ManageEngine
ADSelfService Plus

Installing SSL Certificates for ADSelfService Plus

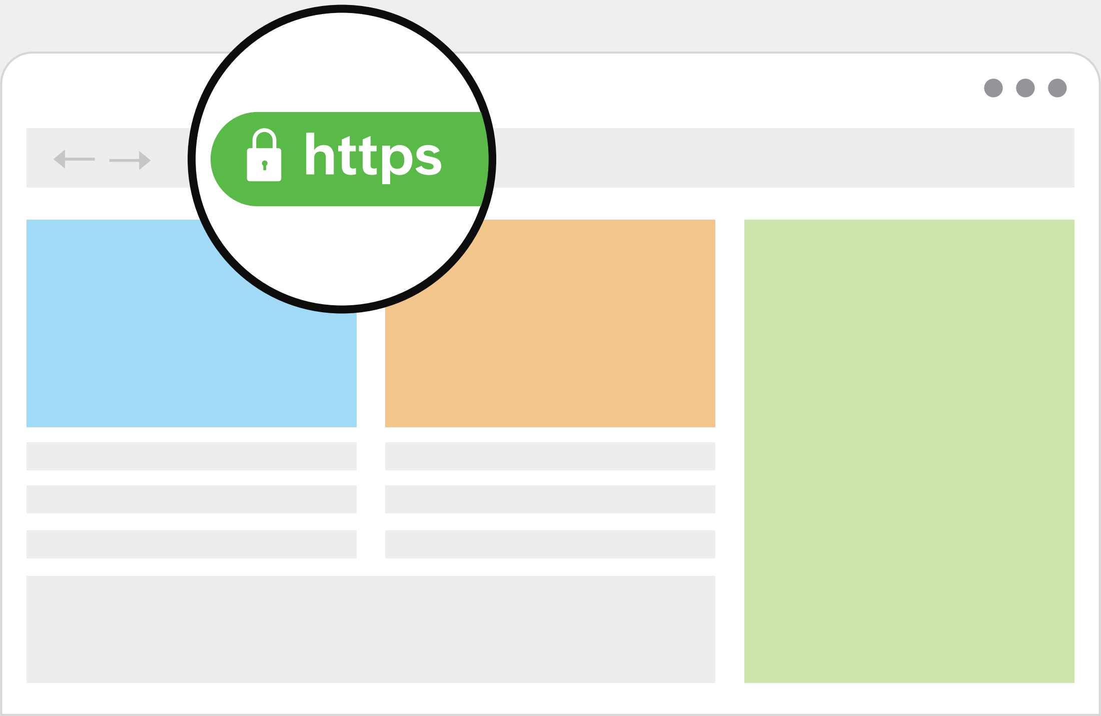


Table of contents

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 (AD) 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
- Multi-factor authentication and conditional access
- Enterprise single-sign on and password synchronization
- Password and account expiry notification
- Password policy enforcer
- 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 more productive IT workforce.

Why install SSL certificates for ADSelfService Plus?

Remote users can 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. Connections between the ADSelfService Plus server and end-user machines, VPNs, and cloud applications must also be secured for secure functioning of the MFA feature. For this, you must enable the HTTPS option under the Connection settings, and install an SSL certificate in ADSelfService Plus

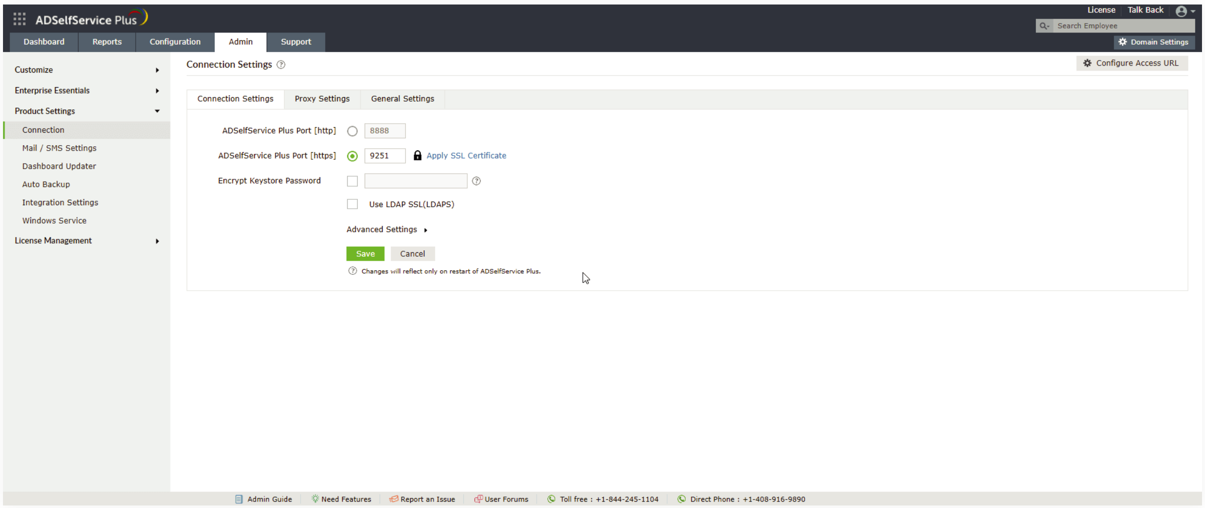
The process consists of four steps:

1. Enable HTTPs in ADSelfService Plus.
2. Generate a CSR file.
3. Submit the generated CSR file to your certificate authority (CA).
4. Bind the CA-signed certificates with ADSelfService Plus.

Configuration steps

Step 1: Enable HTTPS in ADSelfService Plus

- Log in to ADSelfService Plus with admin credentials.
- Navigate to **Admin > Product Settings > Connection.**
- Select **ADSelfService Plus Port [https].**
- If the default port number cannot be used, enter a designated HTTPS port number.
- Click **Save.**



Connection Settings

ADSelfService Plus Port [http] ○ 8888

ADSelfService Plus Port [https] ● 9251 Apply SSL Certificate

Encrypt Keystore Password □

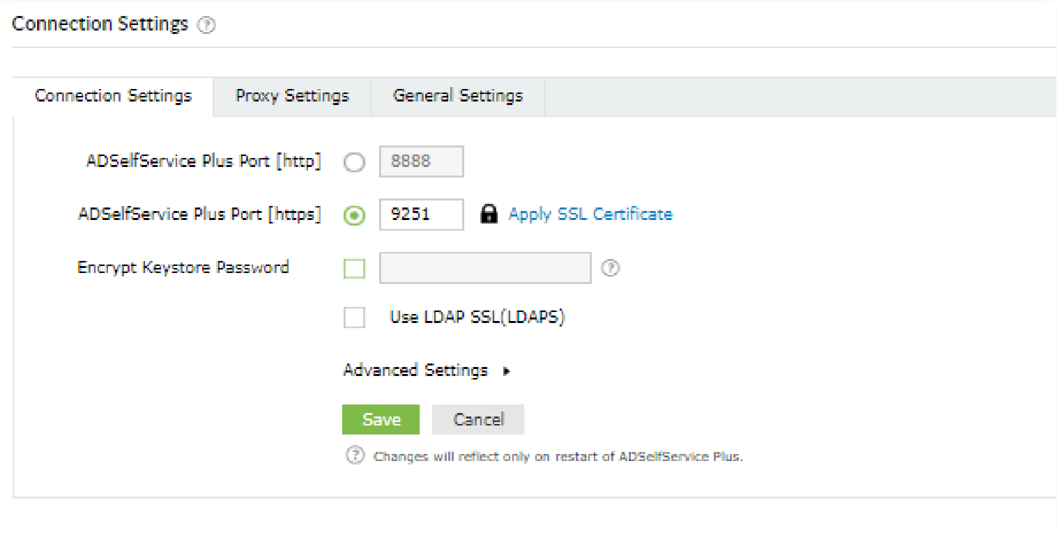
□ Use LDAP SSL(LDAPS)

Changes will reflect only on restart of ADSelfService Plus.

Step 2: Generate a CSR

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

- Click the **Apply SSL Certificate** link.



Connection Settings

ADSelfService Plus Port [http] ○ 8888

ADSelfService Plus Port [https] ● 9251 Apply SSL Certificate

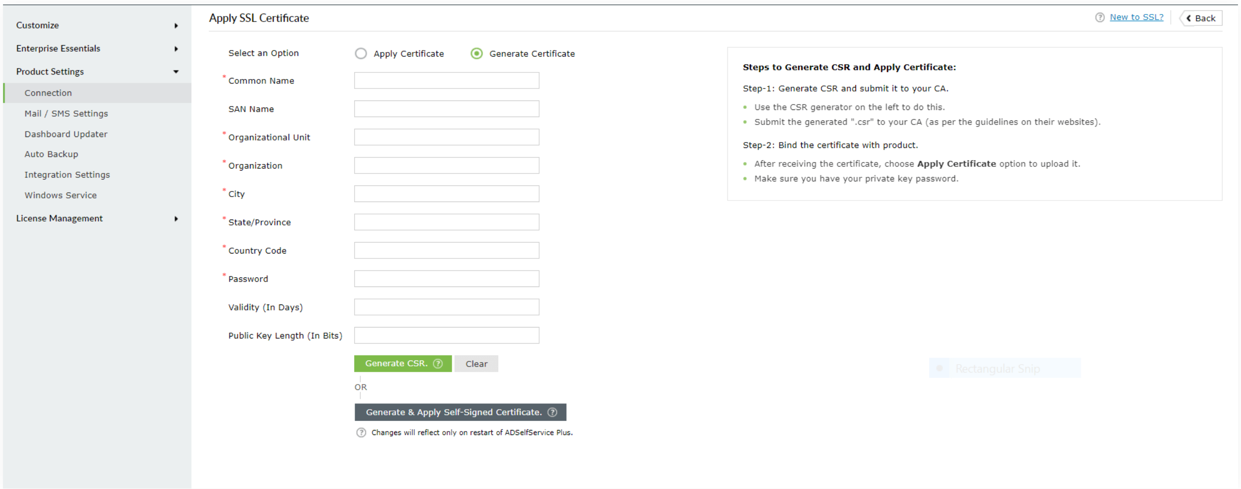
Encrypt Keystore Password □

□ Use LDAP SSL(LDAPS)

Changes will reflect only on restart of ADSelfService Plus.

- Choose **Generate Certificate** and fill in all the necessary fields as given in the below table:

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 your 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



Apply SSL Certificate

Select an Option	○ Apply Certificate ● Generate Certificate
* Common Name	
SAN Name	
* Organizational Unit	
* Organization	
* City	
* State/Province	
* Country Code	
* Password	
Validity (In Days)	
Public Key Length (In Bits)	

Changes will reflect only on restart of ADSelfService Plus.

Steps to Generate CSR and Apply Certificate:

Step-1: Generate CSR and submit it to your CA.

- Use the CSR generator on the left to do this.
- Submit the generated ".csr" to your CA (as per the guidelines on their websites).

Step-2: Bind the certificate with product.

- After receiving the certificate, choose **Apply Certificate** option to upload it.
- Make sure you have your private key password.

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

If you wish to apply for a self-signed certificate, click **Generate & Apply Self-Signed Certificate.** Then follow the next steps.

Step 3: Submit the generated CSR file to your certificate authority (CA)

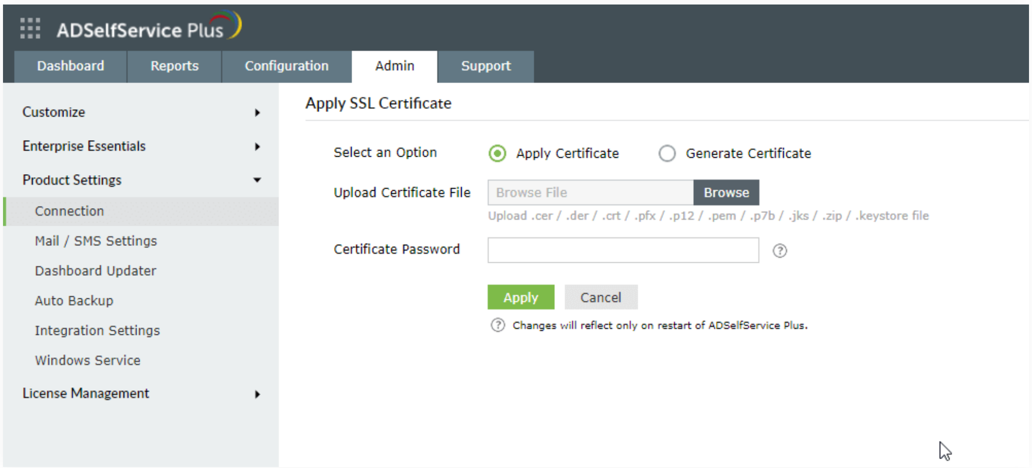
- When you click Generate CSR, *SelfService.csr* will be generated.
- You can locate the *SelfService.csr* file in the certificates folder under *<Install_Directory>\webapps\adssp\* (Default location: *C:\Program Files\ManageEngine\ADSelfService Plus\webapps\adssp\).*
- Submit the *SelfService.csr* file to your CA.

Step 4: Bind the CA-signed certificates with ADSelfService Plus

There are two ways to bind the CA-signed certificates with ADSelfService Plus. One way is through the *Apply Certificate* section in the ADSelfService Plus admin portal, and the other method is manual configuration. Any of the two methods can be used depending on preference. Below are the steps for each method:

Option 1: Using the ADSelfService Plus admin portal

1. In the ADSelfService Plus admin portal, go back to **Admin > Product Settings > Connection.**
2. Click **SSL Certification Tool** next to *HTTPS.*
3. Select **Apply Certificate.**
4. Click **Browse** to upload the certificate.
5. In the *Certificate Password* field, enter the **password** of the uploaded certificate.
6. Click **Apply.**



Apply SSL Certificate

Select an Option ● Apply Certificate ○ Generate Certificate

Upload Certificate File Browse File

Upload .cer / .der / .crt / .pfx / .p12 / .pem / .p7b / .jks / .zip / .keystore file

Certificate Password

Changes will reflect only on restart of ADSelfService Plus.

Option 2: Manual configuration

Prerequisite: 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.

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

2. Copy the **certificate file**, say *cert.pfx*, and paste it in *<Install_Directory>\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:
   - Replace the value of **keystoreFile** with **./conf/cert.pfx.**
   - Replace the value of **keystorePass** with the **password** of your PFX certificate.

   Example: <Connector SSLEnabled="true" acceptCount="100" clientAuth="false" connectionTimeout ="20000" debug="0" disableUploadTimeout="true" enableLookups="false" keystoreFile="./conf/cert.pfx" keystorePass="********" keystoreType="PKCS12" maxSpareThreads="75" maxThreads="150" minSpareThreads="25" nme="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.

Updating the Access URL

Connections to the ADSelfService Plus server are made using the ADSelfService Plus Access URL. Configuring the Access URL to use the HTTPS protocol will ensure that connections to the server are secure.

When installing SSL certificates to protect MFA for machines, VPNs, OWA, and cloud applications—and while installing the login agent on client machines—it is mandatory for the ADSelfService Plus Access URL's protocol to be set to HTTPS.

To do this:

- Go to Admin > **Customize > Product Settings > Connection > Connection Settings > Configure Access URL.**
- In the pop-up that opens, set the **Protocol** to **HTTPS.**
- Click **Save.**

Note: If your deployment of ADSelfService Plus uses an internet-facing endpoint such as a proxy server, the Access URL must point to the proxy server.

Note for FIDO passkey users:

- If you have configured FIDO passkey authentication, setting the Access URL to HTTPS will modify the preconfigured FIDO RP ID, resulting in loss of enrollment data and disenrollment of all users.
- If you are planning on configuring FIDO passkey authentication, ensure that the Access URL is set to HTTPS before configuring FIDO passkey authentication to prevent loss of enrollment data.

Troubleshooting Tips

When I try to import an SSL certificate, I get an error that reads "An unexpected error occurred." What does it mean?

Cause: These errors occur when the certificate is in PFX format with AES encryption, and when the certificate signing request (CSR) is generated by third-party applications or a web server instead of through the ADSelfService Plus admin portal.

Solution: Import the certificate into the Windows Certificate Manager, then export it along with the private key. By default, Windows will encrypt the certificate in TripleDES-SHA1 encryption. This will be successfully accepted by the application.

Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus

RecoveryManager Plus | M365 Manager Plus

ManageEngine
ADSelfService Plus

ADSelfService Plus is an identity security solution to ensure secure and seamless access to enterprise resources and establish a Zero Trust environment. With capabilities such as adaptive multi-factor authentication, single sign-on, self-service password management, a password policy enhancer, remote work enablement and workforce self-service, ADSelfService Plus provides your employees with secure, simple access to the resources they need. ADSelfService Plus helps keep identity-based threats out, fast-tracks application onboarding, improves password security, reduces help desk tickets and empowers remote workforces.

For more information about ADSelfService Plus, visit
www.manageengine.com/products/self-service-password.

$ Get Quote   ⤓ Download