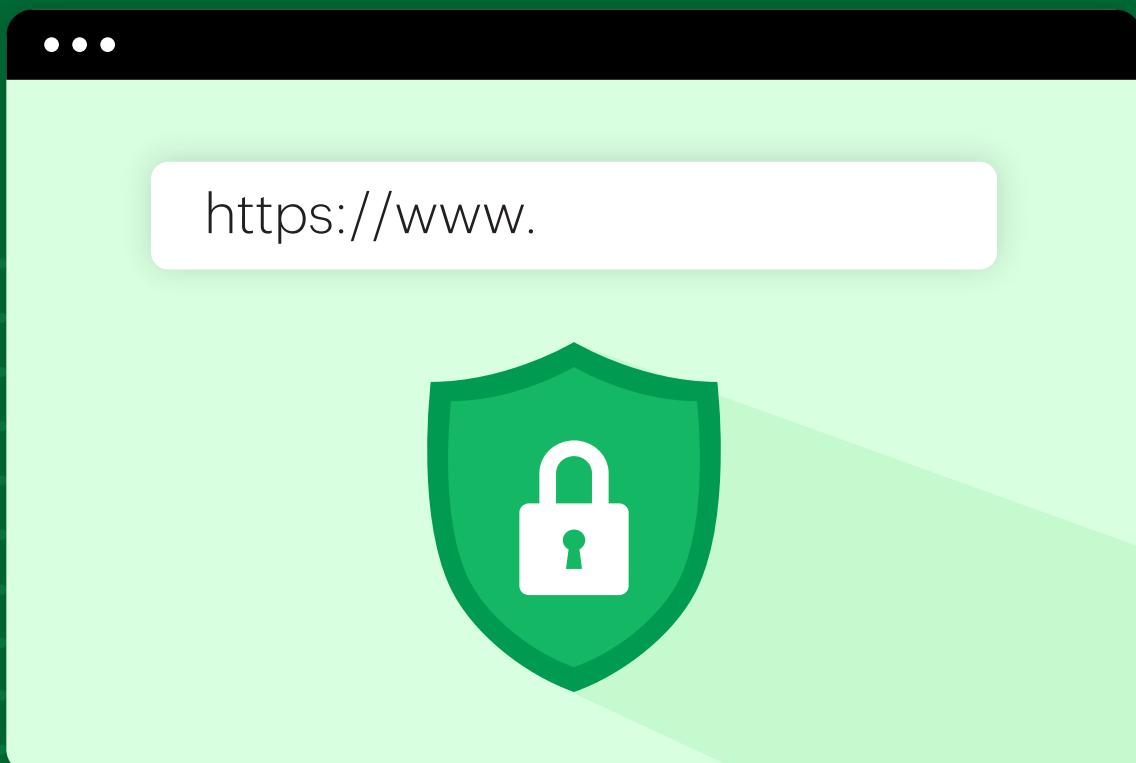


How to install an **SSL CERTIFICATE** in SharePoint Manager Plus



INTRODUCTION

This document will guide you through the process of installing the SSL certificate to secure the connection between SharePoint Manager Plus' server and the user's browser.

1. Enable SSL in SharePoint Manager Plus

1. Log in to SharePoint Manager Plus.
2. Navigate to **Admin > General Settings > Connection**.
3. Check the **Enable SSL Port (HTTPS)** option. The port number 8086 is entered by default. You can change it to a value of your choice.
4. Click **Save** and restart the product for the changes to take effect.

2. Create a certificate signing request (CSR)

1. Stop SharePoint Manager Plus.
 - i. If the product runs as an application, click **Start > All Programs > SharePoint Manager Plus > Stop SharePoint Manager Plus**.
 - ii. If the product runs as a Windows service, click **Start > Run**. Type **services.msc** and stop SharePoint Manager Plus.
2. Open **Command Prompt** and navigate to `<installation_directory>|ManageEngine|SharePoint Manager Plus|jre|bin` where `<installation_directory>` is the location where SharePoint Manager Plus is installed.
3. Execute the following command to create a keystore.

```
keytool -genkey -alias tomcat -keypass <your key password> -keyalg RSA  
-validity 1000 -keystore <domainName>.keystore
```

Replace `<your key password>` with a password of your choice and `<domainName>` with the name of your domain.

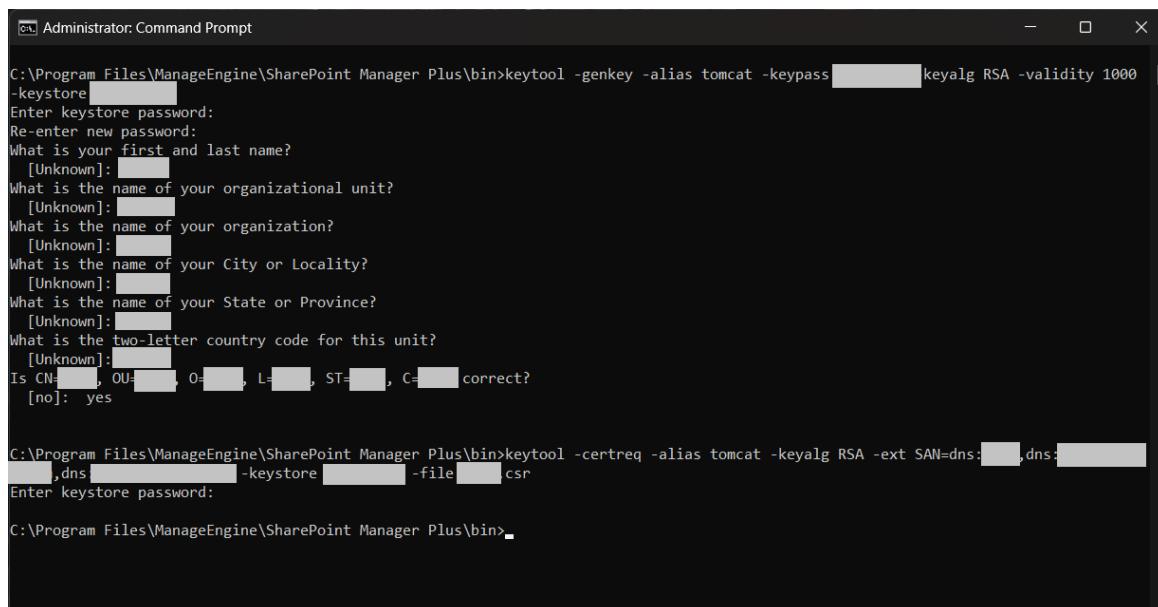
4. Type in your keystore password. To avoid any confusion, try giving the same password as your keypass.
5. You will be prompted to answer the following questions:

Question	Answer
What is your first name and last name?	Enter the NetBIOS or FQDN of the server in which SharePoint Manager Plus is configured.
What is the name of your Organizational unit?	Enter the name of the OU of your choice.
What is the name of your Organization?	Provide the legal name of your organization.
What is the name of your City or Locality?	Enter the city or locality name as provided in your organization's registered address.
What is the name of your state or province?	Enter the name of your state or province as provided in your organization's registered address.
What is the two-letter country code for this unit?	Provide the two-letter code of the country your organization is located in.

6. In the same path, execute the following command to create a CSR with subject alternative name (SAN).

```
keytool -certreq -alias tomcat -keyalg RSA -ext SAN=dns:server_name,dns:server
_name.domain.com,dns:server_name.domain1.com -keystore
<domainName>.keystore -file <domainName>.csr
```

Replace the `<domainName>` with the name of your domain and provide the appropriate **SAN** as shown in the figure below.



```
C:\Program Files\ManageEngine\SharePoint Manager Plus\bin>keytool -genkey -alias tomcat -keypass [REDACTED] -keyalg RSA -validity 1000 -keystore [REDACTED]
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: [REDACTED]
What is the name of your organizational unit?
[Unknown]: [REDACTED]
What is the name of your organization?
[Unknown]: [REDACTED]
What is the name of your City or Locality?
[Unknown]: [REDACTED]
What is the name of your State or Province?
[Unknown]: [REDACTED]
What is the two-letter country code for this unit?
[Unknown]: [REDACTED]
Is CN=[REDACTED], OU=[REDACTED], O=[REDACTED], L=[REDACTED], ST=[REDACTED], C=[REDACTED] correct?
[no]: yes

C:\Program Files\ManageEngine\SharePoint Manager Plus\bin>keytool -certreq -alias tomcat -keyalg RSA -ext SAN=dns:[REDACTED],dns:[REDACTED] -keystore [REDACTED] -file [REDACTED].csr
Enter keystore password:
C:\Program Files\ManageEngine\SharePoint Manager Plus\bin>
```

3. Issue the SSL certificate

a. Issue the SSL certificate using an internal CA.

An internal certificate authority (CA) is a member server or domain controller in a specific domain that has been assigned the role of a CA.

1. Connect to the Microsoft Certificate Services of your internal CA and click on the **Request a certificate** link.

Microsoft Active Directory Certificate Services – SSPQA1-DC1-CA

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

2. Click on **Advanced certificate request** and select the **Submit a certificate by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file** option.

Microsoft Certificate Services – admp

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

- [Create and submit a request to this CA.](#)
- [Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.](#)
- [Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.](#)

Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

3. Copy the content from your .csr file and paste it under the **Saved Request** field.

4. Select **Web Server** as the Certificate Template and click **Submit**.

Microsoft Active Directory Certificate Services – SSPQA1-DC1-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

```
7GxauJyP174NaSHD2uHFAay3L8nrHhQXzbbsLHw^
GV2FLMBB7/GFD5xvAppwCnq1hL1vP53aeP7FXS
1CJulw1IPmLRZ2zVzmb5aepr7PjNZB1e5cfFwxa
t0ipKmJ8N1hcuBgZsvish41IV18L10Gw==^
-----END NEW CERTIFICATE REQUEST-----^
```

Certificate Template:

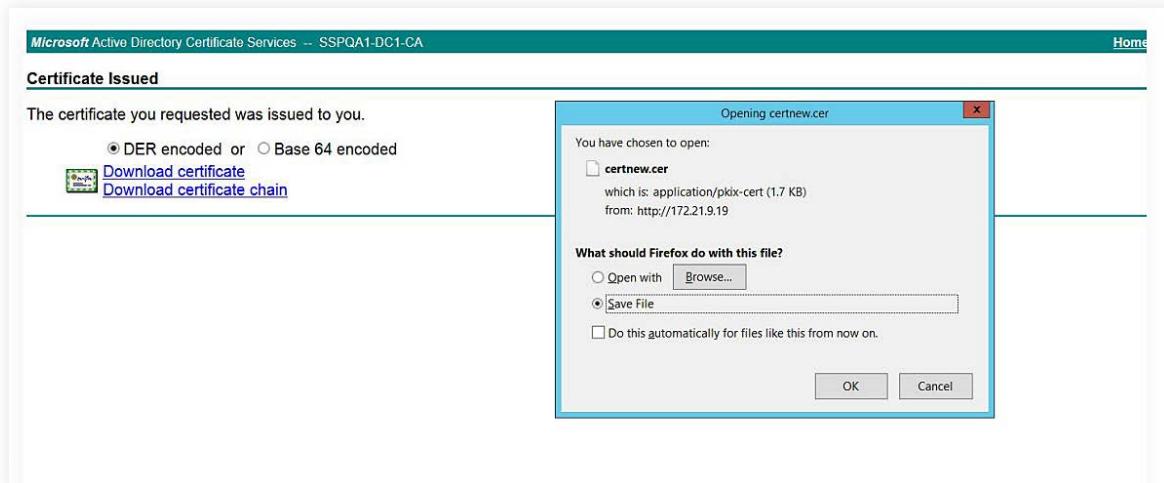
Web Server

Additional Attributes:

Attributes:

Submit >

5. Click the **Download Certificate Chain** link to download the issued **PKCS #7 Certificates** types. The downloaded certificate will be of the **.p7b** file format.
6. Copy and paste this **.p7b** file at **<installation_directory>|ManageEngine|SharePoint Manager Plus|jre|bin**.
7. Return to Microsoft Certificate Services and click the **Home** link at the top-right corner of the page.
8. Click **Download a CA certificate, chain certificate or CRL** link to download the CA root certificate.
9. Click **Download CA certificate** link to download and save the root certificate that is in the **.cer** format.



10. Copy and paste the **.cer** file at **<installation_directory>|ManageEngine|SharePoint Manager Plus|jre|bin**.
11. Open **Command Prompt** and navigate to the **<installation_directory>|ManageEngine|SharePoint Manager Plus|jre|bin** path and execute the following query to import the internal CA certificate into the **.keystore** file.

```
Keytool -import -trustcacerts -alias tomcat -file certnew.p7b -keystore
<keystore_name>.keystore
```

Replace **<keystore_name>** with the name of your keystore.

12. In the same path, execute the following query to add the internal CA's root certificate to the list of trusted CAs in the Java cacerts file.

```
keytool -import -alias <internal CA_name> -keystore ..\lib\security\cacerts -file certnew.cer
```

Note: Open the **.cer** file to get the name of your internal CA. When prompted, provide *changeit* as the keystore password.

b. Issue the SSL certificate using external CAs

1. To request a certificate from an external CA, submit the CSR to that CA.
2. Unzip the certificates returned by your CA and place them in <installation_directory>/ManageEngine/SharePoint Manager Plus/jre/bin folder.
3. Open **Command Prompt** and navigate to the <installation_directory>/ManageEngine/SharePoint Manager Plus/jre/bin folder.
4. Run the respective commands from the given list as applicable to your CA:

A. For GoDaddy certificates

- keytool -import -alias root -keystore <domainname>.keystore -trustcacerts -file gdrootg2.crt
- keytool -import -alias cross -keystore <domainname>.keystore -trustcacerts -file gdrootg2_cross.crt
- keytool -import -alias intermed -keystore <domainname>.keystore -trustcacerts -file gdig2.crt

For further reference, click [here](#).

B. For Verisign certificates

- keytool -import -alias intermediateCA -keystore <domainName>.keystore -trustcacerts -file <your intermediate certificate.cer>
- keytool -import -alias tomcat -keystore <domainName>.keystore -trustcacerts file admanager.cer

C. For Sectigo (previously Comodo CA) certificates

- keytool -import -trustcacerts -alias root -file AddTrustExternalCARoot.crt -keystore <domainName>.keystore
- keytool -import -trustcacerts -alias addtrust -file UTNAddTrustServerCA.crt -keystore <domainName>.keystore
- keytool -import -trustcacerts -alias ComodoUTNServer -file ComodoUTNServerCA.crt -keystore <domainName>.keystore
- keytool -import -trustcacerts -alias essentialSSL -file essentialSSLCA.crt -keystore <domainName>.keystore

For further reference, click [here](#).

D. For Entrust certificates

- keytool -import -alias Entrust_L1C -keystore <keystore-name.keystore> -trustcacerts file entrust_root.cer
- keytool -import -alias Entrust_2048_chain -keystore <keystore-name.keystore> - trustcacerts -file entrust_2048_ssl.cer
- keytool -import -alias -keystore <keystore-name.keystore> -trustcacerts -file <domain-name.cer>

For further reference, click [here](#).

E. For Thawte certificate

a. Purchased directly from Thawte:

- keytool -import -trustcacerts -alias tomcat -file <certificate-name.p7b>
-keystore <keystore-name.keystore>

b. Purchased through the Thawte reseller channel:

- keytool -import -trustcacerts -alias thawteca -file <SSL_PrimaryCA.cer>
-keystore <keystore-name.keystore>
- keytool -import -trustcacerts -alias thawtecasec -file <SSL_SecondaryCA.cer> -keystore
<keystore-name.keystore>
- keytool -import -trustcacerts -alias tomcat -file <certificate-name.cer>
-keystore <keystore-name.keystore>

Note: If you use an external CA which is not in the list mentioned above, please contact your CA for the required commands.

4. Associate the certificate with SharePoint Manager Plus

- Copy the .keystore file from the <installation_directory>|ManageEngine|SharePoint Manager Plus|jre|bin location and paste it at the <installation_directory>|ManageEngine|SharePoint Manager Plus|conf location.
- At the <installation_directory>|ManageEngine|SharePoint Manager Plus|conf location, locate the server.xml file and take a backup of that file.
- Open the server.xml file using an editor and navigate to the last connector tag.
- Replace the value of the keystore file with the location of your keystore ('./conf/<keystore_name>.keystore').
- Replace the value of the keystorePass with the password given during [step 4](#) of the CSR creating process.
- Save the server.xml file and start SharePoint Manager Plus.
 - If the product runs as an application, click **Start > All Programs > SharePoint Manager Plus > Stop SharePoint Manager Plus.**
 - If the product runs as a Windows service, click **Start > Run**. Type **service.msc** and start SharePoint Manager Plus.
- Once the SharePoint Manager Plus service has started, launch the SharePoint Manager Plus client.



Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus
M365 Manager Plus | RecoveryManager Plus

About SharePoint Manager Plus

SharePoint Manager Plus helps manage, report and audit both SharePoint on-premises and SharePoint Online environments. SharePoint Manager Plus enables you to seamlessly manage SharePoint servers, track permission changes, meet compliance requirements and more via a central console. It also provides usage analytics with insights on user behavior and security threat detection using a real-time alert system. Now you can seamlessly migrate from one version of SharePoint to another, or even to SharePoint Online.

For more information about SharePoint Manager Plus, visit
www.manageengine.com/sharepoint-management-reporting/.

\$ [Get Quote](#)

⤵ [Download](#)