ManageEngine
RecoveryManager Plus

RecoveryManager Plus
Quick start guide

Index

Overview

RecoveryManager Plus is an enterprise application backup and recovery solution for Active Directory, Azure Active Directory, Microsoft 365, 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

Disk space	This requirement varies based on the number of backed-up Active Directory and Azure Active Directory objects, the size of your Exchange (on-premises and online) and Google Workspace mailboxes, SharePoint Online and OneDrive for Business sites, Google Workspace user drives, Zoho WorkDrive folders, and the retention period that you set for your backups.
Active Directory and Azure Active Directory backups:	A minimum of 50GB.
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, Google Workspace user drives, and 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 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003 R2

- Windows Server 2003
- Windows 10
- Windows 8
- Windows 7
- Windows Vista
- Windows XP (SP3 & above)

Supported browsers

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

- Internet Explorer 11 and above
- Firefox 4 and above
- Chrome 10 and above
- Microsoft Edge

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. If you want the product to automatically connect to the secondary DC and start gathering changes from the AD database if the primary DC fails, select the **Enable auto-switch on DC failure** option.
7. Enter the **Username** and **Password** of a domain administrator.
8. 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
   AAD 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.

            [Learn how](#) 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.**

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

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

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

            iv. 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**. [Learn how](#) 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.

   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.
8. 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 both on-premises and cloud repositories in RecoveryManager Plus.

Configuring on-premises repositories

When RecoveryManager Plus is installed, a local repository is configured in the installation directory. You can modify the path of the default repository or add a new repository.

To modify the path of the default repository:
1. Navigate to **Admin > Repository > Backup Repositories.**
2. Click on the **On-premises** tab.
3. Click the <edit> icon next to the *RMP-Local* repository.
4. Provide the **new path** in the Repository Path field.
5. Click **Save.**

To configure a new on-premises repository:
1. Navigate to **Admin > Repository > Backup Repositories.**
2. Click on the **On-premises** tab.
3. Click on the **Add on-premises repository** button.
4. Provide a **name** for the repository.
5. Provide the **name** of the server in which you want to store the backups.
   Note:
   Ensure that the server has 64-bit architecture.
6. Provide an admin **username** and **password**. Click **Verify Credentials** to check if the provided credentials have enough privilege.
7. Provide the **path** to the repository.

8. Provide a **TCP Port** to enable communication between RecoveryManager Plus and the server.

   Note:

   If you have enabled a firewall, make sure the specified port is added in the firewall's inbound rules.

9. Set a **JVM Heap Size.**

   Note:

   The JVM Heap Size must be at least 1GB. Also, the JVM Heap Size cannot be more than 50% of target machine's usable RAM size.

10. Click **Save.**

Configuring cloud repositories

RecoveryManager Plus stores Microsoft 365, Google Workspace, and on-premises Exchange backups in Azure Blob Storage and file shares.

To modify the path of the default repository:

1. Navigate to **Admin > Repository > Backup Repositories.**

2. Click the **Cloud** tab.

3. Click the **Add cloud repository** button.

4. To add Azure Blob Storage:

   a. Select **Azure Blob Storage** as the repository type.

   b. Provide a name for the repository, the **Account Name** and **Account Key** of the Azure storage account.

   c. Provide the **Root Container Name.**

5. To add an Azure file share:

   a. Select **Azure File Shares** as the repository type.

   b. Provide a **name** for the repository, the **Account name** and **Account Key** of the Azure storage account.

   c. Provide the **File Share Name.**

6. Select where you wish to store the metadata of the backups from the **Metadata Repository** drop-down box.

   Note:

   Metadata of the Microsoft 365, Google Workspace, and Exchange backups will be stored in the selected metadata repository.

7. Click **Save.**

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

    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.

1. Navigate to **Admin > General Settings > Mail Server.**
2. Specify the **hostname** or **IP address** of the mail server and its **port number.**
3. In the *From Address* field, enter the **email address** that you wish to display as the sender's email while delivering the reports via email.
4. In the To *Address* field, enter the **email address** to which you would like to send the reports.
5. Choose the **Connection Security (SSL/TLS)** from the drop-down menu.
6. Check the **box** next to the *Authentication* field and enter authentication information. By default, anonymous login is used. Enter the **username** and **password** of an administrator of the mail server to avoid anonymous login.
7. To verify your mail server settings, use the **Test Mail** option. A test mail will be sent to the specified mail address.
8. Click **Save.**

Notification settings

1. To notify the admin when the license is about to expire, check the **box** next to the *Enable License/AMS Expiry Notification* field.

2. Click **Save.**

Auto backup

RecoveryManager Plus can automatically back up its database at regular intervals. Using this option, you can back up the built-in PostgreSQL or MS SQL databases configured in the product along with the Elasticsearch databases.

To schedule a database backup:

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

2. Check the **box** next to Enable Database Backup.

3. Select the **Repository** in which you wish to store the backups.

   Note:

   If you have not configured any repository, click the icon to add a new storage repository. Enter a **name** in the *Repository Name* field. In the *Repository Path* field, enter the **shared folder** in which you wish to save the backups. Provide the credentials of a user that can read/write the content in the specified storage location.

4. Select whether you want to schedule the backup daily, weekly, or monthly and at what time from the *Backup Frequency* drop-down.

5. Click **Save.**

Database migration

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

To migrate data from PostgreSQL to MS SQL:

1. Stop the **server** from *Start menu* or invoke the **<RecoveryManager Plus Home>\bin\shutdown.bat** to stop the RecoveryManager Plus server in the Command Prompt.

2. Open the Command Prompt and navigate to **<RecoveryManager Plus Home>\bin.**
   Enter the command **changeDB.bat** to migrate the database with data intact.
   (OR)
   Open the Command Prompt and navigate to **<RecoveryManager Plus Home>\bin.**
   Enter the command **changeDB.bat** false to change the database without data.

3. The Database Setup Wizard will pop up.

4. In this screen, select **MS SQL Server** as the *Server Type*. Available SQL Server instances are listed in a combo box. Enter the **Host Name** and **Named Instance** of the SQL Server from the instances.

5. Select the authentication type using the **Connect Using** option.

6. The options are:

    a. **Windows Authentication:** For Windows Authentication, the credentials of the domain user are automatically taken.

    b. **SQL Server Authentication:** For MS SQL Server Authentication, enter the **Username** and **Password.**

7. 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.

8. Click **Save** to save the MS SQL Server configuration.

    Note:

    It will take few minutes to configure the settings of the SQL Server database.

9. Start the RecoveryManager Plus Server/Service to work with the MS SQL Server as the database.

Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus | M365 Manager Plus

ManageEngine
RecoveryManager Plus

ManageEngine RecoveryManager Plus is a comprehensive backup and recovery solution that empowers administrators to back up and restore their Active Directory, Entra ID, Microsoft 365, Google Workspace, on-premises Exchange and Zoho WorkDrive environments. With its incremental backups, flexible retention policies and multiple modes of restoration, RecoveryManager Plus delivers a holistic solution for backing up data that is critical for your enterprise to function. For more information, visit www.manageengine.com/ad-recovery-manager.

$ Get Quote   ± Download

Support

✉ support@recoverymanagerplus.com   📞 +1.844.245.1108 | US: +1.408.916.9393