ManageEngine
ADSelfService Plus

SSL configuration guide

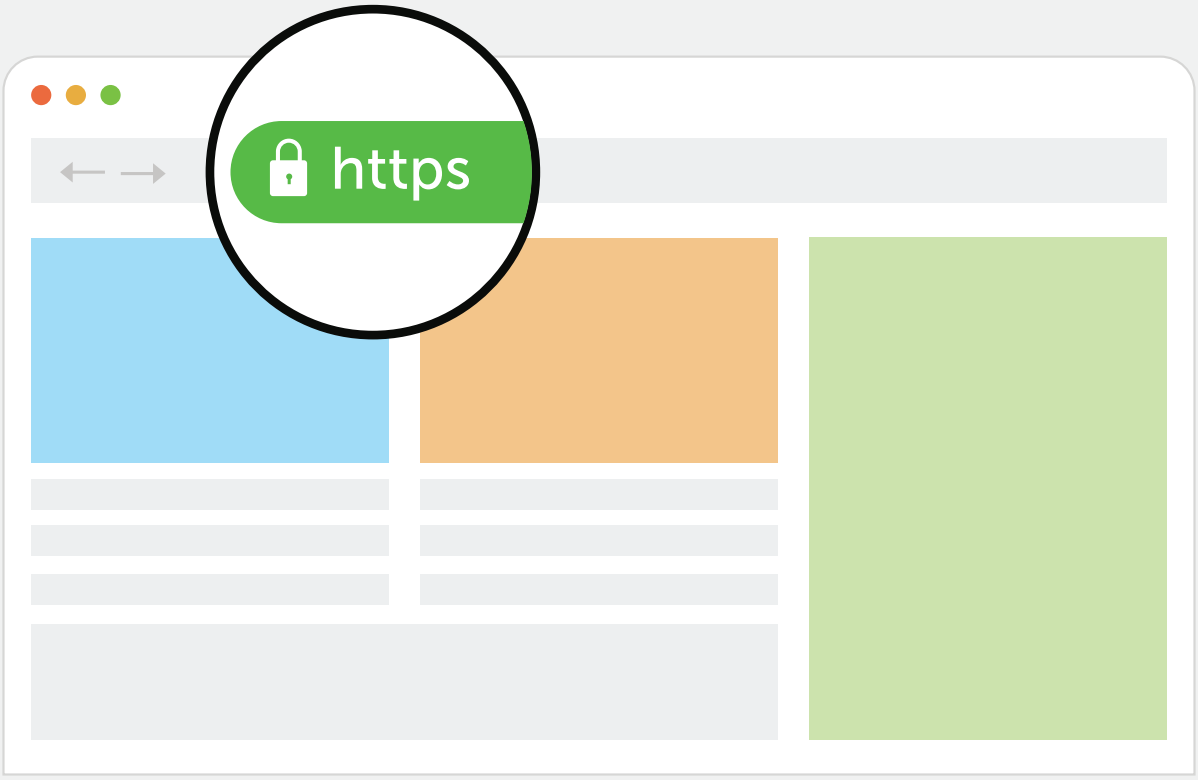


Table Of Contents

Summary

This document guides you through the process of securing the connection between ADSelfService Plus' server and users' browsers using SSL certificates.

Why install SSL certificates for ADSelfService Plus?

Remote users access ADSelfService Plus through a web browser to reset their forgotten passwords. To protect the data transferred between the ADSelfService Plus server and the user's web browser, you need to secure the connection between them.

To do this, you must enable the **HTTPS option** under the *Connection* settings, and install an **SSL certificate** in *ADSelfService Plus*.

Configuration steps

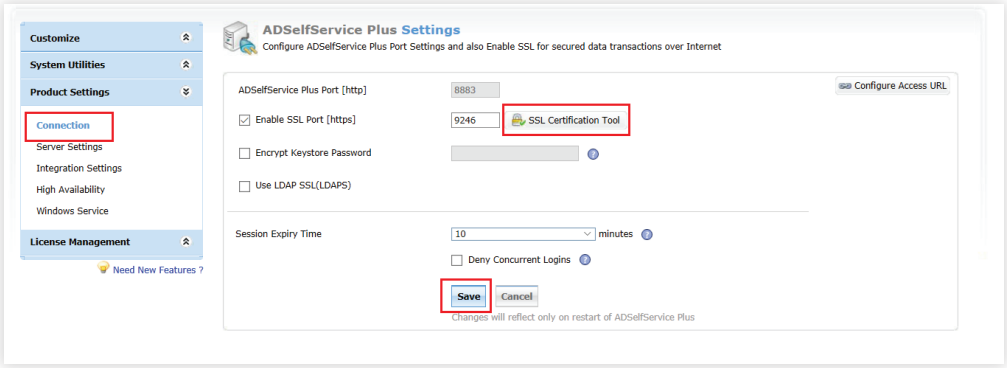
Step 1: **Enable HTTPS in ADSelfService Plus**

1. Log in to **ADSelfService Plus** with admin credentials.
2. Navigate to **Admin > Product Settings > Connection.**
3. Check the **Enable SSL Port [https]** box
4. Click **Save.**

Step 2: **Generating a CSR file**

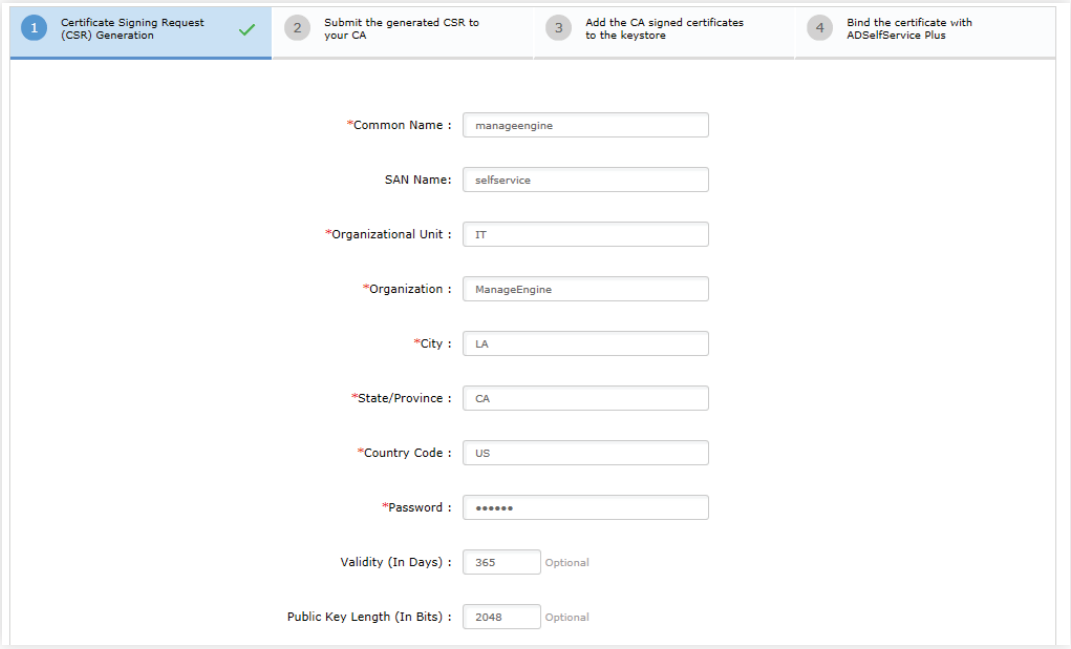
Note: If you already have an SSL certificate, skip to Step 4.

1. In the Connection Settings page, click the SSL Certification Tool button.



2. In the *SSL Tool & Guide* window, below the *Certificate Signing Request (CSR) Generation* section, fill in all the necessary fields. Refer to the table below:

Common Name	The name of the server in which ADSelfService Plus is running.
SAN Name	The names of the additional hosts (sites, IP addresses, etc.) to be protected by the SSL certificate.
Organizational Unit	The department name that you want to appear in the certificate.
Organization	The legal name of your organization.
City	The city name as provided in your organization's registered address.
State/Province	The state/province as provided in your organization's registered address.
Country Code	The two-letter code of the country in which you organization is located.
Password	A password must be at least six characters. The more complex the password, the better the security.
Validity (In days)	The number of days the certificate should be valid. If no value is provided, it will be set to 90 days.
Public Key Length (In bits)	The public key length. The larger the size, the stronger the key. The default size is 1024 bits and can be incremented only in multiples of 64.



3. Once you've entered all the details, click the **Generate CSR** button.

Step 3: **Submit the generated CSR file to your Certification Authority**

1. When you click the **Generate CSR** button, two files—*SelfService.csr* and *SelfService.keystore*—will be generated.
2. You can locate the SelfService.csr file in **<install_dir>\webapps\adssp\certificates** folder and the SelfService.keystore file in **<install_dir>\jre\bin** folder.
3. Submit the **SelfService.csr file** to your Certification Authority (CA).

Step 4: **Add the CA-signed certificates to the keystore, and bind it with ADSelfService Plus**

Based on whether the certificate is for a single domain or a multi-domain/wildcard certificate, the steps may vary.

a. For a single-domain SSL certificate

b. For a multi-domain/wildcard certificate

a. For a single-domain SSL certificate:

Prerequisite: If your certificate is in CER, CRT, PEM, or any other format, convert it to the P7B format. Refer to the Appendix for information on how to convert a certificate to the P7B format.

1. Back up the **server.keystore, SelfService.p12, server.xml, and web.xml files** located at *<Install_Directory>\conf folder* (Default location: *C:\ManageEngine\ADSelfService Plus\conf).*

2. Copy the certificate file, say **cert.P7B,** and paste it under the *<Install Directory>\jre\bin* folder (Default location: *C:\ManageEngine\ ADSelfService Plus\jre\bin).*

3. Open an elevated **Command Prompt** and change the working directory to the **<Install_Directory>\jre\bin folder.**

4. Now, execute the command given below:

   keytool -import -alias tomcat -trustcacerts -file cert.p7b -keystore SelfService.keystore

   Note: *cert.p7b* should be replaced with the name of the P7B certificate file.

5. Copy the **SelfService.keystore file** and paste it in the *<Install_Directory>\conf folder.*

6. Open the **server.xml file,** located in the *<Install_Directory>\conf* folder, in a text editor. Scroll down to the end of the file, where you'll find a connector tag as shown below.

   <Connector SSLEnabled="true".....
   />

7. Modify the following properties:

   a. Replace the value of **keystoreFile** with **./conf/SelfService.keystore.**

   b. Replace the value of **keystorePass** with the password you used while generating the CSR for this certificate file.

   c. Delete the **keystoreType=PKCS12** property.

   Note: The keystoreType property will appear in the Connector tag only if the ADSelfService Plus build is 5701 or above. For lower builds, ignore Step c.

Example: <Connector SSLEnabled="true" acceptCount="100" clientAuth="false" connectionTimeout="20000" debug="0" disableUploadTimeout="true" enableLookups="false" **keystoreFile="./conf/SelfService.keystore"** **keystorePass="********"** maxSpareThreads="75" maxThreads="150" minSpareThreads="25" name="SSL" port="9251" scheme="https" secure="true" sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2" sslProtocol="TLS"/>

8. Restart **ADSelfService Plus,** and check if the certificates are installed correctly.

b. For a multi-domain or Wildcard certificate:

Prerequisites:

- If the certificate bundle you received from your CA is not in the PFX format, make sure you convert the certificate file along with the private key to a PFX file.

- If you've generated the CSR using ADSelfService Plus, then copy the SelfService.keystore file and paste it in the <Install_Directory>\conf folder.

1. Back up the **server.keystore, SelfService.p12, server.xml, and web.xml files** located at *<Install_Directory>\conf folder* (Default location: *C:\ManageEngine\ADSelfService Plus\conf).*

2. Copy the certificate file, say **cert.pfx,** and paste it under the *<Install_Directory>\conf folder* (Default location: *C:\ManageEngine\ ADSelfService Plus\ conf).*

3. Open the **server.xml file,** located in the *<Install_Directory>\conf* folder, in a text editor. Scroll down to the end of the file where you'll find a connector tag as shown below.
   <Connector SSLEnabled="true".....
   />

4. Modify the following properties:
   a. Replace the value of **keystoreFile** with **./conf/Should cert.pfx.**

   b. Replace the value of **keystorePass** with the password you used while generating the CSR for this certificate file.

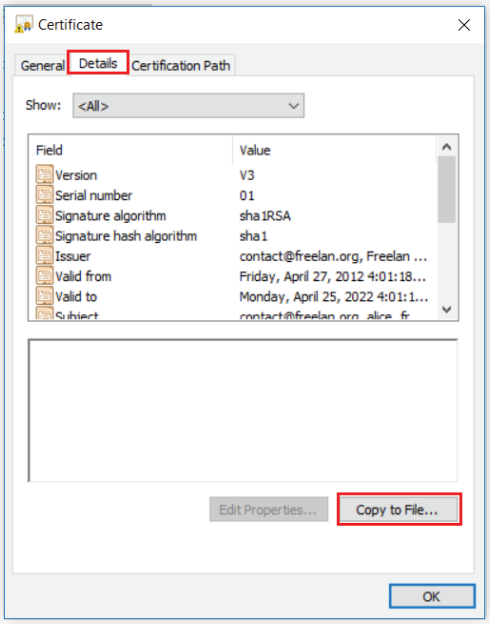
Example: <Connector SSLEnabled="true" acceptCount="100" clientAuth="false" connectionTimeout="20000" debug="0" disableUploadTimeout="true" enableLookups="false" **keystoreFile="./conf/Should cert.pfx.** **keystorePass="********" keystoreType=PKCS12** maxSpareThreads="75" maxThreads="150" minSpareThreads="25" name="SSL" port="9251" scheme="https" secure="true" sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2" sslProtocol="TLS"/>

5. Restart **ADSelfService Plus,** and check if the certificates are installed correctly.

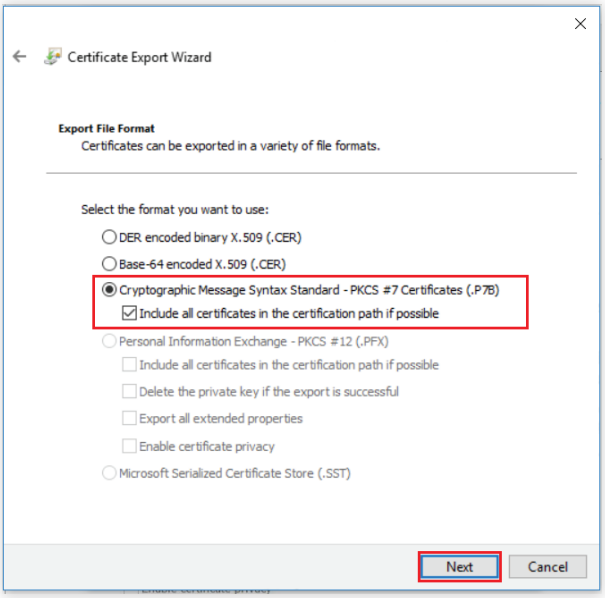
Appendix

1. **Steps to convert a certificate file in CER, CRT, or PEM format to P7B format:**

   - Double-click on the **certificate file** to open it in the Certificate window.
   - Select **Details** and click **Copy to File....**



   - Click **Next** in the *Certificate Export Wizard* that opens.
   - Select the **Cryptographic Message Syntax Standard – PKCS #7 Certificates (.P7B)** option, and check the **Include all certificates in the certification path if possible** box.



- Click **Browse** to select a destination to store the file and enter the **File name.**
- Review the information, and click **Finish.**

2. Preferred cipher for improved security in ADSelfService Plus

```
ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC
_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA"
```