ManageEngine
RecoveryManager Plus

RecoveryManager Plus
Quick start guide

Index

Overview

RecoveryManager Plus is an enterprise application backup and recovery solution for Active Directory, Microsoft Entra ID (formerly Azure AD), Microsoft 365 (SharePoint Online, OneDrive for Business, and Microsoft Teams), Google Workspace, on-premises Exchange, and Zoho WorkDrive. With RecoveryManager Plus, restore just a few objects or your entire environment to any backed-up state.

This document explains how to deploy and configure the important settings of RecoveryManager Plus successfully.

Deployment

System requirements

Hardware	Minimum	Recommended
Processor	2.4GHz	3GHz
Number of cores	4	6 or more
RAM	8GB	16GB

AD and Microsoft Entra ID backups	This requirement varies based on the number of AD objects, Entra ID objects, the size of your domain controller, and the retention period that you set for your backups. RecoveryManager Plus typically compresses backups to a third of their original size. It has a best case compression ratio of 2:1 for domain controller backups.
Exchange, Microsoft 365, Google Workspace, and Zoho WorkDrive backup	RecoveryManager Plus typically compresses backups to a third of their original size. If the total size of the mailboxes, SharePoint Online, and OneDrive for Business sites, Microsoft Teams, Google Workspace user drives, or Zoho WorkDrive folders is 1TB, make sure that you have 1TB of free disk space to store the full backup and all subsequent incremental backups.

Supported platforms

ManageEngine RecoveryManager Plus supports the following Microsoft Windows operating system versions.

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2008
- Windows 11
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Supported browsers

One of the following browsers is required to access the RecoveryManager Plus client.

- Mozilla Firefox
- Google Chrome
- Microsoft Edge
- Internet Explorer 10 and above

Supported databases

ManageEngine RecoveryManager Plus supports the following databases:

- PostgreSQL (default database bundled with RecoveryManager Plus)
- MS SQL

Please refer to our system and port requirements guide for a detailed list of requirements.

Recommended screen resolution

- 1366 x 768 pixels or higher.

Installation

You can install ManageEngine RecoveryManager Plus on any machine in the domain that satisfies the recommended system requirements.

You can install RecoveryManager Plus as:

- An application
- A Windows service

Installing RecoveryManager Plus as an application

By default, RecoveryManager Plus will be installed as an application

1. Click here to download the executable file from the website.
2. Double-click the downloaded file **ManageEngine_RecoveryManagerPlus_64.exe**
    (or **ManageEngine_RecoveryManagerPlus.exe** depending on the version you downloaded)
    to start the installation.
3. Follow the instructions on the InstallShield wizard to complete the installation of
    RecoveryManager Plus.

You can launch the application's web console by:

*   Navigating to **Start > Start RecoveryManager Plus.**
*   Double-clicking the **RecoveryManager Plus shortcut** on the desktop. When opened as an
    application, RecoveryManager Plus runs with the privileges of the user who installed the application.

Installing RecoveryManager Plus as a Windows Service

To install RecoveryManager Plus as a service:

1. Install **RecoveryManager Plus** as an application.
2. Navigate to **Start > All Programs.**
3. Select **RecoveryManager Plus** and click **Install RecoveryManager Plus as Service.**

Alternatively, you can also install RecoveryManager Plus as a service from the notification tray.

1. Install **RecoveryManager Plus** as an application.
2. Click the **notification icon** [🔔] at the top-right corner of the screen.
3. Select the **RecoveryManager Plus is not installed as a service** alert, and then click **Install.**
    This will initiate RecoveryManager Plus service installation in the background.
4. Once you've installed RecoveryManager Plus as a service, you can start the product as a
    Windows Service. When started as a service, RecoveryManager Plus runs with the privileges
    of the system account or the service account (if configured).

Uninstalling RecoveryManager Plus

To uninstall RecoveryManager Plus:

1. Navigate to **Start > All Programs > RecoveryManager Plus > Uninstall RecoveryManager Plus.**

Working with RecoveryManager Plus

Starting RecoveryManager Plus

RecoveryManager Plus can be started either using the system account (when run as a service) or as a user account (when run as an application).

On starting RecoveryManager Plus, the client is automatically launched in the default browser.

Launching the RecoveryManager Plus client

To launch the RecoveryManager Plus client:

1. Open any of the supported web browsers and type **http://<hostname>:8090** in the address bar where *<hostname>* refers to the DNS name of the machine where RecoveryManager Plus is installed.

2. Enter **admin** as the username and password (for first time users) in the respective fields and click **Login**. You can change this default password by navigating to **Admin > Personalization > Change Password.**

Stopping RecoveryManager Plus

To stop RecoveryManager Plus, select **Start > Programs > RecoveryManager Plus > Stop RecoveryManager Plus.**

Setting up RecoveryManager Plus

AD domain configuration

1. Click the **Account Configuration** button located at the top-right corner of the screen.

2. Select the **On-premises AD** tab.

3. Click the **Add New Domain** option located at the top-right of the domain settings section.

4. Enter the **name** of the domain.

5. Click the **Discover DCs** link to automatically detect the domain controllers in the specified domain. ou can also add the domain controller manually by clicking **Add** and providing the name of the DC. If RecoveryManager Plus still cannot identify the domain controller, use the DC name with the Fully Qualified Domain Name.

6. Enter the **Username** and **Password** of a domain administrator.

7. Click **Add** to add the domain details in the product.

Microsoft 365 tenant configuration

Prerequisites

1. A service user account with Global Administrator privileges.

   Note: RecoveryManager Plus doesn't store the Global Administrator credentials anywhere within the product.

Automatic Microsoft 365 tenant configuration

1. Log in to RecoveryManager Plus as an administrator.
2. Click **Account Configuration** button located at the top-right corner of the screen and select the **Microsoft 365 Tenant** tab.
3. If you are configuring your first tenant, click **Configure** using Microsoft 365 Login. Otherwise, choose **Add New Tenant,** and then click *Configure using Microsoft 365 Login.*
4. Click **Proceed** in the pop-up that appears.
5. You will be redirected to the Microsoft 365 login portal. Enter the credentials of a **Global Administrator.**
6. Click **Accept.**
7. An application and service account for RecoveryManager Plus will be created automatically. You will now see a page that displays the list of permissions the application needs. Please note down the application name, which is shown at the top. You will need this later.
8. Go through the list and click **Accept.**

   Note: If you do not want to provide all the required permissions, please configure your tenant manually.
9. You will now be redirected to the RecoveryManager Plus console, where you can see that **Entra Application Status** is success for the account you configured. If it is not successful, you will have to do it manually.

Google Workspace domain configuration

1. Click the Account Configuration button located at the top-right corner of the screen.
2. Select the Google Workspace tab.
3. Select the type of account that you wish to add to RecoveryManager Plus.

   a. Personal account: Selecting this option will allow you to add a personal Google account to RecoveryManager Plus.

   b. Workspace account: Selecting this option will allow you to add a Google Workspace account to RecoveryManager Plus. Once added, you can configure a backup schedule for all users in the workspace.

a. **Adding a personal Google account**

    i. Enter the email address of the user.

    ii. In the **Credentials JSON** field, click the **Browse** button and select the appropriate file.

        <u>Learn how</u> to create a Credentials JSON.

    iii. Click **Configure** to add the user account to RecoveryManager Plus.

    iv. In the page that appears, allow RecoveryManager Plus to access the following information and click **Allow.**

        1. Read, compose, send, and permanently delete all your emails from Gmail

        2. See, edit, create, and delete all of your Google Drive files

        3. See, edit, download, and permanently delete your contacts

        4. See, edit, share, and permanently delete all the calendars you can access using Google Calendar

b. **Adding a Workspace account**

    i. Enter the **email address** of the administrator.

    ii. Provide the **Service Account ID.**

    iii. In the *Service Key* field, click the **Browse** button and select the appropriate **file**. <u>Learn how</u> to create a service account and generate the service key.

    iv. Click **Configure** to add the Workspace to RecoveryManager Plus.

Exchange Server organization configuration

1. Click the **Account Configuration** button located at the top-right corner of the screen.

2. Select the **On-premises Exchange** tab.

3. Select the **Server Type** from the available options: **Global Catalog** and Exchange Server.

4. Provide the Server Name.

5. Enter the **Username** and **Password** of a user who is a member of the Organization Management role group. The username should be entered in the Domain\username format.

6. If your server is an Exchange Server, you'll have the option to **Enable SSL.**

7. The user account used to configure the Exchange organization must have appropriate impersonation rights to back up and restore Exchange mailboxes. Select **Grant Impersonation** to provide the account with this privilege.

8. **Note:** If this option is not selected, you can only back up and restore the mailbox of the user whose email address has been used to configure the Exchange organization.

9. Click **Save.**

Zoho WorkDrive team configuration

1. Log in to the RecoveryManager Plus console as an administrator.
2. Click the **Account Configuration** button located at the top-right corner of the screen.
3. Select the **Zoho WorkDrive** tab.
4. Choose the appropriate data center from the drop-down if your data is not stored in the United States data center.
5. Click **Configure using WorkDrive Login**. This will redirect you to the Zoho accounts sign-in page. Enter your credentials to sign in. The teams for which the user account is a Super Admin or Admin will be added when configured.
6. You will then be redirected to the consent page. By clicking **Accept**, you allow RecoveryManager Plus App to access your account's data.

Configuring backup repositories

You can configure local, NAS/shared, or cloud repositories in RecoveryManager Plus.

Configuring local repositories

When RecoveryManager Plus is installed, a local repository is configured in the installation directory.

1. Navigate to the **Admin** tab and go to **Administration > Backup Repository > Local.**
2. Click the **Add Repository** button in the top-right corner.
3. Enter a name in the **Repository Name** field.
4. Enter the **local path** where you wish to save the backups in the Repository Path field.
5. If required, you can select **Authentication** and provide the **credentials** of a user who can read/write in the specified local path.

Configuring NAS/shared repositories

1. Navigate to the **Admin** tab and go to **Administration > Backup Repository > NAS/Shared.**
2. Click the **Add Repository** button in the top-right corner.
3. Enter a **name** in the *Repository Name* field.
4. Enter the **NAS/Shared path** where you wish to save the backups in the *Repository Path* field.
5. In the *Username* and *Password* fields, provide the **credentials** of a user who can read/write in the specified path.

Configuring cloud repositories

This repository stores Microsoft 365, on-premises Exchange, Google Workspace, and Zoho WorkDrive backups in the following storage services. In addition, the archived data of AD and Entra ID can also be stored in the cloud repositories.

Adding Azure Blob storage as a repository

1. Navigate to the **Admin** tab and go to **Administration > Backup Repository > Cloud.**
2. Click the **Add Repository** button in the top-right corner.
3. Select **Azure Blob Storage** from the *Repository Type* drop-down.
4. Enter a **name** in the *Repository Name* field.
5. Enter the **Account Name** and **Account Key** of the Azure storage account. To learn how to find your Account Name and Account Key, click here.
6. Enter the Root Container Name.

   Note: Metadata of the Microsoft 365, on-premises Exchange, Google Workspace, and Zoho WorkDrive backups will be stored in the default Elasticsearch node.
7. Click **Save.**

Adding Azure Files as a repository

1. Navigate to the **Admin** tab and go to **Administration > Backup Repository > Cloud.**
2. Click the **Add Repository** button in the top-right corner.
3. Select **Azure Files** from the *Repository Type* drop-down.
4. Enter a **name** in the Repository Name field.
5. Enter the **Account Name** and **Account Key** of the Azure storage account. To learn how to find your Account Name and Account Key, click here.
6. Enter the File Share Name.

   Note: Metadata of the Microsoft 365, on-premises Exchange, Google Workspace, and Zoho WorkDrive backups will be stored in the default Elasticsearch node.
7. Click **Save.**

Finding your Azure storage account name and account key

To find the account name and account key for your Azure storage account:

1. Open the Microsoft Azure Portal in your web browser and log in with the credentials of a user who can access the storage account.
2. Select **Storage Accounts** from the Azure services.
3. In the screen that appears, select the storage account for which you would like to find the *Account Name* and *Account Key*. The name displayed at the top-left corner is the name of your storage account.
4. Click **Security + networking** from the left pane and select **Access keys.**
5. Copy **Key1** or **Key2.** You can use either of the keys.
6. Use the *Account Name* and *Account Key* to add your Azure storage account to RecoveryManager Plus.

Adding AWS S3 as a repository

1. Navigate to the **Admin tab** and go to **Administration > Backup Repository > Cloud**.

2. Click the **Add Repository** button in the top-right corner.

3. Select **AWS S3** from the *Repository Type* drop-down.

4. Enter a **name** in the *Repository Name* field.

5. Enter the **Access Key** and **Secret Access Key**. To learn how to find your AWS Access Key and Secret Access Key, click here.

6. Enter the **Bucket Name.**

   Note: Metadata of the Microsoft 365, on-premises Exchange, Google Workspace, and Zoho WorkDrive backups will be stored in the default Elasticsearch node.

7. Click **Save.**

Finding your Access Key and Secret Access Key in AWS

1. Open the AWS Management Console in your web browser.

2. Enter **IAM** in the search bar and select **IAM** under Services.

3. Select **Users** under *Access management* in the left pane.

4. Click **Create user** to create a new user. If a user has already been created, skip to step 5.

   a. Enter a **name** for the user in the *User name* field and click **Next.**

   b. Click **Attach policies directly** and select **AmazonS3FullAccess**. Click **Next.**

   c. Review the details and click **Create user.**

5. Once you have created the user, enter the **user name** in the *search bar.*

6. Select **Security credentials**, scroll to the **Access keys** section, and click **Create access key.**

   a. Select **Third-party service** and click **Next.**

   b. Add a description if needed and click **Create access key.**

7. Copy the Access Key and Secret Access Key to configure your AWS S3 storage account in RecoveryManager Plus.

Adding Wasabi as a repository

1. Navigate to the **Admin** tab and go to **Administration > Backup Repository > Cloud.**

2. Click the **Add Repository** button in the top-right corner.

3. Select **Wasabi** from the **Repository Type** drop-down.

4. Enter a **name** in the *Repository Name* field.

5. Enter the **Access Key** and **Secret Access Key**. To learn how to find your Wasabi Access Key and Secret Access Key, click here.

6. Enter the **Bucket Name**.

   Note: Metadata of the AD, Entra ID, Microsoft 365, on-premises Exchange, Google Workspace, and Zoho WorkDrive backups will be stored in the default Elasticsearch node.

7. Click **Save.**

Finding your Access Key and Secret Access Key in Wasabi

1. Open the Wasabi Console in your web browser.

2. Select **Users** under *Users & Groups* in the left pane.

3. Click **Create User** to create a new user.

4. Enter a **name** for the user in the *Create a Username* field.

5. In the *Type of Access* field, check the **Programmatic (create API keys)** box.

6. Leave the **Multi-Factor Authentication (MFA)** box unchecked and click **Next.**

7. Assign the user to a group if needed and click **Next.**

8. Click the **Attach Policy to User**, select **WasabiFullAccess**, and click **Next.**

9. Review the entered details and click **Create User.**

10. Copy the **Access Key** and **Secret Key** from the pop-up that appears to configure your Wasabi storage account in RecoveryManager Plus.

Enabling SSL

You can enable SSL for RecoveryManager Plus by following the steps listed below.

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

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

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

iv. If you would like to apply an SSL certificate, click the **SSL Certificate Tool** option and perform the desired actions. Click here to learn how to apply or generate an SSL certificate.

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

vi. 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. 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

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

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

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

x. If desired, you can check the **Help us improve the product by sending anonymous usage statistics** option to allow us collect your usage statistics.

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

xii. Click **Save.**

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

SSL configuration

RecoveryManager Plus supports SSL connection to ensure security of data transferred between the browser and the product server.

Steps to apply an SSL certificate

i. Navigate to the **Admin** tab > **General Settings > Product Settings > Connection Settings > SSL Certification Tool.**

    a. If you don't have an SSL certificate, select the **Generate Certificate** option and follow the steps here.

    b. If you already have an SSL certificate, select the **Apply Certificate** option and follow the steps here.

To generate an SSL certificate

i. In the **Common Name** field, enter the name of the server.

    Example: For the URL https://servername:8558, the common name is servername.

ii. In the **SAN Names** field, enter the additional hostnames.

iii. In the **Organizational Unit** field, enter the name of the department that you want to display in the certificate.

iv. In the **Organization** field, enter the legal name of your organization.

v. In the **City** field, enter the name of the city as provided in your organization's registered address.

vi. In the **State/Province** field, enter the name of the state or province as provided in your organization's registered address.

vii. In the **Country Code** field, enter the two-letter code of the country where your organization is located.

viii. In the **Password** field, enter a password that consists of at least six characters to secure the keystore.

ix. In the **Validity (In Days)** field, specify the number of days for which the SSL certificate will be considered valid.

    Note: When no value is entered, the certificate will be considered to be valid for 90 days.

x. In the **Public Key Length (In Bits)** field, specify the size of the public key.

   Note: The default value is 2,048 bits and its value can only be incremented in multiples of 64.

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

a. Generate CSR

This method allows 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 by going to the **<Install_dir>\Certificates** folder.
- Once you have received the certificate files from your CA, follow the steps listed under the To apply an existing SSL Certificate section to apply the SSL certificate.

b. Generate & Apply Self-Signed Certificate

This option allows you to create a self-signed certificate and apply it instantly in 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.

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

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

To apply an existing SSL certificate

If you already have a SSL certificate, follow the steps listed below to apply it.

i . Select **Apply Certificate.**

ii. Choose an **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.

Enabling 2FA

Two-factor authentication (2FA) adds an extra layer of security to the product. When you try to access RecoveryManager Plus, the login process will be complete only after the 2FA is completed. Users with the Admin role can bypass 2FA.

To enable 2FA for your users:

1. Navigate to **Delegation > Configuration > Logon Settings > Two-factor Authentication.**
2. Toggle the **Two-Factor Authentication** button. RecoveryManager Plus provides the following modes of secondary authentication:
   a. Email verification
   b. Google Authenticator
   c. Duo Security
   d. RADIUS authentication
   e. Microsoft Authenticator

Learn how to enable these methods as your secondary authentication factors.

Note:

After configuring 2FA, if users cannot access their phones or face issues with the selected second-factor authentication method, you can use backup verification codes to log in. When enabled, a total of five codes will be generated. Once used, a code will become obsolete and cannot be used again. Users also have the option to generate new codes. Learn how to enable backup verification codes.

Configuring a mail server

You can configure the mail server to send notifications from the product by following the steps listed below. RecoveryManager Plus provides two modes of mail server configuration:

SMTP

API

SMTP

This method allows you to configure a mail server via Basic or OAuth authentication.

To configure an SMTP mail server,

1. Navigate to **Admin > General Settings > Mail Server**.

2. In the **Mode** field, select **SMTP.**

3. Enter your mail server's **Server Name or IP** and **Port Number** in the respective fields.

4. In the **From Address** field, enter the email address that will be used to send out notifications, alerts, etc. from RecoveryManager Plus.

5. In the **Admin Mail Address** field, enter your email address if you wish to receive notifications for the emails sent from RecoveryManager Plus.

6. Select the connection security type from the available options: **SSL, TLS**, or **None.**

7. Select the authentication type from the options provided: **Basic authentication** or **OAuth authentication.**

   a. **Basic authentication**

   i . Enter the **Username** and **Password** to access the mail server.

   ii. If your mail server does not require authentication, leave the fields empty.

   b. **OAuth authentication**

   i. Select your mail provider from the available options: **Microsoft** or **Google.**

   ii. If your mail provider is Microsoft, provide the **Username, Tenant ID, Client ID**, and **Client Secret** in the respective fields. In RecoveryManager Plus, the Azure Cloud is considered the default Azure environment. You can modify the Azure environment setting by clicking the **Choose the appropriate Azure environment link.**

   Note: To learn how to find your Azure Tenant ID, Client ID, and Client Secret, click here.

   c. If your email provider is **Google**, enter the **Google Workspace Client ID** and **Client Secret** in the respective fields, and click **Configure.**

   Note: To learn how to find your Google Workspace Client ID and Client Secret, click here.

8. If you selected **Basic authentication** in step 7, you can have RecoveryManager Plus send a test email by clicking the **Test Mail** button.

9. Click **Save Settings** to save your mail server configuration.

API

This method allows you to configure a mail server via your mail provider's API.

1. Navigate to **Admin > General settings > Mail Server.**

2. In the **Mode** field, select **API.**

3. Select your mail provider from the available options: **Microsoft** or **Google.**

4. In the **From Address** field, enter the email address that will be used to send out notifications, alerts, etc. from RecoveryManager Plus.

5. In the Admin Mail Address field, enter your email address if you wish to receive notifications for the emails sent from RecoveryManager Plus.

6. If your mail provider is Microsoft, provide the **Tenant ID, Client ID**, and **Client Secret** in the respective fields. In RecoveryManager Plus, the Azure Cloud is considered the default Azure environment. You can modify the Azure environment setting by clicking the **Choose the appropriate Azure environment link.**

   Note: To learn how to find your Azure Tenant ID, Client ID, and Client Secret, click here.

7. If your mail provider is **Google**, upload the **JSON private key** file.

   Note: To learn how to get your JSON private key file, click here.

8. Click **Save** settings.

Auto backup

RecoveryManager Plus allows you to configure periodic backups of the database that comes built-in with it. The product also allows you to migrate from the built-in database (PostgreSQL) to Microsoft SQL. To schedule a database backup:

1. Navigate to **Admin tab > Administration > Database Settings > Database Backup.**

2. Mark the check box next to **Enable Database Backup.**

3. In the **Repository** field, click the drop-down box to select from the list of all available repositories. If no repositories are available, click the 📁 icon to add a new storage repository.

4. Enter a name in the **Repository Name** field.

5. In the **Repository Path** field, enter the shared folder where you wish to save the backups. Provide the credentials of a user that can read/write the content in the specified storage location.

6. Click **Add.**

7. Select the frequency at which the database must be backed up from the list of options available: daily, weekly, or monthly.

8. If you have selected **Enforce GDPR Compliance** in Product Settings, you can secure your database backup with a password. Provide a password.

9. Click **Save.**

Auto update

Automatically download and install any issue fix patches from ManageEngine for security vulnerabilities detected within the product. Enabling this feature ensures security patches are updated promptly without having to wait for service packs to be released, thereby reducing the probability of the vulnerability being exploited in your installation.

To enable auto update,

1. Navigate to **Admin tab > Administration > Auto Update.**
2. Mark the check-box against **Automatically download and update issue fix patches.**
3. Select the frequency at which the product will check for patches.

   Note: We recommend setting the frequency as **Daily** to ensure you have the latest fixes enrolled as soon as possible.
4. Click **Save.**

Database migration

In RecoveryManager Plus, you can change the built-in database server (PostgreSQL) to Microsoft SQL Server.

To migrate data from PostgreSQL to Microsoft SQL:

1. Stop the RecoveryManager Plus server.

   a. To stop RMP if it is running as a console:

   Run the shutdown.bat file from <RecoveryManager Plus Home>\bin\ folder in the Command Prompt to stop the RecoveryManager Plus server.

   b. To stop RecoveryManager Plus when it is running as a service:

   Go to **services.msc >** stop RecoveryManager Plus service.

2. To migrate the database from PostgreSQL to Microsoft SQL with all data intact:

   Open Command Prompt and navigate to *<RecoveryManager Plus Home>\bin.* Enter *changeDB.bat* command to migrate the database with the data intact.

   (OR)

   To change the database from PostgreSQL to Microsoft SQL without migrating the data: Open Command Prompt and navigate to the location *<RecoveyManager Plus Home>\bin*. Enter the command changeDB.bat false to migrate the database without data.

3. The *Database Setup Wizard* pop-up will appear on the next screen.

4. Select **Server Type** as **Microsoft SQL Server**. Choose one of the available Microsoft SQL server instances listed in the corresponding drop-down box. Enter the **Host Name** and **Named instance** of the SQL Server from the instance drop-down.

5. Under **Connect Using** options, select one of the authentication types. The options are:

   a. **Windows Authentication**

   For Windows authentication, the credentials of the Domain user are automatically taken.

   b. **SQL Server Authentication**

   For Microsoft SQL Server Authentication, enter the **User Name** and **Password.**

6. Click **Test Connection** to check whether the credentials are correct. If the test fails, the credentials may be wrong; recheck and enter the correct credentials.

7. Click **Save** to save the Microsoft SQL Server configuration. Note that it will take a few minutes to configure the settings of the SQL Server database.

8. Start the RecoveryManager Plus service to work with the Microsoft SQL server as the database.

If the Microsoft SQL server you wish to migrate to has Force encryption enabled, select the check box against SSL connection and follow the steps mentioned below.

To migrate data from PostgreSQL to Microsoft SQL:

1. Covert your Microsoft SQL server certificate to .cer format.

    a. Open **IIS Manager.**

    b. In the middle pane, click **Server Certificates.**

    c. Open the certificate you want to use, then click the **Details** tab.

    d. Click **Copy to file.**

    e. Click **Next** in the Certificate Export Wizard window that appears.

    f. On the *Export Private Key* screen, select **No, do not export the private key**, then click **Next.**

    g. On the *Export File Format* screen, select either *DER encoded binary X.509 (.CER) or Base-64 encoded X.509 (.CER),* then click **Next.**

    h. Enter a name for the file, click Next, and then Finish.

    i. Copy the CER file and place it in

    <Installation_folder>\RecoveryManagerPlus\conf on the machine

    where RecoveryManager Plus is running.

2. Open Command Prompt and navigate to **<Installation directory>\jre\bin** folder of RecoveryManager Plus. Use the command below to associate the Jave KeyStore:

keytool -import -v -trustcacerts -alias myserver -file pathofthecert\certname.cer -keystore"..\lib\security\cacerts" -keypass changeit -storepass changeit -noprompt, where pathofthecert is the location where the certificate has been stored and certname is the certificate name. The certificate will be added to your Java KeyStore.

ManageEngine
RecoveryManager Plus

About RecoveryManager Plus

ManageEngine RecoveryManager Plus is a comprehensive enterprise backup and recovery solution for Active Directory, Microsoft Entra ID, Microsoft 365 (Exchange Online, SharePoint Online, OneDrive for Business and Microsoft Teams), Google Workspace, on-premises Exchange and Zoho WorkDrive environments. With its incremental backups, flexible retention policies, backup immutability and multiple modes of restoration—such as domain controller recovery and object-, item- and attribute-level restoration—RecoveryManager Plus delivers a holistic solution for minimizing downtime and ensuring seamless business continuity by backing up all application's data.

For more information, visit www.manageengine.com/ad-recovery-manager.

| $ Get Quote | ⭳ Download |