ManageEngine
ADManager Plus

Guide to install the **SSL certificate** in **ADManager Plus**

Table Of Contents

This document will help you secure ADManager Plus with SSL certification. Securing ADManager Plus with an SSL certificate ensures that the data exchange between the ADManager Plus server and its web console is safe from any external threats.

What is SSL?

Data exchange between a server and the client over the web, using HTTP, is insecure as data is transferred in plain text. Therefore, transferring critical data through an HTTP-only site can prove to be dangerous. To get rid of this disadvantage of HTTP, HTTPS was developed. HTTPS means HTTP-Secure and it follows the SSL protocol.

Secure Socket Layer (SSL) is a protocol that establishes an encrypted connection between a client and a server so that information can be transferred securely. SSL is used by banking sites or by sites that require the users' personal and confidential data to be entered.

To activate SSL on a web server, an SSL certificate is required. An SSL certificate is a digital certificate that describes the authenticity and the integrity of the domain and also of the company to which the site belongs. To receive an SSL certificate, a Certificate Signing Request (CSR) needs to be created and submitted to a Certification Authority (CA). CA is an entity that verifies all the details mentioned in the CSR (name of the organization & more), and then issues the certificate.

Once the SSL certificate is issued and configured in the server, SSL is automatically initialized.

All these complexities are not visible to the end user. The HTTPS in the URL and the padlock symbol next to it, indicate that SSL is being followed. The end users can also click on the padlock to view the certificate and the details of the certificate.

Steps to enable SSL for ADManager Plus

The steps required to enable SSL in ADManager Plus are listed below:

- Enabling SSL in the ADManager Plus Client.
- Creating the Certificate Signing Request (CSR).
- Issuing the certificate.
- Associating the certificate with ADManager Plus.

a. Enabling SSL in the ADManager Plus Client

- Logon to ADManager Plus, click the Admin tab and click the Connection section.
- Check the Enable SSL option. The port number 8443 is selected automatically.
- Click Save Changes and restart the product for the changes to take effect.

b. Creating the Certificate Signing Request (CSR)

In this step, we will create a keystore and a CSR. A keystore is a repository that contains the public and private keys required for encryption and decryption of data once the connection is established between the client and the server.

1. Stop ADManager Plus (Start---> All Programs---> ADManager Plus---> Stop ADManager Plus)
2. Open command prompt and browse to the <installation_directory>\ManangeEngine\ ADManager Plus\jre\bin path.
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. Replace the <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'.

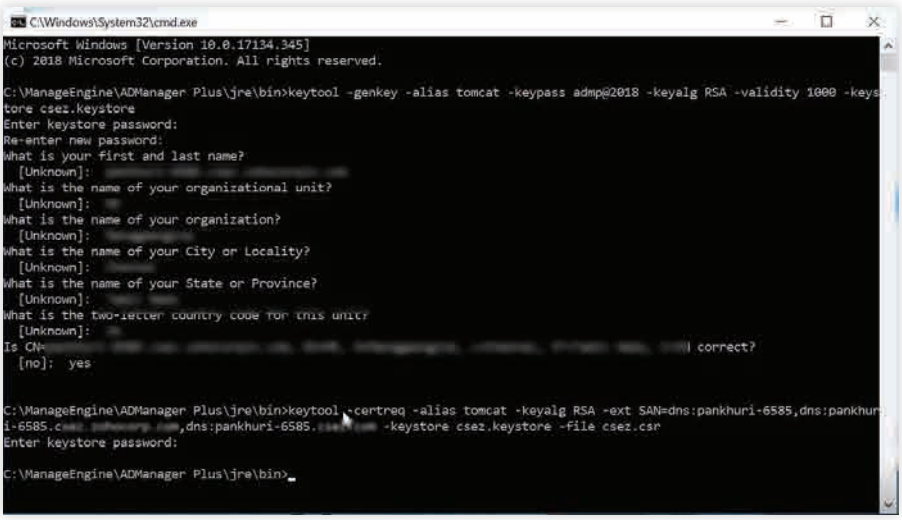
   You will be prompted to answer the following questions:

Sr. No.	Question	Answer
1	What is your first name and last name?	Enter the NetBIOS or FQDN of the server in which ADManager Plus is configured.
2	What is the name of your Organizational Unit?	Enter the name of the OU of your choice.
3	What is the name of your Organization?	Provide the legal name of your organization.
4	What is the name of your City or Locality?	Enter the City or Locality name as provided in your organization's registered address.
5	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.
6	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

Replace the <domainName> with the name of your domain and provide the appropriate Subject Alternatives Names as shown in the figure below:



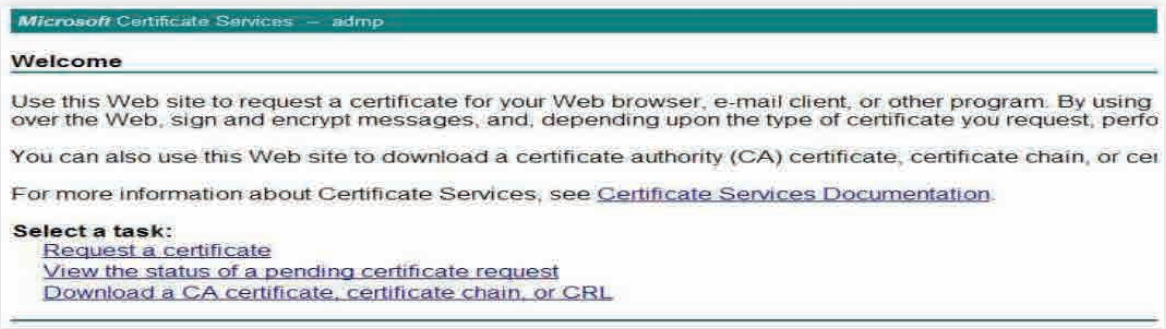
c. Issuing the SSL Certificate

In this step, we will connect to a CA, submit the CSR to the specific CA and get the SSL certificate issued to us.

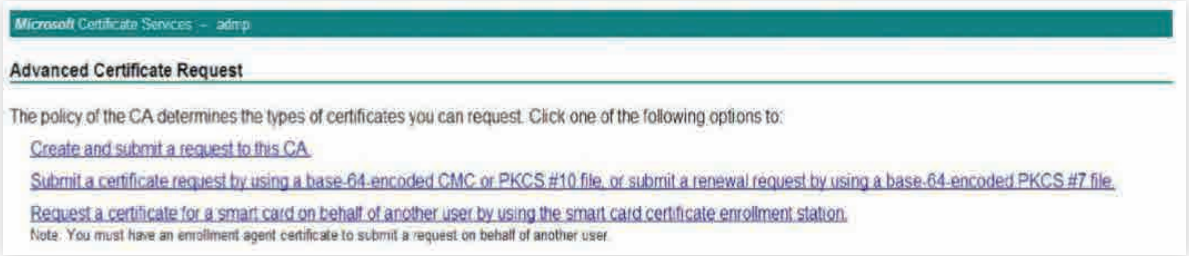
i. Issuing the certificate using an internal CA

An internal 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.**

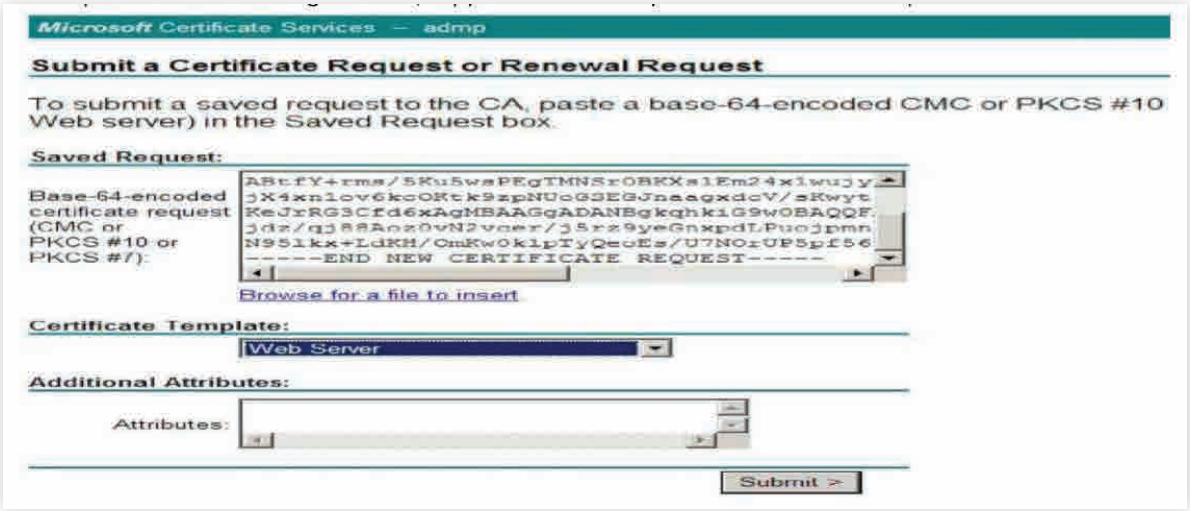


2 Click on **'Advanced certificate request'** and select the **Submit a certificate by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file** option.



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

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

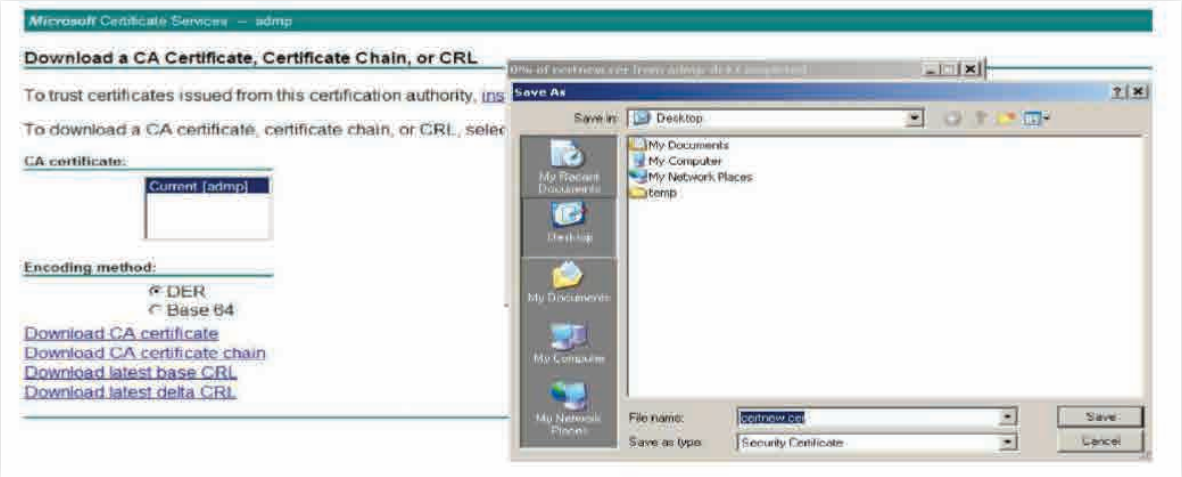


5 Click on the **Download Certificate Chain** link to download the issued **'PKCS #7 Certificates'** types. The downloaded certificate will be of the p7b file format.

6 Copy and paste this '.p7b' file at the <installation_directory>\manageengine\ADManager Plus/jre/bin location.

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

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



9 Click on the **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 the <installation_directory>\ManageEngine\ADManager Plus\jre\bin location.

11 Open command prompt, browse to the <installation_directory>\ManageEngine\ADManager Plus\ jre\bin path and execute the following query to import the internal CA certificate into the '.keystore' file.

i. **Keytool –import –trustcacerts –alias tomcat –file certnew.p7b –keystore <keystore_name >.keystore**

ii. Replace the <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.

i. **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.

ii. Issuing the certificate using an external CA

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

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 the <installation_directory> /ManageEngine/ADManager Plus/jre/bin folder

3. Open the command prompt and navigate to the <installation_directory>/ManageEngine/ ADManager Plus/jre/bin folder

4. Run the respective commands from the given list as applicable to your CA:

1. For "GoDaddy" certificates

i. **keytool -import -alias root -keystore <domainname>.keystore -trustcacerts -file gdrootg2.crt**

ii. **keytool -import -alias cross -keystore <domainname>.keystore -trustcacerts -file gdrootg2_cross.crt**

iii. **keytool -import -alias intermed -keystore <domainname>.keystore -trustcacerts -file gdig2.crt**

2. For "Verisign" certificates

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

ii. **keytool -import -alias tomcat -keystore <domainName>.keystore -trustcacerts file admanager.cer**

3. For "Comodo" certificates

i keytool -import -trustcacerts -alias root -file AddTrustExternalCARoot.crt -keystore <domainName>.keystore

ii keytool -import -trustcacerts -alias addtrust -file UTNAddTrustServerCA.crt -keystore <domainName>.keystore

iii keytool -import -trustcacerts -alias ComodoUTNServer -file ComodoUTNServerCA.crt - keystore <domainName>.keystore

iv keytool -import -trustcacerts -alias essentialSSL -file essentialSSLCA.crt -keystore <domainName>.keystore

4. For “Entrust” certificates

i keytool -import -alias Entrust_L1C -keystore <keystore-name.keystore> -trustcacerts file entrust_root.cer

ii keytool -import -alias Entrust_2048_chain -keystore <keystore-name.keystore> - trustcacerts -file entrust_2048_ssl.cer

iii keytool -import -alias -keystore <keystore-name.keystore> -trustcacerts -file <domain-name.cer>

5. For “Thawte” certificates

a. Purchased directly from Thawte

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

b. Purchased through the “Thawte reseller” channel

i keytool -import -trustcacerts -alias thawteca -file <SSL_PrimaryCA.cer> -keystore <keystore-name.keystore>

ii keytool -import -trustcacerts -alias thawtecasec -file <SSL_SecondaryCA.cer> - keystore <keystore-name.keystore>

iii 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 aforementioned list, please contact your CA for the required commands.

d. Associating the certificate with ADManager Plus

- Copy the '.keystore' file from the <installation_directory>\manageengine\ADManager Plus\jre\bin location and paste it at the <installation_directory>\ manageengine\ADManager Plus\conf location.
- At the <installation_directory>\manageengine\ADManager 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 keystore creation.
- Save the server.xml file and start ADManager Plus (Start---> All Programs---> ADManager Plus---> Start ADManager Plus)
- Once the ADManager Plus service has started, launch the ADManager Plus client.