ManageEngine
ADManager Plus

How to install a

P7B certificate in ADManager Plus.

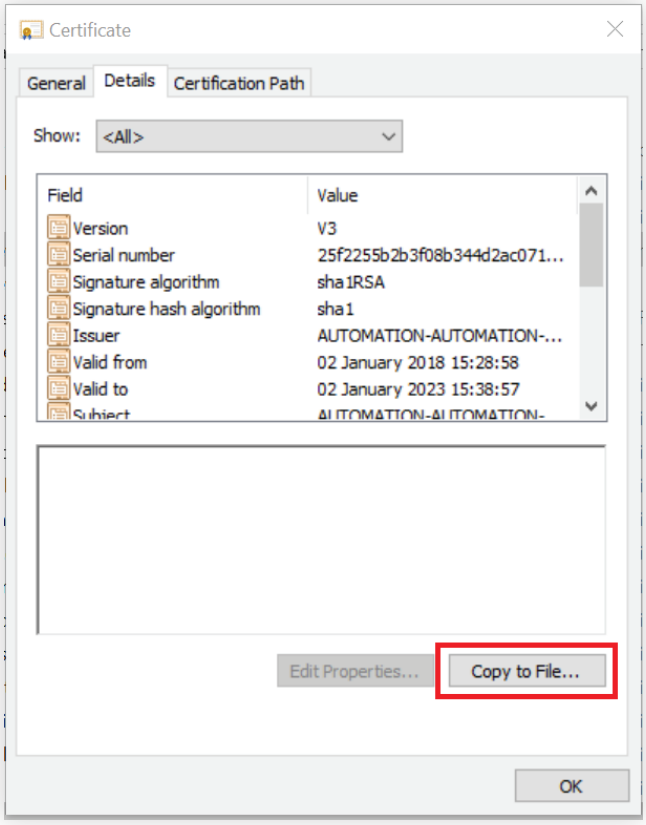
Steps to install the P7B certificate in ADManager Plus:

1. Convert the certificate from the CER format to the P7B file format
   (if the domain certificate is in the CER file format).
2. Add the certificate to the Keystore.
3. Associate the certificate with ADManager Plus.

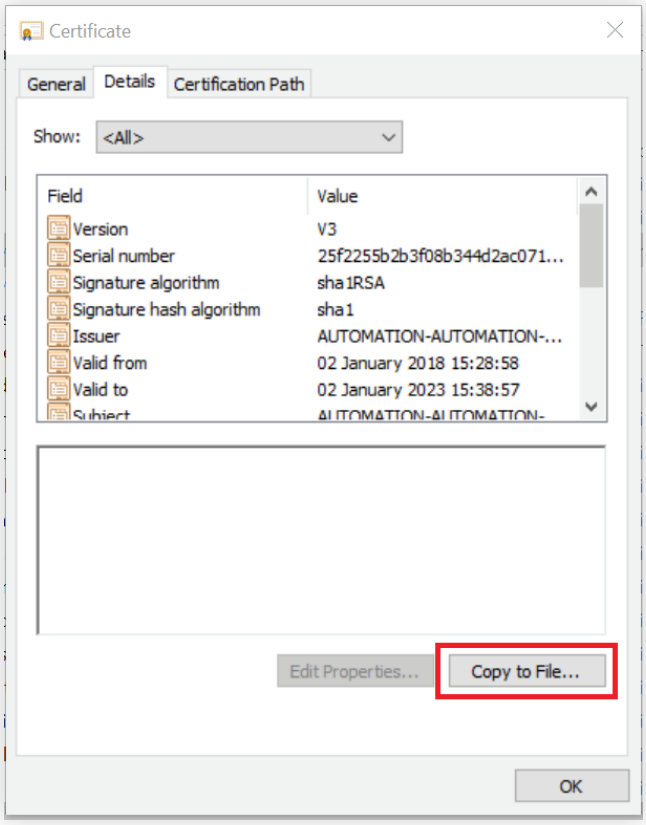
1. Convert the CER file to P7B format.

If the certificate returned by your Certification Authority has a .cer extension, then convert the CER file to the P7B file by following the steps given below:

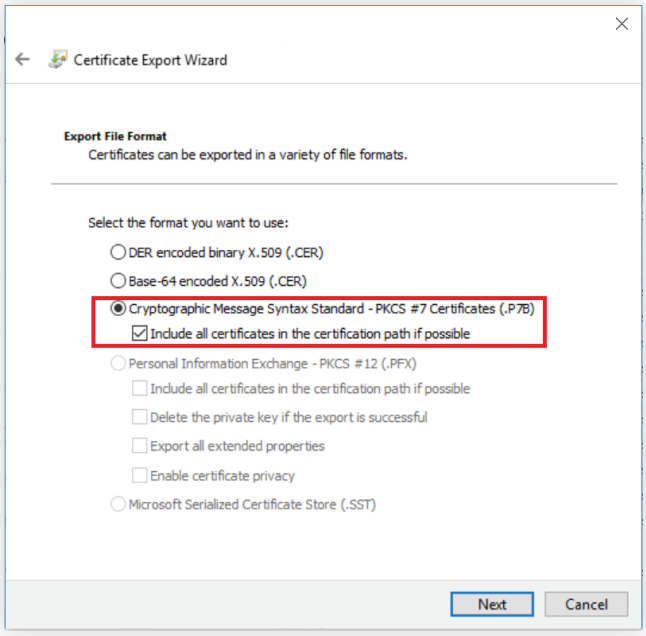
- Open the domain certificate that has been issued for the server on which ADManager Plus is installed and click on the details tab.
- Click the **Copy** to File option.



- The Certificate Wizard window will pop-up. Click on Next.



- Select the Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B) option.
- Select the Include all certificates in the certification path if possible option and click on Next.



- Specify the name of the file and **click Next.**
- **Click Finish.**

2. Add the certificate to the Keystore.

If the domain certificate returned by your CA is in the P7B file format, then follow the steps mentioned below in order to add the certificate to your Keystore.

- Copy the certnew.p7b file and paste it in the **<installationdirectory>\ManageEngine\ADManager Plus\jre\bin folder.**
- Backup the server.keystore, server.xml and web.xml files.
- Open command prompt, browse to the **<installation_directory>\ManageEngine\ADManager Plus\ jre\bin path and execute the following query to import the certificate into the .keystore file.**

```
Keytool –import –trustcacerts –alias tomcat –file certnew.p7b –keystore
<keystore_name >.keystore
```

Replace the <keystore_name> with the name of your keystore.

Note: You can skip this step if you've manually converted the CER file to the P7B format.

3. Associate the certificate with ADManager Plus

- Copy the '.keystore' file from the <installation_directory>\ManageEngine\ADManager Plus\jre\bin location and paste it at the <installation_directory>\ ManageEngine\ADManager Plus\conf location.
- At the <installation_directory>\manageengine\ADManager Plus\conf location, locate the server.xml file and take a backup of that file.
- Open the server.xml file using an editor and navigate to the last connector tag.

  Replace the value of the keystore file with the location of your keystore ('./conf/<keystore_name>.keystore)
- Replace the value of the keystorePass with the keystore password.

server.xml

```
                timestamp="true"/-->
            <!--    <Logger className="com.adventnet.mfw.log.TomcatLog"
                directory="logs"  prefix="localhost_log." suffix=".txt"
                timestamp="true"/>-->

        <!-- Define properties for each web application.  This is only needed
            if you want to set non-default properties, or have web application
            document roots in places other than the virtual host's appBase
            directory.  -->

        <!-- Tomcat Root Context -->
    <Context docBase="/adsm" path="" sessionCookieName="JSESSIONIDADMP">
        <Manager pathname=""/>
    </Context>
    <Context docBase="../help/" path="/help" reloadable="true" useHttpOnly="true"/>
    <!-- Context appBase="webapps" debug="0" docBase="../logs/" path="/logs" reloadable="true" useHttpOnly="true"/ -->
    <Context docBase="../audit-data/" path="/audit-data" reloadable="true" useHttpOnly="true"/>

      </Host>

    </Engine>

<Connector SSLEnabled="true" URIEncoding="UTF-8" acceptCount="100" clientAuth="false" connectionTimeout="20000" disableUploadTimeout="true"
enableLookups="true" keystoreFile="./conf/Mykeystore.keystore" keystorePass="MyPass@123" maxPostSize="-1" maxThreads="150" minSpareThreads="25" name=
"SSL" port="8443" scheme="https" secure="true" sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2" sslProtocol="TLS"/>
</Service>

</Server>
```

- Save the server.xml file and restart ADManager Plus (Start---> All Programs---> ADManager Plus---> Start ADManager Plus)
- Once ADManager Plus starts up, launch the ADManager Plus client and check if the certificates have been installed correctly.