ManageEngine
O365 Manager Plus

O365 Manager Plus:

Guide to enable HTTPS and install SSL certificate

www.o365managerplus.com

Table of Contents

Document Summary

The purpose of this document is to guide you through the process of securing O365 Manager Plus by installing an SSL certificate and enabling HTTPS. In doing so, you ensure that the connection between the web browser and O365 Manager Plus server is safe from security threats such as data eavesdropping and theft.

Why do you need SSL Certification?

O365 Manager Plus can be made available over the internet making it easier for IT admins to get information about Office 365 services from anywhere, anytime. To secure the communication between users' web browsers and O365 Manager Plus server, the connection between these two entities must be secured.

Secure Sockets Layer (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.

Steps to install Certificate Authority (CA) signed certificate

To install the CA signed SSL certificates, use the instructions listed for the specific vendor below.

Important: These instructions might change depending on the certificate issued by the CA.

Note: Please make sure you replace the example values given inside < >.

Step1: Add the CA signed certificates to the keystore

1. Download and unzip the certificate files, which you received from your CA.
2. Open an elevated command prompt and navigate to **<install_directory>\jre\bin** folder

   (By default: C:\ManageEngine\O365 Manager Plus\jre\bin)
3. Now, run the commands from the below list as applicable to your CA:

GoDaddy

If your CA is "***GoDaddy***", then run the following commands:

i. keytool -import -alias root -keystore **<Keystore_Name>.keystore** -trustcacerts -file gd_bundle.crt

ii. keytool -import -alias cross -keystore **<Keystore_Name>.keystore** -trustcacerts -file gd_cross_intermediate.crt

iii. keytool -import -alias intermediate -keystore **<Keystore_Name>.keystore** -trustcacerts -file gd_intermediate.crt

iv. keytool -import -alias **<Alias Specified when creating the Keystore>** -keystore **<Keystore_Name>.keystore** -trustcacerts -file **<CertificateName>.crt**

Verisign

If your CA is **"Verisign"**, then run the following commands:

i. keytool -import -alias intermediateCA -keystore **<Keystore_Name>.keystore** -trustcacerts -file **<your_intermediate_certificate_name>.cer**

ii. keytool -import -alias **<Alias Specified when creating the Keystore>** -keystore **< Keystore_Name>.keystore** -trustcacerts -file **<CertificateName>.cer**

Comodo

If your CA is "**Comodo**", then run the following commands:

i. keytool -import -trustcacerts -alias root -file AddTrustExternalCARoot.crt -keystore **<Keystore_Name>.keystore**

ii. keytool -import -trustcacerts -alias addtrust -file UTNAddTrustServerCA.crt -keystore **<Keystore_Name>.keystore**

iii. keytool -import -trustcacerts -alias ComodoUTNServer -file ComodoUTNServerCA.crt -keystore **<Keystore_Name>.keystore**

iv. keytool -import -trustcacerts -alias essentialSSL -file essentialSSLCA.crt -keystore **<Keystore_Name>.keystore**

v. keytool -import -trustcacerts -alias **<Alias Specified when creating the Keystore>** -file **<Certificate-Name>.crt** -keystore **<Keystore_Name>.keystore**

Step 2: Bind the certificates with O365 Manager Plus

This will configure the O365 Manager Plus server to use the keystore with your SSL certificate.

1. Go to **Admin > General Settings > Connection.** Under **Connection Type,** select **O365 Manager Plus [https]** option.

2. Click **Save** and **shutdown** O365 Manager Plus.

3. Now open the **server.xml** file present in **<install_directory>\conf (By default: C:\ManageEngine\O365 Manager Plus\conf)** folder in a text editor of your choice.

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

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

   a: keystoreFile="./conf/<certificate_file_name>.keystore"

   b: keystorePass="<password>"

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

6. **Save** server.xml file and close it.

7. **Restart** O365 Manager Plus again for the changes to take effect.

Steps to install P7B certificate

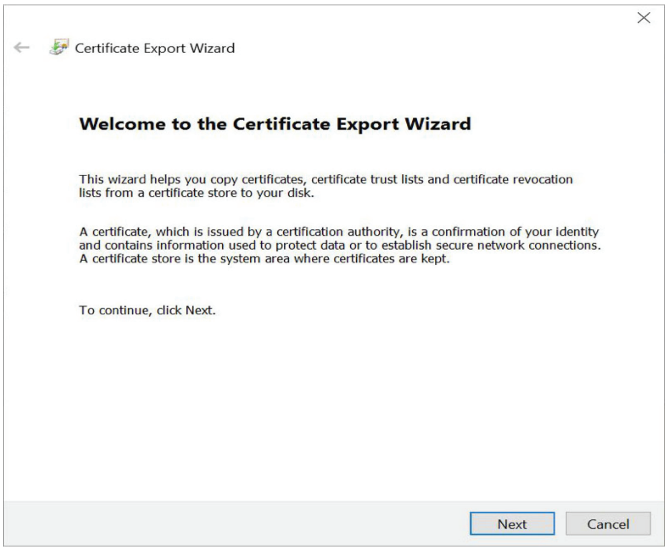
1: Go to **Admin > General Settings > Connection.** Under Connection Settings, **select O365 Manager Plus [https]** option as the connection type.

2: Click **Save** and then shutdown O365 Manager Plus.

3: Double click the Domain Certificate, which has your O365 Manager Plus host/alias name.

4: In the **Details** tab, **click Copy to File.**

5: In the **Certificate Export Wizard** that appears, click **Next.**



Certificate Export Wizard

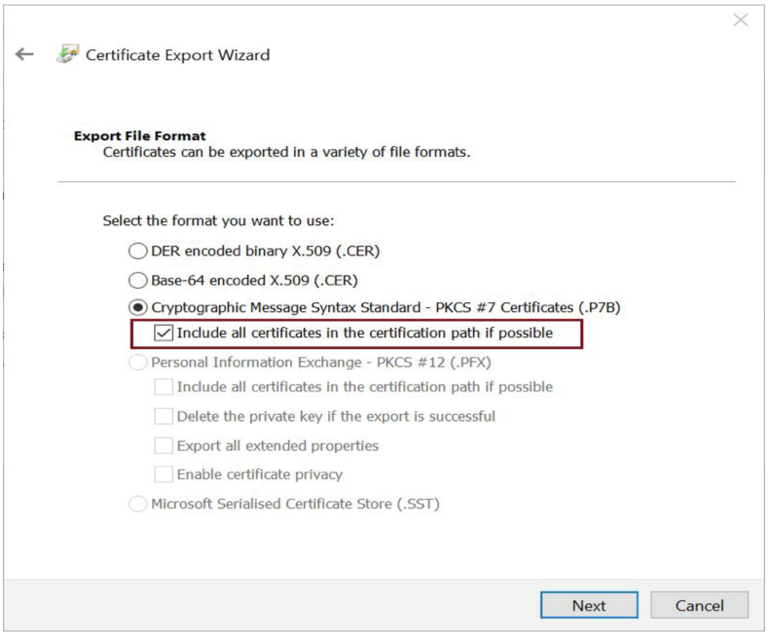
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

6. Select **P7B** file format and click **Next.**



Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)
○ Base-64 encoded X.509 (.CER)
● Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
☑ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
□ Include all certificates in the certification path if possible
□ Delete the private key if the export is successful
□ Export all extended properties
□ Enable certificate privacy
○ Microsoft Serialised Certificate Store (.SST)

7. Type the file name or browse to export the specific file in P7B format.

8. Place the P7B file at: **<install_directory>\jre\bin** (By default: C:\ManageEngine\O365 Manager Plus\jre\bin)

9. Open an elevated command prompt and navigate to **<install_directory>\jre\bin.**

10. Execute the following command:

```
Keytool -import -alias tomcat -trustcacerts -file cert.p7b -keystore <certificate_file_name>.keystore
```

11. Copy the keystore file to: **<install_directory>\conf** (By default: C:\ManageEngine\O365 Manager Plus\conf).

12. Back up the server.xml file.

13. Edit **server.xml** file (at <install_directory>\conf) by replacing the value of the following SSL connector tags at the bottom of the page :

"keystoreFile" with "./conf/<certificate_file_name>.keystore"

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

Eg:

<Connector SSLEnabled="true" acceptcount="100" clientauth="false" connectiontimeout="20000" debug="0" disable-uploadtimeout="true" enablelookups="false" **keystorefile="./conf/<certificate_file_name>.keystore" keystore-pass="<password>"** maxsparethreads="75" maxthreads="150" minsparethreads="25" name="SSL" port="9251" scheme="https" secure="true" sslprotocol="TLS" sslprotocols="TLSv1,TLSv1.1,TLSv1.2"><connector>

14. Save the changes.

15. **Restart** O365 Manager Plus and check if the certificates are installed correctly.

Steps to install wildcard certificates

Step 1: Enable SSL in O365 Manager Plus

Navigate to **Admin > General Settings > Connection.** Under **Connection Settings,** select **[https]** radio button as the **connection type** and click **Save.**

Shutdown O365 Manager Plus.

Step 2: Export PFX/PKCS12 certificate file

Export and save your **PFX/PKCS12** file in **<install_directory>\conf**

(By default: C:\ManageEngine\O365 Manager Plus\conf) folder.

Step 3: Edit Server.xml file to include the wildcard certificate

Now open the **server.xml** file present in **<install_directory>\conf** folder in a text editor of your choice.

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

Now, edit the following values inside that connector tag:

keystoreFile=”./conf/<certificate_file_name.pfx>”

keystorePass=”<password>”

keystoreType=”PKCS12”

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

Step 4: Start O365Manager Plus.

About O365 Manager Plus

O365 Manager Plus is an extensive Office 365 reporting, management, and auditing solution that helps administrators manage their Office 365 setup effortlessly. The web-based, user-friendly interface allows you to manage Exchange Online, Azure Active Directory, Skype for Business, and OneDrive for Business all from one place. O365 Manager Plus provides exhaustive preconfigured reports on Office 365, and also helps you perform complex tasks like bulk user management, bulk mailbox management, secure delegation, and more. It eases compliance management with its built-in compliance reports, and offers advanced auditing to keep your Office 365 setup secure from malicious activities.

About ManageEngine

ManageEngine delivers the real-time IT management tools that empower an IT team to meet an organization’s need for real-timeservices and support. Worldwide, more than 60,000 established and emerging enterprises — including more than 60 percent of the Fortune 500 — rely on ManageEngine products to ensure the optimal performance of their critical IT infrastructure, including networks, servers, applications, desktops and more. ManageEngine is a division of Zoho Corp. with offices worldwide, including the United States, United Kingdom, India, Japan and China.