RMR

Active Directory Edition - Getting Started

Table of Contents

General Information

Equifax, Target, Yahoo, Home Depot, and JP Morgan Chase all have one thing in common – they've all suffered debilitating data breaches in the past few years. Affecting billions of people and costing hundreds of millions of dollars in damages, these breaches are just the tip of the iceberg. Verizon's 2022 annual Data Breach Investigations report lists hundreds of thousands of documented breaches and incidents over the past year alone and those breaches are not just targeting billion dollar businesses. In fact, Verizon states, "most attacks are opportunistic and target not the wealthy or famous, but the unprepared." So, are you prepared for an attack on your Active Directory network?

What is RMR?

RMR (pronounced "armor") is a desktop application that secures your Active Directory network by exposing and closing dangerous security holes. RMR's sophisticated scanning engine combs your network for dozens of issues that have been used to attack Active Directory networks like yours, such as: non-administrators that can grant themselves admin rights, computers with insecure settings, and users with blank passwords. Allow RMR to analyze your domain to locate these issues, then after the scan completes, review your results and fix the issues detected with a single click. With a tool this simple, there's no excuse to leave your network vulnerable.

Proactive Protection

Don't wait until after an attacker takes advantage of your network's lax security to address your problems. RMR analyzes every user, group, computer and group policy object in your directory to proactively identify and shut down known loopholes ***before*** the attacks happen.

Real-time Remediation

New security threats appear constantly as policies change, new programs and files are installed, and new users and computers are added to your network. Run scheduled scans every day to ensure that you detect these new issues as soon as they appear. Address the issues yourself with a single click, or let RMR take care of the problems automatically and find out what happened with a report delivered straight to your email.

Easy Undo

Even the most careful administrators misclick once in a while. That's why RMR comes with a built-in undo feature to easily revert any changes made to your Active Directory objects. Take comfort in the fact that RMR can undo fixes with a single click, perfectly restoring the affected objects to their prior state.

Minimum System Requirements

The following requirements must be met in order to install and run RMR for Active Directory.

- A PC running MS Server 2012/2016/2019/2022, Windows 8/10/11.
- Connection to a 2008, 2012, or 2016 Active Directory network.
- 150MB of disk storage for the software and additional space for scan history files.
- Network user account with domain administrative rights and administrator privileges on the local machine

Installing RMR

Before running your first scan with RMR for Active Directory, it needs to be installed. The RMR installation file is called adrmrXY.exe, where X and Y represent the current major and minor version numbers. Install this program to the computer you want to use to scan Active Directory. The machine you choose must be running in order to run scheduled scans, so we recommend installing to a server or another machine that is rarely turned off.

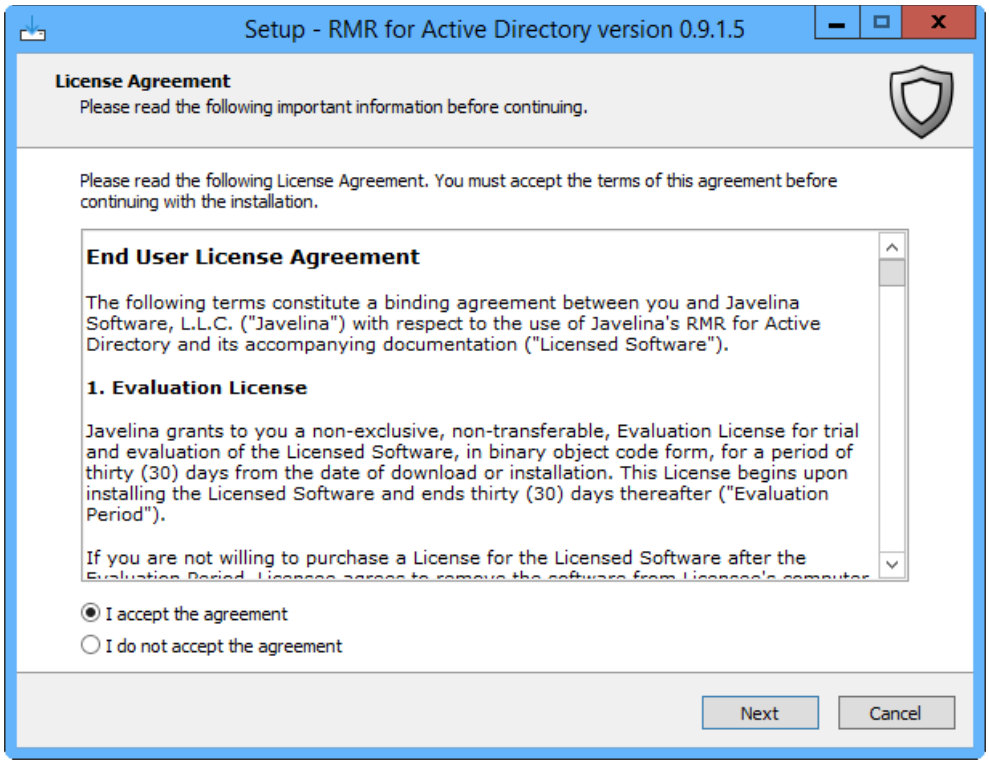

Figure 1: RMR Installer

After reading and agreeing to the End User License Agreement as shown above, continue through the install wizard using the default options for the remaining pages.

Applying your license

RMR is installed with a demonstration license that will allow you to use the software for a short period of time. In order to ensure that your protection does not elapse, the first thing you'll want to do after installing RMR is to apply your license key.

Open the program and click the **Register** button at the bottom of the Status panel on the Home View. Enter your license info exactly as it appears in the email you received, and click OK to save your changes. Assuming you entered the information correctly, you'll notice the **Days Remaining** field in the Status panel has been updated to reflect the new settings.

Using RMR

The following sections of this document will explain the basic things you need to know so that you can start using RMR to protect your Active Directory network. After finishing this document, you should have a solid understanding of the program and be able to navigate it to perform standard scans and repair issues.

Running your first scan

After installing RMR, you'll want to get a feel for the initial state of your network. So, let's run a scan and see exactly how your network security can be improved. From the **Scan** view, choose the **Full Scan** option (pictured below) to start the scan.

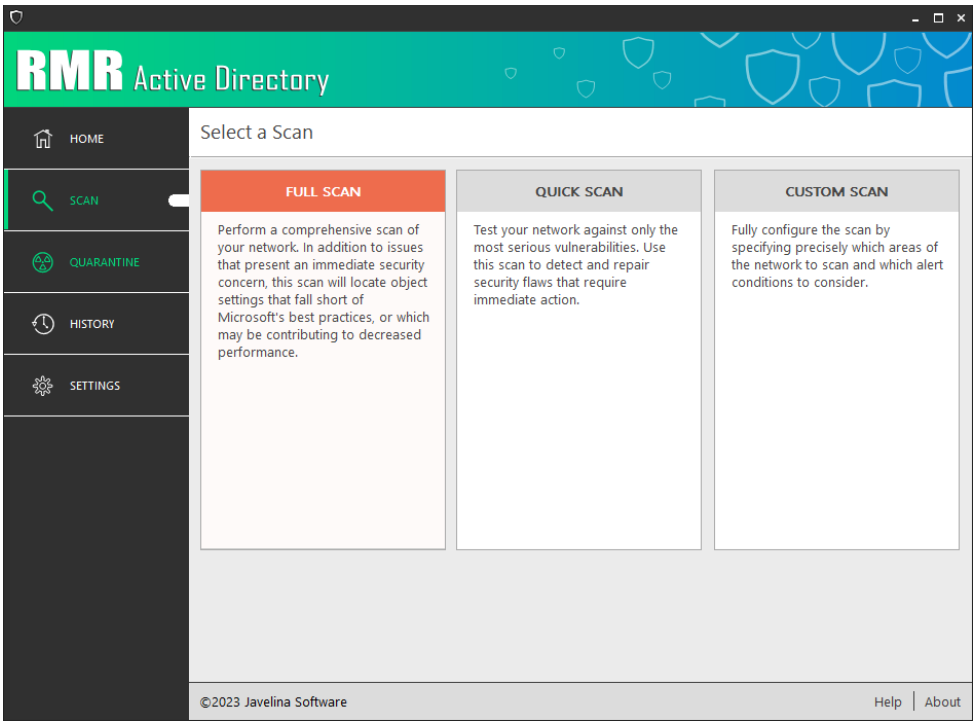

Figure 2: Selecting a Scan

While your scan is running, let's talk about the different types of scans:

Full Scan

Full Scans provide you with a thorough view of the security flaws in your Active Directory network. In addition to issues that require immediate attention, a Full Scan will notify you of situations that could lead to issues long-term including "Users with Old Passwords" and "Computers with Updates Disabled". Such issues, if not resolved, provide avenues of access for uninvited network guests.

Quick Scan

Quick Scans are used to identify the most serious security flaws in your network. These issues provide opportunities for attackers and should be considered as immediate security concerns. As the name implies, the Quick Scan can be used to quickly determine whether you've addressed your network's most critical security holes.

Custom Scan

Custom Scans allow the user to fully configure the scan. Select a specific scan area to quickly identify security issues within a troublesome segment of your directory. Or, toggle individual rules on or off to control which kinds of issues the scan will detect.

Viewing scan results

When your scan completes, you'll be taken to the Scan Summary View where you can see how many issues the scan revealed. Click the **View Details** button to launch the Scan Results dialog, where you can review the issues detected by the scan, and fix them.

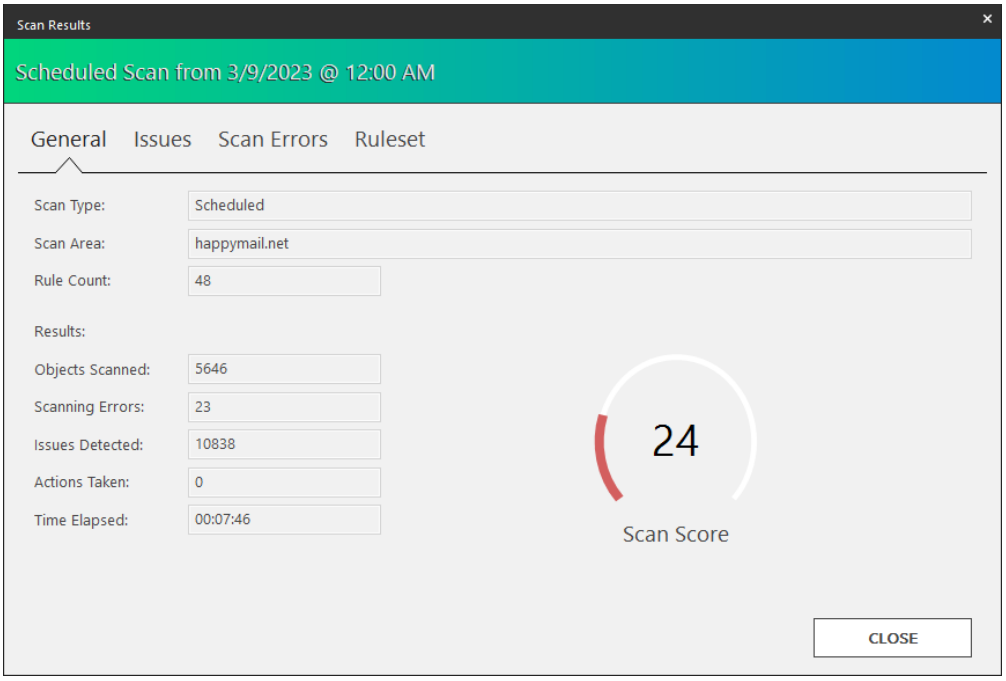

Figure 3: Scan Results dialog

The Scan Results dialog contains the following tab pages:

General

Get a quick summary of the scan, including which type of scan was run and which areas of your network were analyzed. The Scan Score on this tab represents how your network graded out on a scale of 0 to 100. Though a higher score is better, do not assume that a perfect score indicates a network free of security holes. After all, RMR only checks your network against the rules specified, and new vulnerabilities are discovered every day.

Issues

The most important tab of the Scan Results dialog, this is where you'll go to see exactly what issues were discovered, and fix them. This tab contains a table with a row for each issue detected during your scan. Each row contains the Issue Name and Severity, the name of the affected Object, a Recommended Fix, and a list of Actions that have been performed so far. Select one or more rows and click the **Fix** button to perform the Recommended Fix.

Quarantine
A common recommended fix is the Quarantine action. When objects are quarantined, they are disabled and moved to a special OU in Active Directory. From the **Quarantine** view, quarantined objects can be permanently deleted, or restored back to their original location and state.

The following table contains short descriptions for the controls on the Issues tab:

Fix	Perform the recommended fix for each object selected.
Undo	Undo the action(s) that have been performed on the currently selected objects, restoring the objects to their previous state.
Add Exception	Add the currently selected objects to a list of exceptions, so that they will not be detected in future scans. The Exceptions list can be managed from the **Exceptions** tab of the **Settings** view.

Scan Errors

Sometimes, RMR has trouble evaluating rules against objects in your network. This could be because a computer is turned off, restricted access rights, or any number of other situations. When this occurs, these incomplete tests are recorded here, so that administrators can investigate the cause of the error, and manually inspect the objects listed.

Ruleset

The Ruleset tab contains a list of the rules that were used to evaluate your network during this scan. Select a rule and click the **Details** button to read about the purpose of the rule, confirm exactly which settings the rule is checking, and find out how the issue can be manually checked for, or repaired if detected.

Changing the rules

When reviewing the results of your first scan, you may notice that RMR has stricter requirements for several rules than you would prefer (rules like "Inactive User" and "Insecure Password Policy"). Although we would suggest adopting the stricter standards rather than changing the rules, we understand that this is not always possible, at least in a timely fashion.

To that end, RMR's scan rules can be viewed and modified from the **Rules** tab of the **Settings** view.

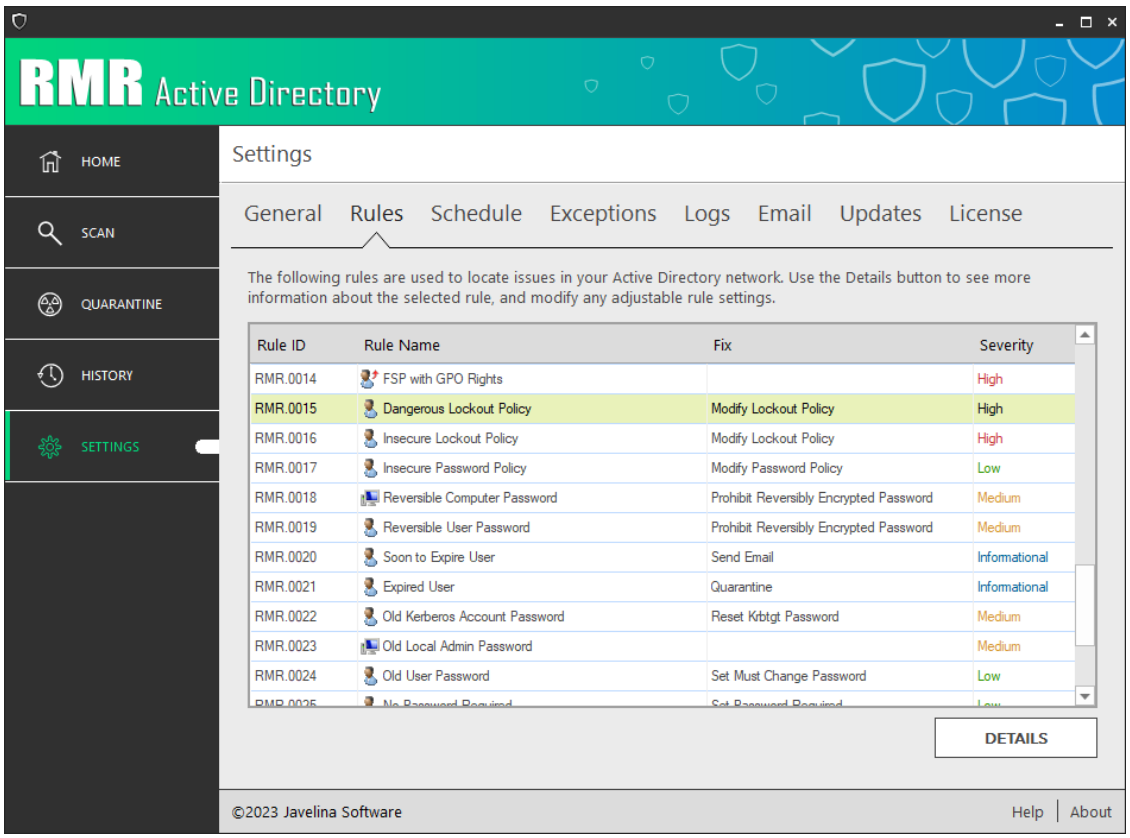

Figure 4: Changing the Rules

Select a rule from the grid, and then click **Details** to launch the Rule Settings dialog. The Rule Settings contains the following tabs:

Rule Info Tab

The Rule Info tab shows basic information about the rule, including its RMR ID and severity rating. It also provides a short description of the security holes that the rule is designed to prevent, and the ramifications of allowing objects to exist in this state.

Rule Settings Tab

Some rules have configurable parameters that control how the rule is evaluated against objects in your Active Directory network. If the rule evaluated during the scan had such configurable parameters, they will be displayed on the Rule Settings tab.

Rule Settings
Changing rule settings from the Rules tab of the Settings page will only affect future scans only. The results from prior scans will not be modified to reflect the new settings.

Fix Tab

The Fix tab contains the recommended fix for the rule. If the rule is used in a scheduled scan with automatic fixes enabled, the actions listed on this tab will be applied to each object found in violation of the rule. For all other types of scans, these are the actions that will occur if the **Fix Now** button is clicked in the Issue Details dialog.

Scheduled scans

RMR is most effective when scans are run on a regular basis. This type of scheduled scan can be set up on the **Schedule** tab of the **Settings** view.

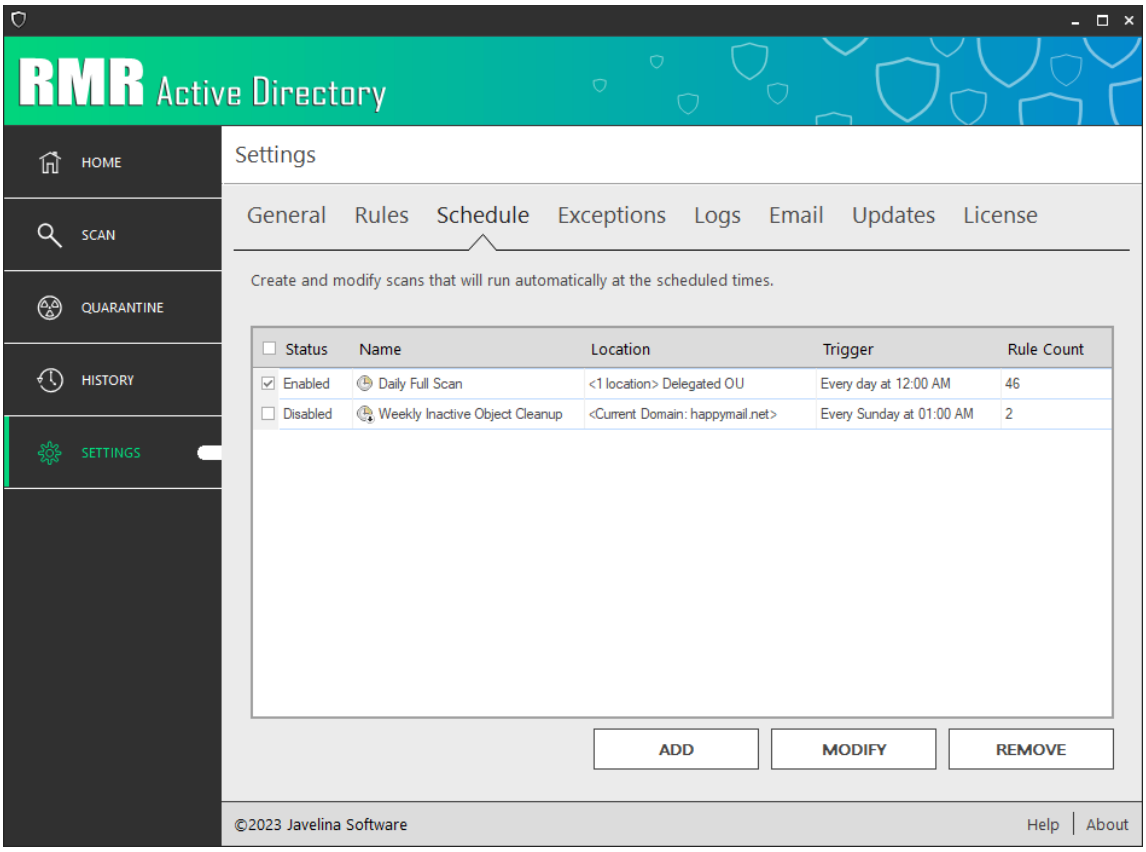

Figure 5: Scheduled Scans

The following table provides a short description of the settings on the Schedule tab:

Scan List	A list of scheduled scans that have been added to RMR. By default, a daily full scan is scheduled at midnight. Use the checkboxes at the left of the grid to enable or disable scheduled scans.
Add	Add a new scheduled scan to RMR.
Modify	Modify the selected scan to change its target area, ruleset, schedule, etc.
Remove	Delete the selected scheduled scan.

Click the **Add** or **Modify** button to launch the Scheduled Scan Editor. This dialog has several controls allowing you to modify the name, schedule, scope, and output settings for the scan, as well as the ruleset used. These settings are described in detail below.

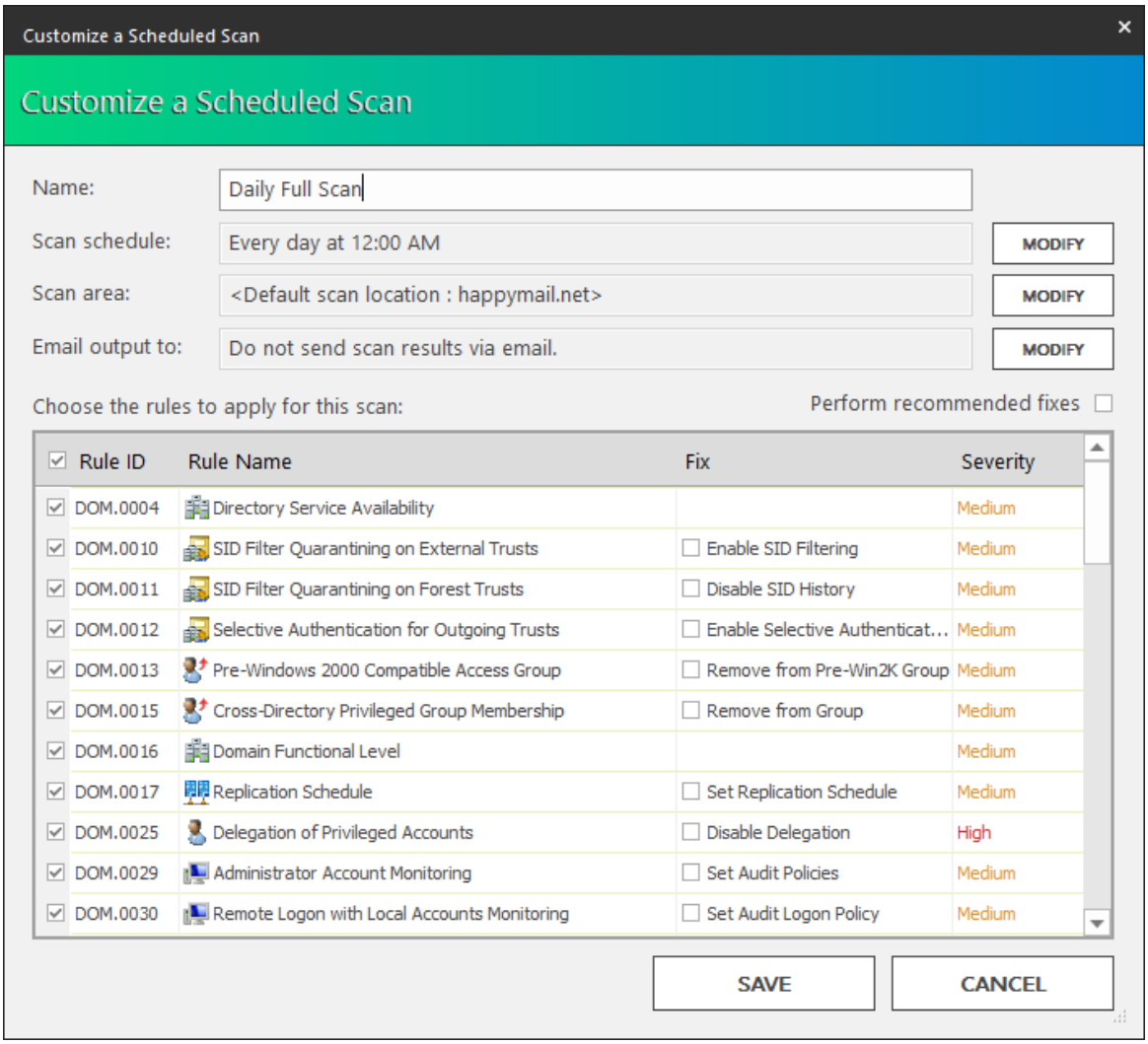

Figure 6: Configuring a scheduled scan

Name

Give a name to your scheduled scan so that you can easily identify it at a later time.

Scan Schedule

Click the **Modify** button to adjust the schedule for automated scans. In addition to the default value of every day, scans can be run on a particular day of the week at the specified time.

> **Picking a scan time**
> In order to scan for computer issues like disabled firewalls, disabled updates, or old passwords on local administrator accounts, RMR must be able to connect to the individual machines on your network. To get the most out of RMR, be sure to pick a scan time when the computers in your network are turned on.

Scope

The scope is the collection of places to be scanned. If you'd like to limit the scan to look for issues in only particularly troublesome segments of your network, click the **Modify** button to manually specify these areas.

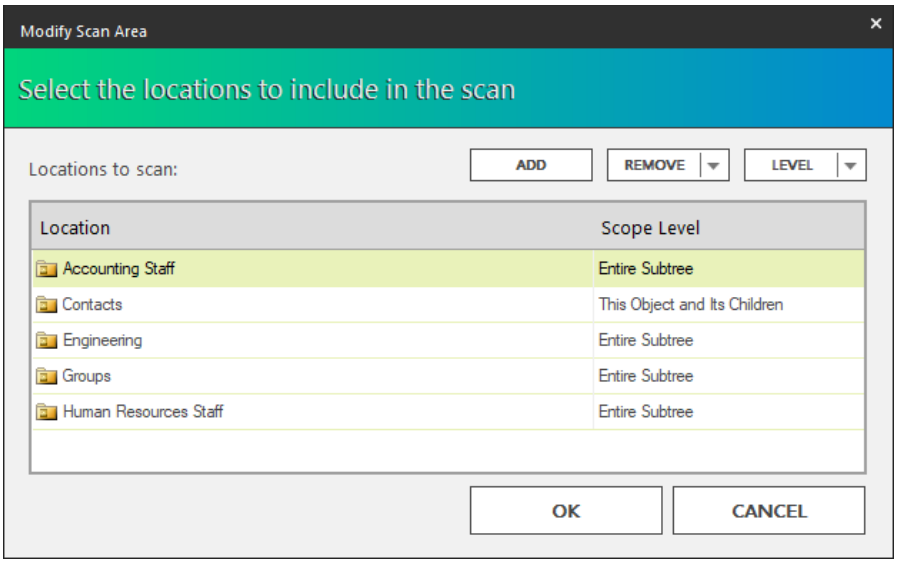

Figure 7: Scope dialog

The following table contains a list of controls on the Modify Scan Area dialog:

Add	Launch the **Active Directory Browser** to insert a new location to scan. In the browser dialog, click Add to move selected OUs to the right list box, then **OK** to add the contents of the right list box to the scan area.
Remove	Remove the selected location from the location list below. Or, select **Remove All** from the arrow to remove all specified locations.
Level	Select how many sub-objects to scan from the selection. Possible values for scope level are defined in the following table.

The following table contains a description of the various choices for Scope Level:

Entire Subtree	Include this container and all of the objects it contains, including subfolders.
This Object and its Children	Include this container and its immediate child objects. Objects in subfolders are not included.
This Object Only	Include this folder object only. All objects within this folder are not scanned.
Exclude this subtree	Exclude this folder and all objects within from the scan.
Exclude this object's children	Exclude this folder and its immediate children from the scan.

Email output to

Send a detailed scan report via email to one or more recipients by clicking the **Modify** button and entering the recipient email addresses (separated by semicolons). The Subject line of the email can also be changed here. Finally, specify a password to encrypt the RMR scan report attachment in the email. This is optional, but highly recommended.

> **Email Settings**
> In order to send scan results via email, RMR uses an SMTP email server. The login, port and other settings for this server are configured on the **Email** tab of the **Settings** view. Attempting to send scan reports without first specifying a mail server will fail.

Scan rules

The main grid on the Schedule Scan Editor contains a list of RMR's scan rules. By default, no rules are included in the scan. Use the checkbox in the Rule ID column to include the rule in the scan, or check the box at the top of the column to include all rules. Any rules left unchecked will be not be considered when analyzing objects for issues.

By default, RMR will not attempt to fix issues detected during scheduled scans. To change this behavior, check the **Perform recommended actions** checkbox immediately above the rule grid. After checking the box, you'll see the Fix column in the grid update to reflect the actions RMR will take upon detecting the issue in your directory. You can toggle on/off individual fixes to control whether specific rule infractions will be addressed automatically.

The specific fixes that will be performed can be modified by editing the corresponding rules on the Rules tab of the Settings view.

Reviewing old scans

After running a scheduled scan, you'll want to see the results and take care of any issues it detected. The results from all previous scans, including scheduled scans, can be analyzed from the **History** view.

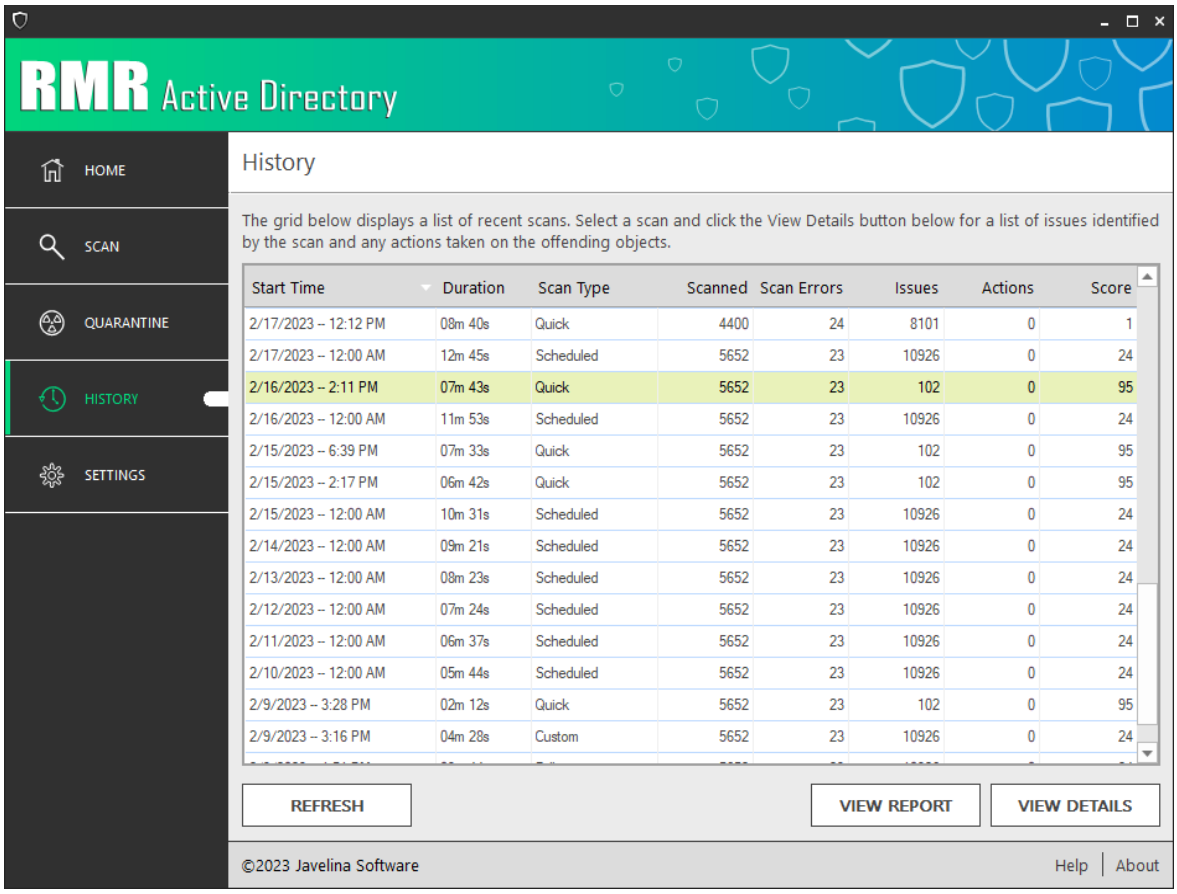

Figure 8: History View

Select a previous scan from the list, and then click **View Details** to see the results from the scan. This will launch the Scan Results dialog for the selected scan, where you can fix the issues detected, as well as undo previous fixes and add exceptions for future scans.

Updating RMR

Updates to RMR can be detected and installed directly from the program. Users with a non-expired license are eligible to receive updates to the software free of charge.

Configuring automatic updates

By default, RMR will check for updates daily at midnight. After finding and downloading an update, it will be installed the next time the program is launched. If these settings are acceptable to you, no changes need to be made. Otherwise, you can configure the update schedule and related settings by navigating to the **Updates** tab of the **Settings** view.

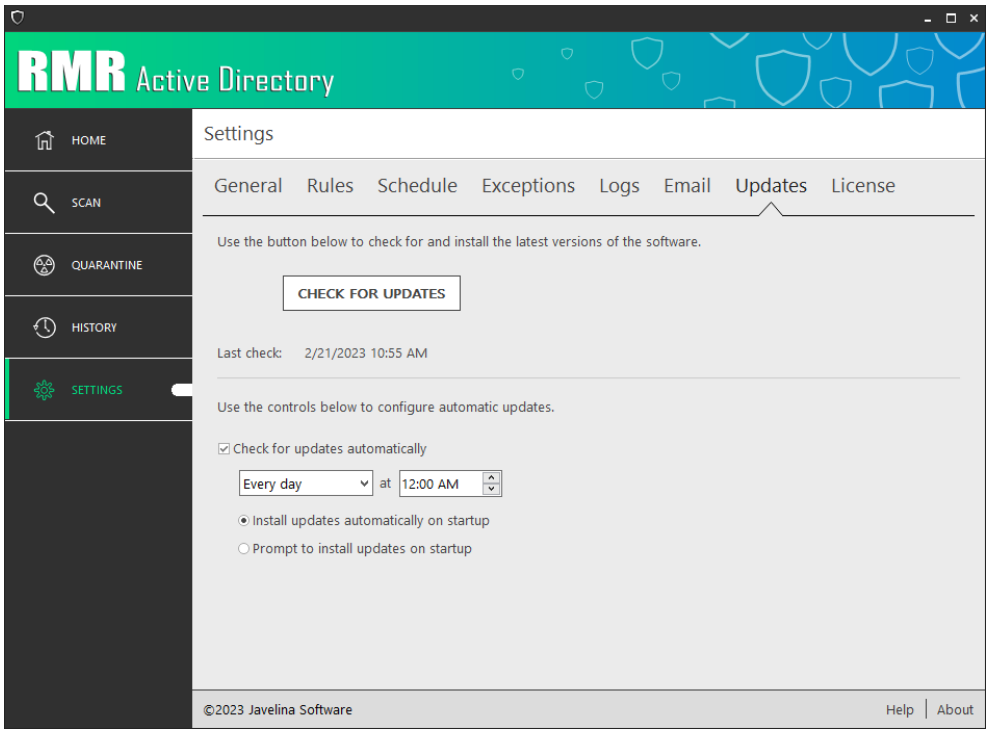

Figure 9: RMR Update Settings

Use the **Check for Updates** button to have RMR check for any available updates. If an update is detected, you will be prompted to install the update. The bottom half of the screen is used to configure automatic updates. The following table has a description of the controls and how they will affect RMR:

Check for updates automatically	Check this box to have the program automatically detect and download updates on a schedule. By default, RMR checks for updates every day at midnight. Clear this box if you want to manually install updates to RMR. **Note:** We recommend keeping this box checked to ensure that you have the latest scan rules and other new features as soon as they are released.
Install updates automatically on startup	Select this option to have RMR automatically install previously downloaded updates when the program is launched.
Prompt to install updates on startup	Select this option if you want the option to delay installing previously downloaded updates. On startup, you will be notified of a pending update, but will be given the option to postpone it until a later time.