Establishing a secure connection

between Exchange Reporter Plus and MS SQL

ManageEngine

Exchange Reporter Plus

Document summary

Exchange Reporter Plus supports an external MS SQL database in addition to the bundled PostgreSQL database. This document is intended for admins who want to secure the connection between their MS SQL database and Exchange Reporter Plus with an SSL certificate. By applying an SSL certificate in the MS SQL server, you can ensure that the data transferred between Exchange Reporter Plus and the SQL server is encrypted and stays secure during transmission.

Note: This guide is for users who have already migrated to MS SQL database. In case you are using a PostgreSQL or MySQL database make sure to migrate to a MS SQL server first.

Prerequisites

- ✓ You'll need a valid SSL certificate in PFX format that isn't expiring soon. If you have a certificate in another format, please convert it to a PFX file. To create a self-signed certificate using IIS, follow the steps mentioned here.

- ✓ The **Common Name** in the subject field of the certificate must be the same as the fully qualified domain name (FQDN) of the machine in which MS SQL Server is installed.

- ✓ The certificate must be issued for server authentication, so the Enhanced Key Usage property of the certificate should include **Server Authentication (1.3.6.1.5.5.7.3.1).**

Steps to check whether your certificate meets these requirements are listed here.

Important: If you've already applied a valid SSL certificate (matching the requirements under *Prerequisites*) in your SQL server, you can start on Step 3.

Step 1

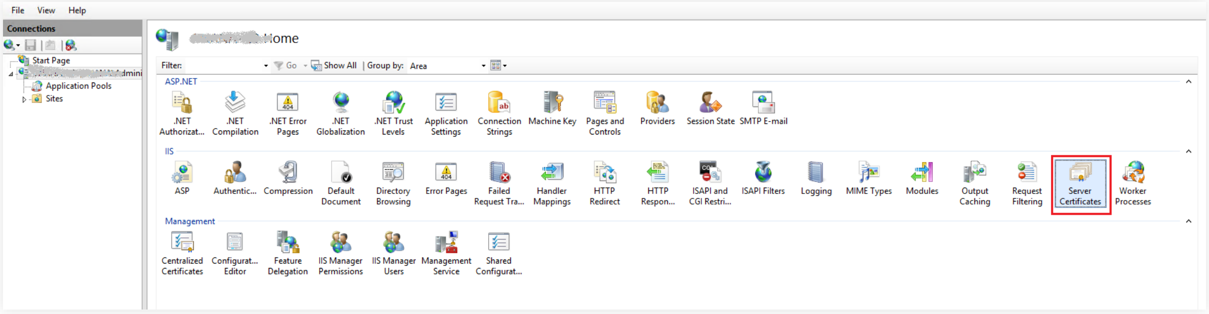
Importing the certificate to the certificate store

If you’re using a self-signed SSL certificate generated using Internet Information Services (IIS) Manager, you can start on Step 2.

If you’re using a certificate generated through other modes, then you must first import it to the certificate store in SQL Server. You can import the certificate using either IIS Manager or the Microsoft Management Console (MMC) snap-in.

Importing the certificate using IIS Manager

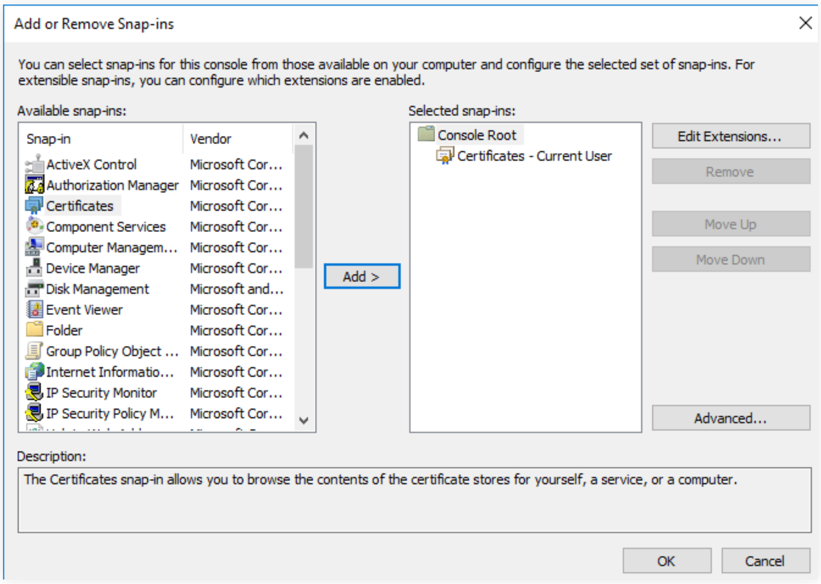
1. Open **IIS Manager.**
2. Click the name of the server in the Connections column in the left pane. In the middle row of icons, double-click **Server Certificates.**



3. Click **Import** in the *Actions* pane.
4. Browse and select the **PFX certificate file.**
5. Enter the **password** that you used while generating the certificate file.
6. Click **OK.**

Importing the certificate using MMC

1. Open **MMC.**
2. From the *File* menu, click **Add or Remove Snap-in.**
3. Select **Certificates**, then click **Add.**


Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
Internet Informatio...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...

Selected snap-ins:

Console Root
Certificates - Current User

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

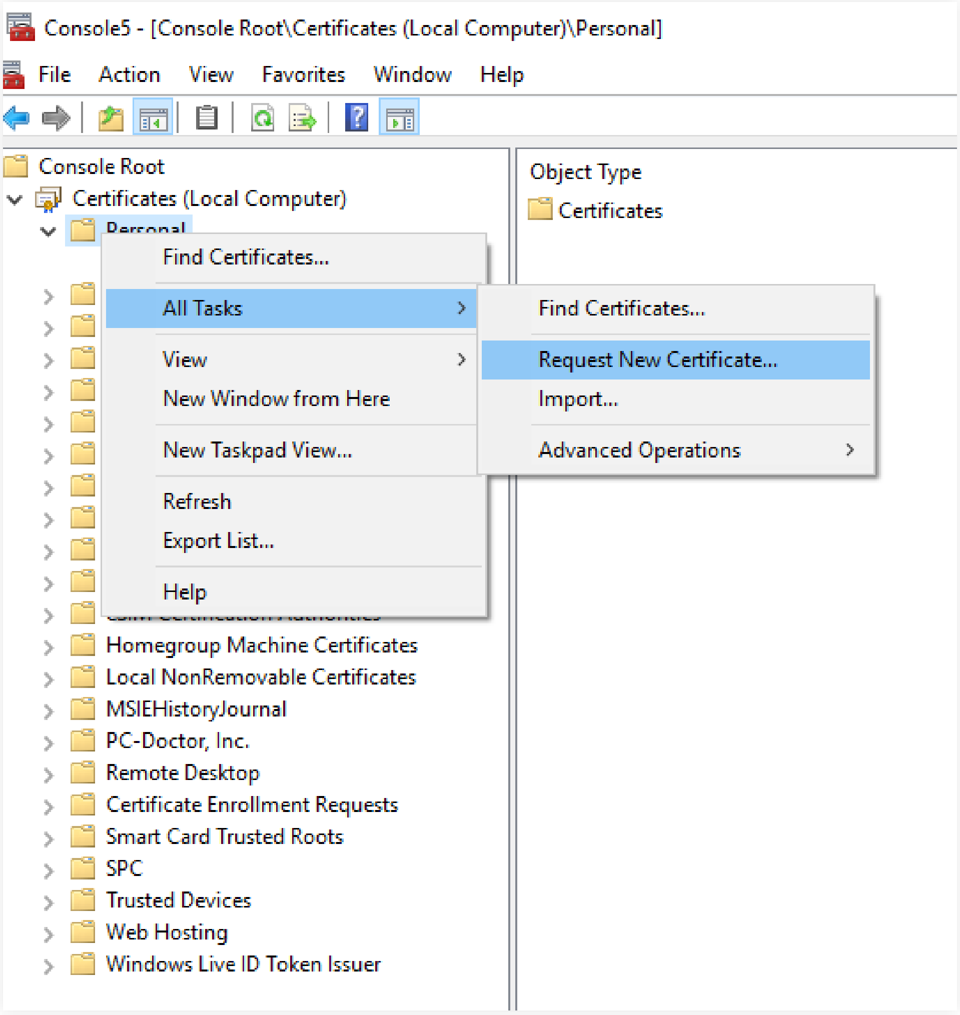
4. You'll be prompted to open the snap-in for your user account, the service account, or the computer account. Select the **Computer Account.**

5. Select **Local computer,** then click **Finish.**

6. Click **OK** to exit the **Add or Remove Snap-ins** window.

7. Back in MMC, double-click **Certificates (Local Computer)** to expand the tree view.

8. Right-click **Personal,** then select **All Tasks > Request New Certificate....**



9. Click **Next** in the *Certificate Request Wizard* that opens.

10. Select **Computer** as the certificate type.

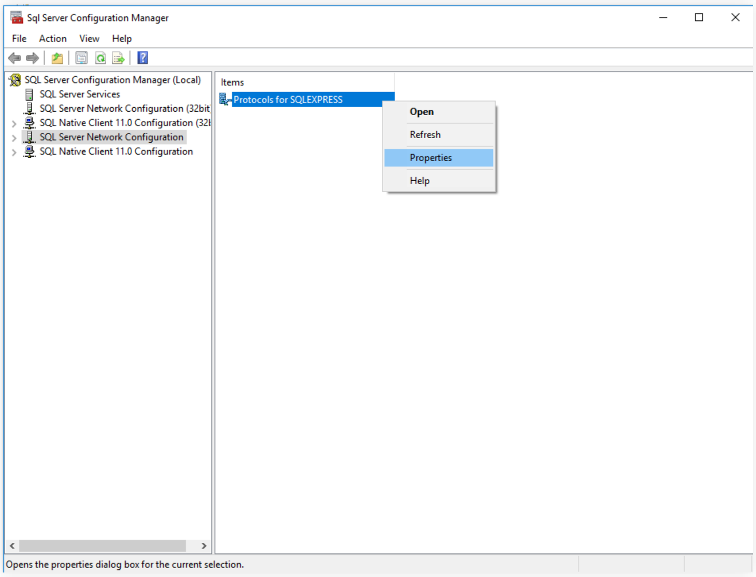
11. You can either enter a name in text box or leave it blank. Then complete the wizard by clicking **Enroll** and **Finish.**

Step 2

Associating the certificate with MS SQL Server

1. Open **SQL Server Configuration Manager.**

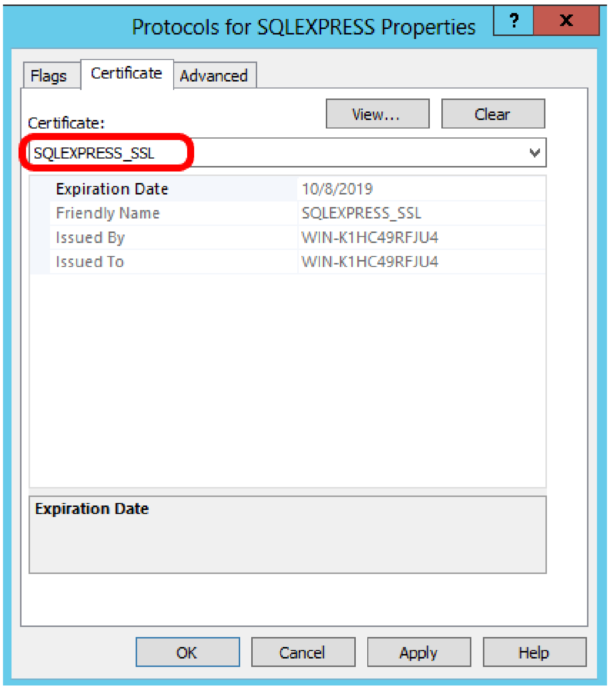
2. Expand **SQL Server Network Configuration** and right-click **Protocols** for the MS SQL Server instance that you want to associate with the certificate. Click **Properties.**


Sql Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit
SQL Native Client 11.0 Configuration (32l
SQL Server Network Configuration
SQL Native Client 11.0 Configuration
Items
Protocols for SQLEXPRESS
Open
Refresh
Properties
Help

Opens the properties dialog box for the current selection.

3. On the *Flags* tab, select **Yes** in the **Force Encryption** box.

4. On the *Certificate* tab, select the certificate you want to use.



Certificate: SQLEXPRESS_SSL

Expiration Date	10/8/2019
Friendly Name	SQLEXPRESS_SSL
Issued By	WIN-K1HC49RFJU4
Issued To	WIN-K1HC49RFJU4

5. Click **OK.**

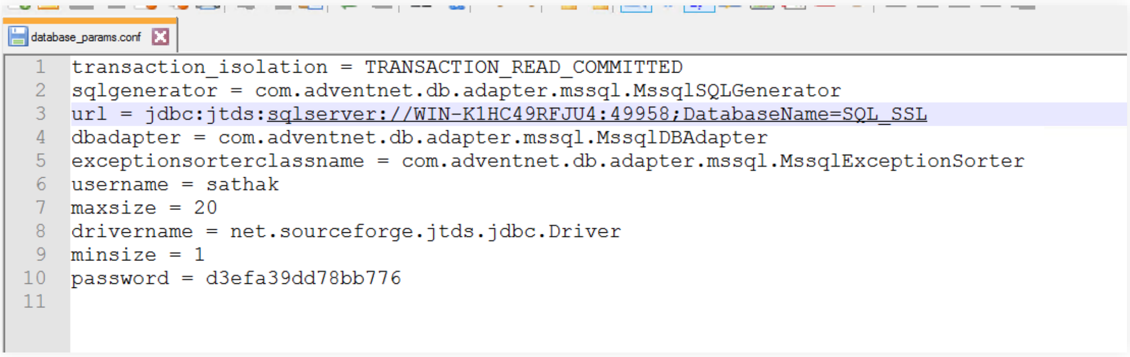
6. Restart SQL Server.

Step 3

Configuring Exchange Reporter Plus

After associating the certificate with SQL Server, you need to configure Exchange Reporter Plus to use the secure connection to the database. Follow the steps below:

1. Go to the Exchange Reporter Plus home folder (*<install_dir>\conf*) and open the *database_params.conf* file in a text editor. By default, the installation path is C:\ManageEngine\Exchange Reporter Plus. Here you will see a list of entries such as **login, password, and url.**



```
transaction_isolation = TRANSACTION_READ_COMMITTED
sqlgenerator = com.adventnet.db.adapter.mssql.MssqlSQLGenerator
url = jdbc:jtds:sqlserver://WIN-K1HC49RFJU4:49958;DatabaseName=SQL_SSL
dbadapter = com.adventnet.db.adapter.mssql.MssqlDBAdapter
exceptionsorterclassname = com.adventnet.db.adapter.mssql.MssqlExceptionSorter
username = sathak
maxsize = 20
drivername = net.sourceforge.jtds.jdbc.Driver
minsize = 1
password = d3efa39dd78bb776

```

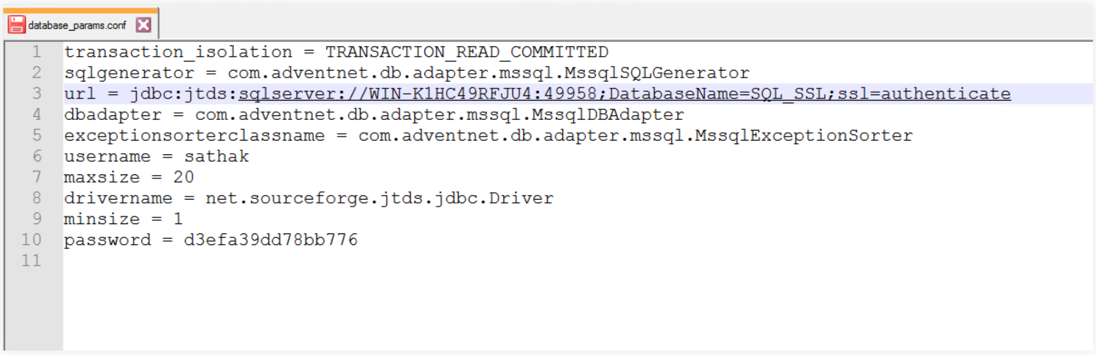
2. Under the url entry, append **ssl=authenticate** to the URL value.

   For example, if the existing entry is:

   url=jdbc:jtds:sqlserver://WIN-K1HC49RFJU4:49958;DatabaseName=SQL_SSL

   Then change it to:

   url=jdbc:jtds:sqlserver://WIN-K1HC49RFJU4:49958;DatabaseName=SQL_SSL;**ssl=authenticate**



```
transaction_isolation = TRANSACTION_READ_COMMITTED
sqlgenerator = com.adventnet.db.adapter.mssql.MssqlSQLGenerator
url = jdbc:jtds:sqlserver://WIN-K1HC49RFJU4:49958;DatabaseName=SQL_SSL;ssl=authenticate
dbadapter = com.adventnet.db.adapter.mssql.MssqlDBAdapter
exceptionsorterclassname = com.adventnet.db.adapter.mssql.MssqlExceptionSorter
username = sathak
maxsize = 20
drivername = net.sourceforge.jtds.jdbc.Driver
minsize = 1
password = d3efa39dd78bb776

```

3. In the same conf folder, open **wrapper.conf** in a text editor.

4. Search for **wrapper.java.additional.** You'll get a list of entries that are numbered starting from 1.

5. Add the line below after the last wrapper.java.additional entry.

   "wrapper.java.additional.xx=-Djsse.enableCBCProtection=false"

   Here **xx** denotes the next value to the preceding line's integer.

   For example:

   wrapper.java.additional.1=-Dcatalina.home=..

   wrapper.java.additional.2=-Dserver.home=..

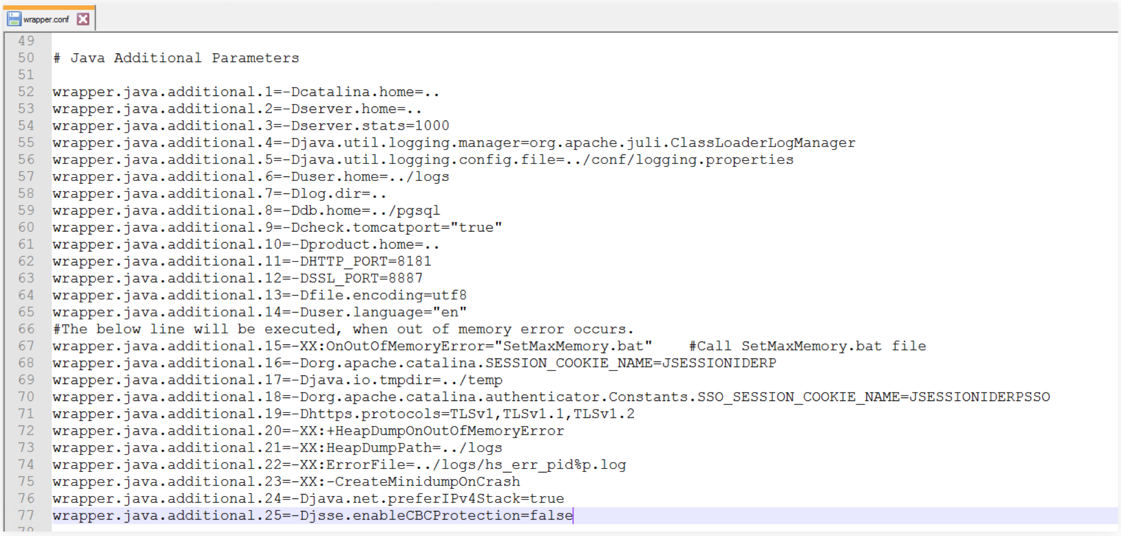
   wrapper.java.additional.3=-Dserver.stats=1000

   ...

   ...

   wrapper.java.additional.12=-DSSL_PORT=8887

   wrapper.java.additional.13=-Djsse.enableCBCProtection=false



```

# Java Additional Parameters

wrapper.java.additional.1=-Dcatalina.home=..
wrapper.java.additional.2=-Dserver.home=..
wrapper.java.additional.3=-Dserver.stats=1000
wrapper.java.additional.4=-Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
wrapper.java.additional.5=-Djava.util.logging.config.file=../conf/logging.properties
wrapper.java.additional.6=-Duser.home=../logs
wrapper.java.additional.7=-Dlog.dir=..
wrapper.java.additional.8=-Ddb.home=../pgsql
wrapper.java.additional.9=-Dcheck.tomcatport="true"
wrapper.java.additional.10=-Dproduct.home=..
wrapper.java.additional.11=-DHTTP_PORT=8181
wrapper.java.additional.12=-DSSL_PORT=8887
wrapper.java.additional.13=-Dfile.encoding=utf8
wrapper.java.additional.14=-Duser.language="en"
#The below line will be executed, when out of memory error occurs.
wrapper.java.additional.15=-XX:OnOutOfMemoryError="SetMaxMemory.bat"    #Call SetMaxMemory.bat file
wrapper.java.additional.16=-Dorg.apache.catalina.SESSION_COOKIE_NAME=JSESSIONIDERP
wrapper.java.additional.17=-Djava.io.tmpdir=../temp
wrapper.java.additional.18=-Dorg.apache.catalina.authenticator.Constants.SSO_SESSION_COOKIE_NAME=JSESSIONIDERPSSO
wrapper.java.additional.19=-Dhttps.protocols=TLSv1,TLSv1.1,TLSv1.2
wrapper.java.additional.20=-XX:+HeapDumpOnOutOfMemoryError
wrapper.java.additional.21=-XX:HeapDumpPath=../logs
wrapper.java.additional.22=-XX:ErrorFile=../logs/hs_err_pid%p.log
wrapper.java.additional.23=-XX:-CreateMinidumpOnCrash
wrapper.java.additional.24=-Djava.net.preferIPv4Stack=true
wrapper.java.additional.25=-Djsse.enableCBCProtection=false
```

6. Restart Exchange Reporter Plus for the changes to take effect.

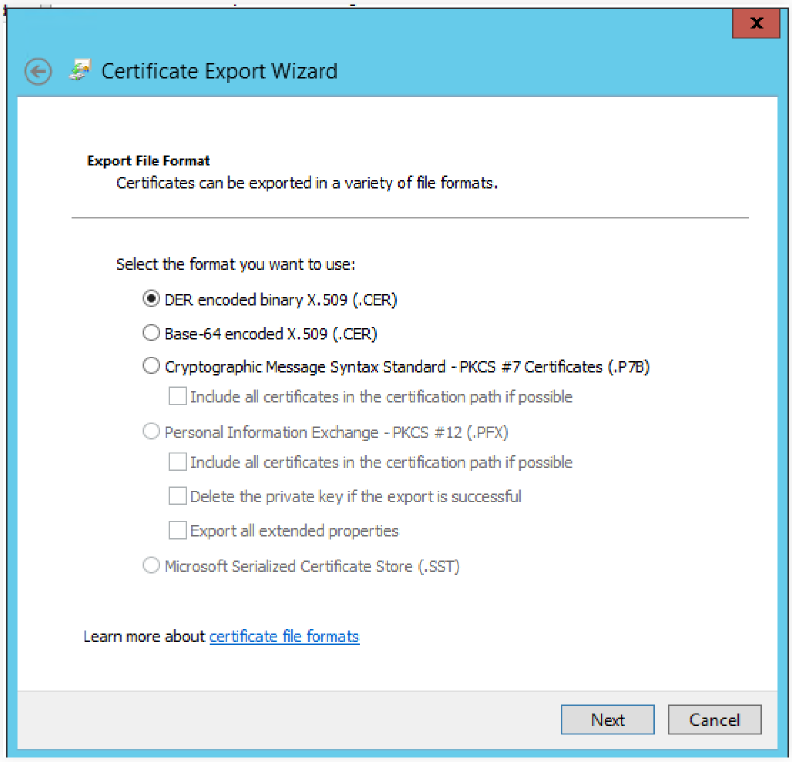
Step 4

Associating the certificate with the Java KeyStore

You need to associate the certificate with the Exchange Reporter Plus Java KeyStore to establish trust.

Follow the steps below on the machine in which Exchange Reporter Plus is installed:

1. Open **IIS Manager.**
2. In the middle pane, click **Server Certificates.**
3. Open the certificate you want to use.
4. Click the **Details** tab.
5. Click **Copy to file.**
6. Click **Next** in the *Certificate Export Wizard* that opens.
7. On the *Export Private Key* screen, select **No, do not export the private key,** and click **Next.**
8. On the *Export File Format* screen, select either **DER encoded binary X.509 (.CER)** or **Base-64 encoded X.509 (.CER)**, and click **Next.**



Export File Format
Certificates can be exported in a variety of file formats.

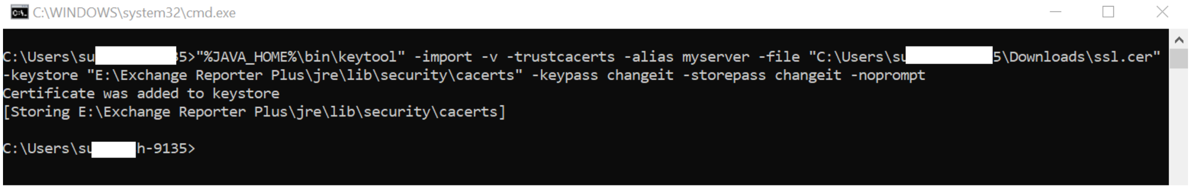
Select the format you want to use:

● DER encoded binary X.509 (.CER)
○ Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
□ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
□ Include all certificates in the certification path if possible
□ Delete the private key if the export is successful
□ Export all extended properties
○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

9. Enter a name for the file, then click **Next.**
10. Click **Finish.**
11. Use the command below to associate the certificate with the Java KeyStore:

```
“%JAVA_HOME%\bin\keytool" -import -v -trustcacerts -alias  myserver -file ssl.cer -keystore
"%JAVA_HOME%\lib\security\cacerts" -keypass changeit -storepass changeit -noprompt
```



C:\WINDOWS\system32\cmd.exe

```
C:\Users\su[redacted]5>"%JAVA_HOME%\bin\keytool" -import -v -trustcacerts -alias myserver -file "C:\Users\su[redacted]5\Downloads\ssl.cer"
-keystore "E:\Exchange Reporter Plus\jre\lib\security\cacerts" -keypass changeit -storepass changeit -noprompt
Certificate was added to keystore
[Storing E:\Exchange Reporter Plus\jre\lib\security\cacerts]

C:\Users\su[redacted]h-9135>
```

Appendix

SSL encryption for failover clustering in SQL Server

If you'd like to use encrypted connections in a clustered environment, you should have a certificate issued to the fully qualified DNS name of the failover clustered instance. This certificate should also be installed on all of the nodes in the failover cluster. Additionally, you'll have to edit the thumbprint of the certificate in the registry because it's set to Null in a clustered environment.

The following steps should be performed on all of the nodes in the cluster:

1. Open the **certificate** using the **MMC Certificates Snap-in.**
2. Copy the **hex value** from the **Thumbprint property** on the *Details* tab to Notepad, and remove the spaces.
3. Start **regedit** and copy the **hex value** to this key: *HKLM\SOFTWARE\Microsoft\Microsoft SQL Server\<YourSQLServerInstance>\MSSQLServer\SuperSocketNetLib\Certificate.*
4. You'll now have to reboot your node, so it's recommended that you failover to another node first.
5. Repeat this procedure on all nodes.

Creating self-signed certificates using IIS

1. Open **IIS Manager.**
2. Click the **server name** in the *Connections* column in the left pane.
3. Double-click **Server Certificates** in the middle pane.
4. Click **Create Self-Signed Certificate** in the Actions column on the right.
5. Enter a name, then click **OK** to proceed.
6. Click **OK.**

You should now see that the **SSL** certificate is valid for one year.

Checking for SSL certificate validity

1. Open **MMC.**
2. On the *File* menu, click **Add or Remove Snap-in.**
3. Select **Certificates** and click **Add.**
4. You will be prompted to open the snap-in for your user account, the service account, or the computer account. Select the **Computer Account.**
5. Select **Local computer,** then click **Finish.**
6. Click **OK** to exit the **Add or Remove Snap-ins** window.
7. Back in MMC, open the **Certificates** snap-in.
8. Double-click **Personal**, then click **Certificates.**
9. In the right pane, locate the **certificate** you're going to use.
10. The value for the **Intended Purpose** column must be **Server Authentication.**
11. The value for the **Issued To** column must be the **server name.**
12. Double-click the **certificate** to view its properties.
13. Under the *General* tab, you should be able to view this message: **You have a private key that corresponds to this certificate.**
14. Under the *Details* tab, the value of the Subject field must be the server name.
15. The value for the **Enhanced Key Usage** field must be **Server Authentication (1.3.6.1.5.5.7.3.1).**
16. Under the *Certificate Path* tab, the **server nam**e must appear under the certification path.

What is Exchange Reporter Plus?

Exchange Reporter Plus is a reporting, change auditing, monitoring, and content search tool for the hybrid Exchange environment and Skype for Business. It features over 450 comprehensive reports on various Exchange objects, such as mailboxes, public folders, and distribution lists, and also on Outlook Web Access and ActiveSync. Configure alerts in Exchange Reporter Plus for instant notifications on critical changes that require your immediate attention.