Certificate Issues

To access SQL Inventory Manager over HTTPS with a self signed certificate you may need to enable SSL on SQL Inventory Manager 2.6 REST service, and add a certificate.

Using a self-signed certificate

A Using a self-signed certificate only works with both IDERA Dashboard and SQL Inventory Manager installed on a local machine.

Creating a self-signed certificate

Before binding a certificate to Inventory Manager 2.6, you need to first add a certificate for IDERA Dashboard. For information on how to create a self signed certificate for Dashboard refer to Resolving the certificate error message.

Important

Make sure that the self-signed certificate created with the steps described above, and the keystore keypair are created to have each server listed as the common name.

Binding a certificate to Inventory Manager 2.6



()

Before you begin

Make sure you perform the instructions in Resolving the certificate error message.

To bind a certificate follow the instructions below:

- 1. Launch the keyStore Explorer application as an Administrator.
- 2. Open the keystore file used for the IDERA Dashboard. When prompted for a password, enter *password*, and click **OK**.
- 3. Right-click on the keypair and select *Export*> *Export* Private Key.

🏃 keystore - KeyStore Explorer 5	.4.3					_		×
File Edit View Tools Examine	Help							
🗋 🖨 🔳 (👟 🏕) 🛎 🛅 🛽	l 🏗 % 📌 🏗	- 🕕 🖻	0	2				
keystore 🕷								
T 🖹 E Entry Name		Algorithm	Key Size	Certif	îcate Expiry	Last Mo	dified	
📅 📑 🗢 🔍 View Detail	s >	RSA	2048	4/7/20	25 8:22:29 PM PDT	4/7/2020	0 8:24:31	PM
Cut Copy	Ctrl+X Ctrl+C							
🚊 Export	2	m Export k	(ey Pair					
🧾 Generate C	SR	👮 Export (Certificate Cl	hain				
🖄 Import CA	Reply >	💡 🔀 Export F	rivate Key					
🦈 Edit Certific	ate Chain	P Export F	ublic Key					
🧾 Sign	>							
💼 Unlock								
. Set Passwo	rd							
🗙 Delete								
🚛 Rename								
Export the Key Pair entry's private key	as PKCS #8, PVK or O	penSSL						

- 4. On the Export Private Key Type window, select OpenSSL, and click OK.
- 5. On the **Export Private Key as OpenSSL from Keystore Entry** window, deselect the *Encri pt* option, update the *Export File* if needed, and click **OK**.

Export Priva	ate Key as Op	enSSL from KeyStore Entry 'localhost'	\times
3	Encrypt:		
Encryptio	n Algorithm:	PBE with DES CBC \sim	
Encryptio	n Password:		
Confir	m Password:		
	PEM:		
	Export File:	ra\Dashboard\WebApplication\conf\localhost.key Browse	
		Export Cancel	

- Steps 6 9 can be performed on a different computer. These steps are related to the OpenSSL tool, which is not required to be intalled on the server hosting the IDERA products.
- 6. Install OpenSSL.
 - 0

You can find a few options available to obtain the software at https://wiki.openssl.org /index.php/Binaries.

- 7. Once you complete the installation of OpenSSI, run the Command Promt as Administrator.
- 8. Change the directory to the bin folder within the installation directory of OpenSSL. Enter the following command:

```
cd "C:\Program Files\OpenSSL-Win64\bin"
```

9. Use the following command as an example to generate the PFX key using the private key and certificate that was previously created.

openssl pkcs12 -export -out <file path to the new personal information exchange file>.pfx -inkey <file path path to private key>.key -in <file path to certificate>.cer

Execute the command, and when prompted for a password, enter *password* for both the export password and the verification password. You will be able to see the newly created PFX key.

▲ The following steps must be performed on the server hosting the IDERA Dashboard and the IDERA SQL Inventory Manager.

10. Open the Microsoft Management Console (MMC) and load the Certificates snap-in. a. Select **Run** from the **Start** menu, enter *mmc*, and click **OK**.

💷 Run		×
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.	
Open:	mmc v	
	This task will be created with administrative privileges.	
	OK Cancel <u>B</u> rowse]

b. On the **MMC** window, from the File menu, select *Add/Remove Snap-in*. The Add or Remove Snap-in windows displays.

c. From the Available snap-ins list, choose Certificates, then select Add.

Remove	Console Root		Î	Vendor	nap-in
Remove Move Up					
Move Up				Microsoft Cor	ActiveX Control
Move Up				Microsoft Cor	Authorization Manager
Move Up				Microsoft Cor	Certificates
. Tore op				Microsoft Cor	Component Services
				Microsoft Cor	Computer Managem
Move Down		Add		Microsoft Cor	Device Manager
	4	- AUG 2		Microsoft and	Disk Management
				Microsoft Cor	Event Viewer
				Microsoft Cor	Folder
				Microsoft Cor	Group Policy Object
				Microsoft Cor	Internet Informatio
				Microsoft Cor	IP Security Monitor
Advanced			~	Microsoft Cor	IP Security Policy M
- available and a second					
				Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor	Folder Group Policy Object Internet Informatio IP Security Monitor

d. In the Certificate snap-in window, select Computer Account, and click Next.

e. In the **Select Computer** window, leave **Local computer** selected, and click **Finish**. f. In the **Add or Remove Snap-in** window, select **Ok**.

nap-in ActiveX Control	Vendor Microsoft Cor Microsoft Cor	^		Console Root	Edit Extensions Remove
Certificates	Microsoft Cor Microsoft Cor				Move Up
Device Manager Disk Management	Microsoft Cor Microsoft and		Add >		Move Down
Event Viewer Folder	Microsoft Cor Microsoft Cor				
Internet Informatio	Microsoft Cor Microsoft Cor				
IP Security Policy M	Microsoft Cor	~			Advanced
scription:					

- 11. Expand Certificates and locate the Personal folder.
- 12. Right-click on the **Personal** folder and select All Tasks> Import.



- 13. Use the Certificate Import Wizard to import the PFX file that was previously created.
- 14. Retrieve the thumbprint of the imported PFX key.
 - a. Double-click on the imported PFX key.
 - b. On the **Certificate** window, go to the *Details* tab.
 - c. Scroll through the list of fields and click Thumbprint.

d. Copy the hexadecimal characters from the box. If this thumbprint is used in code for the x509FindType, remove the spaces between the hexadecimal numbers.

The GUID for the IDERA SQL Inventory Manager is "{af5a4e5f-435c-4333-ab2bcac62e140248}".

15. Run the Command Promt as an Administrator and delete existing bindings to the IDEA SQL Inventory Manager Rest Service port 9276, executing the following command:

```
netsh http delete ssl 0.0.0.0:9276
```

16. Run the Command Promt as an Administrator and bind the new PFX key by using the commands below.

```
netsh
http
add ssl ipport=0.0.0.0:9276 certhash=<thumbprint of the PFX key
(with spaces removed)> appid="{af5a4e5f-435c-4333-ab2b-
cac62e140248}" clientcertnegotiation=enable
```

17. You may create a BAT file to run on startup of Windows, and make sure the certificate is applied when the server starts up, if the service is restarted. The content of the BAT file is the following:

NET START SQLInventoryManagerRestService TIMEOUT /T 2 netsh http delete ssl 0.0.0.0:9276

netsh http add sslcert ipport=0.0.0.0:9276 certhash=<thumbprint of the PFX key (with spaces removed)> appid="{af5a4e5f-435c-4333-ab2b-cac62e140248}"

Configure the service to have a *Manual* start up so the BAT file will start the service.

	iy Manager Rest Service Properties (Eocar comput
General Log On	Recovery Dependencies
Service name:	SQLInventoryManagerRestService
Display name:	Idera SQL Inventory Manager Rest Service
Description:	Process requests from users created on web dashboard.
Path to executab "C:\Program File	ole: s\ldera\SQLInventoryManager\CollectionService\SQLInve
Startup type:	Manual ~
Service status:	Running
Service status: Start	Running Stop Pause Resume
Service status: Start You can specify from here.	Stop Pause Resume the start parameters that apply when you start the service
Service status: Start You can specify from here. Start parameters	Stop Pause Resume the start parameters that apply when you start the service

To add a certificate to the Trusted Root Certification Authorities store in Windows, refer to Manag e Trusted Root Certificates.

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