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.

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 SSL (HTTPS), or you can use the following steps to resolve this issue at no certificate cost.

To resolve the certificate message at no cost

- Download the free KeyStore Explorer utility from the following website: http://keystore-explorer.sourceforge.net/
- 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.



No KeyStore Loaded

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 'keystor	e' X			
Enter Password:	*			
ОК	Cancel			
eyStore Explorer displays a list	of any existing certificates, as	shown in the following im	age.	
keystore - KeyStore Explorer 5.2. File Edit View Tools Examine Help	2			
	1 1 1 1 1	0 0 0 0		
keystore %	Algorithm Key Size	Certificate Expiry	Last Modified	
reate a new key pair by selectin	g the existing key, and then c	licking the Generate Key	Pair icon, as shown	in the following im
File Edit View Tools Examine Help	Generate Key Pair	•]]]]] •]		
keystore 🕷	Algorithm Key Size	Certificate Expiry	Last Modified	
Generate a Key Pair with a self-signed certi	ficate in the active KevStore			

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

G	enerate Key	Pair			×
	Algorithm Sel	ection			
	• RSA	Key Size:		2,048 🕂	
	O DSA	Key Size:		1,024 🔅	
	O EC	Set: /	ANSI X9.62	7	
	Ν	lamed Curve:	:2tnb 19 1v :	1 🔻	
		O	<	Cancel	
٢e	eyStore Explore	begins to genera	ate a new k	ey pair	
_					

Generating Key Pair	스
Generating Key Pair	Ş
Ca	ncel

- 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.

(Generate Key Pair C	ertificate	×
	Version:	C Version 1 C Version 3	
	Signature Algorithm:	SHA-256 with RSA	
	Validity Period:	5 - Year(s)	
	Serial Number:	1489161873	
	Name:		
			Add Extensions
			OK Cancel

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.

I	Name		×						
	Common Name (CN):	localhost	1						
	Organization Unit (OU):	Idera	1						
	Organization Name (O):	Idera, Inc.	1						
	Locality Name (L):	Houston	1						
	State Name (ST):	Texas	1						
	Country (C):	US							
	Email (E):		1						
		OK Cancel							
	Click OK . KeyStore Explorer displays the New Key Pair Entry Alias window.								
	New Key Pair Entry Alia Enter Alias: localhost								

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.
 Type and confirm the password you want to use for the key pair, and then click OK.

Cancel

This password must match the password entered in step 6. ≙

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

OK

New Key Pair Entry Password								
Enter New Password: Confirm New Password:	******							
	OK Cancel							

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.

⊳ ĸe	ysto	re * -	Key5	tore l	Exploi	rer 5.	2.2													
ile	Edit	View	Tool	s Ex	amine	Help	0													
1				et.	8	þ	16	1	- 94	鳧	R		0	a	<u>Ì</u>	Q	0			
keys	tore *	*																		
		E	Entry	Name			Algor	ithm		1	(ey Siz	e		1	Certific	ate Ex	piry	Last	t Modifie	ed
T	ſ	۲	localho	ost			RSA			2	048				3/10/20	022 2:1	10:38 P.	3/10	/2017	2:30:12 P
ሞ	Ĥ	•	tomca	t			RSA			2	048				11/28/	2023 1	2:01:39	9/11	/2015	12:01:43

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

keystore * - KeyStore Explorer 5.	2.2			
ile Edit View Tools Examine Help) 			
l 🖻 🖬 🛸 🤌 👗 🗅	🛅 🌃 🐕 🕱	🕂 🎹 🚥 🕕 🖾	. 🖾 🔍 🛛 🔞	
cut				
T E Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
n 👔 💿 localhost	RSA	2048	3/10/2022 2:10:38 P	3/10/2017 2:30:12 P.
🎢 📋 🔍 tomcat	RSA	2048	11/28/2023 12:01:39	9/11/2015 12:01:43 .
t the selected KevStore entry to the buf	fer			

16. Click the Save icon, as shown in the following image.

keystore *	- KeyStore Explorer	5.2.2	mage.			
File Edit Vie	w Tools Examine H	elp				
			, 🕺 🏗 🚥 🕕			
keystore * 🕷	Save					1
	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified	
T = •	localnost	RSA	2048	3/10/2022 2:10:38	P 3/10/2017 2:3	30:12 P
Save the active	KeyStore to disk					
7. Restart the II 8 Double-click	DERA Dashboard	Web Application	n service. It to see the details			
🚴 keystore -	KevStore Explorer 5.2	2.2				_ 🗆 X
File Edit Vie	Certificate Details fo	r Entry 'localhost'				
	Certificate Hierarchy:					
keystore 🗶						1
					red 7 2:3	30:12 P
	1					
	Version:	3				
	Subject:	CN=localhost,OU=	Idera,O=Idera Inc.,L=	Houston,ST=Texas,C=		
	Issuer:		Idera O=Idera\ Inc. I =	Houston ST=Texas C=		
	1550011					
	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				
	Circulture Alexanthere					
	signature Algorithm:	JSHA256WITHRSA				
	Fingerprint:	SHA-1	7A:F9:2D:5F:DD:1A:04:	88:F6:01:72:CA:26:07:DF	9	
			Export Exte	ensions PEM	ASN.1	
				E	OK	

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

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 Certificat	e from entry 'localhost'	×						
Export Format:	• X.509 O PKCS #7 O PKI Path O SPC							
PEM:								
Export File:	\Idera\Dashboard\WebApplication\conf\Jocalhost.cer Browse							
	Export Cancel							

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

keystore - File Edit Vie	(evStore Explorer 5.2 Certificate Details for	2.2 r Entry 'localhost' X	
	Certificate Hierarchy:		
keystore 🕷	👮 localhost		
			fied
	I		/ 2:30:12 P
	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 TA:F9:2D:5F:DD:1A:04:88:F6:01:72:CA:26:07:Df	
		Export Extensions PEM ASN.1	
		ОК	

21. Open Certificate Manager by pressing Win+R to summon the Run dialog box, type certmgr.msc, and press ENTER.

22. Right-click on the Trusted Root Certification Authorities > Certificate node and select All Tasks > Import.

File Action View Help Image: Second Sec	🧱 certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Certificates]								
Image: Second secon									
Certificates - Current User									
Image: Second Control of	Exp 5/1: 8/1, 12/3 11/9 8/2: 5/2 3/10 12/3 5/9; 1/7; 12/3 5/9; 1/7; 12/3 5/9; 1/7; 12/3 5/9; 1/7; 12/3 5/9; 1/7; 1/7; 5/9; 1/7; 1/								
Add a certificate to a store	Þ								

23. On the Certificate Import Wizard, click Next.



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					
	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 (.P78)					
	Microsoft Senalized Certificate Store (.SST)					
	Learn more about <u>certificate file formats</u>					
	< 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.					
	O Automatically select the certificate store based on the type of certificate					
	Place all certificates in the following store					
	Trusted Root Certification Authorities Browse					
	Learn more about <u>certificate stores</u>					
	< Back Nevt > Cancel					

27. Click Finish.

Certificate Import Wizard						X
			Completing the Certificate Import Wizard The certificate will be imported after you click Finish. You have specified the following settings: Certificate Store Selected by User Content Certificate File Name C:\Program Files\Ide			
28.	Select Yes.			< Back	Finish	Cancel
Security Warning						×
		You are about to install a certificate from a certification authority (CA) claiming to represent: localhost Windows cannot validate that the certificate is actually from "localhost". You should confirm its origin by contacting "localhost". The following number will assist you in this process: Thumbprint (sha 1): 7AF92D5F DD1A0488 F60172CA 2607DF31 8E64223D Warning: If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk. Do you want to install this certificate?				
				Yes	No	

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.

G Idera Dashboard x						
$\leftarrow \rightarrow \mathbf{C}$ Secure https://localhost:9291/login;jsessionid=5D93D78C157C14955FC865A23B965471						
	DERA Domain\Username Credentials Password Log in Log on using Windows Credentials					
4	© Copyright 2014-2016 Idera, Inc.	Þ				

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

IDERA Website Products Purchase	Support	Community	About Us	Resources	Legal
---------------------------------	---------	-----------	----------	-----------	-------