# Resolving the certificate error message

(j)

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.

In environments that have not yet added a certificate signed by a Certification Authority (CA), IDERA users receive a warning message in their browser each time they attempt to open the SSL version of 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

#### Create a self-signed certificate

- 1. Launch Windows Powershell as administrator.
- 2. Create your certificate by running the following command. Leave Windows PowerShell open.

```
$certName = "{certificateName}" ## Replace {certificateName}
Replace {certificateName} with the name that you will use to access the IDERA Dashboard. For example, if you are using the ht
tps://ComputerName:9291 link to access IDERA Dashboard, then use ComputerName . In case, you are using the https://Com
puterName.Domain.com:9291 address then use Computername.Domain.com. In this example we are using localhost .
```

3. Run the following command to configure your certificate settings.

```
$Params = @{
    "DnsName"
                        = @($certName,"{certificateName}") ## If you want to include other addresses
or servers, you must separate each with a comma
    "CertStoreLocation" = "Cert:LocalMachine\My"
    "KeyExportPolicy" = "Exportable"
    "KeySpec"
                       = "Signature"
    "KeyUsage"
                      = @("KeyEncipherment", "DigitalSignature")
    "KeyAlgorithm"
                      = "RSA"
                       = "2048"
    "KeyLength"
    "HashAlgorithm"
                       = "SHA256"
    "NotAfter"
                        = (Get-Date).AddYears(10)
}
## Checks for asterisks in the $certName and replaces it with the underscore character
If ($certName.Contains("*")) {
    $certName = $certName -replace '\*','_'
```

Replace {certificateName} with the certificate name you previously defined in Step 2.

Change the NotAfter parameter value to make your certificate valid for a more extended period.

4. Run the command below to create your certificate defined with the parameters above.

\$cert = New-SelfSignedCertificate @Params

#### Export your certificate private key

Once the certificate is created, you need to export the certificate's private key. To do so, follow the steps below:

1. Export your certificate in .cer format by running the following command.



protect your certificate's private key.

```
$mypwd = ConvertTo-SecureString -String "{myPassword}" -Force -AsPlainText ## Replace {myPassword}
```

3. Run the next command to export your private key, use the password you store in the smypwd variable.

Export-PfxCertificate -Cert \$cert -FilePath "{DesiredPath}\\$certname.pfx" -Password \$mypwd ## Replace
{DesiredPath} with your desired location e.g. C:\Users\Public\Documents

When the private key is exported in a .pfx file, you should be able to check the certificate specifications.

PS ( PS (	:\Windows\system32> :\Windows\system32>	<pre>\$mypwd = ConvertT Export-PfxCertif</pre>	o-Secure icate -C	<pre>String "password" -Force -AsPlainText ert \$cert -FilePath "C:\Users\Public\Documents\\$certname.pfx"</pre>	
	Directory: C:\Users\	Public\Documents			
Mode	e Las	tWriteTime	Length	Name	
-a-	4/5/2023	6:54 PM	2675	windev2302eval.pfx	

#### Import your private key into the Trusted Root Certification Authorities

Complete your certificate configuration by adding the .cer file to the **Trusted Root Certification Authorities** folder in the **Console Root**. To do so, follow the steps below:

1. Open the Microsoft Management Console (MMC) by selecting Start > Run and typing mmc. Click OK.

🖅 Run	×
Ð	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	mmc v
	OK Cancel <u>B</u> rowse

- 2. When the MCC window opens, click File from the menu toolbar, and select Add/Remove Snap-in...
- 3. Select Certificates from the Available snap-ins options and click Add >.
- 4. In the Certificates snap-in window, select Computer Account, and click Next.

5. In the Select Computer window, verify that Local computer is set as the computer you want the snap-in to manage. Click Finish.

Console1 - [Console Root]			= U X
Fix Action View Favorites	Window Help		- 8
New	Ctrl+N		
open	Ctrl+O		Actions
Save		There are no items to show in this view	Console Root
Save As			More Actions
Add/Remove Snap-in Options	Ctrl+M		
1 C:\Users\\ConsoleOne Test 2 services 3 compmgmt			
4 SQLServerManager13			
Exit			

6. Import your certificate (.cer file) into the Trusted Root Certification Authorities folder. To do so, expand Certificates and right-click the Truste d Root Certification Authorities folder. Click All Tasks > Import...

• 🔿 🙍 📰 📋 🧟 📑 🚺				
Console Root Console Root Centificates (Local Computer) Certificates (Local Computer) Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates New Window from He Cient Authon Preview Build Cient Authon Preview Build Cient Authon Cient	Issued To         Import         Import         Import         Import         Issued To         Import         Import	Issued By AAA Certif Baltimore C Class 3 Publ Copyright (c DigiCett Glo DigiCett Glo DigiCett Glo DigiCett Hig DigiCett Hig DigiCett Hig DST Root CA GlobalSign F Go Daddy R Idera Inc ISRG Root X Microsoft Al	icates Aore Actions	

7. Follow the Certificate Import Wizard instructions to import the .cer file previously created.

When adding your certificate or private key using the Certificate Import Wizard, use the password you previously defined in the Export your certificate private key section.

### **Import Key Pair**

1. Download the free KeyStore Explorer utility from http://keystore-explorer.org/ and install it.

2. Open KeyStore Explorer as administrator. On launch, it may ask you to download an updated Java Cryptography Extension (JCE) Unlimited



Strength file. No KeyStore Loaded

- 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.

Cur Open Keystore			~
└── ← → ~ ↑ <mark> </mark>	WebApplication > conf > 🗸 🍾 ඊ	Search conf	م
Organize 🔻 Nev	older	== -	
1.0.11	Name	Date modified	Туре
Quick access	fonts	6/25/2019 10:47 AM	File folder
Desktop	🐔 🍙 idera-dashboard	3/29/2018 7:58 AM	Executable
Downloads	🖈 🏼 🎒 idera-dashboard-core	3/29/2018 8:00 AM	Executable
🖆 Documents	* keystore	3/29/2018 7:57 AM	File
Pictures	Iog4j.properties	3/29/2018 7:57 AM	PROPERTIE
This PC	messages.properties	3/29/2018 7:57 AM	PROPERTIE
-	messages_en.properties	3/29/2018 7:57 AM	PROPERTIE
Network	products_mock.json	3/29/2018 7:57 AM	JSON File
	<u> </u>	3/29/2018 7:57 AM	XSLT Styles
	web.properties	6/25/2019 10:47 AM	PROPERTIE
	<		>
	le name: keystore 🗸	All Files	$\sim$
		Open	Cancel

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

Unlock KeyStore	'keystore'	×
Enter Password	d: •••••	
	ОК	Cancel

	E	Entry Name	Algorithm	Kev Size	Certificate Expiry	Last Modified
7 🔒	0	tomcat	RSA	2048	11/28/2023, 8:01:39 A	9/11/2015, 9:01:4
	0					

7. Select PKCS #12 as the type of key you want to import, and click OK

🚊 🔳 Entry Name	Algorithm Key Size	Certificate Expiry	Last Modified
	Import Key Pair Type Select the type of key pair import req PKCS #12 PKCS #8 PVK OpenSSL	× uired:	
	OK Can	cel	

8. Look for the key you created steps above (in this case, <code>localhost.pfx</code>) and <code>click Choose</code>.

	🔊 Choose PKCS	5 #12 Key Pair											×
	Recent Items	Look In:	key					~	Û	ŧ	N;	::	:=
	Desktop												
	Documents												
	This PC	File Name:											
	<b>1</b>	Files of Type:	PKCS #1	12 KeySt	ore Files (	*.p12	;;*.pfx)						~
	Network							C	Choo	se		Canc	el
9.	Select an alias for	your key, and	click OK.										
	🍌 New Key	Pair Entry Al	ias		×								
	Enter Alias:	localhost											
		(	ж	)	ancel								
10.	In Enter New Pas	<b>sword</b> type "pa	assword",	, confirn	n, and clic	ck Ol	К.						
	🎠 New Key	Pair Entry Pa	ssword				×						
	Enter Ne	w Password:	•••••	•••			0						
	Confirm Ne	w Password:		•••			0						
				(	ОК		Cancel						
11.	When the configu	ration is comple	ted the fo	ollowing	message	e pop	ps up, click <b>O</b> l	к.					
	Import Key Pa	ir			$\times$								
	6 Key	Pair Import S	uccessf	ful.									
				OK									

12. Return to the main KeyStore Explorer window, save your configuration, and close the application.

🐥 File Edit View Tools Exam	ine Help key	store * - Key	Store Explorer 5.5.2	- 0 X
🗅 🖴 🖨 📥 📾 🛍	12 % 死 12 🚥	0	20	
keystore * 🕱				
🔳 🔳 Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
🃅 🚅 🥝 localhost	RSA	2048	4/11/2033, 3:07:30 PM	4/11/2023, 3:22:47 P

KeyStore Type: JKS, Size: 1 entry, Selected: none, Path: 'C:\Program Files\Idera\Dashboard\WebApplication\conf\keystore'

- Close all the opened browsers.
   Restart Idera Dashboard Core Service and Idera Dashboard Web Application Service.
- **15.** Access to **IDERA Dashboard** with the following link https://<{certificateName}>:9291.

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