

Certificate Authentication using KeyStore (Windows)

Configuring Certificate Authentication

In order for the keystore creation process to be successful and allow connection to Anaplan users need to perform several prerequisite steps which are as follows:

1. Download and install OpenSSL
2. Create a new folder on your computers C drive named “certificate”
3. Use the Windows Command Prompt to set an environment variable
4. Create a .pem file using your digital certificate
5. Create a private key
6. Create a KeyStore Bundle file
7. Use the KeyStore Bundle file to create a KeyStore with the .jks extension
8. Import your personal .pem file into Anaplan
9. Import your .cer file into your default web browser

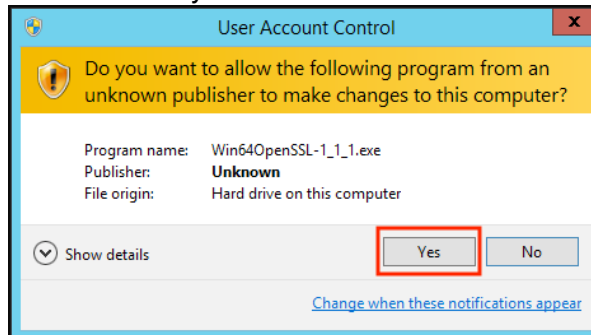
Download and install OpenSSL

1. Go to <https://slproweb.com/products/Win32OpenSSL.html>
2. Scroll down on the page to the downloads section and select the most recent 64 bit version of the installer like in the screen shot below(do not use the lite version):

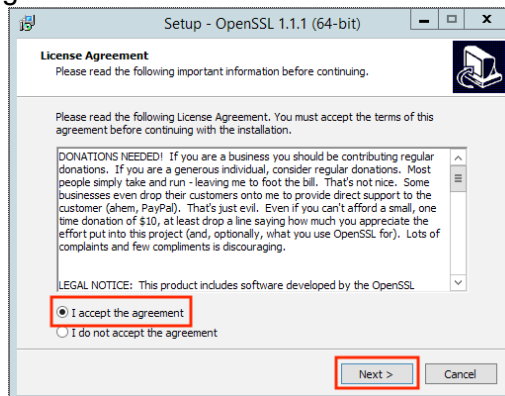
Download Win32 OpenSSL		
Download Win32 OpenSSL today using the links below!		
File	Type	Description
Win64 OpenSSL v1.1.1 Light EXE MSI (experimental)	3MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v1.1.1 (Recommended for users by the creators of OpenSSL). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v1.1.1 EXE MSI (experimental)	43MB Installer	Installs Win64 OpenSSL v1.1.1 (Recommended for software developers by the creators of OpenSSL). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v1.1.1 Light EXE MSI (experimental)	3MB Installer	Installs the most commonly used essentials of Win32 OpenSSL v1.1.1 (Only install this if you need 32-bit OpenSSL for Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v1.1.1 EXE MSI (experimental)	30MB Installer	Installs Win32 OpenSSL v1.1.1 (Only install this if you need 32-bit OpenSSL for Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v1.1.0 Light	3MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v1.1.0 (Recommended for users by the creators of OpenSSL). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v1.1.0	37MB Installer	Installs Win64 OpenSSL v1.1.0 (Recommended for software developers by the creators of OpenSSL). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v1.1.0 Light	3MB Installer	Installs the most commonly used essentials of Win32 OpenSSL v1.1.0 (Only install this if you need 32-bit OpenSSL for Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.

3. Select the “EXE “ option, download and save the file to your local computer.
4. Run the downloaded file by double clicking and follow the prompts to perform the installation. All options should be left to their default settings with few exceptions indicated in the walkthrough below.

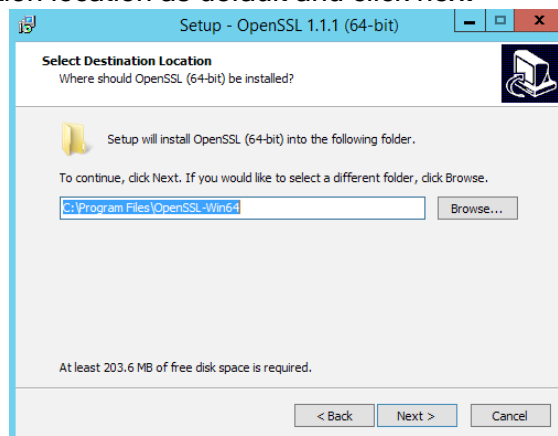
- a. If prompted by Windows UAC click yes



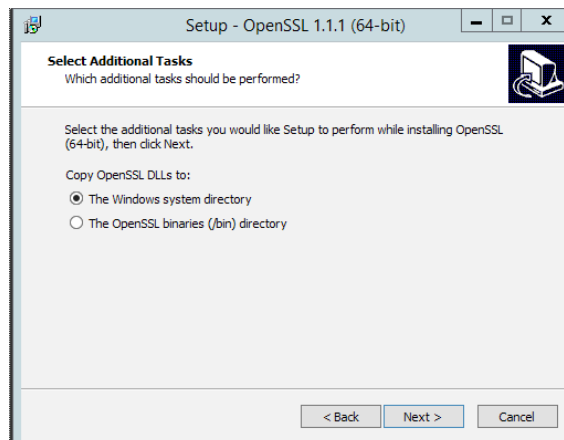
- b. Accept the license agreement and click next



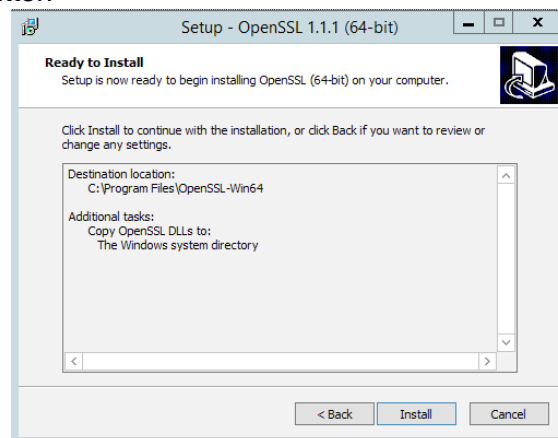
- c. Leave the installation location as default and click next



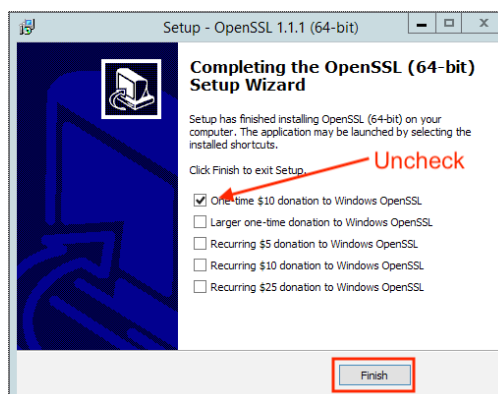
d. Leave the DLL location as default and click next



e. Click the install button



f. Wait for the installation to complete and UNCHECK the option to donate then click Finish.



Create a new folder on your computers C drive named “Certificates”

1. Open a Windows Command Prompt and execute the following commands:
 - a) `cd /`
 - b) `mkdir Certificates`

Use the Windows Command Prompt to set an environment variable

1. Run the following commands (will create an environment variable under system properties):
 - a. `setx RANDFILE "c:\Certificates\rnd"`
 - b. `setx OPENSSL_CONF "c:\Program Files\OpenSSL-Win64\bin\openssl.exe"`

Create a .pem file using your digital certificate

1. Run the following command to include the double quotes to start the OpenSSL program:
 - a. `"C:\Program Files\openssl-win64\bin\openssl.exe"`
2. Next you will extract the .pem file from your digital certificate, to do this enter the following command (Note that the location of your certificate may be different so ensure you use the correct path and certificate name in the command):
 - a. `pkcs12 -in C:\certname.p12 -nokeys -out C:\Certificates\new_cert_name.pem`
 - b. You will be prompted to enter the password for your cert, once you have done that and clicked enter your new .pem file will be placed in the Certificates folder.

Create a Private Key

1. While still in the command prompt window enter the following command:
 - a. `pkcs12 -in C:\cert_name.p12 -nocerts -out c:\Certificates\new private key name).key -nodes`
 - b. When prompted enter your cert password
 - c. Once complete you will have a file with the extension .key in your Certificates folder

Create the KeyStore bundle file and the Keystore

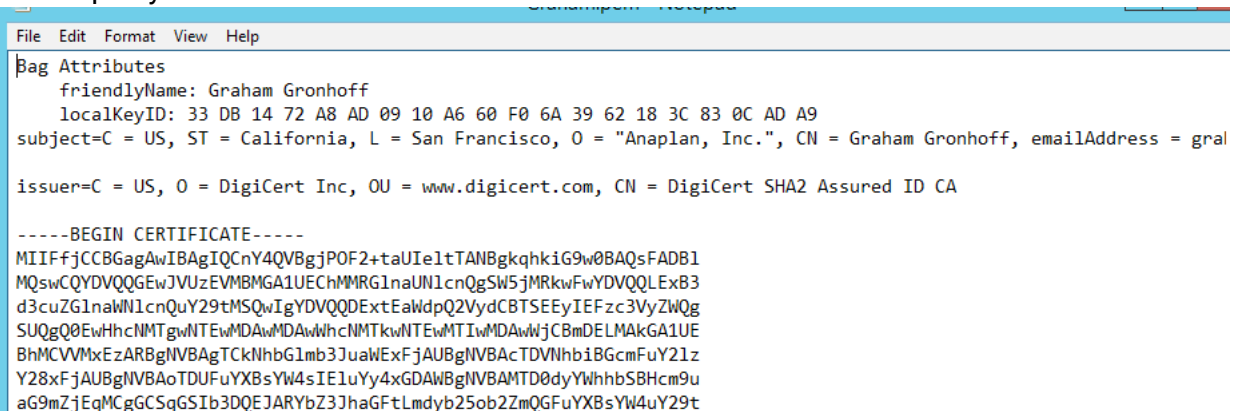
1. In the same window run the command below ensuring you use the correct certs:
 - a. `pkcs12 -export -in c:\Certificates\client_cert.pem -inkey c:\Certificates\Private.key -out c:\Certificates\keystore_bundle.p12 -name (keystore alias goes here)`
 - b. Enter your password
 - c. Re-enter your password
2. Your certificate folder should now contain 3 files, an extracted certificate with the .pem extension, a private key with the .key extension and a keystore bundle file with the .p12 extension.
3. Now you will need to exit the OpenSSL tool by typing "exit" into the command prompt.
4. Once you have exited the tool you will need to perform the following steps to create the keystore itself:
 - a. Change to the root of the C drive by entering "`cd /`"
 - b. Next enter the following command (Your version of Java may be different so enter the path using your installed version): "`Program Files\Java\jdk1.8.0_181\bin\keytool`" - `importkeystore -deststorepass (KS PAssword goes here) -destkeystore c:\new_ks_name.jks -srckeystore c:\Certificates\keystore_bundle.p12 -srcstoretype PKCS12`
 - c. Enter the password for the keystore_bundle.p12 and press enter.
5. Verify that you have a Java Keystore on your C drive (it will have the name you specified and have the extension .jks).

Setup is now complete and you can exit the Windows Command Prompt

Import your personal .pem file into Anaplan

In this portion you will need to perform some basic editing of the .pem file we created in the steps above and perform the import into your Anaplan Tenant to register the certificate for use with Data Integration tasks.

1. Navigate to the certificate directory we creation in the last section and locate you .pem file.
2. Right click the file and open with a text editor (I used notepad but whatever your preferred tool is you can use it here).
3. Once open your cert should look like this:



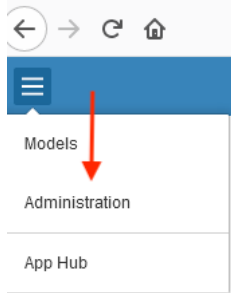
```
File Edit Format View Help
Bag Attributes
  friendlyName: Graham Gronhoff
  localKeyID: 33 DB 14 72 A8 AD 09 10 A6 60 F0 6A 39 62 18 3C 83 0C AD A9
  subject=C = US, ST = California, L = San Francisco, O = "Anaplan, Inc.", CN = Graham Gronhoff, emailAddress = grol
  issuer=C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert SHA2 Assured ID CA

-----BEGIN CERTIFICATE-----
MIIFfjCCBGagAwIBAgIQCnY4QVBgjPOF2+taUIeltTANBgkqhkiG9w0BAQsFADB1
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRG1naUN1cnQgSW5jMRkwFwYDVQQLExB3
d3cuZG1naUN1cnQyY29tMSQwIgYDVQQDEExtEaWdpQ2VydCBTSEYyIEFzc3VyZWQg
SUQgQ00wEwHcNMTgwNTAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
BhMCVVMxEzARBGNVBAgTCKNhbG1mb3JuaWEwFjAUBGNVBAcTDVNhb1BGcmFuY21z
Y28xYjAUBGNVBAoTDUFuYXBsYXN0IE1uYy4xGDAwBgNVBAMTD0dyYW90bSBHcm9u
aG9mZjEgMcGGSqGSIb3DQEJARYbZ3JhaGFtLmdyb250b2ZmQG9uYXBsYXN0Y29t
```

4. In order to load and register your certificate with Anaplan you need to remove all the text from above the line -----BEGIN CERTIFICATE-----
5. Once you have removed the text your file should look like this:

```
File Edit Format View Help
|-----BEGIN CERTIFICATE-----
MIIFfjCCBgAgAwIBAgIQcnY4QVBgjPOF2+taUIe1tTANBgkqhkiG9w0BAQsFADBl
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRG1naUN1cnQgSW5jMRkwFwYDVQQLEwB3
d3cuZG1naWN1cnQyY29tMSQwIgwYDVQQDEXTaWdpQ2VydCBTSEYIEFzc3VyZWQg
SUQgQ0EwHhcNMTgwNTEwMDAwMDAwWWhcNMTkwNTEwMTIwMDAwWjCBMDELMAkGA1UE
BhMCVVMxEzARBgNVBAgTCkNhbg1mb3JuaW50eFjAUBgNVBAcTDVNBbG9uY21z
Y28xY28xY28xY28xY28xY28xY28xY28xY28xY28xY28xY28xY28xY28xY28xY28x
aG9mZjEgMCgGCsGCSqGSIb3DQEJARYbZ3JhaGFtLmdyb25ob2ZmQGFuYX8sYW4uY29t
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAYow7s3/6FGk/EvJJXoa1
7V6xMj/jKbxJ9/BISAx71/pDnIctGYNyCBxHTD+iD8zUZs/6qw7pD00/D2UFVCir5
0qOwrvZDN8fVjtOam+M9g6Y7sJa9GVgU7iKfXvmKotJZBeBDsb1LT1M3e2t6EFJW
KE3Ec4phv/12fqaxj1MR9020N6MH4UZgZ4H01yp2aFHA56z08BZRJZa4KMhLtfHo
ciHd2MLVOfmx1cgMtq/bDYjk8+uvInbusN75ufX5Bn1fh5fieuyXyC4fhx1aG1uB
890mVrIy/cgVPnB2HrFY0HkseK191yZNJCPMdtHuoSkArCAg6KFAo4WaZcGRTj8S
bwIDAQABo4IB9DCCAFAwHwYDVR0jBBgwFoAU5wIjgABP2Ne81AvZP3Q5STI8inkw
HqYDVR0BBYEFDPbFHKorQkQpmDwaJ1iGDyDDK2pMAwGA1UdEwEB/wQCMAAwJgYD
```

6. Save and close the .pem file and open your Anaplan Workspace. In the upper left corner expand the hamburger menu and select "Administration"



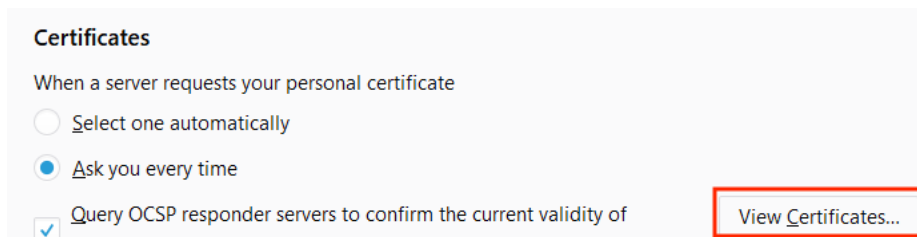
7. From here select the certificates option from the menu and then click the "Add Certificates" button in the upper right. Browse to c:\certificate folder and select your .pem file and click "Import Certificates". Your cert will be loaded and will appear in this section until it is removed:

Administration <<	Certificates			
Users	Certificate ID	Status	User ID	Certificate Issuer
Models	1059	Active	graham.gronhoff@anaplan.com	DigiCert SHA2 Assured ID CA
Business Map				

Import your .cer file into your default web browser

For this example I am going to use Mozilla Firefox, depending on your browser of choice the steps may vary however the process should be largely the same.

1. In your browser select "Options" from the tools menu then select "Privacy and Security".
2. Scroll down until you reach the "Certificates" section then choose "View Certificates"



Certificates

When a server requests your personal certificate

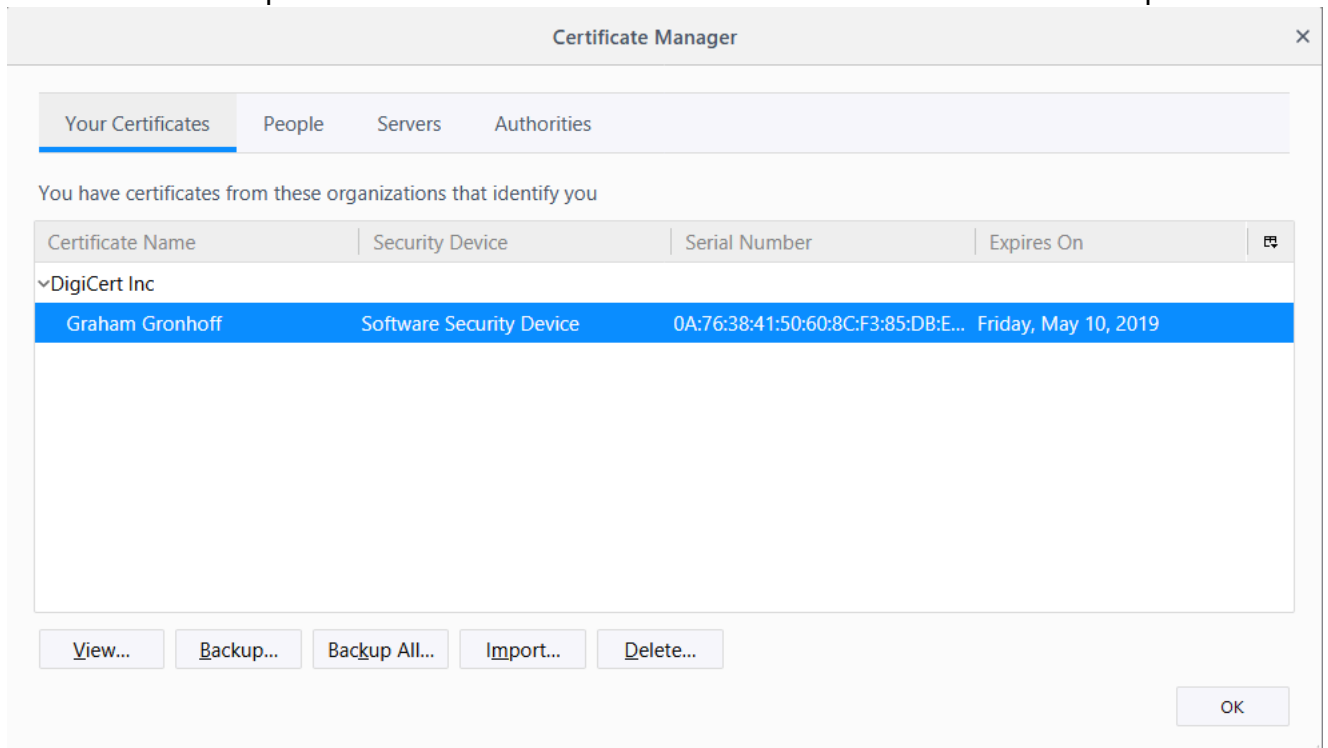
☐ Select one automatically

☒ Ask you every time

☒ Query OCSP responder servers to confirm the current validity of

[View Certificates...](#)

3. Select "Your Certificates" in the top tab and choose "Import". Click browse and navigate to the location of your certificate that is in .p12 format, select it and perform the import.
4. Enter the certificate password and click OK. Your window should now look like the example below:



Example Script for using Cert Auth with Anaplan Connect

@echo off

rem This example lists a user's workspaces

set ServiceLocation="https://api.anaplan.com/"

set Keystore="C:\Your Cert Name Here.jks"

set KeystoreAlias=""

set KeystorePassword=""

set WorkspaceId="Enter WS ID Here"

set ModelId="Enter Model ID here"

set Operation=-service "https://api.anaplan.com" -auth "https://auth.anaplan.com" -W

rem *** End of settings - Do not edit below this line ***

setlocal enableextensions enabledelayedexpansion || exit /b 1

cd %~dp0

set Command=.\\AnaplanClient.bat -s %ServiceLocation% -k %Keystore% -ka %KeystoreAlias% -kp
%KeystorePassword% -workspace %WorkspaceId% -model %ModelId% %Operation%

@echo %Command%

cmd /c %Command%

pause

