Apply an MS SQL Key to the ExtraHop System

ExtraHop firmware version 3.10 and later enables you to use an MS SQL key in order to parse encrypted logins in MS SQL databases. This guide provides basic instructions for applying an MS SQL key and includes the following topics:

- Generating a Certificate
- Exporting the Certificate to PFX Format
- Loading the PFX file to the SQL Server
- Applying the Key to the ExtraHop System
- Viewing the SQL Database on the ExtraHop System

You must use Windows Server 2008 R2 and Microsoft SQL Server 2008 R2 and later to complete this procedure.

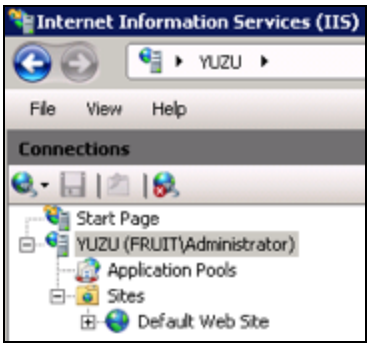
> In order to decrypt SQL logins, you must authenticate using SQL Server Authentication or NTLM Windows Authentication. Kerberos Windows Authentication is not supported.

Generating 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.

Exporting the Certificate to PFX Format

1. Open the Internet Information Services (IIS) Manager.
2. In the left panel, select the host containing the certificate.



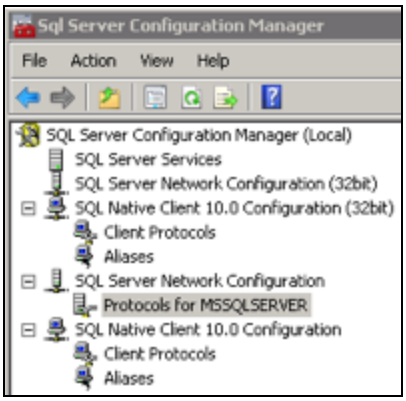
3. Click the **Server Certificates** icon.
4. Select the certificate you want to use in the SQL server, on which the ExtraHop system will perform decryption.

5. In the right panel, click **Export** and navigate to the location on your workstation to store the PFX file.

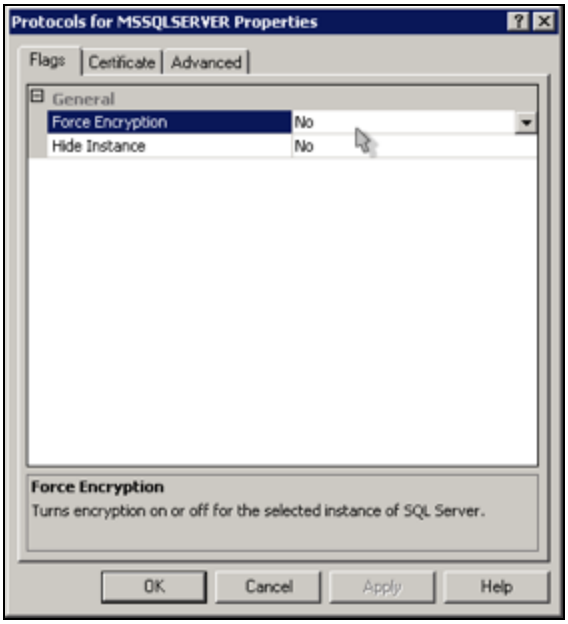
6. Set a password and save the PFX file. The ExtraHop system will require the password later in this procedure.

Loading the PFX file to the SQL Server

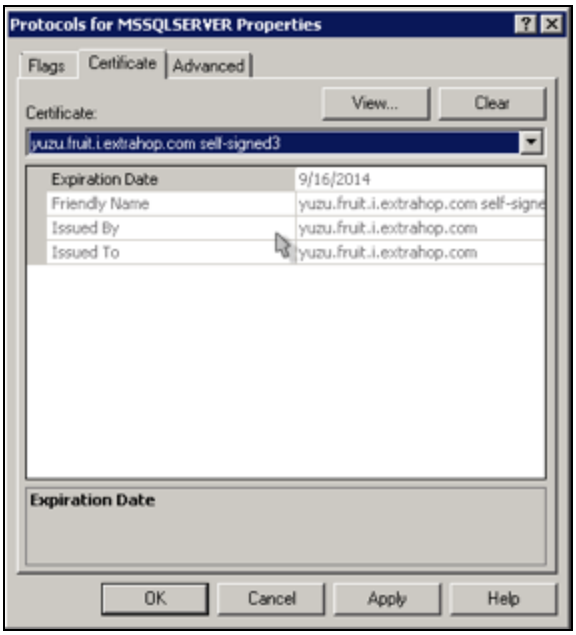
1. Open the SQL Server Configuration Manager.
2. In the left panel, expand **SQL Server Network Configuration**.
3. Click **Protocols for MSSQLSERVER**.



4. On the **Flags** tab, ensure that the **Force Encryption** field is set to **No**.



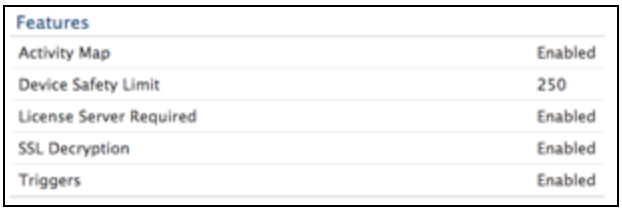
5. Click the **Certificate** tab.
6. Click the **Certificate** drop-down list and select the certificate you want to use.



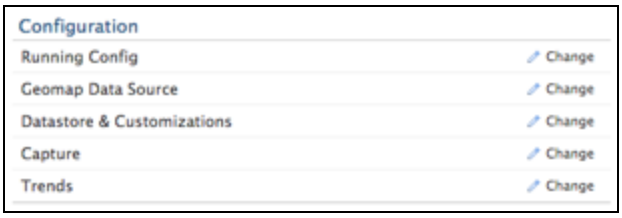
7. Click **OK**.
8. Restart the MSSQLSERVER service.

Applying the Key to the ExtraHop System

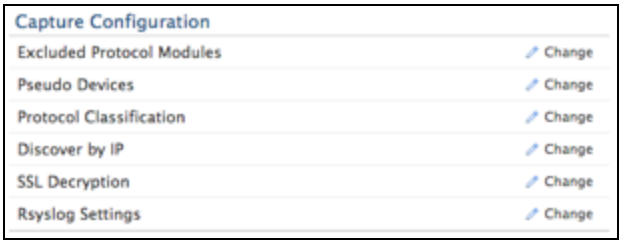
1. Open the ExtraHop Admin UI.
2. Go to the **System Settings** section and click **License** to ensure SSL decryption is enabled. If SSL decryption is not enabled, contact ExtraHop Support for a license.



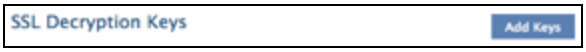
3. Return to the main Admin UI page, go to the **Configuration** section, and click **Capture**.



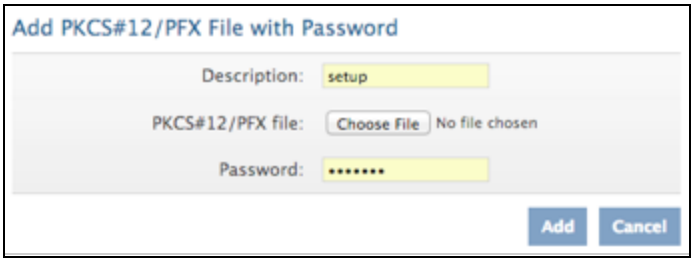
4. Click **SSL Decryption**.



5. Click the **Add Keys** button.

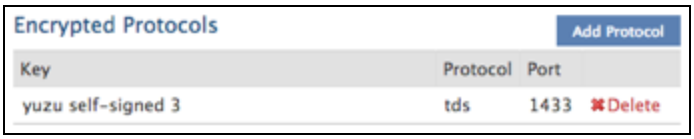


6. In the **Add PKCS#12/PFX File with Password** section, enter a meaningful description in the **Description** field.

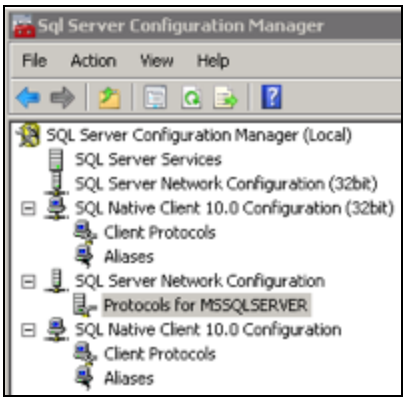


7. Click **Choose File** and navigate the PFX file.
8. Enter the password to access the PFX file.

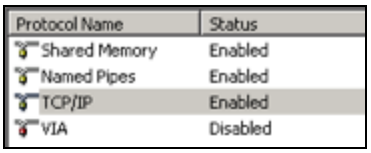
9. In the Admin UI, enter the password again in the **Password** field.
10. Click the **Add** button.
11. Verify the information and click **OK**.
12. (Optional) If this key will be used only for MS SQL decryption, go to **Encrypted Protocols** section and delete the HTTP entry to remove unnecessary CPU overhead to the ExtraHop system.



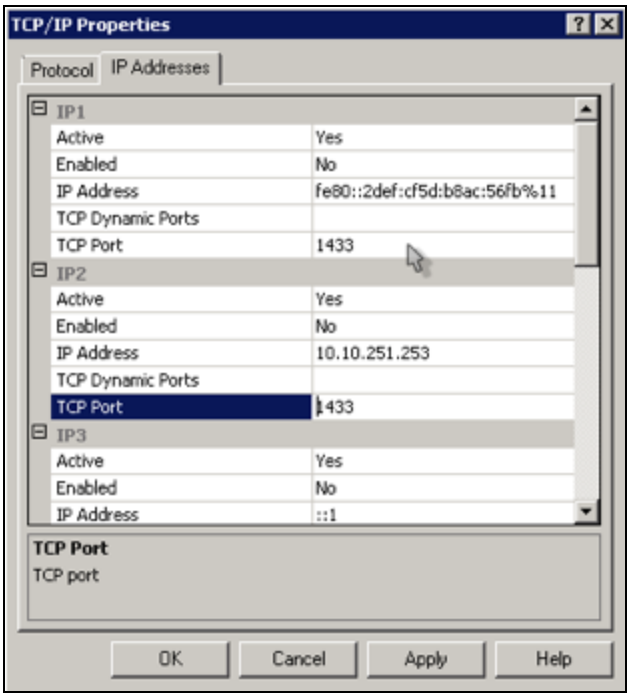
13. Go to the SQL Server Configuration Manager.
14. In the left panel, expand **SQL Server Network Configuration** and select **Protocols for MSSQLSERVER**.



15. Select the **TCP/IP** entry in the list.

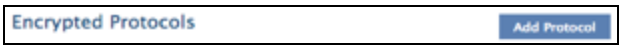


16. In the **TCP/IP Properties** window, note the TCP port and click **OK**. The default TCP port is **1433**.



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

17. In the ExtraHop Admin UI, click the **Add Protocol** button.

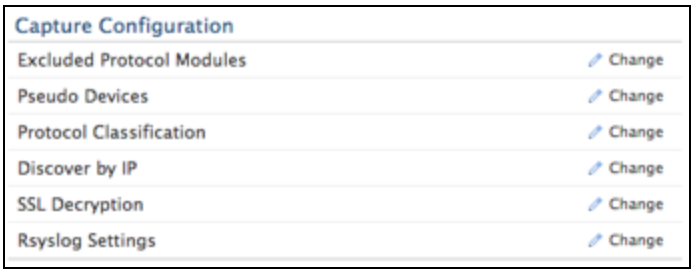


18. On the **Add Encrypted Protocol** page, click the **Protocol** drop-down list and select the **MS SQL Protocol (tds)**.

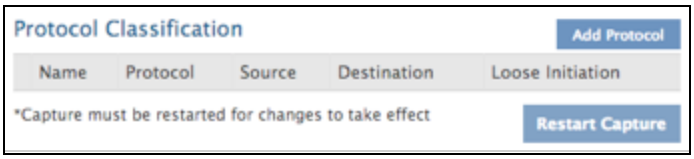
19. Click the **Key** drop-down list and select the key that you created.
20. In the **Port** field, enter the TCP port number you noted in step 16.
21. Click the **Add** button.

(Optional) Using a Non-Standard TCP Port

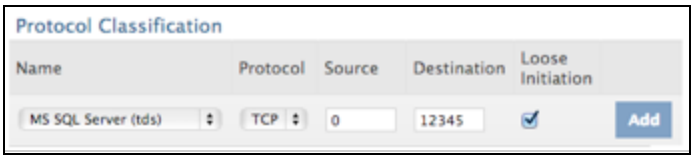
1. If you are using a non-standard TCP port, go to the **Capture Configuration** page and click **Protocol Classification**.



2. On the Protocol Classification page, click the **Add Protocol** button.



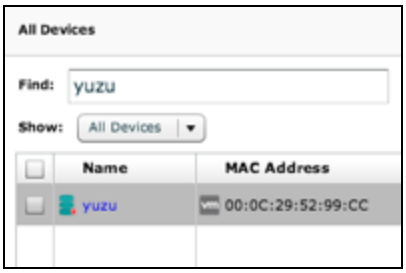
3. Click the **Name** drop-down list and select **MS SQL Server (tds)**, click the **Protocol** drop-down list and select **TCP**, and enter the destination port number.



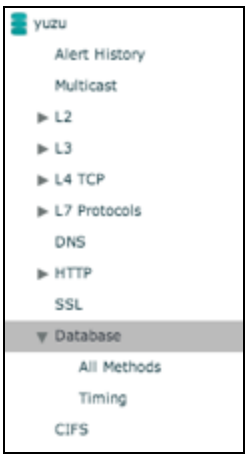
4. Click **Add**.

Viewing the SQL Database on the ExtraHop System

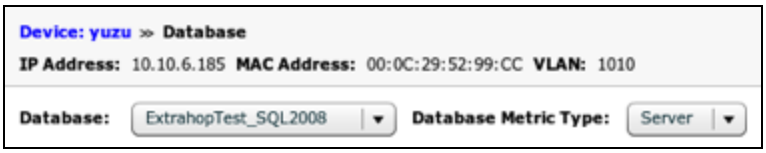
1. Go to the ExtraHop Web UI.
2. In the left panel, click **Devices**.
3. On the **All Devices** page, search for the MS SQL server on which SSL decryption is performed and select it.



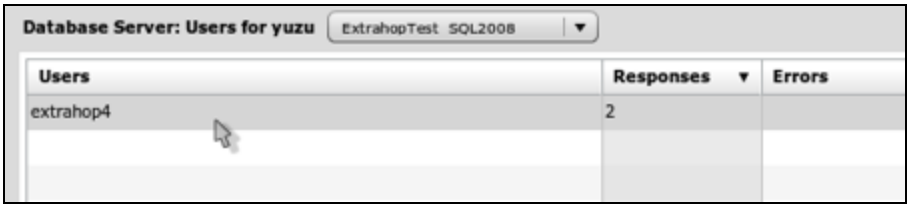
4. In the left panel, select **Database**.



5. Click the **Database** drop-down list and select the new database entry from the PFX filed you loaded earlier.



6. Click the **Users** button to see the user who added the new database.



This example shows database *ExtrahopTest_SQL2008* and user *extrahop4*.