ManageEngine
AD360

Guide to install the **SSL certificate** in AD360

This document will help you secure AD360 and its integrated components with SSL certification. SSL is the de facto standard on the web for establishing an encrypted link between a server and a web browser. It ensures that all data transferred between the server and the browser remains secure. Securing AD360 with an SSL certificate ensures that the data exchange between the AD360 server and the web client is safe from any external threats. To learn more about SSL, refer to the appendix at the end of this document.

Steps to enable HTTPS and apply an SSL certificate for AD360

The steps required to enable SSL in AD360 are listed below:

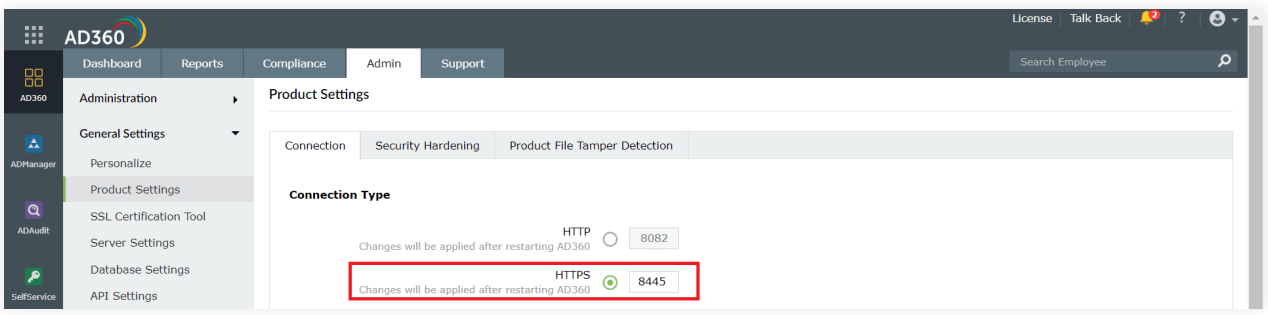
1. Enabling HTTPS in AD360
2. Generate a CSR file or generate and apply a self-signed certificate
3. Submit the CSR file to your certification authority (CA)
4. Bind the CA-signed certificates with AD360

Note: If you have configured high availability in AD360, apply the SSL certificate in the primary server which in turn will be replicated to the secondary server.

Configuration steps

STEP 1 Enable HTTPS in AD360

1. Log in to AD360 with admin credentials.
2. Navigate to **Admin > General Settings > Product Settings > Connection.**
3. Select **HTTPS.**
4. If the default port number cannot be used, enter a designated HTTPS port number.
5. Click **Save.**
6. Restart AD360.



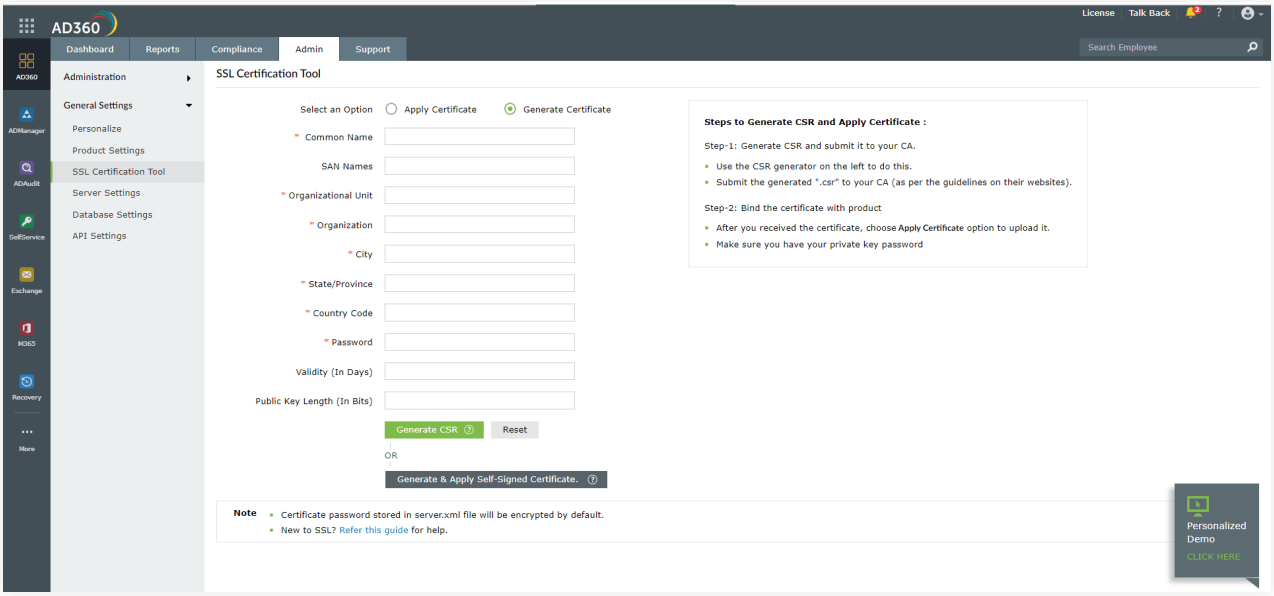
STEP 2 Generate a CSR file or generate and apply a self-signed certificate

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

1. Navigate to **Admin > General Settings > SSL Certification Tool.**

2. Click **Generate Certificate** and fill in all the necessary fields as given in the table below.

Common Name	Enter the hostname used to access AD360. It can also be the AD360 server's hostname.
SAN Names	Enter the hostname used to access AD360. In addition, you can specify additional hostnames (sites, IP addresses, common names, etc.) that must be protected by the certificate.
Organization Unit	Enter the name of the department or the OU that must be specified in the certificate.
Organization	Enter the legal name of your organization.
City	Enter the city where your organization is located.
State/Province	Enter the state and province where your organization is located.
Country Code	Enter the two-letter code of the country where your organization is located.
Password	Enter the password that must be used to protect the certificate. The password must be at least 6 characters in length.
Validity (In Days)	Enter the number of days the certificate should be valid. The default value is 90 days.
Public Key Length (In Bits)	Enter the public key size in bits. The default key size is 2048 bits.



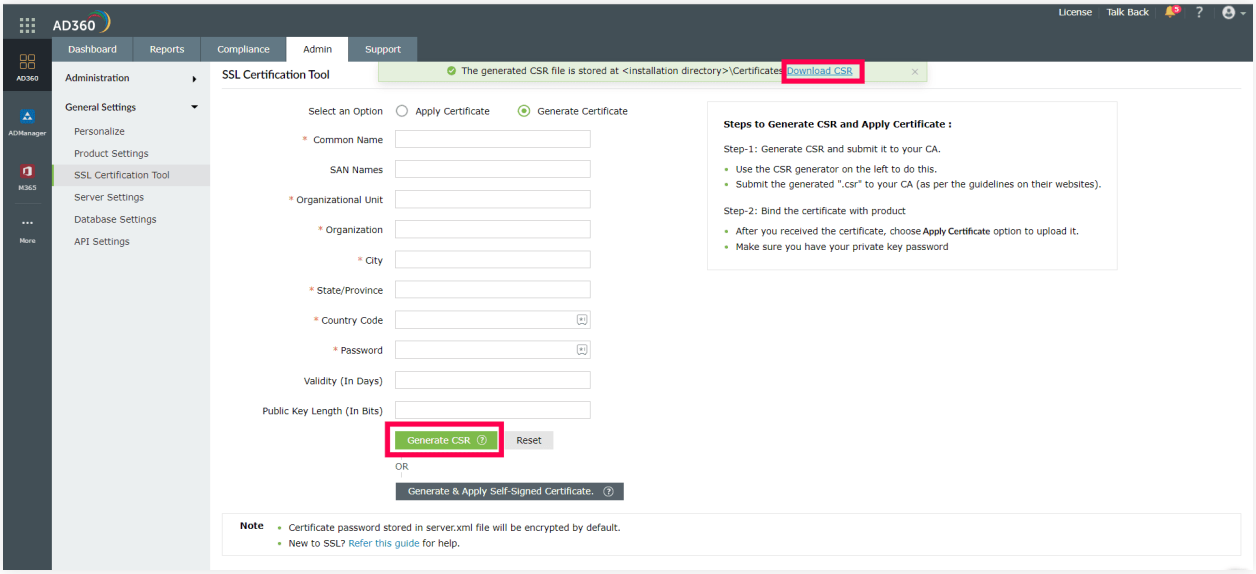
3. Once you have entered all the details, you can select either of these two options:

a. Generate CSR

This method allows you to generate the CSR file and submit it to your CA. Using this file, your CA will generate a custom certificate for your server.

i. Click the **Generate CSR** button.

ii. In the pop-up window message that appears, you can either click Download CSR or manually get the CSR file by going to the *<Install_dir>\Certificates* folder (by default *C:\Program Files\ManageEngine\AD360\Certificates).*



iii. Once you have received the certificate files from your CA, follow the steps listed under step 4 to apply the SSL certificate.

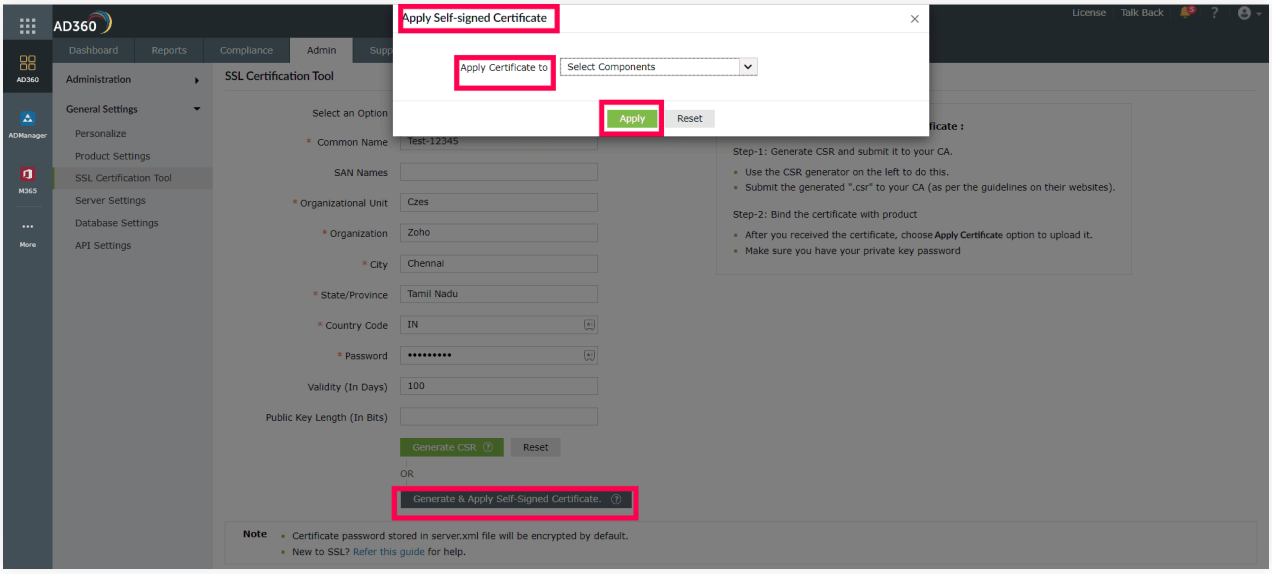
b. Generate and apply a self-signed certificate

This option allows you to create a self-signed certificate and apply it instantly within the product. However, self-signed SSL certificates come with a drawback. Anyone accessing the product secured with a self-signed SSL certificate will be shown a warning, telling them that the website is not trusted (which may cause concern).

If you still want to apply the self-signed certificate, follow these steps:

i. Click **Generate & Apply Self-Signed Certificate.**

ii. In the *Apply Self-Signed Certificate* pop-up window, select the components in which you want to apply the self-signed certificate from the **Apply Certificate to** drop-down box.
Note: If the integrated AD360 components have different access URLs, then those access URLs must be entered in the *SAN Names* field.



iii. Click **Apply.**

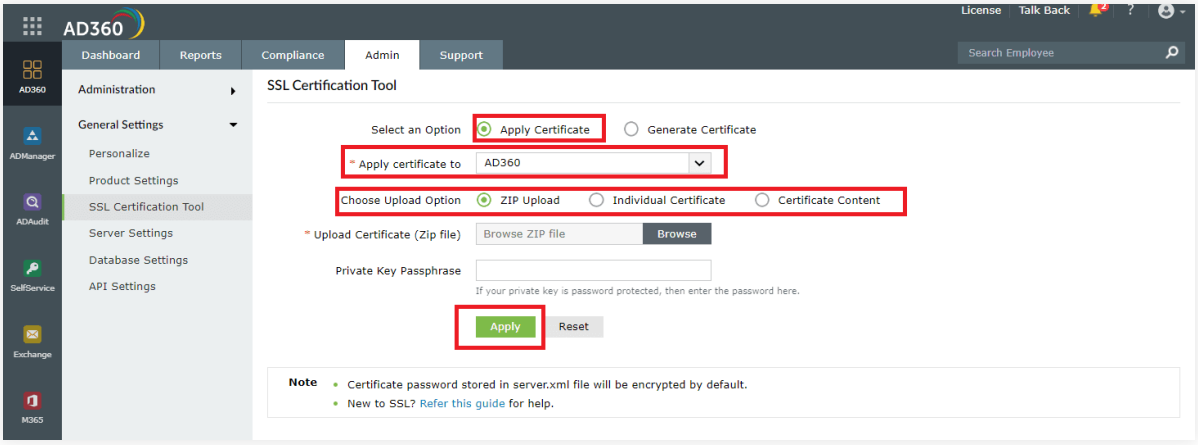
iv. Once you get the message that the SSL certificate has been successfully applied, restart the components for the changes to take effect.

STEP 3 Submit the CSR file to your certification authority (CA)

1. When you click **Generate CSR,** the .csr file gets generated.
2. You can either click **Download CSR** or manually get it by going to the <*Install_dir*>*Certificates* folder.
3. Submit the *.csr* file to your CA.

STEP 4 Bind the CA-signed certificates with AD360

1. Navigate to **Admin > General Settings > SSL Certification Tool.**
2. Select **AD360** in the *Apply certificate* to drop-down menu. You can also choose to apply the SSL certificate to multiple components of AD360.



3. Choose how you would like to import the certificate from the options and fill in the required fields.

a. ZIP Upload: If your CA has given you a ZIP file, then select the **ZIP Upload** option. If your CA has sent you individual certificate files—such as user, intermediary, and root certificates—then combine all of them into a ZIP file. After selecting this option:

i. Browse and upload the ZIP file in the *Upload Certificate (Zip file)* field.

ii. If your certificate's private key is password protected, enter its password in the *Private Key Passphrase* field. This step is necessary if the ZIP file contains the private key.

iii. Click **Apply.**

Note: Please ensure that the ZIP file is not a nested folder and includes the RSA private key along with the certificate bundle in the parent folder.

b. Individual Certificate: If your CA has given only one certificate as a PFX or PEM file, then select the **Individual Certificate** option. After selecting this option:

i. Browse and upload the certificate in the *Upload Certificate* field.

ii. Browse and upload the certificate file *(.cer, .der, .crt, .pfx, .p12, .pem, .p7b, .jks, or .keystore* formats) in the *Upload CA Bundle* field.

iii. If the uploaded certificate is password protected, enter the password in the *Certificate Password* field.

Click **Apply.**

c. Certificate Content: If your CA has sent the certificate content:

i. Copy and paste the certificate content in the *Paste Certificate Content* field.

ii. If your certificate's private key is password protected, enter its password in the *Private Key Passphrase* field.

iii. Click **Apply.**

4. Restart AD360.

Appendix

What is SSL?

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. 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). A CA is an entity that verifies all the details mentioned in the CSR—including the name of the organization and 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 together 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.

Important SSL-related terms

Term	Description
Certificate signing request (CSR)	To receive an SSL certificate, a CSR needs to be created and submitted to a CA.
Certification Authority (CA)	CAs are entities that verify all the details mentioned in a CSR (name of the organization and more), and then issues the certificate. There are two types of CAs: internal CAs and external CAs. An internal CA is a member of a server or domain controller in a specific domain, and has been assigned the role of a CA. External CAs are third-party applications—like Comodo, Verisign, and more—that issue an SSL certificate for your organization.
Keystore	A keystore is a repository that contains the public and private keys required for the encryption and decryption of data once a secure connection is established between the client and the server.

Our Products

Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus

Exchange Reporter Plus | RecoveryManager Plus

ManageEngine AD360 is a unified identity and access management (IAM) solution that helps manage identities, secure access, and ensure compliance. It comes with powerful capabilities like automated identity life cycle management, access certification, risk assessment, secure single sign-on, adaptive MFA, approval-based workflows, UBA-driven identity threat protection and historical audit reports of AD, Exchange Server and Microsoft 365. AD360's intuitive interface and powerful capabilities make it the ideal solution for your IAM needs, including fostering a Zero Trust environment.

For more information, please visit
www.manageengine.com/active-directory-360/.

$ Get Quote Download