Acronis

Acronis Cyber Cloud

Integration with N-able RMM

INTEGRATION GUIDE

Revision: 7/14/2021

Table of contents

1 Introduction

This document describes how to enable and configure the integration of Acronis Cyber Cloud with N-able RMM.

Once set up, the integration enables MSPs to:

- Deploy Acronis on Windows, Linux and macOS devices
- Monitor protected devices
- Apply and revoke protection plans
- Run the following types of automated tasks - backup, antivirus scan, malware scan, vulnerability assessment and patch management

All this functionality is available from within N-able RMM without having to go to the Acronis Cyber Protect web interface.

As an MSP, you can manage any number of N-able RMM accounts, using a single Acronis account.

2 Terminology

- **MSP** - A Managed Service Provider, who uses both N-able RMM and Acronis Cyber Protect
- **Customer** - A client of the MSP
- **Customer tenant** - a customer account on Acronis Cyber Cloud

3 Prerequisites

To use this integration, you should have:

- At least a single fully configured N-able RMM account
- An Acronis Cyber Cloud account with the following characteristics:
  - at least a single setup customer tenant
  - a minimum of one protection plan, configured to be used as the default one

4 How the integration works

The integration between Acronis Cyber Protect Cloud and N-able RMM is script-based and enables remote mass-deployment of Acronis agent on as many workloads as necessary, with minimal efforts.

During installation, the Acronis agent will be deployed on the computer, the computer - registered with the Acronis Cloud and, if configured, a default protection plan will be applied.

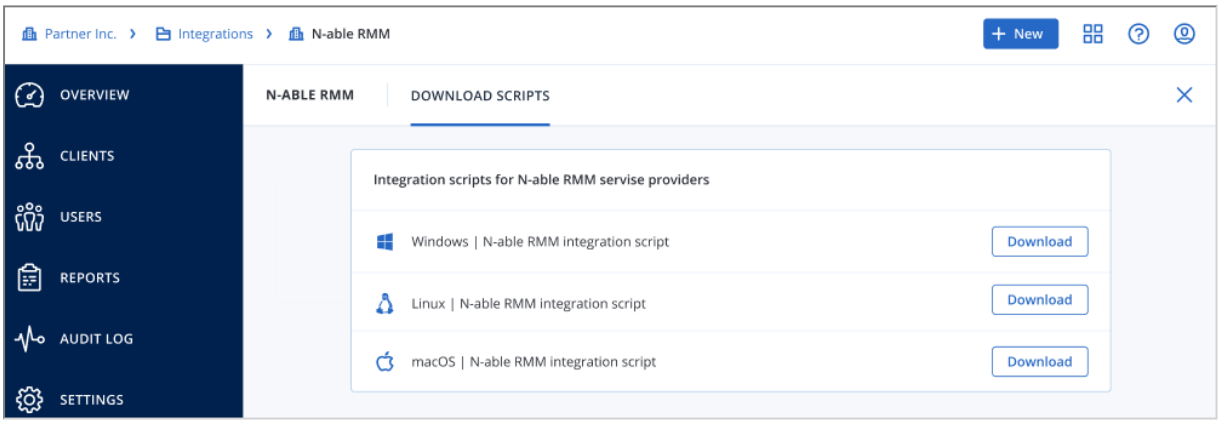
The scripts allow to automate a wide range of cybersecurity tasks by efficiently managing, configuring and monitoring cyber protection plans and statuses through a single interface.

5 Setup

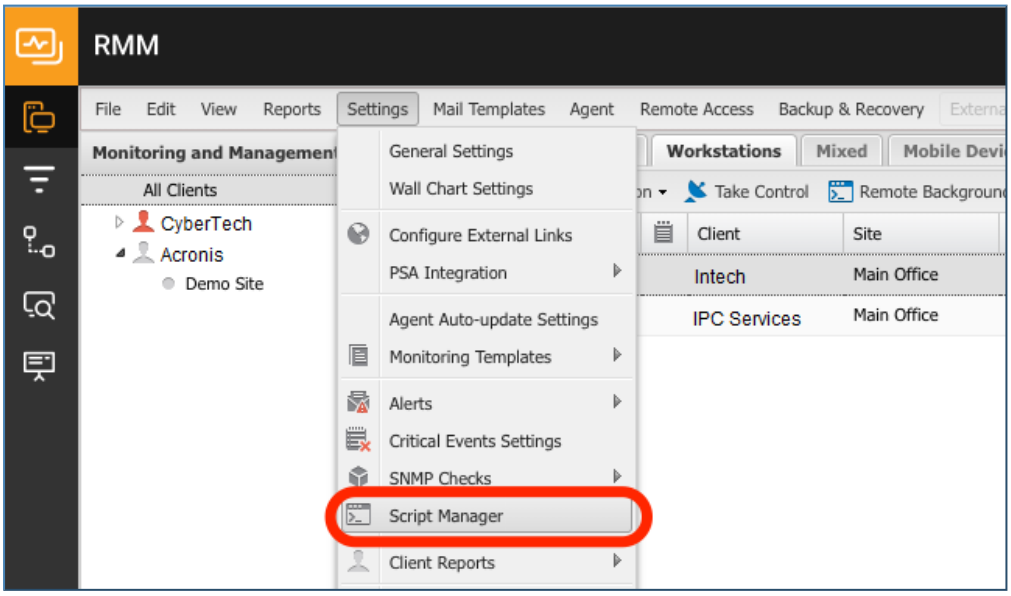
To set up Acronis integration for N-able RMM:

1. Go to **Acronis Cyber Protect Cloud Management Console** > **Settings** > **Integrations**.
2. Click on the **N-able RMM** tile.

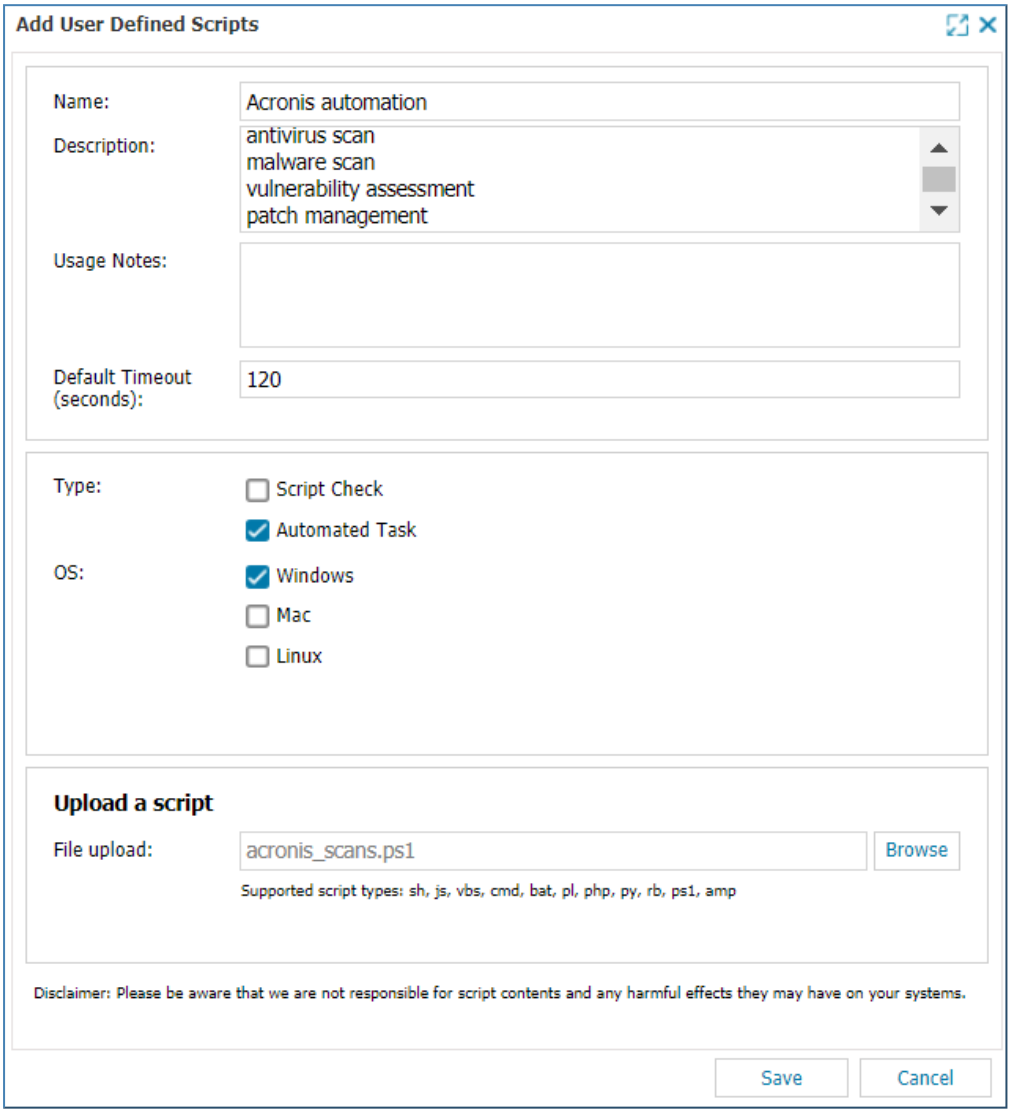
3. Download the Acronis_RMM_Integration.zip file from the **Download Scripts** tab.



4. Go to **N-able RMM** > **Settings** > **Script Manager** and click **New**.



5. Populate the script **Name**, **Description** and **Usage Notes** fields.
6. Check the **Automated Task** script type option and select OS (Windows, Linux, Mac).
7. In the **Upload a script** section, click the **Browse** button, located right next to the **File upload** field, then upload the desired script.



8. Click **Save** to keep the changes.
9. Highlight the device in the north pane.
10. Go to **Tasks** and click **Add Automated Tasks**.
11. Make a script selection.

> **Note**
> Only scripts, associated with the device's Operating System and uploaded for Automated Tasks, are displayed.

12. Click **Next** to configure the Task.
13. Enter or configure the following script parameters:

- **Revoke** with **Yes** and **No** options (set to **No** by default; interpreted **No**, if left empty)
- **TaskType** that accepts one of the following values:
  - backup
  - av_scan
  - malware_scan
  - vulnerability_assessment
  - patch_management
  - Set to **Backup** by default; interpreted as **Backup**, if left empty.
- **Acronis Cloud URL**
- **Acronis Registration Token**
  - the MSP has to manually generate the Registration token with maximum lifetime value in the Acronis Cyber Protect Cloud Management Console and copy the token's value to the N-able RMM parameter.
- **Acronis Data Center URL**

14. Set a Script timeout in the range from 1 to 3600 seconds (default value is 120 seconds) and click **Next**.
15. When done, click **Finish** to save and apply.

For every supported OS (Windows, Linux and mac), there is a total of 5 scripts in the zip file: Acronis Install Agent, Acronis Uninstall Agent, Acronis Manage Protection Plan, Acronis Monitoring and Acronis Scans.

6 Deploying the Acronis Cyber Protection agent

1. In the N-able RMM interface, highlight the device in the north pane.
2. Go to **Tasks**.
3. Right-click on the **Acronis Install Agent** Task.
4. Run an **Automated Task**.
5. Select **OK** in the **Run Task** message.

7 Uninstalling the Acronis Cyber Protection agent

1. In the N-able RMM interface, highlight the device in the north pane.
2. Go to **Tasks**.
3. Right-click on the **Acronis Uninstall Agent** Task.
4. Run an **Automated Task**.
5. Select **OK** in the **Run Task** message.

8 Manage protection plans

1. Highlight the device in the N-able RMM north pane.
2. Go to **Tasks**.
3. Right-click on the **Acronis Manage Protection Plan** Task.
4. Run an **Automated Task**.
5. Select **OK** in the **Run Task** message.

9 Performing Acronis scans and tasks for Windows, Linux and macOS

1. Highlight the device in the N-able RMM north pane.
2. Go to **Tasks** and click **Add Automated Tasks**.
3. Make a script selection.

> **Note**
> Only scripts, associated with the device's Operating System and uploaded for Automated Tasks, are displayed.

4. Click **Next** to configure the Task.

5. In the **Descriptive Name** field, add one of the following:
   - Run a backup
   - Run antivirus scan
   - Run malware scan
   - Run Vulnerability assessment
   - Run Patch Management

6. Enter the **TaskType** script parameter and add one of the following values:
   - backup
   - av_scan
   - malware_scan
   - vulnerability_assessment
   - patch_management

7. Set a **Script timeout** in the range from 1 to 3600 seconds (default value is 120 seconds). Then click **Next** to set the frequency and **Finish** to save and apply.
8. Highlight the device in the N-able RMM north pane.
9. Go to **Tasks** and right-click on the **Acronis Manage Protection Plan** Task.
10. Run an **Automated Task** and click **OK** in the **Run Task** message.

Acronis Scans runs one of the following tasks on the current device:

- Run a backup
- Run antivirus scan
- Run malware scan
- Run Vulnerability assessment
- Run Patch Management

10 Monitoring Windows devices

1. Log into the N-able RMM Dashboard and highlight a Windows device in the north pane.
2. Go to **Tasks** and click **Add Automated Tasks**.
3. Select the **Acronis Monitoring** script.

   Note
   Only scripts, associated with the device's Operating System and uploaded for Automated Tasks, are displayed.

4. Click **Next** to configure the Task.
5. In the **Descriptive Name** field, add **Acronis Monitoring** Task.
6. Enter the **GetAlerts** script parameter and add one of the following values:
   - Yes
   - No
   - Empty – interpreted as No
7. Enter the **Acronis Registration Token** script parameter. You need to manually generate the Registration token with maximum lifetime value in Acronis Cyber Protect Cloud Management Console and copy the token's value to the N-able RMM parameter.
8. Click **Next** to set the frequency.
9. Under **Select Frequency Method**, choose **Once per Day** > **Run on days** (select all weekdays) > **At Time** (set a time of your choice).
10. Click **Next** and then **Finish**.
11. Right-click a Windows device in the north **Servers, Workstations or Mixed** pane (or from the **Server** or **Workstation** drop-down).
12. Select **Monitoring Templates** > **Create Monitoring Template** > **Include tasks** > **Next**. This will open a new template, including the Automated Tasks from the selected Device.
13. In the **Add Monitoring** Template, provide **Acronis Monitoring** as **Template Name** for identification, click the **Active** box to ensure the template is selectable.
14. Configure the **Check Frequency** and **Checks and Tasks** options (links to further information included below).
15. Select the device in the north pane of the N-able RMM Dashboard, go to the **Checks** tab and click **Add**.
16. Choose **Add 24x7 Check** > **Event Log Check**.
17. On the Dashboard as well as in **Alerts** and **Reports**, provide the following identification name for the check: **Acronis Monitoring Event Log**.
18. Under **Event Log to query**, select **Application**.
19. Under **Event types**, select **Information**, **Warning** and **Error**.
20. Under **Event Source**, enter **Acronis Agent** and click **OK**.
21. Once the Check results are uploaded to the Dashboard, output details can be viewed in the **More Information** column.

11 Monitoring of Linux and macOS devices

1. Log into the N-able RMM Dashboard and highlight a Linux or macOS device in the north pane.
2. Go to **Tasks** and click **Add Automated Tasks**.
3. Select the **Acronis Monitoring** script.

> **Note**
> Only scripts, associated with the device's Operating System and uploaded for Automated Tasks, are displayed.

4. Click **Next** to configure the Task.
5. In the **Descriptive Name** field, add the following: **Acronis Monitoring Task Linux/Mac**.
6. Enter the **GetAlerts** script parameter and add one of the following values:
   - Yes
   - No
   - Empty – interpreted as No
7. Enter the **Acronis Registration Token** script parameter. You need to manually generate the Registration token with maximum lifetime value in Acronis Cyber Protect Cloud Management Console and copy the token's value to the N-able RMM parameter.
8. Click **Next** to set the frequency.
9. Under **Select Frequency Method**, choose **Once per Day** > **Run on days** (select all weekdays) > **At Time** (set a time of your choice).
10. Click **Next**, then **Finish**.
11. In the north **Servers, Workstations or Mixed** pane (or from the **Server** or **Workstation** drop-downs), right-click a selected Linux or mac device.
12. Select **Monitoring Templates** > **Create Monitoring Template** > **Include tasks**, then click **Next**.
13. This opens a new template, including the Automated Tasks from the selected Device.
14. In **Add Monitoring Template**, provide the following identification Template name: **Acronis Monitoring**.
15. Click the **Active** box to ensure the template is selectable.
16. Configure the **Check Frequency** and **Checks and Tasks** options (links to further information included below).
17. Select the device in the Dashboard north pane, go to the **Checks** tab and click **Add**.
18. Select **Add DSC Check** > **Log File Check**.
19. In the **Log Name** field, enter pathTo\AcronisAgentDir\AcronisAlerts.log.
20. In the **Contains** field, enter the alert string to search for in the specified log file. For example, it can be just "Warning" or "Error" and will filter all Acronis alerts of this severity.
21. Finally, click **OK**.
22. Once the Check results are uploaded to the Dashboard, output details can be observed in the **More Information** column.