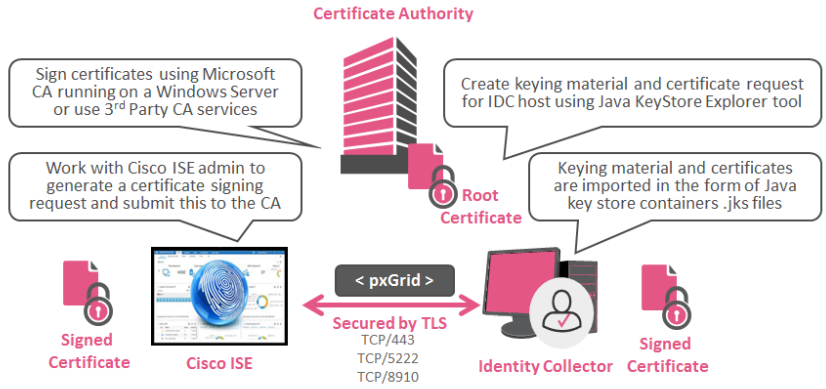
13th March 2019

Establish trust relationship between Cisco ISE and the Identity Collector

This document is based on lab experience and a video published here. The documents describe how you can issue certificates using a Microsoft Certificate Authority to establish trust between a Cisco ISE and a Check Point Identity Collector. Check the TCP ports that need to be allowed between the instances in the Identity Awareness Administration Guide here.

Reserve at least 90min of time for the trust deployment process in case you are not experienced.



Each end entity will require a signed certificate from the CA to establish the trust required for the pxGrid communication. On the ID Collector the certificates will be stored in Java key stores. In this document you will learn how to create these key stores and how to add the keying material and certificates to them.

v1 Feedback is appreciated :-) Peter Elmer, pelmer@checkpoint.com

Preparing Certificate Management Tools

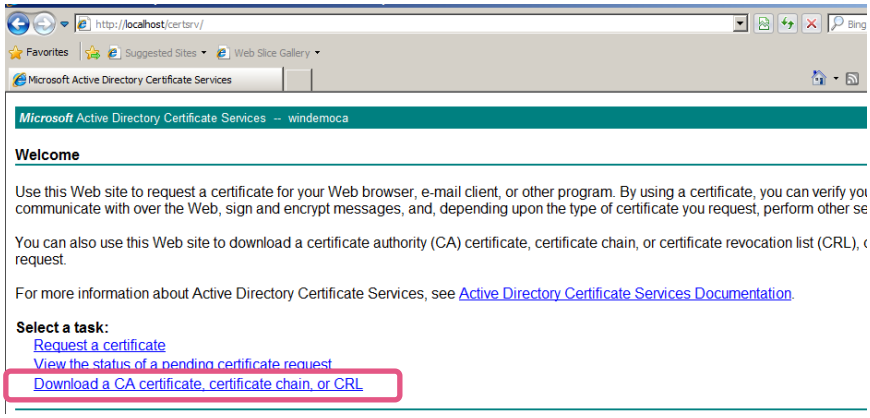
Use 'KeyStore Explorer' on Windows available at https://keystore-explorer.org/downloads.html. The tool is available as well for Linux computers.

All communication requires DNS name resolution and a network diagram will help you during the deployment process. You want the following to be documented and ready:

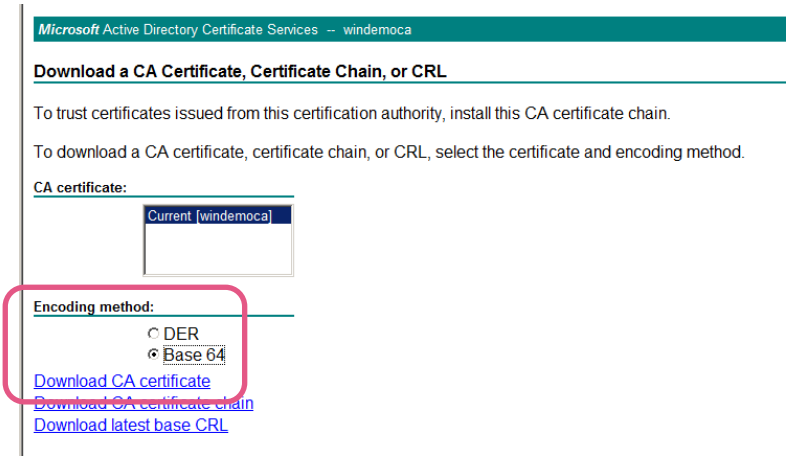
- IP addresses and FQDN of ID Collector host
- The root certificate of the CA issuing the certificates
- Access to Cisco ISE Management interface
- Ensure that Cisco ISE and ID Collector host have connectivity based on DNS name resolution and the following ports (see ID Awareness Administration Guide here for details)
    - HTTPS TCP/443
    - XMPP protocol TCP/5222
    - Bulk Update TCP/8910

You can create a Microsoft Certificate Authority on a Windows Server and access this CA locally using a web browser. Using this CA allows you full control about the certificate processes and avoids time delays when working with 3rd party Certificate Authorities.

http://localhost/certsrv/



Save the CA certificate in base64 format. You need this for later steps.

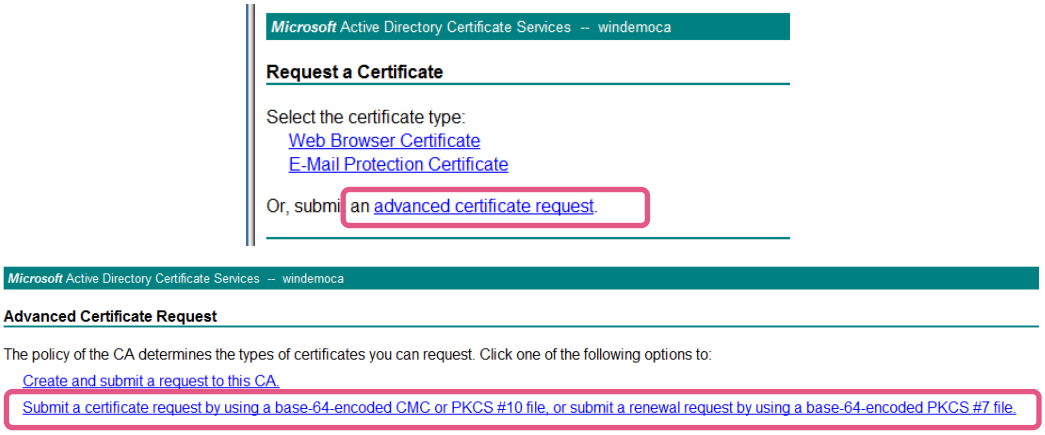


Create the Cisco ISE certificate for pxGrid

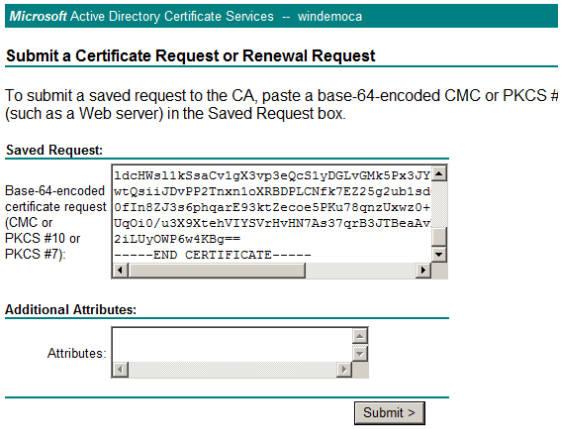
You will need to create a certificate signing request on the Cisco ISE administration interface. The signing request should include the host name of the Cisco ISE as subject name in the request.

The request should be provided in base64 encoded text format. In this way you can paste the request to the relevant menu in the Microsoft CA.

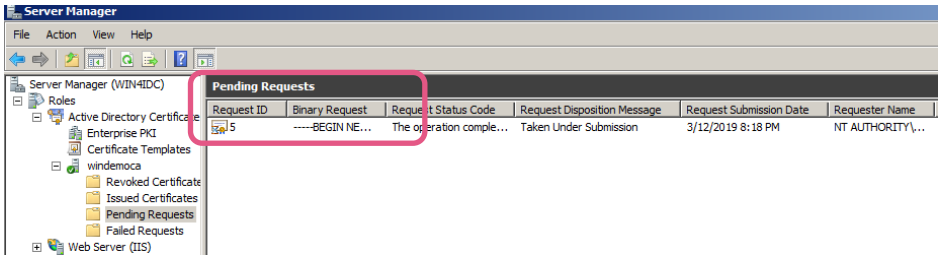
Sign the request coming from the Cisco ISE host on the Microsoft CA



Paste the base64 encoded text and 'submit'.



Issue the certificate request using the 'Service Manager > Active Directory Certificate Authority' menu.



Select the request and use the right click menu to 'issue' the certificate. Use the web interface of the CA to download the certificate to a file.

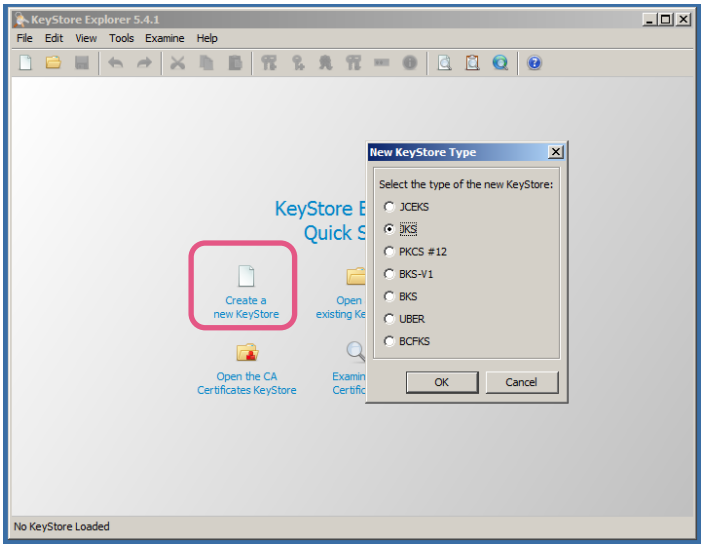
Pass the certificate and the root CA certificate to the Cisco ISE administrator and install them.

Bind to the certificate to the pxGrid service and restart the relevant Cisco ISE application services.

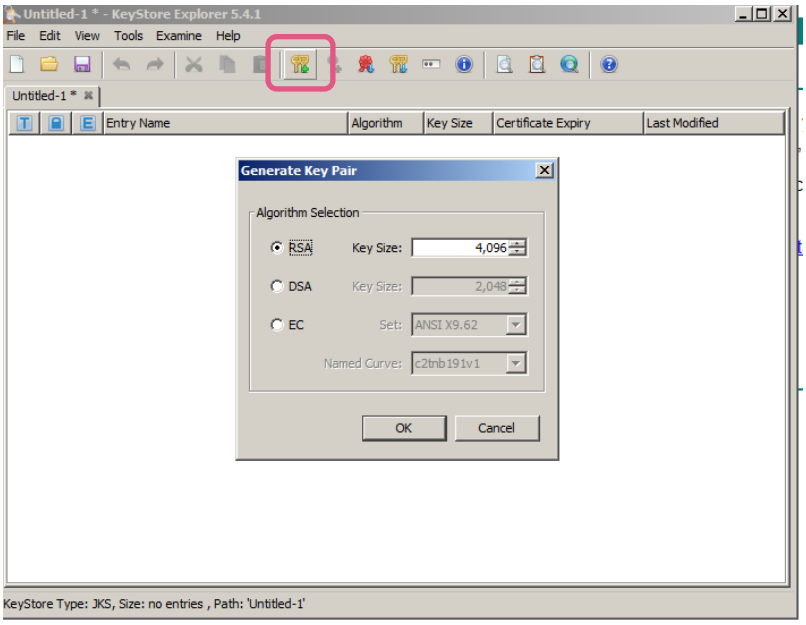
ID Collector Client Java Certificate container

Create a new key store selecting jks format

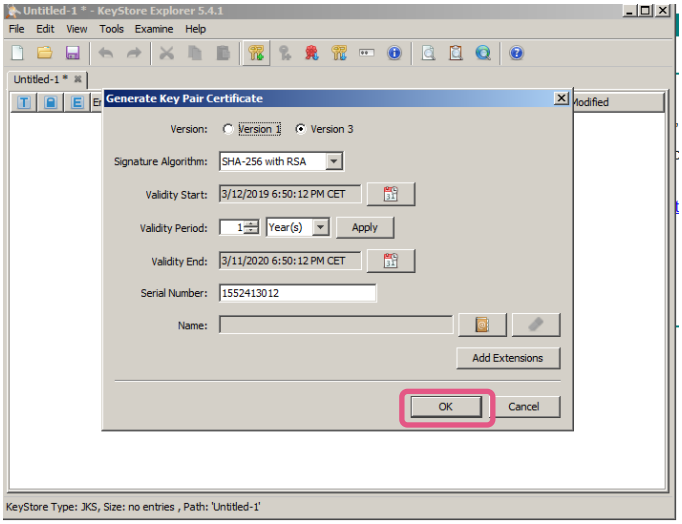
Start ‘KeyStore Explorer’ and select ‘create a new key store’.



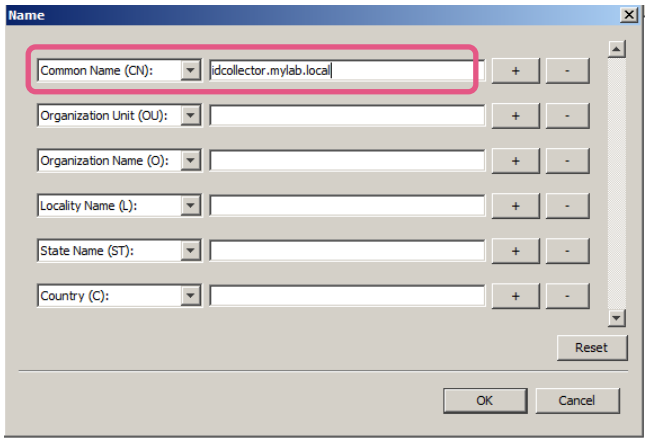
Generate a new private public key pair for the host of the ID Collector (key size should be 4096)



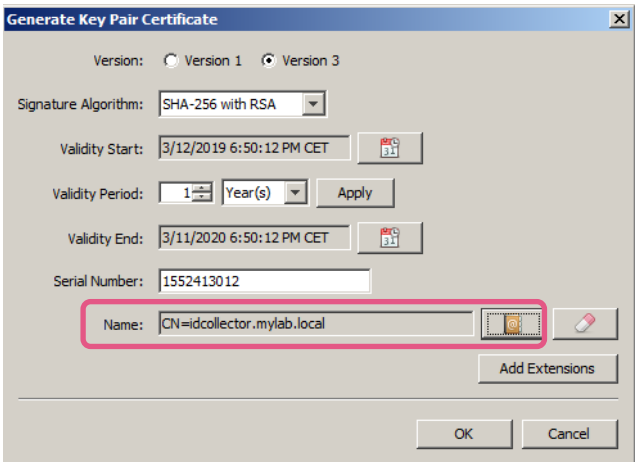
You will see this window.



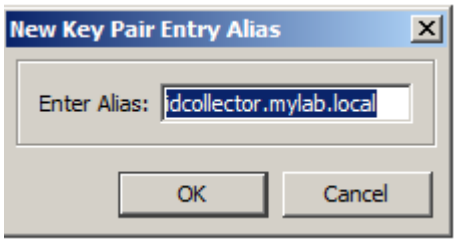
Define a name. The name will become the subject field of the certificate. All other fields can remain empty.



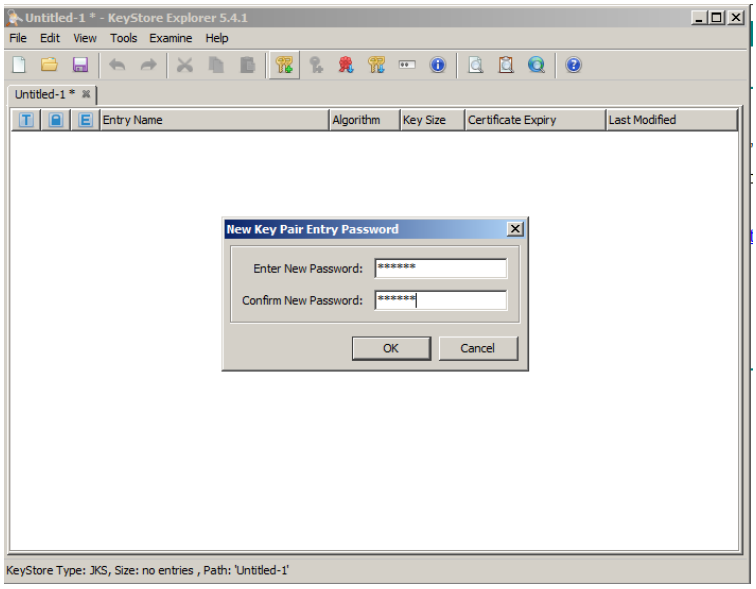
Once you clicked ‘ok’ you will see the ‘name’ field populated.



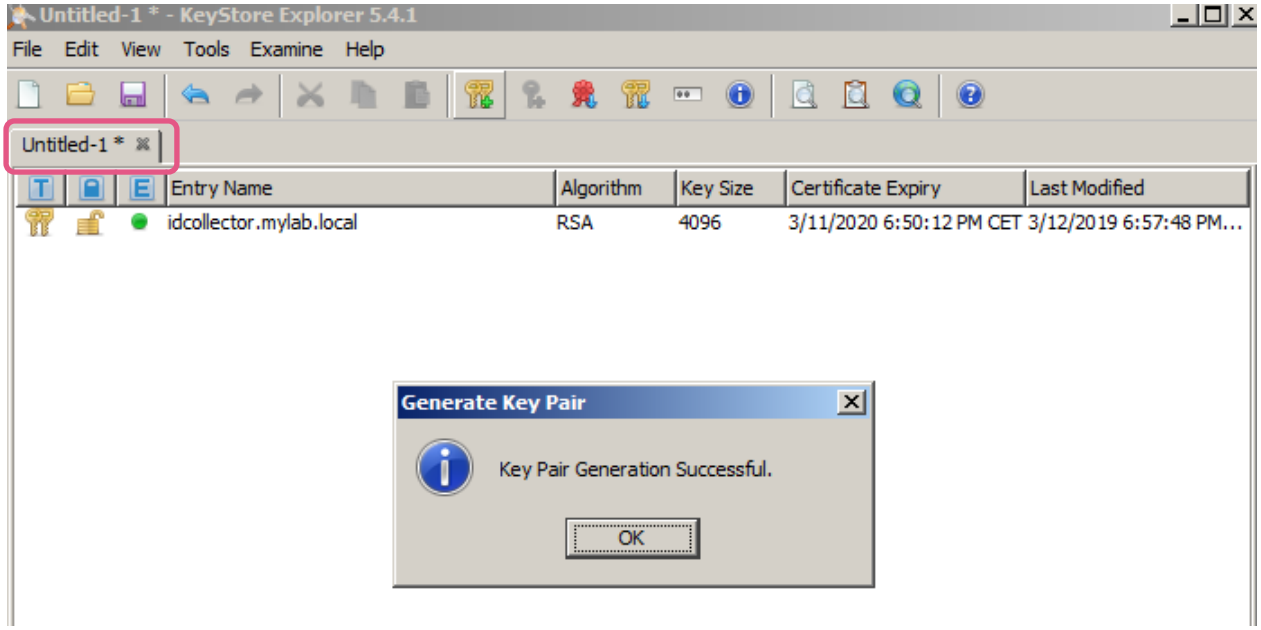
Click ‘ok’ and see the alias for this key pair.



Click ‘ok’ and define a password that will protect the private key. Use something easy i.e. ‘vpn123’ when you are in a PoC environment.

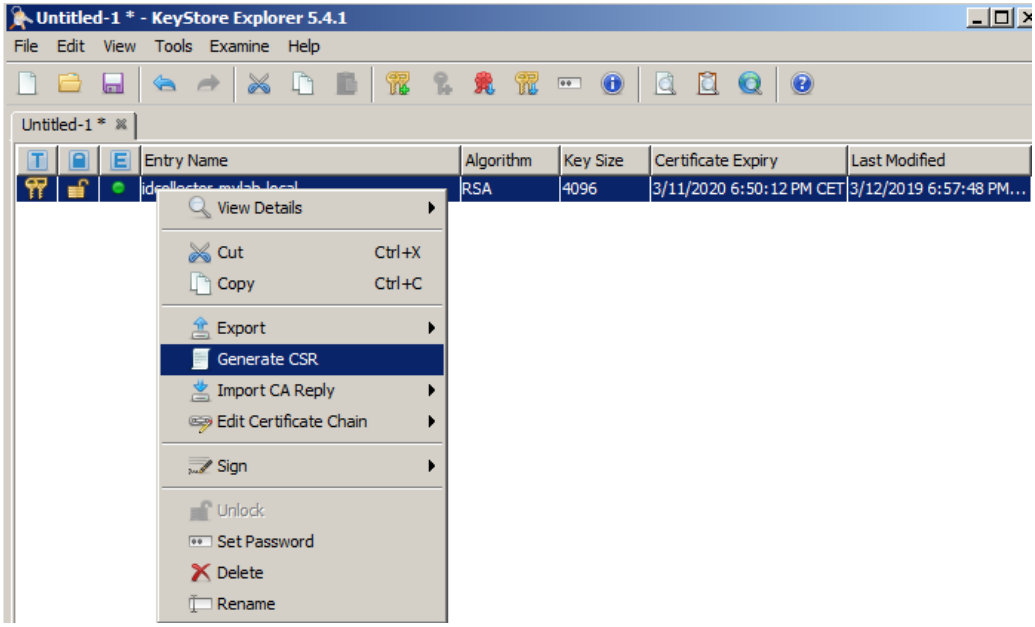


Click ‘ok’ and see that you have generated a private public key pair that can be used to request a certificate. Note the name of the jks object is still ‘untitled’.

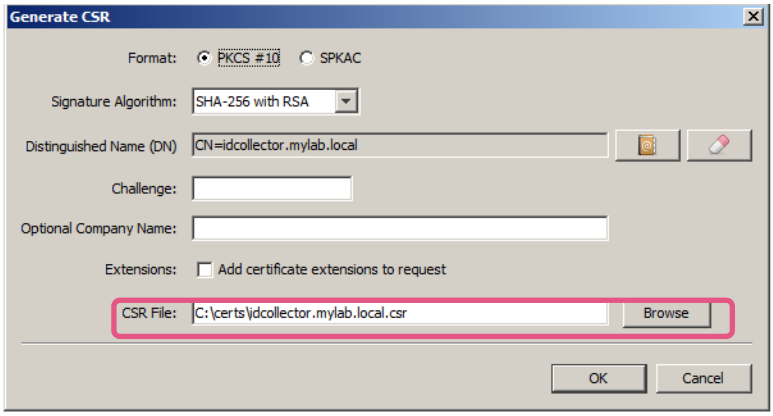


Generate certificate signing request for the ID collector host

Select the key pair, click right and execute the ‘Generate CSR’ dialog.



In the dialog window select the path where you want to save the CSR file and click ‘ok’.



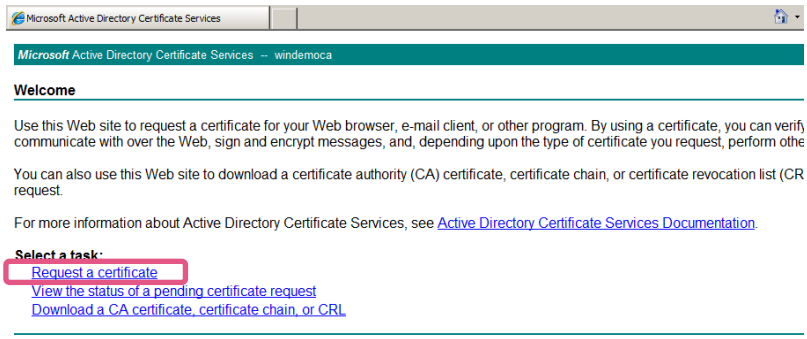
You will see the CSR was generated and find the file in the relevant directory.

Open the csr file using Notepad++ and copy the base64 encoded text including ‘begin’ and ‘end’ lines.

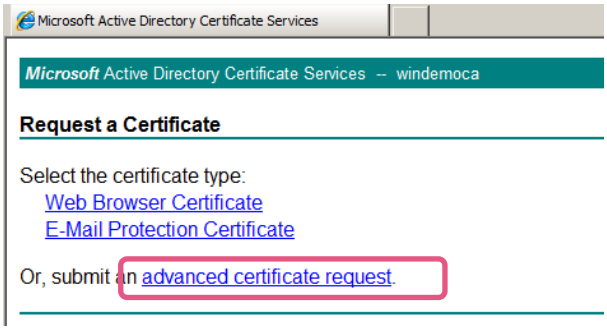
```
-----BEGIN CERTIFICATE REQUEST-----
MIIEZzCCAk8CAQAwIjEgMB4GA1UEAwwXaWRjb2xsZWN0b3IubXlsYWIubG9jYWwwggIiMA0GCSqG
SIb3DQEBAQUAA4ICDwAwggIKAoICAQC/SjTkPQkwDnJVLMtespsP5x66SO4nxin+Ep53GrtXaPqT
6uD7SeH6nu8MG/i5tgcdujO92Zs2iIisWLoYAhB6dwKtJDmczqtb+518xAHS5f5ki1cavO3Ql9cp
vFW8zSowNVxf68ad7O3B11nQhpAKqC5H/GJ1dONsrekmjOwwNDW/5AoJb+B0Bm+B6ktLzUVdBCBI
chzcJka7N8ViyO6xUSMkWf6jhyzPsfa2U3ncxJyGR9z99YI+5bSGArHXZNHp3rcN/Xuo4f0pj6rM
kN+PwAuInMgJgjyM7GgHqT8NhTtz3ZWAtv6UFElglaA4WumtTQgjy46KiCzFam8HoXIHHZutF4My
2mILL8ovWn1Bk7uyxPkiIesxpBKf97PeeDFfG3HRaB/XUDmHV5LSGatm5a7uOWLwY5Q5VFzCPt7V
8jpUlkAbc5fDYXX1DLaBJ1TLvFyrSP6dAHBCX2qWWH7Fjw+mHshn3rxl6mR5VvSh3ScDZD4UVkyq
Tb51deAy5vUq5LTZQzfNUY7tc4Z6MWjVkmNm6f0V5AzCosY4IW8EKkwLzRoTtvb7H6cMwL+haWQU
aZapAEJkB3at7XCGtIM2X5JwTRJDcUoi3oiDyolm80yOCW8ASOt0dXixQPDSXkC4HWCoRaTDvXNd
H+9Mh5AAplg1rURq7X8MRSz4VStfVQIDAQABoAAwDQYJKoZIhvcNAQELBQADggIBALdI8FCnZJ/Z
SjBhuTF7qncyOypdO88GcJO1DAmYkc37nEJLfBalvKAXGQBxxkyCEJOJLgfMF+kJf4V9Xbzd4tmX
FAiqhSlRC8TZQVBWmxRW8MUgZUPy6Am9RESjPwlKjMtYGRPtiZHdWMm+AxGUXW2mT43Zvzidta6N
Waz2fvB6at/s+DXA8vUjE+YX6Ji4xiB0Lvkj3sIQn9oXOVWWHBA4qf46IgdBsYm/9m+cCgULXRfC
UYJQWZ0cgIP0ecSw+44ZXkOUalo0g6d55mtIqZiu5AxKAd8PyXiSjGWzsXG4diuY7AxrKO4/0Am/
ST40z+yXL2jjJl+y0tQPRbl5TJnqFdgPawQ3cJn6vBlISPWO6zFELbMkU6LwUjKfIIulZu9WTsv5
rIJcWr7NwlJyQ2+XTKx5X94yJp8Nf5irZEgEAFtFcOZJrJBU15vNwOH2Z36d69VSKAkcw+gyo3b0
9SYRhd+rHpJO51Zfye1tZ8FNCLwe4jkCA62o/Jlg/1VpUDZn610aEB/ABFfU1FJkNxt1hOclY1ah
RQR/JmOlCfTW5up/AMXLJTzd0YrKK+FEqSNdWFYjsYDBC4TAaN6fCjE3fijwR19gha2sVSVgL41v
rQY+kIawegSYoxkwU2bQh5ey/8j8Lk71oduBJ6SN5NLoMaxFbEgObwZgFciN07wh
-----END CERTIFICATE REQUEST-----
```

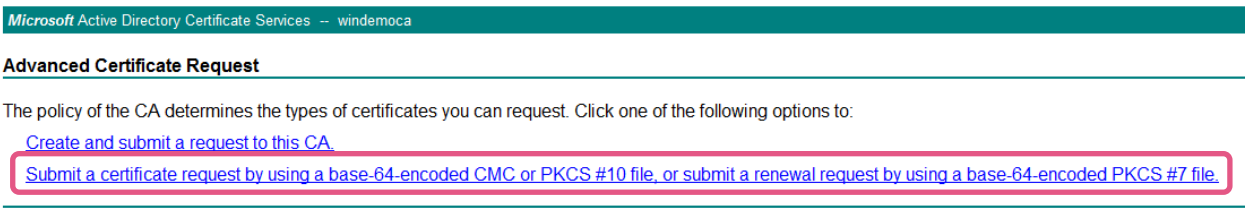
Sign the certificate request on the Microsoft CA

Paste the base64 encoded text into the request form of the Microsoft CA.

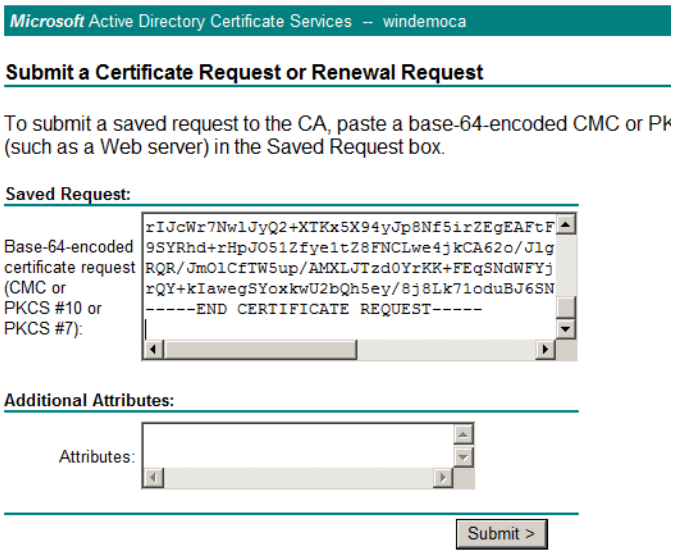


Select ‘advanced request’ and then ‘submit a certificate request by using the link including ‘base-64-encoded’.

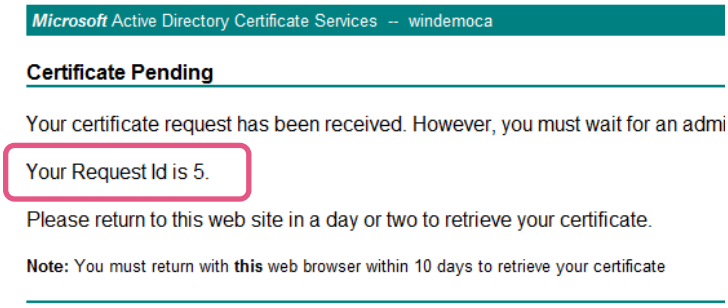




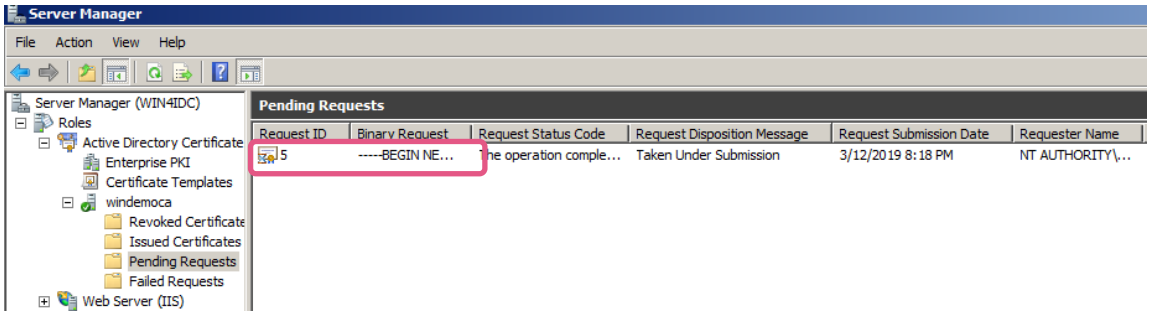
Paste the text and ‘submit’.



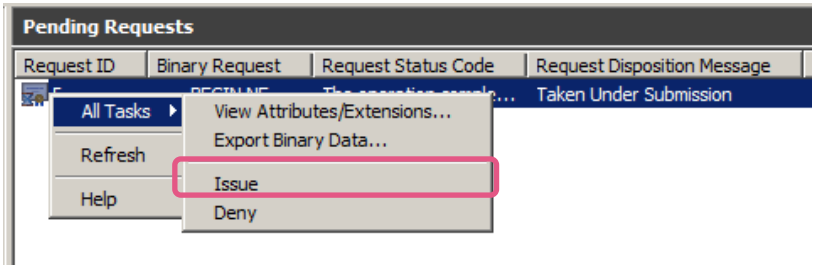
Recall the certificate request ID – here ‘5’.



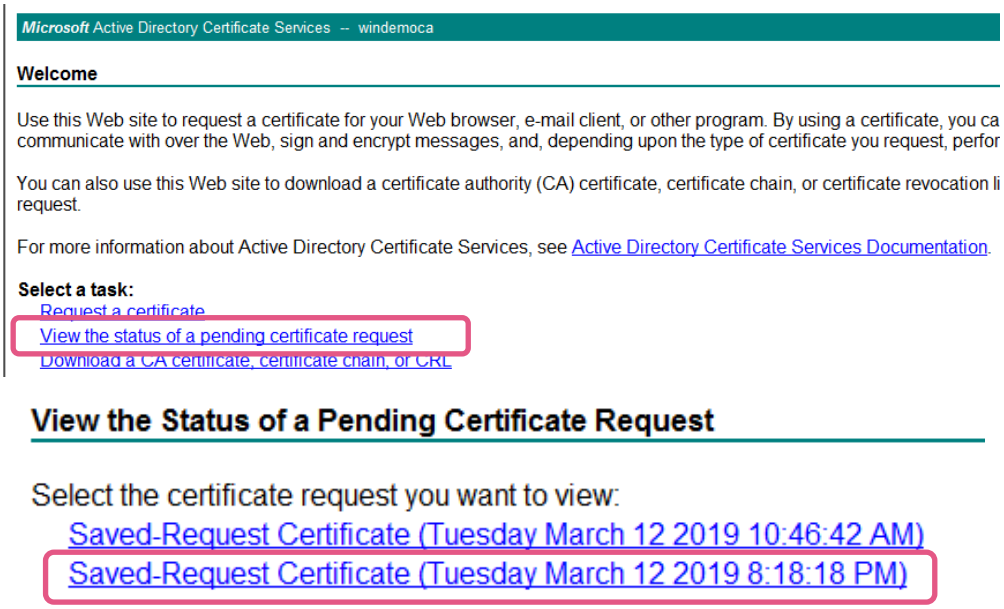
Use the ‘Server Manager > Active Directory Certificate Services’ menu to find the request.



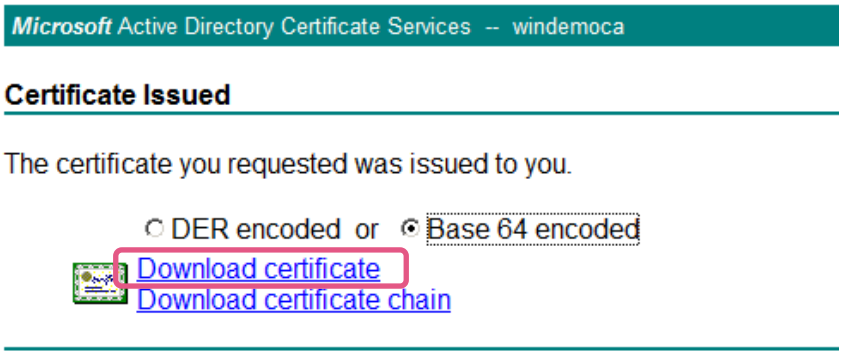
Select the request and use the right click menu to ‘issue’ the certificate.



You can use the web interface to save the signed certificate to a file.



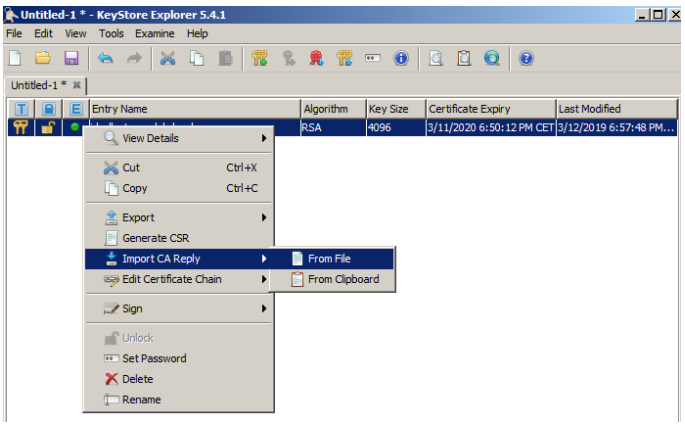
Download the certificate in Base64 format.



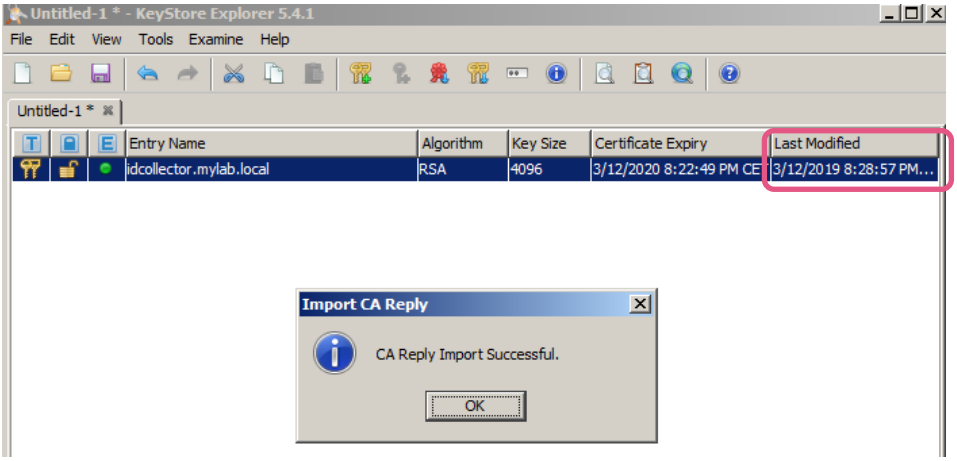
Save the file. You don´t need the certificate chain.

Import the signed certificate into the Java key store

Import the saved certificate file into the Java key store you are creating for the ID Collector client certificate.



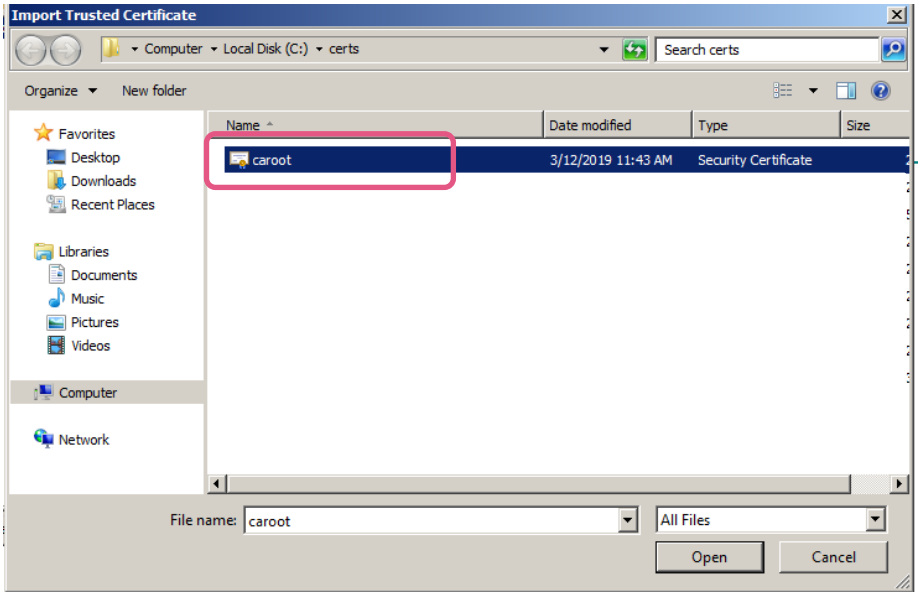
Import the file and click ‘ok’.



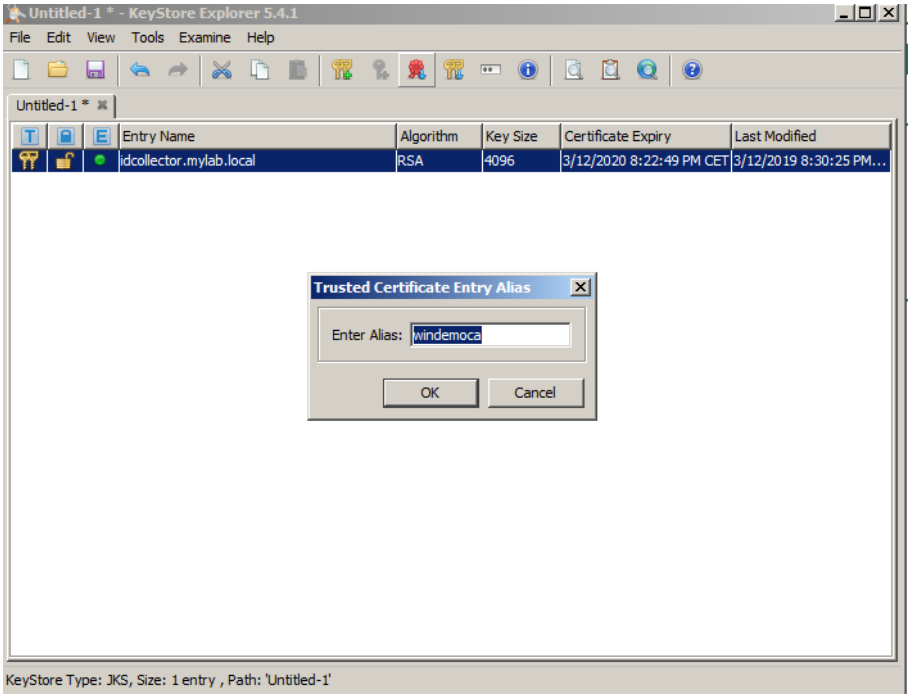
You will see the ‘last modified’ information changed.

Import the Microsoft CA root certificate into the Java key store

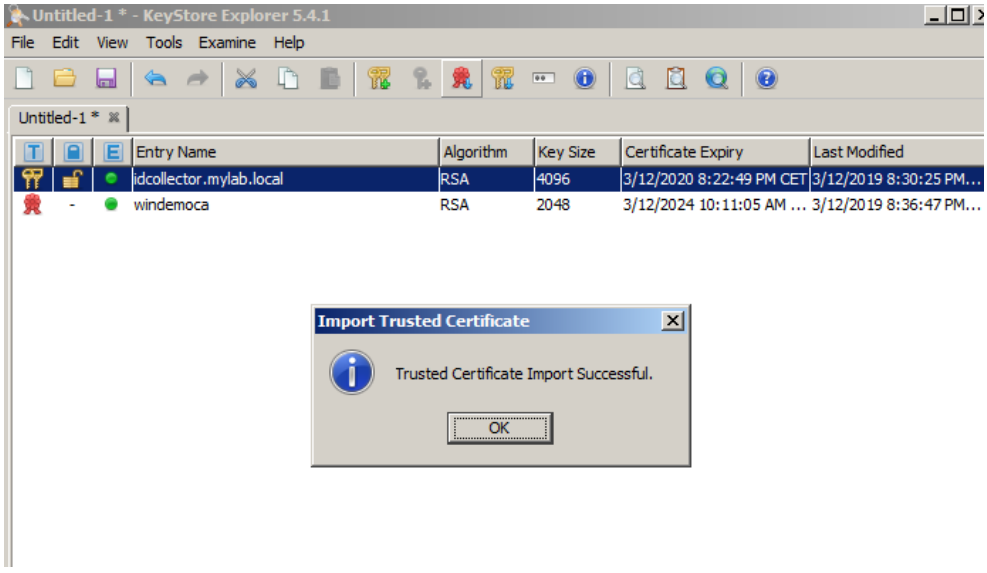
Now you need to import the root certificate from the CA that has signed the certificate for the ID Collector host end entity.



You will get prompted to accept the ‘alias’.

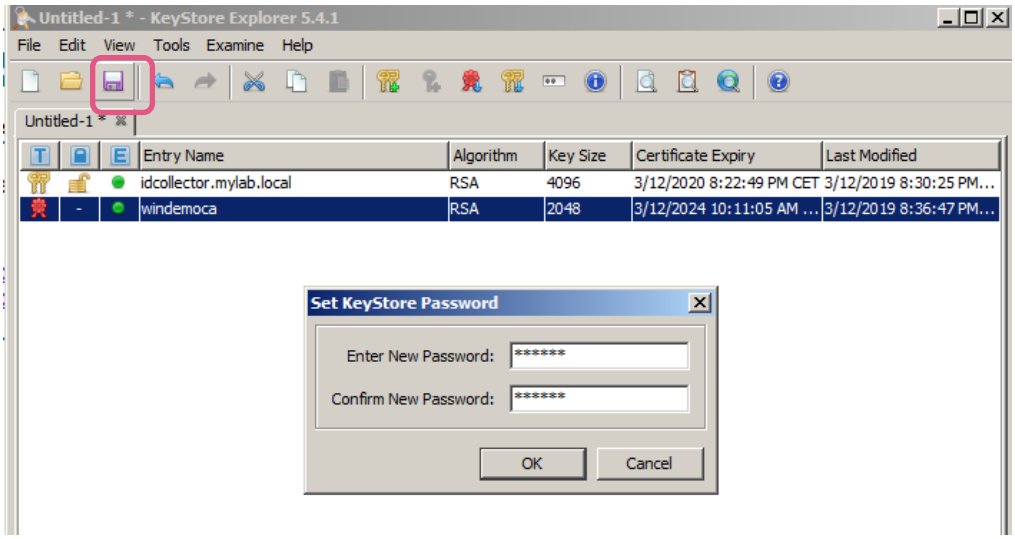


See the import was successful.

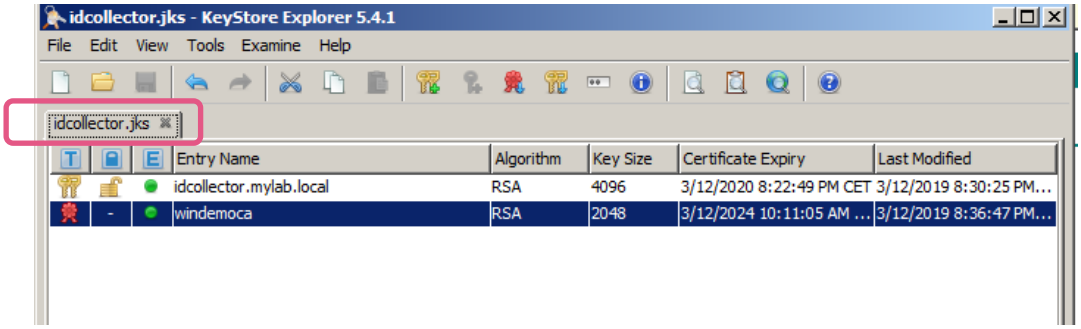


Save the Java jks key store as a file

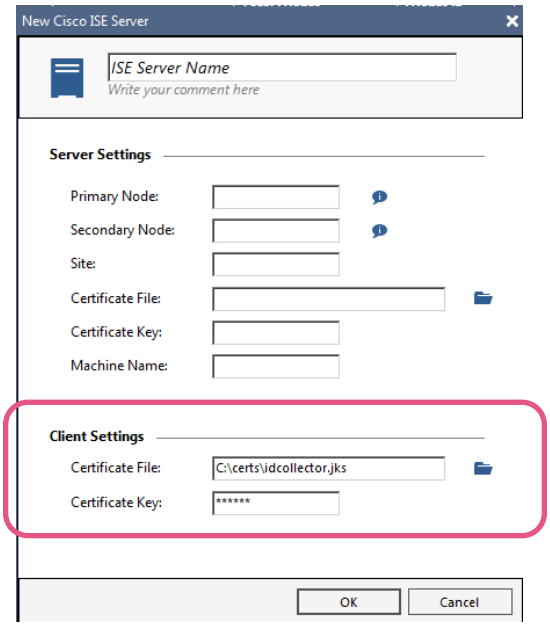
Save the Java jks key store as a file. Define an ‘easy to be remembered password’ when doing a PoC.



Once you clicked ‘ok’ and you saved the file, note that now you see a name given for the tab you are working on.



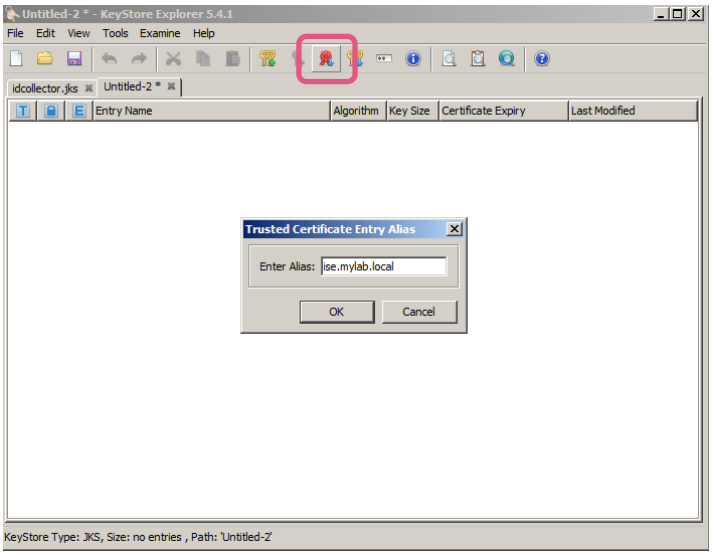
Use this file when configuring the ID collector Cisco ISE object in the ‘client settings’.



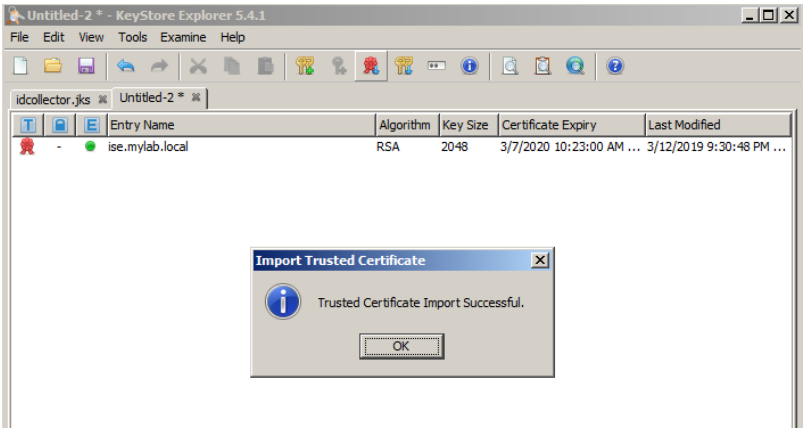
Cisco ISE Server Java Certificate Container

Create a new Java key store in jks format and import the Cisco ISE certificate

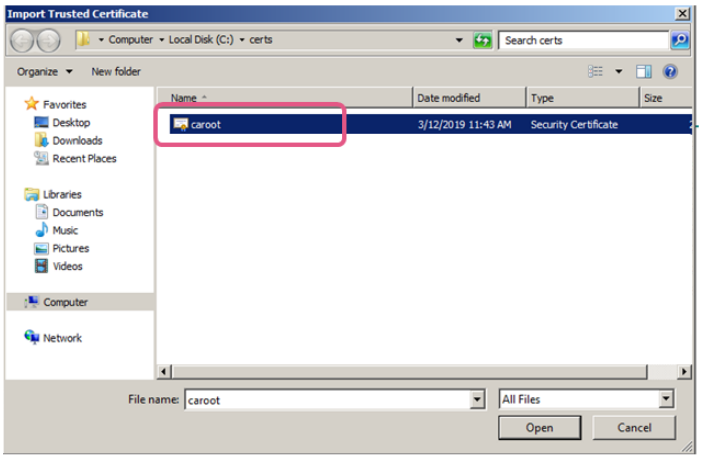
Once you have created the container import the certificate you created for the Cisco ISE earlier.



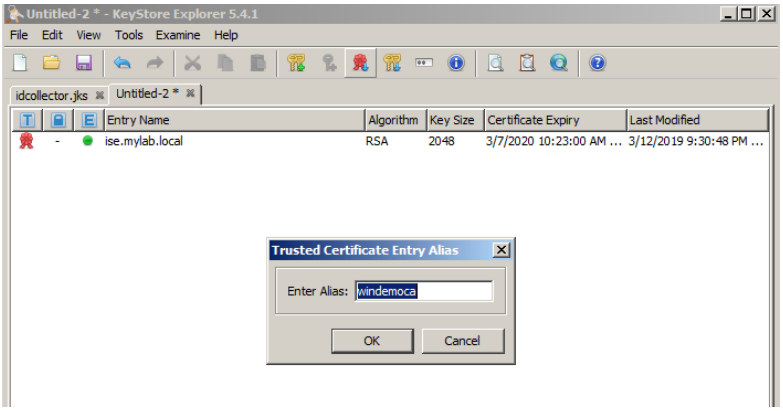
Click ‘ok’ and see the import was successful.



Import the root certificate of the CA that has issued the Cisco ISE certificate

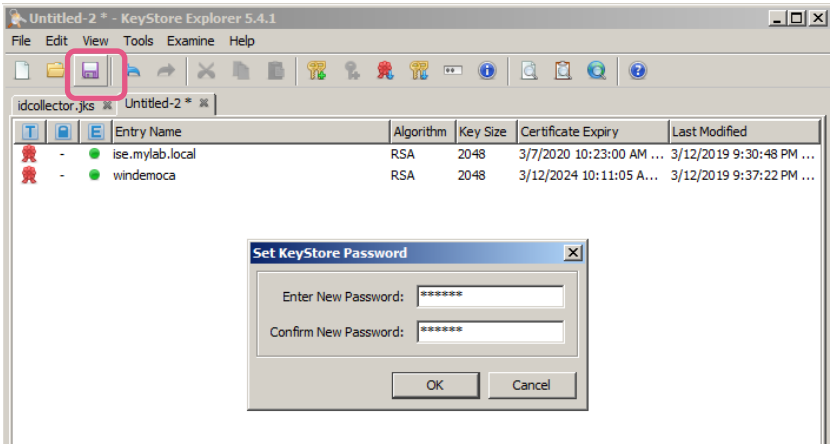


Accept the suggested alias.



Save the Server Java key store as a jks file

Use the save menu and define a password for the Java key store container.



Use this ISEserver.jks file in the ID Collector menu to configure the Server elements representing the Cisco ISE host.