Apply an MS SQL Key to the ExtraHop System

You can apply an MS SQL key to parse encrypted logins in MS SQL databases. This guide includes the following procedures:

- Generate a certificate
- Export the certificate to PFX format
- Load the PFX file to the SQL server
- Apply the key to the ExtraHop system
- View the SQL database on the ExtraHop system

Windows Server 2008 R2 or later and Microsoft SQL Server 2008 R2 or later are required.

Generate a certificate

To complete the procedures in the following sections, you must generate a certificate. Refer to *Configuring Server Certificates in IIS 7* on microsoft.com for more information.

Export the certificate to PFX format

1. Open the Internet Information Services (IIS) Manager.
2. In the left panel, select the host containing the certificate.
3. Click the **Server Certificates** icon.
4. Select the certificate you want to use in the SQL server, on which the ExtraHop system will perform decryption.
5. In the right panel, click **Export** and navigate to the location on your workstation to store the PFX file.
6. Set a password and save the PFX file. The ExtraHop system will require the password later in this procedure.

Load the PFX file to the SQL server

1. Open the SQL Server Configuration Manager.
2. In the left panel, expand **SQL Server Network Configuration**.
3. Click **Protocols for MSSQLSERVER**.
4. On the **Flags** tab, ensure that the **Force Encryption** field is set to **No**.
5. Click the **Certificate** tab.
6. Click the **Certificate** drop-down list and select the certificate.
7. Click the **OK** button.
8. Restart the MSSQLSERVER service.

Apply the key to the ExtraHop system

1. Open the ExtraHop Admin UI.
2. Go to the **System Settings** section and click **License** to ensure SSL decryption is enabled. If SSL decryption is not enabled, contact ExtraHop Support for a license.
3. Return to the main Admin UI page, go to the **System Configuration** section, and click **Capture**.
4. Click **SSL Decryption**.
5. Click the **Add Keys** button.
6. In the **Add PKCS#12/PFX File with Password** section, enter a description in the **Description** field. This field is required.
7. Click **Choose File** and navigate the PFX file.
8. Enter the password to access the PFX file.

9. In the Admin UI, enter the password again in the **Password** field.
10. Click the **Add** button.
11. Verify the information and click the **OK** button.
12. (Optional) If this key is only for MS SQL decryption, go to the **Encrypted Protocols** section of the SSL Decryption Keys page and delete the HTTP entry to remove unnecessary CPU overhead to the ExtraHop system.
13. Go to the SQL Server Configuration Manager.
14. In the left panel, expand **SQL Server Network Configuration** and select **Protocols for MSSQLSERVER**.
15. Select the **TCP/IP** entry in the list.
16. In the **TCP/IP Properties** window, note the TCP port and click the **OK** button. The default TCP port is **1433**.

    If you want to implement another port, specify that number as the TCP port.

17. In the ExtraHop Admin UI, under the Encrypted Protocols section of the SSL Decryption Keys page, click **Add Protocol**.
18. On the **Add Encrypted Protocol** page, click the **Protocol** drop-down list and select the **MS SQL Protocol (tds)**.
19. Click the **Key** drop-down list and select the key that you created.
20. In the **Port** field, enter the TCP port number you noted in step 16.
21. Click the **Add** button.

(Optional) Configure a non-standard TCP port

1. If you implemented a non-standard TCP port, go to the **Capture Configuration** page and click **Protocol Classification**.
2. On the **Protocol Classification** page, click the **Add Protocol** button.
3. Click the **Name** drop-down list and select **MS SQL Server (tds)**, click the **Protocol** drop-down list and select **TCP**, and enter the destination port number.
4. Click the **Add** button.

View the SQL database on the ExtraHop system

1. Go to the ExtraHop Web UI.
2. In the top menu, click **Metrics**.
3. In the left panel, under **Sources**, click **Devices**.
4. On the **All Devices** page, search for the MS SQL server on which SSL decryption is performed and select it.
5. In the left panel, select **Database**.
6. Click the **Database** drop-down list and select the new database entry from the PFX file you loaded earlier.
7. Click the **Users** button to see the user who added the new database.