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.

To resolve the certificate message at no cost

1. Download the free KeyStore Explorer utility from the following website:
   http://keystore-explorer.sourceforge.net/
2. Install the utility.
3. 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.
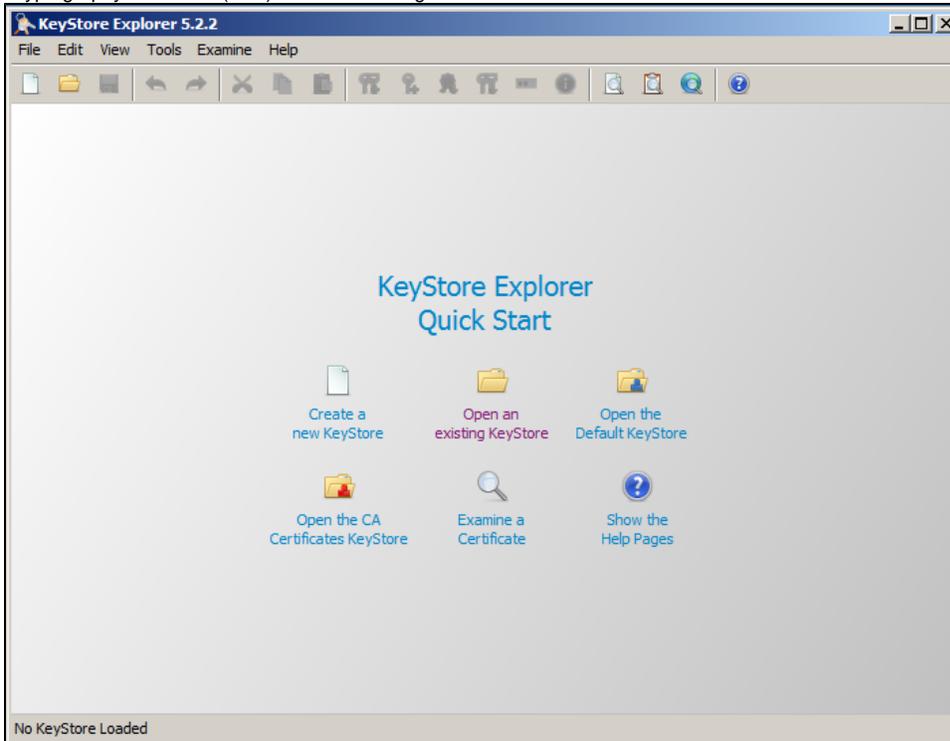
4. Open the KeyStore Explorer console by clicking **Open an existing KeyStore**. KeyStore Explorer displays the Open KeyStore window.

5. Browse to the IDERA Dashboard \conf directory (e.g. C:\Program Files\Idera\Dashboard\WebApplication\conf), and then open the keystore file.
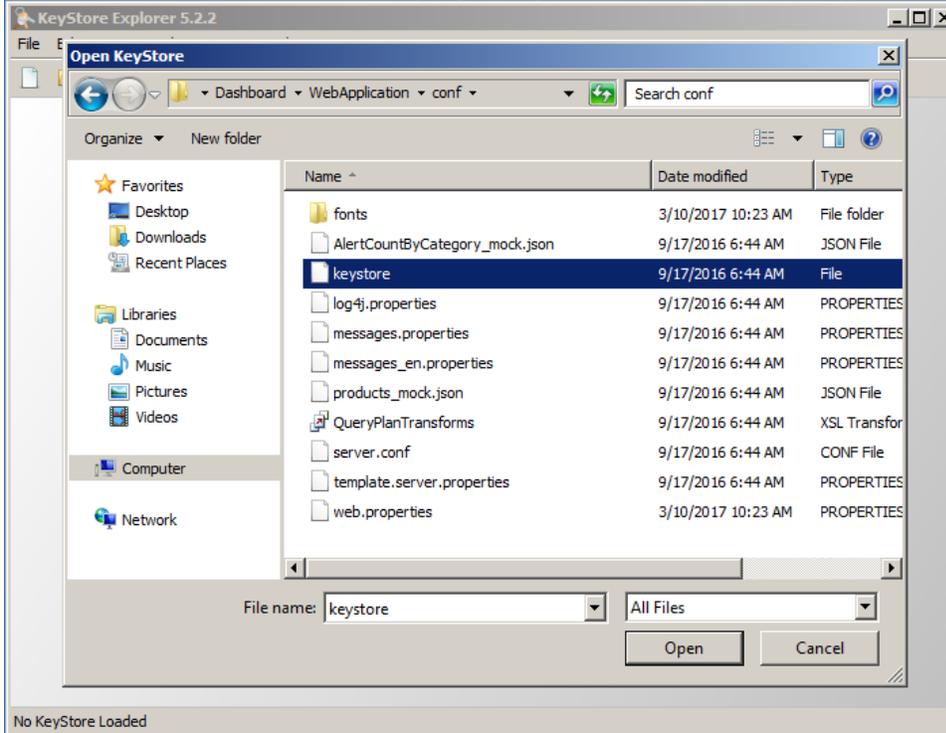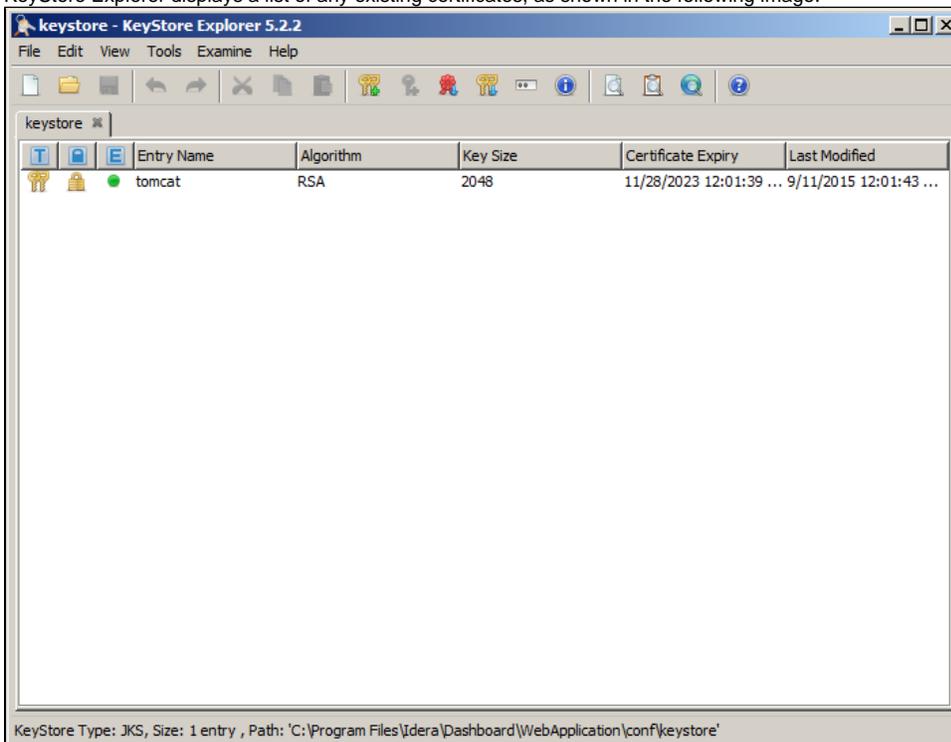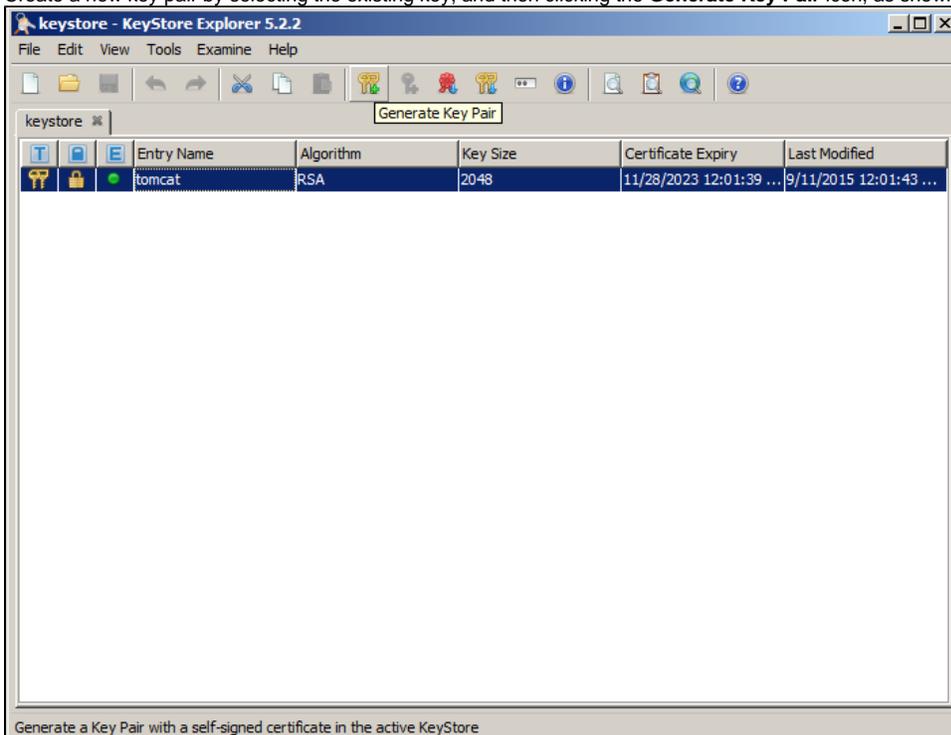

KeyStore Explorer displays the Unlock KeyStore window.
6. In the Enter Password field of the Unlock KeyStore window, type:
`password`
and then click **OK**.

Unlock KeyStore 'keystore'

Enter Password: ********

OK   Cancel

KeyStore Explorer displays a list of any existing certificates, as shown in the following image.

keystore - KeyStore Explorer 5.2.2

File   Edit   View   Tools   Examine   Help

keystore

T	🔒	E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
🔑	🔒	●	tomcat	RSA	2048	11/28/2023 12:01:39 ...	9/11/2015 12:01:43 ...

KeyStore Type: JKS, Size: 1 entry , Path: 'C:\Program Files\Idera\Dashboard\WebApplication\conf\keystore'

**7.** Create a new key pair by selecting the existing key, and then clicking the **Generate Key Pair** icon, as shown in the following image.

keystore - KeyStore Explorer 5.2.2

File   Edit   View   Tools   Examine   Help

Generate Key Pair

keystore

T	🔒	E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
🔑	🔒	●	tomcat	RSA	2048	11/28/2023 12:01:39 ...	9/11/2015 12:01:43 ...

Generate a Key Pair with a self-signed certificate in the active KeyStore

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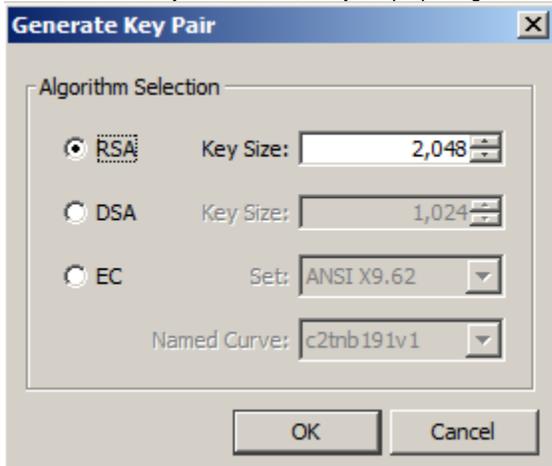

KeyStore Explorer begins to generate a new key pair
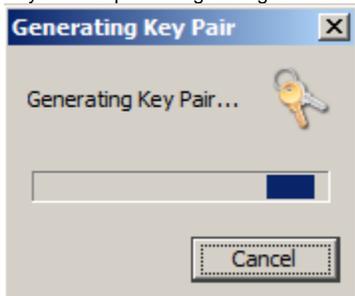
and then displays the Generate Key Pair Certificate window.

9. In 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** fields, select the number of years the certificate is valid. This example uses **5 years**.
10. Click the **Edit Name** icon to enter identifying information.

KeyStore Explorer displays the Name window.

11. In the Name window, 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**.
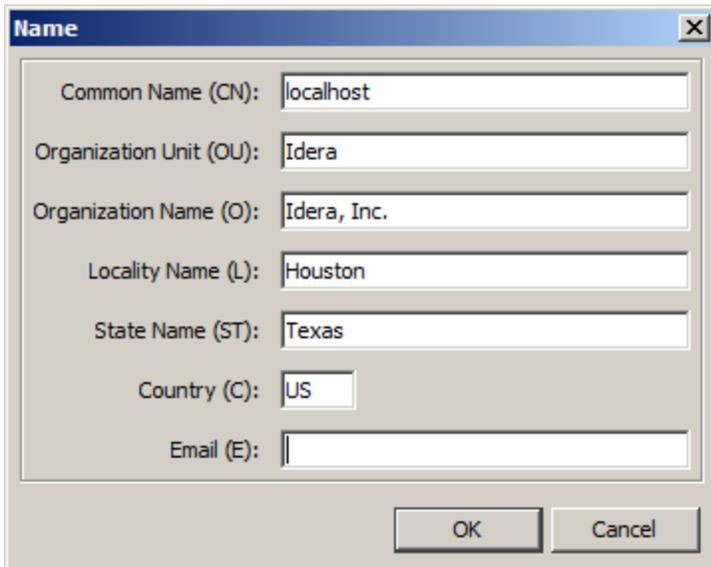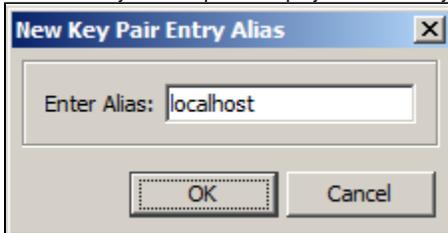
Click **OK**. KeyStore Explorer displays the New Key Pair Entry Alias window.

12. Verify that the displayed alias matches the name of your website, and then click **OK**.
    KeyStore Explorer displays the New Key Pair Entry Password window.
13. 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 6.

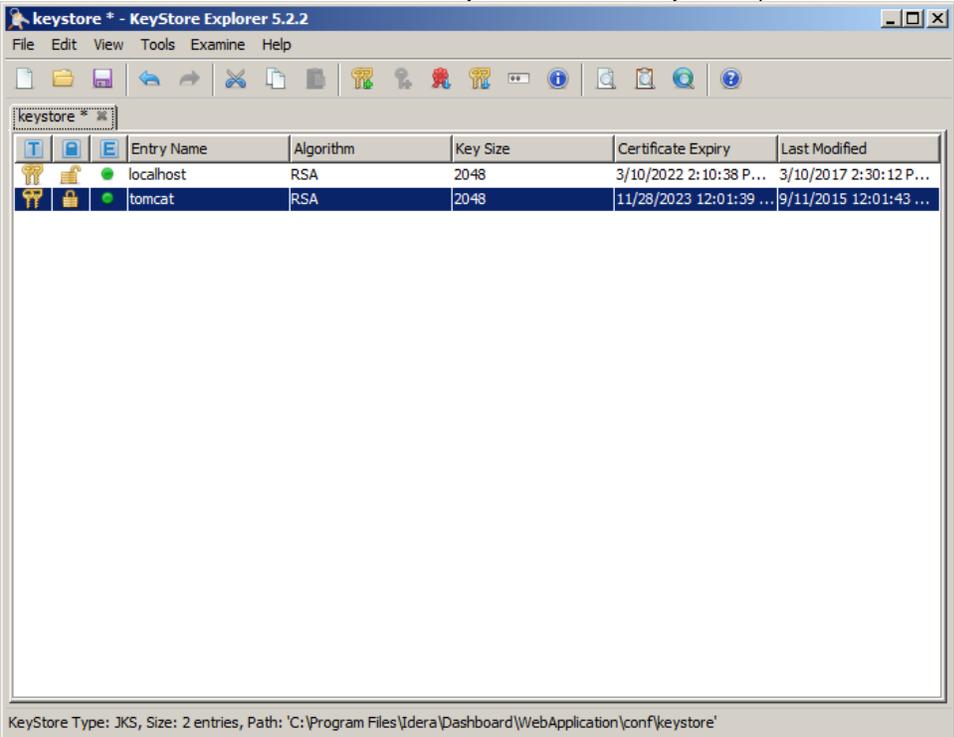In this case, type the following password in both input boxes:
`password`

KeyStore Explorer displays a message stating that the key pair generation is successful.
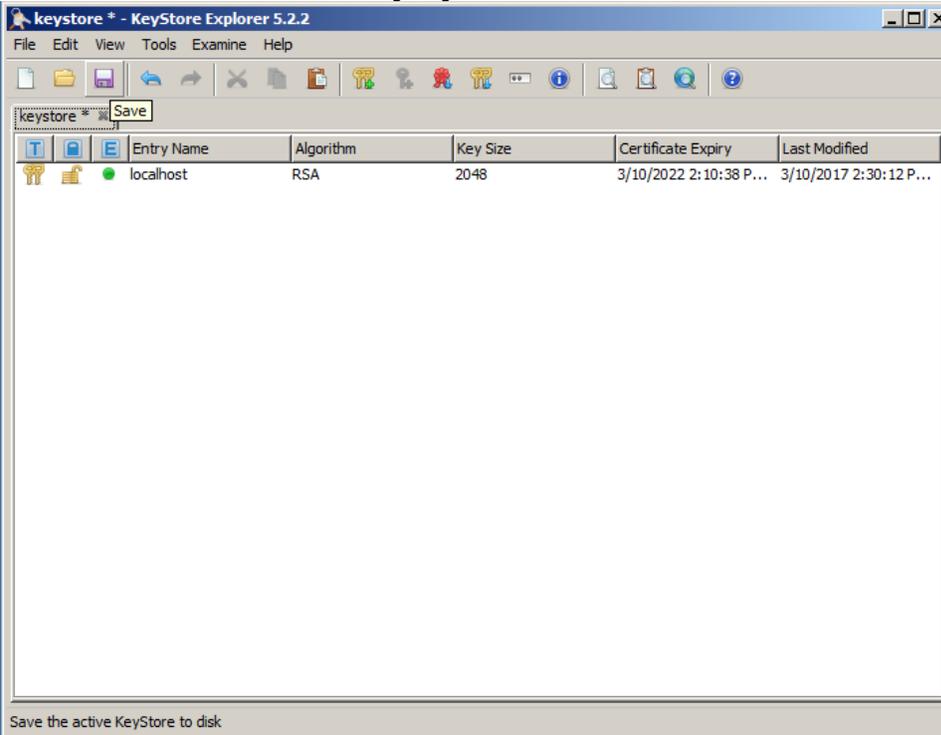
14. Click **OK** to close the success window, and then verify the new line in the KeyStore Explorer certificate list, as shown in the following image.

15. Delete the old certificate by selecting the appropriate line, and then clicking the **Cut** icon, as shown in the following image.
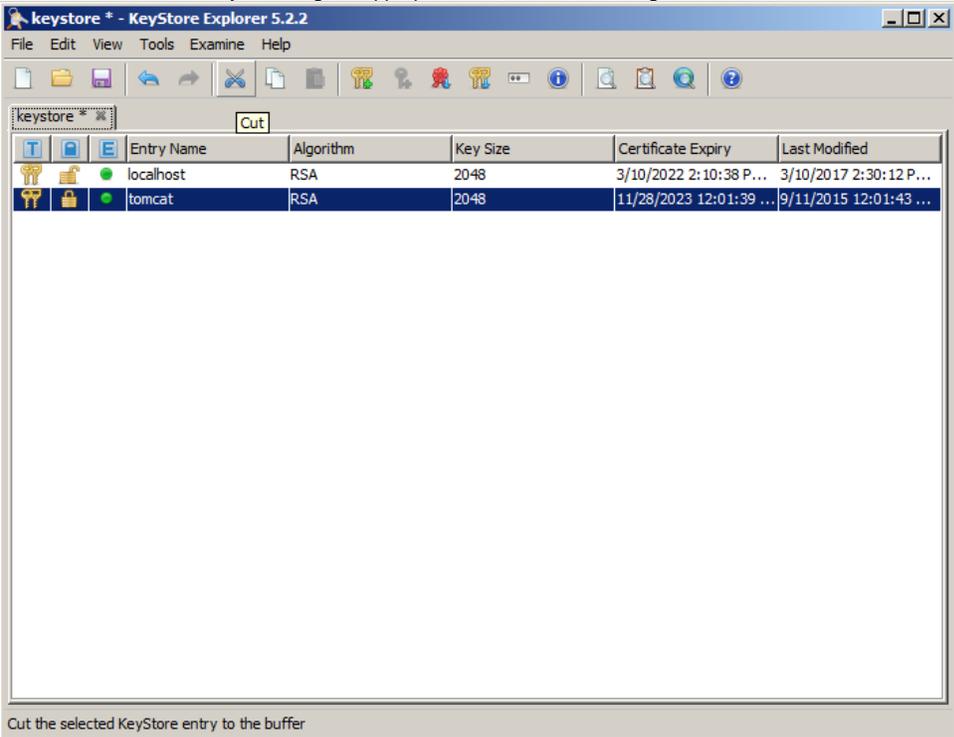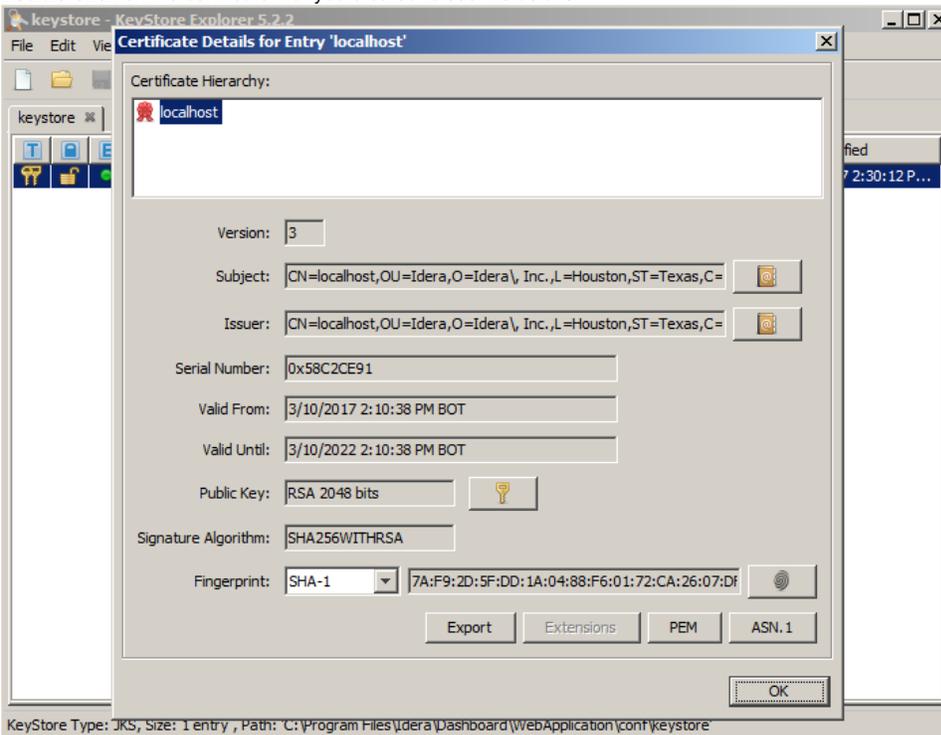
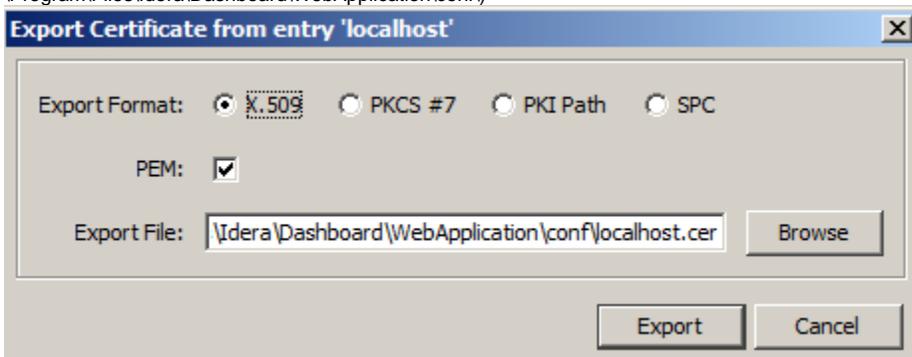16. Click the **Save** icon, as shown in the following image.

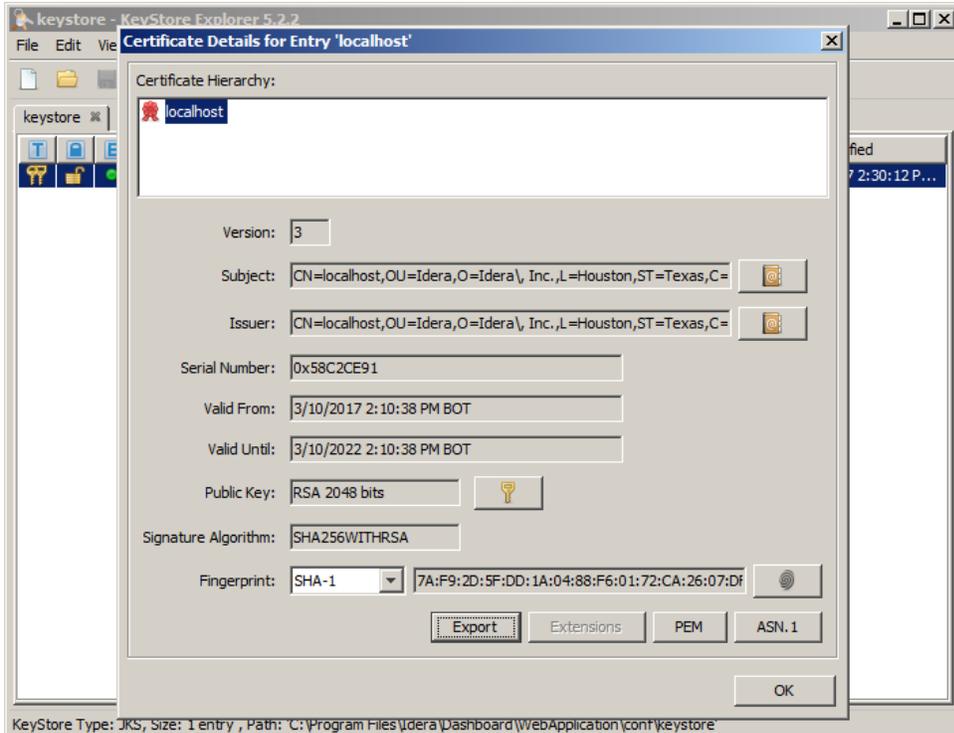17. Restart the IDERA Dashboard Web Application service.
18. **Double-click** on the certificate that you created to see the details.

19. Click **Export** and save the certificate to conf directory in the IDERA Dashboard conf directory (e.g. C: \Program\Files\Idera\Dashboard\WebApplication\conf\)

Export Certificate from entry 'localhost'

Export Format: ⦿ X.509   ○ PKCS #7   ○ PKI Path   ○ SPC

PEM: ☑

Export File: [\Idera\Dashboard\WebApplication\conf\localhost.cer]   [Browse]

[Export]   [Cancel]

20. Click **OK** on the certificate details window to close it.

keystore - KeyStore Explorer 5.2.2

File   Edit   Vie

Certificate Details for Entry 'localhost'

Certificate Hierarchy:

🔴 localhost

Version: 3

Subject: CN=localhost,OU=Idera,O=Idera\, Inc.,L=Houston,ST=Texas,C=

Issuer: CN=localhost,OU=Idera,O=Idera\, Inc.,L=Houston,ST=Texas,C=

Serial Number: 0x58C2CE91

Valid From: 3/10/2017 2:10:38 PM BOT

Valid Until: 3/10/2022 2:10:38 PM BOT

Public Key: RSA 2048 bits

Signature Algorithm: SHA256WITHRSA

Fingerprint: SHA-1 ▼ 7A:F9:2D:5F:DD:1A:04:88:F6:01:72:CA:26:07:DF

[Export]   [Extensions]   [PEM]   [ASN.1]

[OK]

KeyStore Type: JKS, Size: 1 entry , Path: 'C:\Program Files\Idera\Dashboard\WebApplication\conf\keystore'
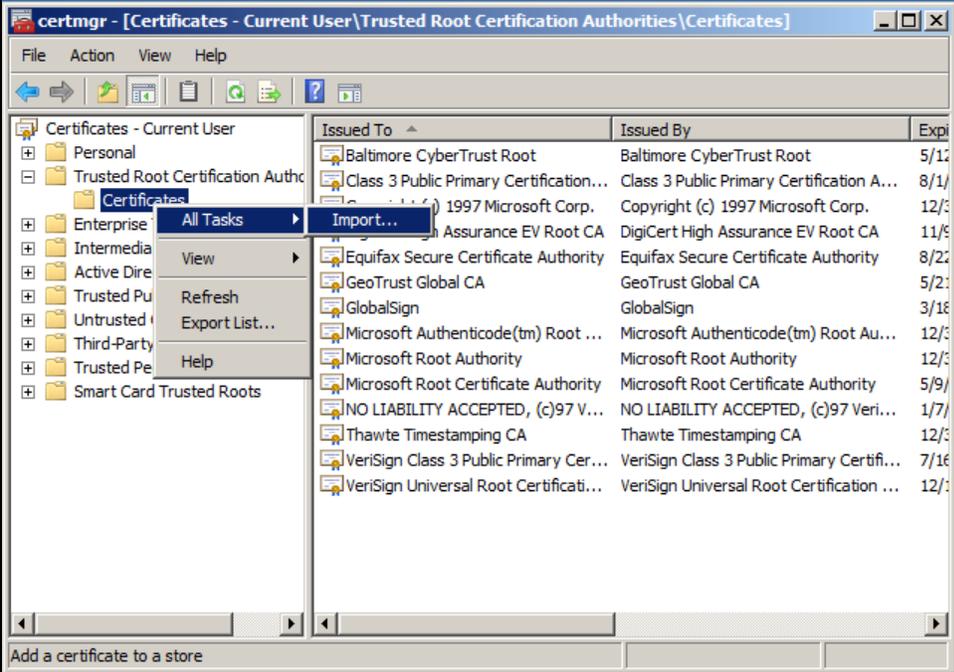
21. Open Certificate Manager by pressing **Win+R** to summon the Run dialog box, type *certmgr.msc*, and press **ENTER**.

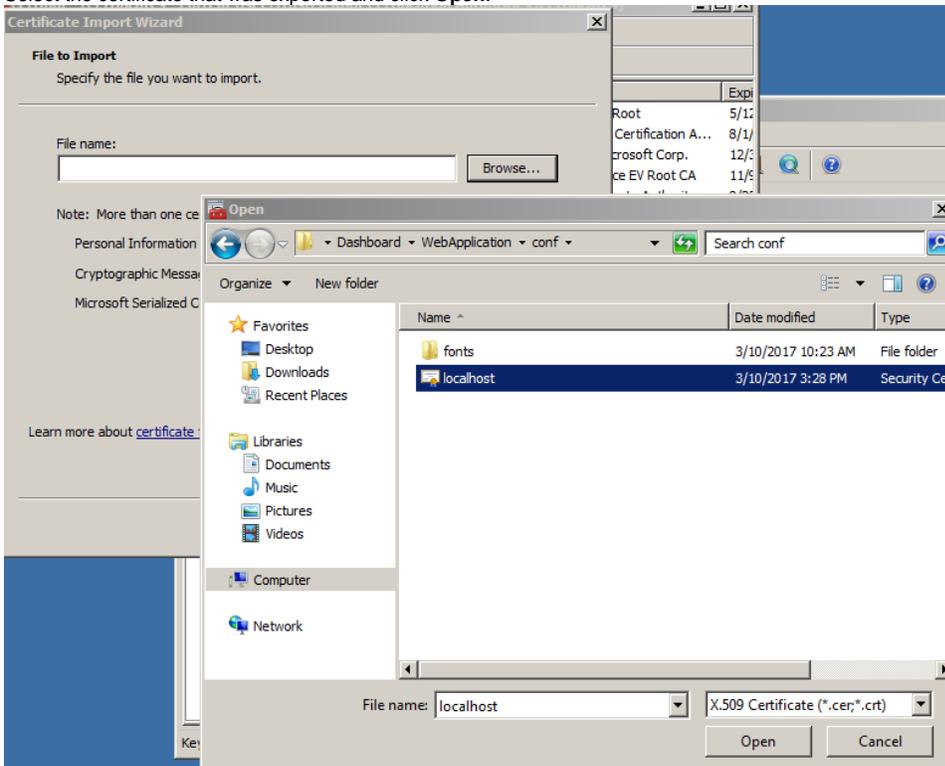If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
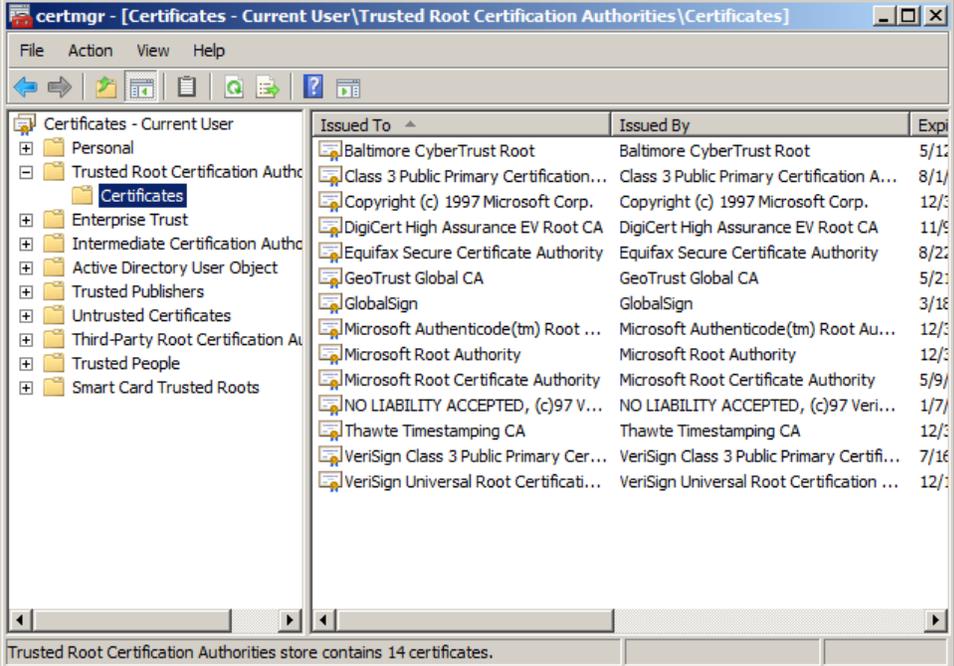
22. Right-click on the **Trusted Root Certification Authorities > Certificate node and select All Tasks > Import.**
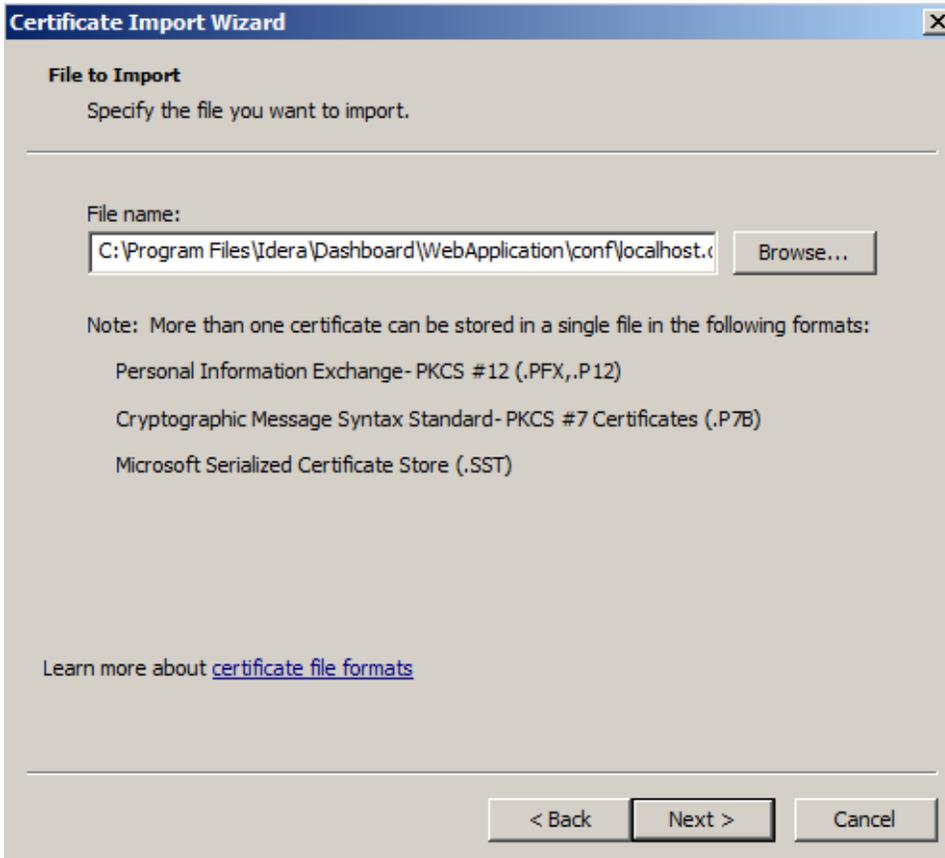
23. On the Certificate Import Wizard, click **Next**.

24. Select the certificate that was exported and click **Open**.

25. Click **Next**.

Certificate Import Wizard ☒

File to Import
Specify the file you want to import.

File name:

| C:\Program Files\Idera\Dashboard\WebApplication\conf\localhost.c | Browse... |

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

| < Back | Next > | Cancel |

26. Select **Place all certificates in the following store**. The correct store would be *Trusted Root Certificate Authorities*. Then click **next**.
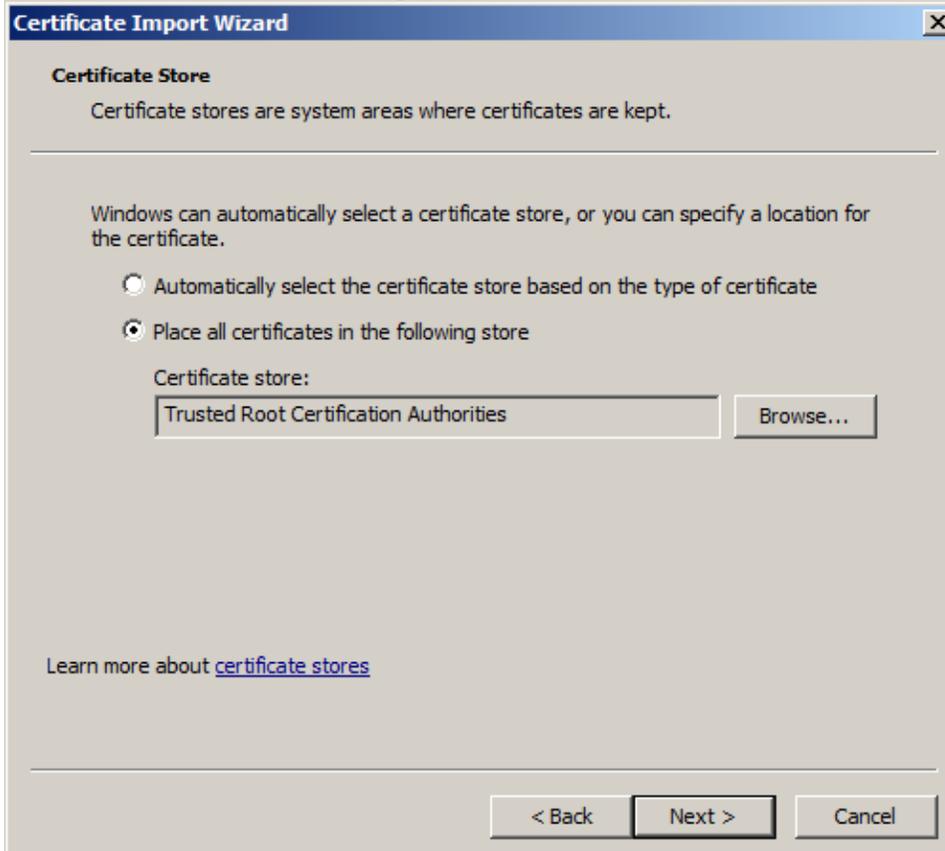
Certificate Import Wizard ☒

Certificate Store
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

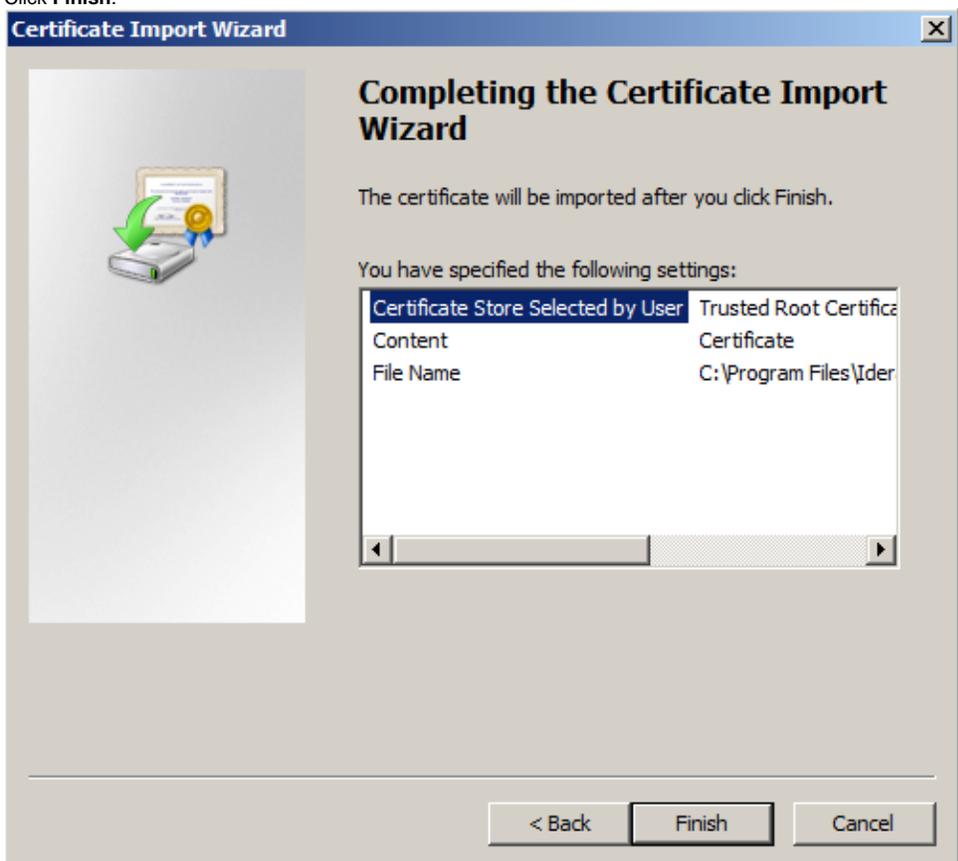○ Automatically select the certificate store based on the type of certificate

⦿ Place all certificates in the following store

Certificate store:

| Trusted Root Certification Authorities | Browse... |

Learn more about certificate stores
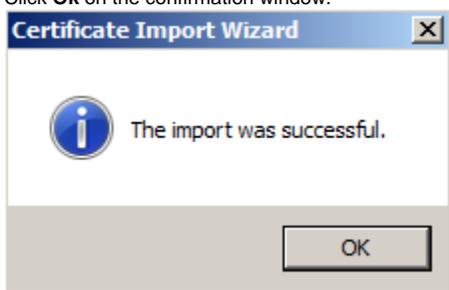
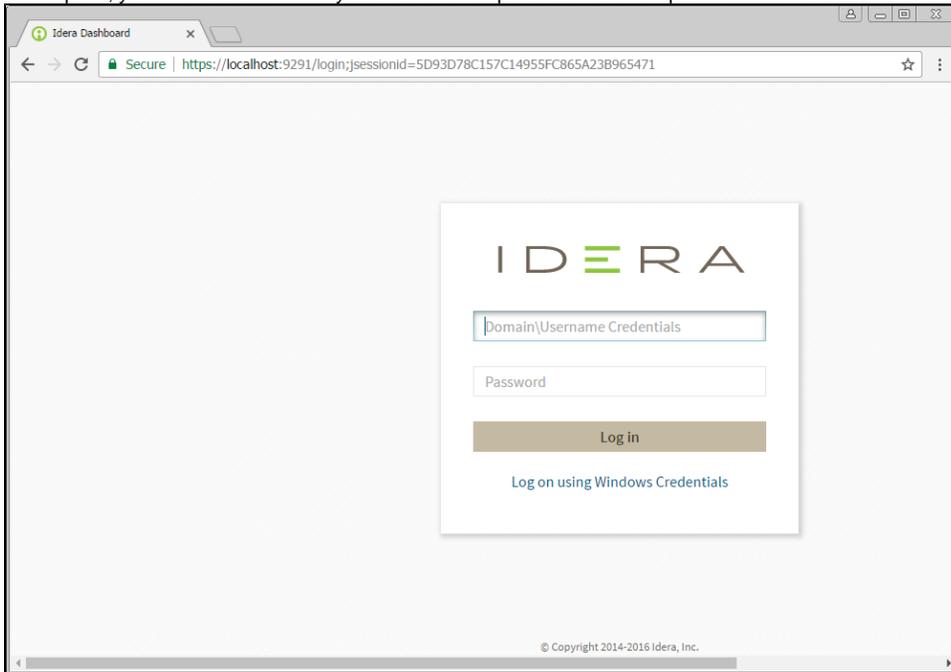| < Back | Next > | Cancel |

27. Click **Finish**.

28. Select **Yes**.

29. Click **Ok** on the confirmation window.

30. At this point, you will need to close any browser that is open and then attempt to **access** the IDERA Dashboard.

IDERA Dashboard provides an integrated user experience for the IDERA products in your environment.

IDERA | **Products** | **Purchase** | **Support** | **Community** | **Resources** | **About Us** | **Legal**