ManageEngine
Exchange
Reporter Plus
Powering IT ahead

Exchange Reporter Plus
SSL Configuration Guide

Table of contents

Necessity of a SSL guide

The purpose behind this document is to help you configure Exchange Reporter Plus for SSL certification. SSL certification protects all the sensitive information sent between users' browser and Exchange Reporter Plus server by encrypting and transmitting the information through a secure channel. This document can help you with the following:

- Overview of Exchange Reporter Plus
- Need for SSL certification
- Steps to enable SSL certification

Overview of Exchange Reporter Plus

Exchange Reporter Plus is a web-based Exchange reporting solution with more than 100 reports on all the Exchange system components like

- Exchange Mailboxes
- Email Traffic
- Outlook Web Access Usage
- Distribution Lists
- Public Folders
- Exchange Information Stores
- Exchange Organization

These reports collect all the vital data from data sources like Active Directory, Exchange Servers, Message Tracking logs, IIS logs and consolidate them into simple reports with graphs and charts.

Why is SSL certification needed?

Exchange Reporter Plus is a web-based software thus making it available even for on-the-fly access. The very purpose behind on-the-fly access is lost when there are chances of data transmitted between the browser and the server being compromised. SSL is the standard security technology on the web for establishing an encrypted secure channel for communication between the browsers and the servers.

Steps for enabling SSL

To configure SSL in Exchange Reporter Plus, the following steps can be followed.

1. Login to Exchange Reporter Plus with admin credentials
2. Go to Admin -> Configurations -> Product Settings
3. Under Connection Settings, click 'Enable SSL Port [https]' checkbox and 'Save' the settings.
4. Restart Exchange Reporter Plus.

Certificate Request Process

Tomcat specific ".keystore" and ".csr" files need to be created before requesting certificates from a certifying authority.

To create .keystore file

1. Open the command prompt
2. Browse to the <installation directory>\jre\bin folder and execute the below command

keytool -genkey -alias tomcat -keypass <your key password> -keyalg RSA -validity 1000 -keystore <keystore_name>.keystore

Note

- After executing the above query , you will be prompted with the following questions.
    a. Enter keystore password.(Try giving the password same as your key password and use plain characters.)
    b. What is your first and last name? (You can either provide the machine name hosting Exchange Reporter Plus application or FQDN here.)
    c. What is the name of your organizational unit?
    d. What is the name of your organization?
    e. What is the name of your City or Locality?
    f. What is the name of your State or Province?
    g. What is the two-letter country code for this unit?

    Finally acknowledge if the entered information is correct or not for the keystore file to be created.

To create .csr (Certificate Signing Request) file

1. Open the command prompt
2. Browse to the <installation directory>\jre\bin folder and execute the below command

keytool -certreq -alias tomcat -keyalg RSA -keystore < keystore_name >.keystore -file <csr_name>.csr

- The .csr file is temporary and should be submitted to the Certifying Authority (CA) to receive CA-singed certificate files.

Request for certificate from Microsoft Certificate Services (internal CA):

The .csr file created is submitted to the certifying authority to receive a CA-singed certificate file. Follow the steps below to submit the file to the CA

1. Connect to Microsoft Certificate Services and click on “Request a certificate” link.
2. Click on “Advanced Certificate Request”
3. Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file
4. Open the “.csr” file using an editor, copy the content and paste it under “Saved Request”
5. Select “Web Server” as “Certificate Template”
6. Click on “Submit” button.
7. The certificate will be issued and click on “Download certificate chain” link to download “PKCS #7 Certificates” types. The downloaded file name should be defined as (certnew.p7b)

Note: Copy and paste the certificate file under “<installation directory>\jre\bin” folder.

8. Click on the “Home” link on the top right hand side corner and click on “Download a CA certificate, chain Certificate or CRL” link to download the CA root certificate.
9. Click on “Download CA certificate” link and save the root certificate. The downloaded file name should be defined as (certnew.cer).

Note: Copy and paste the certificate file under “<installation directory>\jre\bin” folder.

10. Browse to “<installation directory>\jre\bin” location using command prompt to import the internal CA certificate into “**.**keystore” file.
11. Execute the below provided query to import the certificate into “**.**keystore” file.

Keytool –import –trustcacerts –alias tomcat –file certnew.p7b –keystore <keystore_name >.keystore

12. Add your internal CA's root certificate to the list of trusted CAs in the Java cacerts file.
13. Execute the below provided query to add the root certificate into trusted CA list of Java file.

keytool -import -alias <internal CA_name> -keystore ..\lib\security\cacerts -file certnew.cer

Note: Open the "certnew.cer" to get the internal CA name and provide the password as "changeit" when it is prompted.

Associating the certificate with Exchange Reporter Plus

This will configure the Exchange Reporter Plus server to use the keystore with your SSL certificate. To configure Exchange reporter Plus, follow the below steps.

1. Copy the .keystore from "<installation directory>\jre\bin" to "<installation directory> \ conf" folder.
2. Open "server.xml" file located at "<installation directory> \ conf" folder. Take a backup of the "server.xml" file before editing.
3. Replace the value of "keystoreFile" to "**.**/conf/<keystore_name>.keystore" at the last Connector tag (End of the page).
4. Replace the password for "keystorePass" to "password as given while creating keystore".
5. Save the server.xml file and close it.
6. Start Exchange Reporter Plus and connect to a browser.

If you are able to view the Exchange Reporter Plus login console without any warning from the browser, you have successfully installed your SSL certificate in Exchange Reporter Plus!

Glossary

Certifying Authority
An organization that verifies the legitimacy and identity of a company or an individual and issues a digital certificate.

CSR file
Certificate Signing Request file initiated with a certificate provider during certificate generation process. The information of the applicant is contained in the file in an encrypted way.

Keystore
A key database file containing cryptographic entries.

genkey
A command used to generate a new keystore.

alias
Alias is a unique keystore entry.

keypass
A password to protect the private key of the generated key pair.

storepass
A password to protect the integrity of the keystore.

keyalg
Specifies the algorithm to be used to generate the key pair.

Validity
The number of days for which the certificate should be considered valid.