

Acronis Cyber Cloud

Integration with N-able N-sight RMM

Table of contents

Introduction	3
Glossary	4
Prerequisites	5
How the integration works	6
Setting up the integration	7
Setting up the integration in Acronis Management portal	7
Enable integration	7
Configure integration settings	9
Apply customer mapping	10
Download scripts	11
Setting up the integration in N-able N-sight RMM	12
Customer provisioning and deprovisioning	15
Manual provisioning	15
Automatic provisioning	15
Automatic deprovisioning	16
Deploying the Acronis Cyber Protection agent	17
Uninstalling the Acronis Cyber Protection agent	18
Installing the Acronis agent to a Domain Controller	19
Managing protection plans	20
Usage of scripts for macOS and Linux	21
Performing Acronis scans and tasks for Windows	22
Monitoring Windows devices	24

Introduction

This document describes how to enable and configure the integration of Acronis Cyber Cloud with N-able N-sight 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
- Provision RMM customers as new customer tenants in Acronis Cyber Protect Cloud

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

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

Glossary

- **MSP** - a Managed Service Provider, who uses both N-able N-sight 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 N-sight 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 N-sight RMM User guide](#).

Prerequisites

To use this integration, you should have:

- At least a single fully configured N-able N-sight 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

Only customer tenants that are not in Self-service mode or don't have Support Access disabled, can be managed by the integration.

How the integration works

The integration between Acronis Cyber Protect Cloud and N-able N-sight 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.

Setting up the integration

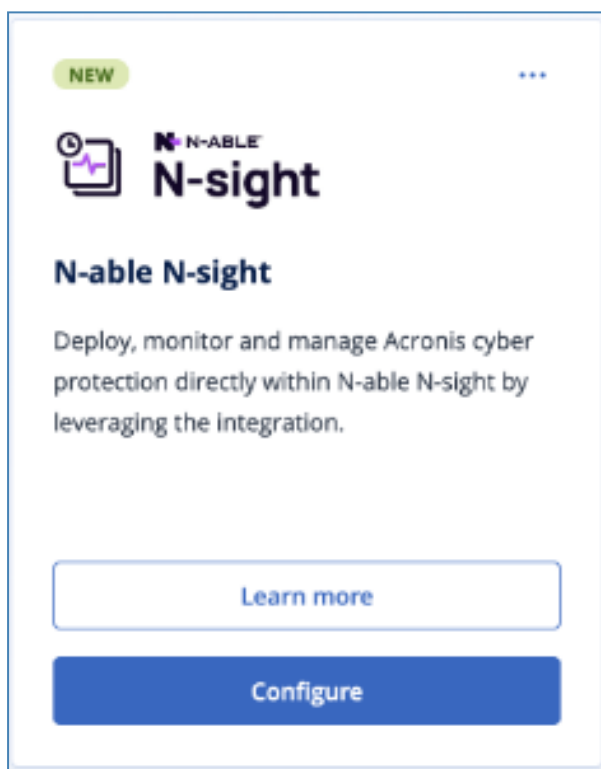
Setting up the integration in Acronis Management portal

To set up the integration, you have to enable it in the Acronis console and provide credentials to connect to the N-able N-sight RMM server. You may also provision customers from RMM by applying customer mapping and configure automatic customer provisioning/deprovisioning. Then download the scripts package, which will be required in order to proceed with the setup in N-able N-sight RMM.

Enable integration

To set up the Acronis integration for N-able N-sight RMM:

1. Go to the **Acronis Management portal** > **Integrations**.
2. Click **Configure** on the N-able N-sight RMM tile:



See [more information](#) about enabling and managing integrations.

3. Provide credentials to your N-able N-sight RMM account:

N-able N-sight

Provide credentials for the existing N-able N-sight account you want to connect.

Full documentation with step-by-step guide is available at:
<https://www.acronis.com/en-us/support/documentation/NableRMM>

▼

Save

See [how to generate API key](#) in N-able.

After having provided correct credentials, you will be redirected to **Integration settings**.

Configure integration settings

1. Go to the **Integration settings** tab.
2. On this page, you can do the following:
 - Modify credentials required for connection to N-able N-sight RMM server
 - [Configure automatic customer provisioning](#)
 - [Configure customer deprovisioning](#)

N-ABLE N-SIGHT

INTEGRATION SETTINGS

CUSTOMER MAPPING

DOWNLOAD SCRIPTS

Credentials

URL	https://www.ut.remote.management/
API Key	*****

Customer provisioning ⓘ

Provision customers as	Production
Activation email address	Not set
Automatically provision customers	Disabled
Two-factor authentication	Disabled

Customer deprovisioning ⓘ

Disable Acronis customer	Disabled
Delete Acronis customer	Disabled

Apply customer mapping


1. Go to the **Customer mapping** tab.
2. Using customer mapping, you can manually provision RMM customers to Acronis or map them to existing customers:

N-ABLE N-SIGHT				INTEGRATION SETTINGS		CUSTOMER MAPPING	DOWNLOAD SCRIPTS	×
+ Map to existing customer tenant		▶ Map to new customer tenant				1 item selected		×
<input type="checkbox"/>	N-able N-sight customer	↓	Mapping	↓	Acronis customer		↓	
<input checked="" type="checkbox"/>	Acronis		Not mapped		—			
<input type="checkbox"/>	Catalin		Not mapped		—			
<input type="checkbox"/>	Erby Industries		Not mapped		—			
<input type="checkbox"/>	Georgi PC		Not mapped		—			

- a. Select N-able N-sight RMM customer from the list and click **Map to existing customer tenant**.
- b. Select Acronis customer and save.

Map to existing customer

Select a customer tenant that will correspond to the "Acronis" account

 Acronis

- c. Select N-able N-sight RMM customer(s) and click **Map to new customer tenant** to create the corresponding new customer in Acronis and map them.

N-ABLE N-SIGHT			
INTEGRATION SETTINGS		CUSTOMER MAPPING	DOWNLOAD SCRIPTS
<div>Filters <input type="text" value="Search in N-able N-sight cust..."/></div>			
<input type="checkbox"/>	N-able N-sight customer ↓	Mapping ↓	Acronis customer ↓
<input type="checkbox"/>	Acronis	✔ Mapped	Acronis
<input type="checkbox"/>	Catalin	Not mapped	—
<input type="checkbox"/>	Erby Industries	Not mapped	—
<input type="checkbox"/>	Georgi PC	Not mapped	—

As a result, a new customer will be created in Acronis, based on the parameters, defined in [Integration settings](#) in **Customer provisioning** section.

Download scripts

1. Go to the **Download scripts** tab.
2. Download the integration scripts packages:


N-ABLE N-SIGHT

INTEGRATION SETTINGS


CUSTOMER MAPPING

DOWNLOAD SCRIPTS


Integration scripts for N-able N-sight

 Windows | N-able N-sight integration script

Download

 Linux | N-able N-sight integration script

Download

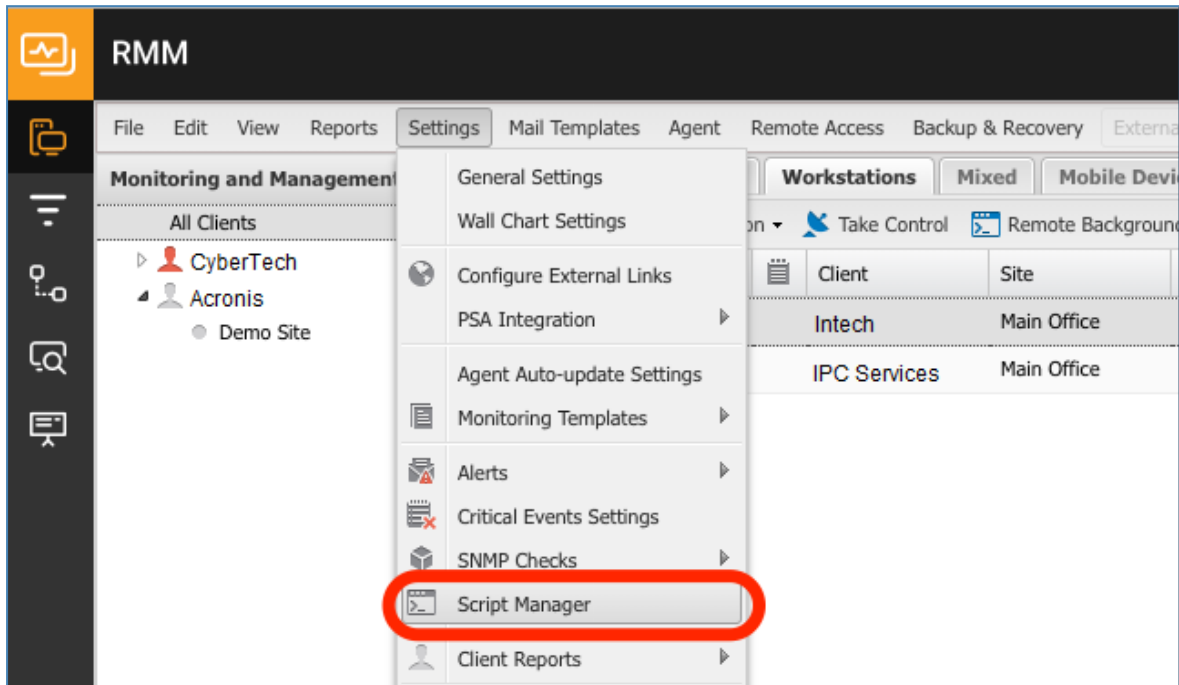
 macOS | N-able N-sight integration script

Download

These packages are required in order to proceed with the setup in N-able N-sight RMM.

Setting up the integration in N-able N-sight RMM

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



2. Populate the script **Name**, **Description** and **Usage Notes** fields.
3. Check the **Automated Task** script type option and select OS (Windows, Linux, macOS).

4. 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

Name:

Description:

antivirus scan
malware scan
vulnerability assessment
patch management

Usage Notes:

Default Timeout (seconds):

Type: ☐ Script Check ☒ Automated Task

OS: ☒ Windows ☐ Mac ☐ Linux

Upload a script

File upload:

Supported script types: sh, js, vbs, cmd, bat, pl, php, py, rb, ps1, amp

Disclaimer: Please be aware that we are not responsible for script contents and any harmful effects they may have on your systems.

5. Click **Save** to keep the changes.
6. Highlight the device in the north pane.
7. Go to **Tasks** and click **Add Automated Tasks**.

8. Select a script.

Note

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

9. Click **Next** to configure the Task.
10. 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
11. Set a Script timeout in the range from 1 to 3600 seconds (default value is 120 seconds) and click **Next**.
 12. When done, click **Finish** to save and apply.

Note

For every supported OS, 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.

Customer provisioning and deprovisioning

The integration makes the onboarding process easier by provisioning new customers from RMM. You can provision new customers manually from the **Customer mapping** tab or configure automatic provisioning in **Integration settings**.

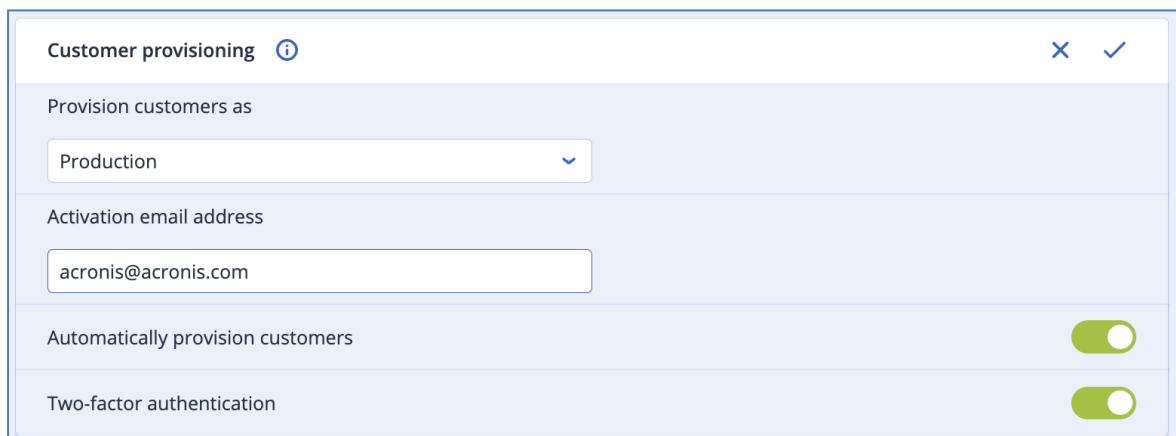
By default, customers are provisioned in **Managed by service provider** mode with the same services enabled as for the service provider and with all quotas set to unlimited.

Manual provisioning

Go to **Customer mapping** tab, see [Apply customer mapping](#).

Automatic provisioning

1. Go to the **Integration settings** tab.
2. Edit the **Customer provisioning** section to define the parameters, necessary to create new customer in Acronis:



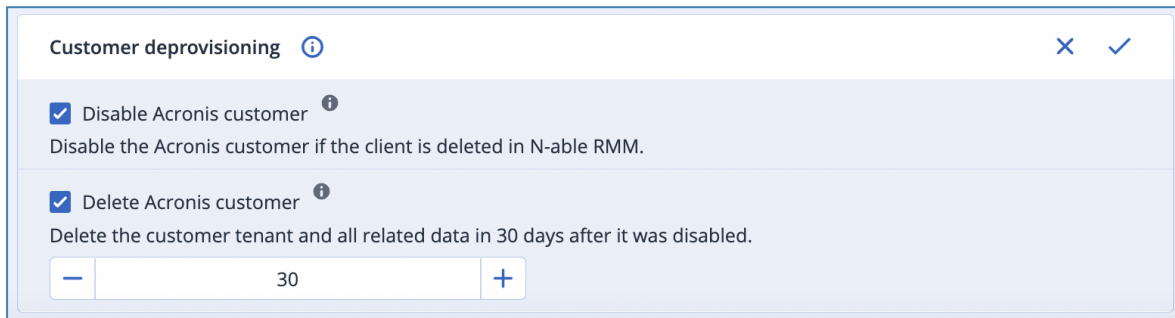
The screenshot shows a 'Customer provisioning' settings window. It has a title bar with a close button (X) and a checkmark button. The window contains four sections: 1. 'Provision customers as' with a dropdown menu set to 'Production'. 2. 'Activation email address' with a text input field containing 'acronis@acronis.com'. 3. 'Automatically provision customers' with a green toggle switch turned on. 4. 'Two-factor authentication' with a green toggle switch turned on.

- a. Provision customer in a **Production** or **Trial** mode
 - b. In the **Activation email address** field, enter the email address of an admin user that has to be created within the new customer tenant. This email will be used to send the activation link.
 - c. Switch the toggle button to enable the **Automatically provision customers** option.
 - d. Switch the toggle button to enable/disable **Two-factor authentication** for the admin user that has to be created within the new customer tenant.
3. Save the configuration.

If the **Automatically provision customers** feature was enabled, every 10 minutes the integration will launch to provision all newly created customers.

Automatic deprovisioning

1. Go to the **Integration settings** tab.
2. Edit the **Customer deprovisioning** section:



Customer deprovisioning ⓘ

☒ **Disable Acronis customer** ⓘ
Disable the Acronis customer if the client is deleted in N-able RMM.

☒ **Delete Acronis customer** ⓘ
Delete the customer tenant and all related data in 30 days after it was disabled.

— 30 +

3. Select the **Disable Acronis customer** option to automatically disable customer tenants in Acronis Cyber Protect Cloud after their deletion in RMM.
4. Select the **Delete Acronis customer** option and define number of days to automatically delete customers in Acronis Cyber Protect Cloud after selected number of days since it was automatically disabled due to deletion in RMM.
Specify 0 days to delete the customer immediately after RMM deletion. To prevent automatic disabled customer deletion, just enable the customer tenant in the Acronis Management console before the selected number of days is over.
5. Save the configuration.

If these features were enabled, every 10 minutes the integration will launch to deprovision customers deleted in RMM. Those customers have to be mapped using [Customer mapping](#).

Deploying the Acronis Cyber Protection agent

1. In the N-able N-sight 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.

Uninstalling the Acronis Cyber Protection agent

1. In the N-able N-sight 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.

Installing the Acronis agent to a Domain Controller

Follow the steps below in order to make an Acronis agent installation on a Domain controller from within N-able N-sight RMM. The integration applies a default protection plan on the DC and the agent runs under the selected user.

1. In the north pane of the N-able N-sight RMM interface, highlight the device on which you will install the agent.
2. Go to **Tasks** and click **Add Automated Task**.
3. In the **User-Defined** section, select the **Acronis Agent Install** script, then click **Next**.
4. Provide **Descriptive Name** for the task.
5. Populate the following script parameters:
 - a. **Acronis Cloud Url**
 - b. **Acronis Registration Token**
 - c. **Domain Controller Username**
 - d. **Domain Controller Password**
6. Click **Next**.
7. Select **Frequency Method** and adjust the **Daily Schedule Settings**.
8. Click **Next** again and set maximum permitted execution time.
9. When done, click **Finish**.
10. Right-click on the task you just created.
11. Click **Run Automated Task**, then **OK** in the **Run Task** message.

Managing protection plans

1. Highlight the device in the N-able N-sight 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.

Usage of scripts for macOS and Linux

For both macOS and Linux, the integration of Acronis Cyber Cloud with N-able N-sight RMM uses the following set of scripts to deliver various activities:

Script name	Functionality	Necessary arguments
Acronis_scans	Run one of the following tasks on the current device: <ul style="list-style-type: none">• Run a backup• Run antivirus scan• Run malware scan• Run vulnerability assessment• Run patch management	What task to run
Acronis_monitoring	This script takes all Acronis agent alerts for the device where it runs and inserts them into the <code>AcronisAlerts.log</code> file, located in the same folder where the script is run	None
Acronis_manage_protection_plan	<ul style="list-style-type: none">• Apply protection plan• Revoke protection plan	<ul style="list-style-type: none">• Registration token• Toggle to set Yes/No
Acronis_install_agent	<ul style="list-style-type: none">• Download installer• Execute installer• Register agent• Optionally, if we have a management token:<ul style="list-style-type: none">◦ Apply protection plan	<ul style="list-style-type: none">• Registration token• Data center URL
Acronis_uninstall_agent	Uninstall Acronis agent	None

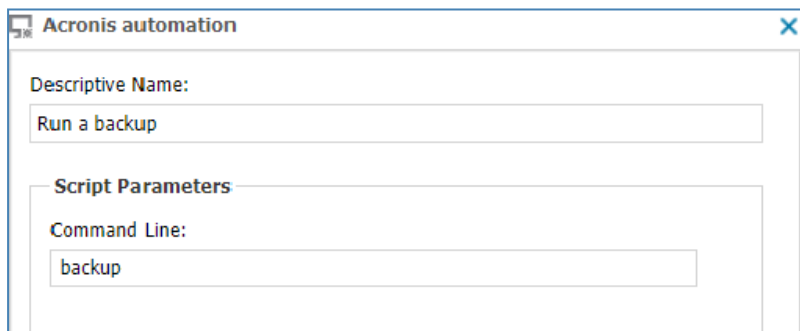
Performing Acronis scans and tasks for Windows

1. Highlight the device in the N-able N-sight 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



The screenshot shows a window titled "Acronis automation". Inside, there is a "Descriptive Name:" label followed by a text input field containing "Run a backup". Below this is a "Script Parameters" section, which contains a "Command Line:" label followed by a text input field containing "backup".

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 N-sight 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

Monitoring Windows devices

1. Log into the N-able N-sight 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 N-sight 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.