SnapCenter Plug-ins Package for Windows

Before you install the SnapCenter Plug-ins Package for Windows, you should be familiar with some basic host system space requirements and sizing requirements.

Item	Requirements
Operating Systems	Microsoft Windows  For the latest information about supported versions, see the <a href="#">NetApp Interoperability Matrix Tool</a> .
Minimum RAM for the SnapCenter plug-in on host	1 GB
Minimum install and log space for the SnapCenter plug-in on host	5 GB   You should allocate sufficient disk space and monitor the storage consumption by the logs folder. The log space required varies depending on the number of the entities to be protected and the frequency of data protection operations. If there is no sufficient disk space, the logs will not be created for the recently run operations.

Item	Requirements
Required software packages	<ul style="list-style-type: none"> <li>• Microsoft .NET Framework 4.7.2 or later</li> <li>• Windows Management Framework (WMF) 4.0 or later</li> <li>• PowerShell 4.0 or later</li> </ul> <p>For the latest information about supported versions, see the <a href="#">NetApp Interoperability Matrix Tool</a>.</p> <p>For .NET specific troubleshooting information, see <a href="#">SnapCenter upgrade or install fails for legacy systems that do not have internet connectivity</a>.</p>

## Exchange Server privileges required

To enable SnapCenter to add Exchange Server or DAG, and to install SnapCenter Plug-in for Microsoft Exchange Server on a host or DAG, you must configure SnapCenter with credentials for a user with a minimum set of privileges and permissions.


You must have a domain user with local administrator privileges, and with local login permissions on the remote Exchange host, as well as administrative permissions on all the nodes in the DAG. The domain user requires the following minimum permissions:

- Add-MailboxDatabaseCopy
- Dismount-Database
- Get-AdServerSettings
- Get-DatabaseAvailabilityGroup
- Get-ExchangeServer
- Get-MailboxDatabase
- Get-MailboxDatabaseCopyStatus
- Get-MailboxServer
- Get-MailboxStatistics
- Get-PublicFolderDatabase
- Move-ActiveMailboxDatabase
- Move-DatabasePath -ConfigurationOnly:\$true
- Mount-Database
- New-MailboxDatabase
- New-PublicFolderDatabase
- Remove-MailboxDatabase
- Remove-MailboxDatabaseCopy
- Remove-PublicFolderDatabase
- Resume-MailboxDatabaseCopy

- Set-AdServerSettings
- Set-MailboxDatabase -allowfilerestore:\$true
- Set-MailboxDatabaseCopy
- Set-PublicFolderDatabase
- Suspend-MailboxDatabaseCopy
- Update-MailboxDatabaseCopy

## Host requirements to install SnapCenter Plug-ins Package for Windows

Before you install the SnapCenter Plug-ins Package for Windows, you should be familiar with some basic host system space requirements and sizing requirements.

Item	Requirements
Operating Systems	<p>Microsoft Windows</p> <p>For the latest information about supported versions, see the <a href="#">NetApp Interoperability Matrix Tool</a>.</p>
Minimum RAM for the SnapCenter plug-in on host	1 GB
Minimum install and log space for the SnapCenter plug-in on host	<p>5 GB</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">  <p>You should allocate sufficient disk space and monitor the storage consumption by the logs folder. The log space required varies depending on the number of the entities to be protected and the frequency of data protection operations. If there is no sufficient disk space, the logs will not be created for the recently run operations.</p> </div>
Required software packages	<ul style="list-style-type: none"> <li>• Microsoft .NET Framework 4.7.2 or later</li> <li>• Windows Management Framework (WMF) 4.0 or later</li> <li>• PowerShell 4.0 or later</li> </ul> <p>For the latest information about supported versions, see the <a href="#">NetApp Interoperability Matrix Tool</a>.</p> <p>For .NET specific troubleshooting information, see <a href="#">SnapCenter upgrade or install fails for legacy systems that do not have internet connectivity</a>.</p>

# Set up credentials for SnapCenter Plug-in for Windows

SnapCenter uses credentials to authenticate users for SnapCenter operations. You should create credentials for installing the plug-in package and additional credentials for performing data protection operations on databases.

## About this task

You must set up credentials for installing plug-ins on Windows hosts. Although you can create credentials for Windows after deploying hosts and installing plug-ins, the best practice is to create credentials after you add SVMs, before you deploy hosts and install plug-ins.

Set up the credentials with administrator privileges, including administrator rights on the remote host.

If you set up credentials for individual resource groups and the username does not have full admin privileges, you must assign at least the resource group and backup privileges to the username.

## Steps

1. In the left navigation pane, click **Settings**.
2. In the Settings page, click **Credential**.
3. Click **New**.

The Credential window is displayed.

4. In the Credential page, do the following:

For this field...	Do this...
Credential name	Enter a name for the credential.

For this field...	Do this...
Username	<p>Enter the user name used for authentication.</p> <ul style="list-style-type: none"> <li>• Domain administrator or any member of the administrator group</li> </ul> <p>Specify the domain administrator or any member of the administrator group on the system on which you are installing the SnapCenter plug-in. Valid formats for the Username field are:</p> <ul style="list-style-type: none"> <li>◦ NetBIOS\UserName</li> <li>◦ Domain FQDN\UserName</li> </ul> <ul style="list-style-type: none"> <li>• Local administrator (for workgroups only)</li> </ul> <p>For systems that belong to a workgroup, specify the built-in local administrator on the system on which you are installing the SnapCenter plug-in. You can specify a local user account that belongs to the local administrators group if the user account has elevated privileges or the User Access control feature is disabled on the host system. The valid format for the Username field is: UserName</p>
Password	Enter the password used for authentication.
Authentication	Select Windows as the authentication mode.

5. Click **OK**.

## Configure gMSA on Windows Server 2012 or later

Windows Server 2012 or later enables you to create a group Managed Service Account (gMSA) that provides automated service account password management from a managed domain account.

### Before you begin

- You should have a Windows Server 2012 or later domain controller.
- You should have a Windows Server 2012 or later host, which is a member of the domain.

### Steps

1. Create a KDS root key to generate unique passwords for each object in your gMSA.
2. For each domain, run the following command from the Windows domain controller: Add-KDSRootKey -EffectiveImmediately
3. Create and configure your gMSA:



- a. Create a user group account in the following format:

```
domainName\accountName$
```

- b. Add computer objects to the group.
- c. Use the user group you just created to create the gMSA.

For example,

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>
```

- d. Run `Get-ADServiceAccount` command to verify the service account.

#### 4. Configure the gMSA on your hosts:

- a. Enable the Active Directory module for Windows PowerShell on the host where you want to use the gMSA account.

To do this, run the following command from PowerShell:

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
[ ] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- b. Restart your host.
- c. Install the gMSA on your host by running the following command from the PowerShell command prompt: `Install-AdServiceAccount <gMSA>`
- d. Verify your gMSA account by running the following command: `Test-AdServiceAccount <gMSA>`

5. Assign the administrative privileges to the configured gMSA on the host.
6. Add the Windows host by specifying the configured gMSA account in the SnapCenter Server.

SnapCenter Server will install the selected plug-ins on the host and the specified gMSA will be used as the service log on account during the plug-in installation.

## Add hosts and install Plug-in for Exchange

You can use the SnapCenter Add Host page to add Windows hosts. The Plug-in for Exchange is automatically installed on the specified host. This is the recommended method for installing plug-ins. You can add a host and install a plug-in either for an individual host or a cluster.

### Before you begin

- You must be a user that is assigned to a role that has the plug-in install and uninstall permissions, such as the SnapCenter Admin.
- When installing a plug-in on a Windows host, if you specify a credential that is not built-in, or if the user belongs to a local workgroup user, you must disable UAC on the host.
- The message queueing service must be running.
- If you are using group Managed Service Account (gMSA), you should configure gMSA with administrative privileges. For information, see [Configure group Managed Service Account on Windows Server 2012 or later for Microsoft Exchange Server](#).

### About this task

- You cannot add a SnapCenter Server as a plug-in host to another SnapCenter Server.
- You can add a host and install plug-in packages either for an individual host or a cluster.
- If an exchange node is part of a DAG, you cannot add only one node into the SnapCenter Server.
- If you are installing plug-ins on a cluster (Exchange DAG), they are installed on all of the nodes of the cluster even if some of nodes do not have databases on NetApp LUNs.

Beginning with SnapCenter 4.6, SCE supports multitenancy and you can add a host using the following methods:

Add host operation	4.5 and earlier	4.6 and later
Add IP-less DAG in cross or different domain	Not supported	Supported
Add multiple IP DAGs with unique names, residing in the same or cross domain	Supported	Supported
Add multiple IP or IP-less DAGs which have same host names and/or DB name in cross domain	Not supported	Supported
Add multiple IP/IP-less DAGs with the same name and cross domain	Not supported	Supported

Add host operation	4.5 and earlier	4.6 and later
Add multiple standalone hosts with the same name and cross domain	Not supported	Supported


Plug-in for Exchange depends on SnapCenter Plug-ins Package for Windows, and the versions must be the same. During the Plug-in for Exchange installation, SnapCenter Plug-ins Package for Windows is selected by default and is installed along with the VSS Hardware Provider.


If SnapManager for Microsoft Exchange Server and SnapDrive for Windows are already installed, and you want to install Plug-in for Exchange on the same Exchange Server, you must unregister the VSS Hardware Provider used by SnapDrive for Windows because it is incompatible with the VSS Hardware Provider installed with Plug-in for Exchange and SnapCenter Plug-ins Package for Windows. For more information, see [How to manually register the Data ONTAP VSS Hardware Provider](#).

### Steps

1. In the left navigation pane, click **Hosts**.
2. Verify that **Managed Hosts** is selected at the top.
3. Click **Add**.
4. In the Hosts page, do the following:

For this field...	Do this...
Host Type	<p>Select <b>Windows</b> as the host type.</p> <p>SnapCenter Server adds the host and then installs on the host the Plug-in for Windows and the Plug-in for Exchange if they are not already installed.</p> <p>Plug-in for Windows and Plug-in for Exchange must be the same version. If a different version of Plug-in for Windows was previously installed, SnapCenter updates the version as part of the installation.</p>


For this field...	Do this...
Host name	<p data-bbox="841 159 1482 226">Enter the fully qualified domain name (FQDN) or the IP address of the host.</p> <p data-bbox="841 260 1482 359">SnapCenter depends on the proper configuration of the DNS. Therefore, the best practice is to enter the fully qualified domain name (FQDN).</p> <p data-bbox="841 392 1442 459">An IP address is supported for untrusted domain hosts only if it resolves to the FQDN.</p> <p data-bbox="841 493 1471 560">If you are adding a host using SnapCenter and it is part of a subdomain, you must provide the FQDN.</p> <p data-bbox="841 594 1471 661">You can enter IP addresses or the FQDN of one of the following:</p> <ul data-bbox="867 695 1101 774" style="list-style-type: none"><li data-bbox="867 695 1101 728">• Stand-alone host</li><li data-bbox="867 743 1081 774">• Exchange DAG</li></ul> <p data-bbox="889 808 1292 842">For an Exchange DAG, you can:</p> <ul data-bbox="915 875 1471 1245" style="list-style-type: none"><li data-bbox="915 875 1438 974">◦ Add a DAG by providing the DAG name, DAG IP address, node name, or node IP address.</li><li data-bbox="915 989 1438 1087">◦ Add the IP less DAG cluster by providing the IP address or the FQDN of one of the DAG cluster nodes.</li><li data-bbox="915 1102 1471 1245">◦ Add IP less DAG that resides in the same domain or different domain. You can also add multiple IP/IP less DAGs with the same name but different domains.</li></ul> <div data-bbox="873 1287 1446 1461" style="border: 1px solid #ccc; padding: 10px;"><p data-bbox="873 1352 927 1402"></p><p data-bbox="987 1287 1446 1461">For a stand-alone host or an Exchange DAG (cross-domain or same domain), it is recommended to provide FQDN or the IP address of the host or DAG.</p></div>


For this field...	Do this...
Credentials	<p>Select the credential name that you created, or create the new credentials.</p> <p>The credential must have administrative rights on the remote host. For details, see information about creating a credential.</p> <p>You can view details about the credentials by positioning your cursor over the credential name that you specified.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Credentials authentication mode is determined by the host type that you specify in the Add Host wizard.</p> </div>

5. In the Select Plug-ins to Install section, select the plug-ins to install.

When you select Plug-in for Exchange, SnapCenter Plug-in for Microsoft SQL Server is deselected automatically. Microsoft recommends that SQL Server and Exchange server not be installed on the same system due to the amount of memory used and other resource usage required by Exchange.

6. (Optional) Click **More Options**.

For this field...	Do this...
Port	<p>Either retain the default port number or specify the port number.</p> <p>The default port number is 8145. If the SnapCenter Server was installed on a custom port, that port number will be displayed as the default port.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>If you manually installed the plug-ins and specified a custom port, you must specify the same port. Otherwise, the operation fails.</p> </div>
Installation Path	<p>The default path is C:\Program Files\NetApp\SnapCenter.</p> <p>You can optionally customize the path.</p>
Add all hosts in the DAG	Select this check box when you add a DAG.
Skip preinstall checks	Select this check box if you already installed the plug-ins manually and you do not want to validate whether the host meets the requirements for installing the plug-in.

For this field...	Do this...
Use group Managed Service Account (gMSA) to run the plug-in services	<p>Select this check box if you want to use group Managed Service Account (gMSA) to run the plug-in services.</p> <p>Provide the gMSA name in the following format: <i>domainName\accountName\$</i>.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  <p>gMSA will be used as a log on service account only for SnapCenter Plug-in for Windows service.</p> </div>

7. Click **Submit**.

If you have not selected the Skip prechecks check box, the host is validated to determine whether it meets the requirements to install the plug-in. If the minimum requirements are not met, the appropriate error or warning messages are displayed.

If the error is related to disk space or RAM, you can update the web.config file located at `C:\Program Files\NetApp\SnapCenter WebApp` to modify the default values. If the error is related to other parameters, you must fix the issue.



In an HA setup, if you are updating web.config file, you must update the file on both nodes.

8. Monitor the installation progress.

## Install Plug-in for Exchange from the SnapCenter Server host using PowerShell cmdlets

You should install the Plug-in for Exchange from the SnapCenter GUI. If you do not want to use the GUI, you can use PowerShell cmdlets on the SnapCenter Server host or on a remote host.

### Before you begin

- SnapCenter Server must have been installed and configured.
- You must be a local administrator on the host or a user with administrative privileges.
- You must be a user that is assigned to a role that has the plug-in, install, and uninstall permissions, such as the SnapCenter Admin.
- You must have reviewed the installation requirements and types of supported configurations before installing the Plug-in for Exchange.
- The host on which you want the Plug-in for Exchange installed must be a Windows host.

### Steps

1. On the SnapCenter Server host, establish a session using the *Open-SmConnection* cmdlet, and then enter your credentials.
2. Add the host on which you want to install the Plug-in for Exchange using the *Add-SmHost* cmdlet with the required parameters.

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](#).

The host can be a standalone host or a DAG. If you specify a DAG, the *-IsDAG* parameter is required.

3. Install the Plug-in for Exchange using the *Install-SmHostPackage* cmdlet with the required parameters.

This command installs the Plug-in for Exchange on the specified host, and then registers the plug-in with SnapCenter.

## Install the SnapCenter Plug-in for Exchange silently from the command line

You should install Plug-in for Exchange from within the SnapCenter user interface. However, if you cannot for some reason, you can run the Plug-in for Exchange installation program unattended in silent mode from the Windows command line.

### Before you begin

- You must have backed up your Microsoft Exchange Server resources.
- You must have installed the SnapCenter plug-in packages.
- You must delete the earlier release of SnapCenter Plug-in for Microsoft SQL Server before installing.

For more information, see [How to Install a SnapCenter Plug-In manually and directly from the Plug-In Host](#).

### Steps

1. Validate whether *C:\temp* folder exists on the plug-in host and the logged in user has full access to it.
2. Download the SnapCenter Plug-in for Microsoft Windows from *C:\ProgramData\NetApp\SnapCenter\Package Repository*.

This path is accessible from the host where the SnapCenter Server is installed.

3. Copy the installation file to the host on which you want to install the plug-in.
4. From a Windows command prompt on the local host, navigate to the directory to which you saved the plug-in installation files.
5. Enter the following command to install the plug-in.

```
snapcenter_windows_host_plugin.exe"/silent /debuglog"<Debug_Log_Path>" /log"<Log_Path>"  
BI_SNAPCENTER_PORT=<Num> SUITE_INSTALLDIR="<Install_Directory_Path>"  
BI_SERVICEACCOUNT=<domain\administrator> BI_SERVICEPWD=<password>  
ISFeatureInstall=HPPW,SCW,SCE
```

For example:

```
C:\ProgramData\NetApp\SnapCenter\Package Repository\snapcenter_windows_host_plugin.exe"/silent  
/debuglog"C:\HPPW_SCSQL_Install.log" /log"C:\temp" BI_SNAPCENTER_PORT=8145  
SUITE_INSTALLDIR="C:\Program Files\NetApp\SnapCenter"  
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password  
ISFeatureInstall=HPPW,SCW,SCE
```



All the parameters passed during the installation of Plug-in for Exchange are case sensitive.

Enter the following values for the variables:

Variable	Value
<code>/debuglog"&lt;Debug_Log_Path&gt;</code>	Specify the name and location of the suite installer log file, as in the following example:  <code>Setup.exe /debuglog"C:\PathToLog\setupexe.log</code>
BI_SNAPCENTER_PORT	Specify the port on which SnapCenter communicates with SMCore.
SUITE_INSTALLDIR	Specify host plug-in package installation directory.
BI_SERVICEACCOUNT	Specify SnapCenter Plug-in for Microsoft Windows web service account.
BI_SERVICEPWD	Specify the password for SnapCenter Plug-in for Microsoft Windows web service account.
ISFeatureInstall	Specify the solution to be deployed by SnapCenter on remote host.

6. Monitor the Windows task scheduler, the main installation log file `C:\Installdebug.log`, and the additional installation files in `C:\Temp`.
7. Monitor the `%temp%` directory to check if the `msiexe.exe` installers are installing the software without errors.





The installation of Plug-in for Exchange registers the plug-in on the host and not on the SnapCenter Server. You can register the plug-in on the SnapCenter Server by adding the host using the SnapCenter GUI or PowerShell cmdlet. After the host is added, the plug-in is automatically discovered.

## Monitor SnapCenter plug-in package installation status




You can monitor the progress of SnapCenter plug-in package installation by using the Jobs page. You might want to check the progress of installation to determine when it is complete or if there is an issue.

### About this task

The following icons appear on the Jobs page and indicate the state of the operation:

-  In progress
-  Completed successfully



-  Failed
-  Completed with warnings or could not start due to warnings
-  Queued

## Steps

1. In the left navigation pane, click **Monitor**.
2. In the **Monitor** page, click **Jobs**.
3. In the **Jobs** page, to filter the list so that only plug-in installation operations are listed, do the following:
  - a. Click **Filter**.
  - b. Optional: Specify the start and end date.
  - c. From the Type drop-down menu, select **Plug-in installation**.
  - d. From the Status drop-down menu, select the installation status.
  - e. Click **Apply**.
4. Select the installation job and click **Details** to view the job details.
5. In the **Job Details** page, click **View logs**.

# 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.



CA Certificate RSA key length should be minimum 3072 bits.

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 <b>Yes</b> , import the private key, and then click <b>Next</b> .
Import File Format	Make no changes; click <b>Next</b> .
Security	Specify the new password to be used for the exported certificate, and then click <b>Next</b> .
Completing the Certificate Import Wizard	Review the summary, and then click <b>Finish</b> to start the import.



Importing certificate should be bundled with the private key (supported formats are: \*.pfx, \*.p12, and \*.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"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

## 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.

### Before you begin

- 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.

## Configure SnapManager 7.x for Exchange and SnapCenter to coexist

To enable SnapCenter Plug-in for Microsoft Exchange Server to coexist with SnapManager for Microsoft Exchange Server, you need to install SnapCenter Plug-in for Microsoft Exchange Server on the same Exchange Server on which SnapManager for Microsoft Exchange Server is installed, disable SnapManager for Exchange schedules, and configure new schedules and backups using SnapCenter Plug-in for Microsoft Exchange Server.

### Before you begin

- SnapManager for Microsoft Exchange Server and SnapDrive for Windows are already installed, and SnapManager for Microsoft Exchange Server backups exist on the system and in the SnapInfo directory.
- You should have deleted or reclaimed backups taken by SnapManager for Microsoft Exchange Server that you no longer require.
- You should have suspended or deleted all schedules created by SnapManager for Microsoft Exchange Server from the Windows scheduler.
- SnapCenter Plug-in for Microsoft Exchange Server and SnapManager for Microsoft Exchange Server can coexist on the same Exchange Server, but you cannot upgrade existing SnapManager for Microsoft Exchange Server installations to SnapCenter.

SnapCenter does not provide an option for the upgrade.

- SnapCenter does not support restoring Exchange databases from SnapManager for Microsoft Exchange Server backup.

If you do not uninstall SnapManager for Microsoft Exchange Server after the SnapCenter Plug-in for Microsoft Exchange Server installation and later want to restore a SnapManager for Microsoft Exchange Server backup, you must perform additional steps.

## Steps

1. Using PowerShell on all DAG nodes, determine whether the SnapDrive for Windows VSS Hardware Provider is registered: *vssadmin list providers*

```
C:\Program Files\NetApp\SnapDrive>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
  Provider type: Hardware
  Provider Id: {ddd3d232-a96f-4ac5-8f7b-250fd91fd102}
  Version: 7. 1. 4. 6845
```

2. From the SnapDrive directory, unregister the VSS Hardware Provider from SnapDrive for Windows: *navssprv.exe -r service -u*
3. Verify that the VSS Hardware Provider was removed: *vssadmin list providers*
4. Add the Exchange host to SnapCenter, and then install the SnapCenter Plug-in for Microsoft Windows and the SnapCenter Plug-in for Microsoft Exchange Server.
5. From the SnapCenter Plug-in for Microsoft Windows directory on all DAG nodes, verify that the VSS Hardware Provider is registered: *vssadmin list providers*

```
[PS] C:\Windows\system32>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
  Provider type: Hardware
  Provider Id: {31fca584-72be-45b6-9419-53a3277301d1}
  Version: 7. 0. 0. 5561
```

6. Stop the SnapManager for Microsoft Exchange Server backup schedules.
7. Using the SnapCenter GUI, create on-demand backups, configure scheduled backups, and configure retention settings.
8. Uninstall SnapManager for Microsoft Exchange Server.

If you do not uninstall SnapManager for Microsoft Exchange Server now and later want to restore a

SnapManager for Microsoft Exchange Server backup:

- a. Unregister SnapCenter Plug-in for Microsoft Exchange Server from all DAG nodes: *navssprv.exe -r service -u*

```
C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft  
Windows>navssprv.exe -r service -u
```

- b. From the *C:\Program Files\NetApp\SnapDrive\* directory, register SnapDrive for Windows on all DAG nodes: *navssprv.exe -r service -a hostname\username -p password*

## 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.