Acronis

Acronis Cyber Cloud
Integration with N-able RMM

INTEGRATION GUIDE

Revision: 8/6/2021
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 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 Glossary

- **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
- **North pane** - the north pane of the Asset Tracking Dashboard in N-able RMM contains overview information at Client and/or Site level. The information displayed depends on the left menu selection: whether computers or assets are chosen (for example, Other Network Devices or Software and Hardware item).

For more information, refer to the N-able RMM User guide.
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 of Acronis agents, the devices will be 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.

If anywhere throughout this document, you have to provide a registration token, here are the steps to obtain it:

1. Log in to the Cyber Protection console.
2. Click Add Device and scroll down to Registration token. Then click GENERATE.
3. Select a token with a maximum lifetime value and click GENERATE TOKEN.
4. Copy the generated token.
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).
7. In the **Upload a script** section, click the **Browse** button, located right next to the **File upload** field, then upload the desired script.

![Add User Defined Scripts](image)

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. Select a script.

**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)

**Note**
This parameter is used to apply or revoke a Protection plan.

• Optionally, set **TaskType** to one of the following values or leave empty to use **Backup**:
  ◦ backup
  ◦ av_scan
  ◦ malware_scan
  ◦ vulnerability_assessment
  ◦ patch_management

• **Acronis Cloud URL**
• **Acronis Registration Token** - see **instructions** on how to get it
• **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.

**Note**
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.
4. Run an Automated Task.
5. Select OK in the Run Task message.
9 Performing Acronis scans and tasks for Windows

1. Highlight the device in the N-able RMM north pane.
2. Go to Tasks and click Add Automated Tasks.
3. Select a 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. Optionally, enter a Description.
6. In the Script Parameters section, enter one of the values listed below, which represents the type of task that needs to be run:
   - 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. Click Next to set the frequency.
7. Under Select Frequency Method, choose Once per Day > Run on days (select all weekdays) > At Time (set a time of your choice).
8. Click Next and then Finish.
9. Right-click a Windows device in the north Servers, Workstations or Mixed pane (or from the Server or Workstation drop-down).
10. Select Monitoring Templates > Create Monitoring Template > Include tasks > Next. This will open a new template, including the Automated Tasks from the selected Device.
11. In the Add Monitoring Template, provide Acronis Monitoring as Template Name for identification, click the Active box to ensure the template is selectable.
12. Configure the Check Frequency and Checks and Tasks options (links to further information included below).
13. Select the device in the north pane of the N-able RMM Dashboard, go to the Checks tab and click Add.
14. Choose Add 24x7 Check > Event Log Check.
15. On the Dashboard as well as in Alerts and Reports, provide the following identification name for the check: Acronis Monitoring Event Log.
16. Under Event Log to query, select Application.
17. Under Event types, select Information, Warning and Error.
18. Under Event Source, enter Acronis Agent and click OK.
19. Once the Check results are uploaded to the Dashboard, output details can be viewed in the More Information column.