Acronis

Acronis Cyber Cloud

Integration with Datto RMM

INTEGRATION GUIDE

Revision: 10/8/2021

Table of contents

1 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
- Get tickets for any alerts, related to such workloads

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

2 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

3 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

4 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.

5 Mapping

The integration uses the mapping listed below:

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

6 How the integration works

The Acronis integration for Datto RMM consists of two parts:

- Configuration done from the Acronis Management console 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.

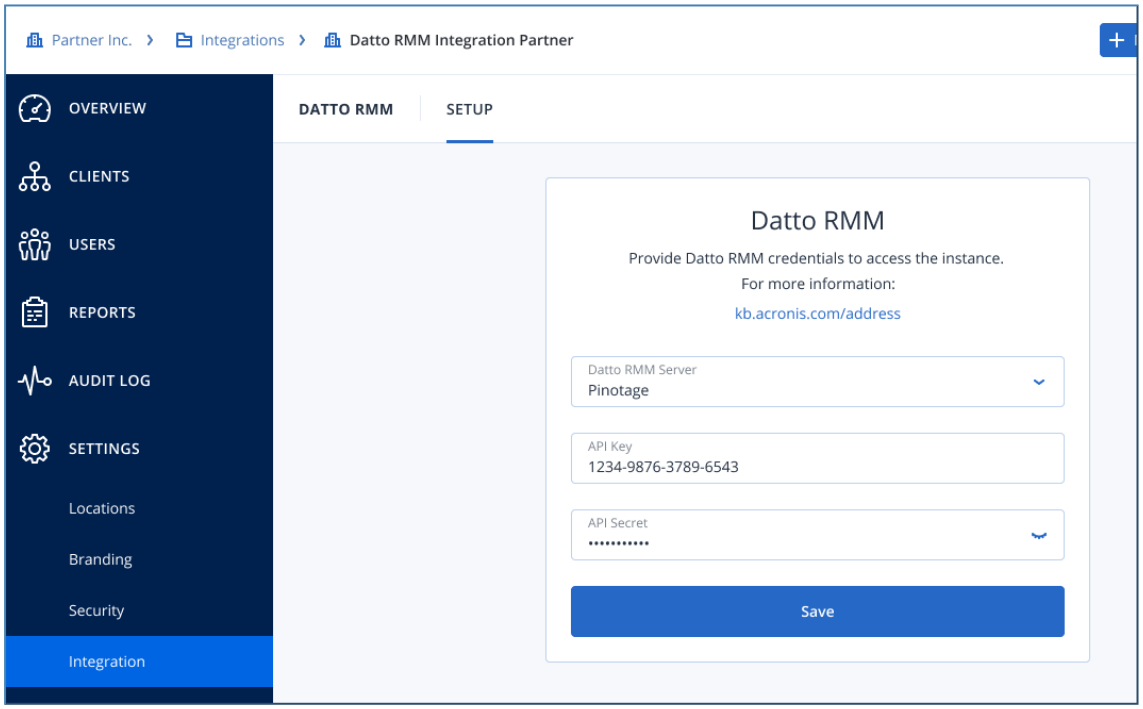
6.1 Limitations of this integration

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.

7 Set up 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 existing Acronis customer tenants.

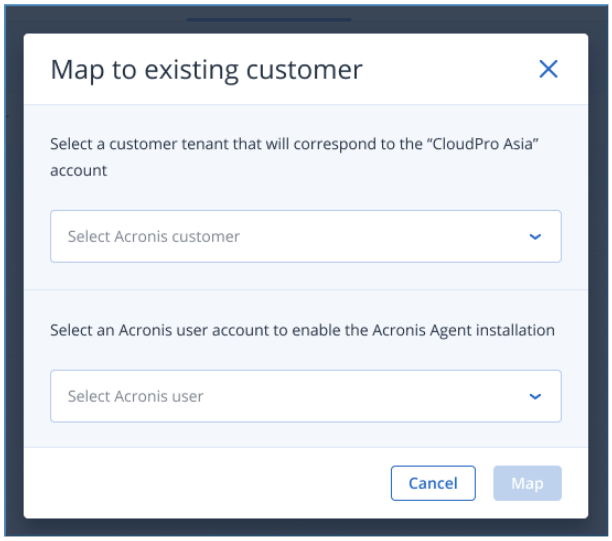
1. Make sure that the API on your Datto RMM instance is enabled.
2. Next, create an API key and secret for the user, necessary to manage the integration. Find detailed steps on how to do this in the Datto documentation > How to Activate the API. We advise you to create a separate user in Datto RMM, only for the Acronis integration purposes.
3. Go to the **Acronis Management console** > **Integrations** and click on the **Datto RMM** tile.
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
   b. Provide the API key and secret you created in step 2.



   c. Click **Save**.
5. 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.

a. Select a site and click **Map to existing tenant**.
b. In the window that opens next, select an existing:
   i. customer tenant
   ii. user for this customer tenant. All new workloads will be registered to this user in Acronis.

> **Note**
> This user should have administrator permissions.



c. 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.

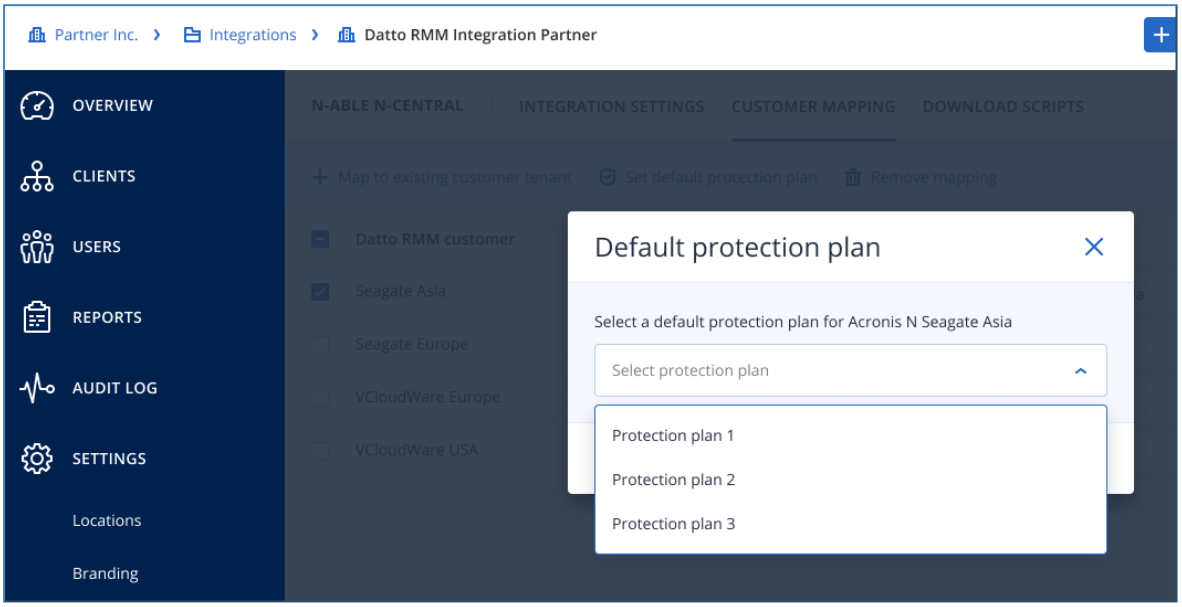
Continue the setup by optionally assigning default protection plans to all of your mapped sites or proceed with downloading the components.

7.1 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**.

7.2 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 Acronis Cyber 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.

7.3 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 console** > **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.

7.4 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 console** > **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.

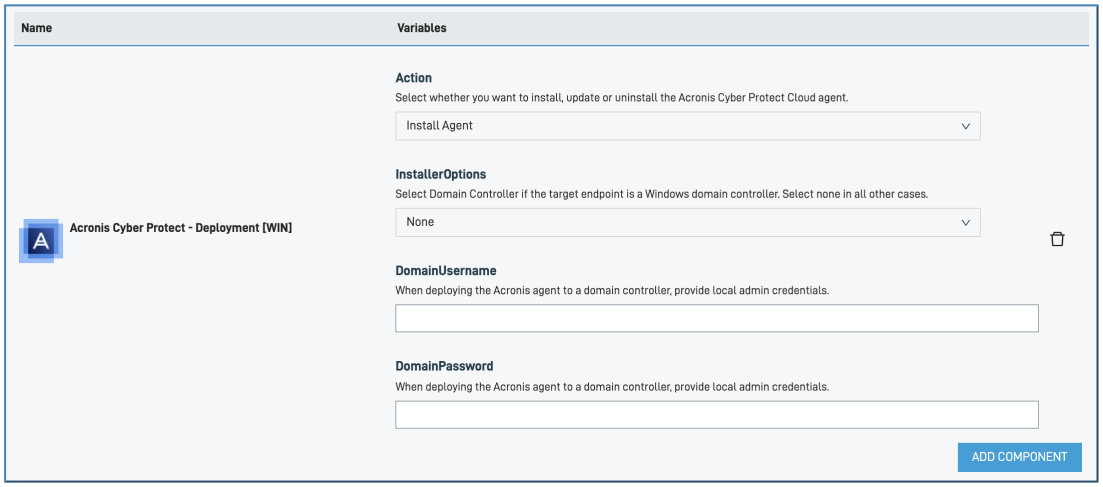
To change the mapping of an existing site, already mapped to an existing Acronis customer tenant:

1. Go to the **Acronis Management console** > **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.

8 Deploy Acronis on workloads

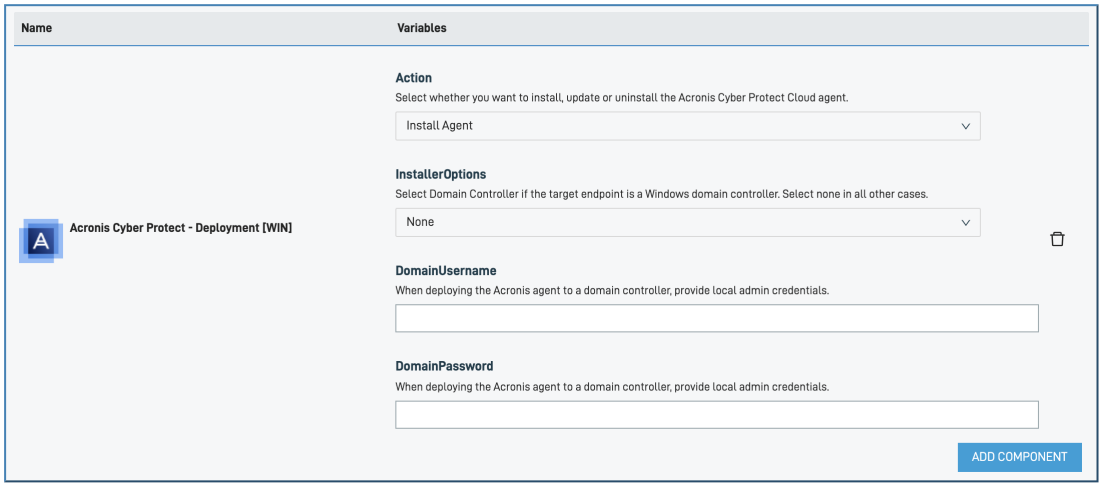
By using the deployment components (downloaded as part of the setup), you can schedule deployment of Acronis on any Windows, Mac or Linux workload, managed by Datto RMM:

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)



      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.



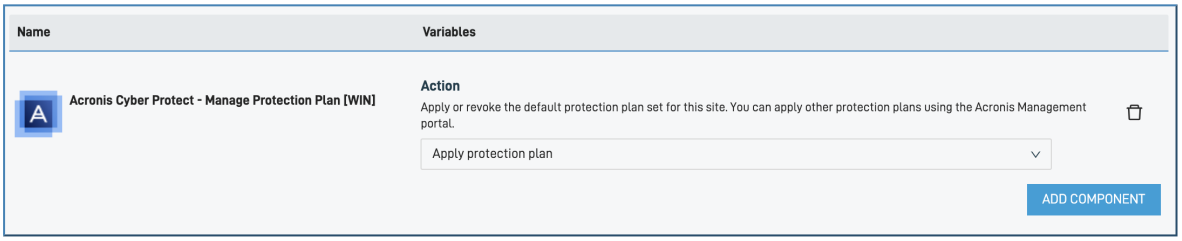
6. Optionally, set advanced options, alerts, emails and job recipients, the same way as in the regular Datto RMM workflow.
7. Click **Save** to store these settings and schedule the job.

9 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.



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.

10 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.

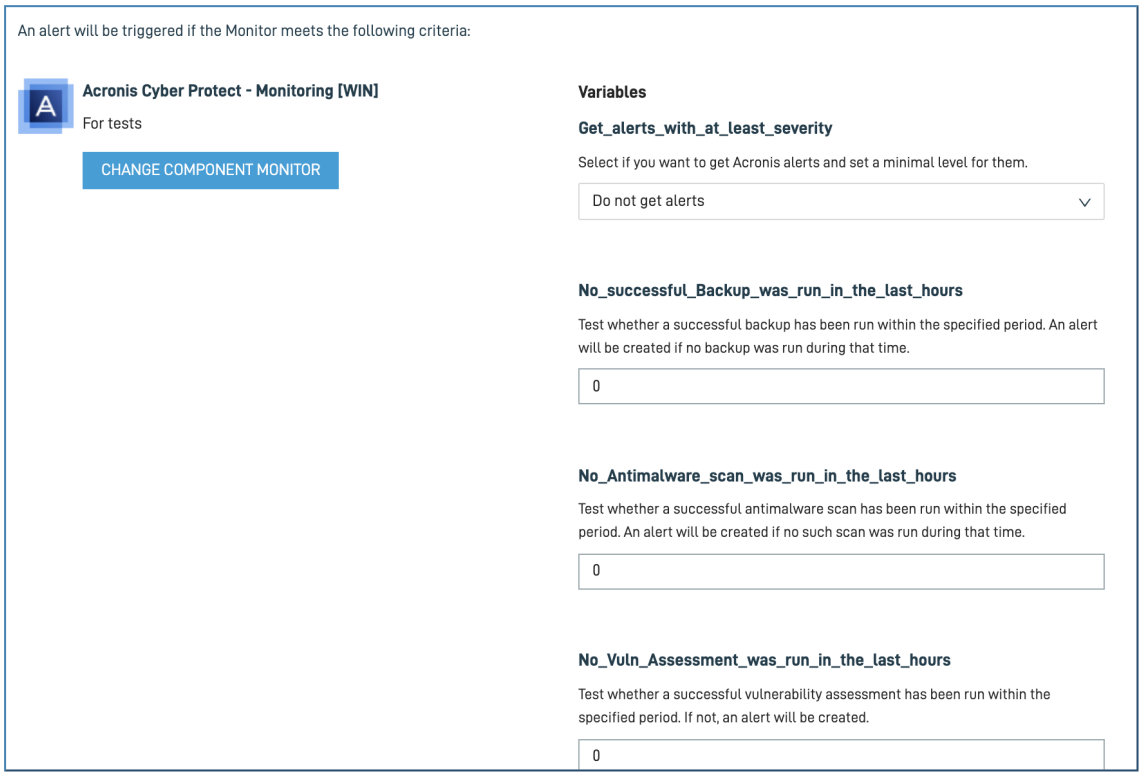
To monitor statuses or get Acronis alerts, do the following:

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 console 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**.

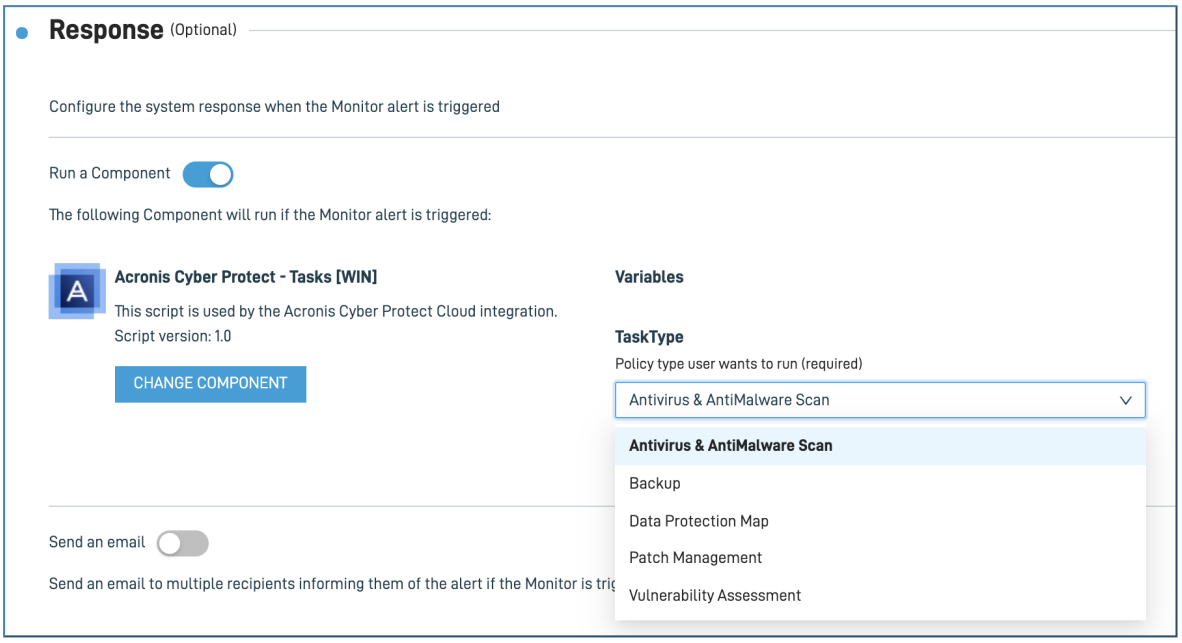


10. Configure the statuses you want to be reported. For each such status, select the UDF where to store the value.
    a. **Acronis_agent_version**: the version number of the Acronis Cyber Protect agent installation.
    b. **Acronis_Protection_Plan**: the name of the currently applied protection plan(s).
    c. **Acronis_Protection_Status**: the Protection status of the workload.
    d. **Acronis_Cyberfit_Score**: the #CyberFit score for the workload.
    e. **Acronis_last_backup_date**: the date and time when the last successful backup was made.
    f. **Acronis_next_backup_date**: the date and time when the next backup is scheduled.
    g. **Acronis_last_antimalware_scan_date**: the date and time when the last antimalware scan was done.
    h. **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. 19)).



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

11 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.

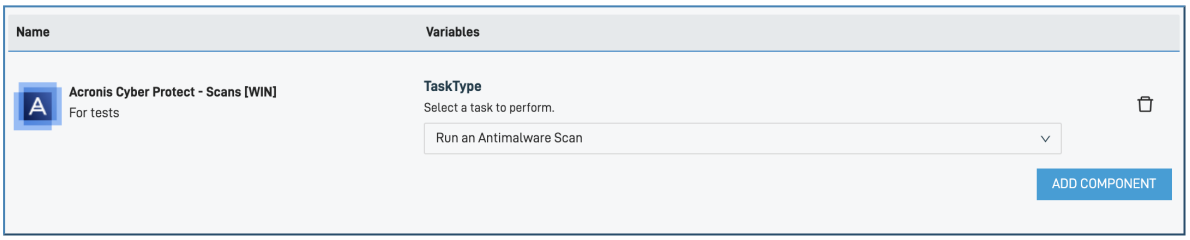
These components can be used as Quick Jobs, Jobs or a Response in Monitoring policies.

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.



- **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.