Acronis

acronis.com

Acronis Cyber Cloud

Integration with Ninja One

Integration Guide

REVISION: 9/25/2023

Table of contents

Introduction

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

Once setup, the integration enables you to:

- Deploy Acronis on Windows, Linux and Mac devices
- Monitor protected devices
- Apply and revoke protection plans
- Run the following types of automated tasks - backup, antivirus scan, malware scan, vulnerability assessment and patch management
- Provision NinjaOne organizations as new customer tenants in Acronis Cyber Protect Cloud
- Uninstall Acronis agents from Windows, Linux and Mac devices

All this functionality is available from within NinjaOne, without having to go to the Acronis Cyber Protect web interface.

Glossary

- **MSP** - A Managed Service Provider, who uses both NinjaOne and Acronis Cyber Protect
- **Customer** - A client of the MSP
- **Partner tenant** - the MSP account on Acronis Cyber Cloud
- **Customer tenant** - the customer account on Acronis Cyber Cloud

Prerequisites

To use this integration, you should have:

- At least a single, fully configured NinjaOne account
- An Acronis Cyber Cloud account with:
  - at least one customer tenant and one user, setup with Acronis administration permissions
  - 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.

How the integration works

The integration between Acronis Cyber Protect Cloud and NinjaOne RMM is script-based and enables remote mass-deployment of Acronis agent on as many workloads as necessary, with minimal efforts. The scripts are downloaded from the Acronis Management portal and uploaded to and scheduled from NinjaOne RMM.

During the installation of Acronis agents, the devices will be registered with the Acronis Cloud and, if configured, a default protection plan will be applied.

Besides agent installation, the scripts allow also to automate a wide range of cybersecurity tasks.

In order for a script to run, it has to be supplied with the registration token, which will identify the Acronis customer tenant and the protection plan (if selected). For instructions on how to provide a registration token, see Generate Registration token.

Additionally, the integration provides the possibility to provision new customers from NinjaOne RMM to Acronis and configure devices' Acronis statuses for monitoring through NinjaOne custom fields. In order for the integration to get access to NinjaOne's API, a client application has to be registered. For further details, see Generate Client App ID.

Setting up the integration

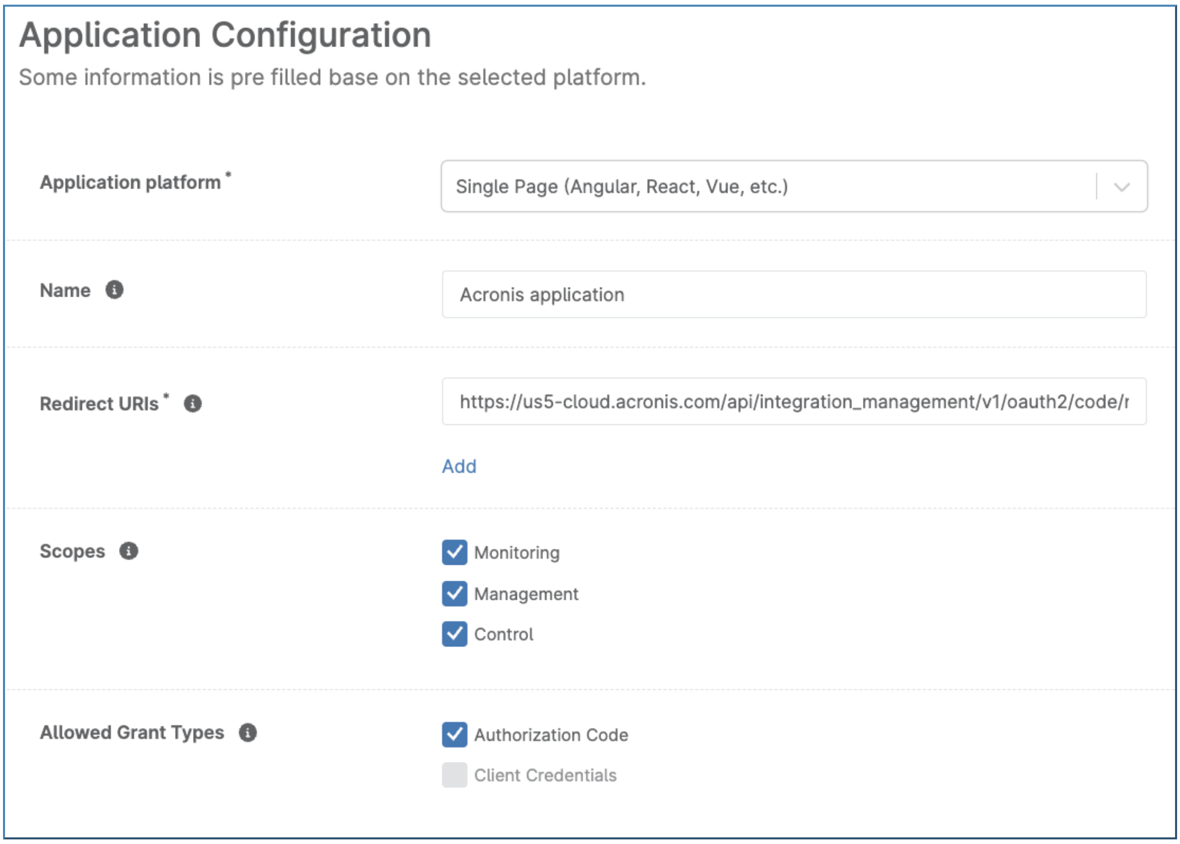
Generate Registration token

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

1. Log in to the Acronis Cyber Protection console.
2. Click **Add Device** and scroll down to **Registration token**. Then click **GENERATE**.
3. Select a token with a maximum lifetime value and click **GENERATE TOKEN**.
4. Copy the token you just generated.

Generate Client App ID

1. Log into NinjaOne.
2. Go to **Administration** > **Apps** > **API** > **Client App IDs in NinjaOne**.
3. Create a new API token with below settings:



Application Configuration

Some information is pre filled base on the selected platform.

Application platform * Single Page (Angular, React, Vue, etc.)

Name Acronis application

Redirect URIs * https://us5-cloud.acronis.com/api/integration_management/v1/oauth2/code/r

Scopes
☑ Monitoring
☑ Management
☑ Control

Allowed Grant Types
☑ Authorization Code
□ Client Credentials

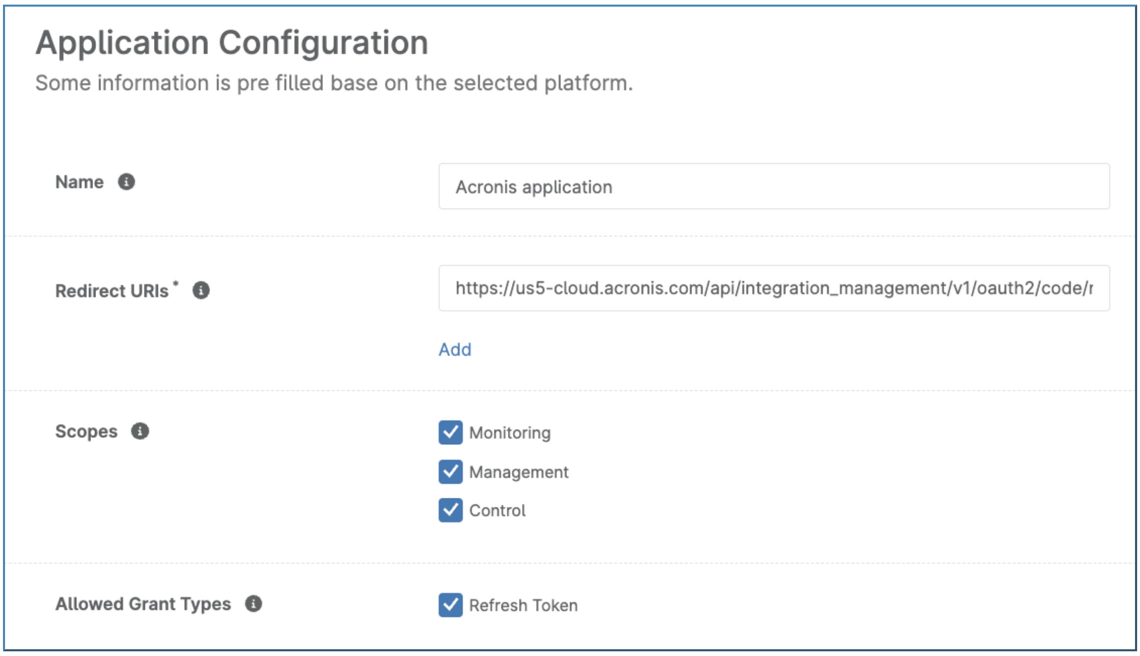
   a. **Application platform** - select **Single Page** from the drop-down
   b. **Name** - enter your label, for example: **Acronis application**
   c. **Redirect URLs** - provide the corresponding redirect address: https://<acronis_url>/api/integration_management/v1/oauth2/code/ninja, where <acronis_url> is your Acronis

Cyber Protect Cloud console URL.
Example of a valid redirect url for us5 data center: https://us5-cloud.acronis.com/api/integration_management/v1/oauth2/code/ninja

d. For **Scopes**, enable the following options:
   - **Monitoring**
   - **Management**
   - **Control**

e. For **Allowed Grant Types**, enable **Authorization Code** and save.

f. Enable **Refresh token** and 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.

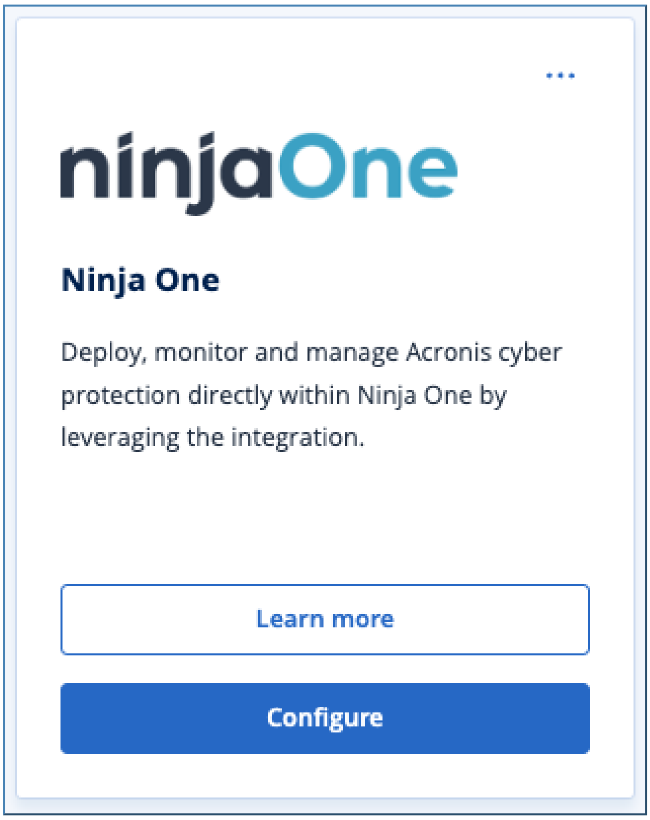
4. Copy **Client ID** for the created API token to use when configuring integration in the Acronis Cyber Protection console.

Setting up the integration in Acronis Management portal

Enable integration

To set up the Acronis integration for NinjaOne:

1. Go to the **Acronis Management portal** > **Integrations**.
2. Click **Configure** on the NinjaOne tile:

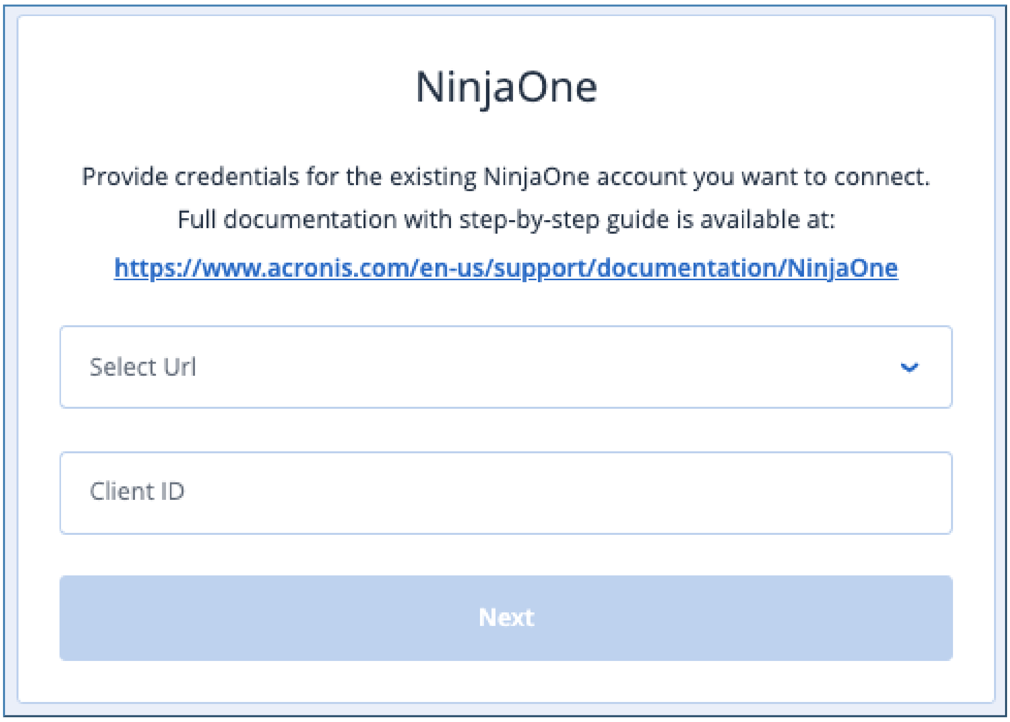


Ninja One

Deploy, monitor and manage Acronis cyber protection directly within Ninja One by leveraging the integration.

See more information about enabling and managing integrations.

3. Provide credentials to your NinjaOne account:

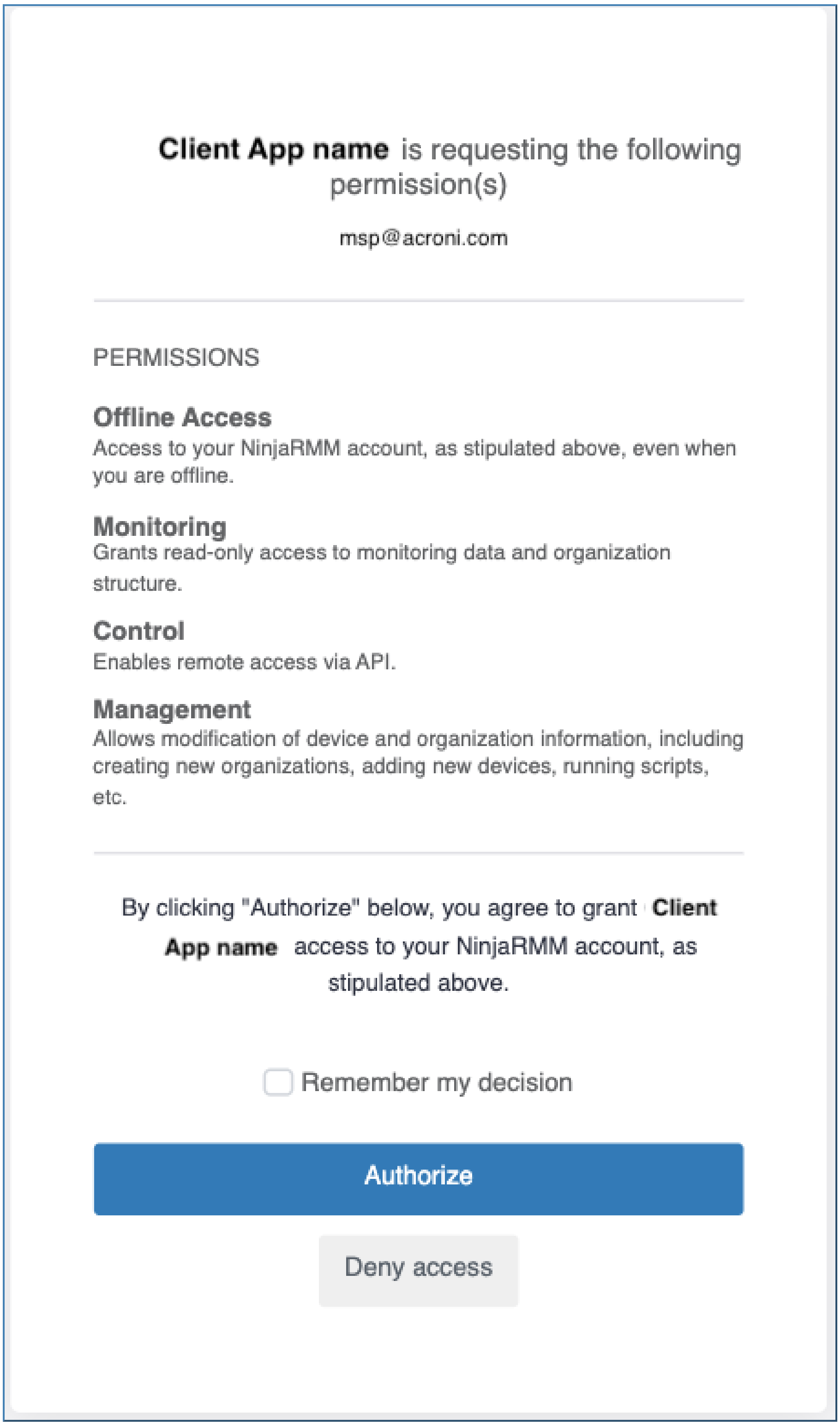


NinjaOne

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

See how to generate Client App ID in NinjaOne.

4. After having provided correct credentials, you will be prompted to authorize Acronis to get API access to NinjaOne account:



Client App name is requesting the following permission(s)

msp@acroni.com

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 **Client App name** access to your NinjaRMM account, as stipulated above.

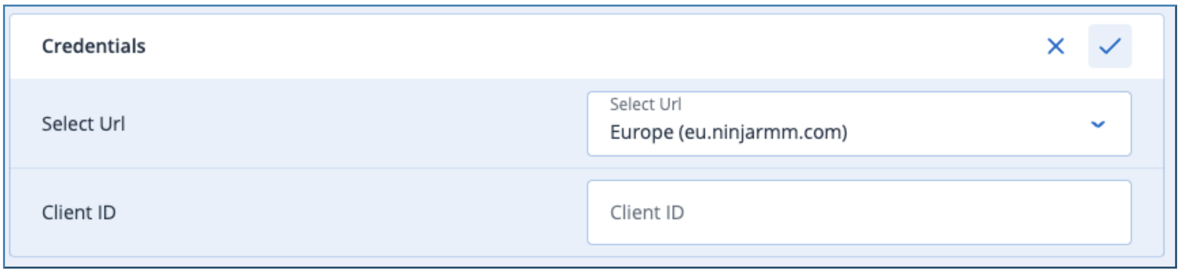
□ Remember my decision

5. Click **Authorize** to proceed.

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

Configure integration settings

1. On the **Integration settings** tab, you can update **Credentials**.



Credentials

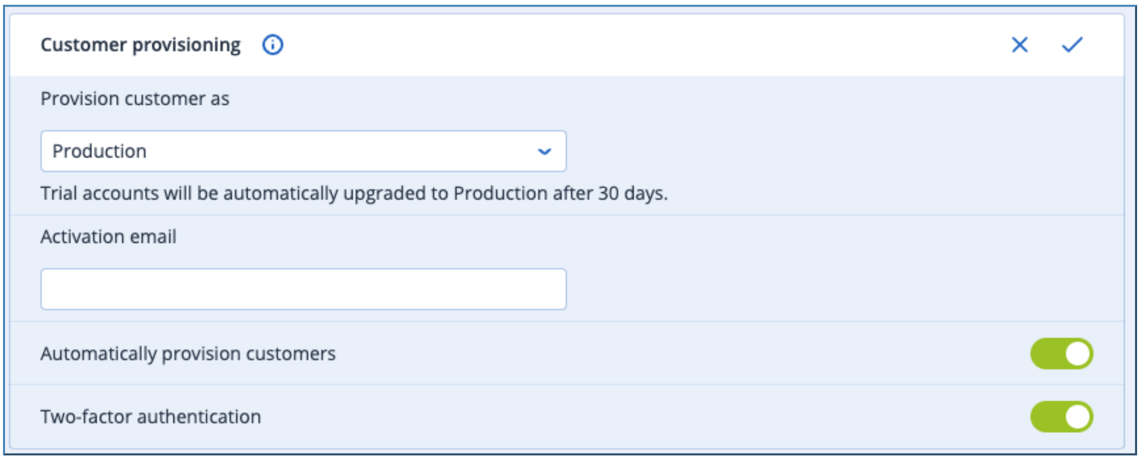
Select Url — Europe (eu.ninjarmm.com)

Client ID — Client ID

2. In the **Customer provisioning** section, configure the parameters required to create new customers in Acronis Cyber Protect Cloud:
   a. In the **Provision customer as** drop-down, select the mode of customer creation - **Production** or **Trial**.
   b. Provide **Activation email** - the address of the administrator user, which will be created for the new customer, where the user activation link will be sent.
   c. Switch the **Automatically provision customers** toggle button to enable or disable all customers newly registered in NinjaOne to be automatically created in Acronis Cyber Protect Cloud.

   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.

   d. Switch the **Two-factor authentication** toggle button to enable or disable the corresponding option for new customers.



Customer provisioning

Provision customer as — Production

Trial accounts will be automatically upgraded to Production after 30 days.

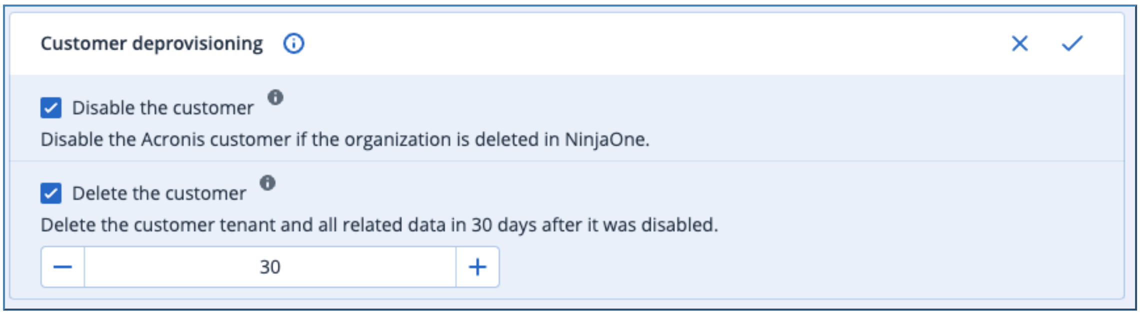
Activation email

Automatically provision customers — on

Two-factor authentication — on

3. In **Customer deprovisioning**, set the following options:
   a. Select the **Disable the customer** checkbox to disable the Acronis customer if the organization is deleted in NinjaOne.

   b. Mark the **Delete the customer** checkbox to delete the customer tenant and all related data in the specified number of days after it was disabled.



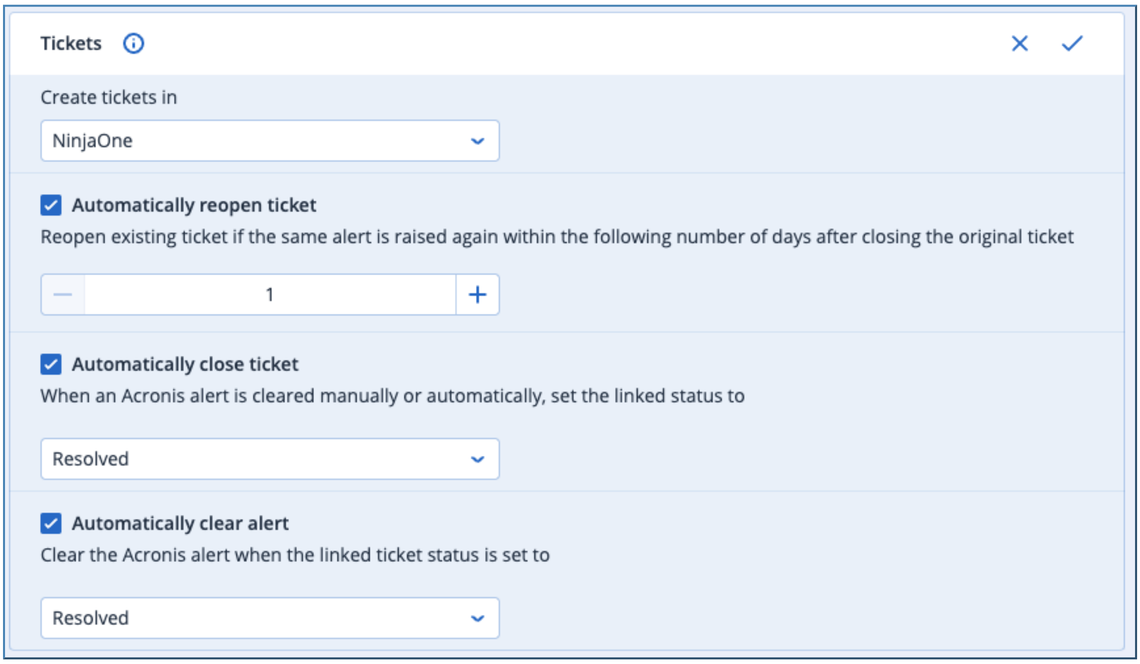
Customer deprovisioning

☑ Disable the customer
Disable the Acronis customer if the organization is deleted in NinjaOne.

☑ Delete the customer
Delete the customer tenant and all related data in 30 days after it was disabled.

— 30 +

4. In the **Tickets** section:
   a. From the **Create tickets in** drop-down list, select the ticketing system to enable automatic tickets creation based on Acronis alerts: **NinjaOne**, **Advanced Automation** (available if the corresponding service is activated) or disable the ticketing creation option.
   b. Enable the **Automatically reopen ticket** option to reopen existing tickets if the same alert is raised again within the specified number of days after closing the original ticket.
   c. Enable the **Automatically close ticket** option, so that when an Acronis alert is cleared either manually or automatically, the linked status will be set to the value, selected from the drop-down list.
   d. Enable the **Automatically clear alert** option to clear Acronis alerts when the linked ticket status is set to the value, selected from the drop-down list.



Tickets

Create tickets in
NinjaOne

☑ Automatically reopen ticket
Reopen existing ticket if the same alert is raised again within the following number of days after closing the original ticket

— 1 +

☑ Automatically close ticket
When an Acronis alert is cleared manually or automatically, set the linked status to
Resolved

☑ Automatically clear alert
Clear the Acronis alert when the linked ticket status is set to
Resolved

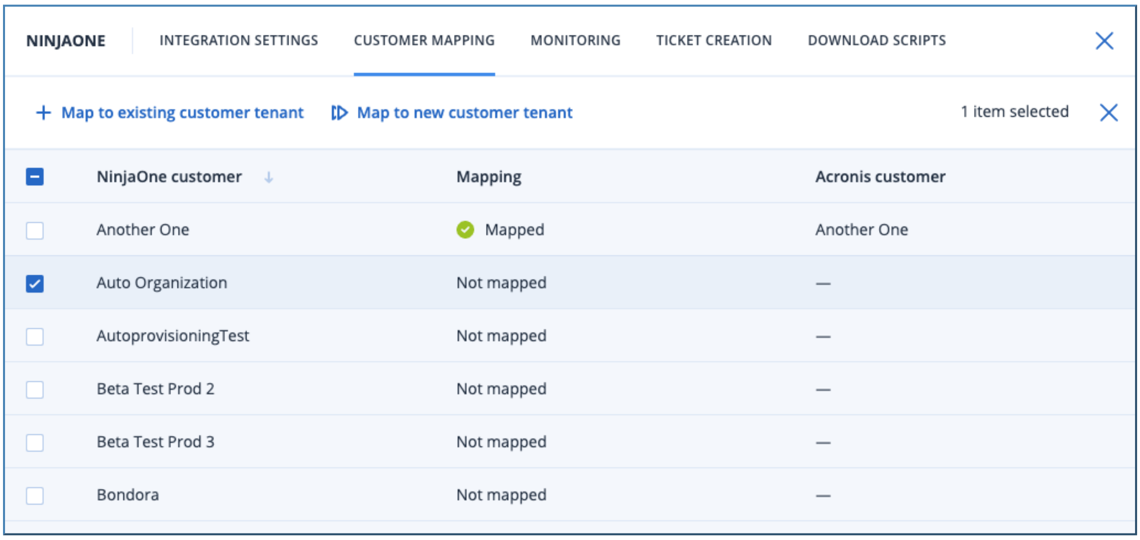
Apply customer mapping

Mapping NinjaOne organizations to Acronis customer tenants is necessary for the integration to link those entities and to be able to perform automatic synchronization of monitoring statuses and alerts.

Important

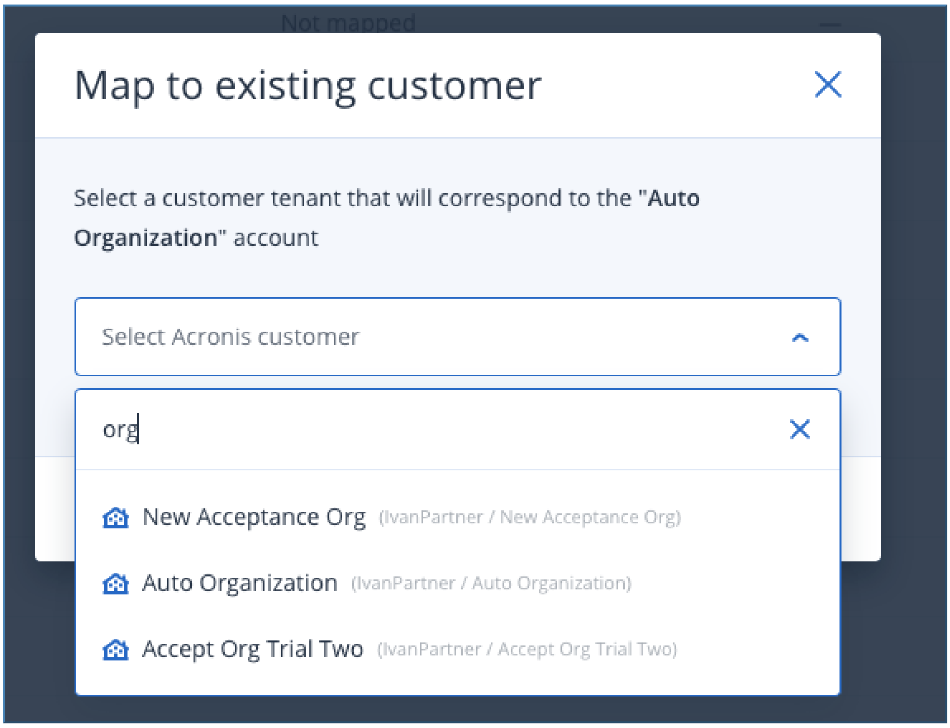
Make sure to map already existing customer tenants (registered in Acronis Cyber Protect Cloud) before enabling automatic customer provisioning in order to avoid customer tenant duplication.

1. Go to the **Customer mapping** tab.
2. Using customer mapping, you can manually provision RMM customers to Acronis or map them to existing customers:
   a. Select NinjaOne customer from the list and click **Map to existing customer tenant**.



☐	NinjaOne customer ↓	Mapping	Acronis customer
☐	Another One	✓ Mapped	Another One
☑	Auto Organization	Not mapped	—
☐	AutoprovisioningTest	Not mapped	—
☐	Beta Test Prod 2	Not mapped	—
☐	Beta Test Prod 3	Not mapped	—
☐	Bondora	Not mapped	—

b. Select Acronis customer and save.



Not mapped

Map to existing customer

Select a customer tenant that will correspond to the "**Auto Organization**" account

Select Acronis customer
org
New Acceptance Org (IvanPartner / New Acceptance Org)
Auto Organization (IvanPartner / Auto Organization)
Accept Org Trial Two (IvanPartner / Accept Org Trial Two)

c. Select NinjaOne customer(s) and click **Map to new customer tenant** to create the corresponding new customer in Acronis and map them.

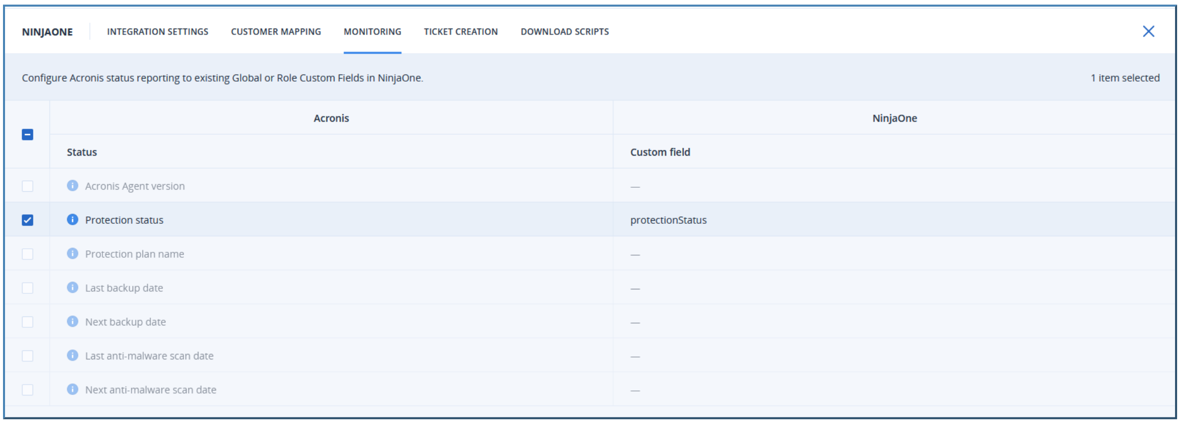
As a result, a new customer will be created in Acronis, based on the parameters, defined in Integration settings in **Customer provisioning** section.

Configure monitoring

As long as the integration has been enabled and customer mapping is done already, you can proceed with mapping Acronis statuses to NinjaOne custom fields.

To do that:

1. Go to **Acronis Management portal** > **Integrations** > **NinjaOne** > **Configure** > **Monitoring** tab.
2. Here you can see an up-to-date list of monitoring statuses and existing custom fields of Role or Global type in the NinjaOne account. Select statuses that have to be monitored in NinjaOne.



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

1 item selected

	Acronis	NinjaOne
☐	Status	Custom field
☐	Acronis Agent version	—
☑	Protection status	protectionStatus
☐	Protection plan name	—
☐	Last backup date	—
☐	Next backup date	—
☐	Last anti-malware scan date	—
☐	Next anti-malware scan date	—

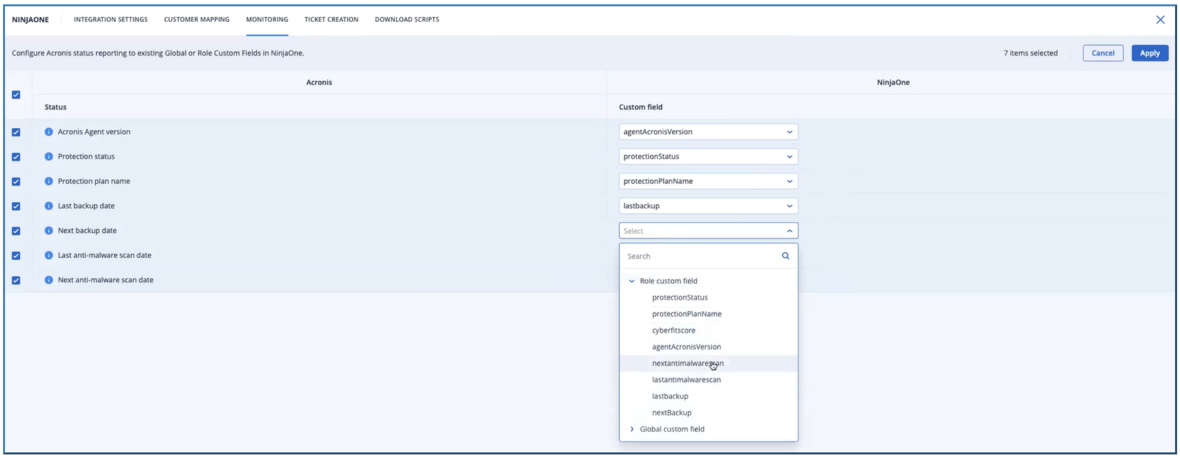
.

3. Map statuses of your choice to custom fields in NinjaOne by selecting a value from the drop-down list in the **Custom field** column.

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 types, applicable for the selected status:

- **Text** for Statuses: "Acronis Agent version", "Protection status", "Protection plan name"
- **Date/Time** for Statuses: "Last backup date", "Next backup date", "Last anti-malware scan date", "Next anti-malware scan date"



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

7 items selected

	Acronis	NinjaOne
☑	Status	Custom field
☑	Acronis Agent version	agentAcronisVersion
☑	Protection status	protectionStatus
☑	Protection plan name	protectionPlanName
☑	Last backup date	lastbackup
☑	Next backup date	Select
☑	Last anti-malware scan date	
☑	Next anti-malware scan date	

See more information about managing custom fields in NinjaOne.

4. Click **Apply** to keep these changes.
5. If mapping was successful, you will see such notification in the lower right corner.

As a result, for every mapped workload under each mapped customer tenant in NinjaOne, the respective statuses will be updated to the selected custom fields.

To create new custom fields:

1. Go to **NinjaOne** > **Administration** > **Devices** > **Role Custom Fields**/**Global Custom Fields**.
2. Select either **Role** or **Global** custom field.
3. Create one or more new custom fields of your own.

See also View device status.

Configure ticketing

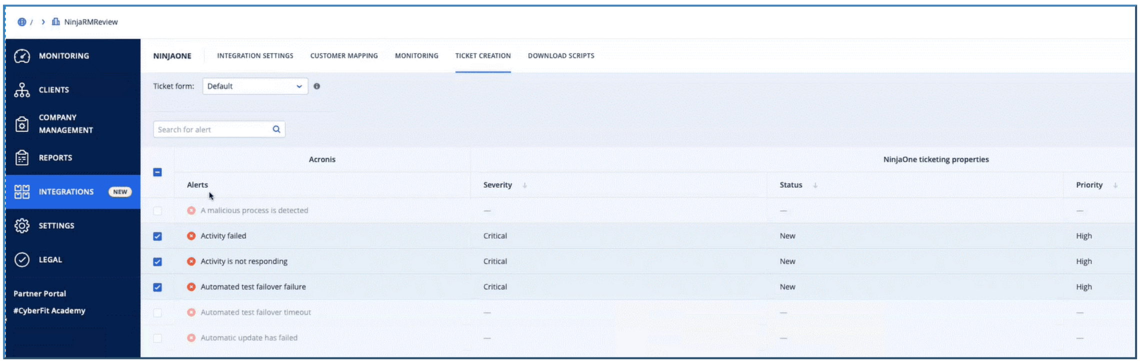
Ticket creation is a functionality that configures which alerts, raised in Acronis, to have corresponding tickets, created in NinjaOne. All standard Acronis alerts can be synced except for the ones, configured in the Monitoring plans of the Advanced Management pack.

Ticket synchronization

Ticket synchronization translates Acronis Cyber Cloud alerts into NinjaOne tickets. Alerts are synced with created tickets in both directions every 10-15 mins for all mapped customers. You can select alert types, configure creating and auto-closing rules, as well as assign priority, status and other ticket parameters.

Ticketing creation configuration

1. Go to the **Ticket creation** tab and enable the feature if it was not before (it can also be enabled from Integration settings).
2. Select the **Ticket form** from the drop-down list of available values. Forms are defined in NinjaOne and only those without obligatory fields can be selected for automatic ticket creation.
3. Select alert types, which have to be synced as tickets to NinjaOne.
4. For each alert type, define the parameters to be used for ticket creation in NinjaOne:
   a. Severity
   b. Status
   c. Priority



Ticket form: Default

	Acronis	NinjaOne ticketing properties		
☐	Alerts	Severity	Status	Priority
☐	A malicious process is detected	—	—	—
☑	Activity failed	Critical	New	High
☑	Activity is not responding	Critical	New	High
☑	Automated test failover failure	Critical	New	High
☐	Automated test failover timeout	—	—	—
☐	Automatic update has failed	—	—	—

5. Click **Apply** to keep these settings.

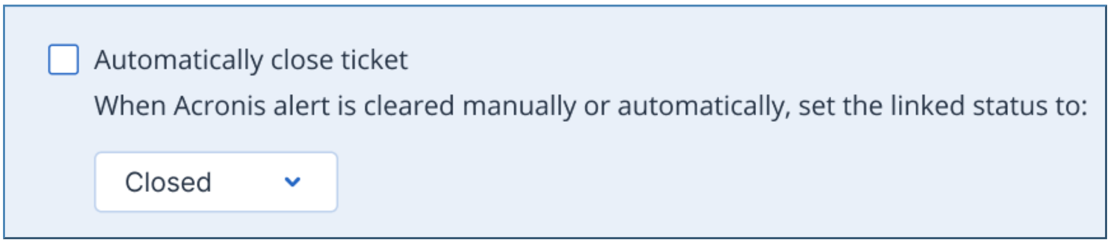
After the ticketing feature is enabled, the required alert types are selected and ticketing parameters for them are configured. Tickets will be automatically created and synced for all mapped customers.

Resolving tickets in NinjaOne

In this scenario, the integration can resolve a linked ticket in NinjaOne when the originating Acronis alert has been already cleared.

By default, this option is disabled. To turn it on:

1. Go to the **Integration settings** tab.
2. Locate the **Tickets** section and open it for editing.
3. Enable the **Automatically resolve ticket** option.
4. Use the **Status** drop-down list to select the desired value for setting the ticket to resolved state.



□ Automatically close ticket

When Acronis alert is cleared manually or automatically, set the linked status to:

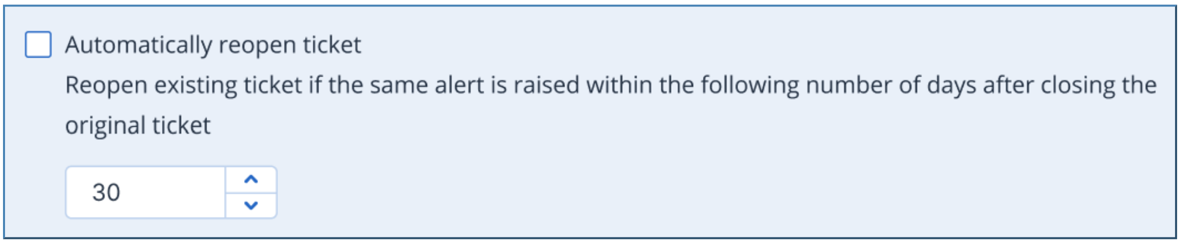
Closed

Reopening tickets in NinjaOne

In this scenario, the integration can reopen an already resolved ticket within a specified period of time after the resolution.

By default, this option is disabled. To turn it on:

1. Go to the **Integration settings** tab.
2. Locate the **Tickets** section and open it for editing.
3. Enable the **Automatically reopen ticket** option.
4. In the **Days** numeric field, set maximum number of days that should have passed after closing the ticket and before the integration creates a new one.



□ Automatically reopen ticket

Reopen existing ticket if the same alert is raised within the following number of days after closing the original ticket

30

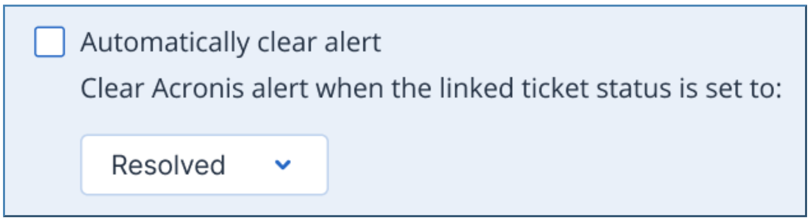
In this case, the integration will not create a new ticket for the alert, but rather reopen the closed one. If the number of days passed since the original ticket has been resolved are more than the number configured in the option above, then a new ticket will be created.

Clearing alerts in Acronis

In this scenario, the integration can clear an originating Acronis alert by detecting if linked NinjaOne ticket has been resolved.

By default, this option is disabled. To turn it on:

1. Go to the **Integration settings** tab.
2. Locate the **Tickets** section and open it for editing.
3. Enable the **Automatically clear alert** option.
4. Use the **Status** drop-down list to select a value for the ticket status to clear the Acronis alert.



□ Automatically clear alert

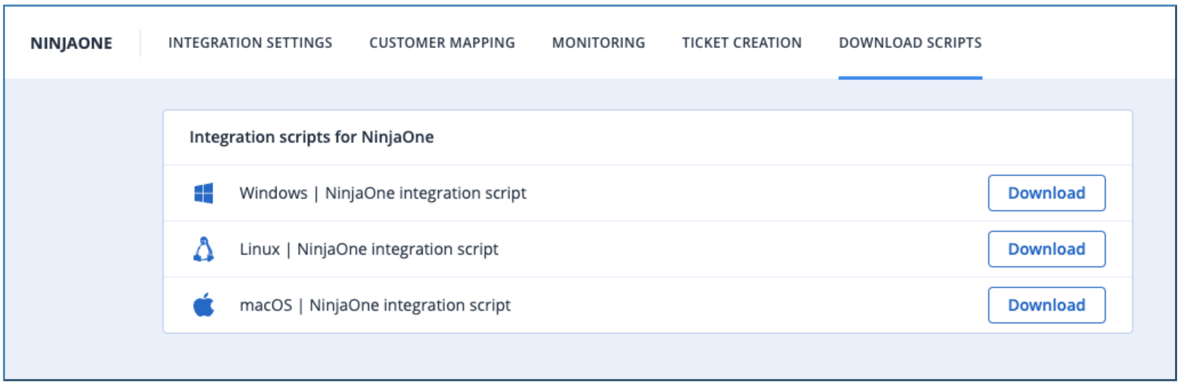
Clear Acronis alert when the linked ticket status is set to:

Resolved

In this case, the integration will clear the originating Acronis alert.

Download scripts

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



Integration scripts for NinjaOne

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

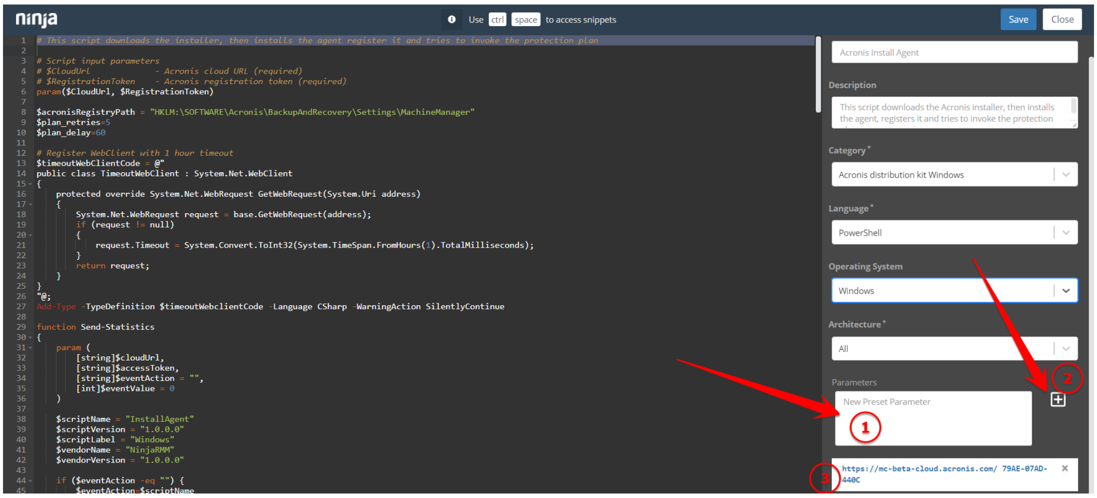
These packages are required in order to proceed with the setup in NinjaOne.

Setting up the integration in NinjaOne

1. Go to **NinjaOne** > **Administration** > **Library** > **Scripting**.
2. Locate the scripts downloaded from Acronis and upload individually the ones of your choice.

> **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, just import the scripts from the NinjaOne interface, the way they have been downloaded from the Acronis console or drag and drop the files.

3. Next:
   a. Give a proper name (similar to the script's file name)
   b. Enter a description
   c. Assign to a category
   d. Select the language of the imported script (PowerShell for Windows and ShellScript for Linux)
   e. Select an operating system
   f. Select architecture (**All** is recommended)
   g. For each of the following scripts:
      i. **Acronis_install_agent**: in the **New Preset Parameter** field, add a parameter by entering the currently used Acronis Datacenter URL, followed by a blank space and Acronis registration token (see more details). Click on the **+** button to create a parameter. The newly created parameter should resemble the following example: "https://mc-beta-cloud.acronis.com 79AE-07AD-440C"



```
# This script downloads the installer, then installs the agent register it and tries to invoke the protection plan

# Script input parameters
# $CloudUrl              - Acronis cloud URL (required)
# $RegistrationToken     - Acronis registration token (required)
param($CloudUrl, $RegistrationToken)

$acronisRegistryPath = "HKLM:\SOFTWARE\Acronis\BackupAndRecovery\Settings\MachineManager"
$plan_retries=5
$plan_delay=60

# Register WebClient with 1 hour timeout
$timeoutWebClientCode = @"
public class TimeoutWebClient : System.Net.WebClient
{
    protected override System.Net.WebRequest GetWebRequest(System.Uri address)
    {
        System.Net.WebRequest request = base.GetWebRequest(address);
        if (request != null)
        {
            request.Timeout = System.Convert.ToInt32(System.TimeSpan.FromHours(1).TotalMilliseconds);
        }
        return request;
    }
}
"@;
Add-Type -TypeDefinition $timeoutWebclientCode -Language CSharp -WarningAction SilentlyContinue

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

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

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

Acronis Install Agent

Description: This script downloads the Acronis installer, then installs the agent, registers it and tries to invoke the protection

Category *: Acronis distribution kit Windows

Language *: PowerShell

Operating System: Windows

Architecture *: All

Parameters: New Preset Parameter

https://mc-beta-cloud.acronis.com/ 79AE-07AD-440C

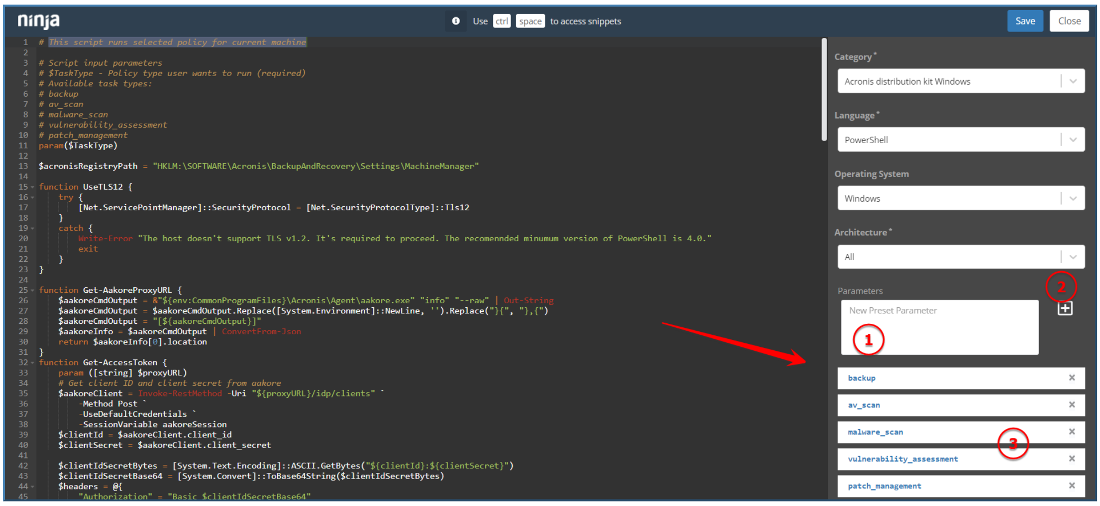
Click **Save**, then **Close**.

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.

ii. **Acronis_scans**: add the following 5 individual parameters:

- backup
- av_scan
- malware_scan
- vulnerability_assessment
- patch_management



```
# 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 UseTLS12 {
    try {
        [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
    }
    catch {
        Write-Error "The host doesn't support TLS v1.2. It's required to proceed. The recomennded minumum version of PowerShell is 4.0."
        exit
    }
}

function Get-AakoreProxyURL {
    $aakoreCmdOutput = &"${env:CommonProgramFiles}\Acronis\Agent\aakore.exe" "info" "--raw" | Out-String
    $aakoreCmdOutput = $aakoreCmdOutput.Replace([System.Environment]::NewLine, '').Replace("}{", "},{")
    $aakoreCmdOutput = "[${aakoreCmdOutput}]"
    $aakoreInfo = $aakoreCmdOutput | ConvertFrom-Json
    return $aakoreInfo[0].location
}
function Get-AccessToken {
    param ([string] $proxyURL)
    # Get client ID and client secret from aakore
    $aakoreClient = Invoke-RestMethod -Uri "${proxyURL}/idp/clients" `
        -Method Post `
        -UseDefaultCredentials `
        -SessionVariable aakoreSession
    $clientId = $aakoreClient.client_id
    $clientSecret = $aakoreClient.client_secret

    $clientIdSecretBytes = [System.Text.Encoding]::ASCII.GetBytes("${clientId}:${clientSecret}")
    $clientIdSecretBase64 = [System.Convert]::ToBase64String($clientIdSecretBytes)
    $headers = @{
        "Authorization" = "Basic $clientIdSecretBase64"
```

Category*

Acronis distribution kit Windows

Language*

PowerShell

Operating System

Windows

Architecture*

All

Parameters

New Preset Parameter

backup ×

av_scan ×

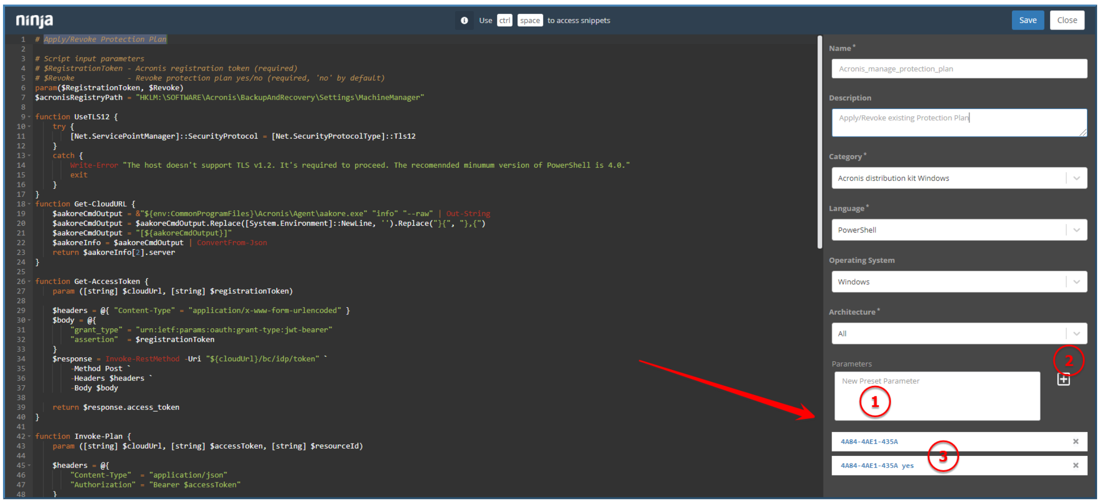
malware_scan ×

vulnerability_assessment ×

patch_management ×

iii. **Acronis_manage_protection_plan**: add the following 2 separate parameters:

- Acronis registration token (see more details)
- Acronis registration token, followed by a blank space and "**yes**"



```
# Apply/Revoke Protection Plan

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

function UseTLS12 {
    try {
        [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
    }
    catch {
        Write-Error "The host doesn't support TLS v1.2. It's required to proceed. The recomennded minumum version of PowerShell is 4.0."
        exit
    }
}
function Get-CloudURL {
    $aakoreCmdOutput = &"${env:CommonProgramFiles}\Acronis\Agent\aakore.exe" "info" "--raw" | Out-String
    $aakoreCmdOutput = $aakoreCmdOutput.Replace([System.Environment]::NewLine, '').Replace("}{", "},{")
    $aakoreCmdOutput = "[${aakoreCmdOutput}]"
    $aakoreInfo = $aakoreCmdOutput | ConvertFrom-Json
    return $aakoreInfo[2].server
}

function Get-AccessToken {
    param ([string] $cloudUrl, [string] $registrationToken)

    $headers = @{ "Content-Type" = "application/x-www-form-urlencoded" }
    $body = @{
        "grant_type" = "urn:ietf:params:oauth:grant-type:jwt-bearer"
        "assertion"  = $registrationToken
    }
    $response = Invoke-RestMethod -Uri "${cloudUrl}/bc/idp/token" `
        -Method Post `
        -Headers $headers `
        -Body $body

    return $response.access_token
}

function Invoke-Plan {
    param ([string] $cloudUrl, [string] $accessToken, [string] $resourceId)

    $headers = @{
        "Content-Type"  = "application/json"
        "Authorization" = "Bearer $accessToken"
    }
```

Name *: Acronis_manage_protection_plan

Description: Apply/Revoke existing Protection Plan

Category *: Acronis distribution kit Windows

Language *: PowerShell

Operating System: Windows

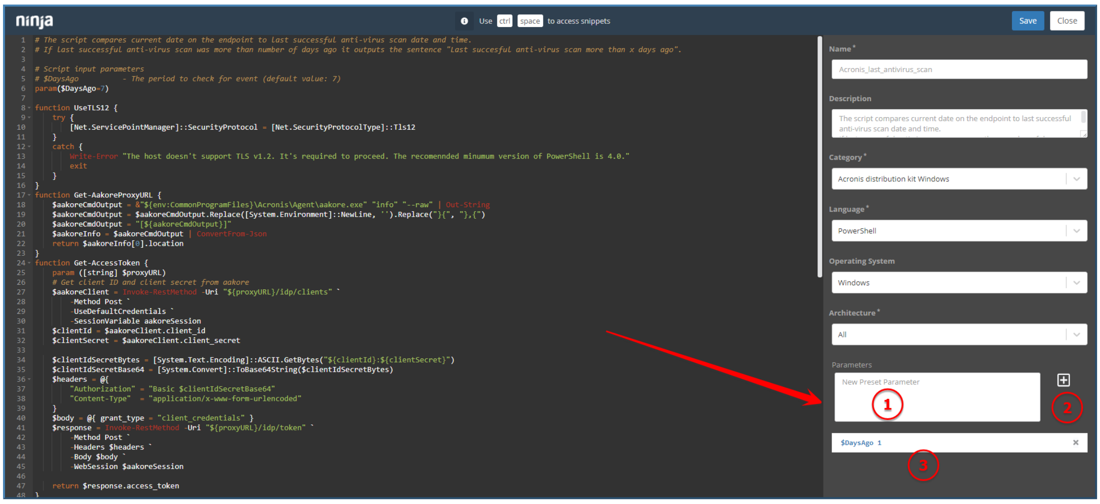
Architecture *: All

Parameters: New Preset Parameter

4A84-4AE1-435A ×

4A84-4AE1-435A yes ×

iv. **Acronis_last_antivirus_scan** (Windows): add the $DaysAgo parameter, followed by a blank space and a number (the period to check for event - default value: 7)



```
# The script compares current date on the endpoint to last successful anti-virus scan date and time.
# If last successful anti-virus scan was more than number of days ago it outputs the sentence "Last succesful anti-virus scan more than x days ago".

# Script input parameters
# $DaysAgo          - The period to check for event (default value: 7)
param($DaysAgo=7)

function UseTLS12 {
    try {
        [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
    }
    catch {
        Write-Error "The host doesn't support TLS v1.2. It's required to proceed. The recomennded minumum version of PowerShell is 4.0."
        exit
    }
}
function Get-AakoreProxyURL {
    $aakoreCmdOutput = &"${env:CommonProgramFiles}\Acronis\Agent\aakore.exe" "info" "--raw" | Out-String
    $aakoreCmdOutput = $aakoreCmdOutput.Replace([System.Environment]::NewLine, '').Replace("}{", "},{")
    $aakoreCmdOutput = "[${aakoreCmdOutput}]"
    $aakoreInfo = $aakoreCmdOutput | ConvertFrom-Json
    return $aakoreInfo[0].location
}
function Get-AccessToken {
    param ([string] $proxyURL)
    # Get client ID and client secret from aakore
    $aakoreClient = Invoke-RestMethod -Uri "${proxyURL}/idp/clients" `
        -Method Post `
        -UseDefaultCredentials `
        -SessionVariable aakoreSession
    $clientId = $aakoreClient.client_id
    $clientSecret = $aakoreClient.client_secret

    $clientIdSecretBytes = [System.Text.Encoding]::ASCII.GetBytes("${clientId}:${clientSecret}")
    $clientIdSecretBase64 = [System.Convert]::ToBase64String($clientIdSecretBytes)
    $headers = @{
        "Authorization" = "Basic $clientIdSecretBase64"
        "Content-Type"  = "application/x-www-form-urlencoded"
    }
    $body = @{ grant_type = "client_credentials" }
    $response = Invoke-RestMethod -Uri "${proxyURL}/idp/token" `
        -Method Post `
        -Headers $headers `
        -Body $body `
        -WebSession $aakoreSession

    return $response.access_token
}
```

Name *
Acronis_last_antivirus_scan

Description
The script compares current date on the endpoint to last successful anti-virus scan date and time.

Category *
Acronis distribution kit Windows

Language *
PowerShell

Operating System
Windows

Architecture *
All

Parameters
New Preset Parameter

$DaysAgo 1

v. **Acronis_last_malware_scan** (Windows & macOS): add the $DaysAgo parameter, followed by a blank space and a number (the period to check for event - default value: 7)

vi. The rest of the scripts do not require any preset parameters.

Note

The NinjaOneScriptsWindows.zip file contains a total of 10 scripts, NinjaOneScriptsLinux.zip - 6 scripts and NinjaOneScriptsMacOS.zip - 8.

Customer provisioning and deprovisioning

Before proceeding with the provisioning and deprovisioning of Acronis customer tenants for new organizations in NinjaOne, make sure that the integration is enabled. Then you can set up the following options:

- When a new organization is added to NinjaOne, a corresponding Acronis customer tenant is automatically created and linked.
- When an organization is removed from NinjaOne, the linked Acronis customer tenant is first disabled and then after a configurable number of days, deleted.

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.

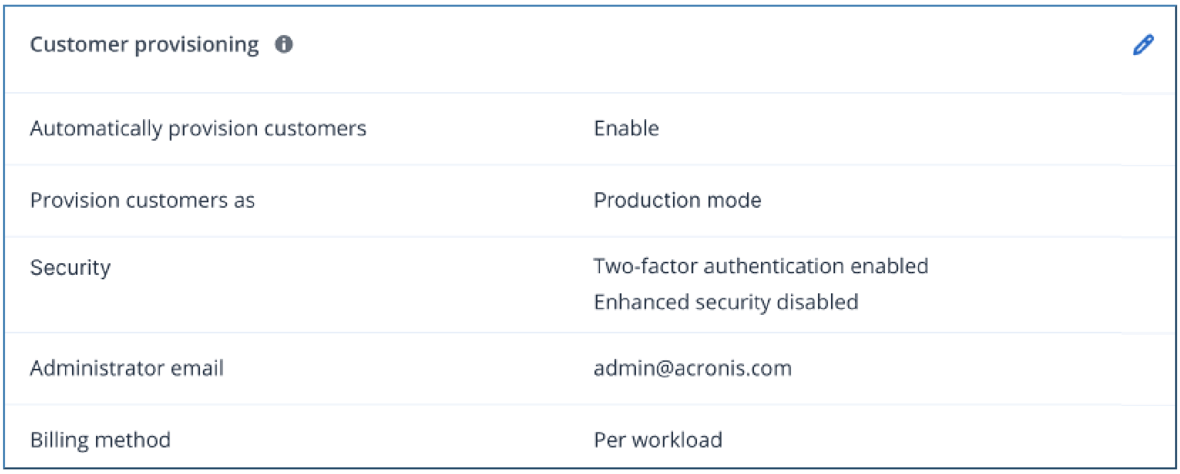
Manual provisioning of Acronis customer tenants

Go to **Customer mapping** tab, see how to apply customer mapping.

Automatic provisioning of Acronis customer tenants

These settings are used to create customers and accounts in the Acronis Management portal.

1. Go to **Acronis Management portal** > **Integrations** > **NinjaOne** tile > **Setting** > **Integration Settings** tab.
2. Scroll down to the **Customer provisioning** section and open it for editing:



Customer provisioning

Automatically provision customers	Enable
Provision customers as	Production mode
Security	Two-factor authentication enabled Enhanced security disabled
Administrator email	admin@acronis.com
Billing method	Per workload

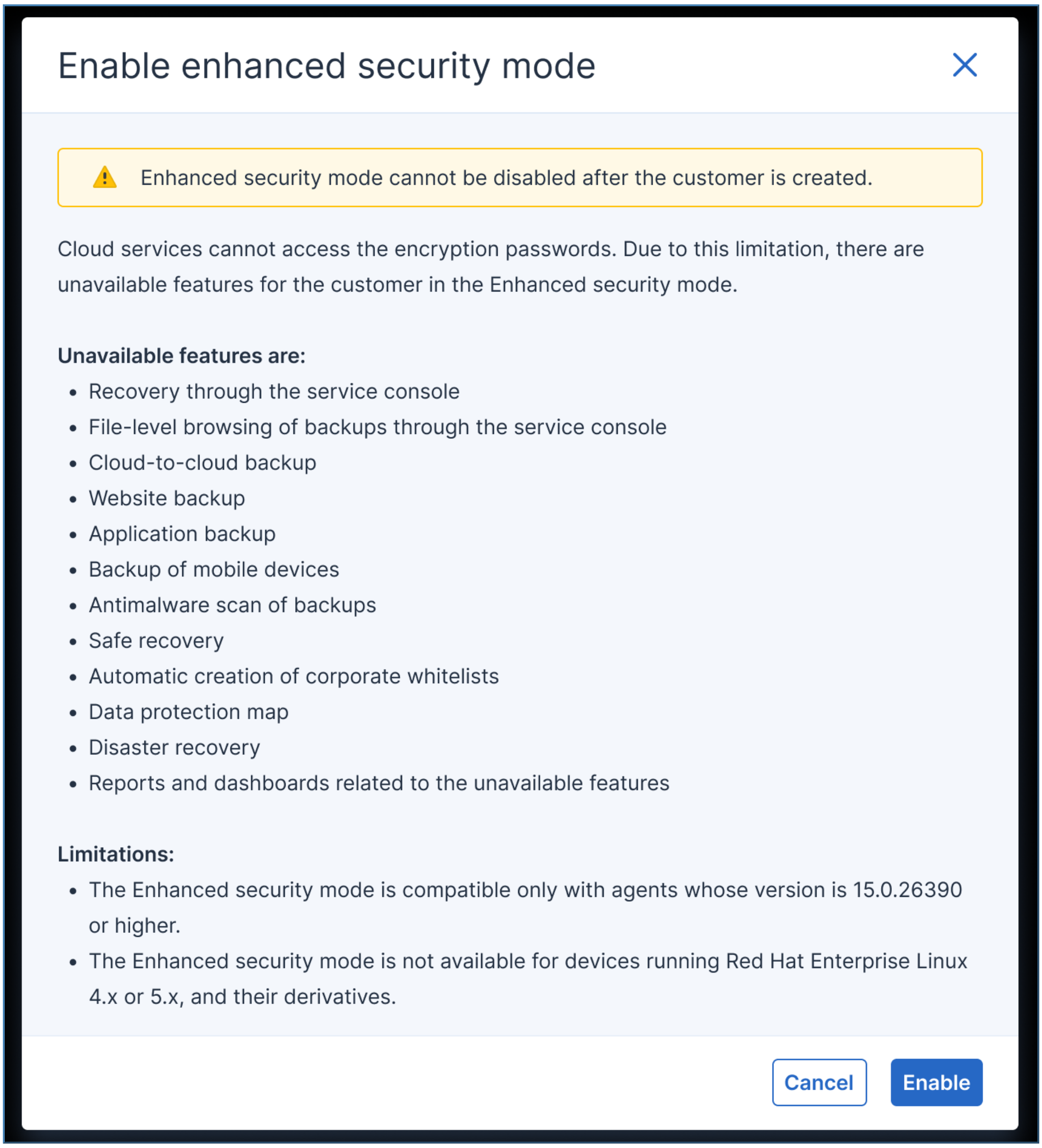
   a. Select the **Automatically provision customers** checkbox to enable the automatic creation of Acronis customers for new organizations in NinjaOne.

   b. For **Provision customers as**, select the mode, in which the tenant will use the services: **Trial** or **Production** (default).

c. In the **Security** section:

   i. Use the **Two-factor authentication** checkbox to enable or disable 2FA (it is originally turned on).

   ii. Click the **Advanced security settings** link to display the **Enable enhanced security mode** window:



Enable enhanced security mode

⚠ Enhanced security mode cannot be disabled after the customer is created.

Cloud services cannot access the encryption passwords. Due to this limitation, there are unavailable features for the customer in the Enhanced security mode.

Unavailable features are:

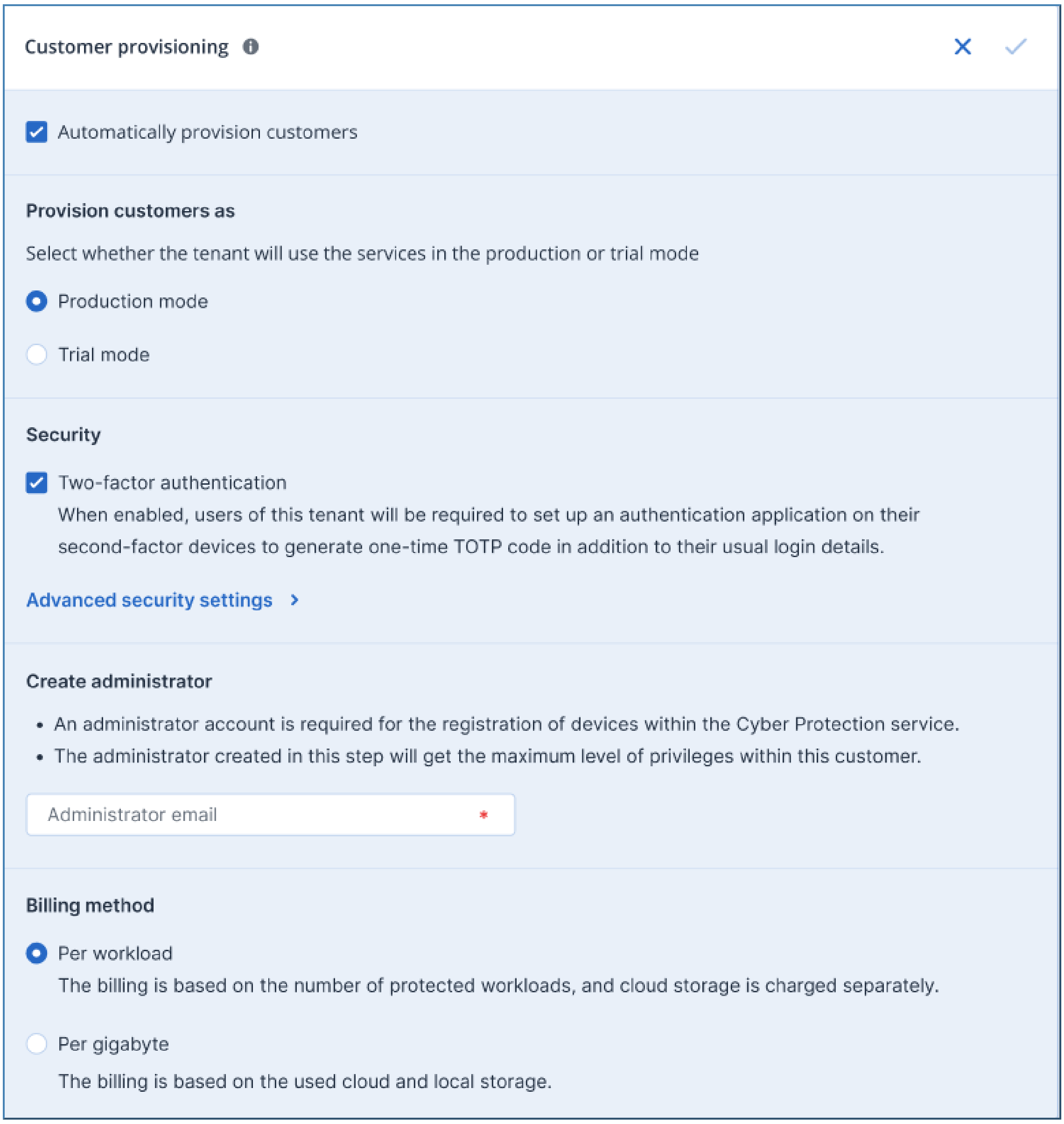
- Recovery through the service console
- File-level browsing of backups through the service console
- Cloud-to-cloud backup
- Website backup
- Application backup
- Backup of mobile devices
- Antimalware scan of backups
- Safe recovery
- Automatic creation of corporate whitelists
- Data protection map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

Limitations:

- The Enhanced security mode is compatible only with agents whose version is 15.0.26390 or higher.
- The Enhanced security mode is not available for devices running Red Hat Enterprise Linux 4.x or 5.x, and their derivatives.

Review carefully the information available, then click either **Enable** or **Cancel**.

d. In the **Create administrator** field, provide a valid email address of a user account:



Customer provisioning

☑ Automatically provision customers

Provision customers as

Select whether the tenant will use the services in the production or trial mode

● Production mode

○ Trial mode

Security

☑ Two-factor authentication

When enabled, users of this tenant will be required to set up an authentication application on their second-factor devices to generate one-time TOTP code in addition to their usual login details.

Advanced security settings >

Create administrator

- An administrator account is required for the registration of devices within the Cyber Protection service.
- The administrator created in this step will get the maximum level of privileges within this customer.

Administrator email *

Billing method

● Per workload

The billing is based on the number of protected workloads, and cloud storage is charged separately.

○ Per gigabyte

The billing is based on the used cloud and local storage.

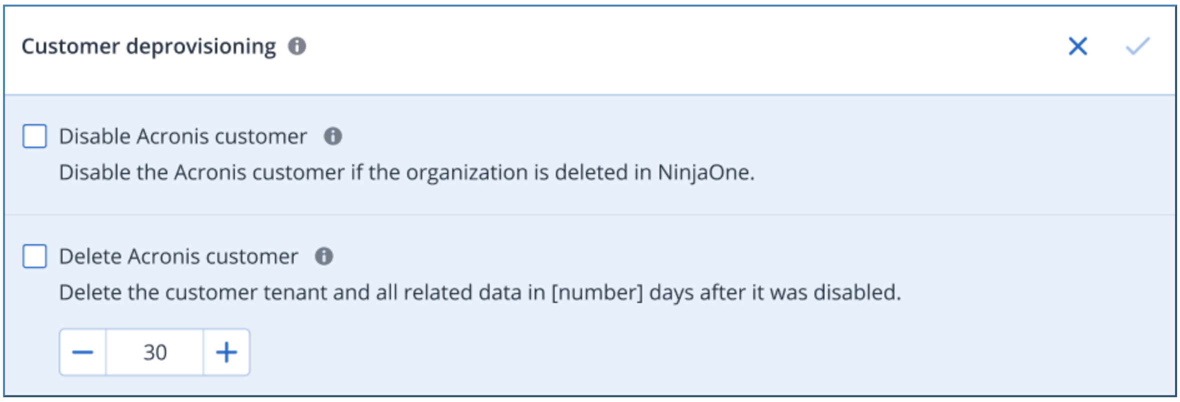
e. For **Billing method**, select one of the two possible options: **Per workload** (default) or **Per gigabyte**.

3. Click **Save**.

Automatic deprovisioning of Acronis customer tenants

These settings are used to disable and delete customers and accounts in the Acronis Management protal.

1. Go to **Acronis Management portal** > **Integrations** > **NinjaOne** tile > **Setting** > **Integration Settings** tab.
2. Scroll down to the **Customer deprovisioning** section and open it for editing:



Customer deprovisioning

□ Disable Acronis customer

Disable the Acronis customer if the organization is deleted in NinjaOne.

□ Delete Acronis customer

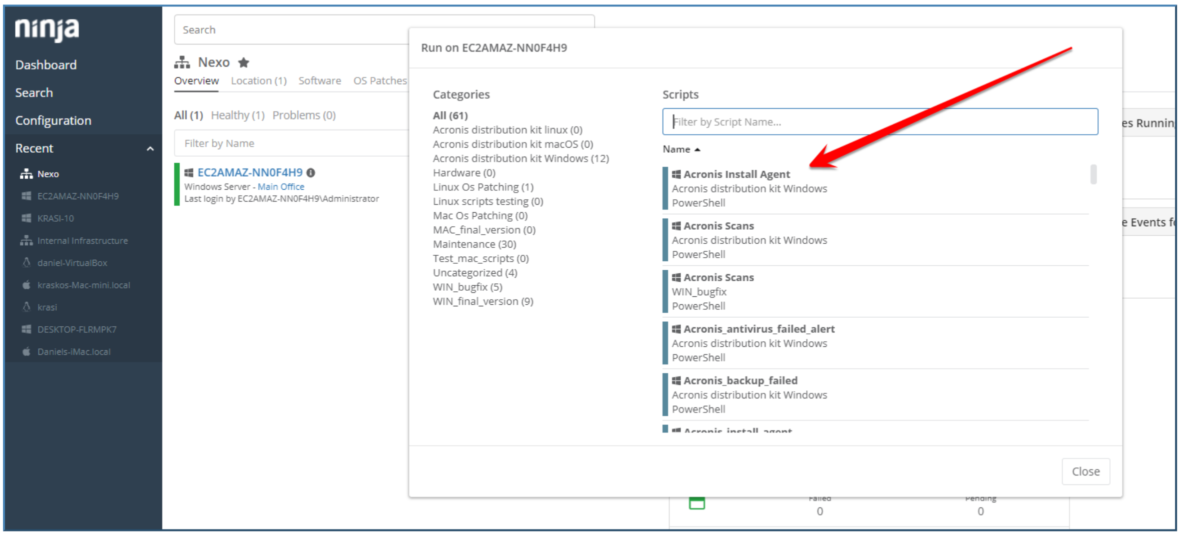
Delete the customer tenant and all related data in [number] days after it was disabled.

− 30 +

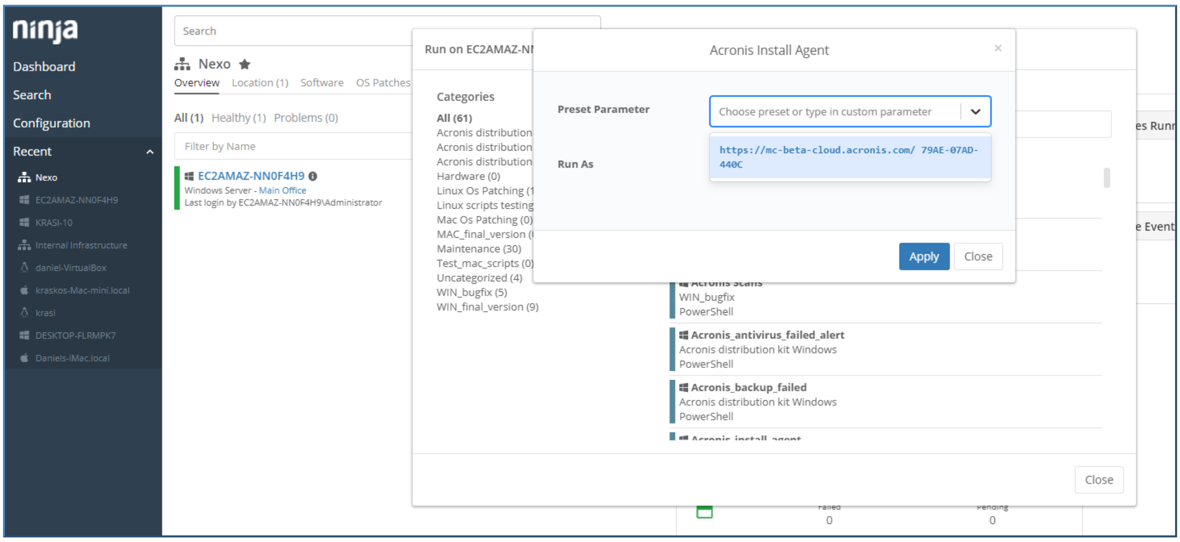
   a. Select the **Disable Acronis customer** checkbox, to automatically deactivate Acronis customers for which organizations have been already deleted in NinjaOne.
   b. Select the **Delete Acronis customer** checkbox (possible only if you have marked the previous option in step a). Then in the numeric field below, specify number of days, after which the Acronis customer tenant and all related data will be permanently erased (after it was disabled because of organization deletion in NinjaOne). If you enter "0" days, this will delete the customer immediately after RMM deletion.
      To prevent automatic deletion, just enable the customer tenant in Acronis Cyber Protect Cloud before the selected number of days have passed.
3. Click **Save**.

Deploying Acronis Cyber Protection agent (Windows, Linux and macOS)

1. In the NinjaOne interface, go to **Dashboard** > **Organizations** and click on the organization you want to manage.
2. Hover over a device of your choice, then navigate to **Run Script** and click **From Library**.
3. Click on the **Acronis Install Agent** script (pay attention to the device's OS and the script's target OS).



4. In the pop-up that appears next, click **Preset Parameter** and select the value configured for this script in the previous chapter.
5. In the **Run As** drop-down list, select the **System** value.



`https://mc-beta-cloud.acronis.com/ 79AE-07AD-440C`

6. Click **Apply**, then **Yes**.

Uninstalling the Acronis Cyber Protection agent (Windows, Linux and macOS)

1. In the NinjaOne interface, go to **Dashboard** > **Organizations** and click on the organization you want to manage.
2. Hover over a device of your choice, then navigate to **Run Script** and click **From Library**.
3. Click on the **Acronis Uninstall Agent** script (pay attention to the device's OS and the script's target OS).
4. In the pop-up that appears next:
   a. Leave the **Preset Parameter** field empty
   b. In the **Run As** drop-down list, select **System**.
5. Click **Apply**, then **Yes**.

Managing Protection Plan (Windows, Linux and macOS)

1. In the NinjaOne interface, go to **Dashboard** > **Organizations** and click on the organization you want to manage.
2. Hover over a device of your choice, then navigate to **Run Script** and click **From Library**.
3. Click on the **Acronis manage protection plan** script (pay attention to the device's OS and the script's target OS).
4. In the pop-up that appears next:
    a. If you want to apply a protection plan, associated with this token: click **Preset Parameter** and select the value with **Acronis registration token** only
    b. 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**
5. In the **Run As** drop-down list, select the **System** value.
6. Click **Apply**, then **Yes**.

Performing Acronis scans and tasks (Windows, Linux and macOS)

1. In the NinjaOne interface, go to **Dashboard** > **Organizations** and click on the organization you want to manage.
2. Hover over a device of your choice, then navigate to **Run Script** and click **From Library**.
3. Click on the **Acronis scans** script (pay attention to the device's OS and the script's target OS).
4. In the pop-up that appears next, click the **Preset Parameter** drop-down list and select one of the following values, which represents the type of task that needs to be run:
   - backup
   - av_scan
   - malware_scan
   - vulnerability_assessment
   - patch_management
5. In the **Run As** drop-down list, select the **System** value.
6. Click **Apply**, then **Yes**.

Monitoring

Monitoring Acronis statuses using NinjaOne custom fields

NinjaOne custom fields for devices can be used to monitor Acronis statuses such as:

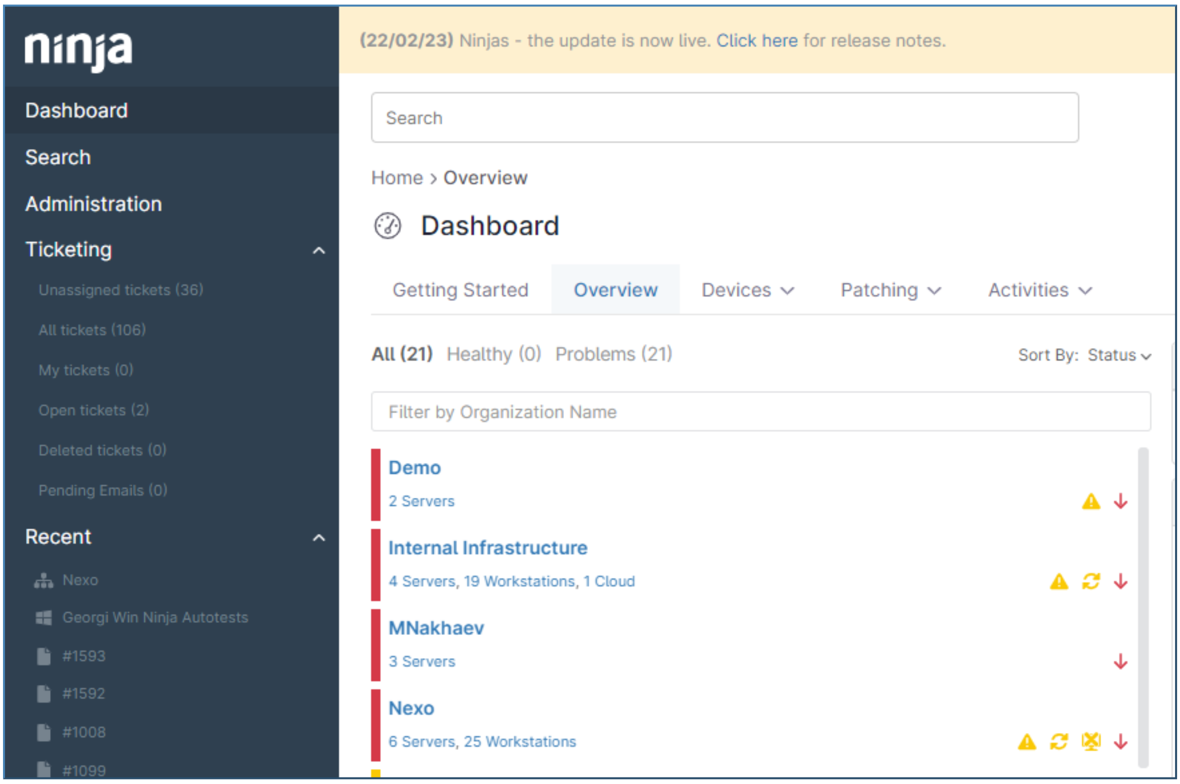
- Acronis Agent version
- Protection status
- Protection plan name
- Last backup date
- Next backup date
- Last antimalware scan date
- Next antimalware scan date

See Configure monitoring for more details on how to map Acronis statuses to NinjaOne custom fields.

View Acronis statuses on devices in NinjaOne

To check Acronis statuses for devices in NinjaOne, you should go to the organization where it is mapped:

1. Go to **NinjaOne** > **Dashboard** > **Organization**.



(22/02/23) Ninjas - the update is now live. Click here for release notes.

Home > Overview

Dashboard

All (21) Healthy (0) Problems (21)

Sort By: Status

Filter by Organization Name

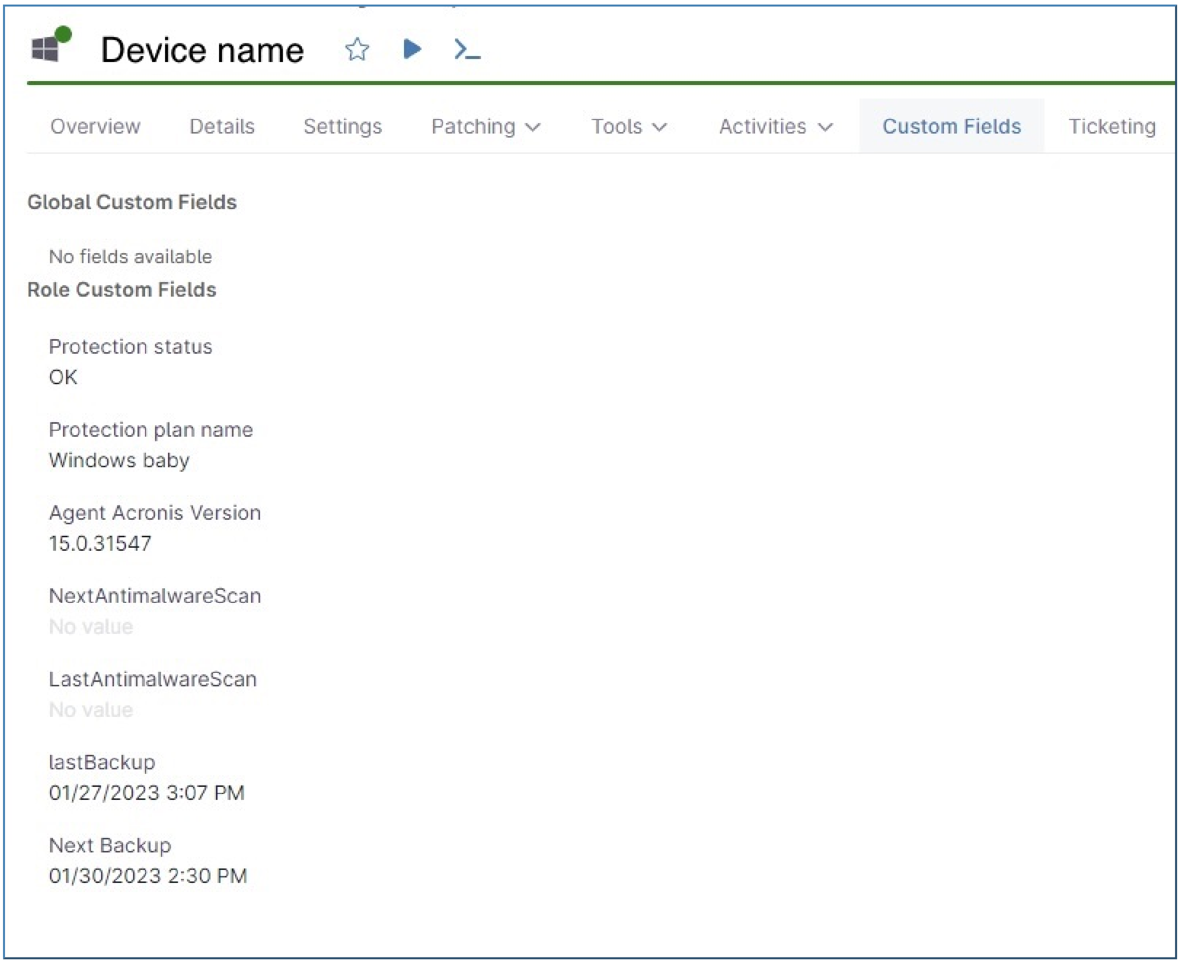
Demo
2 Servers

Internal Infrastructure
4 Servers, 19 Workstations, 1 Cloud

MNakhaev
3 Servers

Nexo
6 Servers, 25 Workstations

2. Navigate to the custom fields under this device.



Global Custom Fields

No fields available

Role Custom Fields

Protection status
OK

Protection plan name
Windows baby

Agent Acronis Version
15.0.31547

NextAntimalwareScan
No value

LastAntimalwareScan
No value

lastBackup
01/27/2023 3:07 PM

Next Backup
01/30/2023 2:30 PM

Note

Make sure that the **API permission** for the custom field, selected in NinjaOne, is set to include the **Write** option. Otherwise, the status update may fail.

Monitoring using scripts

This is the legacy tool that uses scripts to monitor Acronis statuses.

Monitoring scripts functionality

The following scripts are currently in use:

- **Acronis_backup_failed** - counts the number of open alerts of **backup failed** type and outputs the "**x backups failed**" sentence.

- **Acronis_antivirus_failed_alert** - counts the number of open alerts of "**Active Protection service is not running**" & "**Continuous Data Protection failed**" types and outputs the "**Active protection service failed x times**" sentence.

- **Acronis_malware_detected_alert** - counts cumulatively the total number of open alerts of "**Malware is detected and blocked (ODS)**" and "**Malware is detected and blocked (RTP)**" types and outputs the "**x MALWARE THREADS has been found**" sentence.

- **Acronis_last_backup** - 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 "**Last succesful backup more than x days ago**" sentence.

- **Acronis_last_antivirus_scan** - 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 "**Last succesful antivirus scan more than x days ago**" sentence.

- **Acronis_last_malware_scan** - 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 "**Last succesful antimalware scan more than x days ago"** sentence.

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

In order to manually run a monitoring script:

1. In the NinjaOne interface, go to **Dashboard** > **Organizations** and click on the organization you want to manage.
2. Hover over a device of your choice, then navigate to **Run Script** and click **From Library**.
3. Click on the monitoring script you want to run.
4. In the pop-up that appears next, select **Preset Parameter**, in case the script requires any.
5. In the **Run As** drop-down list, select the **System** value.
6. Click **Apply**, then **Yes**.

In order to create a NinjaOne scheduled task for repetitive monitoring script execution:

1. Navigate to **Configuration** > **Tasks**.
2. Click **New Task** in the top right corner.
3. For the newly created task, specify:
   a. name
   b. schedule
   c. optionally, description.
4. Click **Add Script** in the top right to specify what script to run in the task. This will open the **Script Library**. You can select any of the Acronis monitoring scripts listed there.
5. While adding scripts to your scheduled task, you will be prompted to specify **Preset parameters** and one of the following ways to run the script as:
   - System
   - current user
   - using your store credentials.
6. In the **Run As** drop-down list, select the **System** value.
7. Next, navigate to the **Targets** tab on the left page side.
8. Click **Add** in the top right.
9. Specify any desired organization(s), device(s) and/or group(s) to run the task on, then click **Apply**.
10. Finally, click **Save**.