How to install an SSL certificate in RecoveryManager Plus

ManageEngine
RecoveryManager Plus

Document summary

This document guides you through the process of securing the connection between the ManageEngine RecoveryManager Plus server and the user's browser with Secure Sockets Layer (SSL) certificates.

RecoveryManager Plus overview

RecoveryManager Plus, an enterprise application backup and recovery solution, helps you overcome any disaster caused by unwanted changes in your IT environment. Back up your AD, Microsoft Entra ID, Microsoft 365, Google Workspace, Exchange, and Zoho WorkDrive environments from a single console and restore any object, site, or mailbox whenever you need it. This solution offers:

- Incremental backups
- Granular restoration
- Restart-free recovery
- Backup retention
- Multiple storage options

How to install SSL certificates for RecoveryManager Plus

RecoveryManager Plus supports an SSL connection to ensure the security of data transferred between the browser and the product server. Protecting data transferred during remote access requires a secure connection between the web browser and the RecoveryManager Plus server. Connections between the RecoveryManager Plus server and end-user machines, VPNs, and cloud applications must also be secured. For these, you must enable the HTTP/HTTPS option under the Connection settings, and install an SSL certificate in RecoveryManager Plus.

Configuration steps

Step 1: Enable HTTP/HTTPS in RecoveryManager Plus

i. Login to RecoveryManager Plus with admin credentials.

ii. Navigate to the **Admin** tab **> General Settings > Product Settings > Connection Settings.**

iii. Choose your connection type. You can choose either **HTTP** or **HTTPS.**

iv. Specify the port number of your choice after choosing the connection type. (Default ports for RecoveryManager Plus are HTTP: 8090, HTTPS: 8558).

v. Click **Save.**

Step 2: Generate a CSR and apply the certificate

Note: If you already have an SSL certificate, skip to Step 3.

i. Click the **SSL Certificate Tool** option.

ii. Check **Keystore Password** that appears when you select HTTPS and enter the keystore password.

iii. Click the **Advanced** option to use and specify the TLS versions and cipher suites of your choice.

a. In the **TLS** drop-down menu, select the TLS versions you want.

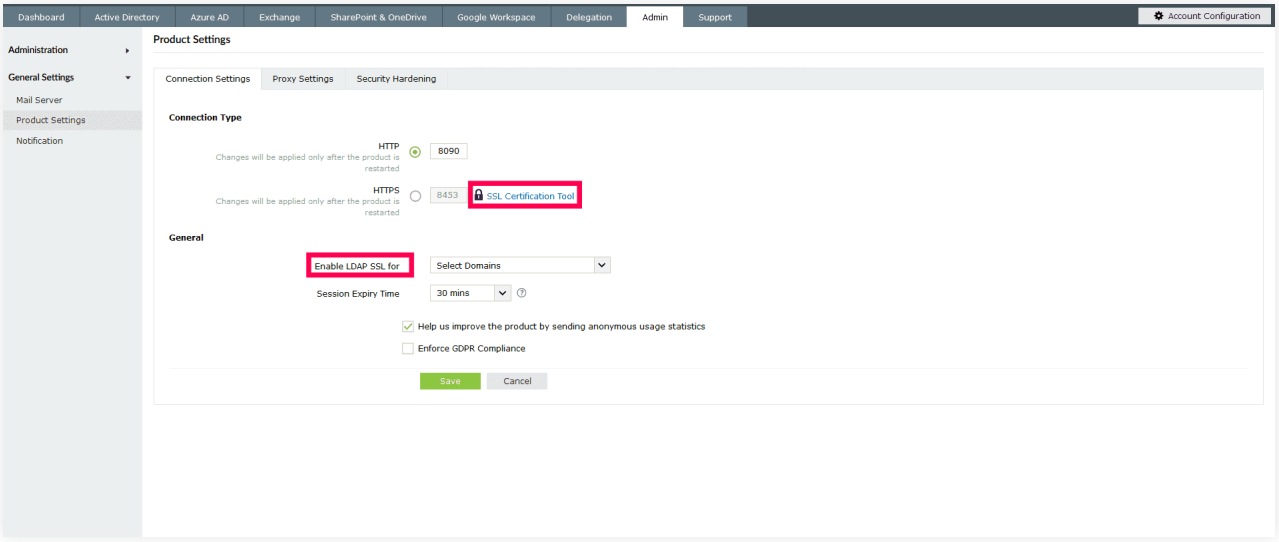
b. You can also select the cipher suites you want to use in the cipher field.

c. We support the following cipher suites:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

iv. .You can also specify the cipher suites you want to use in the **Ciphers** field.

v. Select the domain for which you wish to enable LDAP SSL from the **Enable LDAP SSL** for drop-down menu.



vi. Select the desired **Session Expiry Time** from the options in the drop-down menu.

vii. Check the **Help us improve the product by sending anonymous usage statistics** option to allow us collect information to help us develop exciting new features for RecoveryManager Plus.

viii. Select **Enforce GDPR Compliance** to mask sensitive information from being displayed in the UI and to protect your database backups with a password.

ix. Click **Save.**

Note: For the changes made under **Connection Settings** to take effect, you must restart the RecoveryManager Plus.

If you don't have an SSL certificate, select the **Generate Certificate** option and fill in all the necessary fields as given in the below table.

Common Name	The name of the server in which RecoveryManager Plus is running.
SAN Names	The names of the additional hosts (sites, IP addresses, etc.) to be protected by the SSL certificate.
Organizational Unit	The name of the department that you want to display in the certificate.
Organization	The legal name of your organization.
City	The city name as provided in your organization's registered address.
State/Province	The state or province as provided in your organization's registered address.
Country Code	The two-letter code of the country in which your organization is located.
Password	A password that consists of at least six characters to secure the keystore.
Validity (In Days)	The number of days for which the SSL certificate will be considered valid; if no value is provided, it will be set to 90 days.
Public Key Length (In Bits)	The public key length. The default value is 2,048 bits and its value can only be incremented in multiples of 64.

After all values have been entered, you can select either of these two options:

- **Generate CSR**

  This method enables you to generate the Certificate Signing Request (CSR) file and submit it to your certificate authority (CA). Using this file, your CA will generate a custom certificate for your server.

  - Click **Download CSR** or manually get it from the **<Install_dir>\Certificates** folder.
  - Once you have received the certificate files from your CA, follow the steps listed under the Apply an existing SSL Certificate section to use the SSL certificate.

- **Generate & Apply Self-Signed Certificate**

  This option enables you to create a self-signed certificate and apply it instantly to the product. However, self-signed SSL certificates come with a drawback. Anyone accessing the product secured with a self-signed SSL certificate will be shown a warning that says the website is not trusted, which may cause concern.

  If you want to apply the self-signed certificate, follow the steps given below:

  - Click **Apply Self-Signed Certificate.**
  - Once you receive the message that SSL certificate has been successfully applied, restart the product for the changes to take effect.

Step 3: Apply an existing SSL certificate

If you already have a SSL certificate, select the **Apply Certificate** option and follow the steps listed below.

i. Select **Apply Certificate.**

ii. Select your preference from **Choose Upload Option** based on the certificate file type.

a. ZIP Upload

- If your CA has sent you a ZIP file, then select **ZIP Upload. Browse** and upload the ZIP file.
- If your CA has sent you individual certificate files, such as user, intermediary, and root certificates, you can put all these certificate files in a ZIP file and upload it.
- If your certificate's **private key is password** protected, enter its password in the Private Key Passphrase field.

b. Individual Certificates

- If your CA has sent you just one certificate file (PFX or PEM format), then select **Individual Certificates.**
- Browse and upload the certificate in the **Upload Certificate** field.
- Browse and upload the additional certificate files provided by your CA in the **Upload CA Bundle** field.
- If the uploaded certificate is password protected, enter the password that must be provided to access it in the **Certificate Password** field.

c. Certificate Content

- If your CA has sent the certificate content, then choose the **Certificate Content** option, and paste the certificate content in the **Paste Certificate Content** field.
- If your certificate's private key is password protected, enter its password in the **Private Key Passphrase** field.

Note: Only Triple DES encrypted private keys are currently supported.

iii. Click **Apply.**

iv. Restart the product for the changes to take effect.