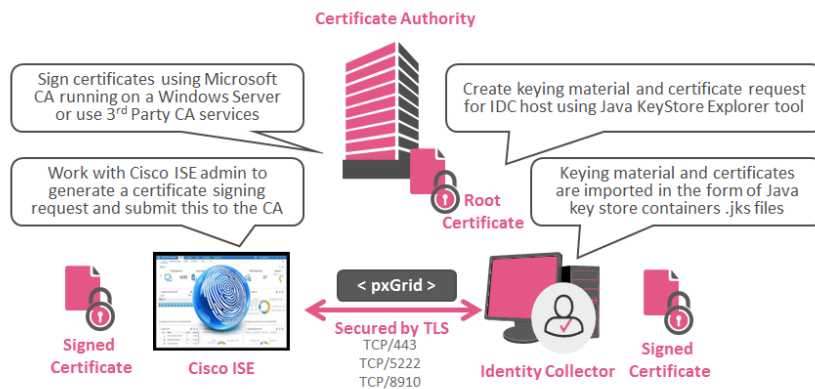


Establish trust relationship between Cisco ISE and the Identity Collector

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.

Preparing Certificate Management Tools.....	2
Create the Cisco ISE certificate for pxGrid.....	3
Sign the request coming from the Cisco ISE host on the Microsoft CA.....	3
ID Collector Client Java Certificate container	4
Create a new key store selecting jks format	4
Generate certificate signing request for the ID collector host	7
Sign the certificate request on the Microsoft CA	8
Import the signed certificate into the Java key store	10
Import the Microsoft CA root certificate into the Java key store.....	11
Save the Java jks key store as a file	13
Cisco ISE Server Java Certificate Container.....	14
Create a new Java key store in jks format and import the Cisco ISE certificate.....	14
Import the root certificate of the CA that has issued the Cisco ISE certificate	14
Save the Server Java key store as a jks file	15

Preparing Certificate Management Tools

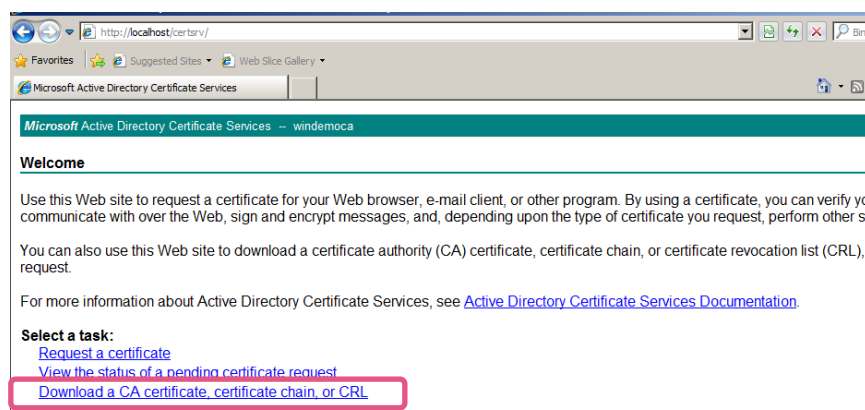
Use 'KeyStore Explorer' on Windows available at <https://keystore-explorer.org/downloads.html>. The tool is available as well for Linux computers.

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:

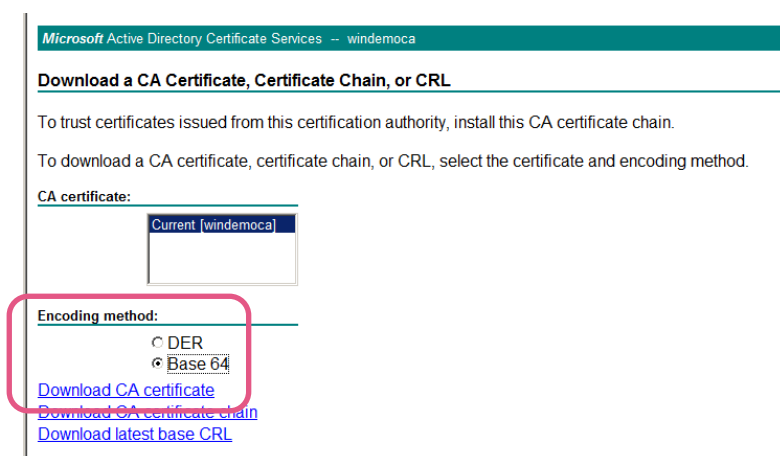
- IP addresses and FQDN of ID Collector host
- The root certificate of the CA issuing the certificates
- Access to Cisco ISE Management interface
- Ensure that Cisco ISE and ID Collector host have connectivity based on DNS name resolution and the following ports (see ID Awareness Administration Guide [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

Microsoft Active Directory Certificate Services -- windemoca

Request a Certificate

Select the certificate type:
[Web Browser Certificate](#)
[E-Mail Protection Certificate](#)

Or, submit **an advanced certificate request.**

Microsoft Active Directory Certificate Services -- windemoca

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:
[Create and submit a request to this CA.](#)
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Paste the base64 encoded text and 'submit'.

Microsoft Active Directory Certificate Services -- windemoca

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS # (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

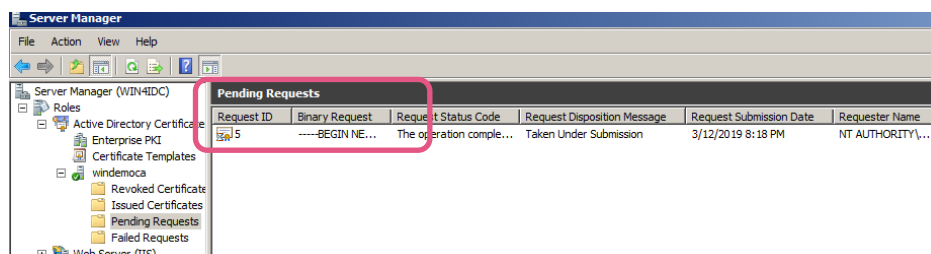
```
1dcHWa11kSaaCv1gX3vp3eQcS1yDGLvGMK5Fx3JY  
wtQs1iJDvFP2Tnxm1cXRBDPLCNfk7EZ25g2ub1ed  
0fIn82J3s6phqarE93ktZecoe5PKu78gnzUkwz0+  
Uq010/us3X9XtehVIYSVzHvHN7As37qrB3JTBea2v  
2iLJyOWP6w4KBg==  
-----END CERTIFICATE-----
```

Additional Attributes:

Attributes:

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.

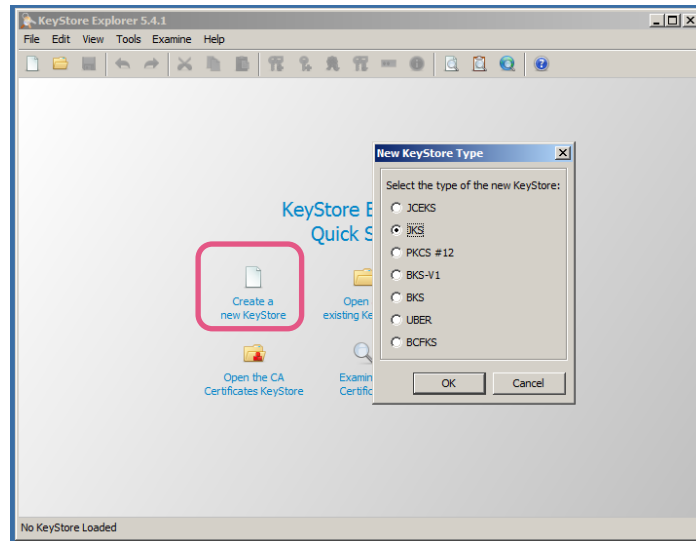
Pass the certificate and the root CA certificate to the Cisco ISE administrator and install them.

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

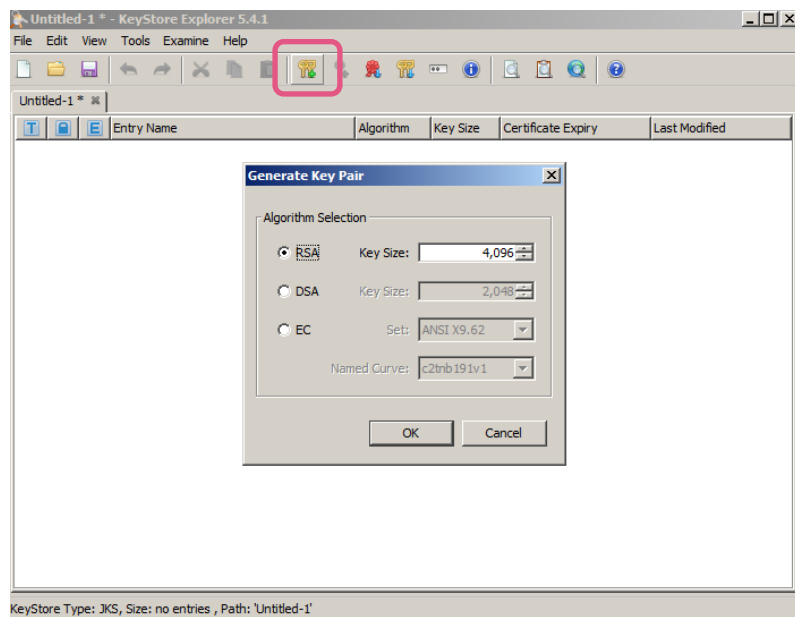
ID Collector Client Java Certificate container

Create a new key store selecting jks format

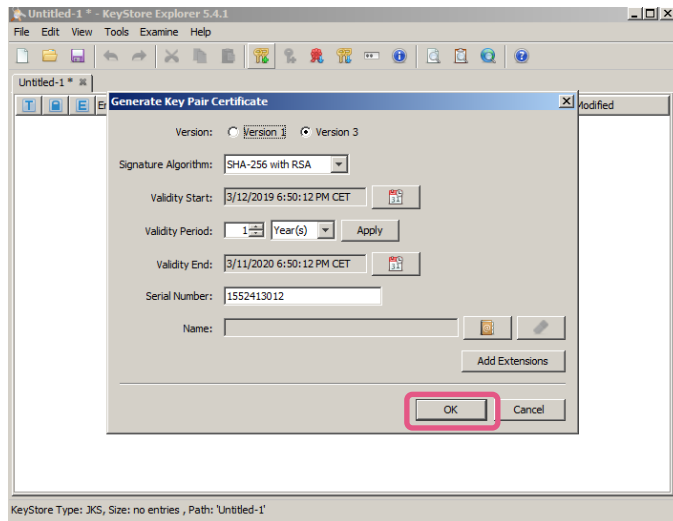
Start 'KeyStore Explorer' and select 'create a new key store'.



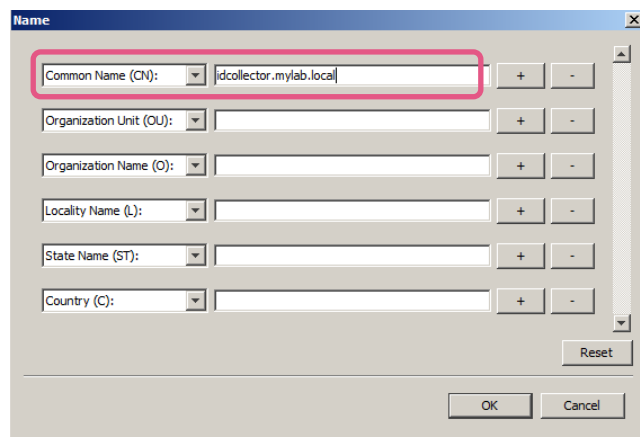
Generate a new private public key pair for the host of the ID Collector (key size should be 4096)



You will see this window.



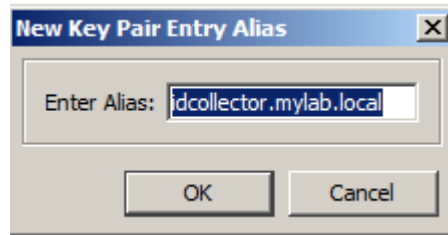
Define a name. The name will become the subject field of the certificate. All other fields can remain empty.



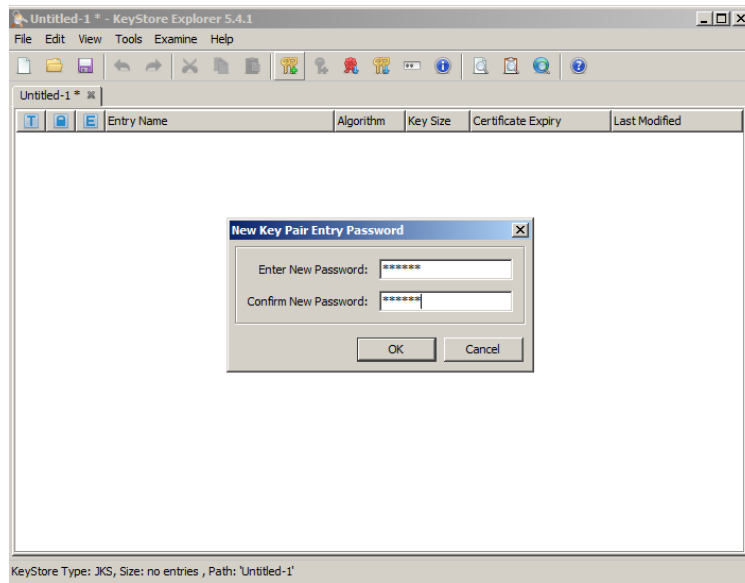
Once you clicked 'ok' you will see the 'name' field populated.



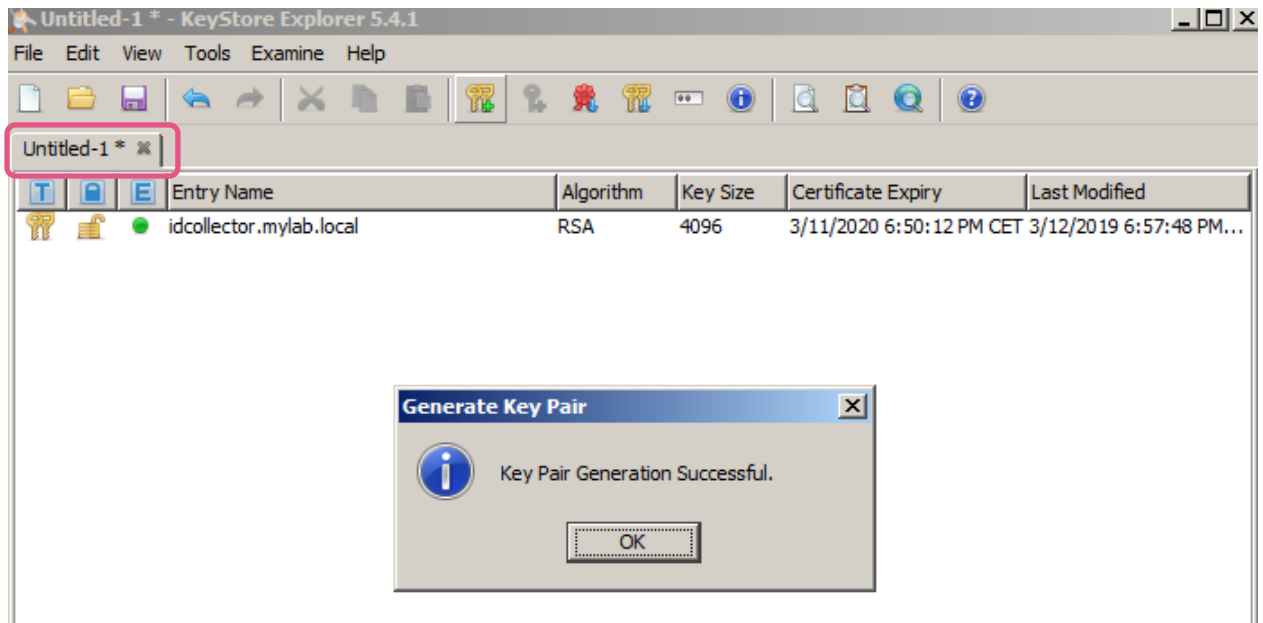
Click 'ok' and see the alias for this key pair.



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.

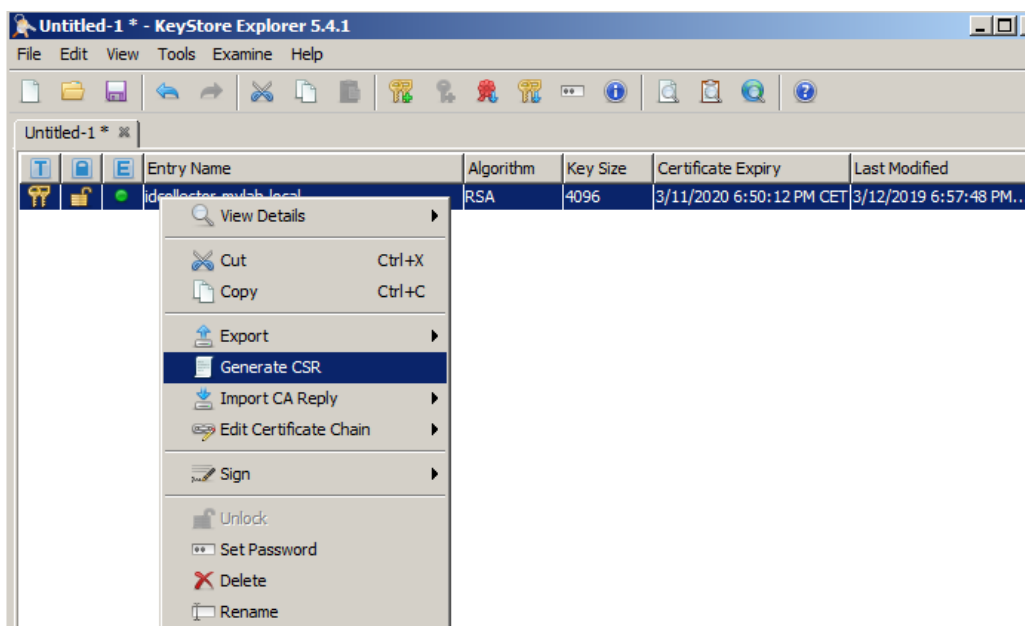


Click 'ok' and see that you have generated a private public key pair that can be used to request a certificate. Note the name of the jks object is still 'untitled'.

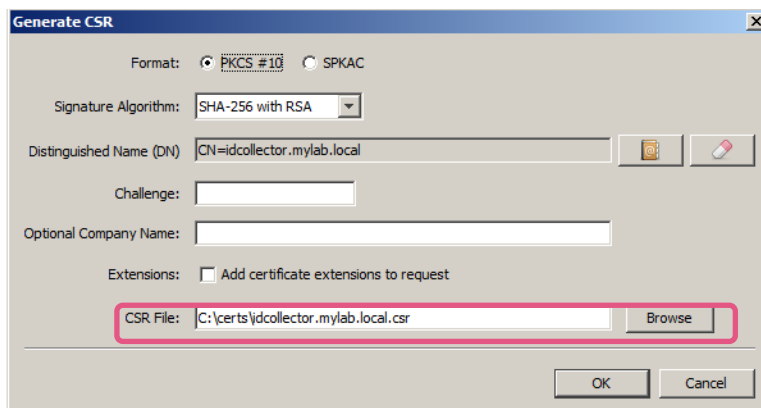


Generate certificate signing request for the ID collector host

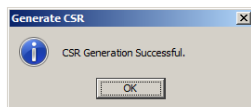
Select the key pair, click right and execute the 'Generate CSR' dialog.



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.



idcollector.mylab.local.csr

3/12/2019 7:10 PM

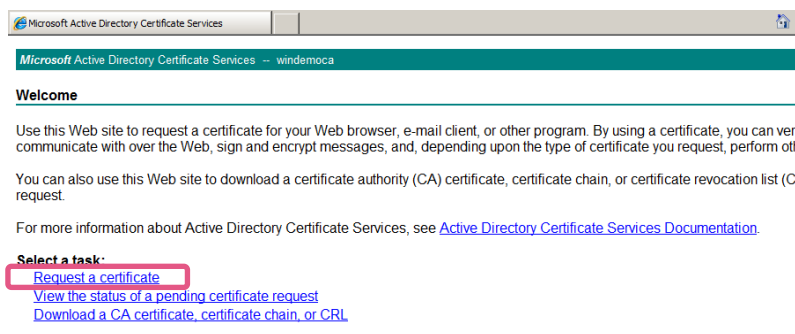
CSR File

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

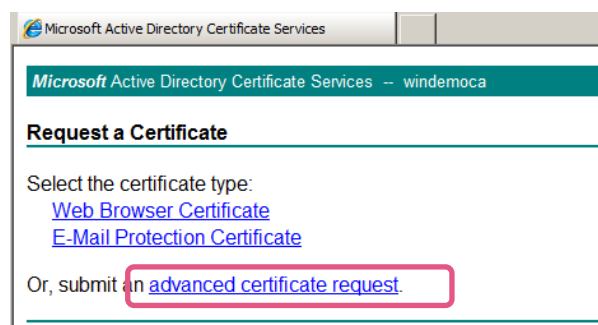
```
1 -----BEGIN CERTIFICATE REQUEST-----
2 MIIEZzCCAk8CAQAwIjEgMB4GA1UEAwXaWRjb2xsZWNoY3IubXlsYWUubG9jYWwggIiMA0GCSqG
3 SIb3DQEBAQUAA4ICDwAwggIKAoICAQC/SjTkPQkwDnJVLmtespsF5x66SO4nxin+Ep53GrtXaPqT
4 6uD7SeH6nu8MG/i5tgcdujO92Zs2iIisWLoYAhB6dwKtJDmczqtB+518xAHS5f5ki1cavO3Ql9cp
5 vFW8zSowNVxf68ad7O3B1lnQhpAKgC5H/GJ1dONsrekjOwwNDW/5AoJb+B0Bm+B6ktLzUVdBCBI
6 chzcJka7N8ViyO6xUSMkWF6jhyzPsfaf2U3ncxJyGR9z99YI+5bSGArHXZNhp3rcN/Xuo4f0pj6rM
7 kN+PwAuInMgJgJyM7GgHqT8NhTtz3ZWAvtv6UFE1g1aA4WumtTQgJy46KiCzFam8HoXIHHZutF4My
8 2mILL8ovWn1Bk7uyxPkiIesxpBKf97PeeDFfG3HRaB/XUDmHV5LSGatm5a7uOWLwY5Q5VFzCPT7V
9 8jpUlKAbc5fDYXX1DLaBJ1TLvFyrSP6dAHBCX2qWWH7Fjw+mHshn3rx16mR5VvSh3ScDZ4UVkyq
10 Tb51deAy5vUq5LTZQzfnUY7tc4Z6MWjVkmNm6f0V5AzCosY4IW8EKkWLzRoTtvb7H6cMwL+haWQU
11 aZapAEJk3at7XCgtIM2X5JwTRJdcUoi3oiDyolm80yOCW8ASot0dXiXQPDSXkC4HWC0rATDvXND
12 H+9Mh5AAp1g1rURq7X8MRSz4VStfVQIDAQABoAAwDQYJKoZIhvcNAQELBQADggIBALdI8FCnZJ/Z
13 SjBhuTF7qncyOypdO88GcJo1DAmYkc37nEJLfbalvKAXGQBxxkyCEJOJLgfmf+kJf4V9Xbd4tmX
14 FAiqhS1RC8TZQVBWmxRW8MUGZUPy6Am9RESjPw1KjMtYGRPtizHdWMm+AxGUXW2mT43Zvzidta6N
15 Waz2fvB6at/s+DXA8vUjE+YX6Ji4xiB0LvkJ3sIQn9oXOVWWHBA4qf46IgdBsYm/9m+cCgULXRfc
16 UYJQW20cgIP0ecSw+44ZKxOUa1o0g6d55mtIqZiu5AxKAd8PyX1SjGWzsXG4diuY7AxxKO4/0Am/
17 ST40z+yXL2jjJ1+y0tQPRb15TJnqFdgPawQ3cJn6vB1ISPWO6zFELbMkU6LwUjKfI1u1Zu9WTsv5
18 rIJCw7Nw1JyQ2+XTKx5X94yJp8Nf5irZEGEAftFcOZJrJBU15vNwOH2Z36d69VSKakcw+gyo3b0
19 9SYRhd+rHpJ051Zfye1tZ8FNCLwe4jkCA62o/Jlg/1VpUDZn610aEB/ABFFU1FJkNxt1hOclYlah
20 RQR/JmO1CfTW5up/AMXLJTz0YrKK+FEqSNdWfYjsYDBC4TAaN6fCjE3fijwr19gha2sVSVgL41v
21 rQY+kIawegSYoxkwU2bQh5ey/8j8Lk71oduBJ6SN5NLoMaxFbEgObwZgFcIN07wh
22 -----END CERTIFICATE REQUEST-----
23
```

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'.



Microsoft Active Directory Certificate Services -- windemoca

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

[Create and submit a request to this CA.](#)

[Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.](#)

Paste the text and 'submit'.

Microsoft Active Directory Certificate Services -- windemoca

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PK (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
zIJcWz7Nw1JyQ2+XTKx5X94yJp8Nf5ir2EgEAFtF
9SYRhd+rHpJO51Zfyet28FNCLwe4jkCA62o/Jlg
RQR/JmO1CfTW5up/AMXLJTzd0YrKK+FEqSNdWfYj
zQY+kIawegSYoxkwU2bQh5ey/8j8Lk71oduBJ6SN
-----END CERTIFICATE REQUEST-----
```

Additional Attributes:

Attributes:

Submit >

Recall the certificate request ID – here '5'.

Microsoft Active Directory Certificate Services -- windemoca

Certificate Pending

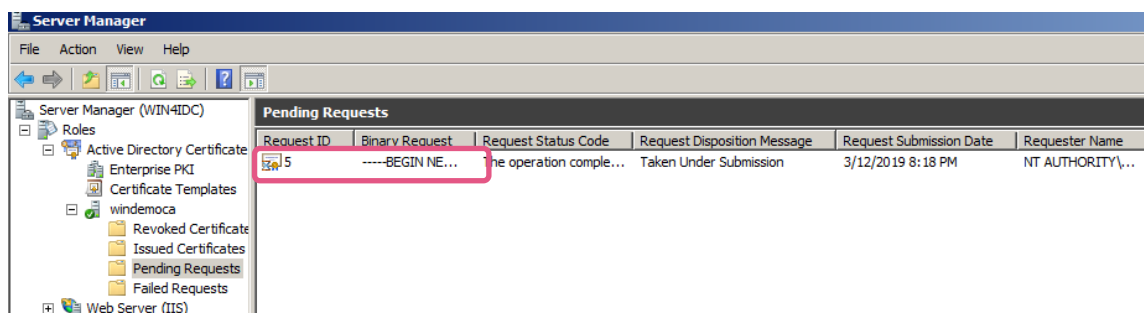
Your certificate request has been received. However, you must wait for an adm

Your Request Id is 5.

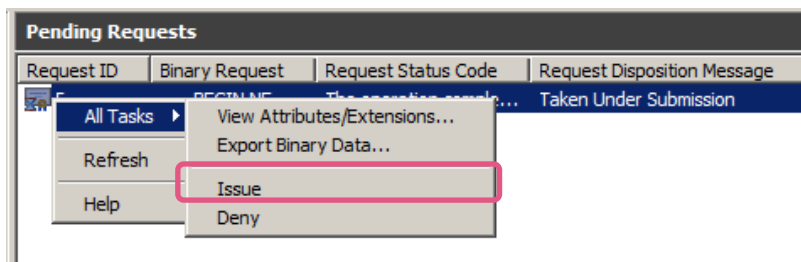
Please return to this web site in a day or two to retrieve your certificate.

Note: You must return with **this** web browser within 10 days to retrieve your certificate

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.

Microsoft Active Directory Certificate Services - windemoca

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

View the Status of a Pending Certificate Request

Select the certificate request you want to view:

[Saved-Request Certificate \(Tuesday March 12 2019 10:46:42 AM\)](#)

[Saved-Request Certificate \(Tuesday March 12 2019 8:18:18 PM\)](#)

Download the certificate in Base64 format.

Microsoft Active Directory Certificate Services - windemoca

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded

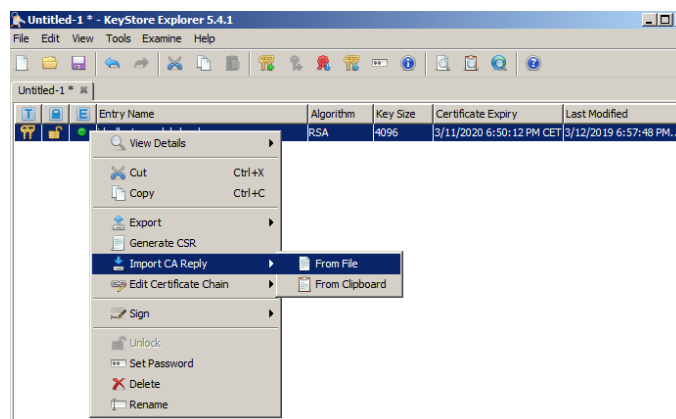
[Download certificate](#)

[Download certificate chain](#)

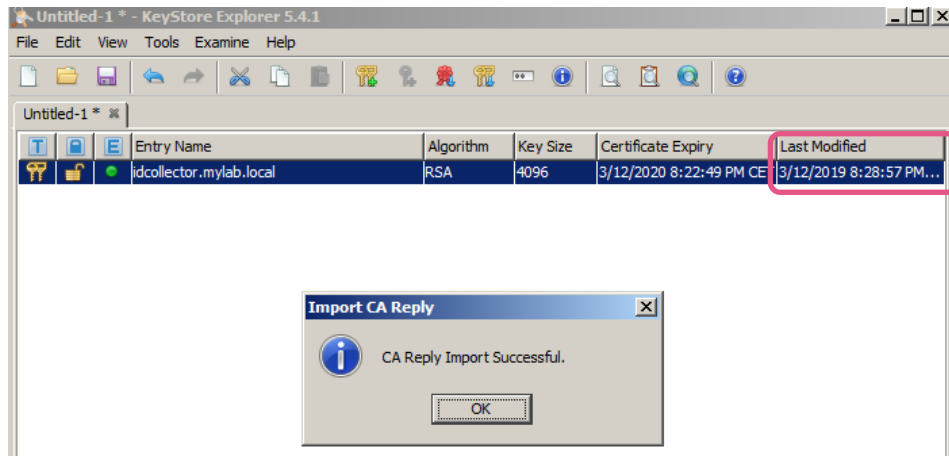
Save the file. You don't need the certificate chain.

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.



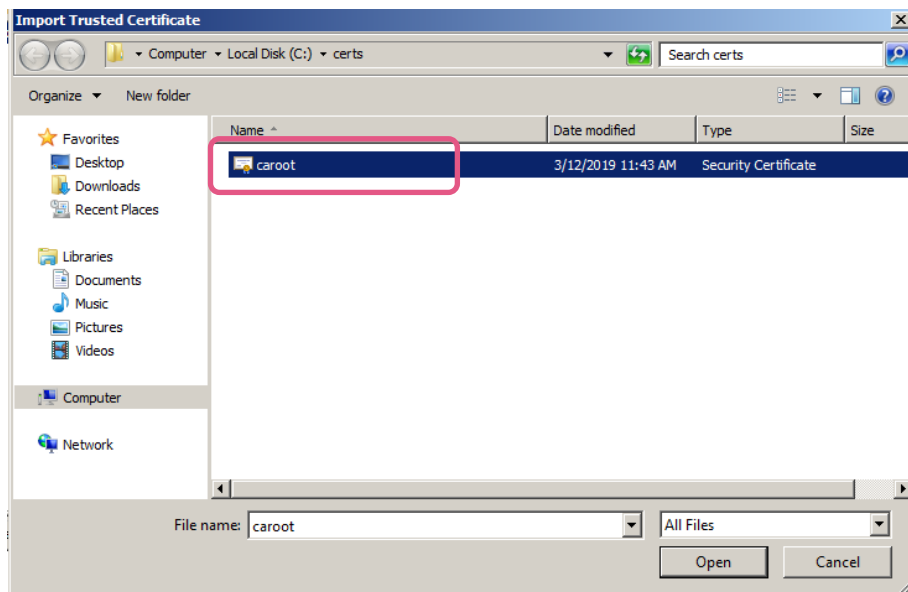
Import the file and click 'ok'.



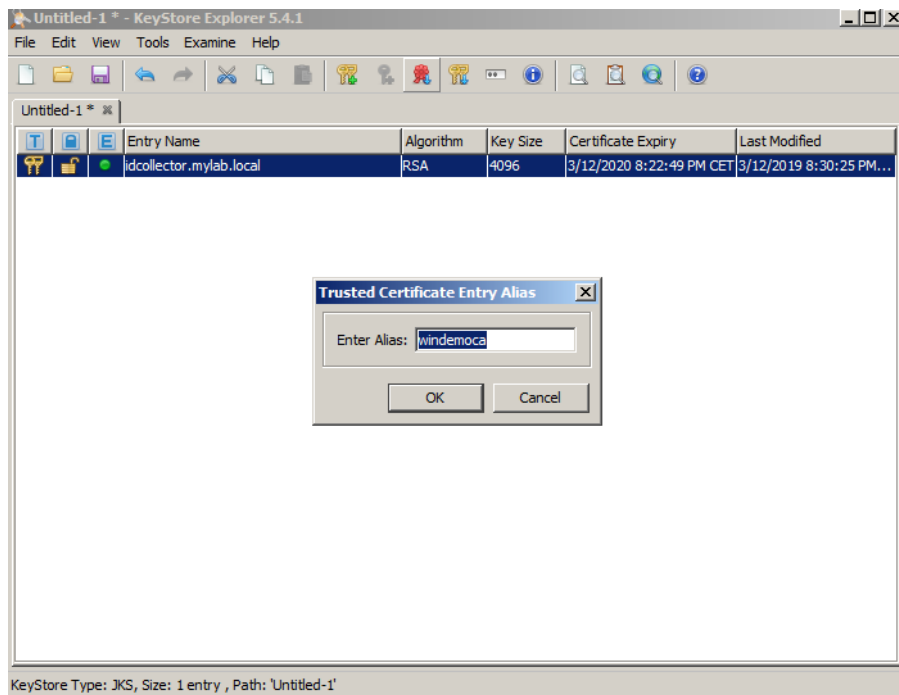
You will see the 'last modified' information changed.

Import the Microsoft CA root certificate into the Java key store

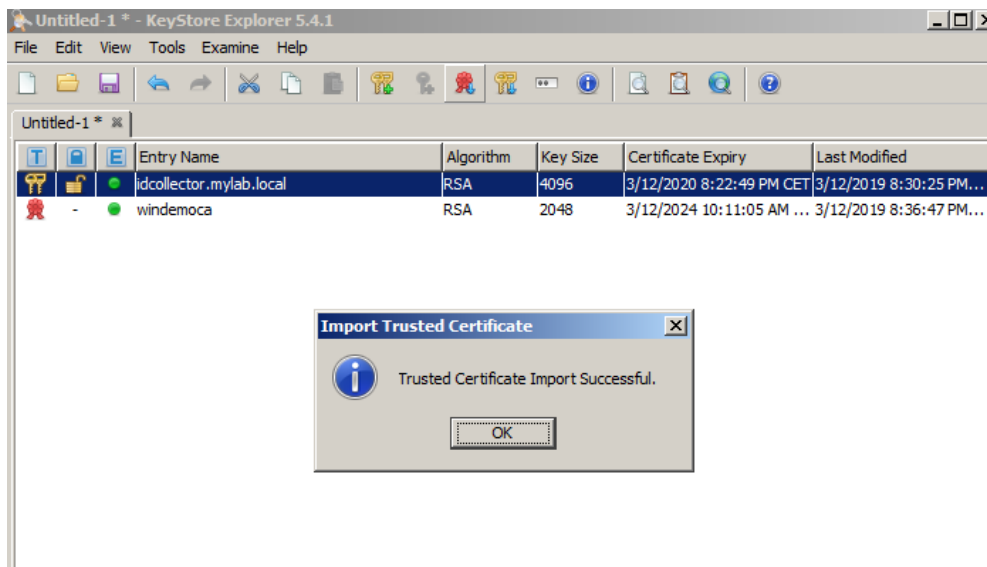
Now you need to import the root certificate from the CA that has signed the certificate for the ID Collector host end entity.



You will get prompted to accept the 'alias'.

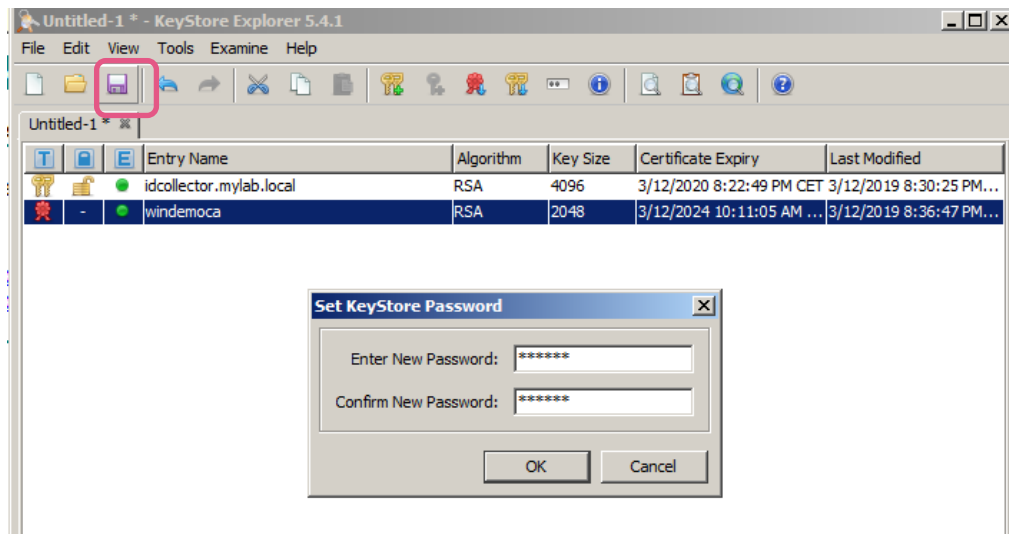


See the import was successful.

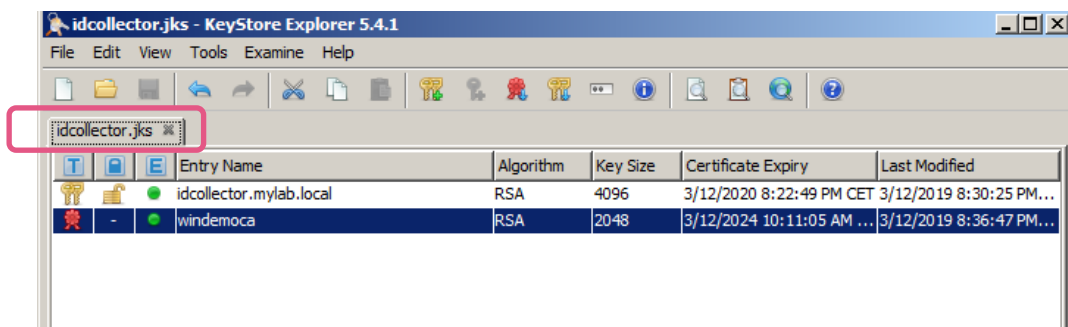


Save the Java jks key store as a file

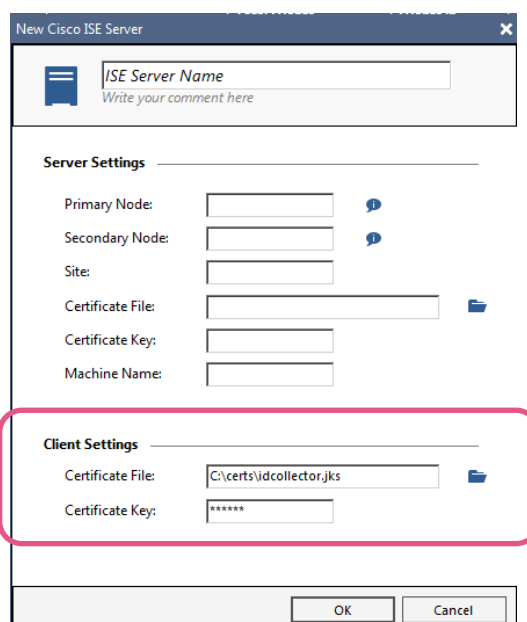
Save the Java jks key store as a file. Define an 'easy to be remembered password' when doing a PoC.



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



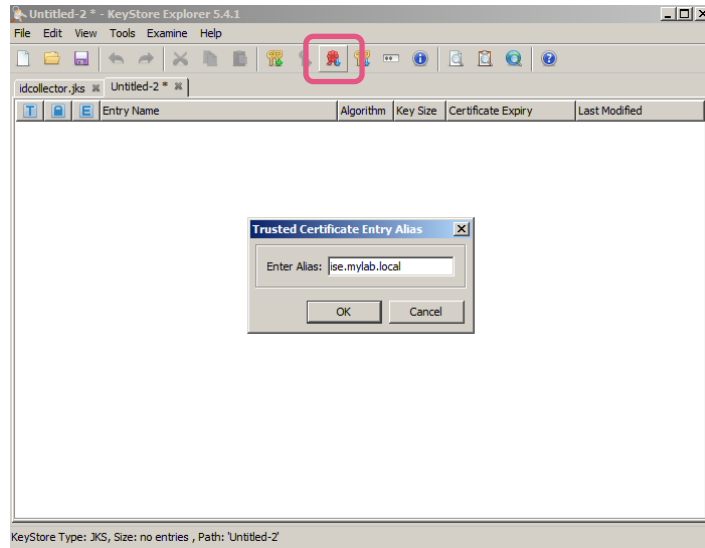
Use this file when configuring the ID collector Cisco ISE object in the 'client settings'.



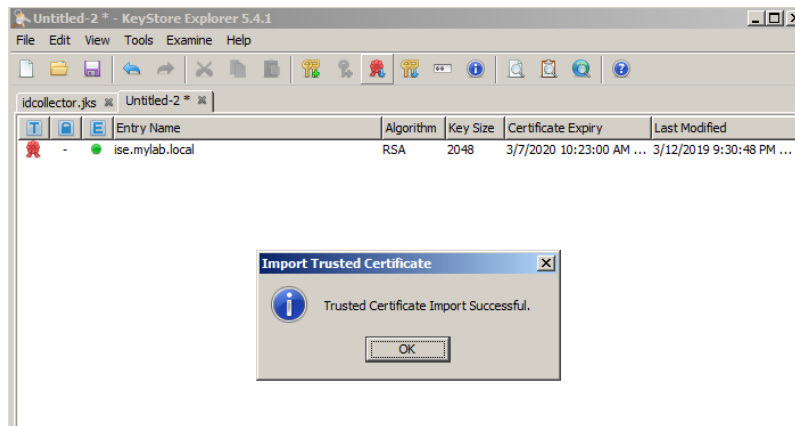
Cisco ISE Server Java Certificate Container

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

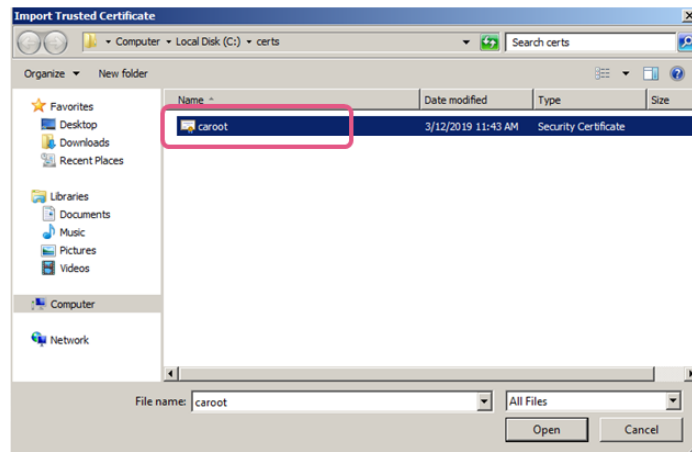
Once you have created the container import the certificate you created for the Cisco ISE earlier.



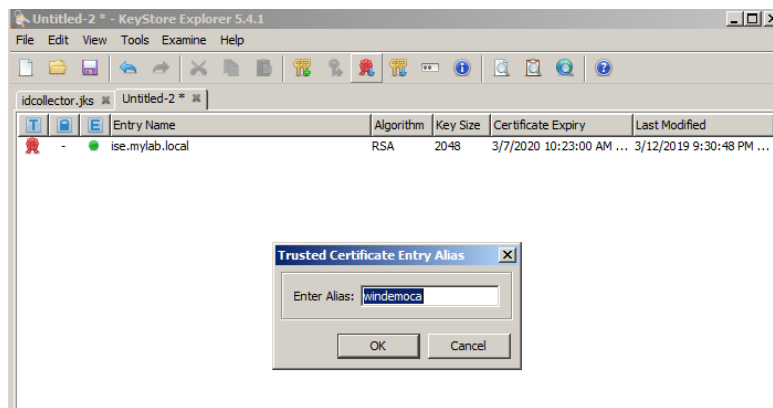
Click 'ok' and see the import was successful.



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

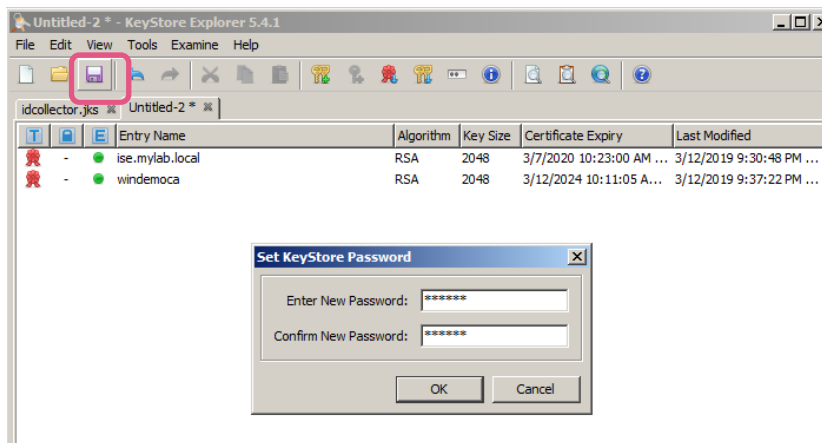


Accept the suggested alias.



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.

