ManageEngine
RecoveryManager Plus

BEST PRACTICES GUIDE

Tips and guidelines to get the most out of **RecoveryManager Plus.**

www.recoverymanagerplus.com

We thank you for choosing RecoveryManager Plus for your Active Directory, Azure Active Directory, SharePoint Online, OneDrive for Business, Exchange Online, and on-premises Exchange backup needs. Before installing the product, please take a few minutes to go through our best practices. These are based on our experience, research, and product testing.

This guide is broken down into the following sections:

1. Scope of the product

Active Directory

You can use RecoveryManager Plus to back up and recover AD running on:

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Exchange Server

You can use RecoveryManager Plus to back up and recover Exchange mailboxes from:

- Microsoft Exchange Server 2010 SP1
- Microsoft Exchange Server 2010 SP2
- Microsoft Exchange Server 2010 SP3
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019

Azure Active Directory

You can use RecoveryManager Plus to back up all objects in your Azure Active Directory environment.

Exchange Online, SharePoint Online, OneDrive for Business.

You can use RecoveryManager Plus to back up all Exchange Online mailboxes, SharePoint Online and OneDrive for Business sites.

2. Hardware requirements

Processor	2.13GHz or higher
RAM	8GB minimum; 16GB is recommended
Disk space	Depends on the number of AD objects, Azure AD objects, Exchange mailboxes and SharePoint Online and OneDrive for Business sites backed up. RecoveryManager Plus typically compresses backups to a third of their original size. If the total size of the AD and Azure AD objects, mailboxes, SharePoint Online and OneDrive for Business sites is 1TB, make sure that you have 2TB of free disk space to store the full backup and all subsequent incremental backups.

3. Operating systems

3.1 Installing RecoveryManager Plus on client machines

RecoveryManager Plus can be installed on machines running the following operating systems:

- Windows Server 2008 and above
- Windows Vista SP2 and later

3.2 32-bit vs. 64-bit operating systems

You can run RecoveryManager Plus on both 32-bit and 64-bit operating systems for Active Directory, Azure Active Directory, SharePoint Online, and OneDrive for Business environment backup, but you must run RecoveryManager Plus on a 64-bit OS to back up Exchange (on-premises and Exchange Online).

We recommend running RecoveryManager Plus on a 64-bit operating system for better performance.

4. Databases

RecoveryManager Plus comes with a built-in PostgreSQL database. However, the product also supports MS SQL databases.

If your company is a large enterprise, MS SQL is ideal for a few reasons:

- It's easier to manage and organize data in MS SQL, especially when working with a large amount of data.
- MS SQL is a self-tuning database that requires less manual configuration.
- The backup process in MS SQL is easier and faster than PostgreSQL.
- Parameters can be added to avoid DB lock and table lock in MS SQL.

5. Browsers

RecoveryManager Plus supports the following browsers:

- Internet Explorer 8 and later
- Mozilla Firefox
- Google Chrome

6. Security and mail settings

To improve the performance and security of the product, we recommend you take the following actions.

6.1. Run RecoveryManager Plus as a service

This ensures that you don't have to restart the application in case the system in which RecoveryManager Plus is installed restarts.

To install and start RecoveryManager Plus as a service:

- Stop RecoveryManager Plus if it is running
- For Windows 8 and later, **Start > All Apps > RecoveryManager Plus > Stop RecoveryManager Plus.**
- For all other OS versions, **Start > All Programs > RecoveryManager Plus > Stop RecoveryManager Plus.**

Install as a service

- For Windows 8 and later, **Start > All Apps > RecoveryManager Plus > Install RecoveryManager Plus as a service.**
- For all other OS versions, **Start > All Programs > RecoveryManager Plus > NT Service > Install RecoveryManager Plus as a service.**

Start RecoveryManager Plus as a service

- Navigate to **Start** menu > **Run** and type **services.msc.**
- Right-click **ManageEngine RecoveryManager Plus** and then click on **Properties.**
- Navigate to **Logon Tab** and choose **This Account.** Provide the credentials of an administrator and click **OK.**
- Right-click **ManageEngine RecoveryManager Plus** and click **Start.**

6.2 Change the default admin password

When you log in to RecoveryManager Plus for the first time, the default username and password to login is admin and admin. It is imperative to change the default password to something more complex and restrict network access from others who can access the application.

To change the default admin password,

- Open RecoveryManager Plus and log in as the administrator using the default password.
- Click the icon in the top-right corner of the screen.
- Click **Change Password.**
- Enter the **Old Password.**
- Provide a **New Password** and confirm it in the succeeding field.
- Click **Update.**

6.3 Running the product in HTTPS

To run RecoveryManager Plus in HTTPS,

- Log in to RecoveryManager Plus and navigate to **Admin** tab > **General Settings > Connection.**
- Select the **Enable SSL Port** checkbox for secure transfer of data via encryption. Use the default SSL port 8558 or use a port number of your choice.
- Click **Save.**

6.4 Configure a mail server

When you configure a mail server with RecoveryManager Plus, the application can send email notifications to administrators on the status of backup and restoration operations. This will allow administrators to monitor scheduled backups without having to open the application every time.

To configure a mail server:

1. Navigate to **Admin** tab > **General Settings** > **Server.**
2. Specify the **hostname or IP address** and **Port Number** of the mail server.
3. In the **From Address** field, enter the mail address that has to be displayed as the sender's email when reports are delivered via email.
4. In the **To Address** field, enter the mail address to which you'd like to send the reports.
5. Choose the **Connection Security (SSL/TLS)** from the drop-down menu.
6. Mark the check box against the **Authentication** field and enter the 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.**

6.5 Configure a notification profile.

Define the actions for which you wish to be notified.

1. Navigate to **Admin** tab > **General Settings** > **Notification.**
2. Click the **Create New Notification** button located at the top-right corner of the screen.
3. Provide an identifiable name in the field provided.
4. In the **Operations** field, select the component and actions for which you wish to receive notifications.
5. In the AD tab, select the domain from the drop-down box. Select the operations for which you wish to be notified (Backup, Restore, Recycle, Rollback).
6. In the Exchange tab, select the tenant/organization from the drop-down box. Select the operations for which you wish to be notified (Backup, Restore).
7. In the SharePoint tab, select the **Tenant** from the drop-down box. Select the operations for which you wish to be notified (Backup, Restore).

8. You can choose to be notified for all operations, or operations that have ended in failure, or get a consolidated notification mail at fixed intervals. Select an option depending on your choice:
   All operations carried out by the product.
   All operations that have ended in failure.
   Scheduled notifications.
9. Email notifications can be sent to multiple mail addresses. To send notifications to multiple mail addresses, separate each email address by a comma (,).
   Note: Mail addresses provided in this field will have higher priority than the mail address provided in the Mail Server section.
10. Click **Save.**

7. Best practices for AD backups

7.1 Active Directory object backup and recovery

7.1.1 Repository

By default, both full and incremental backups of AD objects are stored in the Elasticsearch database that comes bundled with RecoveryManager Plus. You can configure the product to store backups on any other machine.

Configurations relating to your AD backups are stored in the pgSQL database that comes bundled with RecoveryManager Plus. You can also use an MS SQL database.

The storage space required depends on the number of full backups you want to keep.

7.1.2 Incremental backup frequency

We recommend running incremental backups daily during non-business hours.

8. Exchange backup and recovery

8.1 Azure Active Directory object backup and recovery

8.1.1 Repository

By default, both full and incremental backups of Azure AD objects are stored in the Elasticsearch database that comes bundled with RecoveryManager Plus. You can configure the product to store backups on any other machine.

Configurations relating to your AD backups are stored in the pgSQL database that comes bundled with RecoveryManager Plus. You can also use an MS SQL database.

The storage space required depends on the number of full backups you want to keep. We recommend retaining at least three full backups.

8.1.2 Incremental backup frequency

We recommend running incremental backups daily during non-business hours.

9 Exchange backup and recovery

9.1 Repository

Full and incremental backups of Exchange (on-premises and Exchange Online) mailbox items are stored in a storage repository of your choice. You can configure the product to store backups on the local machine, any other machine in the network, or on cloud storage solutions like Azure Blob Storage and Azure file shares.

Configurations related to your Exchange backups are stored in the pgSQL database that comes bundled with RecoveryManager Plus. You can also use an MS SQL database.

The required space varies based on the number and size of the mailboxes being backed up, as well as your retention policy.

9.2 Incremental backup frequency

We recommend running incremental backups daily during non-business hours to minimize the time it takes to complete backups and ensure minimal changes occur to mailboxes when they're being backed up.

10. SharePoint Online/OneDrive for Business backup and recovery

10.1 Repository

Full and incremental backups of SharePoint Online and OneDrive for Business items are stored in a storage repository of your choice. You can configure the product to store backups on the local machine, any other machine in the network, or on cloud storage solutions like Azure Blob Storage and Azure file shares.

Configurations relating to your SharePoint Online and OneDrive for Business backups are stored in the pgSQL database that comes bundled with RecoveryManager Plus. You can also use an MS SQL database.

The required space varies based on the number and size of the SharePoint Online and OneDrive for Business sites being backed up, as well as your retention policy.

10.2 Incremental backup frequency

We recommend running backups daily during non-business hours to minimize the time it takes to complete backups and ensure minimal changes occur to the sites when they're being backed up.