ManageEngine
RecoveryManager Plus

Security hardening

for RecoveryManager Plus

www.recoverymanagerplus.com

Table of Contents

Abstract

With the increasing amount of attention on information security, it is essential for all IT administrators to strengthen security within their existing infrastructure to avoid possible breaches. This document focuses on the best ways to configure RecoveryManager Plus to ensure that your information stays secure.

Security hardening for RecoveryManager Plus

1. Following the principle of least privilege

RecoveryManager Plus backs up and restores multiple enterprise applications such as Active Directory, Azure Active Directory, Microsoft 365, Google Workspace, and Exchange servers. To configure backups for each application, a privileged account is required to configure the application with RecoveryManager Plus.

Application	Privilege required
Active Directory	Domain administrator
Azure Active Directory	Administrator with the **Global Admin** role
Exchange Online	User must be a member of the **Organization Management** role group
SharePoint Online and OneDrive for Business	User must be assigned the **SharePoint Administrator** role
Google Workspace	Administrator
On-premises Exchange	User must be a member of the **Organization Management** role group

The listed privilege is the least required privilege for backup and recovery of Azure AD, Microsoft 365, Google Workspace, and on-premises Exchange applications. However, for AD backup and restoration, a domain administrator account has several elevated rights and privileges not required by RecoveryManager Plus. You can create a dedicated service account that only has the required privileges and permissions needed for RecoveryManager Plus to perform its job. Here are the least privileges and permissions required for RecoveryManager Plus to back up your AD environment.

2. Securing the built-in admin account

RecoveryManager Plus comes with a built-in admin account with ultimate privileges. By default, this account's password is the same for every customer of RecoveryManager Plus. It is imperative that you change the password as soon as you log in to the product for the first time. RecoveryManager Plus will prompt you to change the password when you log in;, you need to change this password in order to properly secure it. If this step is overlooked, you will leave your system vulnerable.

3. Enabling HTTPS for secure communication

We recommend that you use HTTPS over HTTP to ensure secure transportation of information between the RecoveryManager Plus server and your web browser. You can enable HTTPS by following the steps listed below:

1. Log in to **RecoveryManager Plus** as an administrator.
2. Navigate to **Admin > General Settings > Connection.**
3. Check the box next to **Enable SSL Port [HTTPS]**. Use the default SSL port 8558 or use a port number of your choice.
4. Click **Save.**

These settings can be further optimized from within the following XML file:

1. Navigate to the location where RecoveryManager Plus is installed.
2. Open **conf\server.xml.**
3. Find the **HTTPS connector** corresponding to your configured SSL port number and optimize the settings as required.

If you choose to allow only a particular version of Transport Layer Security (TLS), namely TLSv1, TLSv1.1, or TLSv1.2, you can disable the other versions by modifying the **sslEnabledProtocols** parameter, keeping only the required TLS versions. For example:
sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"

4. Restricting logon access to the RecoveryManager Plus server

To further strengthen RecoveryManager Plus' security, we recommend that you restrict logon access to the RecoveryManager Plus server, thereby preventing unwarranted access. You can define the local policy settings for a specific set of users in the User Rights Assignment tab within the Group Policy Management Editor. You can choose to **Allow log on locally or Allow log on through Remote Desktop Services.** This way, you reduce the attack surface of your infrastructure.

5. Restricting access to the RecoveryManager Plus installation folder

Administrators can restrict access to the RecoveryManager Plus installation folder by modifying folder permissions. This ensures that no one except permitted users have access to RecoveryManager Plus' files.

6. Delegating and auditing technicians

Technician roles can be configured to restrict technicians from viewing just the modules they are given access to or performing specific functions such as restoration, roll back, or modifying backup settings configured in the product. In addition, RecoveryManager Plus provides a detailed, user-based audit trail of all actions performed by each technician. Learn more about restricting technicians' access and auditing technicians' actions.

7. Restricting database access from within the UI

RecoveryManager Plus, by default, disables database access from within its user interface and permits only the default administrator account to enable this option. The administrator can choose which accounts can or cannot access the database by creating separate technician roles with the necessary privileges. Learn how to create a custom role.

8. Using LDAP over SSL

RecoveryManager Plus allows administrators to enable **Lightweight Directory Access Protocol (LDAP)** over **Secure Sockets Layer (SSL)** to ensure that all communication of Active Directory data is encrypted. You can enable LDAP over SSL by following these steps:

1. Log in to **RecoveryManager Plus** as an administrator.
2. Navigate to **Admin > General Settings > Connection.**
3. Check the box next to **Enable LDAP SSL.**
4. Click **Save.**

9. CAPTCHA settings

To protect against bot-based, brute-force attacks attempting to break into the RecoveryManager Plus server, enable a CAPTCHA image on the login page. Users must enter the text shown in the CAPTCHA image (or played through audio) in order to log in to the product.

To configure a CAPTCHA for logins:

1. Log in to **RecoveryManager Plus** as an administrator.
2. Navigate to **Delegation > Configuration > Logon Settings > General.**
3. Under CAPTCHA Settings, check the box next to **Enable CAPTCHA on login page.**
4. RecoveryManager Plus provides two options to display a CAPTCHA.
   a. Select **Always show CAPTCHA** to display a CAPTCHA every time someone tries to log in to the product.
   b. Select **Show CAPTCHA after invalid login attempts** to enable a CAPTCHA only after a certain number of invalid login attempts. Enter the number of invalid login attempts allowed and the time (in minutes) that must pass before the invalid login counter is reset.
5. Select **Enable Audio CAPTCHA** to offer an audio reading of the CAPTCHA for visually impaired users. When this option is selected, only numeric values will be used for CAPTCHA. If the browser you use does not support audio CAPTCHA, the usual CAPTCHA (a combination of alphabets and numbers) will be displayed.
6. Click **Save.**

10. Block users

Temporarily prevent users or technicians from logging in to RecoveryManager Plus after a specified number of failed logon attempts within a certain period.

To create criteria for blocking users:

1. Log in to **RecoveryManager Plus** as an administrator.
2. Navigate to **Delegation > Configuration > Logon Settings > General.**
3. Under Block User Settings, check the box next to **Block user after invalid login attempts.**
4. In the Invalid attempts limit field, enter the **maximum number** of consecutive bad logons that you wish to permit. Enter the **duration** within which the specified number of bad logon attempts must happen to trigger blocking the user in the Within field.
5. Specify the **time** for which the user account must remain blocked in the Block user for field.
   Note: Please refer to the table below for the cases in which the domain's account lockout policy will apply instead of the settings configured in the **Block Users** settings.

Block Users settings	Condition	Domain Account Lockout Policy	Which would be applied
Number of invalid attempts	greater than	Account Lockout Threshold	Domain policy
Within field's value	greater than	Reset account lock out counter	Domain policy
Block duration	lesser than	Account lockout duration	Domain policy

6. Click **Save.**

11. Two-factor authentication

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 when 2FA 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 **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. Click on the name of any method to learn how to set up that method as the second authentication factor.
    a. Email verification
    b. Google Authenticator
    c. RSA SecurID
    d. Duo Security
    e. RADIUS Authentication

a. Email verification

When this option is selected, RecoveryManager Plus sends a verification code via email to the user's email address. The user has to enter the verification code to successfully login.

Prerequisites: To use this method as your secondary authentication method, it is mandatory to have configured a mail server with RecoveryManager Plus. If you haven't already, follow the steps listed here to configure a mail server.

1. Mark the checkbox against **Enable Email verification.**
2. Provide a subject line and message of your choice. You can personalize the message with Macros. To view the list of available Macros, click on the **Macros** link at the bottom of the message text box.
3. Click **Save.**

b. Google Authenticator

When this option is selected, users will be required to enter a six-digit security code generated by the Google Authenticator app for identity verification.

1. Click on the Enable Google Authenticator button.
2. When users next try to log in to RecoveryManager Plus, they will be prompted to add Google Authenticator as a verification method after authentication using username and password is successful. Select **Google Authenticator** and click **Next.**
3. Install and open Google Authenticator on your mobile phone.
4. Navigate to **Scan a QR code** in your Google Authenticator app and scan the QR code present in the RecoveryManager Plus login screen. Copy the code displayed in the authenticator app and enter the code in the space provided on the login page.
5. Mark the checkbox against **Trust this browser** if you do not want to verify every time you log in to this particular device. You will only be asked to verify once every 180 days.
   Note: Do not use this option if more than one person use the same machine.
6. Click **Verfiy Code.**

c. RSA SecurID

Users can use the security codes generated by the RSA SecurID mobile app, hardware tokens, or tokens received via mail or SMS to log in to RecoveryManager Plus.

1. Log in to your RSA admin console (e.g., https://RSA machinename.domain DNS name/sc).
2. Navigate to **Access > Authentication Agents.** Click **Add New.**
3. Add RecoveryManager Plus server as an **Authentication agent** and click **Save.**
4. Navigate to **Access > Authentication Agents** and, click **Generate Configuration File.**
5. Download **AM_Config.zip** (Authentication Manager config).
6. Extract **sdconf.rec** from the **AM_Config.zip to <-installation-dir>/bin.** If there is a file named **securid** (node secret file), copy it too.
7. In RecoveryManager Plus, mark the checkbox against **Enable RSA SecurID.**
8. Click **Browse** and select the **sdconf.rec** file.
9. Click **Save.**

d. Duo Security

Users can use the six digit security codes generated by the Duo mobile app or push notification to log in to RecoveryManager Plus.

1. Login to your Duo Security account (e.g., https://admin-325d33c0.duosecurity.com) or sign up for a new account, and log in.
2. Navigate to the **Applications** section in the left pane.
3. Click on the **Protect an Application** option.
4. Search for **Web SDK** and click on **Protect this Application.**
5. Copy the **Integration Key, Secret Key**, and **API Hostname.**
6. In the RecoveryManager Plus console, mark the checkbox against **Enable Duo Security.**
7. Paste the **Integration Key, Service Key, and API Hostname** copied in the previous step.
8. Select the Desired Username Pattern from the available choices and click **Save.**

   Note 1: Please make sure you select the exact username pattern you use in Duo Security.

   Note 2: If you are using older versions of Internet Explorer, then add the API hostname (e.g., https://api-325d33c0.duosecurity.com) and admin console (e.g., https://admin-325d33c0.duosecurity.com) as a trusted or intranet site.

e. RADIUS Authentication

RADIUS-based two-factor authentication for RecoveryManager Plus can be configured in two steps.

Step 1: Integrate RADIUS with RecoveryManager Plus

1. Log in to RADIUS server.
2. Navigate to the **clients.conf** file (/etc/raddb/clients.conf).
3. Add the following snippet in the clients.conf file.

   client <RecoveryManagerPlusServerName>
   {
   ipaddr = xxx.xx.x.xxx
   secret = <secretCode>
   nastype = other
   }
4. Restart the RADIUS server.

Step 2: Configure RecoveryManager Plus for RADIUS

1. In RecoveryManager Plus, check the box next to **Enable RADIUS Authentication.**
2. Provide the **Server Name/IP address** and the **Server Port** in the respective fields.
3. Select the **Authentication Scheme** from the drop-down menu.
4. Provide the **Secret Key** that was added to the **clients.conf** file in **RADIUS** server.
5. Select the **Desired Username Pattern** from the available choices.
6. Provide a limit for the **Request Time Out (in seconds)** and click **Save.**

   Note: The username pattern is case sensitive. Please make sure you select the exact pattern (uppercase or lowercase) you use in your RADIUS server.

Need help?

If you have trouble configuring any of the above mentioned settings, please contact us at support@recoverymanagerplus.com. You can also schedule a free, personalized demo to receive expert guidance on tightening up your IT infrastructure's security.

To learn more about how RecoveryManager Plus can help you secure your enterprise applications, please visit: https://www.manageengine.com/ad-recovery-manager/.