ManageEngine
ADSelfService Plus

Installing SSL Certificates for ADSelfService Plus

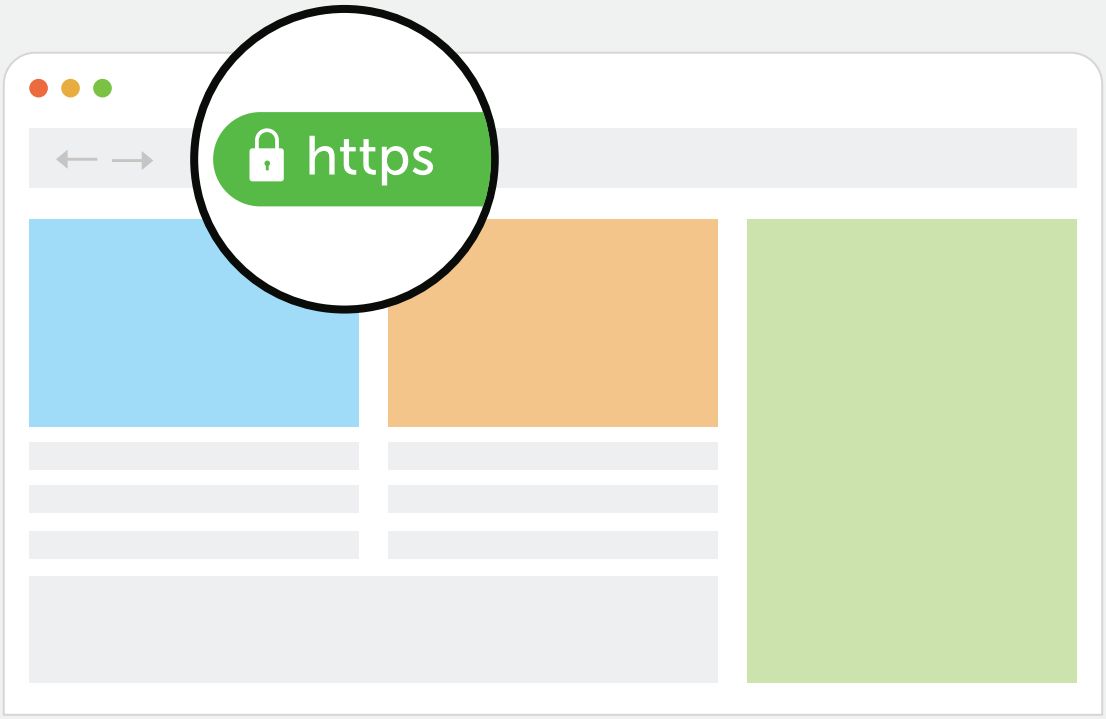


Table Of Contents

Document Summary

This document guides you through the process of securing the connection between the ADSelfService Plus' server and the users' browser using Secure Sockets Layer (SSL) certificates.

ADSelfService Plus Overview

ManageEngine ADSelfService Plus, an integrated Active Directory self-service password management and single sign-on solution, helps reduce password reset tickets and spares end users the frustration caused by computer downtime. It offers,

- Self-service password reset and account unlock
- Password and account expiration notifier
- Password policy enforcer
- Enterprise single sign-on and password synchronizer
- Windows logon two-factor authentication
- Directory self-update and employee search

These features, designed to strike a balance between ensuring network security and ease-of-access, warrants improved ROI, and a productive IT workforce.

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 users' web-browser, you need to secure the connection between them. For this, you must install an SSL certificate in ADSelfService Plus and enable the HTTPS option under the Connection settings.

The following steps walks you through the entire process:

i. Generate a CSR file

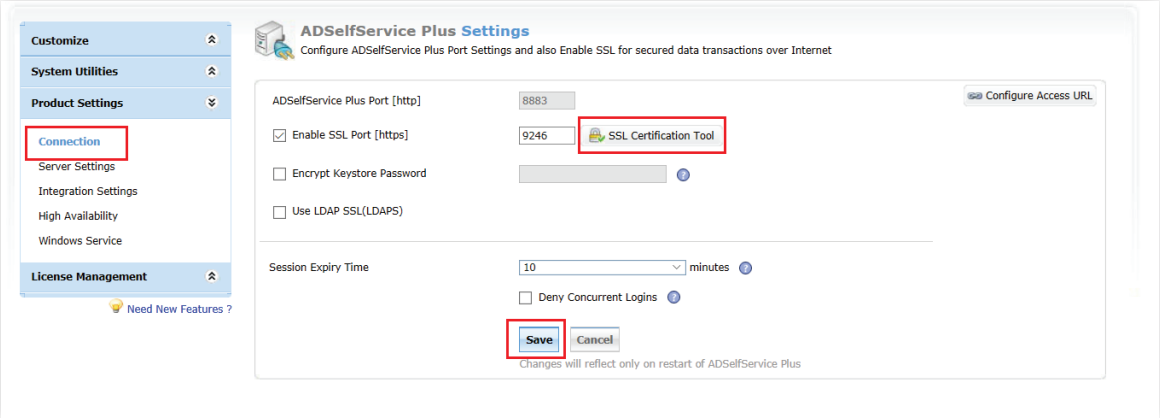
ii. Submit the generated file to your Certification Authority

iii. Add the CA signed certificates to the keystore

iv. Bind the certificates with ADSelfService Plus

Step 1: **Generate a CSR file**

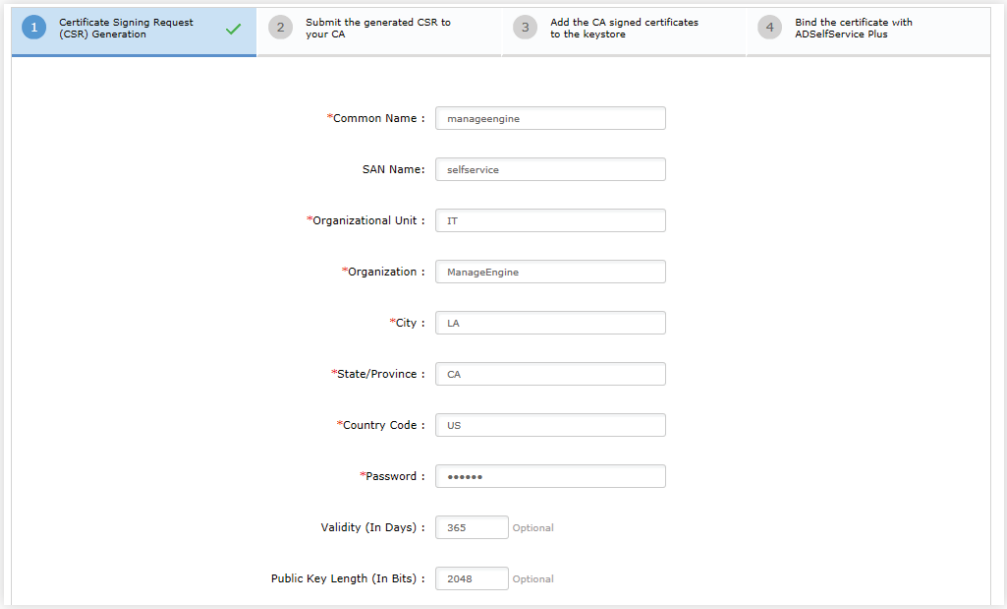
- Log in to ADSelfService Plus web-console with admin credentials.
- Navigate to **Admin** → **Product Settings** → **Connection.**
- Select the **Enable SSL Port (https)** checkbox.
- Click the **SSL Certification Tool** button.



- In the **SSL Tool & Guide** window, under the **Certificate Signing Request (CSR) Generation** section, fill in the details based on the table given below.

Common Name	The name of the server in which ADSelfService Plus is running.
SAN Name	The names of the additional host names (sites, IP addresses, etc.) to be protected by a single SSL Certificate.
Organizational Unit	The department name that you want to appear in the certification.
Organization	Provide the legal name of your organization.
City	Enter the city name as provided in your organization's registered address.

State/Province	Enter the State/Province as provided in your organization's registered address.
SAN Name	The names of the additional host names (sites, IP addresses, etc.) to be protected by a single SSL Certificate.
Country Code	Provide the 2-letter code of the country in which your organization is located.
Password	Enter a password of at least 6 characters.
Validity (In days)	Specify the no. of days the certificate should be valid. If no value is provided, the validity will be taken as 90 days
PublicKey Length (In bits)	Provide the public key length. Larger the size, stronger the key. Default size is 1024 bits and can be incremented only in multiples of 64.



- Click the **Generate CSR** button.

Step 2: **Submit the generated CSR file to your Certification Authority**

- When you click the **Generate CSR** button, two files namely **SelfService.csr** and **SelfService. keystore** will be generated. You can locate the CSR file at **<install_dir>\webapps\adssp\certificates.**
- Submit the generated CSR file to your Certification Authority (CA).

Step 3: **Add the CA signed certificates to the keystore**

Once you receive the certificate from the Certification Authority (CA), follow the steps below:

a. For P7B certificate:

i. Copy the *cert.P7B* file received from the CA and paste it under the **<Install Directory>\jre\bin** folder **(Default location:** C:\ManageEngine\ ADSelfService Plus\jre\bin).

ii. Backup the server.keystore file.

iii. Open an elevated command prompt and execute the following command: **keytool -import -alias tomcat -trustcacerts -file cert.p7b -keystore server.keystore.**

b. For PFX certificate:

i. Copy the **PFX/PKCS12** file received from the CA and paste it under the **<installation_dir>\conf** folder **(Default location:** C:\ManageEngine\ ADSelfService Plus\ conf).

Step 4: **Bind the certificates with ADSelfService Plus**

a. For P7B certificate, follow these steps:

i. Backup the *server.xml* file **(Location:** <Install Directory>\conf).

ii. Edit the *server.xml* file by replacing the value of the following SSL connector tags at the bottom of the page:

"**keystoreFile**" with "**./conf/SelfService.keystore**"

"**keystorePass**" with whatever password you entered in the CSR generator.

Example: <Connector SSLEnabled="true" acceptcount="100" clientauth="false" connectiontimeout="20000" debug="0" disableuploadtimeout="true" enablelookups="false" **keystorefile="./conf/selfservice.keystore" keystorepass="keystore_password"** maxsparethreads="75" maxthreads="150" minsparethreads="25" u/name="SSL" port="9251" scheme="https" secure="true" sslprotocol="TLS" sslprotocols="TLSv1,TLSv1.1,TLSv1.2"><connector>

iii. Restart ADSelfService Plus and check if the certificates are installed correctly.

b. For PFX certificate, follow these steps:

i. Backup the server.xml file.

ii. Open the **server.xml** file present in **<installation_dir>\conf** folder in a text editor of your choice.

iii. Go to the **end of the XML file** and search for the **connector tag** (that starts like, <Connector SSLEnabled="true" ...../>).

iv. Now, edit the following values inside that connector tag:

"**keystoreFile**" with **"./conf/"**

"**keystorePass="** with the respective password.

"**keystoreType"** as "**PKCS12"**

E.g.: <Connector SSLEnabled="true" acceptCount="100" clientAuth="false" connectionTimeout="20000" debug="0" disableUploadTimeout="true" enableLookups="false" **keystoreFile="./conf/YOUR_CERT_FILE.pfx" keystorePass= "PASSWORD" keystoreType="PKCS12"** maxSpareThreads="75" maxThreads="150" minSpareThreads="25" name="SSL" port="443" scheme="https" secure="true" sslProtocol="TLS"/>

v. Restart ADSelfService Plus.

Important:

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"
```

About ADSelfService Plus

ADSelfService Plus is an integrated AD self-service password management and SSO solution. It offers password self-service, password expiration reminders, a self-service directory updater, a multi-platform password synchronizer, and SSO for cloud applications. ADSelfService Plus supports IT help desks by reducing password reset tickets and spares end users the frustration caused by downtime.

For more information, please visit www.manageengine.com/products/self-service-password.

$ Get Quote Download