Acronis

acronis.com

NinjaOne Integration

C25.03

Configuration Guide

REVISION: FRIDAY, JUNE 20, 2025

Table of contents

Introduction

This guide describes how to activate and configure the integration of Acronis Cyber Cloud with NinjaOne.

Integration functionality

Customers

- Provision NinjaOne organizations as new customer tenants in Acronis.
- Deprovision deleted NinjaOne organizations from Acronis.

Tickets

- Create NinjaOne tickets when an Acronis alert is registered on a protected workload.
- Reset the status of NinjaOne tickets when the source Acronis alert is cleared.
- Clear the source Acronis alert when a NinjaOne ticket changes status.
- Reopen NinjaOne tickets if the source Acronis alert reoccurs within a specified period of time.

Monitoring status

- Monitor and update Acronis agent status of protected workloads in NinjaOne.

Script-based functionality

Integration scripts enable a variety of Acronis cybersecurity tasks from within NinjaOne. Using the integration scripts, you can:

- Install the Acronis agent on Windows, Linux, and Mac workloads.
- Uninstall the Acronis agent from Windows, Linux, and Mac workloads.
- Apply and revoke Acronis protection plans.
- Perform Acronis scan tasks on protected workloads.

Prerequisites

NinjaOne prerequisites

- An administrator account in NinjaOne.
- A NinjaOne Client App ID.

Note
For more information, see Generating a NinjaOne Client App ID.

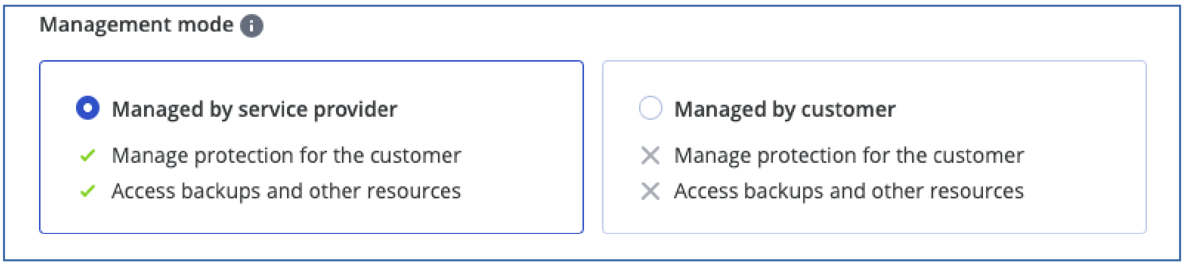
Acronis prerequisites

- You must have a fully configured Acronis Cyber Cloud partner tenant account.
- The user account that you use to activate and configure the integration must be a Company Administrator.
- You must not have disabled support access.

Note
For more information, see the Management Portal Partner Administrator guide.

- [Optional] One or more customer tenants.

Note
Only customer tenants that are provisioned as **Managed by service provider** will appear as active for mapping.



Management mode

● Managed by service provider
✓ Manage protection for the customer
✓ Access backups and other resources

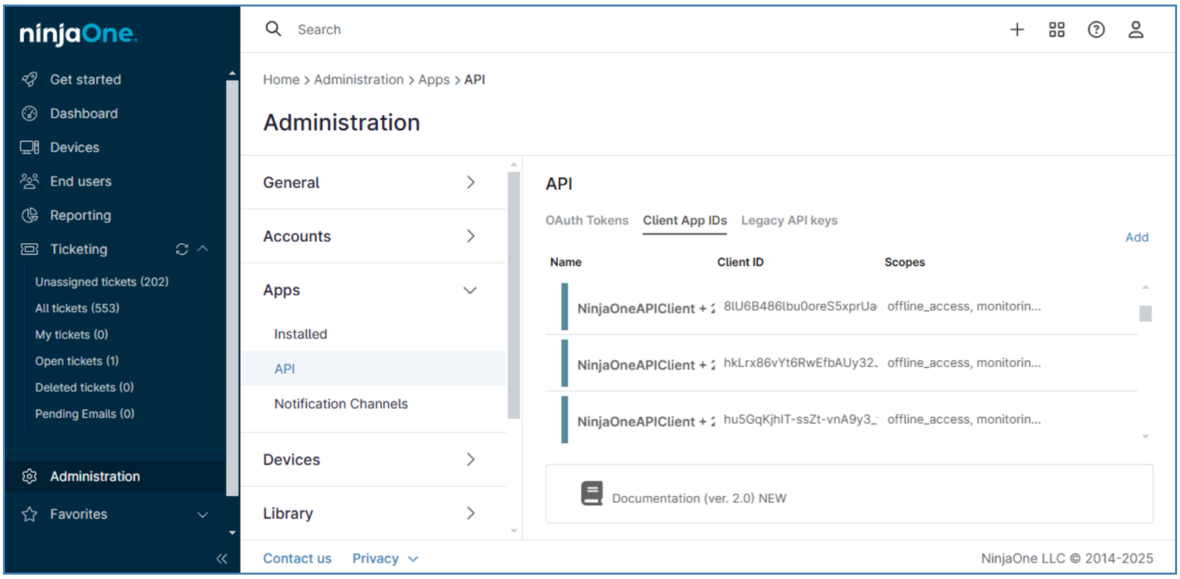
○ Managed by customer
✗ Manage protection for the customer
✗ Access backups and other resources

- [Optional] One or more protection plans.

Generating a NinjaOne Client App ID

To generate a NinjaOne Client App ID

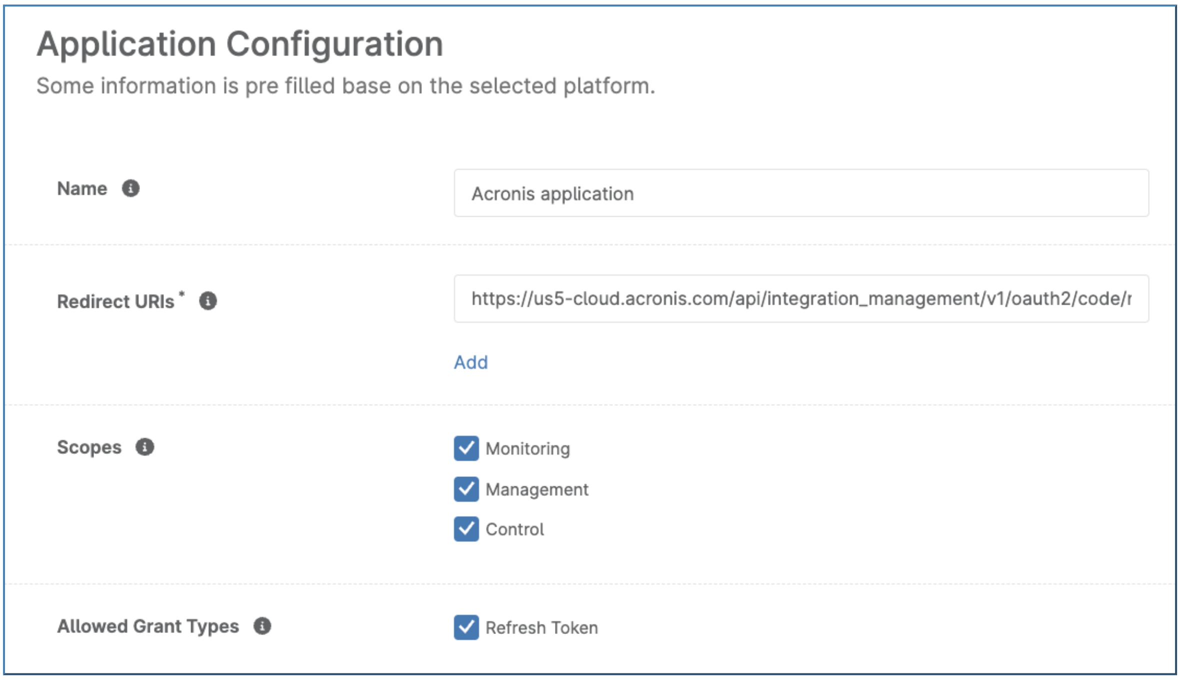
1. Log in to NinjaOne.
2. Select **Administration** > **Apps** > **API**.
3. Select the **Client App IDs** tab.



Name	Client ID	Scopes
NinjaOneAPIClient + 2	8lU6B486lbu0oreS5xprUa	offline_access, monitorin...
NinjaOneAPIClient + 2	hkLrx86vYt6RwEfbAUy32.	offline_access, monitorin...
NinjaOneAPIClient + 2	hu5GqKjhIT-ssZt-vnA9y3_	offline_access, monitorin...

4. Click **Add**.
5. Select **Single Page (Angular, React, Vue, etc.)** from the **Application platform dropdown list.**
6. Enter a **Name** for the client application. For example, **Acronis application.**
7. In **Redirect URIs**, provide the redirect address `https://<acronis_url>/api/integration_management/v1/oauth2/code/ninja`, where `<acronis_url>` is your Acronis Cyber Protect Cloud console URL.

   An example of a valid redirect url for the Acronis US5 data center is: `https://us5-cloud.acronis.com/api/integration_management/v1/oauth2/code/ninja`
8. In **Scopes**, enable **Monitoring**, **Management**, and **Control.**
9. Select the **Authorization Code** checkbox in the **Allowed Grant Types** field.
10. Click **Save**.
11. Verify your MFA and click **Continue**.
12. Enable **Refresh token** and click **Save**.



Application Configuration

Some information is pre filled base on the selected platform.

Name	Acronis application
Redirect URIs *	https://us5-cloud.acronis.com/api/integration_management/v1/oauth2/code/r
Scopes	☑ Monitoring ☑ Management ☑ Control
Allowed Grant Types	☑ Refresh Token

Important

If this option is not available to configure in the **Application configuration** form, save it, find it in the list and click **Edit**. Then enable **Refresh token** and save again.

13. Copy **Client ID** for the client app and note it down somewhere safe.

Note

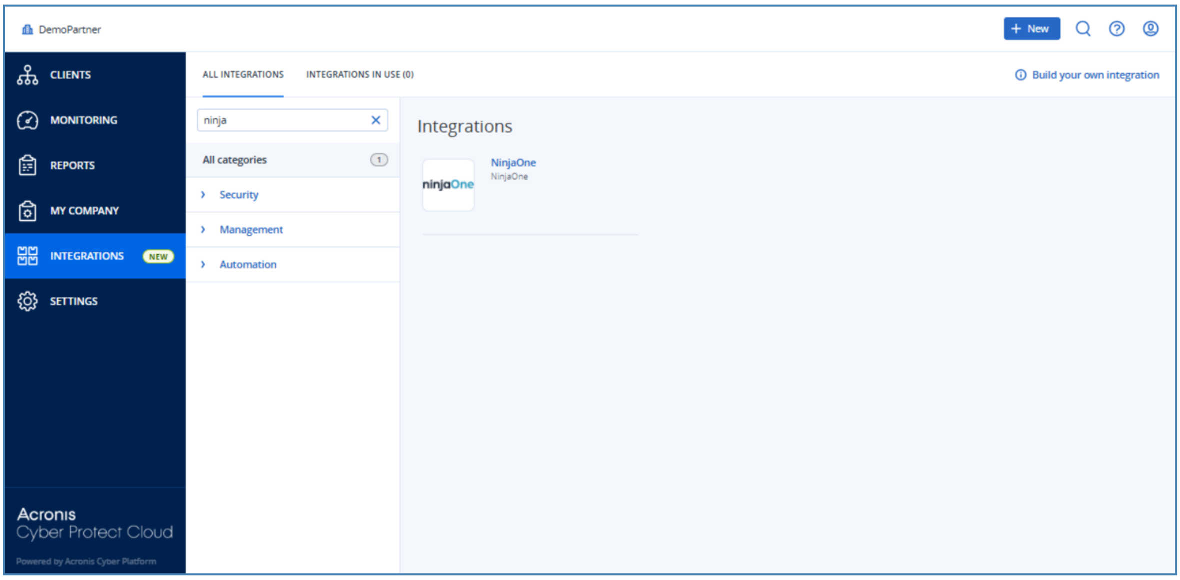
You need this value to activate the integration.

Activating the integration

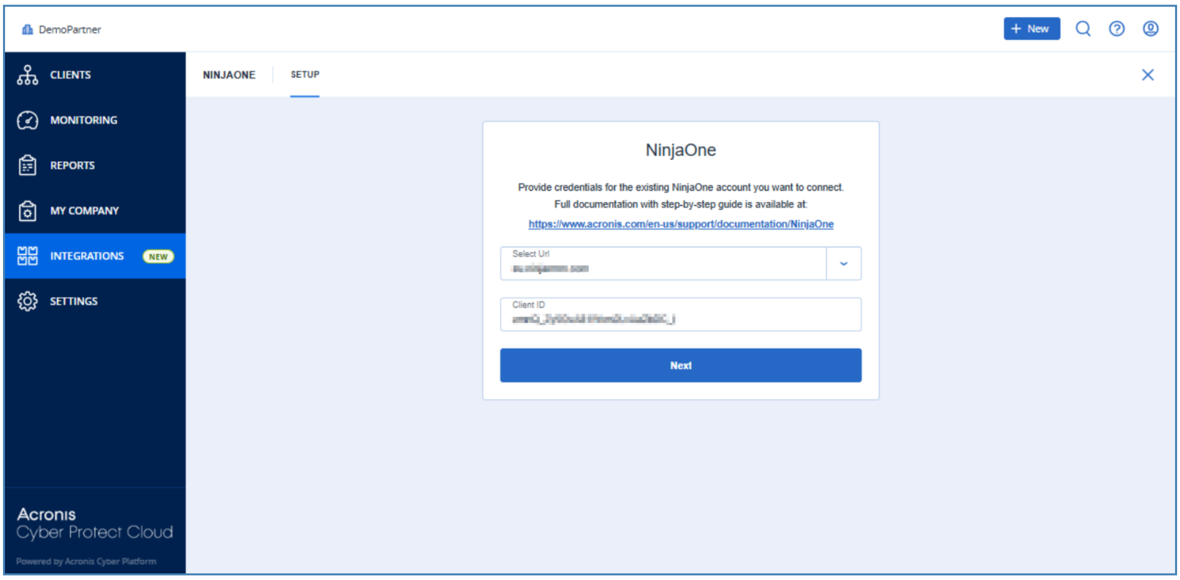
To activate the integration

1. Log in to Acronis Management Portal.
2. Select **INTEGRATIONS** from the main menu.
3. Search for the NinjaOne catalog card.

> **Note**
> For more information, see the Management Portal partner administrator guide.



4. Hover over the NinjaOne catalog card and click **Configure**.



NinjaOne

Provide credentials for the existing NinjaOne account you want to connect.
Full documentation with step-by-step guide is available at:
https://www.acronis.com/en-us/support/documentation/NinjaOne

Select Url: [redacted]

Client ID: [redacted]

Next

5. Select the URL of your NinjaOne account data center.

Note

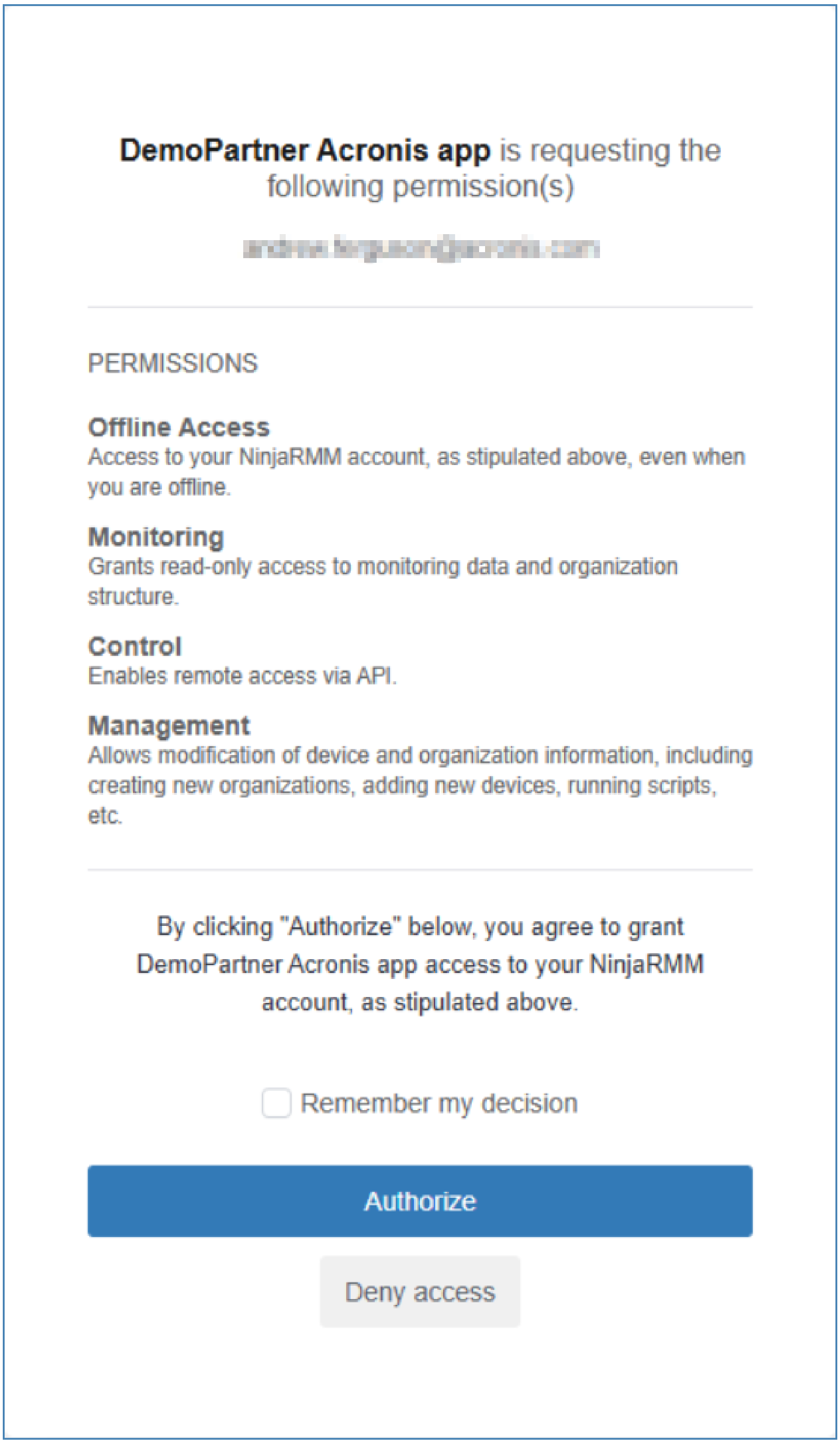
If the data center you want to connect to does not appear in the dropdown list, and its address ends in `.ninjarmm.com`, you can enter it manually.

6. Enter the **Client ID** for the client application you created.

Note

For more information, see Generating a NinjaOne Client App ID.

7. Click **Next**.



DemoPartner Acronis app is requesting the following permission(s)

[redacted]

PERMISSIONS

Offline Access
Access to your NinjaRMM account, as stipulated above, even when you are offline.

Monitoring
Grants read-only access to monitoring data and organization structure.

Control
Enables remote access via API.

Management
Allows modification of device and organization information, including creating new organizations, adding new devices, running scripts, etc.

By clicking "Authorize" below, you agree to grant DemoPartner Acronis app access to your NinjaRMM account, as stipulated above.

☐ Remember my decision

8. Click **Authorize**.

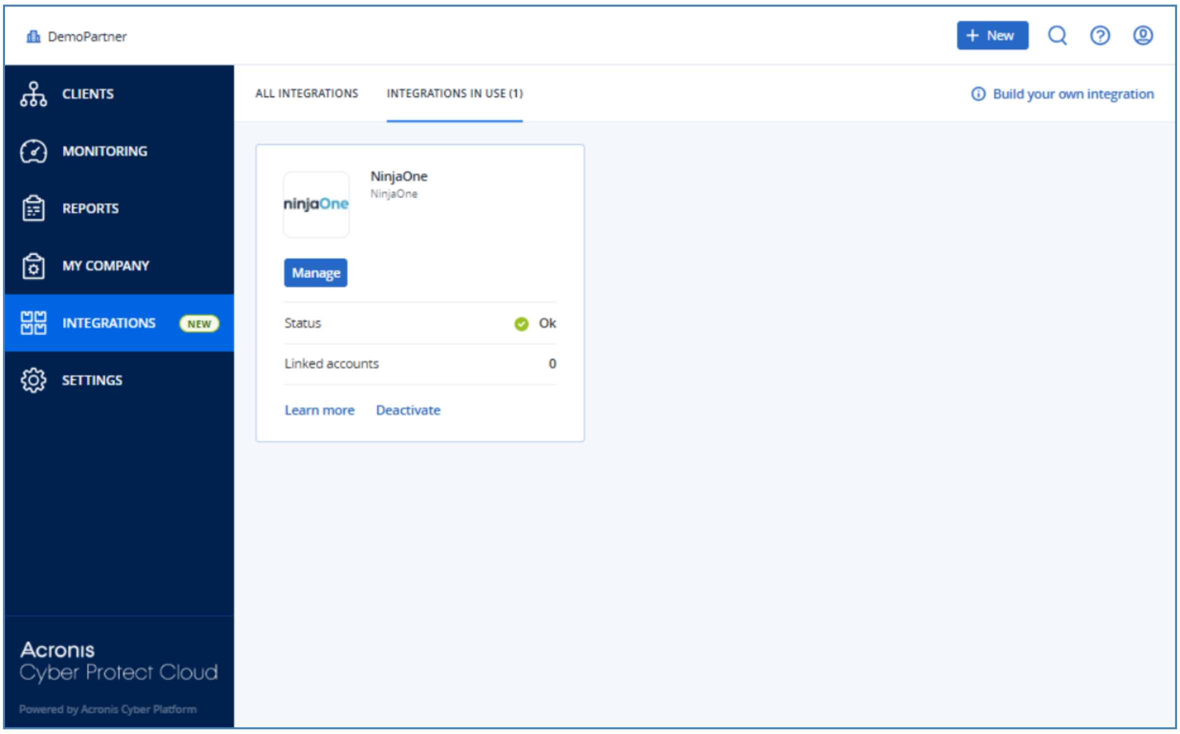
Opening the integration

To open the integration

1. Log in to Acronis Management Portal as administrator.
2. Select **INTEGRATIONS** on the main menu.
3. Select the **INTEGRATION IN USE** tab.
4. Locate the NinjaOne integration catalog card.

Note

For more information, see the Management Portal partner administrator guide.



Status Ok

Linked accounts 0

5. Click **Manage**.

Settings

The **INTEGRATION SETTINGS** tab contains sections for:

- Credentials

  Used to manage API access to your NinjaOne account.
- Features

  Used to manage which features of the integration are enabled, and the settings for each feature. This contains subsections, with settings for:
  - Customer mapping
  - Ticket mapping

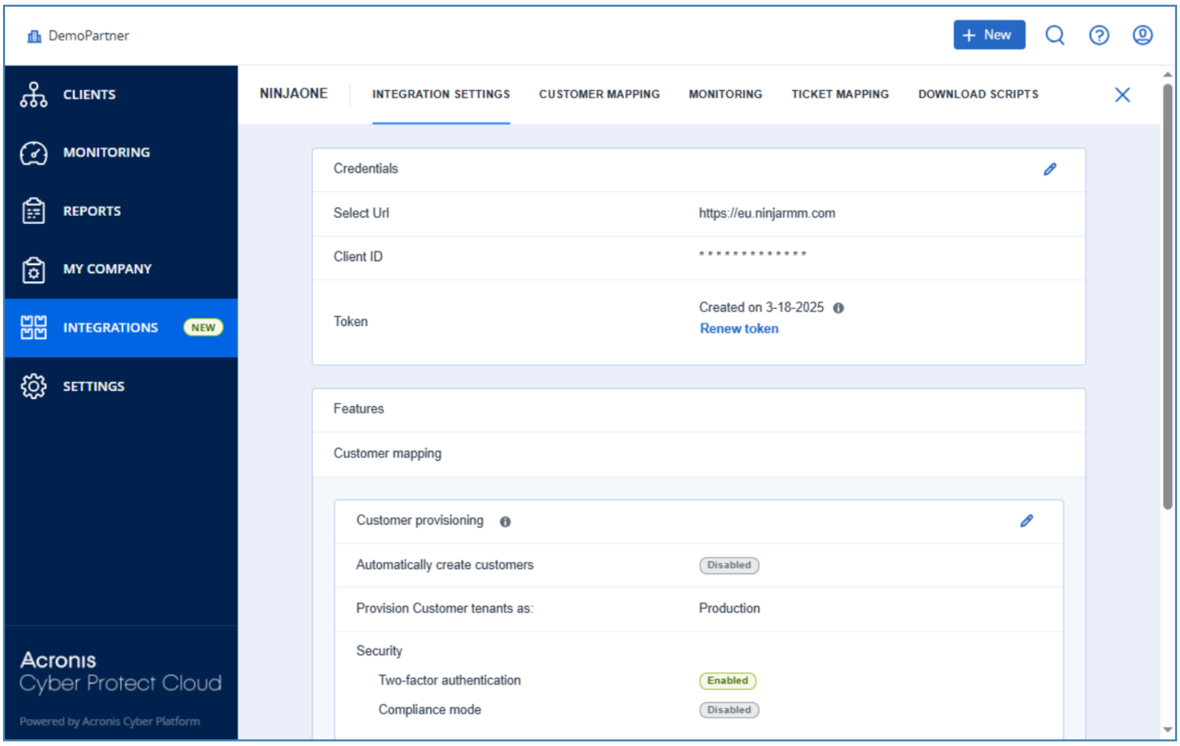
To manage integration settings

1. [If required] Open the integration.
2. Select the **INTEGRATION SETTINGS** tab.

Changing NinjaOne credentials

To change NinjaOne credentials

1. Open the integration.
2. Select the **INTEGRATION SETTINGS** tab.



Credentials

Select Url https://eu.ninjarmm.com

Client ID *************

Token Created on 3-18-2025 Renew token

Features

Customer mapping

Customer provisioning

Automatically create customers Disabled

Provision Customer tenants as: Production

Security

Two-factor authentication Enabled

Compliance mode Disabled

3. [Optional] Click **Renew token** to renew the NinjaOne API token.

Note

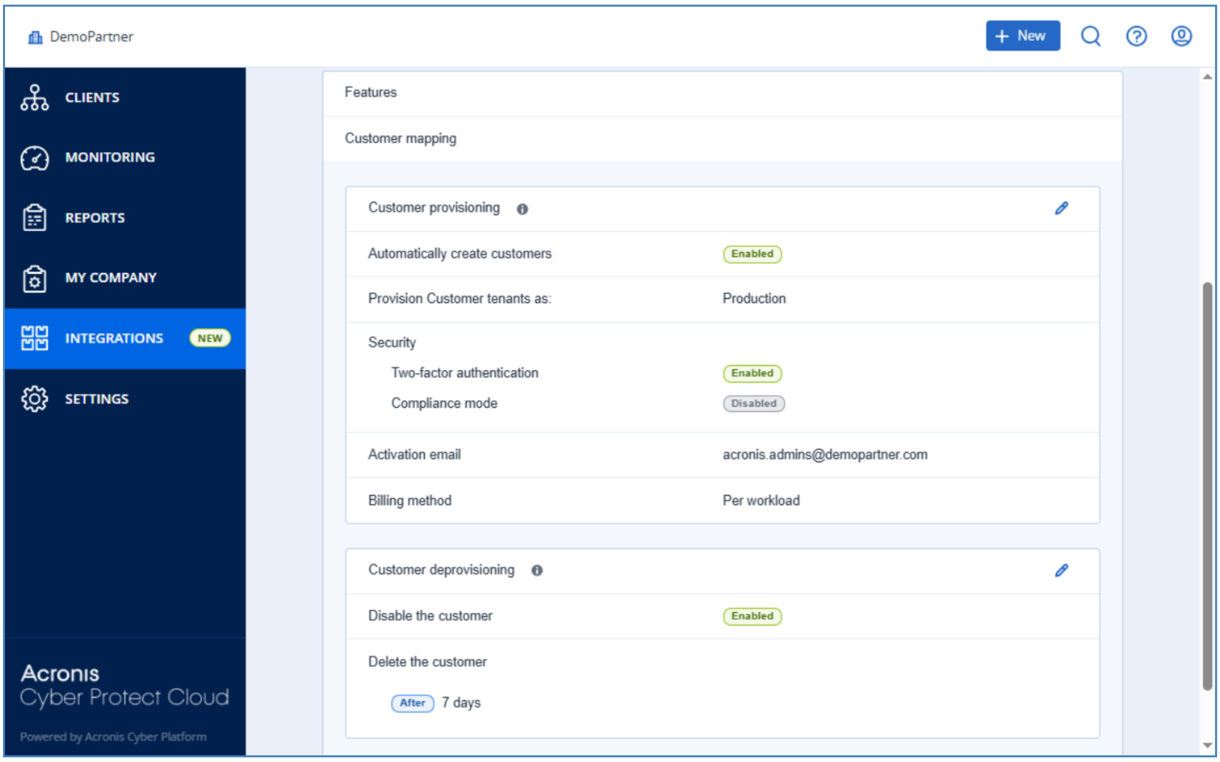
Check the relevant token expiration date in NinjaOne, at **Administration** > **Apps** > **API** > **OAuth Tokens** tab

4. In the **Credentials** section, click ✎.
5. From the dropdown list, select the NinjaOne URL, or enter it manually.
6. Enter the **Client ID**.
7. Click ✓.

Customer mapping settings

In the **Customer mapping** section, you can define settings for:

- Customer provisioning
- Customer deprovisioning



Customer provisioning

Automatically create customers	Enabled
Provision Customer tenants as:	Production
Security	
Two-factor authentication	Enabled
Compliance mode	Disabled
Activation email	acronis.admins@demopartner.com
Billing method	Per workload

Customer deprovisioning

Disable the customer	Enabled
Delete the customer	
After 7 days	

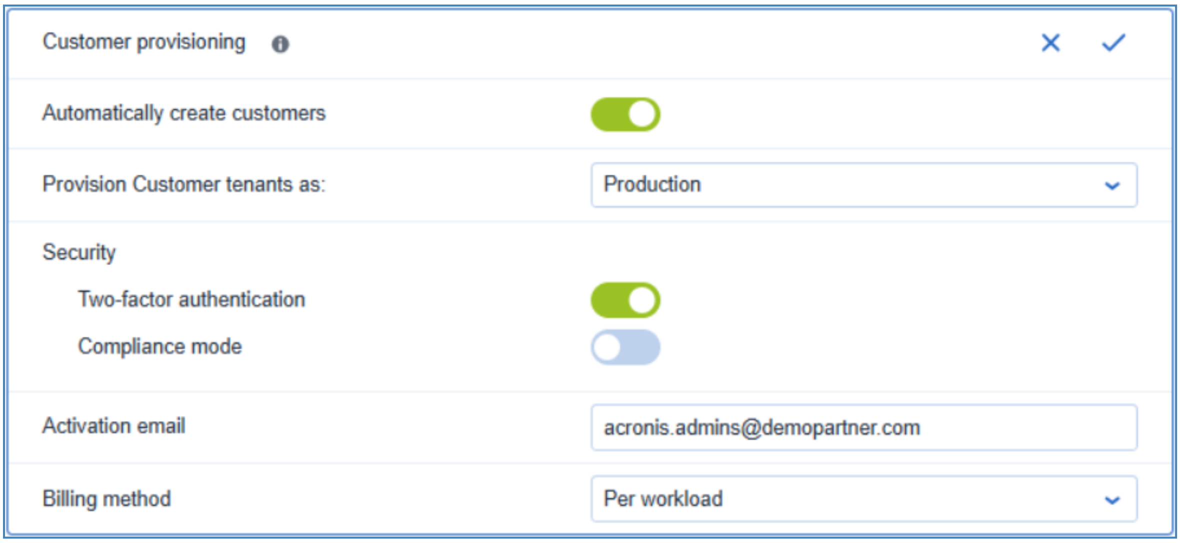
Customer provisioning

In the **Customer mapping** > **Customer provisioning** section, you configure the parameters required to create new Acronis customer tenants and user accounts.

To configure customer provisioning

1. Open the integration.
2. Select the **INTEGRATION SETTINGS** tab.

3. Scroll down to the **Customer mapping** > **Customer provisioning** section, and click ✎.



Customer provisioning ⓘ ✕ ✓

Automatically create customers: on

Provision Customer tenants as: Production

Security

Two-factor authentication: on

Compliance mode: off

Activation email: acronis.admins@demopartner.com

Billing method: Per workload

4. Turn the **Automatically create customers** toggle switch on or off.
   If you enable this feature, newly created NinjaOne organizations are automatically provisioned and mapped in Acronis.

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

> **Important**
> Make sure that you have mapped NinjaOne organizations which are already registered as Acronis customer tenants. Otherwise, these customers will be duplicated after enabling automatic customer provisioning.

5. Select the **Provision customer tenants as** setting from the dropdown list:
   - **Production** (default)
   - **Trial**

   > **Note**
   > Customers in trial mode have full access to all integration functionality for the duration of the trial.
   > They are automatically switched to production mode after 30 days.

6. Turn the **Two-factor authentication** toggle switch on or off.
   If turned on, new customer tenants are provisioned with two-factor authentication.

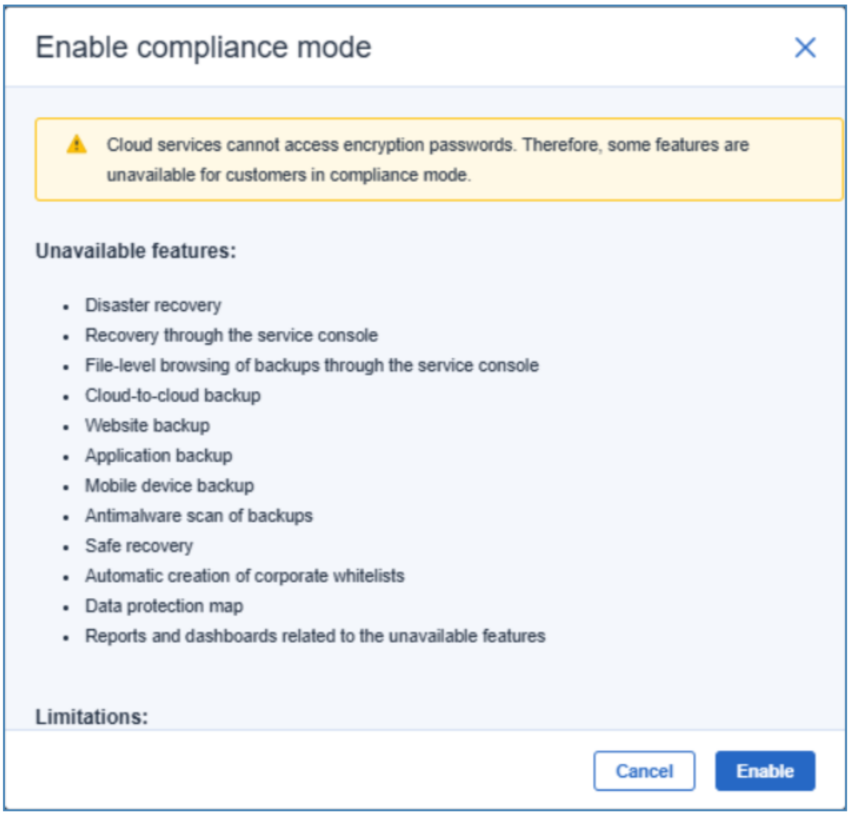
> **Note**
> For more information, see the Management Portal Partner Administrator guide.

7. Turn the **Compliance mode** toggle switch on or off.
   Compliance mode is designed for higher security demands. It requires mandatory encryption for

all backups and allows only locally set encryption passwords.

Note
For more information, see the Management Portal Partner Administrator guide.

If you enable compliance mode, carefully review the information presented, then click **Enable**.



Enable compliance mode

Cloud services cannot access encryption passwords. Therefore, some features are unavailable for customers in compliance mode.

Unavailable features:

- Disaster recovery
- Recovery through the service console
- File-level browsing of backups through the service console
- Cloud-to-cloud backup
- Website backup
- Application backup
- Mobile device backup
- Antimalware scan of backups
- Safe recovery
- Automatic creation of corporate whitelists
- Data protection map
- Reports and dashboards related to the unavailable features

Limitations:

8. Enter an **Administration email**.
   This is the administrator user email for provisioned Acronis customers.

Note
Administrator user activation links are sent to this email address. The user must be activated.

9. Select the **Billing method** from the dropdown list.
   - **Per Workload**
     Based on the number of protected workloads. Cloud storage is charged separately.
   - **Per gigabyte**
     Based on the cloud and local storage used.
10. Click ✓.

Customer deprovisioning

When a mapped organization is removed from NinjaOne, the integration can deprovision the mapped Acronis customer.

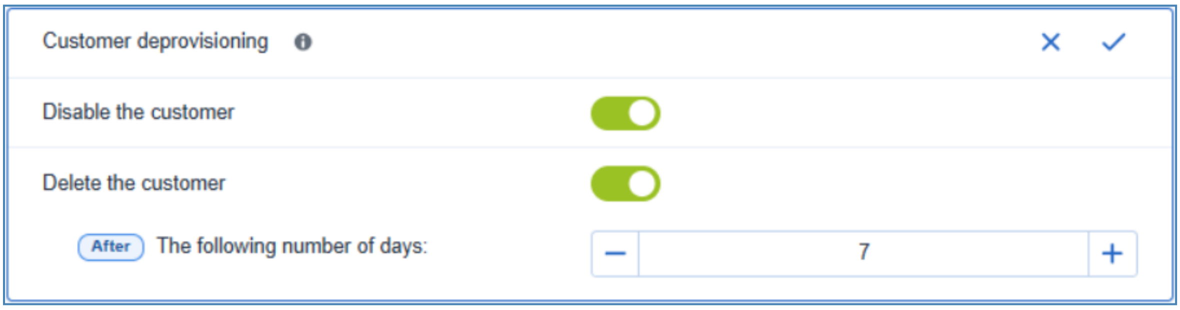
Note

Deprovisioning is a two-step process:

1. The integration disables the Acronis customer.
2. [After a specified number of days] The integration deletes the Acronis customer and all related data.

To configure customer deprovisioning

1. Open the integration.
2. Select the **INTEGRATION SETTINGS** tab.
3. In the **Customer deprovisioning** section, click ✎.



Customer deprovisioning ✕ ✓

Disable the customer ●

Delete the customer ●

After The following number of days: − 7 +

4. Turn the **Disable the customer** toggle switch on of off.
   If you enable this functionality, when a NinjaOne organization which you mapped to an Acronis customer is removed, the mapped Acronis customer is disabled.
5. [If you turn on the **Disable the customer** toggle switch] Turn the **Delete the customer** toggle switch on or off.
   If you enable this functionality, Acronis customers which have been disabled by the previous setting and all related data are subsequently deleted. You must use the number picker to specify how many days after disablement the deletion occurs.

   Note

   If you select 0 days, the integration deletes the Acronis customer at the first sync after it is disabled.

   Important

   You can prevent customer deletion by re-enabling the Acronis customer in Management Portal before the specified number of days have passed.

6. Click ✓.

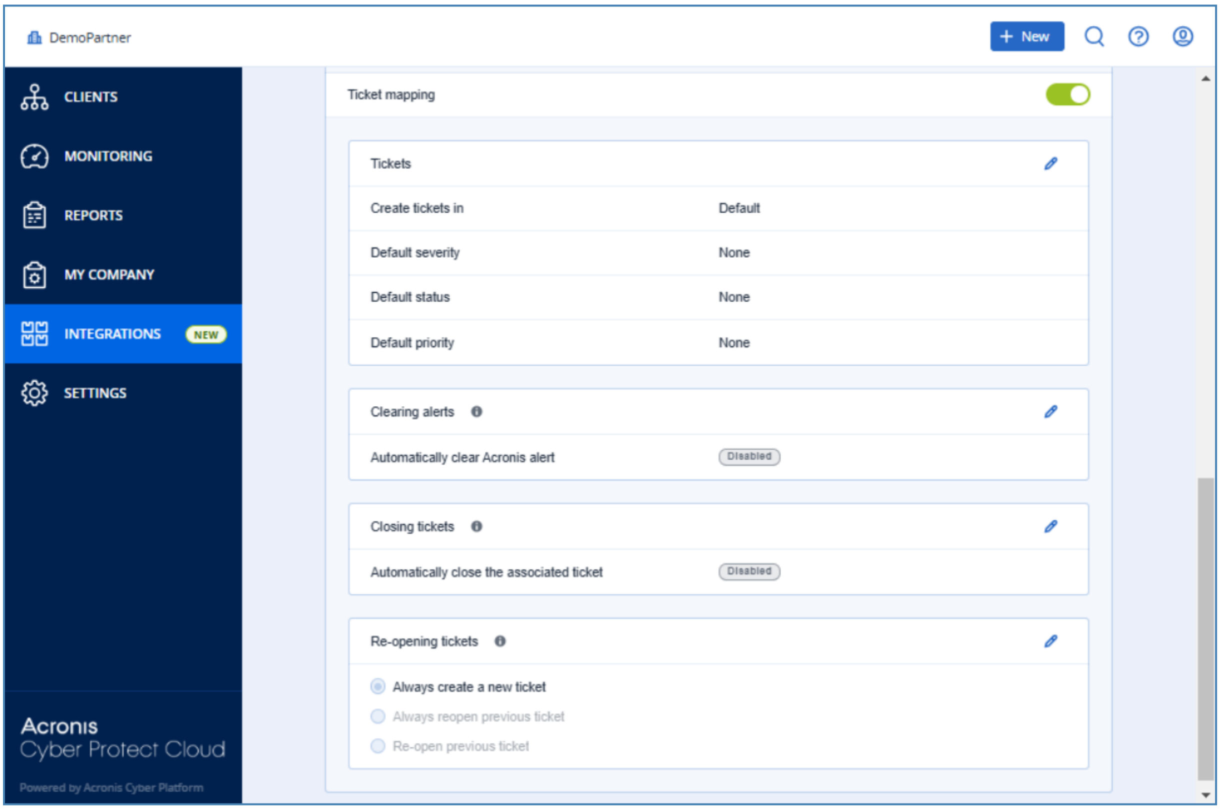
Ticket mapping settings

When you activate the integration, ticket mapping is disabled by default.
Enable the feature by turning on the **Ticket mapping** toggle switch.

Note
You must have at least one ticket type in NinjaOne. Otherwise, an error will occur.

In the **Ticket mapping** section, you can define settings for:

- Ticket mapping defaults
- Clearing Acronis alerts
- Closing NinjaOne tickets
- Reopening NinjaOne tickets



Ticket mapping

Tickets

Create tickets in Default

Default severity None

Default status None

Default priority None

Clearing alerts

Automatically clear Acronis alert Disabled

Closing tickets

Automatically close the associated ticket Disabled

Re-opening tickets

● Always create a new ticket
○ Always reopen previous ticket
○ Re-open previous ticket

Ticket mapping defaults

Ticket mapping defaults pre-populate the fields when you map tickets in the **TICKET MAPPING** tab.

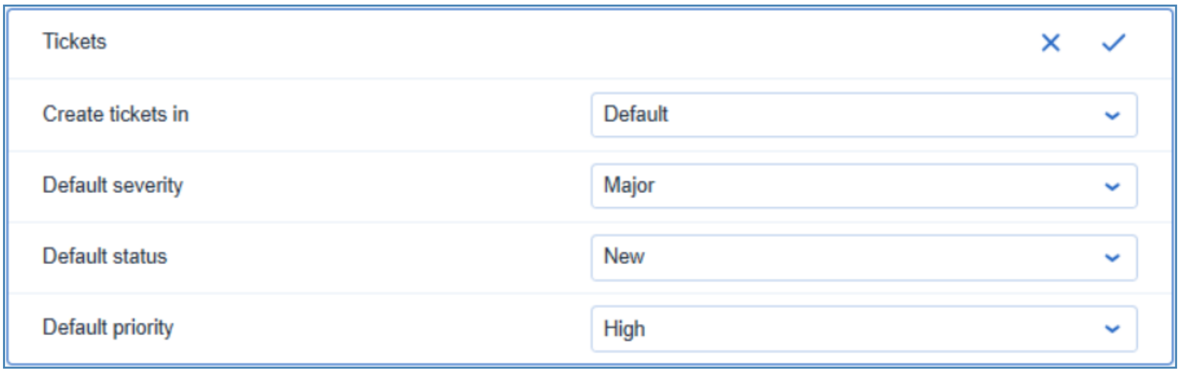
Note
The available values for each default depend on the configuration of NinjaOne.

To set ticket mapping defaults

1. Open the integration.
2. Select the **INTEGRATION SETTINGS** tab.
3. Scroll down to **Ticket mapping** > **Tickets**.

Note
This option is only available if **Ticket mapping** is enabled.
If **Ticket mapping** is disabled, enable it by turning on the toggle switch.
You must have at least one ticket type in NinjaOne. Otherwise, an error will occur when you enable ticket mapping.

4. Click ✎ to edit the settings.



Tickets ✕ ✓

Create tickets in	Default
Default severity	Major
Default status	New
Default priority	High

5. [Optional] Change the **Create ticket in** setting.
6. [Optional] Select the **Default severity**.
7. [Optional] Select the **Default status**.
8. [Optional] Select the **Default priority**.
9. Click ✓ .

Clearing Acronis alerts

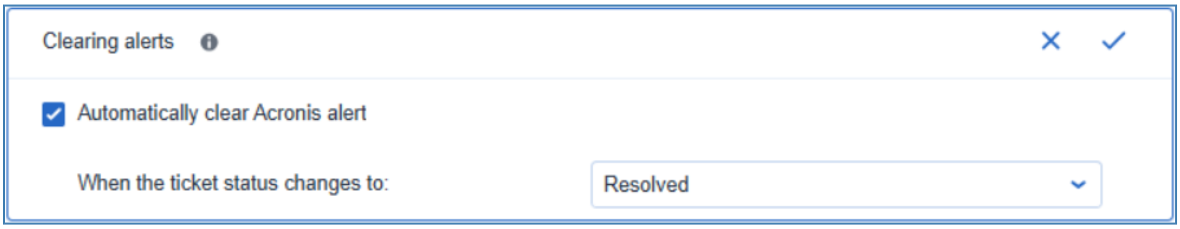
The integration can clear source Acronis alerts when their corresponding NinjaOne tickets change to a specific status.

To clear Acronis alerts

1. Open the integration.
2. Select the **INTEGRATION SETTINGS** tab.
3. Scroll down to **Ticket mapping** > **Clearing alerts**.

Note
This option is only available if **Ticket mapping** is enabled.
If **Ticket mapping** is disabled, enable it by turning on the toggle switch.
You must have at least one ticket type in NinjaOne. Otherwise, an error will occur when you enable ticket mapping.

4. Click ✎ to edit the settings.


Clearing alerts

☑ Automatically clear Acronis alert

When the ticket status changes to: Resolved

5. To enable the feature, select the **Automatically clear Acronis alert** checkbox.
6. [When the feature is enabled] Select a NinjaOne ticket status from the dropdown list.
7. Click ✓.

Acronis alerts will be cleared when the NinjaOne ticket is set to the selected status.

Closing NinjaOne tickets

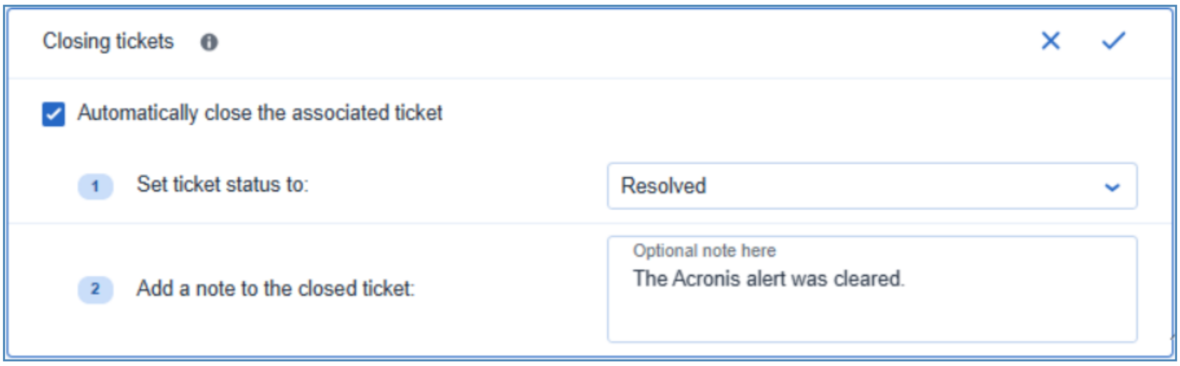
The integration can automatically close NinjaOne tickets which originated from Acronis alerts when the Acronis alert is cleared. This applies to Acronis alerts which are cleared either manually or automatically.

To close NinjaOne tickets

1. Open the integration.
2. Select the **INTEGRATION SETTINGS** tab.
3. Scroll down to **Ticket mapping** > **Closing tickets**.

Note
This option is only available if **Ticket mapping** is enabled.
If **Ticket mapping** is disabled, enable it by turning on the toggle switch.
You must have at least one ticket type in NinjaOne. Otherwise, an error will occur when you enable ticket mapping.

4. Click 🖉 to edit the settings.


Closing tickets

☑ Automatically close the associated ticket

1 Set ticket status to: Resolved

2 Add a note to the closed ticket: The Acronis alert was cleared.

5. To enable the feature, select the **Automatically close the associated ticket** checkbox.
6. In the dropdown list, select the status to which to set NinjaOne tickets if the Acronis alert is cleared.
7. [Optional] Enter a note to add to the NinjaOne ticket.
8. Click ✓.

Re-opening NinjaOne tickets

When an Acronis alert is raised again on the same device within a certain amount of time, the integration can either:

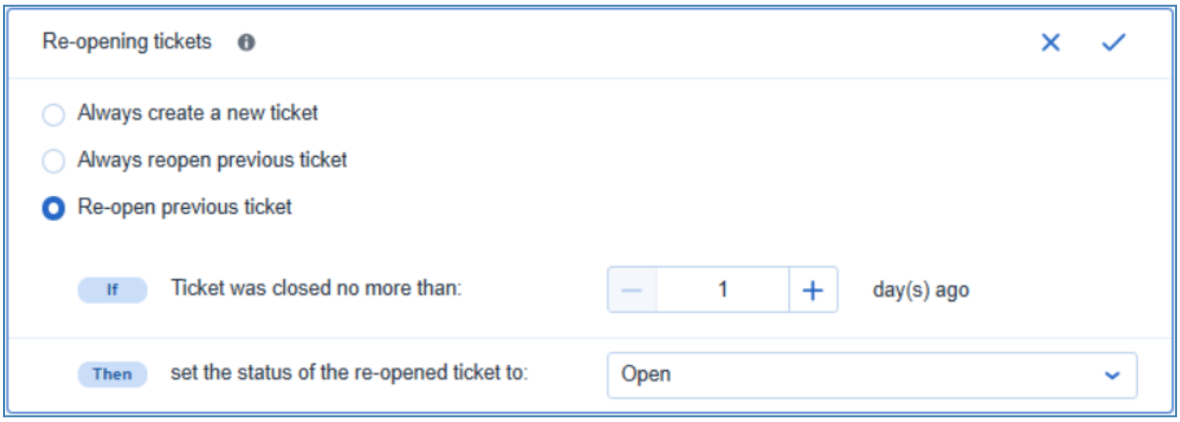
- Create a new NinjaOne ticket (default behavior).
- Re-open the previously closed NinjaOne ticket.
- Re-open the previously closed NinjaOne ticket only if the Acronis alert reoccurs within a specific time frame after the previous NinjaOne ticket was closed.

To change re-opening tickets settings

1. Open the integration.
2. Select the **INTEGRATION SETTINGS** tab.
3. Scroll down to the **Ticket mapping** > **Re-opening tickets**.

   > **Note**
   > This option is only available if **Ticket mapping** is enabled.
   > If **Ticket mapping** is disabled, enable it by turning on the toggle switch.
   > You must have at least one ticket type in NinjaOne. Otherwise, an error will occur when you enable ticket mapping.

4. Click 🖉.



Re-opening tickets

○ Always create a new ticket
○ Always reopen previous ticket
● Re-open previous ticket

If Ticket was closed no more than: 1 day(s) ago

Then set the status of the re-opened ticket to: Open

5. Select the **Always create a new ticket**, **Always re-open previous ticket** or **Re-open previous ticket** radio button.
6. [If you selected **Re-open previous ticket**] Specify the maximum number of days to have passed since the previous NinjaOne ticket closed in the **Ticket was closed no more than** number counter.
   (the maximum is 365 days)
7. [If you selected either of the reopen options] Specify the status of the NinjaOne ticket after reopening.
8. Click ✓.

Customers

You must map NinjaOne organizations with Acronis customer tenants so that the integration can perform synchronization of monitoring statuses and alerts for those entities.

The CUSTOMER MAPPING tab

The **CUSTOMER MAPPING** tab lists all your NinjaOne organizations. It displays:

- NinjaOne organization name.
- The status of the integration mapping for the NinjaOne organization.
    - **Not mapped** indicates that the NinjaOne organization is not linked to an Acronis customer.
    - **Mapped** indicates that the NinjaOne organization is linked to an Acronis customer tenant.
    - **Mapping error** means that an error occurred with the existing or while trying to apply a new mapping. For more details, click on the information icon right next to the status. Mapping errors will be cleared automatically on the next list reload, when the reason for the failure has been addressed.
- [For mapped NinjaOne organizations] The corresponding Acronis customer tenant.

Mapping customers

There are two ways to map NinjaOne organizations to Acronis customer tenants.

Mapping to existing Acronis customer tenants

If an appropriate Acronis customer tenant already exists, you can map a single NinjaOne organization to it.

Note
For more information, see Mapping to an existing Acronis customer tenant.

Provisioning and mapping to new Acronis customer tenants

If there is no appropriate Acronis customer tenant, the integration can provision a new one and map the NinjaOne organization to it.

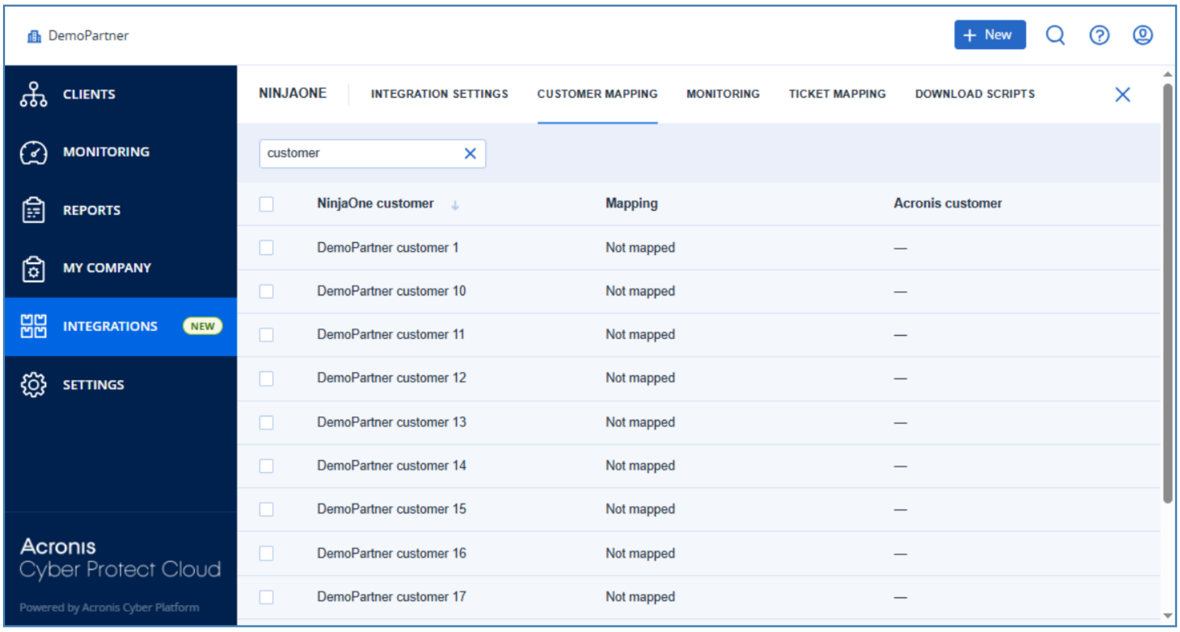
Note
For more information, see Mapping to new Acronis customer tenants.

Mapping to an existing Acronis customer

If an appropriate Acronis customer already exists, you can map a NinjaOne organization to it.

To map to an existing Acronis customer

1. Open the integration.
2. Select the **CUSTOMER MAPPING** tab.
3. [Optional] Type in the **Search** field to filter the list based on the NinjaOne organization names.



customer

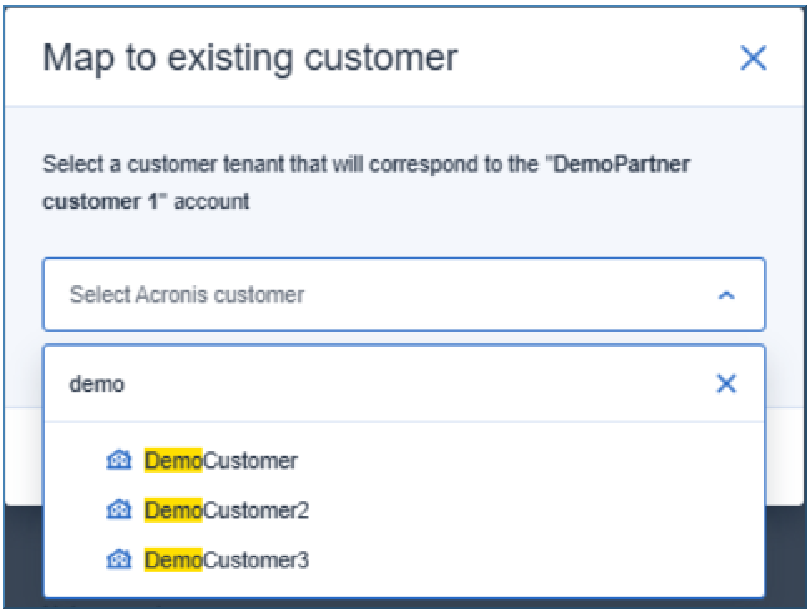
□	NinjaOne customer	Mapping	Acronis customer
□	DemoPartner customer 1	Not mapped	—
□	DemoPartner customer 10	Not mapped	—
□	DemoPartner customer 11	Not mapped	—
□	DemoPartner customer 12	Not mapped	—
□	DemoPartner customer 13	Not mapped	—
□	DemoPartner customer 14	Not mapped	—
□	DemoPartner customer 15	Not mapped	—
□	DemoPartner customer 16	Not mapped	—
□	DemoPartner customer 17	Not mapped	—

4. Select the NinjaOne organization you want to map.
5. Click **Map to existing customer tenant**.

> **Note**
> This button is only available if you select a single NinjaOne organization.
> You cannot map multiple NinjaOne organizations to a single Acronis customer.

6. Select an Acronis customer tenant from the dropdown.

> **Note**
> Use the **Search** option to filter the list.



Map to existing customer

Select a customer tenant that will correspond to the "DemoPartner customer 1" account

7. Click **Map**.

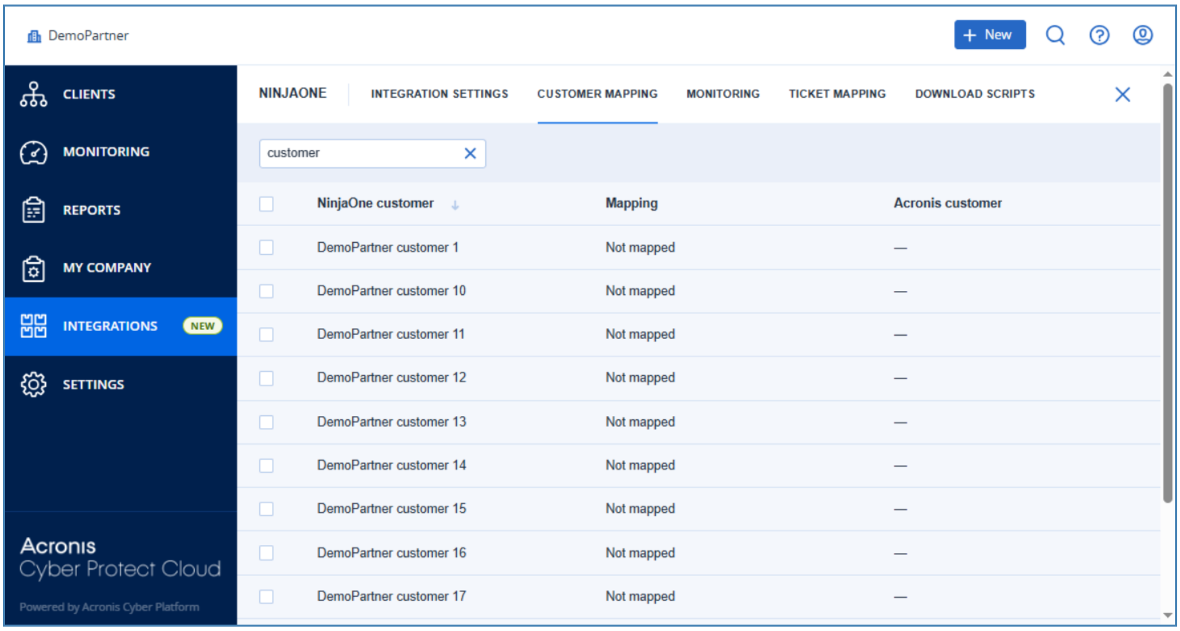
Mapping to a new Acronis customer

If there is no appropriate Acronis customer, the integration can provision a new customer tenant in Acronis and map the NinjaOne organization to it.

You can select multiple NinjaOne organizations for this action. The integration provisions new Acronis customers and maps each NinjaOne organization to the corresponding one.

To map to a new Acronis customer

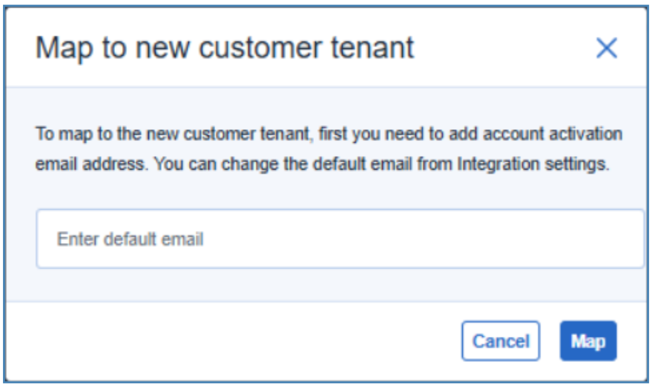
1. Open the integration.
2. Select the **CUSTOMER MAPPING** tab.
3. [Optional] Type in the **Search** field to filter the list based on the NinjaOne organization names.



customer

□	NinjaOne customer	Mapping	Acronis customer
□	DemoPartner customer 1	Not mapped	—
□	DemoPartner customer 10	Not mapped	—
□	DemoPartner customer 11	Not mapped	—
□	DemoPartner customer 12	Not mapped	—
□	DemoPartner customer 13	Not mapped	—
□	DemoPartner customer 14	Not mapped	—
□	DemoPartner customer 15	Not mapped	—
□	DemoPartner customer 16	Not mapped	—
□	DemoPartner customer 17	Not mapped	—

4. Select the NinjaOne organizations you want to map.
5. Click **Map to new customer tenant**.
6. [If you selected multiple customers] Verify the list of organizations to provision and map, then click **Map customers**.
7. [If you have not yet specified **Activation email** in the **Customer provisioning** section of the **INTEGRATION SETTINGS** tab] Enter an activation email.


Map to new customer tenant

To map to the new customer tenant, first you need to add account activation email address. You can change the default email from Integration settings.

Enter default email

Note

The email you enter here is assigned as the default **Activation email** value. For more information, see Customer provisioning.

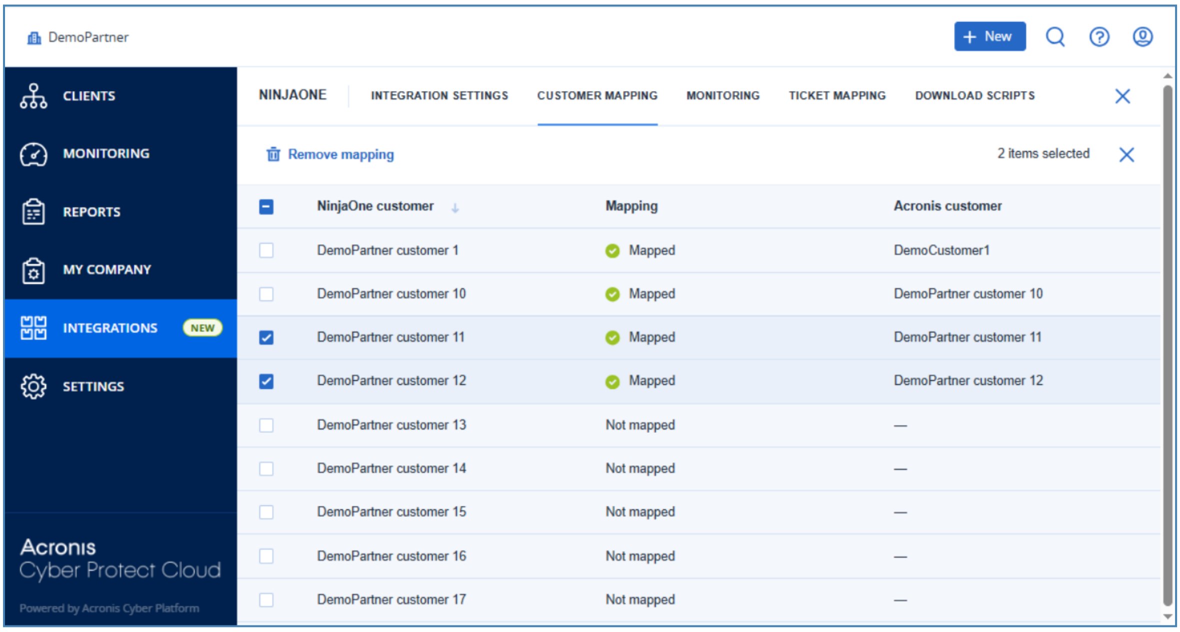
Removing a customer mapping

Note

The Acronis customer tenant and associated storage usage are unaffected, and NinjaOne tickets which have been created for unmapped customers are also unaffected.

To remove a customer mapping

1. Open the integration.
2. Select the **CUSTOMER MAPPING** tab.
3. [Optional] Type in the **Search** field to filter the list.
4. Select the organizations for which you want to remove the mapping.



2 items selected

☐	NinjaOne customer ↓	Mapping	Acronis customer
☐	DemoPartner customer 1	✓ Mapped	DemoCustomer1
☐	DemoPartner customer 10	✓ Mapped	DemoPartner customer 10
☑	DemoPartner customer 11	✓ Mapped	DemoPartner customer 11
☑	DemoPartner customer 12	✓ Mapped	DemoPartner customer 12
☐	DemoPartner customer 13	Not mapped	—
☐	DemoPartner customer 14	Not mapped	—
☐	DemoPartner customer 15	Not mapped	—
☐	DemoPartner customer 16	Not mapped	—
☐	DemoPartner customer 17	Not mapped	—

5. Click **Remove mapping**.
6. Check the list of mappings to be removed, and click **Remove**.

Monitoring

To monitor the Acronis statuses in NinjaOne, you must first create custom fields in NinjaOne for the stauses you want the integration to report, and then map the Acronis status fields to the NinjaOne custom fields you created. The integration will manage the custom fields per device.

There are seven Acronis agent status reporting fields available through the integration:

- Acronis agent version (text)
- Protection status (text)
- Protection plan name (text)
- Last backup date (date/time)
- Next backup date (date/time)
- Last antimalware scan date (date/time)
- Next antimalware scan date (date/time)

Creating NinjaOne custom fields

You must create a NinjaOne custom field for each Acronis agent status reporting field you want the integration to update.

There are seven Acronis agent status reporting fields available through the integration:

- Acronis agent version (text)
- Protection status (text)
- Protection plan name (text)
- Last backup date (date/time)
- Next backup date (date/time)
- Last antimalware scan date (date/time)
- Next antimalware scan date (date/time)

To create NinjaOne custom fields

1. Log in to NinjaOne.
2. Navigate to **Administration** > **Devices.**
3. Select either **Role Custom Fields** or **Global Custom Fields**.
4. Create the custom fields.

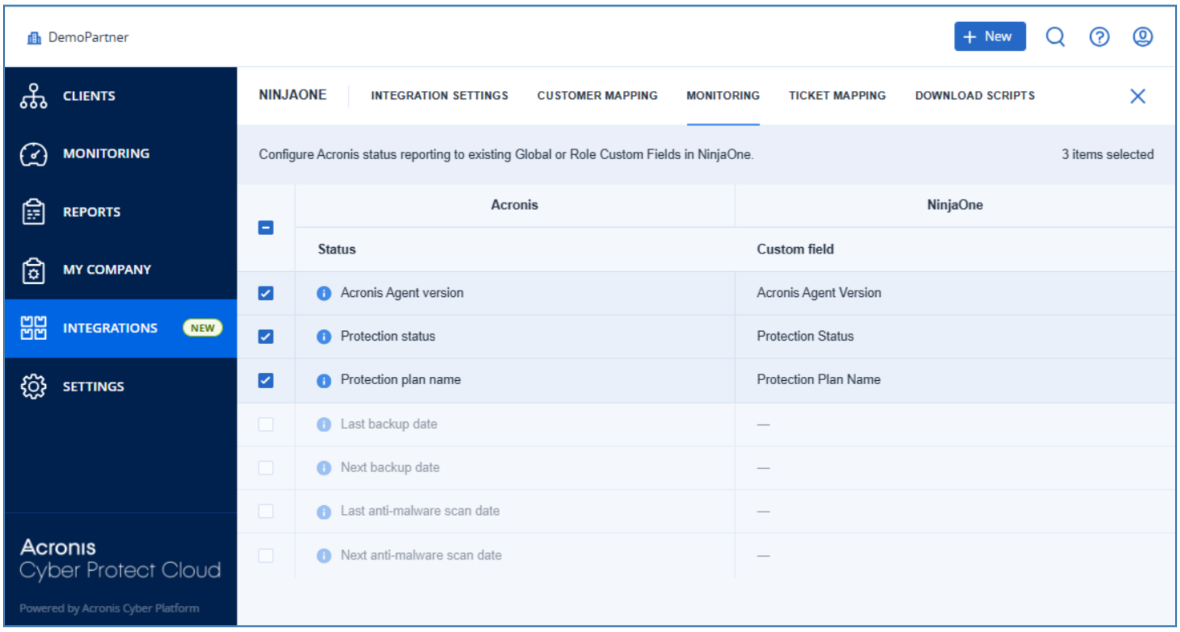
Important
Make sure that the **API permission** for the custom field selected in NinjaOne is set to include the read/write option. Otherwise, the status update might fail.

Mapping Acronis status fields to NinjaOne custom fields

You must map Acronis agent status fields to the NinjaOne custom fields you create for the integration to update those Acronis-protected device statuses on NinjaOne.

To map Acronis status fields to NinjaOne custom fields

1. Open the integration.
2. Select the **MONITORING** tab.



Configure Acronis status reporting to existing Global or Role Custom Fields in NinjaOne.

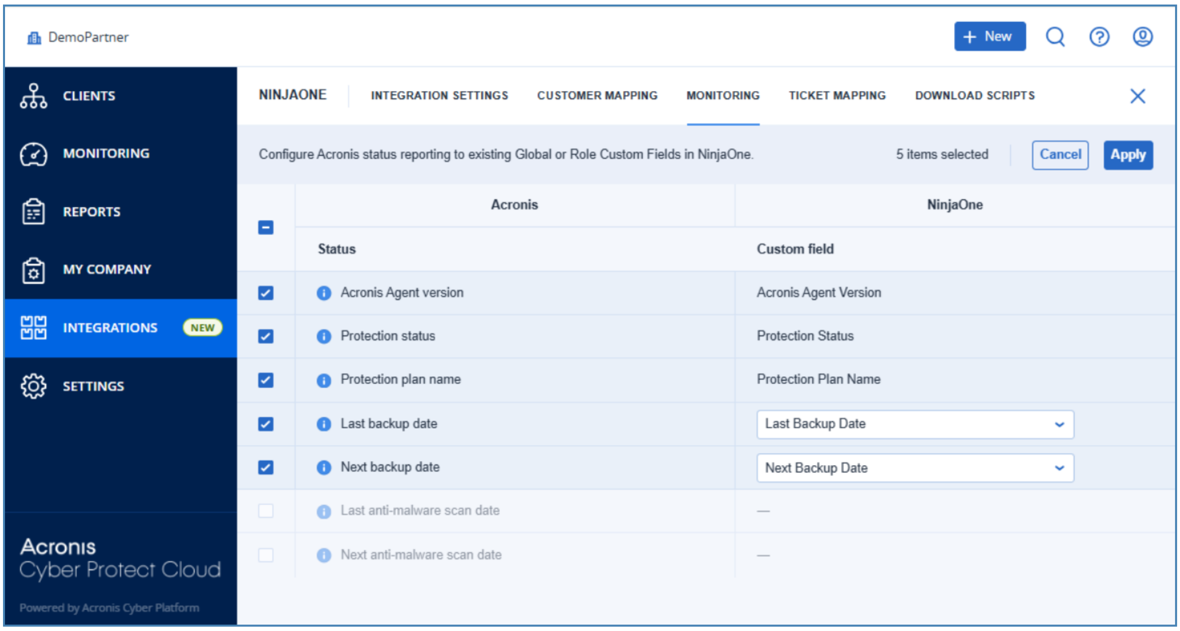
3 items selected

	Acronis	NinjaOne
⊟	Status	Custom field
☑	Acronis Agent version	Acronis Agent Version
☑	Protection status	Protection Status
☑	Protection plan name	Protection Plan Name
□	Last backup date	—
□	Next backup date	—
□	Last anti-malware scan date	—
□	Next anti-malware scan date	—

3. Select the Acronis status field checkboxes that you want to monitor on NinjaOne.

Note
To remove a monitor mapping, clear the Acronis status field checkbox.

4. From the dropdown lists, select the NinjaOne custom field to which to map each Acronis status field status.



Configure Acronis status reporting to existing Global or Role Custom Fields in NinjaOne.

	Acronis	NinjaOne
▬	Status	Custom field
☑	Acronis Agent version	Acronis Agent Version
☑	Protection status	Protection Status
☑	Protection plan name	Protection Plan Name
☑	Last backup date	Last Backup Date
☑	Next backup date	Next Backup Date
□	Last anti-malware scan date	—
□	Next anti-malware scan date	—

Important

The custom fields are available for selection only if the API permissions for them are set to read/write, and if they are of the same type as the status.

- Text for Acronis Agent version, Protection status, Protection plan name.
- Date/time for Last backup date, Next backup date, Last anti-malware scan date, Next anti-malware scan date.

5. Click **Apply**.

Checking Acronis statuses of NinjaOne devices

The custom fields of a NinjaOne device which is protected by the integration includes all the Acronis status fields which you mapped to the custom fields you created.

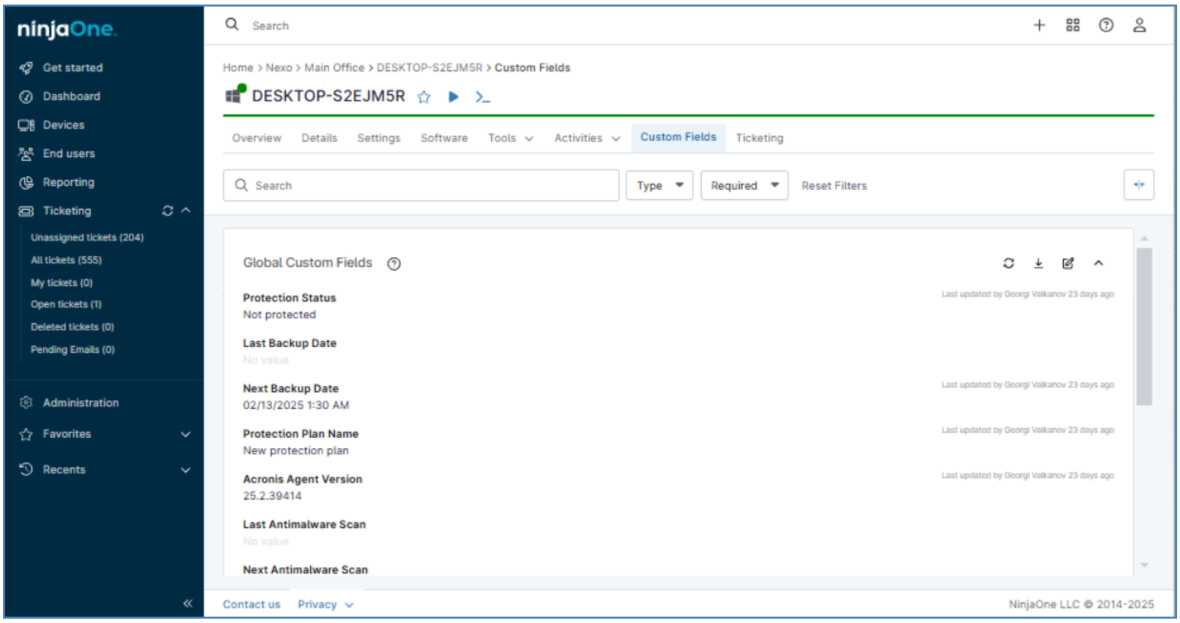
Note

For more information, see Mapping Acronis agent status fields to NinjaOne custom fields.

To check Acronis statuses of NinjaOne devices

1. Log in to NinjaOne.
2. Select Devices.
3. Select the NinjaOne device you want to check.

4. Select the **Custom Fields** tab.



Protection Status
Not protected
Last updated by Georgi Valkanov 23 days ago

Last Backup Date
No value

Next Backup Date
02/13/2025 1:30 AM
Last updated by Georgi Valkanov 23 days ago

Protection Plan Name
New protection plan
Last updated by Georgi Valkanov 23 days ago

Acronis Agent Version
25.2.39414
Last updated by Georgi Valkanov 23 days ago

Last Antimalware Scan
No value

Next Antimalware Scan

Tickets

When ticket mapping is enabled, the integration creates a NinjaOne ticket when a mapped Acronis alert occurs on a protected workload of an Acronis customer which is mapped to a NinjaOne organization.

Ticket mapping configures which Acronis alerts trigger the creation of tickets in NinjaOne. All standard Acronis alerts can be synced, except for those configured in the Monitoring plans of the Acronis RMM pack.

When the integration creates a ticket in NinjaOne:

- The NinjaOne **Brief Description** field is set to correspond to the Acronis alert title.
- The NinjaOne **Severity**, **Status**, and **Priority** fields are set to the mapped alert configuration.

Ticket synchronization

Ticket synchronization creates NinjaOne tickets for any Acronis alerts which have occured for mapped customers since the previous synchronization. Synchronization is bi-directional and occurs every 10-15 mins.

Additional integration ticket functionality

The integration can also:

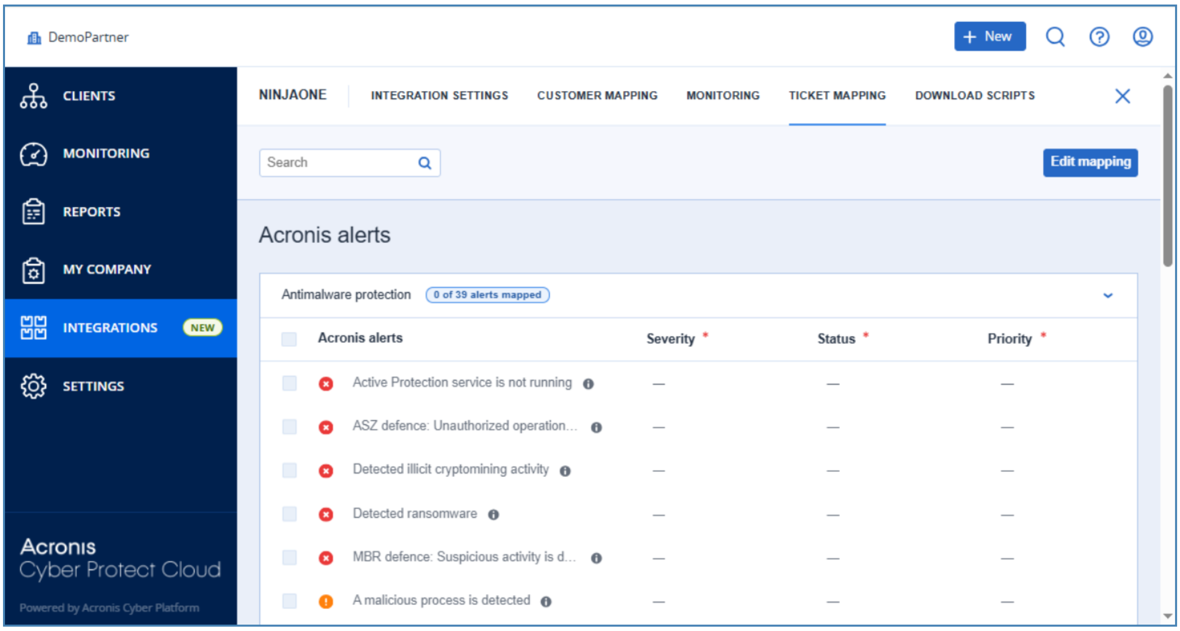
- Clear Acronis alerts automatically when mapped NinjaOne tickets change to a predetermined status.
- Close NinjaOne tickets automatically when the mapped Acronis alert is cleared.
  The NinjaOne ticket is changed to a predetermined status, and a predetermined note can also be added to the NinjaOne ticket.
- Reopen NinjaOne tickets if the same Acronis alert is raised for the same protected device within a predetermined period of time.

Mapping Acronis alerts to NinjaOne tickets

Note
If multiple tickets that you want to map have the same or similar values for the ticket **Severity**, **Status**, and/or **Priority** fields, you can configure ticket mapping defaults to more efficiently map multiple tickets.

To map Acronis alerts to NinjaOne tickets

1. Open the integration.
2. Select the **TICKET MAPPING** tab.



□	Acronis alerts	Severity *	Status *	Priority *
□	Active Protection service is not running	—	—	—
□	ASZ defence: Unauthorized operation...	—	—	—
□	Detected illicit cryptomining activity	—	—	—
□	Detected ransomware	—	—	—
□	MBR defence: Suspicious activity is d...	—	—	—
□	A malicious process is detected	—	—	—

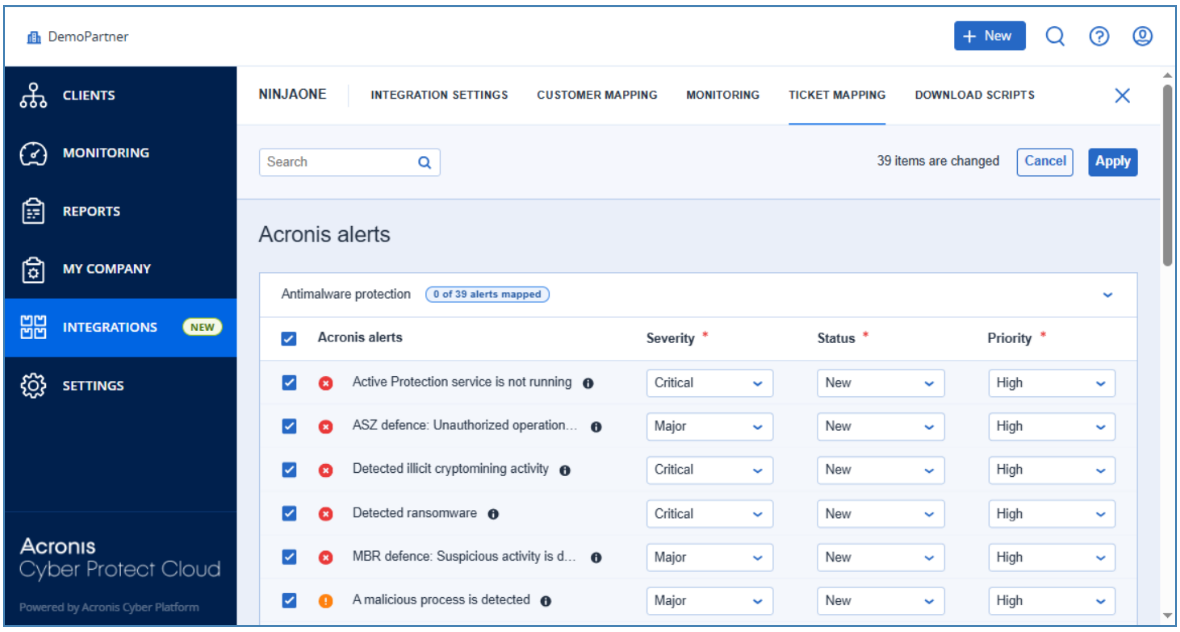
3. Click **Edit mapping**.
4. Locate the Acronis alerts you want to map, and select their checkboxes.

Note

The **TICKET MAPPING** tab groups Acronis alerts by the alert source (antimalware protection, backup, EDR, etc.). Each alert group displays a running total of how many alerts are mapped.

You can dynamically filter the contents of the Acronis alert lists by typing a string in the **Search** field at the top of the page.

5. [To delete existing ticket mappings] Clear the checkboxes of previously mapped Acronis alerts.
6. [Optional] Modify ticket field values, as required.



☑	Acronis alerts	Severity *	Status *	Priority *
☑	Active Protection service is not running	Critical	New	High
☑	ASZ defence: Unauthorized operation...	Major	New	High
☑	Detected illicit cryptomining activity	Critical	New	High
☑	Detected ransomware	Critical	New	High
☑	MBR defence: Suspicious activity is d...	Major	New	High
☑	A malicious process is detected	Major	New	High

Note

Initially, the values of the ticket **Severity**, **Status**, and **Priority** fields are set to the ticket mapping defaults specified in **INTEGRATION SETTINGS** > **Ticket mapping** > **Tickets**.

If you haven't set a default, the ticket field will be null, and you must set the field manually.

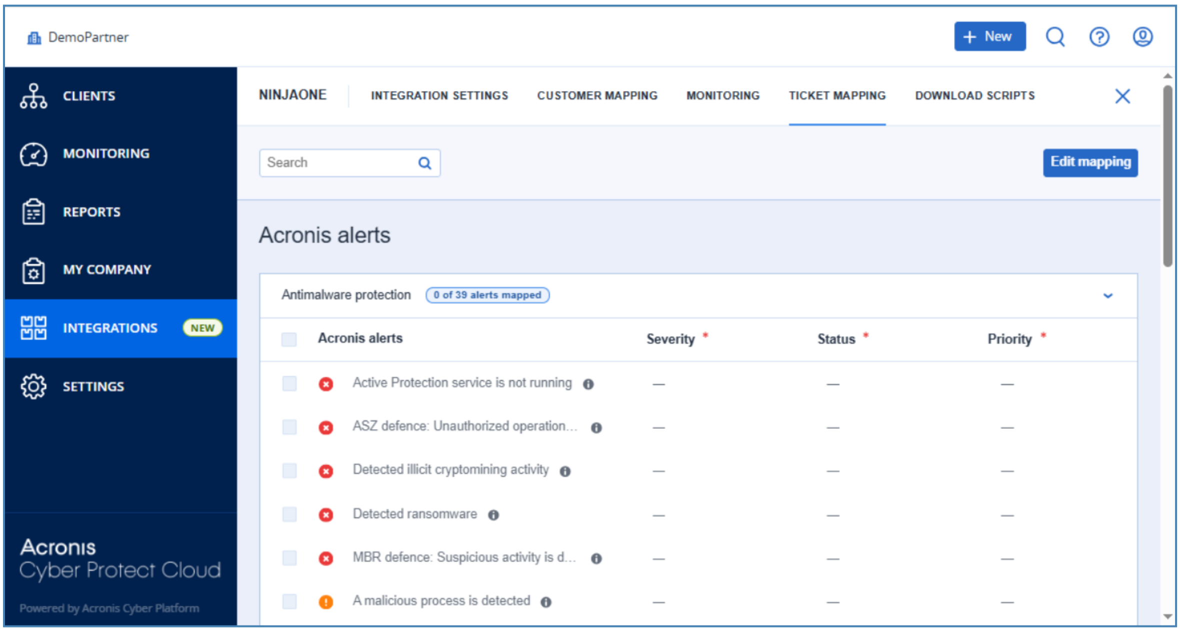
7. Click **Apply**.

Deleting ticket mappings

You can also map Acronis alerts to NinjaOne tickets while deleting ticket mappings.

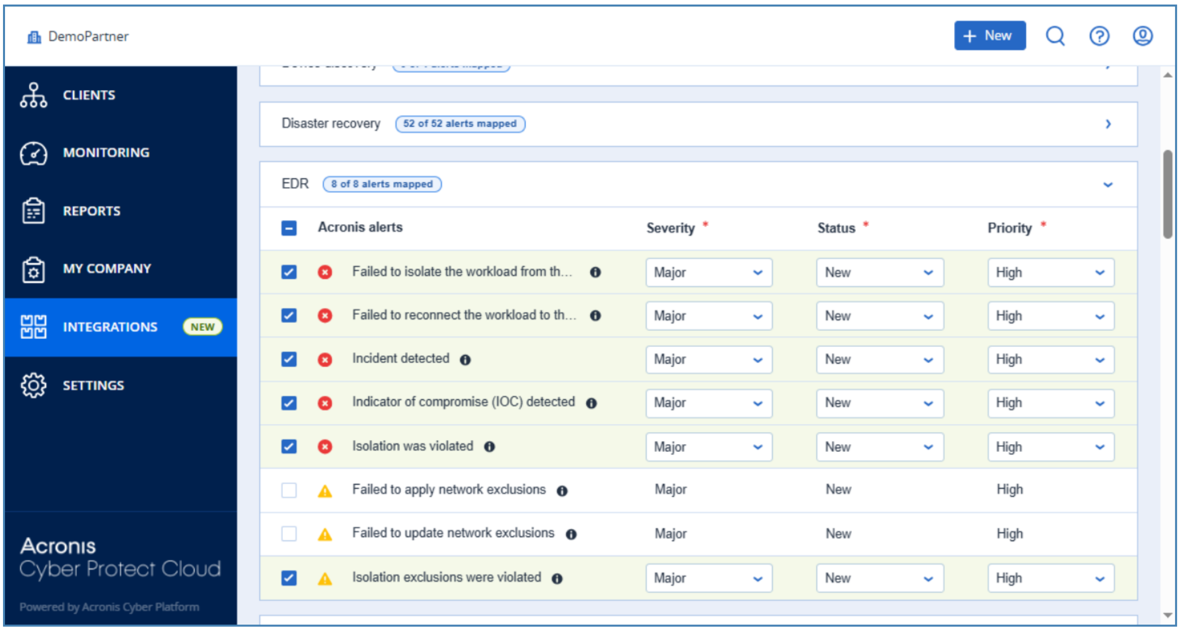
To delete ticket mappings

1. Open the integration.
2. Select the **TICKET MAPPING** tab.



□	Acronis alerts	Severity *	Status *	Priority *
□	Active Protection service is not running	—	—	—
□	ASZ defence: Unauthorized operation...	—	—	—
□	Detected illicit cryptomining activity	—	—	—
□	Detected ransomware	—	—	—
□	MBR defence: Suspicious activity is d...	—	—	—
□	A malicious process is detected	—	—	—

3. Click **Edit mapping**.
4. Locate the Acronis alerts for which you want to delete the mappings, and clear their checkboxes.



Disaster recovery 52 of 52 alerts mapped

EDR 8 of 8 alerts mapped

	Acronis alerts	Severity *	Status *	Priority *
☑	Failed to isolate the workload from th...	Major	New	High
☑	Failed to reconnect the workload to th...	Major	New	High
☑	Incident detected	Major	New	High
☑	Indicator of compromise (IOC) detected	Major	New	High
☑	Isolation was violated	Major	New	High
□	Failed to apply network exclusions	Major	New	High
□	Failed to update network exclusions	Major	New	High
☑	Isolation exclusions were violated	Major	New	High

5. Click **Apply**.

Scripts

Script-based functionality

Integration scripts enable a variety of Acronis cybersecurity tasks from within NinjaOne. Using the integration scripts, you can:

- Install the Acronis agent on Windows, Linux, and Mac workloads.
- Uninstall the Acronis agent from Windows, Linux, and Mac workloads.
- Apply and revoke Acronis protection plans.
- Perform Acronis scan tasks on protected workloads.

Scripts are bundled into OS-specific script packages, which you must download from the integration management interface and then upload to the NinjaOne scripting library.

Script packages

The integration includes 3 script packages. Each package includes scripts for Acronis actions on a specific operating system:

- `NinjaOneScriptsWindows.zip` for Windows contains 10 PowerShell scripts.
- `NinjaOneScriptsMacOS.zip` for MacOS contains 8 shell scripts.
- `NinjaOneScriptsLinux.zip` for Linux contains 6 shell scripts.

Script	Windows	MacOS	Linux
Acronis_install_agent	✓	✓	✓
Acronis_uninstall_agent	✓	✓	✓
Acronis_scans	✓	✓	✓
Acronis_manage_protection_plan	✓	✓	✓
Acronis_last_backup*	✓	✓	✓
Acronis_backup_failed*	✓	✓	✓
Acronis_last_malware_scan*	✓	✓	✗
Acronis_malware_detected_alert*	✓	✓	✗
Acronis_last_antivirus_scan*	✓	✗	✗
Acronis_antivirus_failed_alert*	✓	✗	✗

Note

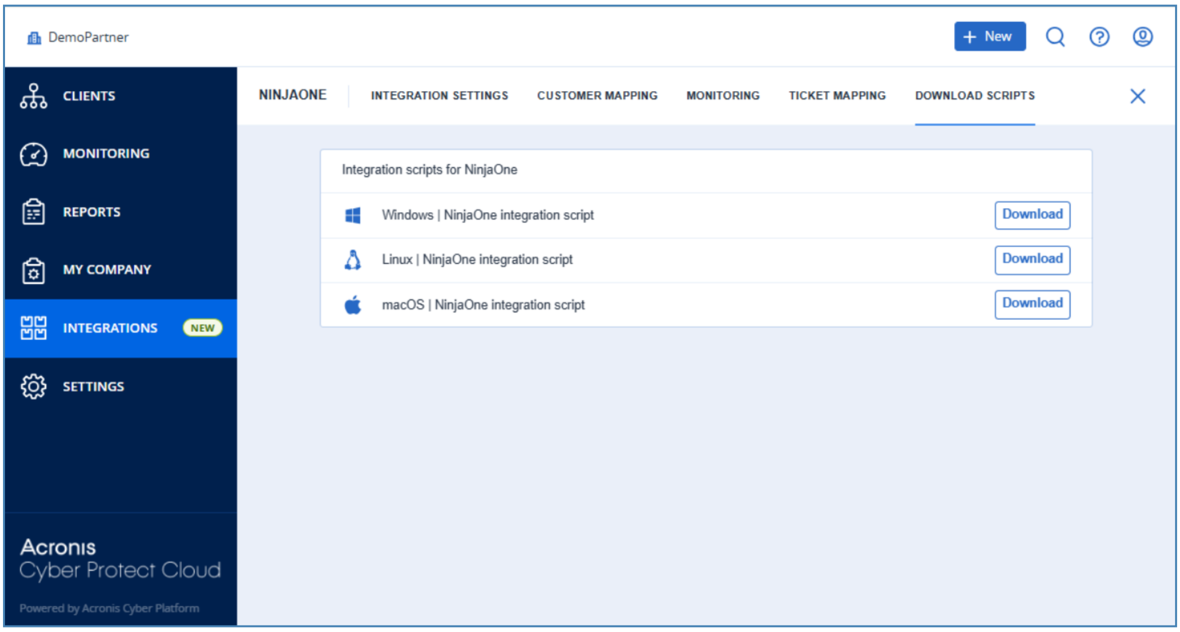
* These scripts are legacy monitoring scripts.
For more information, see Monitoring using scripts (legacy functionality).

To set up the integration script functionality in NinjaOne, you must download the script packages for the operating systems you require for your workloads and then upload them to NinjaOne scripting library.

Downloading script packages

To download a script package

1. Open the integration.
2. Select the **DOWNLOAD SCRIPTS** tab.



Integration scripts for NinjaOne

Windows | NinjaOne integration script
Linux | NinjaOne integration script
macOS | NinjaOne integration script

3. Click **Download** for the script packages you require.
4. Unzip the packages to a local folder.

Uploading integration scripts to NinjaOne

Note

In order for some scripts to run, they must be supplied with a registration token which identifies the Acronis customer tenant and protection plan (if selected), and/or the Acronis data center (DC) URL. The registration token is automatically generated by Acronis, and both values are stored in NinjaOne custom fields.

For more information on how to set up the custom fields in NinjaOne, see Creating custom fields.

To upload integration scripts to NinjaOne

1. Log in to NinjaOne.
2. Select ⚙ Administration.
3. Select **Library** > **Automation**.
4. Click **+ Add** > **Import from file**.
5. Locate folder to which you unzipped the downloaded script packages.
6. Select one of the script files to upload and click **Open**.

   > **Important**
   > Whereas Windows follows the original convention of a carriage return plus a line feed (CRLF) for line endings, operating systems like Linux and Mac use only the line feed (LF) character. In order to prevent issues when running the script, avoid copying/pasting scripts to NinjaOne. Instead, import the scripts through the NinjaOne interface, the way they have been downloaded from the Acronis console or drag and drop the files.

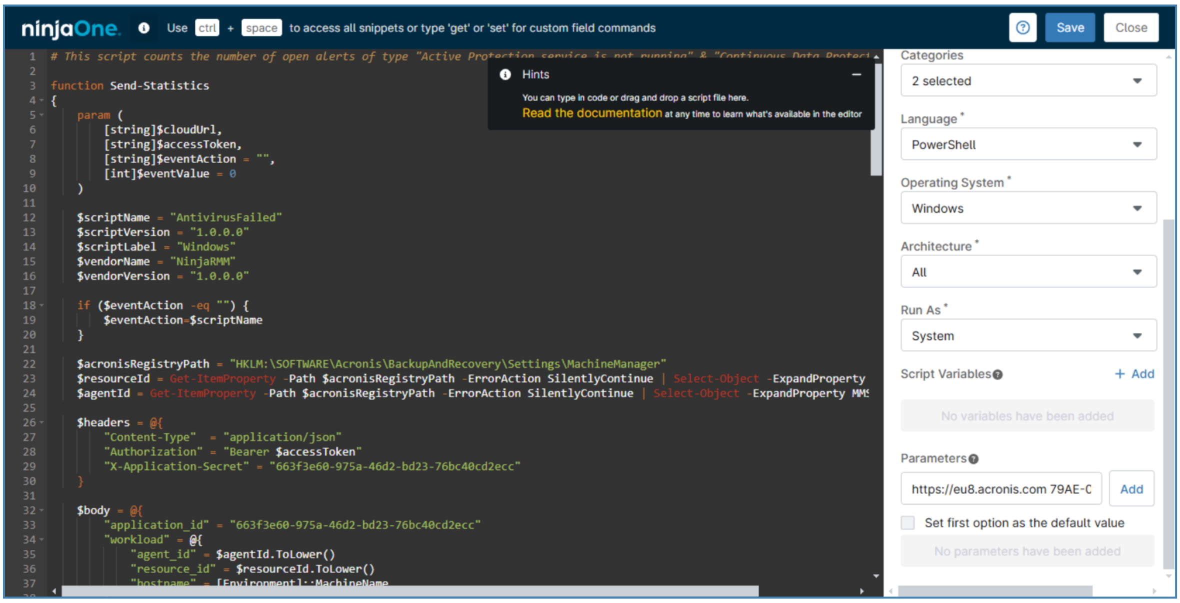
7. Enter a **Name** for the script.
8. Enter a **Description**.
9. Select one or more **Categories** from the dropdown list.
10. Select the **Language** from the dropdown list (PowerShell for Windows and ShellScript for Linux).
11. Select the **Operating System** from the dropdown list.
12. Select the **Architecture** from the dropdown list.
    (We recommend **All**).
13. Create Parameters for the scripts, as follows:

    Acronis_install_agent

    Enter the Acronis Data Center URL, followed by a blank space, followed by the Acronis registration token.

    > **Note**
    > For more information, see Generating a registration token.
    > The optional value for Protection Plan can be used in combination with this script to apply the selected protection plan.

    The parameter should look something like this: `https://eu8.acronis.com 79AE-07AD-440C`.



ninjaOne
Use ctrl + space to access all snippets or type 'get' or 'set' for custom field commands
Save
Close
Hints
You can type in code or drag and drop a script file here.
Read the documentation at any time to learn what's available in the editor
+ Add
Add

```powershell
# This script counts the number of open alerts of type "Active Protection service is not running" & "Continuous Data Protecti

function Send-Statistics
{
    param (
        [string]$cloudUrl,
        [string]$accessToken,
        [string]$eventAction = "",
        [int]$eventValue = 0
    )

    $scriptName = "AntivirusFailed"
    $scriptVersion = "1.0.0.0"
    $scriptLabel = "Windows"
    $vendorName = "NinjaRMM"
    $vendorVersion = "1.0.0.0"

    if ($eventAction -eq "") {
        $eventAction=$scriptName
    }

    $acronisRegistryPath = "HKLM:\SOFTWARE\Acronis\BackupAndRecovery\Settings\MachineManager"
    $resourceId = Get-ItemProperty -Path $acronisRegistryPath -ErrorAction SilentlyContinue | Select-Object -ExpandProperty
    $agentId = Get-ItemProperty -Path $acronisRegistryPath -ErrorAction SilentlyContinue | Select-Object -ExpandProperty MMS

    $headers = @{
        "Content-Type"  = "application/json"
        "Authorization" = "Bearer $accessToken"
        "X-Application-Secret" = "663f3e60-975a-46d2-bd23-76bc40cd2ecc"
    }

    $body = @{
        "application_id" = "663f3e60-975a-46d2-bd23-76bc40cd2ecc"
        "workload" = @{
            "agent_id" = $agentId.ToLower()
            "resource_id" = $resourceId.ToLower()
            "hostname" = [Environment]::MachineName
```

Categories: 2 selected

Language *: PowerShell

Operating System *: Windows

Architecture *: All

Run As *: System

Script Variables: No variables have been added

Parameters: https://eu8.acronis.com 79AE-C

□ Set first option as the default value

No parameters have been added

Click **Add**.

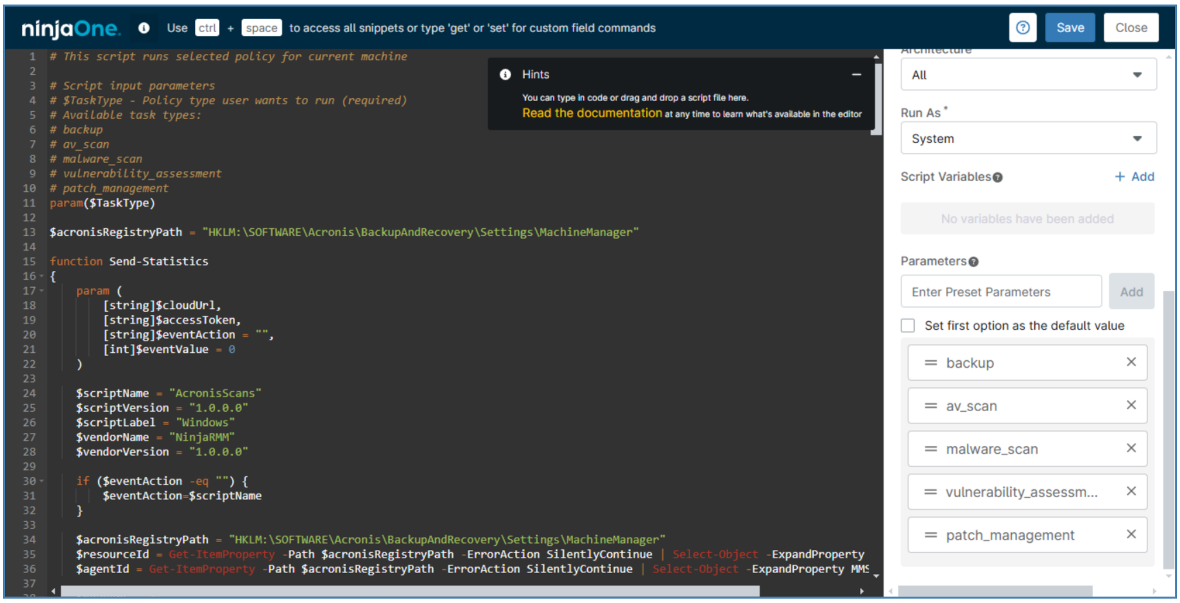
Important

As long as a registration token is generated for a specific customer tenant, the script will be applicable to devices, associated with this particular tenant. In order to be able to run the script for another customer tenant, the token parameter has to be updated or the script copied and supplied with a token value for each customer.

Acronis_scans

Add five parameters as follows:

- `backup`
- `av_scan`
- `malware_scan`
- `vulnerability_assessment`
- `patch_management`



Use ctrl + space to access all snippets or type 'get' or 'set' for custom field commands

Hints

You can type in code or drag and drop a script file here.
Read the documentation at any time to learn what's available in the editor

```
# This script runs selected policy for current machine

# Script input parameters
# $TaskType - Policy type user wants to run (required)
# Available task types:
# backup
# av_scan
# malware_scan
# vulnerability_assessment
# patch_management
param($TaskType)

$acronisRegistryPath = "HKLM:\SOFTWARE\Acronis\BackupAndRecovery\Settings\MachineManager"

function Send-Statistics
{
    param (
        [string]$cloudUrl,
        [string]$accessToken,
        [string]$eventAction = "",
        [int]$eventValue = 0
    )

    $scriptName = "AcronisScans"
    $scriptVersion = "1.0.0.0"
    $scriptLabel = "Windows"
    $vendorName = "NinjaRMM"
    $vendorVersion = "1.0.0.0"

    if ($eventAction -eq "") {
        $eventAction=$scriptName
    }

    $acronisRegistryPath = "HKLM:\SOFTWARE\Acronis\BackupAndRecovery\Settings\MachineManager"
    $resourceId = Get-ItemProperty -Path $acronisRegistryPath -ErrorAction SilentlyContinue | Select-Object -ExpandProperty
    $agentId = Get-ItemProperty -Path $acronisRegistryPath -ErrorAction SilentlyContinue | Select-Object -ExpandProperty MMS
```

Architecture: All

Run As *: System

Script Variables + Add

No variables have been added

Parameters

Enter Preset Parameters Add

□ Set first option as the default value

- backup
- av_scan
- malware_scan
- vulnerability_assessm...
- patch_management

Acronis_manage_protection_plan

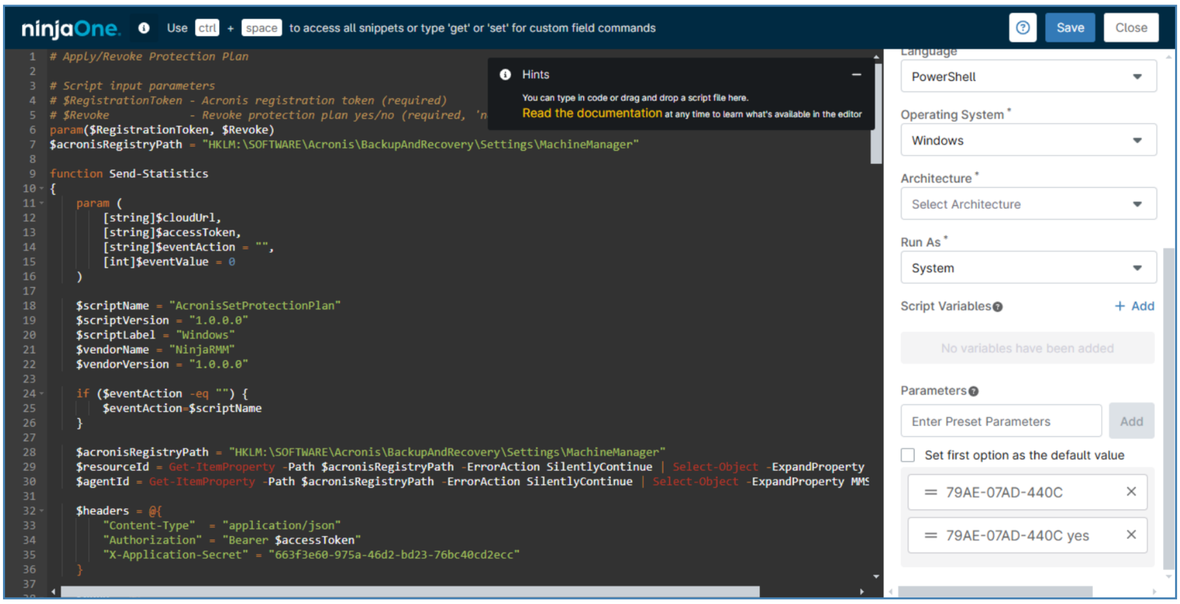
Add two parameters as follows:

- Acronis registration token.
- Acronis registration token, followed by a space, followed by `yes`.

Note

For more information, see Generating a registration token.

The optional value for Protection Plan can be used in combination with this script to apply the selected protection plan.



Use ctrl + space to access all snippets or type 'get' or 'set' for custom field commands

Hints

You can type in code or drag and drop a script file here.
Read the documentation at any time to learn what's available in the editor

```
# Apply/Revoke Protection Plan

# Script input parameters
# $RegistrationToken - Acronis registration token (required)
# $Revoke            - Revoke protection plan yes/no (required, 'n
param($RegistrationToken, $Revoke)
$acronisRegistryPath = "HKLM:\SOFTWARE\Acronis\BackupAndRecovery\Settings\MachineManager"

function Send-Statistics
{
    param (
        [string]$cloudUrl,
        [string]$accessToken,
        [string]$eventAction = "",
        [int]$eventValue = 0
    )

    $scriptName = "AcronisSetProtectionPlan"
    $scriptVersion = "1.0.0.0"
    $scriptLabel = "Windows"
    $vendorName = "NinjaRMM"
    $vendorVersion = "1.0.0.0"

    if ($eventAction -eq "") {
        $eventAction=$scriptName
    }

    $acronisRegistryPath = "HKLM:\SOFTWARE\Acronis\BackupAndRecovery\Settings\MachineManager"
    $resourceId = Get-ItemProperty -Path $acronisRegistryPath -ErrorAction SilentlyContinue | Select-Object -ExpandProperty
    $agentId = Get-ItemProperty -Path $acronisRegistryPath -ErrorAction SilentlyContinue | Select-Object -ExpandProperty MMS

    $headers = @{
        "Content-Type"  = "application/json"
        "Authorization" = "Bearer $accessToken"
        "X-Application-Secret" = "663f3e60-975a-46d2-bd23-76bc40cd2ecc"
    }
```

Language: PowerShell

Operating System *: Windows

Architecture *: Select Architecture

Run As *: System

Script Variables + Add

No variables have been added

Parameters

Enter Preset Parameters Add

□ Set first option as the default value

- 79AE-07AD-440C
- 79AE-07AD-440C yes

Acronis_last_antivirus_scan

(Windows only)

(Windows and MacOs only)

Add one or more (integer) parameters to represent the number of days since the previous antivirus scan event. For example, you could specify options of 1 day, 2 days, 5 days, and 1 week:

- 1
- 2
- 5
- 7

> **Note**
> If you do not specify any parameters, the default value is 7.

Acronis_last_malware_scan

(Windows and MacOs only)

Add one or more (integer) parameters to represent the number of days since the previous antivirus scan event. For example, you could specify options of 1 day, 2 days, 5 days, and 1 week:

- 1
- 2
- 5
- 7

> **Note**
> If you do not specify any parameters, the default value is 7.

All other scripts

No paramters are required.

14. Click **Save**, then **Close**.
15. Repeat steps 4 to 14 for all the scripts you want to upload.

Installing the Acronis agent

You can install the Acronis agent on Windows, Linux, and macOS devices.

During installation of the Acronis agent on a workload, the integration registers the workload with Acronis and, if configured, applies a default protection plan.

To install the Acronis agent

1. Log in to NinjaOne.
2. Select Devices.
3. Select the devices on which you want to install the Acronis agent.
4. Select **Run** > **Run Automation** > **Script**.
5. Locate the script you created when you uploaded the `Acronis_install_agent` script.

> **Note**
> For more information, see Uploading the integration scripts to NinjaOne.

Important

Make sure that the device OS matches the script target OS.

6. Click **Preset Parameter** and select the value configured for this script.
7. Select **System** from the **Run As** dropdown list.
8. Click **Run**, then **Yes**.

Uninstalling the Acronis agent

To uninstall the Acronis agent

Note

If **Self-protection and Agent Uninstallation Protection** are enabled in the Acronis protection plan, you must first perform these steps:

1. Log in to Acronis Protection Console.
2. Navigate to the customer tenant > **Settings** > **Agents**.
3. Locate the Acronis NinjaOne agent in the list, and click on the row.
4. In the **Actions** panel, go to **Agent Update Settings**.
5. Under **Set the permitted duration for the agent to be uninstalled or updated**, select the duration of the maintenance window needed to uninstall the agent.

1. Log in to NinjaOne.
2. Select Devices.
3. Select the devices on which you want to install the Acronis agent.
4. Select **Run** > **Run Automation** > **Script**.
5. Locate the script you created when you uploaded the `Acronis_uninstall_agent` script.

Note

For more information, see Uploading the integration scripts to NinjaOne.

Important

Make sure that the device OS matches the script target OS.

6. Leave **Preset Parameter** empty.
7. Select **System** from the **Run As** dropdown list.
8. Click **Run**, then **Yes**.

Performing scans tasks

You can use scripts to perform Acronis scan tasks on protected devices.
Available scan tasks are OS-dependent.

Scan task	Windows	MacOS	Linux
backup	✓	✗	✓
av_scan	✓	✗	✗
malware_scan	✓	✓	✓
vulnerability_assessment	✓	✓	✓
patch_management	✓	✗	✗

To perform scan tasks

1. Log in to NinjaOne.
2. Select Devices.
3. Select the devices on which you want to install the Acronis agent.
4. Select **Run** > **Run Automation** > **Script**.
5. Locate the script you created when you uploaded the `Acronis_scans` script.

   Note
   For more information, see Uploading the integration scripts to NinjaOne.

   Important
   Make sure that the device OS matches the script target OS.

6. Select the type of scan task that needs to be run from the **Preset Parameter** dropdown.
7. Select **System** from the **Run As** dropdown list.
8. Click **Run**, then **Yes**.

Managing protection plans

To manage protection plans

1. Log in to NinjaOne.
2. Select Devices.
3. Select the devices on which you want to install the Acronis agent.
4. Select **Run** > **Run Automation** > **Script**.
5. Locate the script you created when you uploaded the `Acronis_manage_protection_plan` script.

   Note
   For more information, see Uploading the integration scripts to NinjaOne.

Important

Make sure that the device OS matches the script target OS.

6. [If you want to apply a protection plan associated with this token] Click **Preset Parameter** and select the value with **Acronis registration token** only.
7. [If you want to revoke a protection plan associated with this token] Click **Preset Parameter** and select the value with **Acronis registration token**, followed by **yes**.
8. Select **System** from the **Run As** dropdown list.
9. Click **Run**, then **Yes**.

Monitoring using scripts (legacy functionality)

Note

This is legacy functionality, which uses scripts to monitor Acronis statuses instead of monitoring through custom fields.

Monitoring scripts functionality

The following monitoring scripts are included in the script packages:

Script	Functionality
Acronis_last_backup All OSs	Compares the current endpoint date to the last successful backup date and time. If last successful backup is later than the number of days ago, it outputs the sentence `Last succesful backup more than x days ago`.
Acronis_backup_failed All OSs	Counts the number of open alerts of backup failed type, and outputs the sentence `x backups failed`.
Acronis_last_malware_scan Windows and MacOS only	Compares the current endpoint date to the last successful antimalware scan date and time. If last successful antimalware scan was later than the number of days ago, it outputs the sentence `Last succesful antimalware scan more than x days ago`.
Acronis_malware_detected_alert Windows and MacOS only	Cumulatively counts the total number of open alerts of type `Malware is detected and blocked (ODS)` and `Malware is detected and blocked (RTP)`, and outputs the sentence `x MALWARE THREADS has been found`.
Acronis_last_antivirus_scan Windows only	Compares the current endpoint date to the last successful antivirus scan date and time. If last successful antivirus scan was later than the number of days ago, it outputs the sentence `Last succesful`

Script	Functionality
	`antivirus scan more than x days ago`.
Acronis_antivirus_failed_alert Windows only	Counts the number of open alerts of type `Active Protection service is not running` and `Continuous Data Protection failed`, and outputs the sentence `Active protection service failed x times`.

Each monitoring script can be set as either manually or repetitively executed with a NinjaOne scheduled task.

To manually run a monitoring script

1. Log in to NinjaOne.
2. Select Devices.
3. Select the devices on which you want to install the Acronis agent.
4. Select **Run** > **Run Automation** > **Script**.
5. Locate the script you want to run.

> **Note**
> It will have the name you gave it when you uploaded the Acronis script. For more information. see Uploading the integration scripts to NinjaOne.

> **Important**
> Make sure that the device OS matches the script target OS.

6. Select a value from the **Preset Parameter** dropdown, if the script requires any.
7. Select **System** from the **Run As** dropdown list.
8. Click **Run**, then **Yes**.

To create a NinjaOne scheduled task for repetitive monitoring script execution

1. Log in to NinjaOne.
2. Select Devices.
3. Select the devices on which you want to install the Acronis agent.
4. Select **Create** > **Scheduled task**.
5. Specify:
   a. **Name**
   b. [Optional] **Description**.
   c. **Schedule** > **Repeats** from the dropdown list and supply further scheduling information, as required.
6. Click **Add**.
7. Locate and select the script you want to add to the scheduled task.

Note

They will have the name you gave them when you uploaded the Acronis scripts. For more information, see Uploading the integration scripts to NinjaOne.

Important

Make sure that the device OS matches the script target OS.

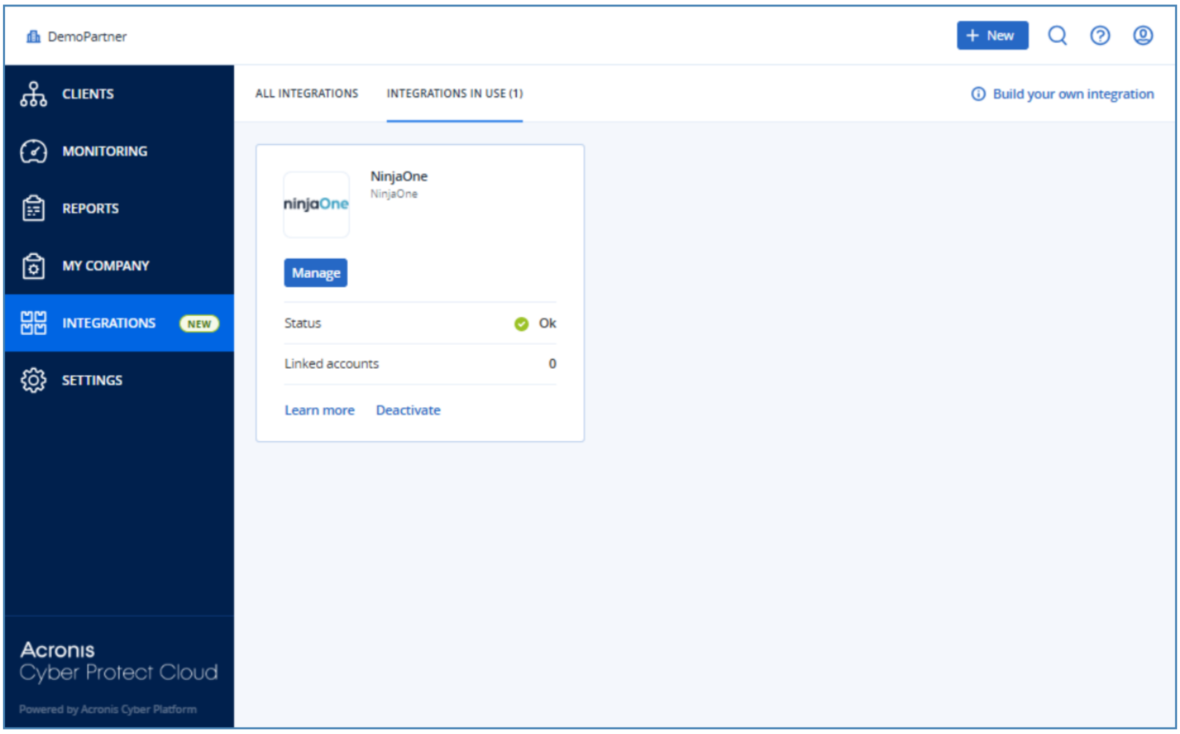
8. Select System from the **Run As** dropdown list.
9. Select the appropriate **Preset Parameter** from the dropdown list.
10. Click **Save**.

Deactivating the integration

To deactivate the integration

1. Log in to Acronis Management Portal as administrator.
2. Select **INTEGRATIONS** on the main menu.
3. Select the **INTEGRATION IN USE** tab.
4. Locate the NinjaOne integration catalog card.

Note
For more information, see the Management Portal partner administrator guide.



5. Click **Deactivate**.
6. Click **Delete**.

Index