ManageEngine
SharePoint Manager Plus

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** option. The port number 8086 is entered by default. You can change it to a value of your choice.
4. Click **Save.**

2. Create a certificate signing request (CSR)

1. Stop SharePoint Manager Plus **(Start > All Programs > SharePoint Manager Plus > 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 000 -keystore <domainName> .keystore

<key password> is a password of your choice and <domainName> is the name of your domain.

4. Type in your Keystore password. To avoid any confusion, try giving the same password as your keypass.

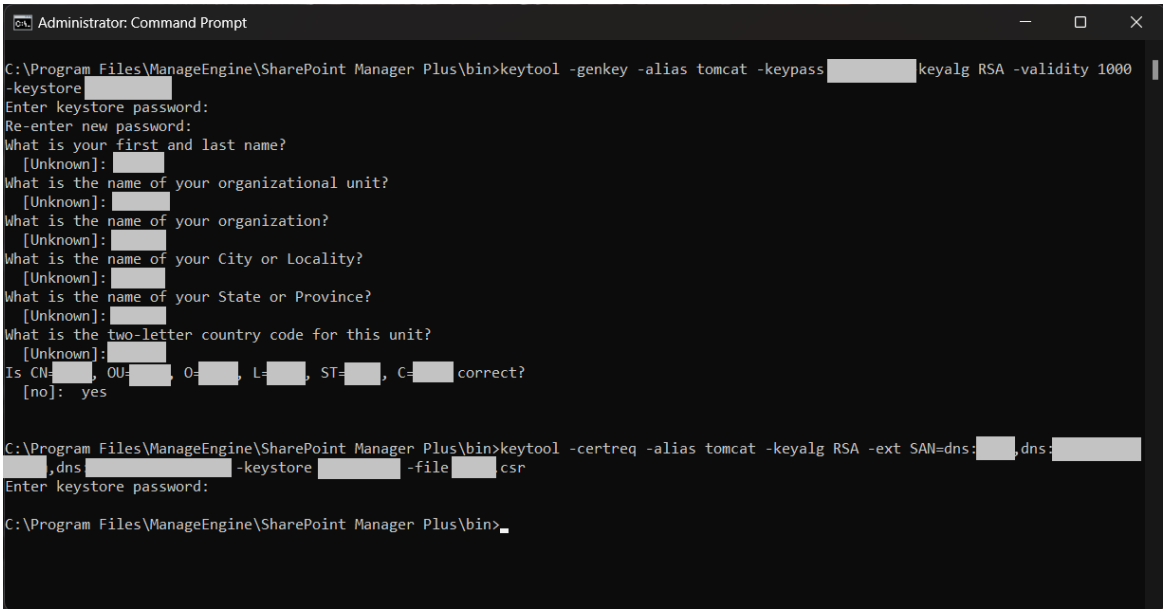
You will be prompted to answer the following questions:

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.

5. 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

<domainName> is the name of your domain. Provide the appropriate SAN as shown in the figure below.

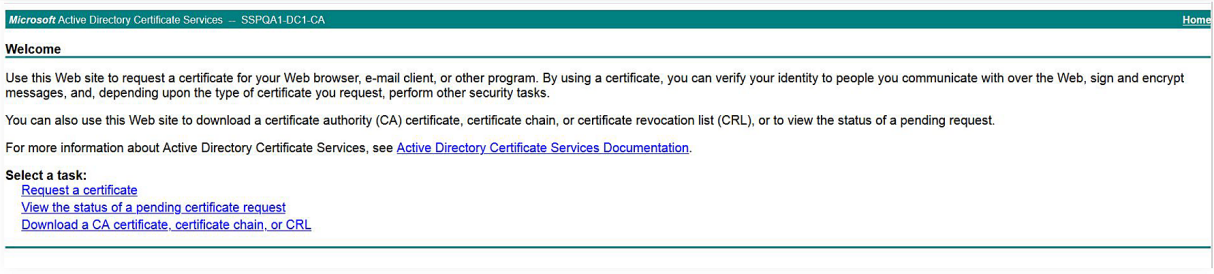


3. Issue the SSL certificate

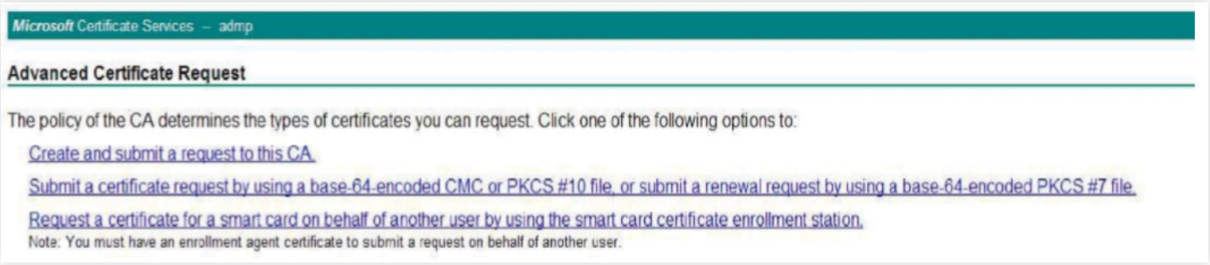
1. Issue the SSL certificate using an internal CA.

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.

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

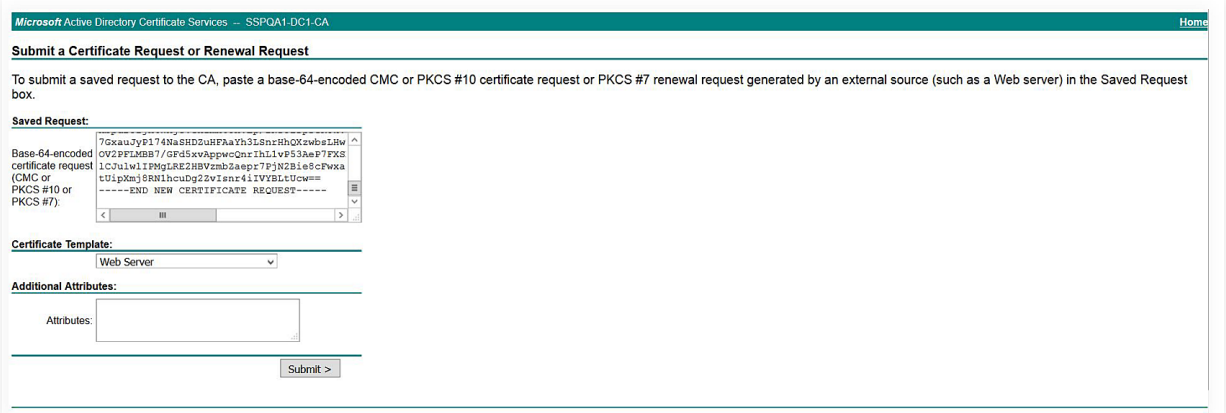


ii. Click on **Advanced certificate request** and select the **Submit a certificate by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file** option.



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

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



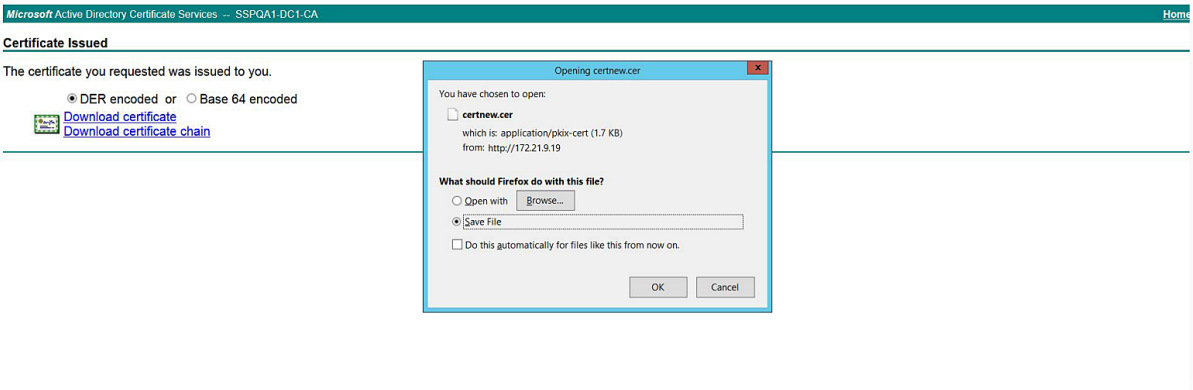
v. Click **Download Certificate Chain** link to download the issued '**PKCS #7 Certificates**' types.
The downloaded certificate will be of the .p7b file format.

vi. Copy and paste this .p7b file at <installation_directory>\ManageEngine\ SharePoint Manager Plus\jre\bin.

vii. Return to Microsoft Certificate Services and click the **Home** link at the top-right corner of the page.

viii. Click **Download a CA certificate, chain certificate or CRL** link to download the CA root certificate.

ix. Click **Download CA certificate** link to download and save the root certificate that is in the .cer format.



x. Copy and paste the '.cer' file at <installation_directory>\ManageEngine\ SharePoint Manager Plus\jre\bin.

xi. 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 *.keyDownload CA certificatestore* file.

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

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

xii. 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.

2. Issue the SSL certificate using external CAs

i. To request a certificate from an external CA, submit the CSR to that CA.

ii. Unzip the certificates returned by your CA and place them in <installation_directory>/ManageEngine /SharePoint Manager Plus/jre/bin.

iii. Open **Command Prompt** and navigate to the <installation_directory>/ManageEngine/ SharePoint Manager Plus/jre/bin.

iv. 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

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 SharePointmanager.cer

C. For "Comodo" 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

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>

E. For Thawte certificates

- Purchased directly from Thawte:
  - keytool -import -trustcacerts -alias tomcat -file <certificate-name.p7b> -keystore <keystore-name.keystore>
- 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

1. 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.*
2. At the *<installation_directory>\ManageEngine\SharePoint Manager Plus\conf* location, locate the server.xml file and take a backup of that file.
3. Open the server.xml file using an editor and navigate to the last connector tag.
4. Replace the value of the keystore file with the location of your keystore ('./conf/<keystore_name>.keystore).
5. Replace the value of the keystorePass with the password given during Step 4 of the CSR creating process.
6. Change the value of *keystoreType* to **JKS.**
7. Save the server.xml file and start SharePoint Manager Plus **(Start > All Programs > SharePoint Manager Plus > Start SharePoint Manager Plus).**
8. 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

ManageEngine
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