

Acronis Cyber Cloud

Integration with Datto RMM

Table of contents

Introduction	3
Terminology	4
Prerequisites	5
Localization	6
Permissions and roles	7
Mapping	8
How the integration works	9
Limitations of this integration	9
Set up the integration	10
Enable the integration	10
Configure integration settings	12
Apply customer mapping	13
Set an optional default protection plan	14
Remove or change a default protection plan	15
Remove or change a mapping	15
Download the components	16
Customer provisioning and deprovisioning	17
Manual provisioning	17
Automatic provisioning	17
Automatic deprovisioning	18
Deploy Acronis on workloads	19
Apply or revoke a protection plan	21
Monitoring and alerts	22
Run manual tasks	25
Alternative components usage	26

Introduction

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

Once setup, the integration enables MSPs to:

- Deploy Acronis on Windows, Mac and Linux workloads, managed by Datto RMM
- Monitor protected workloads
- Provision RMM customers as new customer tenants in Acronis Cyber Protect Cloud
- Get tickets for any alerts, related to such workloads

This functionality is available from within Datto RMM, without having to go to the Acronis Management portal.

Terminology

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

Prerequisites

To use this integration, you should have the following:

- A fully configured Datto RMM account
- An Acronis Cyber Cloud account with:
 - at least a single, setup customer tenant
 - optionally, at least 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.

Localization

This integration is available in the following languages:

- English
- German
- Spanish
- Hungarian
- French
- Italian
- Portuguese
- Swedish

The components are currently available in English only.

Permissions and roles

Only partner tenant users with Company Administrator roles are allowed to enable/disable or edit the integration.

All other users have Read-only access. This means that they can view, but not modify the integration settings.

Mapping

The integration uses the mapping listed below:

DATTO RMM ENTITY	ACRONIS ENTITY
Account	Partner tenant
Site	Customer tenant
Endpoint	Workload

How the integration works

The Acronis integration for Datto RMM consists of two parts:

- Configuration done from the Acronis Management portal in the following way:
 - a. Connect your Datto RMM account to your Acronis partner tenant
 - b. Map Datto RMM sites to Acronis customer tenants
 - c. Optionally, set a default protection plan for each site
- Datto components - available from the Datto RMM ComStore:
 - Acronis Cyber Protect - Deployment [WIN]
 - Acronis Cyber Protect - Deployment [MAC]
 - Acronis Cyber Protect - Deployment [LIN]
 - Acronis Cyber Protect - Manage Protection Plan [WIN]
 - Acronis Cyber Protect - Manage Protection Plan [MAC]
 - Acronis Cyber Protect - Manage Protection Plan [LIN]
 - Acronis Cyber Protect - Monitor [WIN]
 - Acronis Cyber Protect - Monitoring [MAC/LIN]
 - Acronis Cyber Protect - Tasks [WIN]
 - Acronis Cyber Protect - Tasks [MAC]
 - Acronis Cyber Protect - Tasks [LIN]

Each component is essentially a script that can be run on a workload or endpoint.

These scripts can:

- download, install and register the Acronis agent
- apply and revoke a protection plan
- run various manual jobs
- collect monitoring statuses and alerts, related to the endpoint the script is run on.

Once the integration is configured, it will create a site-level variable to store the registration key. This key is automatically refreshed by the integration and used by the components.

Limitations of this integration

When monitoring scripts, access is allowed only to protection statuses and alerts, related to the workload the script is run on. That's why you will have to run the respective component on every workload you want to monitor.

Set up the integration

Enable the integration

The first steps in setting up the integration are the exchange of API keys, necessary for Acronis to access your Datto RMM account, and to map any existing Datto RMM sites to new or existing Acronis customer tenants.

1. Make sure that the API on your Datto RMM instance is enabled.
2. Next, create an API key and secret for the user, necessary to manage the integration. Find detailed steps on how to do this in the [Datto documentation > How to Activate the API](#). We advise you to create a separate user in Datto RMM, only for the Acronis integration purposes.
3. Go to the **Acronis Management portal > Integrations** and click on the **Datto RMM** tile. See [more information](#) about enabling and managing integrations.
4. In the window that opens next, provide the following information:
 - a. Select the Datto RMM datacenter that hosts your account. The following options are supported:
 - i. Pinotage
 - ii. Merlot
 - iii. Concord
 - iv. Zinfandel
 - v. Syrah
 - vi. Vidal

- b. Provide the API key and secret you created in step 2.

Datto RMM

Provide credentials for the existing Datto RMM account you want to access.

Full documentation with step-by-step guide is available at:

<https://www.acronis.com/en-us/support/documentation/DattoRMM>

Datto RMM Server

API Key

CIJ8VRV6EI5Q8QEC68PSA5FTRQF1PC

API Secret

.....

Save

- c. Click **Save**.

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 Datto server
 - [Configure customer provisioning](#)
 - [Configure customer deprovisioning](#)

DATTO RMM

INTEGRATION SETTINGS

CUSTOMER MAPPING

Credentials

Datto RMM Server

Concord

API Key

CIJ8VRV6EI5Q8QEC68PSA5FTRQF1PCVB

API Secret

Customer provisioning ⓘ

Automatically provision customers

Enabled

Activation email address

admin@test.com

Two-factor authentication

Disabled

Provision customers as

Production

Customer deprovisioning ⓘ

Disable Acronis customer

Enabled

Delete Acronis customer

30 day(s) after it was disabled

Apply customer mapping

On the **Mappings** screen, map your Datto RMM sites to Acronis customer tenants. You will see a list of all sites, available in your Datto RMM account. Select a site and click one of the following options:

DATTO RMM INTEGRATION SETTINGS CUSTOMER MAPPING ×				
+ Map to existing customer tenant		▶ Map to new customer tenant		1 item selected ×
<input type="checkbox"/>	Datto RMM customer ↓	Mapping ↓	Acronis customer ↓	Default Protection Plan
<input type="checkbox"/>	AN_Beta_Lin	✔ Mapped	AN_Beta_Lin	—
<input checked="" type="checkbox"/>	AN_TestSite_ci3	Not mapped	—	—
<input type="checkbox"/>	AN_TestSite_Lin	Not mapped	—	—
<input type="checkbox"/>	bolzhat	Not mapped	—	—
<input type="checkbox"/>	Customerprovtest2	Not mapped	—	—
<input type="checkbox"/>	customerprovtest4	Not mapped	—	—

- **Map to new customer tenant** - to create and map the corresponding new customer in Acronis. As a result, this customer will be created in Acronis, based on the parameters, defined in Customer provisioning section > [Integration settings](#).

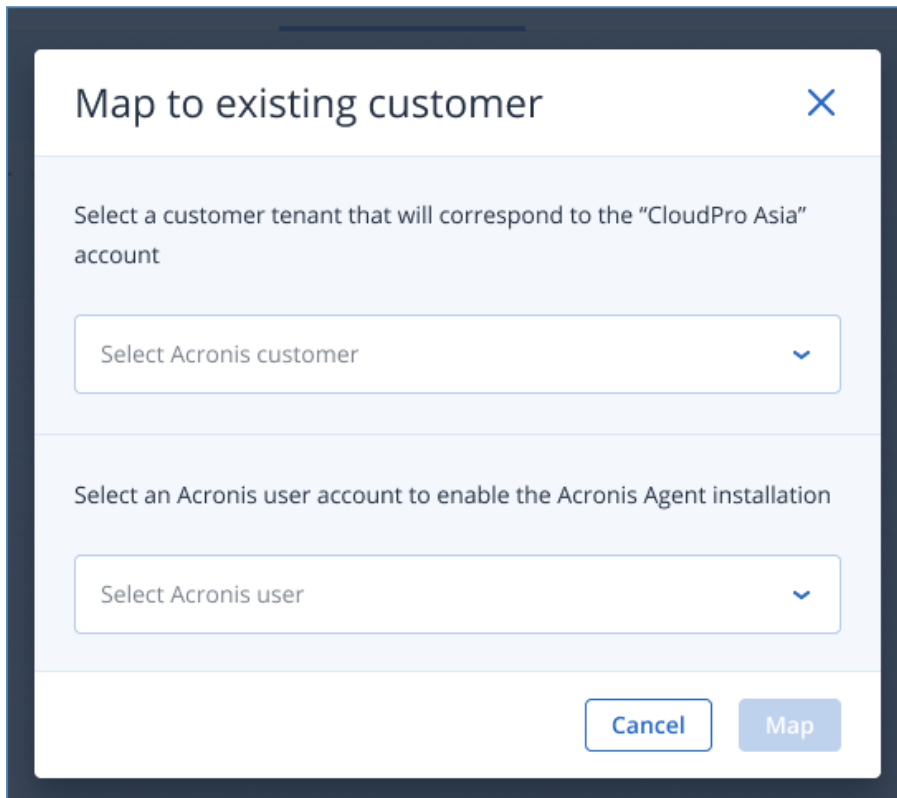
- **Map to existing customer tenant**

In the window that opens next, select an existing:

- customer tenant
- user for this customer tenant. All new workloads will be registered to this user in Acronis.

Note

This user should be assigned with the **Company administrator** role.



Finally, click **Map**.

At this point, the integration will create a site-level custom variable to store the registration key. The key is regularly updated by the integration and used by the components.

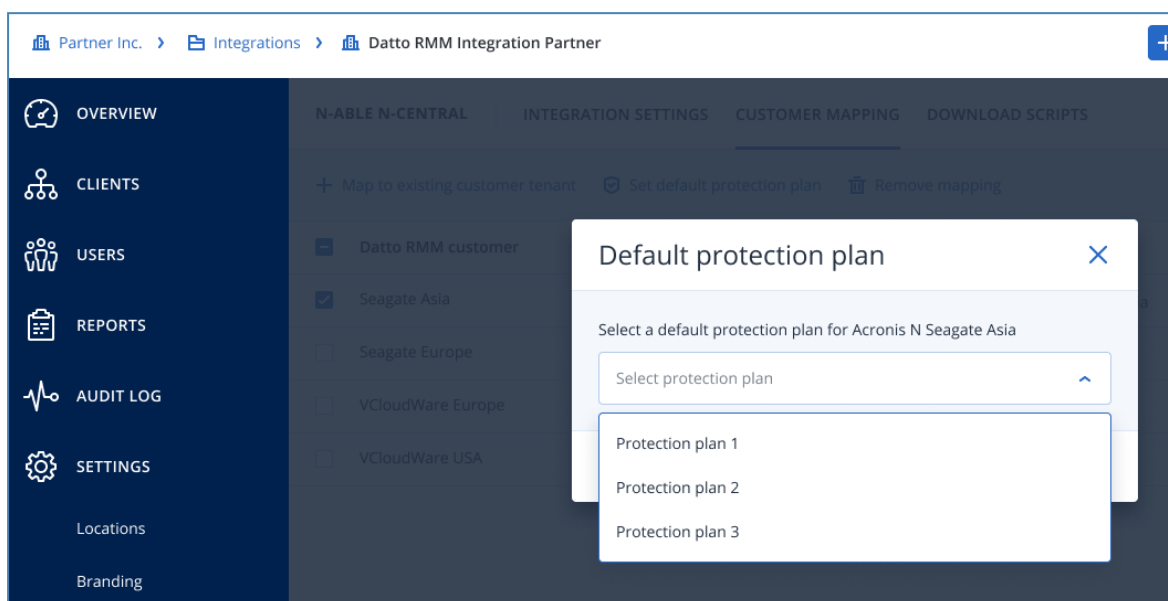
Continue the setup by optionally assigning default protection plans to all of your mapped sites or proceed with downloading the components.

Set an optional default protection plan

Once your sites are successfully mapped to customer tenants, you can set each a default protection plan. The plan that will be applied on every new workload should be registered using the integration's deployment components.

To set a default protection plan:

1. Select a mapped site and click **Default protection plan**.
2. In the window that opens, make a selection from the drop-down menu with available plans for the mapped tenant.



3. Once you are done, click **Set**.

Remove or change a default protection plan

To remove or change a configured default protection plan, do the following:

1. Go to the **Acronis Management portal > Integrations**.
2. On the **Datto RMM** tile, click the three dots (...) and select **Settings** from the drop-down menu.
3. Go to the **Customer Mapping** tab and select the site, for which you want to change or remove the default protection plan.
4. Click **Default protection plan**.
5. In the window that opens, click **Remove protection plan** or select a new one.
6. Click **Set** to store the changes you just made.

Remove or change a mapping

To remove the mapping between a Datto RMM site and an Acronis customer tenant:

1. Go to the **Acronis Management portal > Integrations**.
2. On the **Datto RMM** tile, click on the three dots (...) and select **Settings** from the drop-down menu.
3. Go to the **Customer Mapping** tab and select the site, for which you want to remove the mapping.

4. Click **Remove mapping**.
5. Click **Disconnect** in the confirmation window.

To change the mapping of an existing site, already mapped to an existing Acronis customer tenant:

1. Go to the **Acronis Management portal > Integrations**.
2. On the **Datto RMM** tile, click the three dots (...) and select **Settings** from the drop-down menu.
3. Go to the **Customer Mapping** tab and select the site, for which you want to change the mapping.
4. Click **Map to existing customer tenant**.
5. In the window that opens next, select a new customer tenant.
6. Click **Map** to save the changes you just made.

Download the components

From within Datto RMM, go to **ComStore > Category: All Components** and search for Acronis.

You will see the following components:

- Acronis Cyber Protect - Deployment [WIN]
- Acronis Cyber Protect - Deployment [MAC]
- Acronis Cyber Protect - Deployment [LIN]
- Acronis Cyber Protect - Manage Protection Plan [WIN]
- Acronis Cyber Protect - Manage Protection Plan [MAC]
- Acronis Cyber Protect - Manage Protection Plan [LIN]
- Acronis Cyber Protect - Monitor [WIN]
- Acronis Cyber Protect - Monitoring [MAC/LIN]
- Acronis Cyber Protect - Tasks [WIN]
- Acronis Cyber Protect - Tasks [MAC]
- Acronis Cyber Protect - Tasks [LIN]

Add the ones you need to your Component Library.

Note

Acronis Backup Monitor [WIN] is an older component, published by Datto. It doesn't support AcronisCyber Cloud and can't work with the current integration. For questions and further support about it, please contact [Datto](#) directly.

This completes the configuration. You can now proceed with [Deployment](#), [Monitoring](#) or [Tasks](#).

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

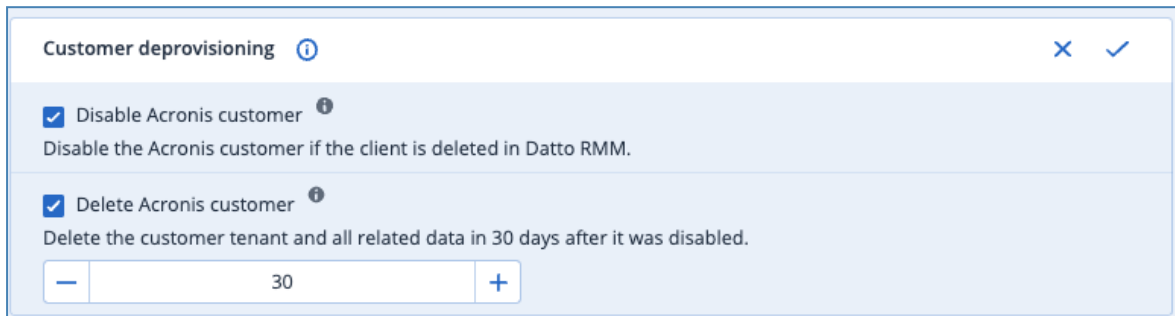
1. Go to the **Integration settings** tab.
2. Edit the **Customer provisioning** section to define the parameters, necessary to create new customer in Acronis:

- 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 Datto RMM.

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

— 30 +

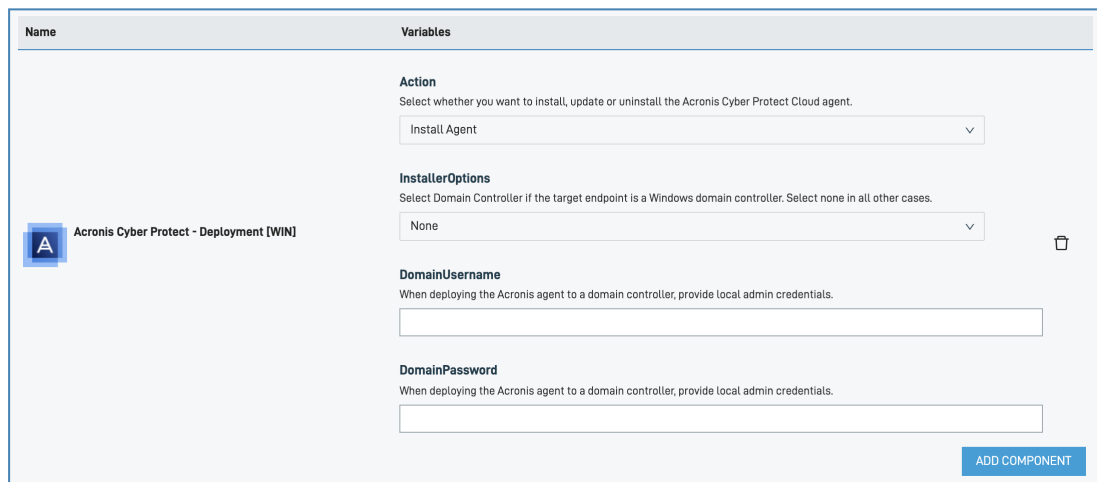
3. Select the **Disable Acronis customer** option to automatically disable customer tenants in Acronis Cyber Protect Cloud after their deletion in RMM.
4. Select the **Delete Acronis customer** option and define number of days to automatically delete customers in Acronis Cyber Protect Cloud after selected 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](#).

Deploy Acronis on workloads

By using the deployment components (downloaded as part of the setup), you can schedule deployment of Acronis on any Windows, Mac or Linux workload, managed by Datto RMM:

1. From within Datto RMM, go to **Jobs > New Job**.
2. Set a name for the new job and schedule when it should run.
3. Add job targets (workloads) that are already known to Datto RMM.
4. Add the Acronis installation component to the job, by selecting either:
 - Acronis Cyber Protect - Deployment [WIN]
 - Acronis Cyber Protect - Deployment [MAC]
 - Acronis Cyber Protect - Deployment [LIN]
5. In the **Variables** section:
 - a. Select what to do with the agent:
 - i. Install (default)





The screenshot shows the 'Variables' configuration page for the 'Acronis Cyber Protect - Deployment [WIN]' component. The page is divided into two main sections: 'Name' and 'Variables'. The 'Variables' section contains the following fields:

- Action:** A dropdown menu with the option 'Install Agent' selected. The description reads: 'Select whether you want to install, update or uninstall the Acronis Cyber Protect Cloud agent.'
- InstallerOptions:** A dropdown menu with the option 'None' selected. The description reads: 'Select Domain Controller if the target endpoint is a Windows domain controller. Select none in all other cases.'
- DomainUsername:** A text input field. The description reads: 'When deploying the Acronis agent to a domain controller, provide local admin credentials.'
- DomainPassword:** A text input field. The description reads: 'When deploying the Acronis agent to a domain controller, provide local admin credentials.'

An 'ADD COMPONENT' button is located at the bottom right of the form.

- ii. Update
- iii. Uninstall

- b. If you are installing the Windows agent, you'll see additional options for installation to a domain controller.
 - i. Select **Domain Controller** from the **InstallerOptions** drop-down menu.
 - ii. Provide username and password for the local admin on the domain controller.

Name	Variables
 Acronis Cyber Protect - Deployment [WIN]	<p>Action Select whether you want to install, update or uninstall the Acronis Cyber Protect Cloud agent.</p> <p>Install Agent ▾</p>
	<p>InstallerOptions Select Domain Controller if the target endpoint is a Windows domain controller. Select none in all other cases.</p> <p>None ▾ </p>
	<p>DomainUsername When deploying the Acronis agent to a domain controller, provide local admin credentials.</p> <p><input type="text"/></p>
	<p>DomainPassword When deploying the Acronis agent to a domain controller, provide local admin credentials.</p> <p><input type="password"/></p>
<p>ADD COMPONENT</p>	


- 6. Optionally, set advanced options, alerts, emails and job recipients, the same way as in the regular Datto RMM workflow.
- 7. Click **Save** to store these settings and schedule the job.

Apply or revoke a protection plan

During the integration setup, you can apply or revoke the protection plan, set as the default choice.

To do this:

1. From within Datto RMM, go to **Jobs > New Job** or use the **Quick Job** feature.
2. Set a name for the new job and schedule when it should run.
3. Add job targets (workloads), already known to Datto RMM.
4. Add the Acronis installation component to the job, by selecting either:
 - a. Acronis Cyber Protect - Manage Protection Plan [WIN]
 - b. Acronis Cyber Protect - Manage Protection Plan [MAC]
 - c. Acronis Cyber Protect - Manage Protection Plan [LIN]
5. In the **Variables** section, select whether you want to apply or revoke the protection plan.

Name	Variables
 Acronis Cyber Protect - Manage Protection Plan [WIN]	<p>Action</p> <p>Apply or revoke the default protection plan set for this site. You can apply other protection plans using the Acronis Management portal.</p> <div>Apply protection plan ▼</div> <div>ADD COMPONENT</div>

6. Optionally, set advanced options, alerts, emails and job recipients, the same way as in a regular Datto RMM workflow.
7. Click **Save** to store and schedule the job.

Monitoring and alerts

The integration provides two components used to get Acronis alerts and Protection statuses from protected workloads.

The Acronis Cyber Protect - Monitoring [MAC/LIN] component can be used for both Mac and Linux.

To monitor statuses or get Acronis alerts, do the following:

1. Create a new monitoring policy in Datto RMM.
2. In the **New Policy** window:
 - a. Provide a name
 - b. Set the **Type** option to **Monitoring**.
3. Click **Next**.
4. Add **Targets**.
5. Click **Add Monitor**.
6. In the window that opens, set **Monitor Type** to **Component Monitor**, then click **Next**.
7. In **Monitor Details**, use the drop-down menu under **Run the Component Monitor**, to select either:
 - Acronis Cyber Protect - Monitoring [WIN]
 - Acronis Cyber Protect - Monitoring [MAC/LIN]
8. Optionally, configure whether to get alerts:
 - **Get_alerts_with_at_least_severity**: select **Do not get alerts** to get only Protection statuses or set the minimal severity level of open Acronis alerts you would like to be reported to Datto RMM. Default value: **Do not get alerts**.


Note

The integration will report the alerts as long as they remain open in Acronis. Once you have resolved the root cause of any open alert, go to the Acronis Mangement portal and close it.

9. Configure recent backup and scan alerts:
 - a. **No_succesful_Backup_was_run_in_the_last_hours**: set the time period (in number of hours), within which a successful backup should have been run. If no successful backup was run during this time interval, an alert will be created. Default value: **do not report**.
 - b. **No_Antimalware_scan_was_run_in_the_last_hours**: set the time period (in number of hours), within which an antimalware scan should have been run. If no such scan was run during this time, an alert will be created. Default value: **do not report**.
 - c. **No_Vuln_Assessment_was_run_in_the_last_hours**: set the number of hours within which a vulnerability assessment should have been run. If this assessment was not run during the specified period, an alert will be created. Default value: **do not report**.
 - d. **No_Patch_Managemen_was_run_in_the_last_hours**: set the number of hours within which a patch management scan should have been run. If no such scan was run during this time interval, an alert will be created. Default value: **do not report**.

- e. **No_DataProtectionMap_was_run_in_the_last_hours**: set the number of hours within which a data protection map should have been run. If no such map was run during this time, an alert will be created. Default value: **do not report**.

An alert will be triggered if the Monitor meets the following criteria:


Acronis Cyber Protect - Monitoring [WIN]
 For tests
[CHANGE COMPONENT MONITOR](#)

Variables

Get_alerts_with_at_least_severity
 Select if you want to get Acronis alerts and set a minimal level for them.

No_successful_Backup_was_run_in_the_last_hours
 Test whether a successful backup has been run within the specified period. An alert will be created if no backup was run during that time.

No_Antimalware_scan_was_run_in_the_last_hours
 Test whether a successful antimalware scan has been run within the specified period. An alert will be created if no such scan was run during that time.

No_Vuln_Assessment_was_run_in_the_last_hours
 Test whether a successful vulnerability assessment has been run within the specified period. If not, an alert will be created.

10. Configure the statuses you want to be reported. For each such status, select the UDF where to store the value.
- Acronis_agent_version**: the version number of the Acronis Cyber Protect agent installation.
 - Acronis_Protection_Plan**: the name of the currently applied protection plan(s).
 - Acronis_Protection_Status**: the Protection status of the workload.
 - Acronis_Cyberfit_Score**: the #CyberFit score for the workload.
 - Acronis_last_backup_date**: the date and time when the last successful backup was made.
 - Acronis_next_backup_date**: the date and time when the next backup is scheduled.
 - Acronis_last_antimalware_scan_date**: the date and time when the last antimalware scan was done.
 - Acronis_next_antimalware_scan_date**: the date and time when the next antimalware scan is scheduled.

Note

All dates are reported in the workload local timezone, which may be different from what is displayed in the Acronis Management portal.

11. Configure how frequently you want this monitor to run and set **Alert** and **Auto Resolution** details.

12. Optionally, in the **Response details** section, configure one of the Task components to be automatically run to resolve issues (see "Run manual tasks" (p. 25)).

● **Response** (Optional)

Configure the system response when the Monitor alert is triggered

Run a Component ☒

The following Component will run if the Monitor alert is triggered:

A

Acronis Cyber Protect - Tasks [WIN]

This script is used by the Acronis Cyber Protect Cloud integration.
Script version: 1.0

CHANGE COMPONENT

Variables

TaskType

Policy type user wants to run (required)

Antivirus & AntiMalware Scan

Antivirus & AntiMalware Scan

Backup

Data Protection Map

Patch Management

Vulnerability Assessment

Send an email ☐

Send an email to multiple recipients informing them of the alert if the Monitor is triggered

13. Complete and use the monitor policy the same way as usually in Datto RMM.

Run manual tasks

The integration includes several components for running one-off tasks on workloads that already have an Acronis Cyber Protect agent installed and a protection plan applied.


These components can be used as Quick Jobs, Jobs or a Response in Monitoring policies.

The following components are available:

- Acronis Cyber Protect - Tasks [WIN]
- Acronis Cyber Protect - Tasks [MAC]
- Acronis Cyber Protect - Tasks [LIN]

Each component has a single **TaskType** parameter with the following options (if available for that operating system):

- **Run an Antimalware Scan** (default) will run a manual antimalware scan on the selected workloads.

Name	Variables
 Acronis Cyber Protect - Scans [WIN] For tests	TaskType Select a task to perform. <div>Run an Antimalware Scan</div> <div>ADD COMPONENT</div>

- **Run a Backup** will run a backup on the selected workload without waiting for the next scheduled backup.
- **Run a Data Protection Map** will run a data protection map scan on the selected workloads.
- **Run a Patch Management Scan** will run a patch management scan on the selected workloads.
- **Run a Vulnerability Assessment** will run a vulnerability assessment on the selected workloads.

Alternative components usage

Important

The scenario described further is a workaround, not the preferred method of using this integration.

There can be situations when you may want to use the components, but cannot or would simply prefer to not set up the configuration in the Acronis Management portal. In such cases, you can manually create and maintain case-sensitive variables instead, with values (the registration token) that expire. This is required for every *site* you want to use the *components* for.

For each individual Datto RMM site you want to set up for manual components usage, do the following:

1. In **Datto RMM**, navigate to the particular site you want to set up.
2. Go to **Settings**, then scroll down to **Variables**.
3. Create a new variable, called **acronisToken**.
4. In the **Acronis Management portal**, locate the customer tenant you want to map to the site.
5. Go to **Manage Services > Devices** and click on **Add new device**.
6. Scroll down to **Registration Token** and click on the **Generate** button.
7. Set each of the following:
 - a. **Token lifetime** - the default value is 3 days, maximum - 12 months. Shorter values are generally considered more secure.
 - b. A **user** for the current customer tenant. All devices will be registered with this user.
 - c. Optionally, a **default protection plan**. This is necessary for the **Apply and Revoke Protection Plan** functionality in the components.
8. Click on **Generate Token** and copy the token value.
9. Go back to **Datto RMM** and populate the **Variable value** field with the token value from the **acronisToken** variable created earlier.
10. Create a second variable, called **registrationURL**.
11. Go to the **Acronis Management portal** and from the address bar of your browser, copy the URL domain, including the ".com" part and without the "/". This URL varies depending on the data center your Acronis account is created on.
12. Go back to **Datto RMM** and paste the URL into the **Variable value** field for the **registrationURL** variable you have created.

Repeat these steps for every site you want to use the components for.

Warning!

Be careful not to miss the date, on which you have to refresh the registration tokens!

Note

The variables are case-sensitive. Make sure to enter and copy their values correctly. Don't use blank spaces anywhere, including their addition after variable names or values.

Any of the above described issues may cause failure in the way the components work. If you have any concerns, always double-check your variables.