ManageEngine
M365 Manager Plus

Guide to enable HTTPS and install SSL certificate

www.microsoft365managerplus.com

Table of Contents

Document summary

This document guides you through the process of installing an SSL certificate and enabling HTTPS. In doing so, you can ensure the connection between the web browser and the M365 Manager Plus server is safe from security threats such as data eavesdropping and theft. Click here to learn what SSL is and what you need to know before setting it up.

SSL configuration

ManageEngine M365 Manager Plus supports SSL connections to ensure security of data transferred between the browser and the product server.

Steps to apply the SSL certificate

Let's see how to generate and apply a SSL certificate.

1. Navigate to **Settings → Admin → General Settings → Connection → SSL Certification Tool.**
2. If you don't have a SSL certificate, select the **Generate Certificate** option and follow the steps here.
3. If you already have a SSL certificate, select the **Apply Certificate** option and follow the steps here.

Generate certificate

1. In the **Common Name** field, enter the name of the server.

   Example: For the URL **https://servername:9251**, the common name is **servername**.
2. In the **Organizational Unit** field, enter the department's name that you want to be displayed in the certificate.
3. In the **Organization** field, enter the legal name of your organization
4. In the **City** field, enter the name of the city as provided in your organization's registered address.
5. In the **State/Province** field, enter the name of the state or province as provided in your organization's registered address.
6. In the **Country Code** field, enter the two letter code of the country where your organization is located.
7. In the **Password** field, enter a password that consists of at least six characters to secure the keystore.
8. In the **Validity (In Days)** field, specify the number of days for which the SSL certificate will be considered valid.

   Note: When no value is entered, the certificate will be considered to be valid for 90 days.
9. In the **Public Key Length (In Bits)** field, specify the size of the public key.

   Note: The default value is 2,048 bits and its value can only be incremented in multiples of 64.

10. After all values have been entered, 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 **Download CSR** or manually get it by going to the **<Install_dir>\Certificates** folder.

ii. Once you have received the certificate files from your CA, follow the steps listed under Apply Certificate to apply the SSL certificate.

b. Apply Self-signed Certificate

This option allows you to create a self-signed certificate and apply it instantly in 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 **Apply Self-Signed Certificate.**

ii. You'll be taken directly to step 3.

iii. Here, **select the components** in which you want to apply the self-signed certificate from **Apply certificate** to drop-down box.

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

Apply certificate

If you already have a SSL certificate, follow the steps listed below to apply it.

1. In the **Apply Certificate** to drop-down, select the component for which you want to apply the SSL certificate.
2. Choose an **Upload Option** based on the certificate file type.

a. ZIP upload:

i. If your CA has sent you a ZIP file, then select ZIP Upload, and upload the file.

ii. If your CA has sent you individual certificate files—user, intermediary, and root certificates—then you can put all these certificate files in a ZIP file and upload it.

b. Individual Certificates:

i. If your CA has sent you just one certificate file (PFX or PEM format), then select Individual Certificates, and upload the file.

ii. If your CA has sent the certificate content, then paste the content in a text editor and save it as a CER, CRT, or PEM format, and upload the file.

c. **Certificate Content:**

i. If your CA has sent you a ZIP file, then select ZIP Upload, and upload the file.

ii. If your CA has sent you individual certificate files—user, intermediary, and root certificates—then you can put all these certificate files in a ZIP file and upload it.

3. If the certificate file requires a password, then enter it in the **Certificate Password** field. Or, if the certificate contains a password-protected private key, enter the password in the **Private Key Passphrase** field.
Note: Only Triple DES encrypted private keys are currently supported.
4. Click **Apply.**
5. Finally, restart the product.

Enabling HTTPS

We recommend that you use HTTPS over HTTP to ensure secure transportation of information over your network. You can do this from within the user interface under the *Admin* tab. Navigate to the settings found under **Settings → Admin tab → Connection → Connection Settings.**

1. Click the **Advanced** option that appears after you click on *M365 Manager Plus (https)* to use and specify the TLS versions and cipher suites of your choice.
2. In the **TLS** drop-down menu, select the TLS versions you want.
   a. You can also select the cipher suites you want to use in the cipher field. We support the following cipher suites:

   i. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
   ii. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
   iii. TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
   iv. TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
   v. TLS_RSA_WITH_AES_128_CBC_SHA
   vi. TLS_RSA_WITH_AES_256_CBC_SHA
   vii. TLS_RSA_WITH_AES_128_CBC_SHA256
   viii. TLS_RSA_WITH_AES_256_CBC_SHA256
3. You can also specify the cipher suites you want to use in the **Ciphers** field.
4. Click **Save.**

With these changes, you can secure all communication through M365 Manager Plus and strengthen security.

Appendix

What is SSL?

An acronym for Secure Socket Layer, SSL is an encryption technology to secure the data exchange between a website and its visitor's web browser. Normally, when a user communicates with a website, say, to submit credit card information, the data travels to the server as plain text, which is susceptible to data theft.

If this data is encrypted, then no eavesdropper can read it. Thus, it's really very important to secure a website with SSL.

Certificates and Certifying Authority (CA)

SSL Certificate

This is a digital identity of a company and ensures that a visitor is talking only to its intended website, and that whatever data is submitted to the site is encoded and reaches only the intended site. This system is analogous to banks recognizing their customers by their signatures. In this case, the browsers (thereby the end users) are programmed to trust these CA presented certificates.

Certifying Authority

Regulatory organizations, with the help of standard policies, issue certificates to a domain, declaring them trustworthy. Every certificate generated is unique to the company being certified, which makes identification easy. CAs secure all necessary information about a company before issuing a certificate for it and also keep updating it in their records, which adds to the trustworthiness.
Some of the popular CAs are Verisign, Comodo, GoDaddy, etc.

Keystore

Keystore is specifically designed to store various kinds of encryption information.

CSR

For a CA to generate an SSL certificate for a company, it first collects the information about the company and other identifiers such as public key (digital signature), and then binds them all with its certificate (which could be a piece of encrypted token or something similar). In doing so, it generates a unique identifier for the company.

Every certificate issuance process begins with a "certificate request" from the company. CAs refer to this process as "Certificate Signing Request". The CAs accept the company information and digital signatures in a special form of file: the ".csr" file.
The usual SSL issuance process involves three steps:

- First, you generate a CSR and submit it to the CA.
- CA binds this CSR with its digital signatures and returns it.
- Now, you bind all this with your company domain.

Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus

Exchange Reporter Plus | RecoveryManager Plus

ManageEngine
M365 Manager Plus

M365 Manager Plus is an extensive Microsoft 365 tool used for reporting, managing, monitoring, auditing, and creating alerts for critical incidents. With its user-friendly interface, you can easily manage Exchange Online, Azure Active Directory, Skype for Business, OneDrive for Business, Microsoft Teams, and other Microsoft 365 services from a single console.

$ Get Quote Download