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, Microsoft Entra ID (formerly Azure Active Directory), Microsoft 365, Google Workspace, on-premises Exchange, and Zoho WorkDrive backup needs. We have compiled this best practices guide 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 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2011
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7

Exchange Server

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

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

Active Directory

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

Microsoft Entra ID

You can use RecoveryManager Plus to back up all objects in your Microsoft Entra ID environment.

Exchange Online, SharePoint Online, and OneDrive for Business

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

Google Workspace

You can use RecoveryManager Plus to back up all mailboxes and user drives in your Google Workspace environment.

Zoho WorkDrive

You can use RecoveryManager Plus to back up all items in your Zoho WorkDrive Teams and the members' drive.

2. Hardware requirements

Hardware		Minimum requirement
Processor		2.13GHz or higher
RAM		8GB minimum; 16GB is recommended
Disk space	Active Directory / Microsoft Entra ID	This requirement varies based on the number of AD objects, Microsoft Entra ID objects, the size of your domain controller, and the retention period that you set for your backups. RecoveryManager Plus has a best case compression ratio of 2:1 for domain controller backups.
	Microsoft 365	This requirement varies based on the number of backed-up Exchange Online mailboxes, the size of your SharePoint Online and OneDrive for Business sites, and the retention period that you set for your backups. RecoveryManager Plus typically compresses backups to a third of their original size. If the uncompressed total size of the mailboxes, SharePoint Online, and OneDrive for Business sites is 1TB or more, make sure that you have at least 1TB of free disk space to store the full backup and all subsequent incremental backups.

	Google Workspace/ Zoho WorkDrive	This requirement varies based on the number of backed-up mailboxes, the size of your Google Workspace user drives, the size of your Zoho WorkDrive folders, and the retention period that you set for your backups. RecoveryManager Plus typically compresses backups to a third of their original size. If the uncompressed total size of the mailboxes, user drives, and folders is 1TB or more, make sure that you have at least 1TB of free disk space to store the full backup and all subsequent incremental backups.
	On-premises Exchange	This requirement varies based on the number of backed-up Exchange mailboxes and the retention period that you set for your backups. RecoveryManager Plus typically compresses backups to a third of their original size. If the uncompressed total size of the mailboxes is 1TB or more, make sure that you have at least 1TB 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 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7

4. Databases

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

If your company is a large enterprise, Microsoft SQL might be preferred for a few reasons:

- It's easier to manage and organize data in Microsoft SQL, especially when working with a large amount of data.
- Microsoft SQL is a self-tuning database that requires less manual configuration.
- The backup process in Microsoft SQL is easier and faster than PostgreSQL.
- Parameters can be added to avoid database lock and table lock in Microsoft 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 the **Start** menu > **Run** and type **services.msc**.
  Right-click **ManageEngine RecoveryManager Plus** and then click on **Properties.**
- Navigate to **LogonTab** 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 Enabling SSL

To enable SSL in RecoveryManager Plus,

1. Navigate to the **Admin tab → General Settings → Product Settings → Connection Settings.**
2. Choose your connection type as **HTTPS.**
3. Specify the port number of your choice after choosing the connection type. (Default port for RecoveryManager Plus - HTTPS: 8558).
4. 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.
5. Check **Keystore Password** that appears when you select HTTPS and enter the keystore password.
6. Click the **Advanced** option to use and specify the TLS versions and cipher suites of your choice.
   - In the **TLS** drop-down menu, select the TLS versions you want.
   - 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

7. You can also specify the cipher suites you want to use in the **Ciphers** field.
8. Select the domain for which you wish to enable LDAP SSL from the Enable LDAP SSL for drop-down menu.
9. Select the desired **Session Expiry Time** from the options in the drop-down box.
10. Check the **Help us improve the product by sending anonymous usage statistics** option to allow us collect your usage statistics.
11. Select **Enforce GDPR Compliance** to mask sensitive information from being displayed in the UI and to protect your database backups with a password. Setting a password for database backups is mandatory when GDPR compliance is enabled.
12. Click **Save.**

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

6.3.1 SSL configuration

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

Steps to apply SSL certificate

1. Navigate to the **Admin tab → General Settings → Product Settings → Connection Settings → SSL Certification Tool.**
   - If you don't have a SSL certificate, select the **Generate Certificate** option and follow the steps here.
   - If you already have a SSL certificate, select the **Apply Certificate** option and follow the steps here.

To generate SSL certificate

1. In the **Common Name** field, enter the name of the server.
   Example: For the URL https://servername:8558, the common name is servername.
2. In the **SAN Names** field, enter additional hostnames.
3. In the **Organizational Unit** field, enter the name of the department that you want to display in the certificate.
4. In the **Organization field**, enter the legal name of your organization.
5. In the **City** field, enter the name of the city as provided in your organization's registered address.

6. In the **State/Province field,** enter the name of the state or province as provided in your organization's registered address.
7. In the **Country Code** field, enter the two letter code of the country where your organization is located.
8. In the **Password** field, enter a password that consists of at least 6 characters to secure the keystore.
9. 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.
10. In the Public Key Length (In Bits) field, specify the size of the public key. Note: The default value is 2048 bits and its value can only be incremented in multiples of 64.
11. After all values have been entered, you can select either of these two options:

- **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 To apply an existing SSL Certificate section to apply the SSL certificate.
- **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 telling them that the website is not trusted, which may cause concern.

  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.

1. Select **Apply Certificate.**
2. Choose an Upload Option based on the certificate file type.

- **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.

- **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.
- Browser 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.
- **Certificate Content:**
- If your CA has sent the certificate content, then choose 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.

3. Click **Apply.**
4. Restart the product for the changes to take effect.

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.

RecoveryManager Plus provides two modes of mail server configuration:

1. SMTP
2. 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
   - OAuth authentication

Basic authentication

- Enter the **Username** and **Password** to access the mail server.
- If your mail server does not require authentication, leave the fields empty.

OAuth authentication

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

- 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.

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

6.5 Configure a notification profile

Define the actions for which you wish to be notified.

1. Navigate to the **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.**

6.6 Configure Two-factor authentication

Two-factor authentication 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 two-factor authentication is completed. Users with the **Admin** role can bypass TFA.

To enable TFA,

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

For detailed information on how to configure each of these secondary authentication methods, click here.

7. Best practices for AD domain controller backup

7.1 Repository

Configure a shared repository or make the local repository "shared" to retain backups of multiple domain controllers.

7.2 Encryption

We recommend enabling encryption for your backups to secure them.

7.3 Full backup frequency

We recommend scheduling full backups once every week.

7.4 Retention

Define a retention period for your backups, and discard older backups automatically once the retention period expires. We recommend retaining backups for at least one month.

7. 5 Suggested domain controller to configure

To perform forest-level restoration, having a writable domain controller is mandatory. In addition to this, it is advisable to back up domain controllers that are:

- Running Windows Server 2012 or higher versions as a virtual machine on a hypervisor that supports VM-Generation ID.
- A domain controller stored in a location that is easily accessible, whether physical or virtual, preferably located in a datacenter for convenient isolation during forest recovery.
- A domain controller that is running Domain Name System role and is hosting the forest and domain(s) zone.
- A domain controller which is the primary domain controller for domain-level recovery.
- A domain controller configured as a Global Catalog.

8. Best practices for AD backup

8.1 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 a Microsoft SQL database.

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

8.2 Incremental backup frequency

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

8.3 Archival duration

Define a retention period for your Active Directory backups, and delete them once the retention period expires. You can re-index the backed up files as and when necessary to facilitate restoration. We recommend setting the index retention to six months and the archive retention to 24 months.

9. Best practices for Microsoft Entra ID backup

9.1 Repository

By default, both full and incremental backups of Microsoft Entra ID 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 Microsoft Entra ID backups are stored in the pgSQL database that comes bundled with RecoveryManager Plus. You can also use a Microsoft 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.

9.2 Incremental backup frequency

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

9.3 Archival duration

Define a retention period for your Microsoft Entra ID backups, and archive them once the retention period expires. You can re-index the backed up files as and when necessary to facilitate restoration. We recommend setting the index retention to six months and the archive retention to 24 months.

10. Best practices for SharePoint Online/OneDrive for Business backup

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 Files. 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 a Microsoft 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.

11. Best practices for Google Workspace backup

11.1 Repository

Full and incremental backups of Google Workspace items are stored in a storage repository of your choice. You can configure RecoveryManager Plus to store backups on the local machine, on any other machine in the network, or on cloud storage solutions like Azure Blob Storage and Azure Files.

Configurations related to your Google Workspace backups are stored in the pgSQL database that comes bundled with RecoveryManager Plus. You can also use a Microsoft SQL database. The required space varies based on the number and size of the mailboxes being backed up, along with your retention policy.

11.2 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 while they're being backed up.

12. Best practices for Exchange backup

12.1 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 Files.

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

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

12.2 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.

13. Best practices for Zoho WorkDrive backup

13.1 Repository

Full and incremental backups of Zoho WorkDrive items are stored in a storage repository of your choice. You can configure RecoveryManager Plus to store backups on the local machine, on any other machine in the network, or on cloud storage solutions like Azure Blob Storage and Azure Files.

Configurations related to your Zoho WorkDrive backups are stored in the pgSQL database that comes bundled with RecoveryManager Plus. You can also use a Microsoft SQL database. The required space varies based on the number and size of the items being backed up along with your retention policy.

13.2 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 while they're being backed up.

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—such as domain controller recovery and object-, item- and attribute-level 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