Binding certificates for distributed installations

These instructions are applied when SQLDM and Dashboard are installed on different servers. They are the continuation of the Resolving Dashboard certificate error message, which means the Dashboard certificate was already created.



Common Name

Under the Resolving Dashboard certificate error message instructions, verify that the certificate and the keystore keypair are created to have each server listed as a Common Name (Step 9).

If you have not installed KeyStore Explorer, download it, and install the application.

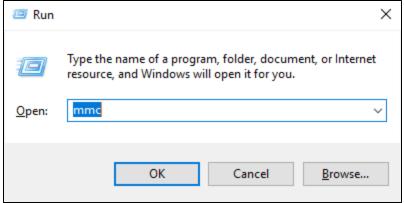
Dashboard and SQL Diagnostic Manager installed on different machines

This scenario considers that both products are installed on different servers:

- Dashboard is installed and is being accessed on <u>Server 1</u>.
- SQLDM Services are installed on <u>Server 2.</u>

Once your Dashboard certificate is created on Server 1, follow the steps below

1. Open the Microsoft Management Console (MMC) by selecting Run from the Start menu, enter "mmc", and click OK.



- 2. When the MMC window opens, click File from the menu toolbar, and select Add/Remove Snap-in...
- 3. The Add or Remove Snap-ins window opens, Add Certificates, and click OK.
- 4. Configure the steps of the Certificate snap-in wizard, and click Finish.
- 5. Close the Add or Remove Snap-in window by clicking OK.

6. Expand Certificates, right-click the Personal folder, select All Tasks, and click Import... Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates] 🝒 File Action View Favorites Window Help 🗢 🤿 | 🙇 🔐 📋 🗎 🖟 🔞 📳 Console Root Action Issued To Issued By Certificates (Local Computer) 🖫 ldera Inc Idera Inc Certificates 写 localhost localhost More Actions Certificates All Tasks Request New Certificate... ✓ III Trusted Root Ce Certificates Import... Enterprise Trust Advanced Operations Intermediate Co Trusted Publish New Taskpad View.. Untrusted Certi Refresh Third-Party Roc Trusted People Export List... Client Authenti Help Preview Build R Test Roots AAD Token Issuer eSIM Certification Authorities OEM eSIM Certification Authorities Passpoint Trusted Roots Remote Desktop Certificate Enrollment Requests

- 7. Import the . cer certificate under the Trusted Root Certificate Authorities folder on Server 2.
- 8. Import the .pfx certificate under the Personal folder on Server 2.
- 9. Retrieve the thumbprint of the imported PFX key.
 - a. Double-click the imported PFX key.
 - b. On the Certificate window, go to the Details tab.
 - c. Scroll down and click Thumbprint. You need to copy the characters from the box.



ontains actions that can be performed on the item

If the thumbprint has extra spaces between the hexadecimal numbers, remove them. For example, the thumbprint ""a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b" should be edited to ""a909502dd82ae41433e6f83886b00d 4277a32a7b".

- 10. Follow these last steps to bind the new PFX key by using the commands below:
 - a. Open CMD as an Administrator and execute the following command to delete existing bindings to the IDERA SQL Diagnostic Manager Rest Service on Server 2:

netsh http delete ssl 0.0.0.0:5171

b. Bind the PFX key by using the following command in an elevated command prompt session on Server 2, GUID SQLDM: 0051d7ed-de72-46d3-ae44-97d566b1ca5a

netsh http add sslcert ipport=0.0.0.0:5171 certhash="<PFX key's thumbprint>" appid="{0051d7ed-de72-46d3ae44-97d566b1ca5a} " clientcertnegotiation=enable // Remove the spaces from the PFX Key's thumbprint

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