How to install an **SSL certificate** in RecoveryManager Plus

ManageEngine
RecoveryManager Plus

STEP 1 Enable SSL in the RecoveryManager Plus client

1. Log in to RecoveryManager Plus.
2. Navigate to **Admin tab > General Settings > Connection.**
3. Check the **Enable SSL Port** option. The port number 8558 is entered by default. You can change it to a value of your choice.
4. Click Save Changes and restart the product for the changes to take effect.

STEP 2 Create a Certificate Signing Request (CSR)

1. Stop RecoveryManager Plus (Start ⟶ All Programs ⟶ RecoveryManager Plus ⟶ Stop RecoveryManager Plus)
2. Open command prompt and navigate to <installation_directory>\ManageEngine\RecoveryManager Plus\jre\bin where <installation_directory> is where RecoveryManager Plus is installed.
3. Execute the following command to create a Keystore.

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

   <key password> is a password of your choice and <domainName> is the name of your domain.
4. Type in your Keystore password. To avoid any confusion, try giving the same password as your 'keypass'.

   You will be prompted to answer the following questions:

What is your first name and last name?	Enter the NetBIOS or FQDN of the server in which RecoveryManager Plus is configured.
What is the name of your Organizational Unit?	Enter the name of the OU of your choice.
What is the name of your organization?	Provide the legal name of your organization.
What is the name of your city or locality?	Enter the city or locality name as provided in your organization's registered address.
What is the name of your state or province?	Enter the name of your state or province as provided in your organization's registered address.
What is the two-letter country code for this unit?	Provide the two-letter code of the country your organization is located in.

5. In the same path, execute the following command to create a CSR with Subject Alternative Name (SAN).

```
keytool -certreq -alias tomcat -keyalg RSA -ext SAN=dns:server_name,dns:server_name.domain.com,dns:server_name.domain1.com -keystore <domainName>.keystore -file <domainName>.csr
```

<domainName> is the name of your domain and provide the appropriate Subject Alternatives Names.

STEP 3 Issue the SSL certificate

1. **Issue the SSL certificate using an internal CA.**

   An internal CA is a member server or domain controller in a specific domain that has been assigned the role of a CA.

   i Connect to the Microsoft Certificate Services of your internal CA and click on the Request a certificate link.

   Microsoft request a certificate

   ii Click on 'Advanced certificate request' and select the Submit a certificate 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 option.

   Advanced certificate request

   iii Copy the content from your '.csr' file and paste it under the Saved Request field.

   iv Select the Web Server as the Certificate Template and click Submit.
   Submit a certificate request or renewal request

   v Click on the Download Certificate Chain link to download the issued 'PKCS #7 Certificates' types. The downloaded certificate will be of the p7b file format.

   vi Copy and paste this '.p7b' file at the <installation_directory>\ManageEngine\RecoveryManager Plus\jre\bin location.

   vii Return to the Microsoft Certificate Services and click on the Home link at the top-right corner of the page.

   viii Click on the Download a CA certificate, chain certificate or CRL link to download the CA root certificate.

ix Click on the Download CA certificate link to download and save the root certificate that is in the '.cer' format.

x Copy and paste the '.cer' file at the <installation_directory>\ManageEngine\ RecoveryManager Plus\jre\bin location.

xi Open the command prompt and navigate to the **<installation_directory>\ManageEngine\ RecoveryManager Plus\jre\bin** path and execute the following query to import the internal CA certificate into the '.key
Download CA certificatestore' file.

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

Replace the <keystore_name> with the name of your keystore.

xii In the same path, execute the following query to add the internal CA's root certificate to the list of trusted CAs in the Java cacerts file.

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

Note: Open the '.cer' file to get the name of your internal CA. When prompted, provide 'changeit' as the keystore password.

2. **Issue the SSL certificate using external CAs.**

i To request a certificate from an external CA, submit the CSR to that CA.

ii Unzip the certificates returned by your CA and place them in the <installation_directory> /ManageEngine/RecoveryManager Plus/jre/bin folder

iii Open the command prompt and navigate to the <installation_directory>/ ManageEngine/RecoveryManager Plus/jre/bin folder

iv Run the respective commands from the given list as applicable to your CA:

A. For "GoDaddy" certificates

- keytool -import -alias root -keystore <domainname>.keystore -trustcacerts -file gdrootg2.crt
- keytool -import -alias cross -keystore <domainname>.keystore -trustcacerts -file gdrootg2_cross.crt
- keytool -import -alias intermed -keystore <domainname>.keystore -trustcacerts -file gdig2.crt

B. For "Verisign" certificates

- keytool -import -alias intermediateCA -keystore <domainName>.keystore -trustcacerts -file <your intermediate certificate.cer>
- keytool -import -alias tomcat -keystore <domainName>.keystore -trustcacerts file recoverymanager.cer

C. For "Comodo" certificates

- keytool -import -trustcacerts -alias root -file AddTrustExternalCARoot.crt -keystore <domainName>.keystore
- keytool -import -trustcacerts -alias addtrust -file UTNAddTrustServerCA.crt -keystore <domainName>.keystore
- keytool -import -trustcacerts -alias ComodoUTNServer -file ComodoUTNServerCA.crt - keystore <domainName>.keystore
- keytool -import -trustcacerts -alias essentialSSL -file essentialSSLCA.crt -keystore <domainName>.keystore

D. For Entrust certificates

- keytool -import -alias Entrust_L1C -keystore <keystore-name.keystore> -trustcacerts file entrust_root.cer
- keytool -import -alias Entrust_2048_chain -keystore <keystore-name.keystore> - trustcacerts -file entrust_2048_ssl.cer
- keytool -import -alias -keystore <keystore-name.keystore> -trustcacerts -file <domain-name.cer>

E. For Thawte certificates

- Purchased directly from Thawte:
  - keytool -import -trustcacerts -alias tomcat -file <certificate-name.p7b> -keystore <keystore-name.keystore>
- Purchased through the Thawte reseller channel:
  - keytool -import -trustcacerts -alias thawteca -file <SSL_PrimaryCA.cer> -keystore <keystore-name.keystore>
  - keytool -import -trustcacerts -alias thawtecasec -file <SSL_SecondaryCA.cer> - keystore <keystore-name.keystore>
  - keytool -import -trustcacerts -alias tomcat -file <certificate-name.cer> -keystore <keystore-name.keystore>

Note: If you use an external CA which is not in the list mentioned above, please contact your CA for the required commands.

STEP 3 Associate the certificate with RecoveryManager Plus

1. Copy the '.keystore' file from the <installation_directory>\ManageEngine\ RecoveryManager Plus\jre\bin location and paste it at the <installation_directory> \ManageEngine\RecoveryManager Plus\conf location.
2. At the <installation_directory>\ManageEngine\RecoveryManager Plus\conf location, locate the 'server.xml' file and take a backup of that file.
3. Open the server.xml file using an editor and navigate to the last connector tag.
4. Replace the value of the keystore file with the location of your keystore ('./conf/<keystore_name>.keystore).
5. Replace the value of the 'keystorePass' with the password given during keystore creation.
6. Save the server.xml file and start RecoveryManager Plus (Start ⟶ All Programs ⟶ RecoveryManager Plus ⟶ Start RecoveryManager Plus).
7. Once the RecoveryManager Plus service has started, launch the RecoveryManager Plus client.

Click here to download a guide on how to install an SSL certificate in RecoveryManager Plus.