

Resolving the certificate error message

i There are multiple ways for you to create a self-signed certificate. The steps in this topic include KeyStore Explorer, a free third-party utility. This product is not supported by IDERA and is only an example.

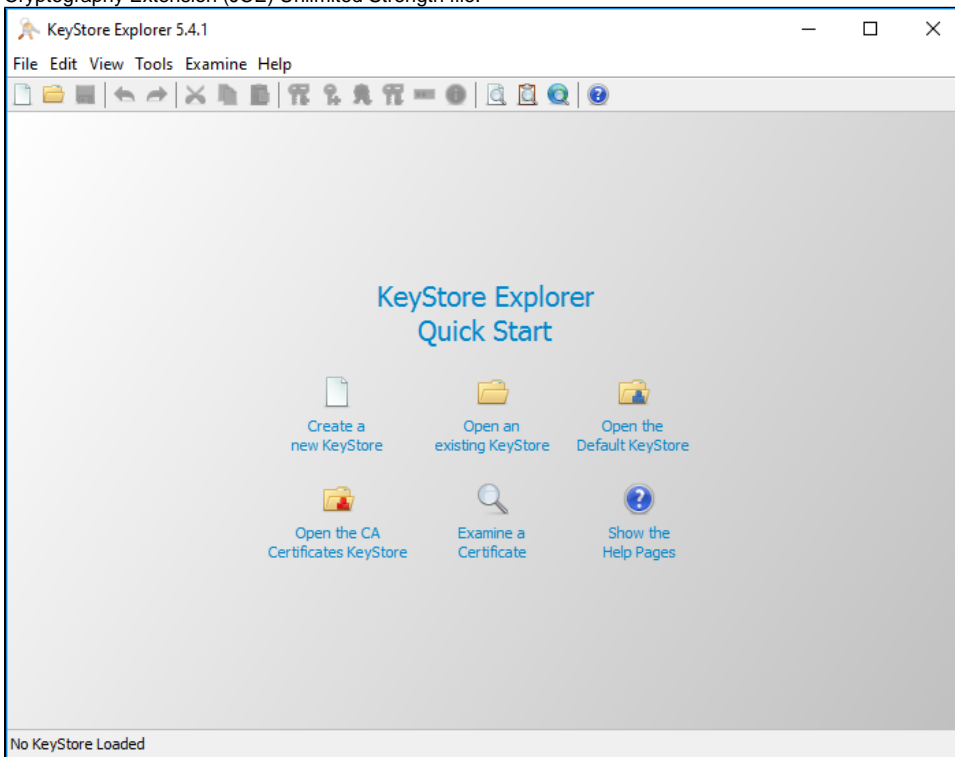
i IDERA Dashboard must be installed prior to performing this task.

IDERA users in environments that have not yet added a certificate signed by a Certification Authority (CA) receive a warning message in their browser each time they attempt to open the SSL version of the IDERA Dashboard. Note that the default certificate provided with an IDERA product **is not signed by any well-known CA and is intended only for use in testing purposes ONLY**. You can resolve this issue by adding a signed CA using the steps provided in [Run IDERA Dashboard over TLS \(HTTPS\)](#), or you can use the following steps to resolve this issue at no certificate cost.

Adding a self-signed certificate

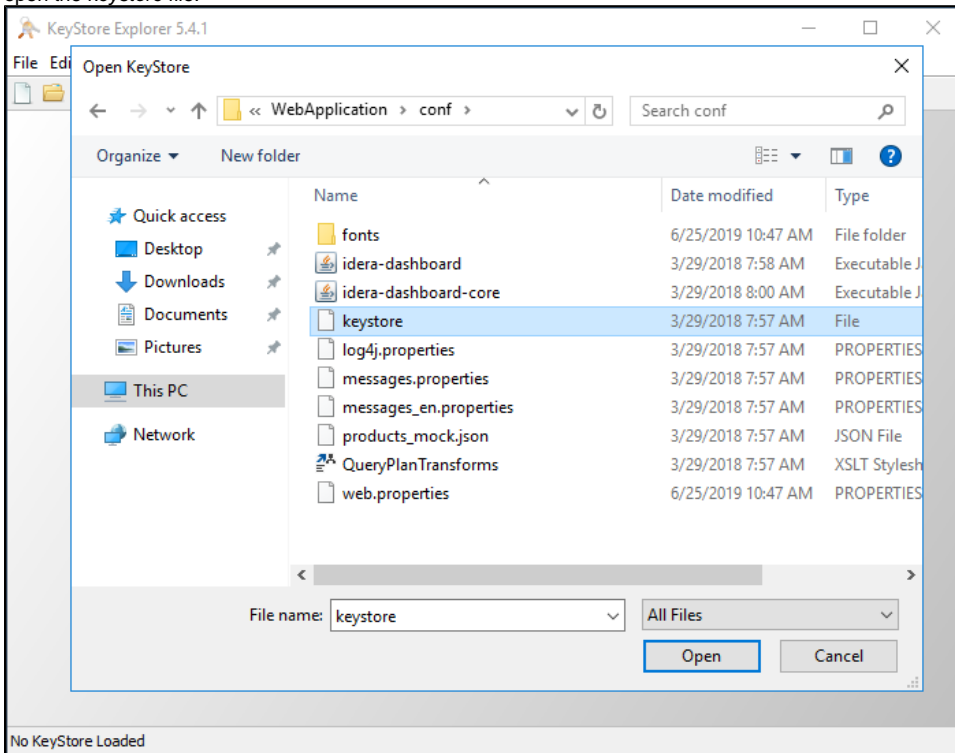
Creating a Certificate

1. Download the free KeyStore Explorer utility from <http://keystore-explorer.sourceforge.net/> and install it.
2. Open KeyStore Explorer. KeyStore Explorer displays the following Quick Start options. On launch, it may ask you to download an updated Java Cryptography Extension (JCE) Unlimited Strength file.

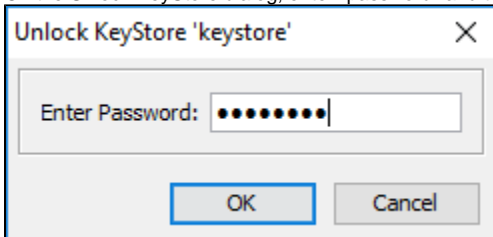


3. Click **Open an existing KeyStore**.

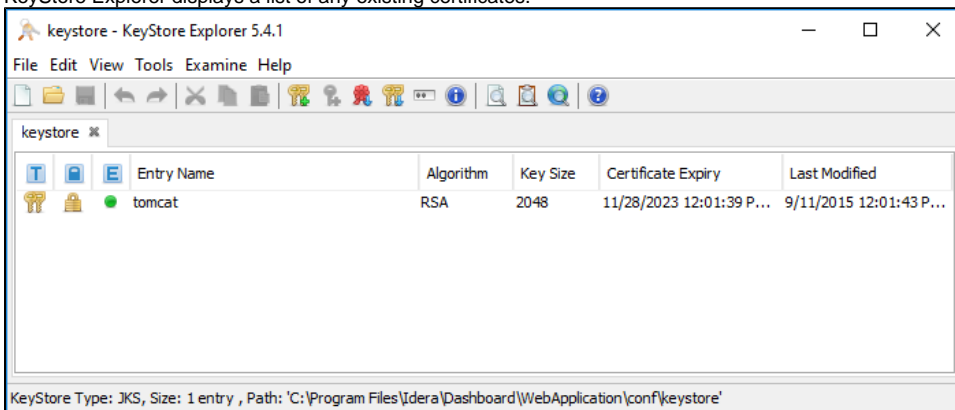
4. Browse to the IDERA Dashboard *conf* directory, the default path is `C:\Program Files\Idera\Dashboard\WebApplication\conf` , and open the *keystore* file.



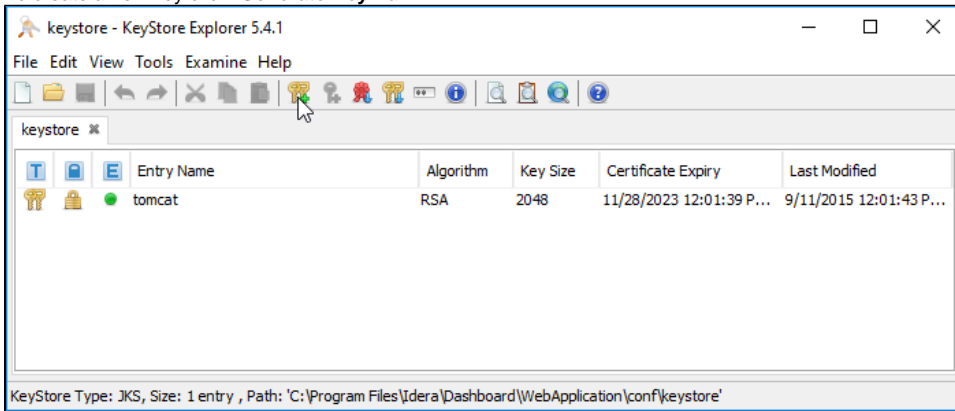
5. On the Unlock KeyStore dialog, enter "password" and then click **OK**.



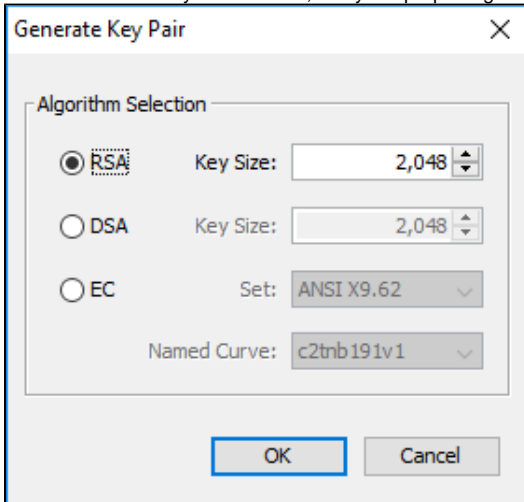
KeyStore Explorer displays a list of any existing certificates.



6. To create a new key click **Generate Key Pair**.

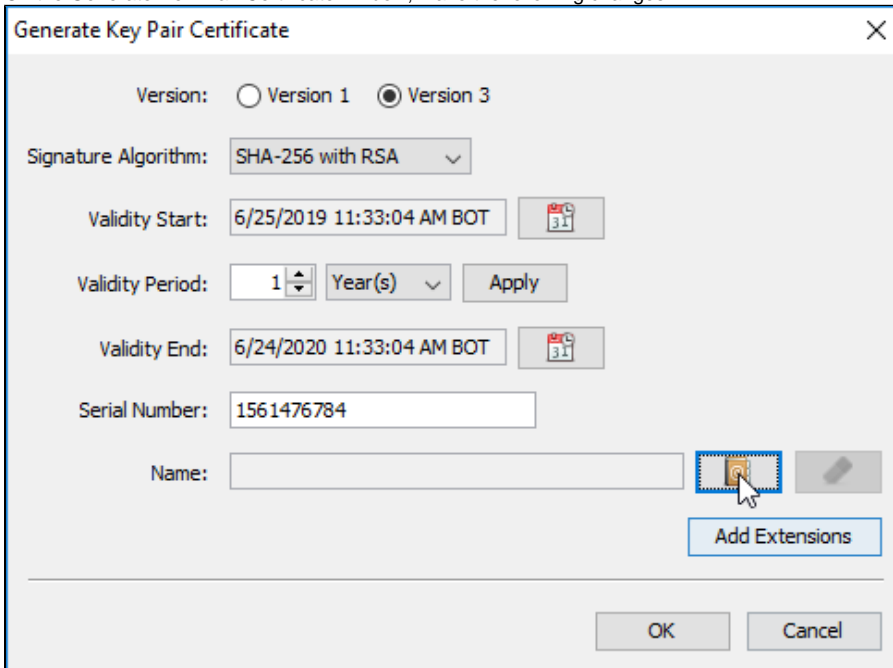


7. On the Generate Key Pair window, verify the proper algorithm is selected, and then click **OK**.



KeyStore Explorer begins to generate a new key pair

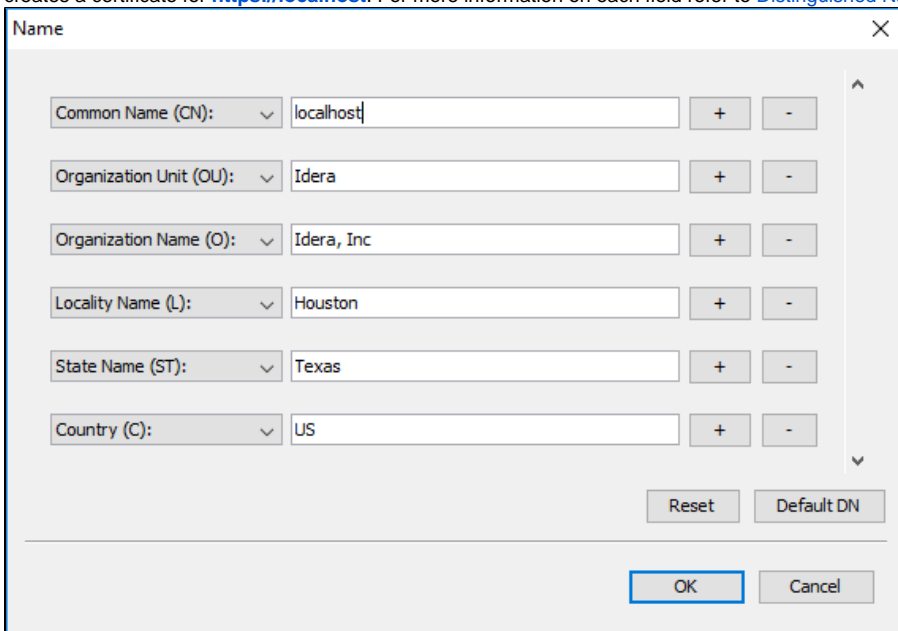
8. On the Generate New Pair Certificate window, make the following changes:



- In the **Signature Algorithm** list, select **SHA-1 with RSA** or **SHA-256 with RSA**. This example uses **SHA-1 with RSA**.
- In the **Validity Period** field set the number of years the certificate is valid, this example uses 5 years, and click **Apply**.
- Click the **Edit Name** button to open the **Name** window.

9. On the **Name** window Click the **Edit Name** icon to enter identifying information. In the Name dialog, complete each of the available fields. The entry in the **Common Name (CN)** field should correlate with the name of the website.

In essence, the name that you provide should match the URL that you intend to use. For example, the following image shows an entry that creates a certificate for <https://localhost>. For more information on each field refer to [Distinguished Name Fields](#)



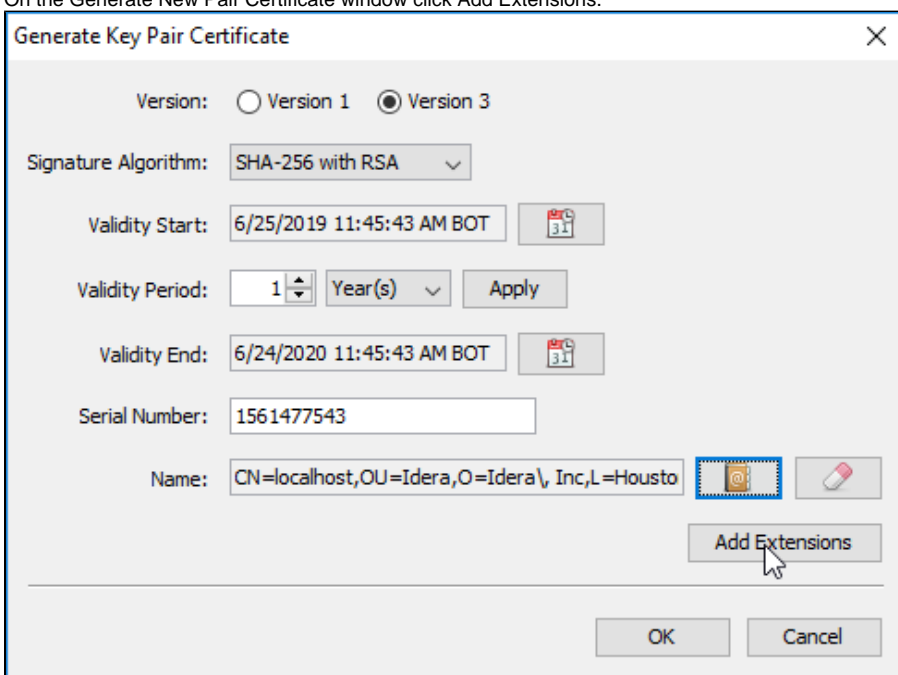
A dialog box titled "Name" with a close button (X) in the top right corner. It contains several fields for a Distinguished Name (DN):

- Common Name (CN): localhost
- Organization Unit (OU): Idera
- Organization Name (O): Idera, Inc
- Locality Name (L): Houston
- State Name (ST): Texas
- Country (C): US

Each field has a dropdown arrow on the left and plus/minus buttons on the right. At the bottom right, there are "Reset" and "Default DN" buttons. At the bottom center, there are "OK" and "Cancel" buttons.

Once you fill your information click **OK**.

10. On the Generate New Pair Certificate window click Add Extensions.

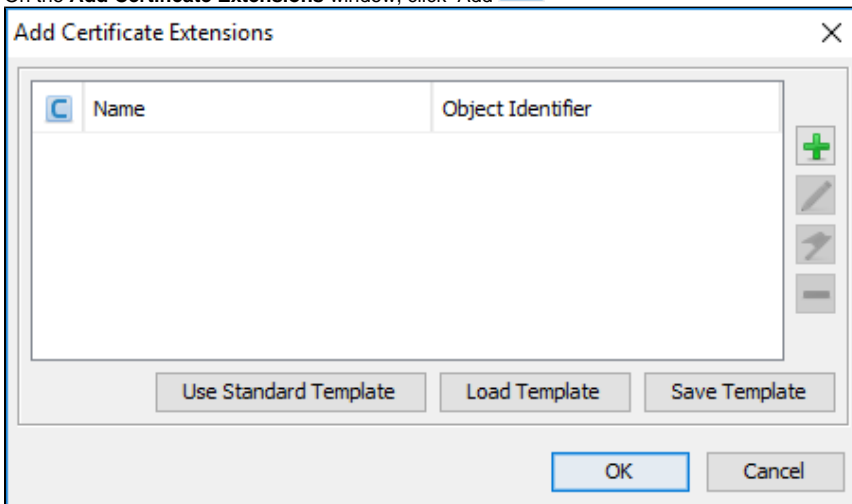


A dialog box titled "Generate Key Pair Certificate" with a close button (X) in the top right corner. It contains the following fields and controls:

- Version: ☐ Version 1 ☒ Version 3
- Signature Algorithm: SHA-256 with RSA
- Validity Start: 6/25/2019 11:45:43 AM BOT
- Validity Period: 1 Year(s) Apply
- Validity End: 6/24/2020 11:45:43 AM BOT
- Serial Number: 1561477543
- Name: CN=localhost,OU=Idera,O=Idera, Inc,L=Houston

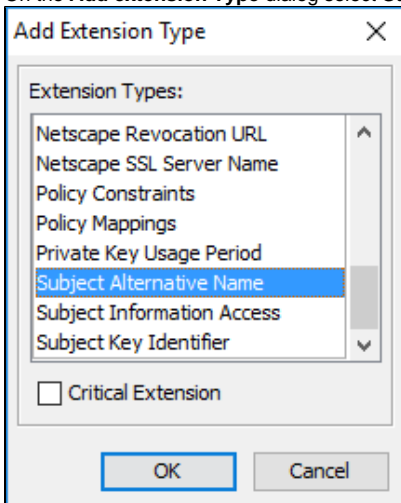
At the bottom right, there is an "Add Extensions" button with a mouse cursor pointing to it. At the bottom center, there are "OK" and "Cancel" buttons.

11. On the **Add Certificate Extensions** window, click Add 



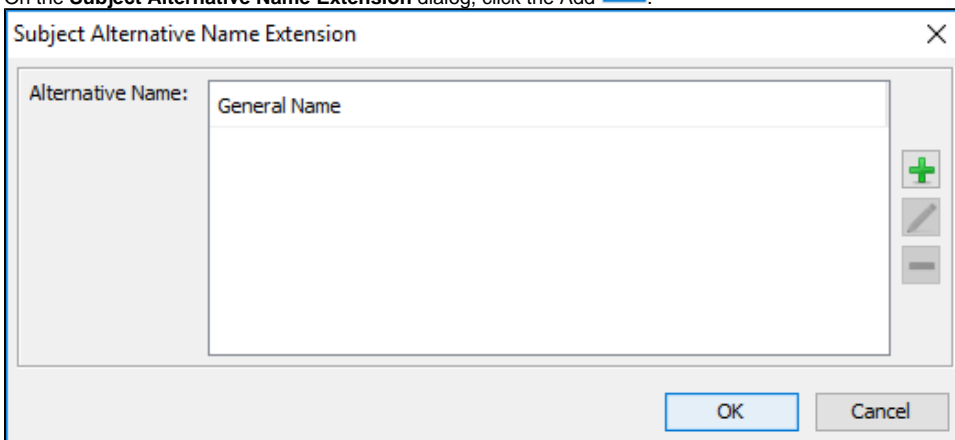
The **Add Certificate Extensions** dialog box features a table with two columns: **Name** and **Object Identifier**. The table is currently empty. To the right of the table are three icons: a green plus sign for adding, a pencil for editing, and a minus sign for deleting. Below the table are three buttons: **Use Standard Template**, **Load Template**, and **Save Template**. At the bottom right are **OK** and **Cancel** buttons.

12. On the **Add extension Type** dialog select **Subject Alternative Name** and click **OK**.



The **Add Extension Type** dialog box contains a list box titled **Extension Types:** with the following items: Netscape Revocation URL, Netscape SSL Server Name, Policy Constraints, Policy Mappings, Private Key Usage Period, **Subject Alternative Name** (highlighted), Subject Information Access, and Subject Key Identifier. Below the list box is an unchecked checkbox labeled **Critical Extension**. At the bottom are **OK** and **Cancel** buttons.

13. On the **Subject Alternative Name Extension** dialog, click the Add .



The **Subject Alternative Name Extension** dialog box has a label **Alternative Name:** next to a text field containing **General Name**. To the right of the text field are three icons: a green plus sign for adding, a pencil for editing, and a minus sign for deleting. At the bottom are **OK** and **Cancel** buttons.

14. On the **Alternative Name** dialog, select **DNS Name**. In the **General Name Value** field, enter the Fully Qualified Domain Name of the server on which the IDERA Dashboard exists. Click **OK** on all windows to save your changes.

Alternative Name [X]

General Name Type:

☐ Directory Name
 ☒ **DNS Name**
☐ IP Address
 ☐ Registered ID

☐ RFC 822 Name
 ☐ URI
 ☐ UPN

General Name Value:

OK Cancel

15. On the New Key Pair Entry Alias dialog, verify that the displayed alias matches the name of your website and then click **OK**.

New Key Pair Entry Alias [X]

Enter Alias:

OK Cancel

16. KeyStore Explorer displays the New Key Pair Entry Password window. Type and confirm the password you want to use for the key pair, and then click **OK**.



This password must match the password entered in step 5.

In this case, type the following password in both input boxes:
password

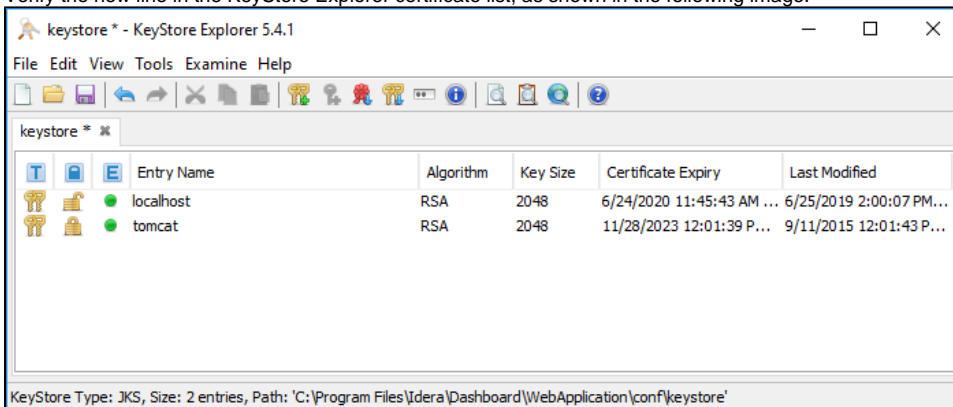
New Key Pair Entry Password [X]

Enter New Password:

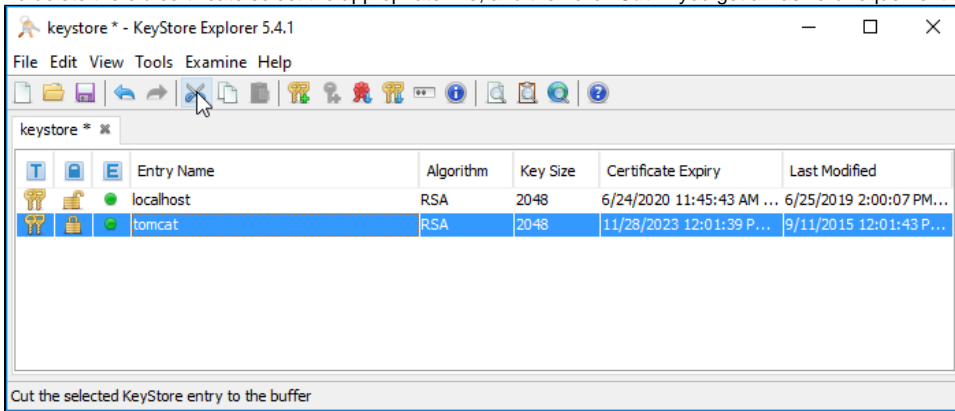
Confirm New Password:

OK Cancel

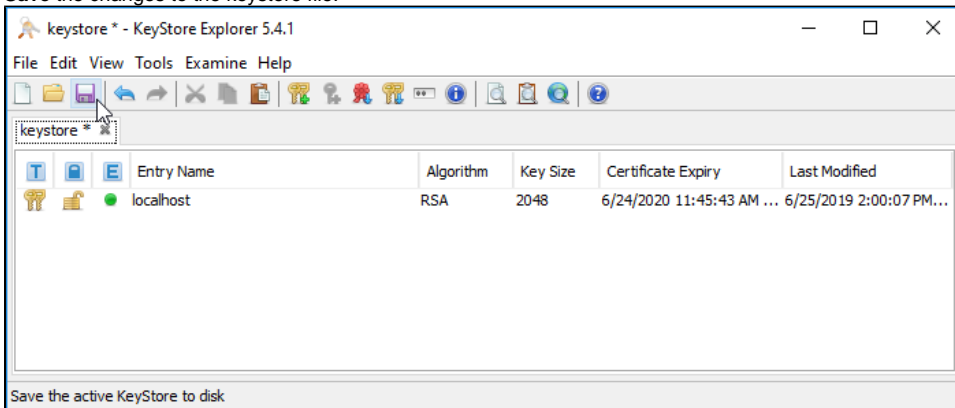
17. Verify the new line in the KeyStore Explorer certificate list, as shown in the following image.



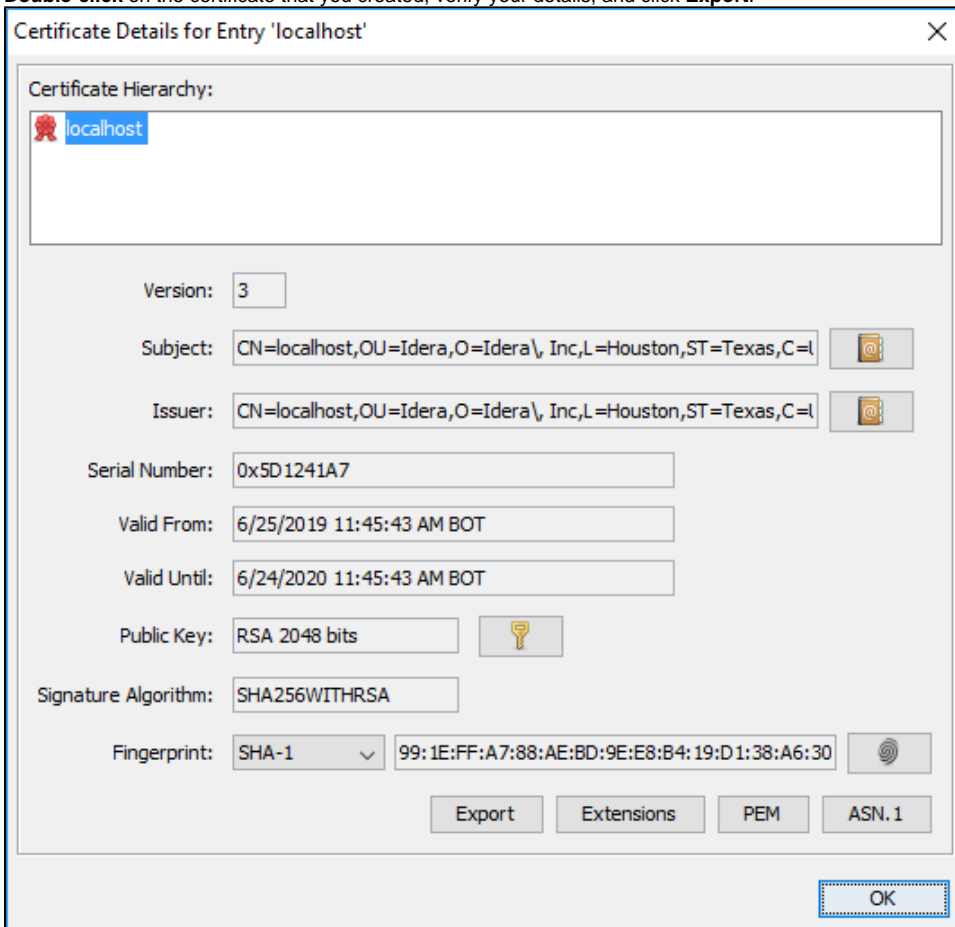
18. To delete the old certificate select the appropriate line, and then click **Cut**. If you get a Password requirement use the one from step 5.



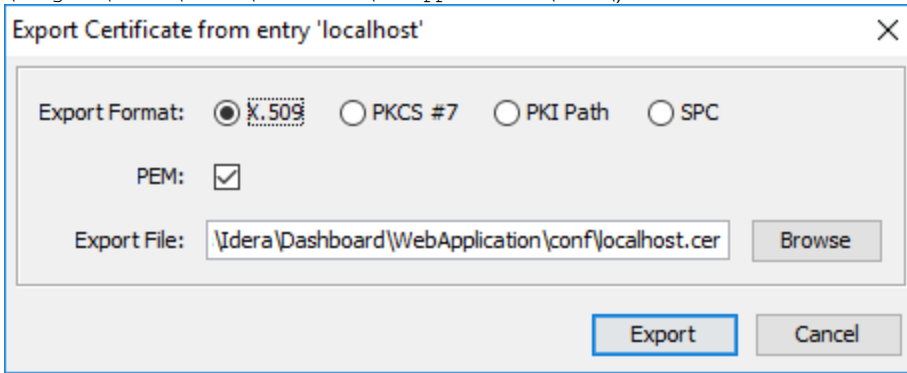
19. **Save** the changes to the keystore file.



20. **Double-click** on the certificate that you created, verify your details, and click **Export**.



21. On the Export Certificate dialog save the certificate in the IDERA Dashboard *conf* directory (e.g. `C:\Program\Files\Idera\Dashboard\WebApplication\conf\`)



22. Return to the main *KeyStore Explorer* window and close the application.
23. Restart the **Idera Dashboard Core Service** and **Idera Dashboard Web Application Service**.

Adding a certificate

To add a certificate to the Trusted Root Certification Authorities store in Windows, refer to [Manage Trusted Root Certificates](#).