Apply an MS SQL key to the ExtraHop system

Published: 2024-04-02

The following procedures explain how to apply an MS SQL key to the ExtraHop system. After completing this procedure, you will be able to view all users associated with your databases and monitor their activity.

To complete this procedure, Windows Server 2008 R2 or later and Microsoft SQL Server 2008 R2 or later are required.

You should have experience administering the Internet Information Services (IIS) Manager and MS SQL server to complete these procedures.

Export the certificate to PFX format

Before you begin
To complete the procedures in the following sections, you must first generate a server certificate. For more information, see Configuring Server Certificates in IIS 7 on the Microsoft website.

1. Open the Internet Information Services (IIS) Manager.
2. From the left panel, select the host that contains the server certificate.
3. Click the **Server Certificates** icon.
4. Select the certificate for the SQL server that the ExtraHop system will perform decryption on.
5. From the right panel, click **Export** and browse to a location on your computer to store the PFX file.
6. Set a password and save the PFX file.

   Note: You will need this password for a later procedure in this guide.

Load the PFX file to the SQL server

1. Open the SQL Server Configuration Manager.
2. From the left panel, expand **SQL Server Network Configuration**.
3. Click **Protocols for MSSQLSERVER**.
4. Click the **Certificate** tab.
5. From the **Certificate** drop-down list, select the server certificate.
6. Click **OK**.
7. Restart the MSSQLSERVER service.

Apply a key to the ExtraHop system

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Appliance Settings section, click **License**.
3. In the Features section, verify that SSL decryption is enabled.
   If SSL decryption is disabled, contact ExtraHop Support for a license.
4. Return to the main Administration page.
5. In the System Configuration section, click **Capture**.
6. Click **SSL Decryption**.
7. Click **Add Keys**.

8. (Required) In the Add PKCS#12/PFX File with Password section, type a description in the Description field.
9. Click **Choose File** and navigate to the PFX file.
10. Type the password for the PFX file that you set earlier.
11. Type the password again in the Password field.
12. Click **Add**.
13. Verify the information and click **OK**.
14. Optional: If this key is only for MS SQL decryption, you can delete the entry for HTTP in the Encrypted Protocols section on the SSL Decryption Keys page.
    Removing the HTTP entry removes unnecessary CPU overhead to the ExtraHop system.
15. Open the SQL Server Configuration Manager.
16. In the left panel, expand SQL Server Network Configuration, and select **Protocols for MSSQLSERVER**.
17. Select **TCP/IP**.
18. In the TCP/IP Properties window, note the TCP port number, and then click **OK**. The default TCP port is 1433.

    Note: If you want to configure a different TCP port number, specify that number in this step. You must also complete the following procedure: (Optional) Configure a non-standard TCP port.
19. Return to the ExtraHop Administration settings, in the Encrypted Protocols section of the SSL Decryption Keys page, click **Add Protocol**.
20. On the Add Encrypted Protocol page, from the **Protocol** drop-down list, select **MS SQL Protocol (tds)**.
21. From the **Key** drop-down list, select the key that you created.
22. In the Port field, type the TCP port number you specified in the SQL Server Configuration Manager.
23. Click **Add**.

(Optional) Configure a non-standard TCP port

Complete the steps in this procedure if you modified the default TCP port in the previous procedure.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the System Configuration section, click **Capture**.
3. Click **Protocol Classification**.
4. Click **Add Protocol**.
5. From the **Name** drop-down list, select **MS SQL Server (tds)**.
6. From the **Protocol** drop-down list, select **TCP**.
7. In the Destination field, type the port number you configured earlier.
8. Click **Add**.

View the SQL database on the ExtraHop system

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click **Assets**, and then click **Devices** in the left panel.
3. From the device list, click the name of the MS SQL server that you added SSL decryption for.
4. In the left panel, select **Database**.
5. Hover your cursor over any top-level metric value (such as **Responses**), and select **By Database** from the drop-down list.

You can now view metrics for the SQL database that were previously obscured by SSL encryption.