ManageEngine
ADManager Plus

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

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?

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). 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.

Important SSL-related terms:

Term	Description
Certificate Signing Request (CSR)	To receive an SSL certificate, a Certificate Signing Request (CSR) needs to be created and submitted to a Certificate Authority (CA).
Certificate Authority (CA)	CA is an entity that verifies all the details mentioned in the CSR (name of the organization and more), and then issues the certificate. There are two types of CAs: internal CA and 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. 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 encryption and decryption of data once a secure connection is established between the client and the server.

Steps to enable HTTPS and apply an SSL certificate 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)
- Submitting the CSR to your CA
- Binding of the CSR with digital signatures by the CA
- Associating the certificate with ADManager Plus

The SSL Certificate Tool in ADManager Plus allows you to:

1. Apply an existing certificate
2. Generate CSR and apply certificate

Steps to apply an existing SSL certificate in ADManager Plus:

1. Log in to ADManager Plus and navigate to the **Admin** tab.
2. Under General Settings, click **Connection**.
3. Select *Enable HTTPS mode*. The default port number for HTTPS is 8443. Specify the desired port number if you wish to use a different port.
4. Click the **SSL Certificate Tool** option.
5. Select the **Apply Certificate** option.
6. Choose how you would like to import the certificate from the options and fill in the required fields:
   - **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 in a ZIP file. After selecting this option,
     - Browse and upload the ZIP file in the **Upload Certificate (Zip file)** field.
     - If your certificate's private key is password protected, enter its password in the **Private Key Passphrase** field.
     - Click **Apply**.
   - **Individual Certificate:** If your CA has given only one certificate in the PFX or PEM format, then select the **Individual Certificate** option. After selecting this option,
     - Browse and upload the certificate in the **Upload Certificate** field.
     - Browse and upload the .ca file in the **Upload CA Bundle** field.
     - If the uploaded certificate is password protected, enter the password in the **Certificate Password** field.
     - Click **Apply**.
   - **Certificate Content:** If your CA has sent the certificate content,
     - Copy and paste the certificate content in the **Paste Certificate Content** field.
     - If your certificate's private key is password protected, enter its password in the **Private Key Passphrase** field.
     - Click **Apply.**
7. Restart ADManager Plus.

Steps to generate CSR and apply the certificate:

1. Log in to ADManager Plus and navigate to the **Admin** tab.
2. Expand the *General Settings* section in the left navigation pane and click on **Connection.**
3. Select **Enable HTTPS mode**. The default port number for HTTPS is 8443. Specify the desired port number if you wish to use a different port.
4. Click the **SSL Certificate Tool** option.
5. Select **Generate Certificate** and fill in the required fields.
   - **Common Name:** Enter the name of the server where ADManager Plus is running.
   - **SAN Names:** 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 1024 bits.
6. Click on **Generate CSR** to generate a CSR certificate and click the **Download CSR** option in the popup or manually get it from the <Install_dir>\Certificates folder. Send the downloaded CSR to your CA and get it signed. Upload the CA-signed CSR by following the steps listed under Steps to apply an existing SSL certificate in ADManager Plus.
7. If you'd like to generate a self-signed certificate, click **Generate & Apply Self-Signed Certificate.**

Our Products

AD360 | Log360 | ADAudit Plus | ADSelfService Plus | M365 Manager Plus | RecoveryManager Plus

ManageEngine
ADManager Plus

ADManager Plus is a unified management and reporting solution for Active Directory, Microsoft 365, Exchange, and Google Workspace. The solution offers more than 200 out-of-the-box, actionable reports that fetch vital data across multiple platforms. With its help desk delegation capability, admins can define roles and delegate tasks securely to non-admin users. Other capabilities of ADManager Plus include file permissions management, automated stale account cleanup, GPO management, and customizable workflows. Admins can also manage Active Directory on-the-go with iOS and Android apps.

Get Quote Download