Acronis

acronis.com

Acronis Cyber Cloud

Integration with Kaseya VSA

Integration Guide

REVISION: 9/7/2023

Table of contents

Introduction

This document describes how to install and use the Acronis Cyber Protect plugin for Kaseya VSA. The integration with Acronis Cyber Protect enables managed service providers to easily back up and protect devices directly from the Kaseya VSA interface without going to the Acronis Cyber Protect web interface.

Once the plugin is installed and configured, the data protection properties become automatically available for all servers and workstations in any location.

The service providers can:

- Provision new Acronis Cyber Protect customers
- Remotely install and update the protection agent on the devices
- Easily apply and revoke the pre-defined protection plan at customer or device level
- Monitor protection status for errors and warnings
- Leverage the native Kaseya VSA reporting, ticketing and alerting functionality for handling backup events

Service providers can create unique protection plans from the Acronis Cyber Protect web interface. Those protection plans are then synchronized and available for import and further usage in the Kaseya VSA interface.

Recovery is performed exclusively via the Acronis Cyber Protect web interface.

Terminology conventions

In this document, the Acronis Cyber Protect plugin will be referred to as "Acronis plugin" and the Acronis Cyber Protect web interface as “Acronis Management portal” or simply "Management portal".

Prerequisites

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

System requirements

Acronis plugin

The Acronis plugin can be installed on Kaseya VSA R95 or later.

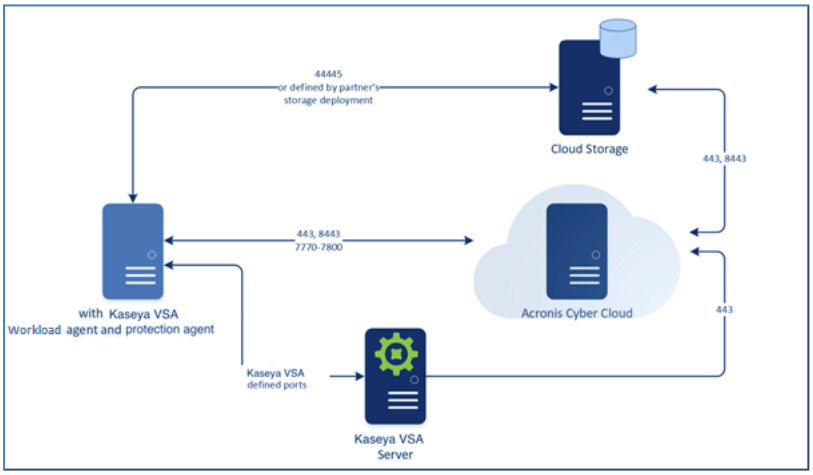
Acronis agents

Agents are applications that perform data backup, recovery, protection and other operations on Acronis-managed devices. An agent can be installed under any operating system, supported by Kaseya VSA - Windows, Linux or macOS.
Find a full list here: http://help.kaseya.com/WebHelp/EN/VSA/9050000/reqs/index.asp#home.htm

For a complete list of Acronis-supported operating systems, refer to the Acronis Cloud documentation.

Network requirements

The diagram below illustrates the network connections necessary for the Acronis plugin.



User rights

In Kaseya VSA, two levels of access rights exist to differentiate between administrator and general technician users.

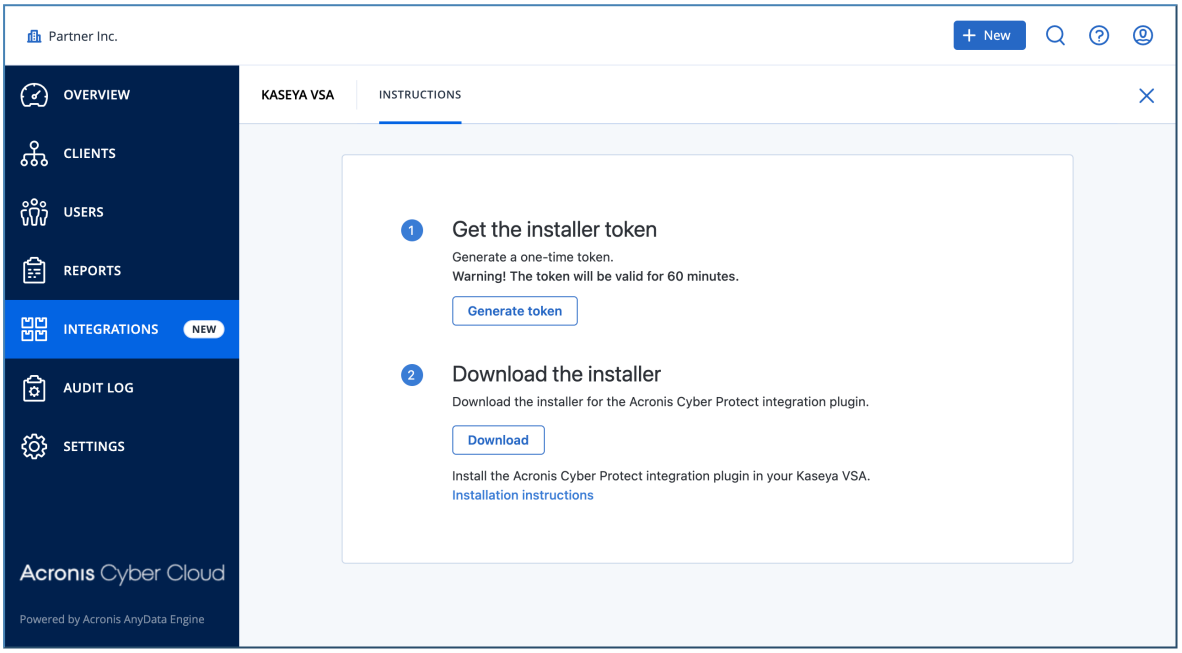
1. **Administrator access**
   In order to have full access to the plugin, including installation, the administrator's ConnectWise.Automate user class must have the **Core** > **Plugin Manager** permission set to **Access**.
2. **Technician access**
   For technicians, who should not have access to the Plugin Manager, but do need the full functionality of the Acronis integration, make sure that their user class has the **Plugin** > **Acronis Cyber Cloud** permission set to **Access**.

Apart from the administrator, it is not necessary for any other user, to have **Plugin Manager** access in order to use the integration.

Configuring the integration

To configure the integration using Acronis Cyber Protect

1. Go to the **Acronis Management portal** > **Integrations** and click on **Kaseya VSA**.
   See more information about enabling and managing integrations.
2. On the screen that opens, get the installer token and download the VSAZ installer.



3. Install the VSAZ file in the following directory:
   Kaseya VSA > **System** > **License Manager** > **Third Party** > **Install**
4. Follow the on-screen instructions to complete and activate the installation.

Installing an update

In order to update to a newer version of the Kaseya VSA integration, simply follow the steps, outlined in "Configuring the integration" (p. 8).

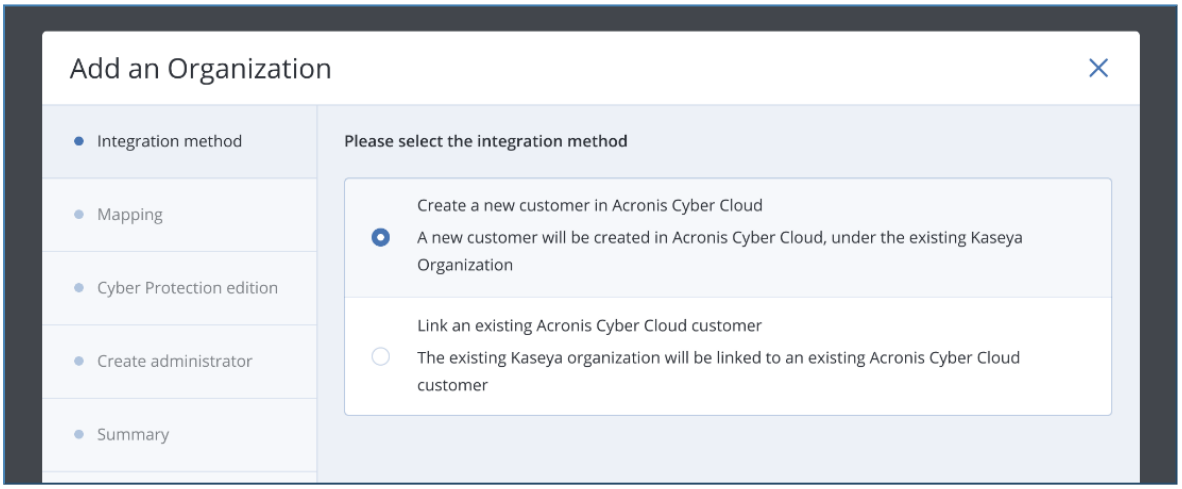
Managing customers

To enable device protection, you must link Kaseya VSA organizations to Acronis Cyber Protect customers. Do this by either:

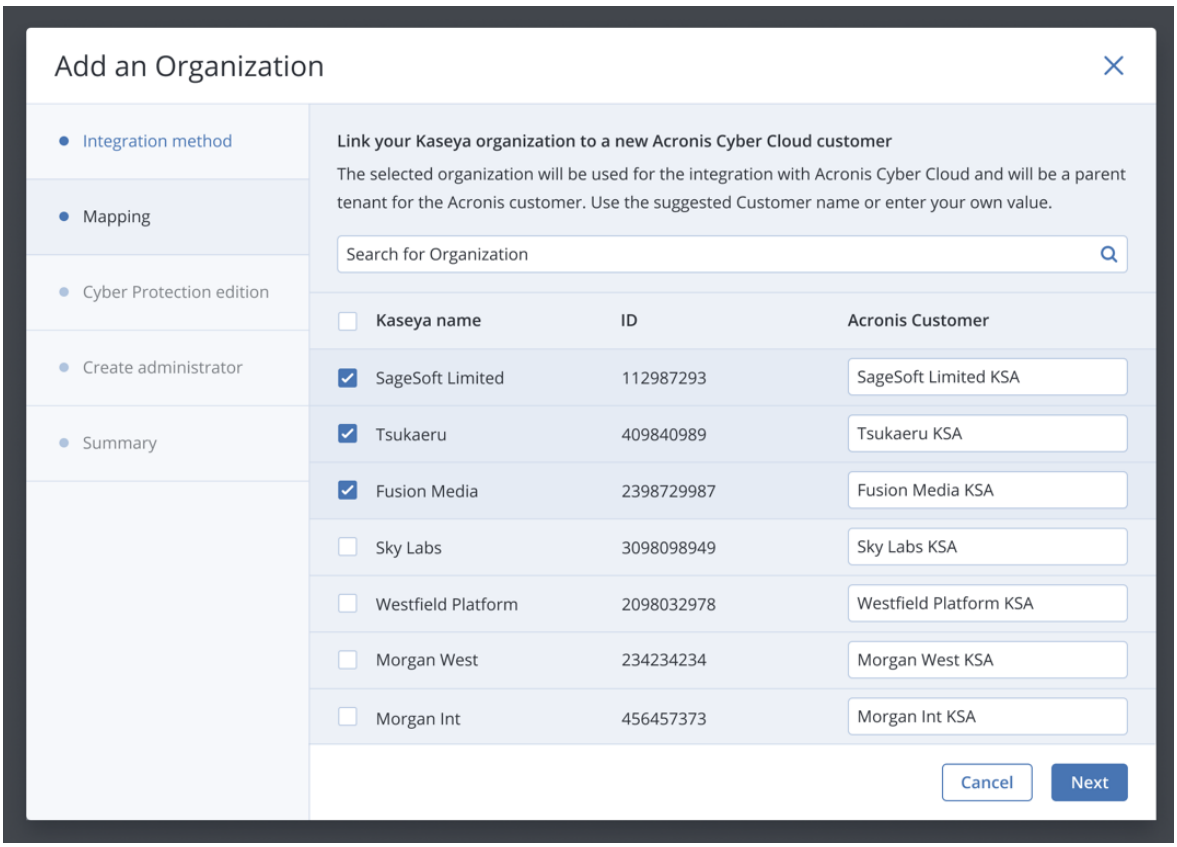
- **Creating a new Acronis customer tenant**
  If you do not have a customer in Acronis Cyber Protect to link to, then you can create such from within the Kaseya VSA module. The login and password of the newly created tenant will be used automatically when clicking **Go to Acronis Cyber Protect console** in the Kaseya VSA interface.
- **Linking an existing Acronis customer tenant to Kaseya VSA organization**
  If you already have a customer tenant in Acronis Cyber Protect, select and link them to a Kaseya VSA organization.

Create a new Acronis customer tenant and link to a Kaseya VSA organization

1. Click the **Add organization** button in the Kaseya VSA module.
2. Select the following option: **Create a new customer in Acronis Cyber Cloud**.

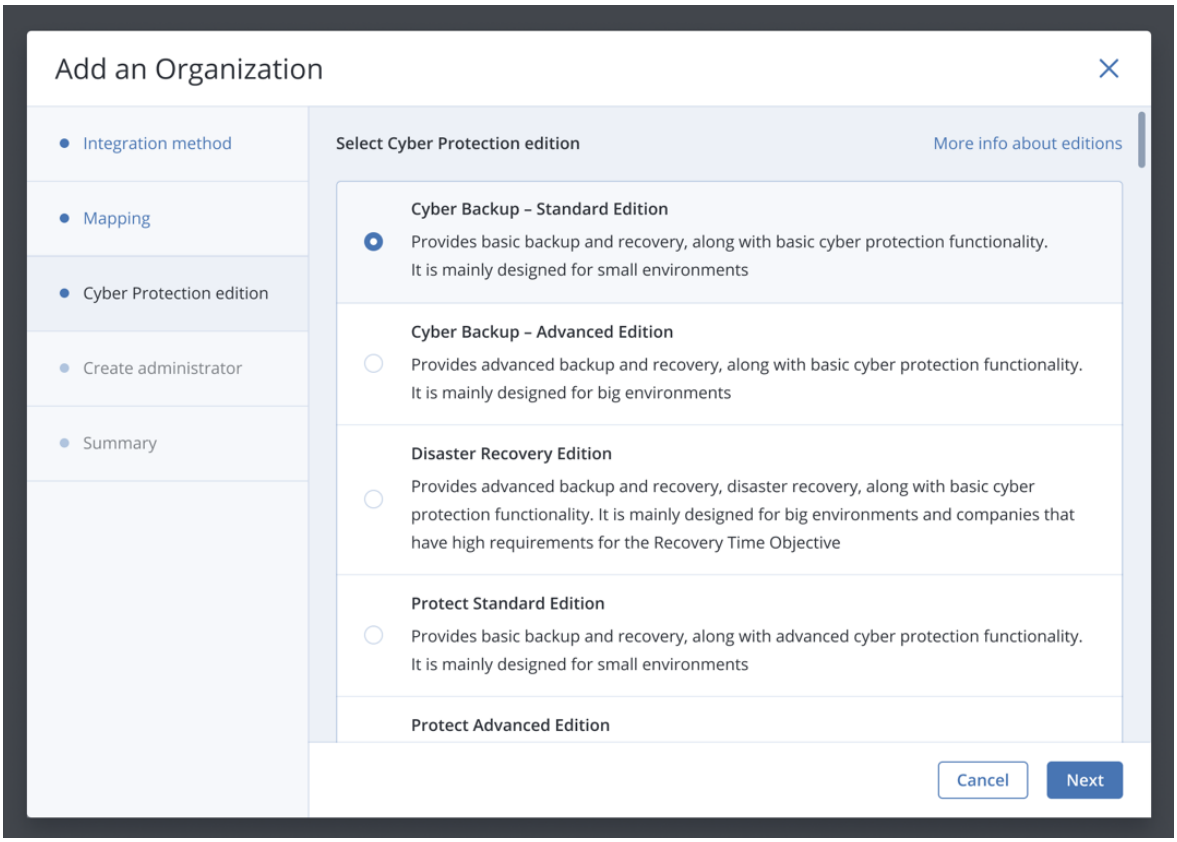


3. In the **Mapping** step, select the Kaseya organization that you would like to create a new Acronis customer for. You can create multiple customers (up to 20) by selecting more than one organization.
   The integration module will suggest a name for the Acronis customer by appending the “KSA” suffix after the Kaseya organization name. You are allowed to change the name at this step.

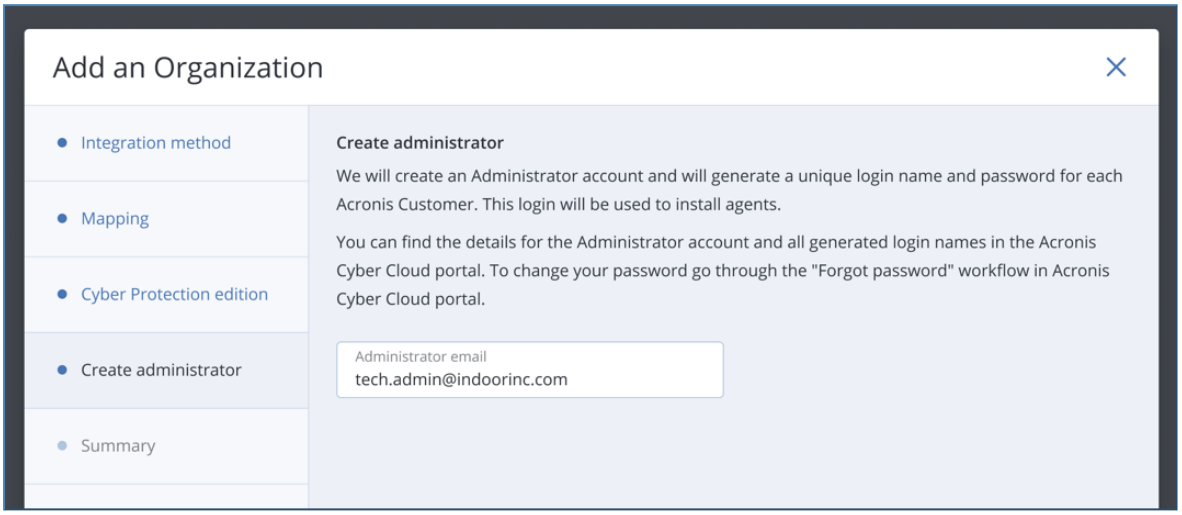


4. Choose an Acronis Cyber Protection edition for the new Acronis customers.

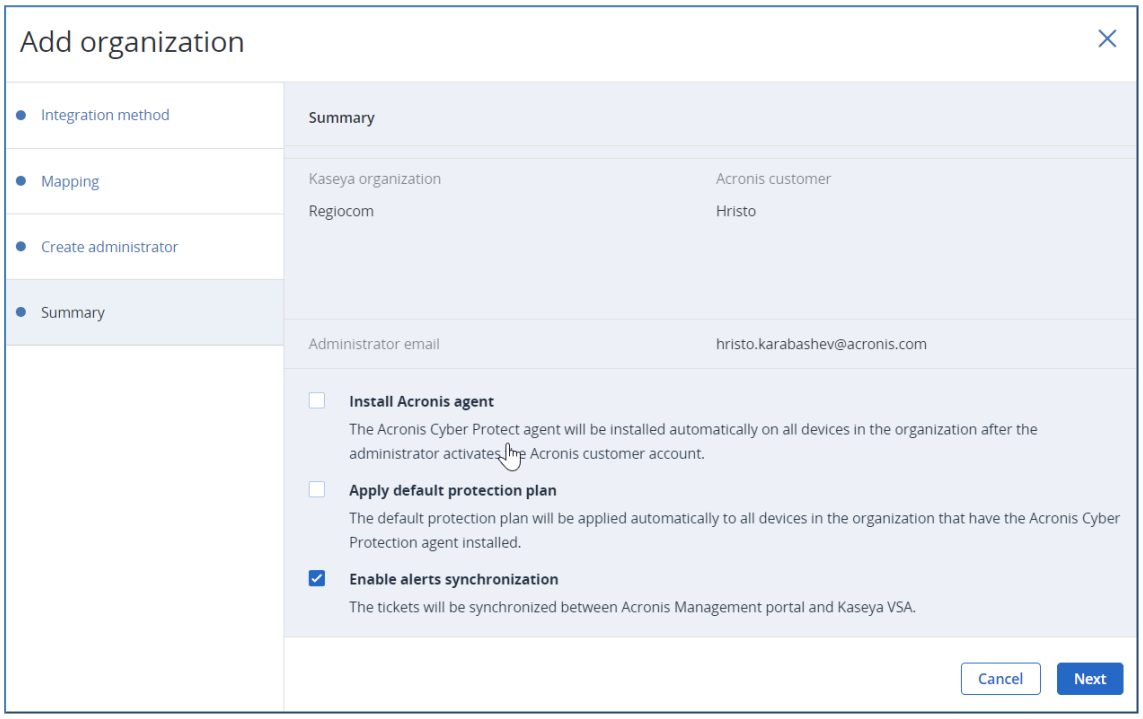
Note
The same Cyber Protection edition will be applied to all new customers created within the same session.



5. To create an Administrator, provide an email address. The integration will generate individual login and password for each Acronis customer and use these credentials to install Acronis agents from within Kaseya VSA.



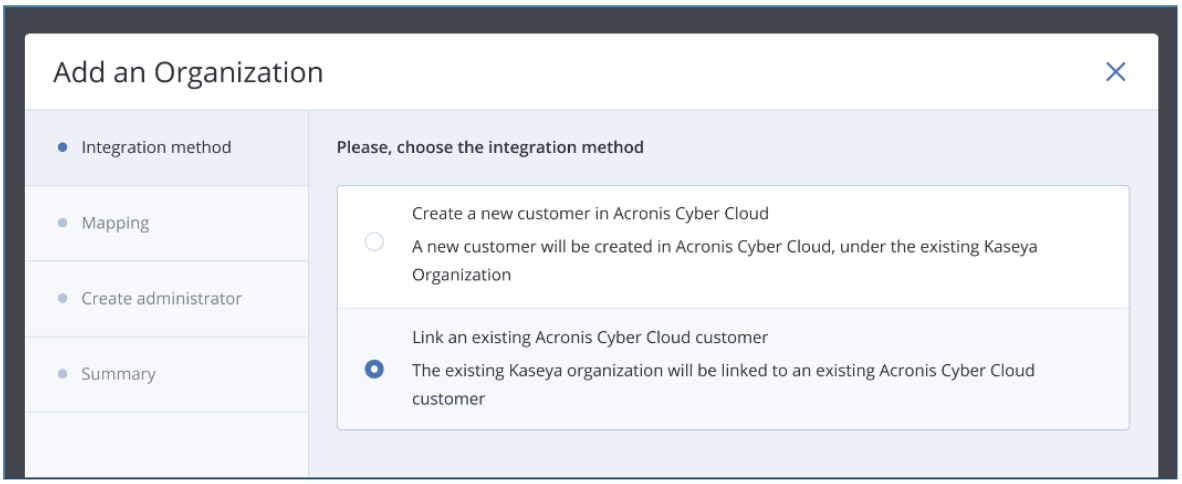
6. Finally, a **Summary** screen will appear with information about the newly created Acronis customer tenants and the Kaseya organizations they were connected to.
   Select any of the available options:
   a. **Install Acronis agent** – enable this checkbox to allow the integration to install Acronis agents automatically to all devices that don't have Acronis installed yet.
   b. **Apply default protection plan** – the Acronis Cyber Protect default protection plan will be automatically applied to all devices without plans.



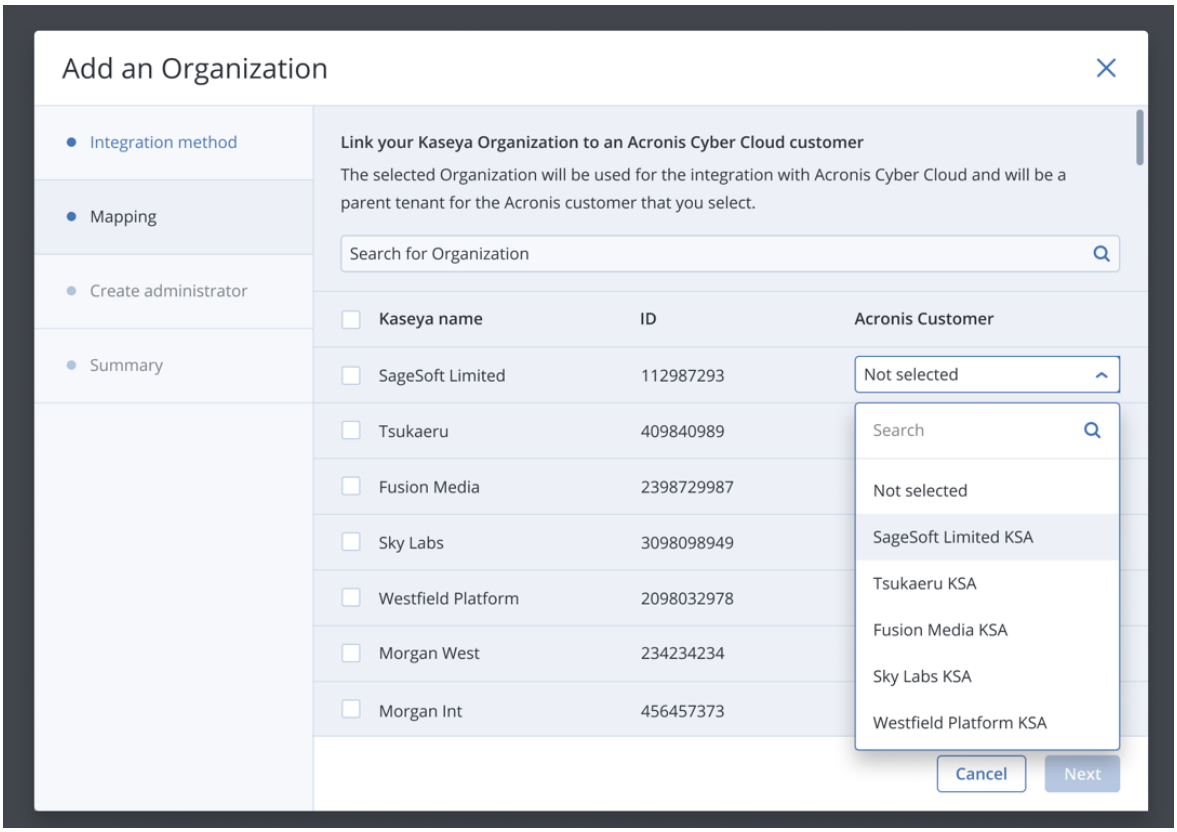
   c. **Enable alerts synchronization** - mark this option if you want to turn on tickets sync between the Acronis Management portal and Kaseya VSA.

Link an existing Acronis customer tenant to a Kaseya organization

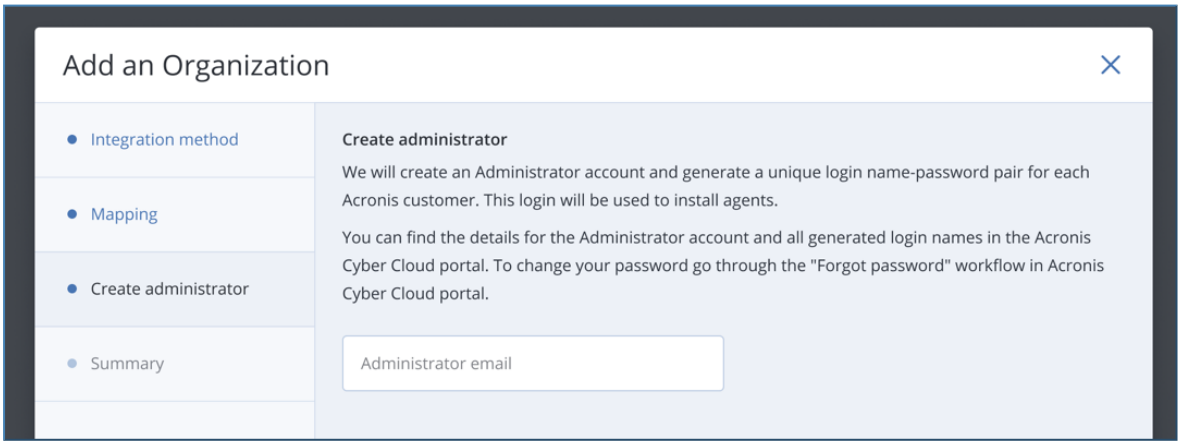
1. Click the **Add organization** button in the Kaseya VSA module.
2. Select the **Link an existing Acronis Cyber Cloud customer** option.



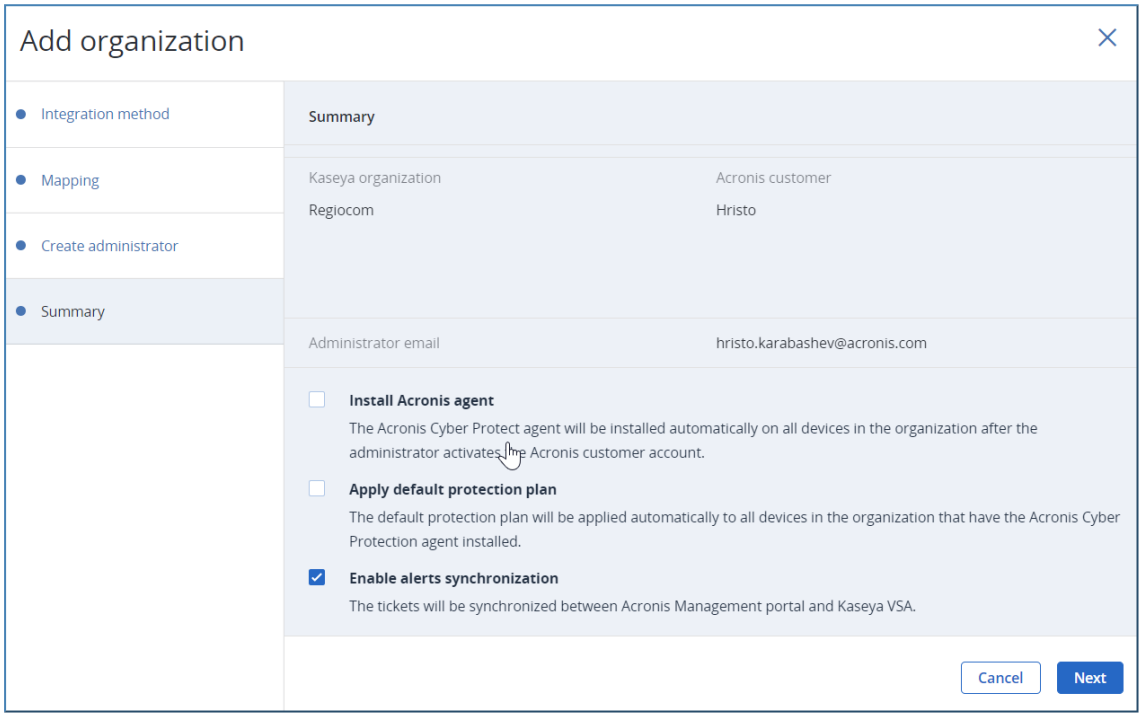
3. In the **Mapping** step, select a **Kaseya organization** and map it to an Acronis customer. You can create up to 20 mappings at once.



4. Add an email address for Administrator login, which will be used only to install agents from the integration. A new administrator account will be created for integration usage and existing Administrator logins will remain unchanged.



5. At the end, you'll see a **Summary** screen with information about the newly created Acronis customer tenants and the Kaseya organization they are mapped to.
   Select any of the available options:
   a. **Install Acronis agent** – by enabling this checkbox, you allow the integration to install Acronis agents automatically to all devices that don't have Acronis installed yet.
   b. **Apply default protection plan** – the Acronis Cyber Protect default protection plan will be automatically applied to all devices where necessary.



   c. **Enable alerts synchronization** - mark this option if you want to turn on tickets sync between the Acronis Management portal and Kaseya VSA

Administrator account

As a necessary functional part of the mapping process, the integration creates an Administrator user for each customer tenant.

This special type of user is created as a *service account*, granted limited privileges and doesn't use 2FA, even if it is enabled for all the rest of the users.

Although it is possible in the Management portal to switch this user to a regular account and enable the 2FA, you are not recommended to do so as it will break the integration's functionality.

The *service account* user type is designed to provide optimal security, specifically for scripts and integrations such as the Kaseya VSA.

Installation of Acronis Cyber Protect agents

Installation of agents under Windows

An Acronis Cyber Protect agent must be installed on every device that you want to back up and protect. There are two installation methods:

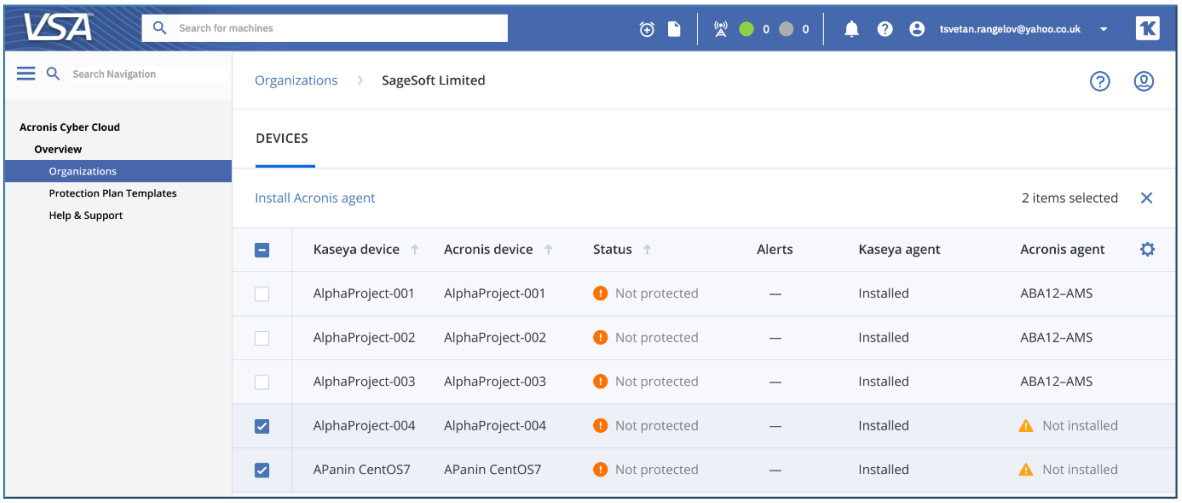
- Manual
  - Installing the agent at a customer level
  - Installing the agent at a device level
- Automatic
  - Installing the agent at a customer level

Manual installation

This method allows you to install agents on any device within an organization.

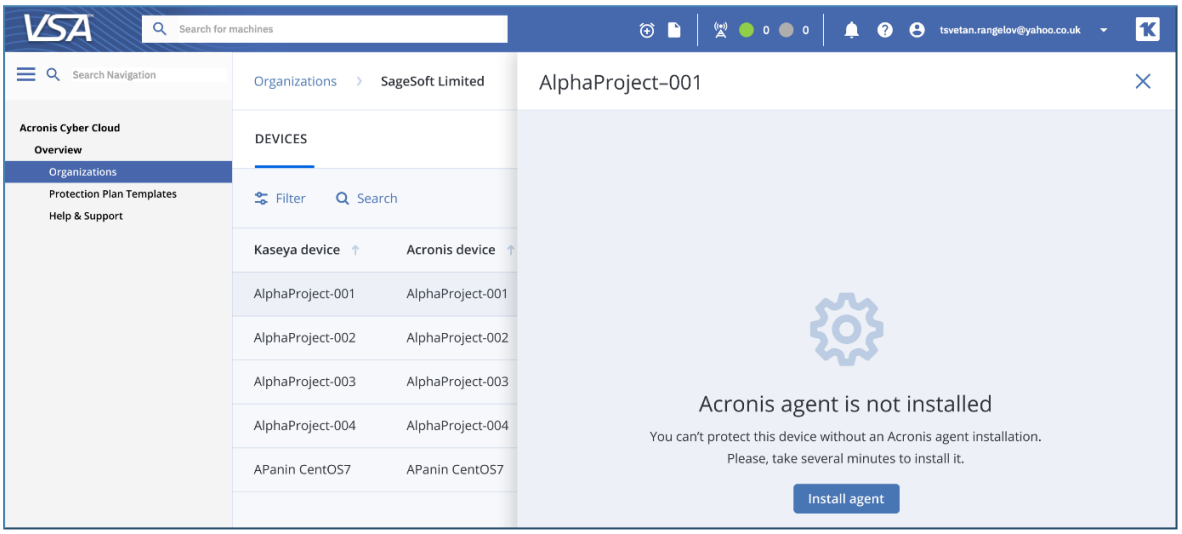
To install the Acronis Cyber Protect agents at a customer level

1. Go to the Acronis Cyber Protect module in Kaseya VSA.
2. Click on a customer.
3. All devices for this customer will be displayed in the **Devices** table.
4. Select all devices that you want to install the agent on. To identify which devices do not have cyber protection agents, sort the **Acronis agent** column in the **Devices** table.
5. Click on **Install Acronis Agent**.



To install a cyber protection agent at a machine level

1. Select a customer from the **Organizations** tab.
2. Double-click the machine, then a side panel appears.
3. Click on **Install agent**.



Automatic installation

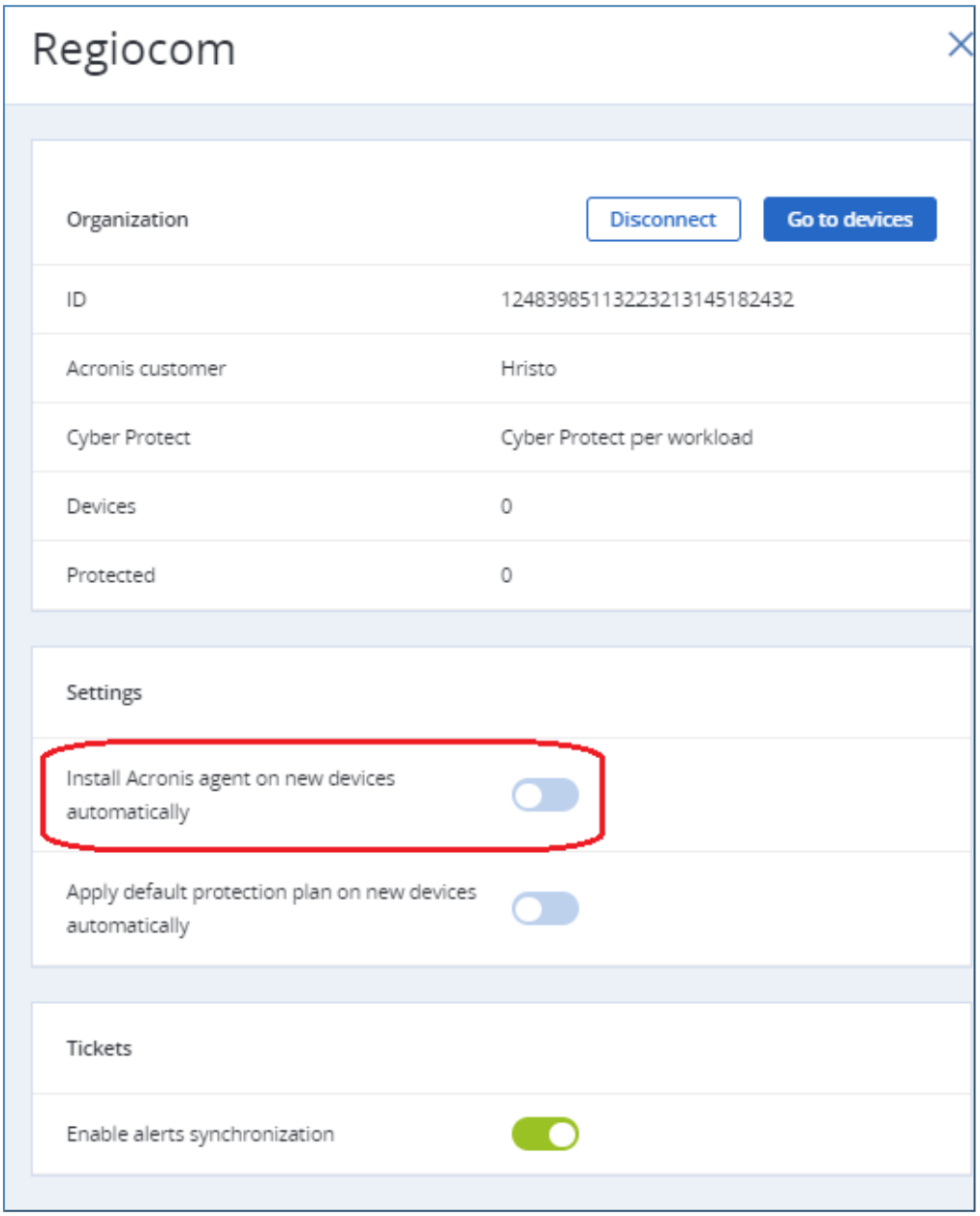
There are two ways to install cyber protection agents at a customer level:

When creating or linking Acronis customers

1. Execute steps 1 through 4, as already described in either of the workflows: **Create a new Acronis customer tenant** or **Link an existing Acronis customer tenant with a Kaseya organization**.
2. On the **Summary** screen, select the **Install Acronis agents automatically** checkbox. Then a cyber protection agent will be silently installed on any machine added to the customer later.

From the Organizations list

1. In your Acronis Cyber Protect module, choose an organization from the **Organizations list**.
2. In the side panel that appears next, under **Settings**, enable the **Install Acronis agents on new devices automatically** option.



Installation of agents under macOS or Linux

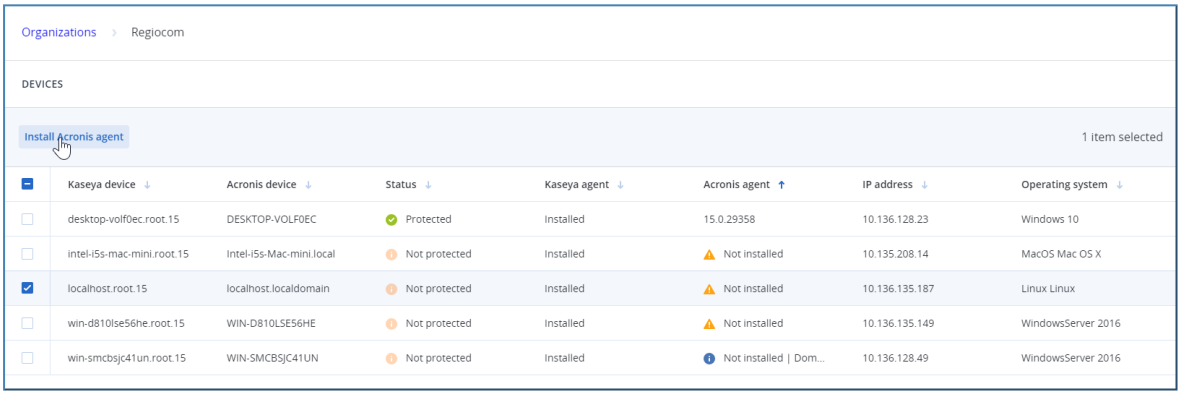
Agent installation can be done on one or more machines at the same time. Possible scenarios include:

- Manual or automatic installation
- Installation with procedure or scheduled procedure

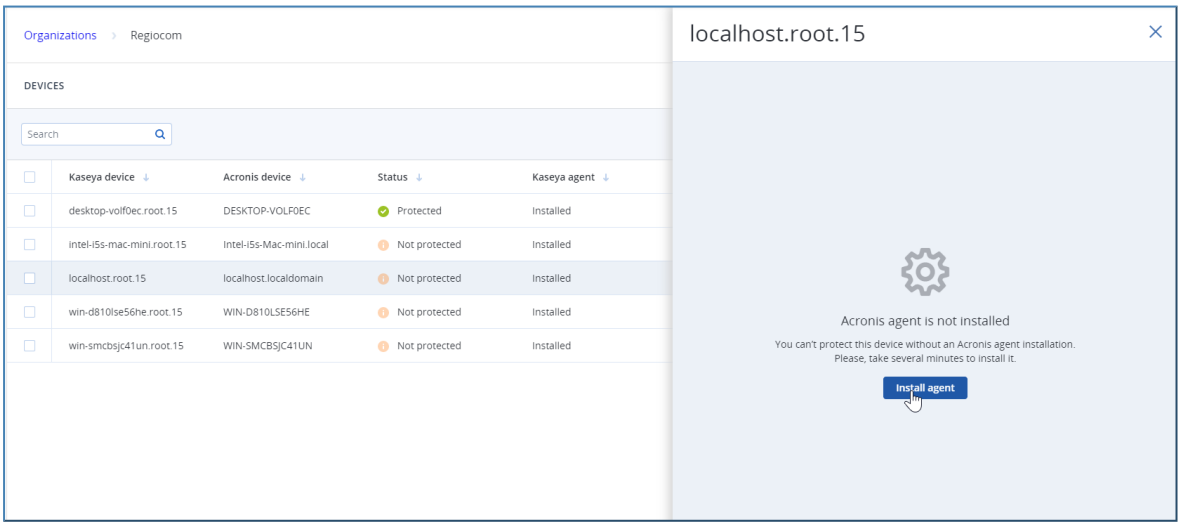
Manual installation

This type of installation is done from the **Organizations** list:

1. In your Acronis Cyber Protect module, choose an organization from the **Organizations** list.
2. Navigate to the **Devices** tab to display all machines that currently belong to this organization.



3. Select the one you want to protect and in the header menu, click **Install Acronis agent**.

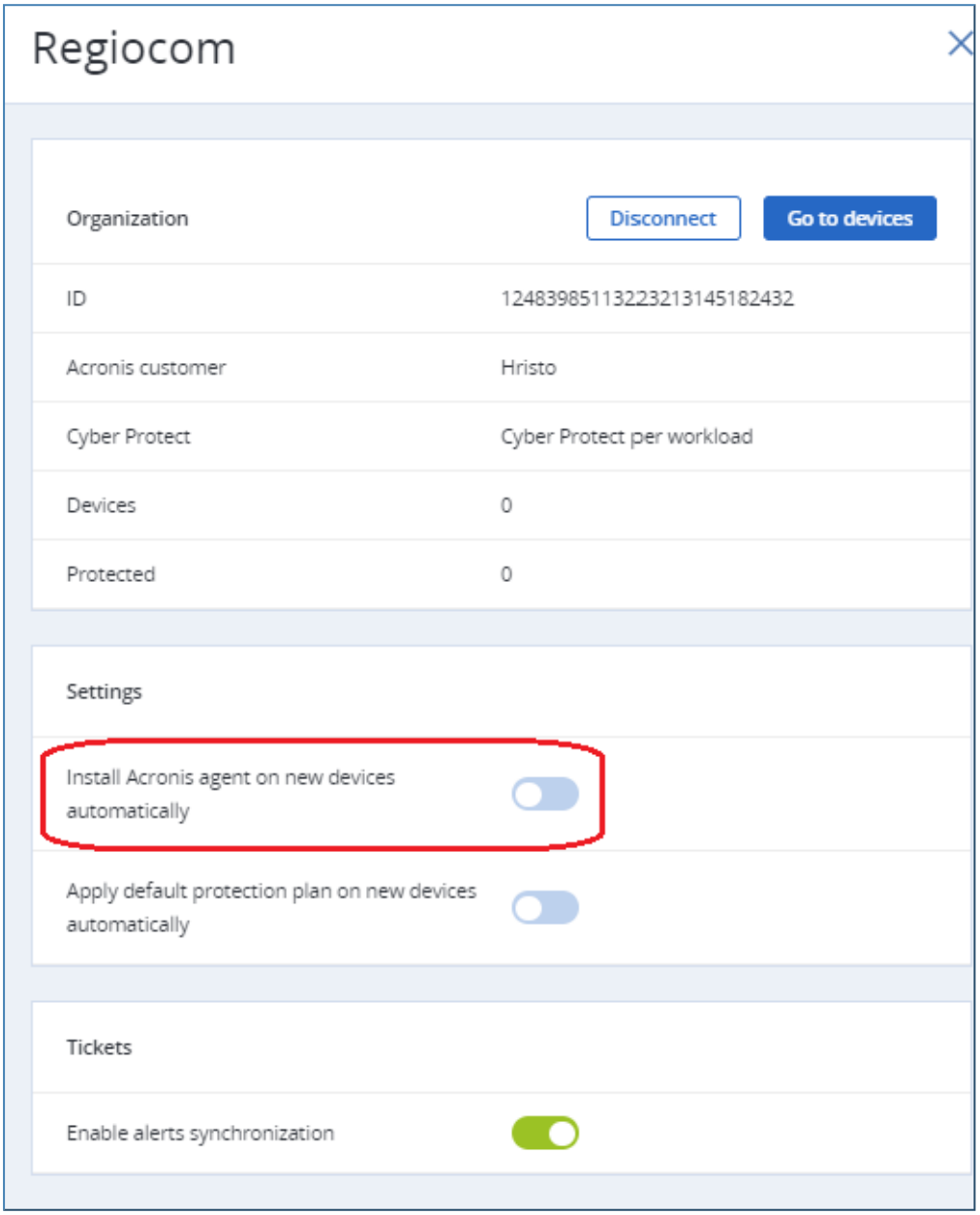


4. You will see a confirmation that Acronis agent installation is in progress.

Automatic installation

This type of installation is done via the integration module:

1. Go to **Acronis Cyber Protect** > **Organization** > **Devices** > **Settings**.
2. Switch the **Install Acronis agent on new devices automatically** toggle button.



When a new machine is added to this organization, the Acronis agent will be automatically installed on it.

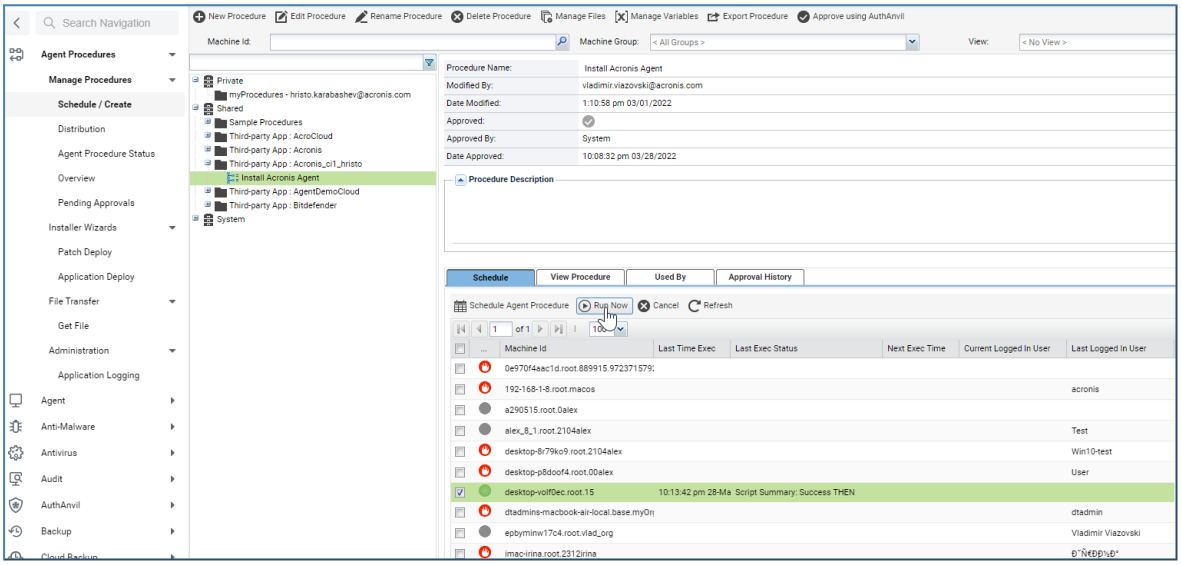
To check whether the license has expired:

1. Go to **Acronis Cyber Protect** > **Devices**.
2. Select the machine you want to protect and in the header menu, click **Install Acronis agent**.

3. If the license has expired on this machine, you will see a "**Blocking install issues**" message.
4. You should ask the customer to renew the license and then execute the above steps.

Installation with procedure

1. Go to **Kaseya VSA** and locate the **Agent Procedures** folder.
2. In the left pane menu, go to **Manage Procedures** > **Schedule/Create**.
3. In the expanded folders tree, locate and click the **Install Acronis agent** procedure.

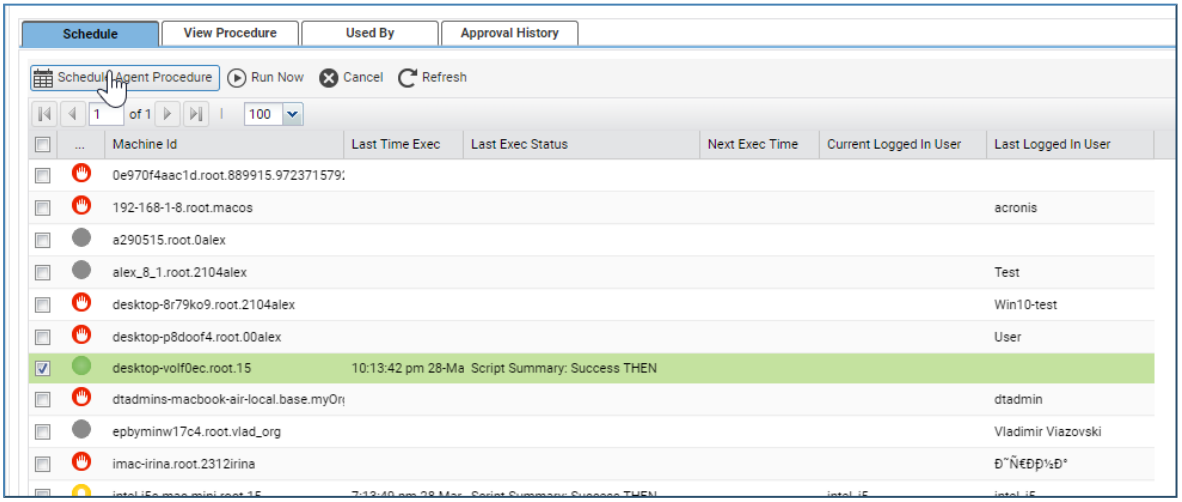


4. Select on which machines to execute the script and click **Run now**. This will apply the procedure on the selected machines.

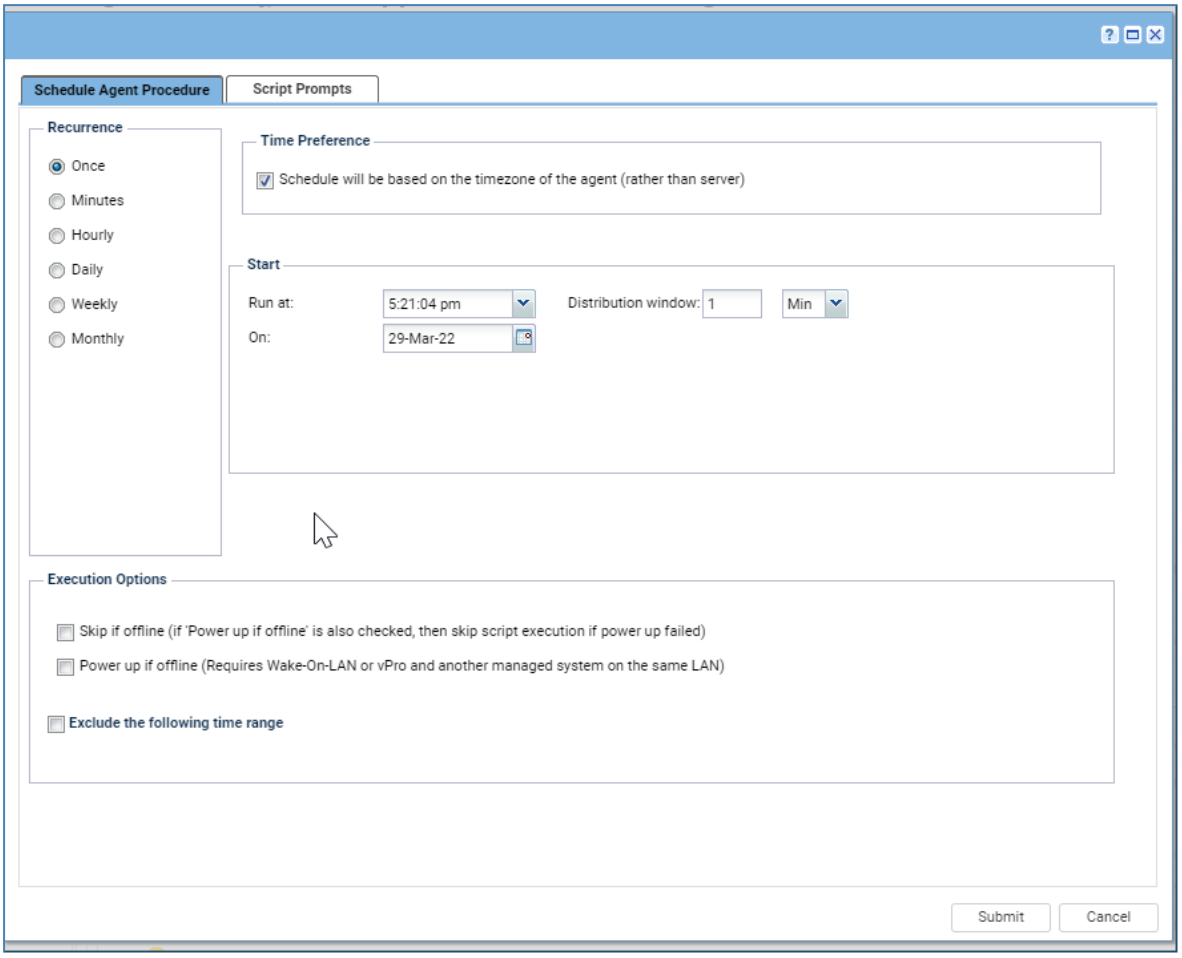
Installation with scheduled procedure

You can also schedule when to run the script.

1. Execute steps 1 through 3 above, then click on the **Schedule Agent Procedure** option.



2. Set the necessary schedule properties: **Recurrence**, **Time Preference**, **Start**, etc.



3. Click **Submit**.

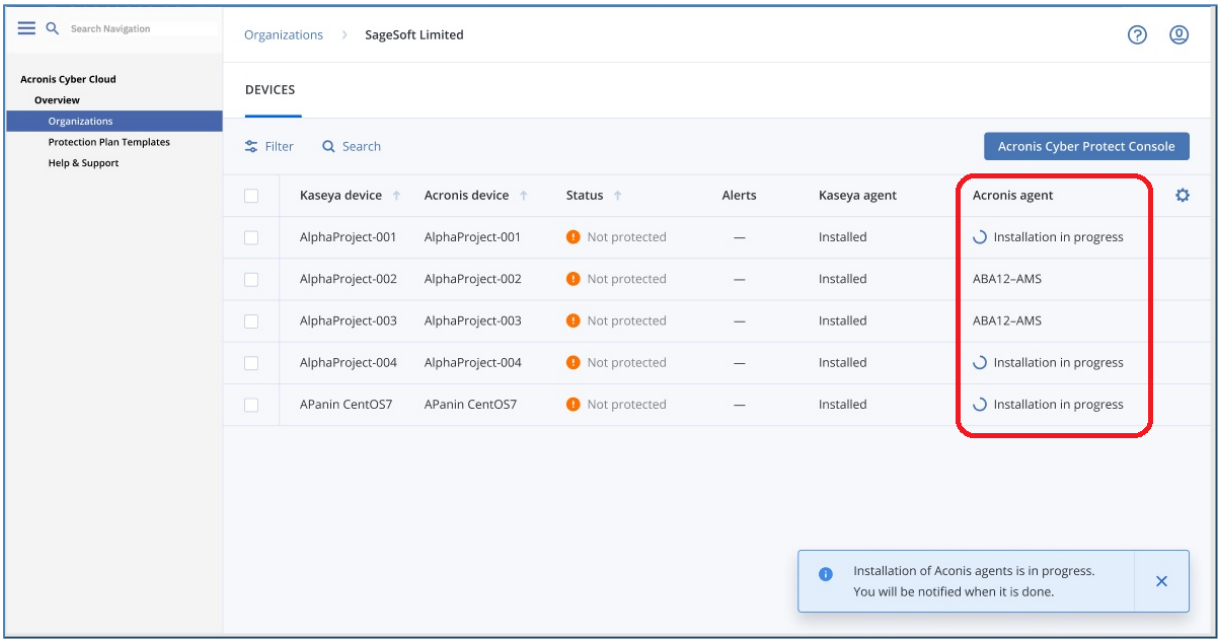
Domain Controller deployment

When deploying Acronis to a Windows Domain Controller, credentials are required for the agent installation.

Several different installation scenarios are possible, depending on whether you are deploying simultaneously on:

- single or multiple endpoints
- workstations or Domain Controllers only, or a combination of both.

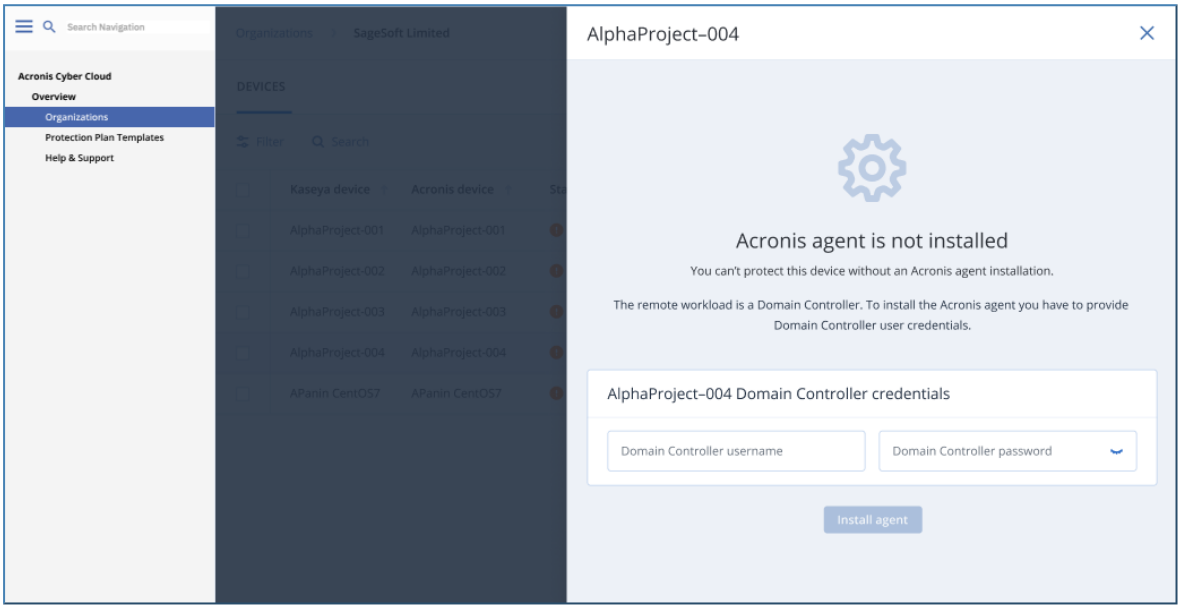
In all of the above cases, the progress of the installation can be monitored from the following screen with list of devices:



When the installation is complete, the Domain Controller(s) should have also been registered.

Installation on a single workload

1. Select a single workload that doesn't have an Acronis installation yet.
2. The integration checks if it is a Domain Controller.
3. You will be asked to provide credentials.

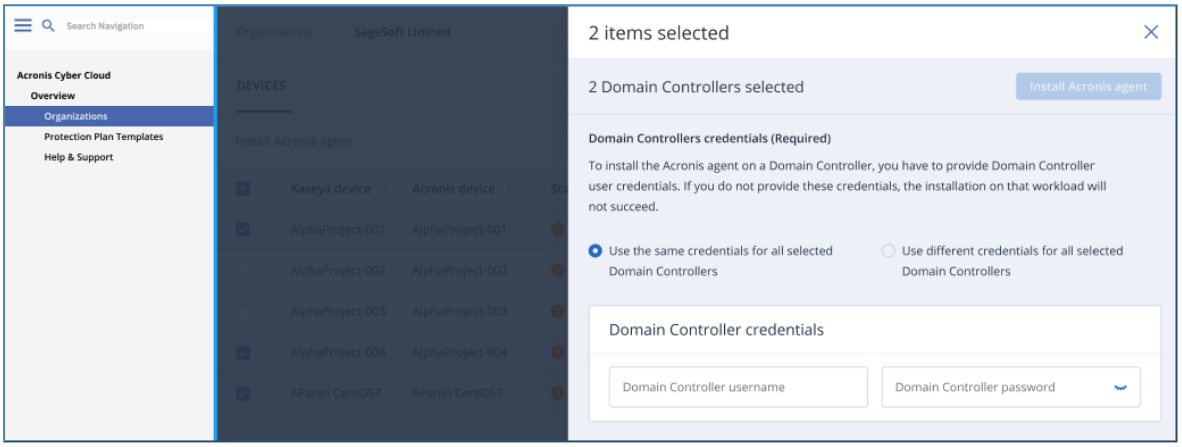


4. When done, click **Install agent**.

Installation on multiple workloads

Multiple Domain Controllers

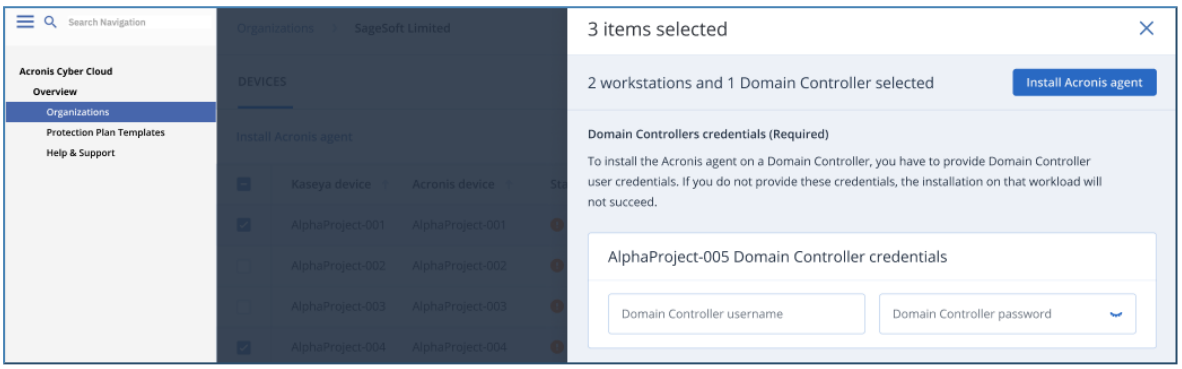
1. Select the necessary number of workloads by clicking on their checkboxes.
2. The integration detects the exact number of workloads in the selection and for each one, checks whether it is a Domain Controller.



3. You will be asked to provide user credentials with the following two options:
   a. apply the same credentials to all selected workloads
   b. use different credentials, in which case you have to enter each pair of username and password individually
4. When done, click **Install Acronis agent** to proceed with the installation.

Single Domain Controller and Multiple Workstations

1. Select the necessary number of workloads by clicking on their checkboxes.
2. The integration detects the exact number of workloads in the selection and for each one, checks whether it is a Domain Controller.

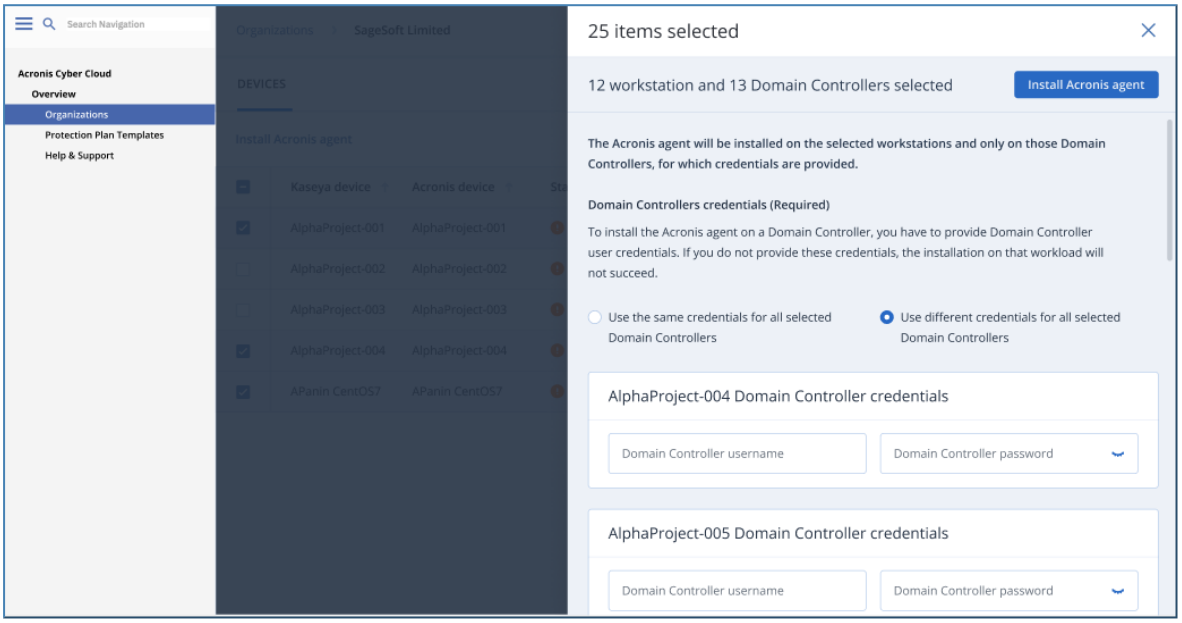


3. For the workload, identified as a Domain Controller, you will be asked to provide user credentials.
4. Once the credentials have been filled in, click **Install Acronis agent** to proceed with the installation.

The Acronis agent will be then installed on all selected workstations and on those Domain Controllers, for which credentials are provided.

Multiple Domain Controllers and Single or Multiple Workstations

1. Select the necessary number of workloads by clicking on their checkboxes.
2. The integration detects the exact number of workloads in the selection and checks how many of them are Domain Controllers.

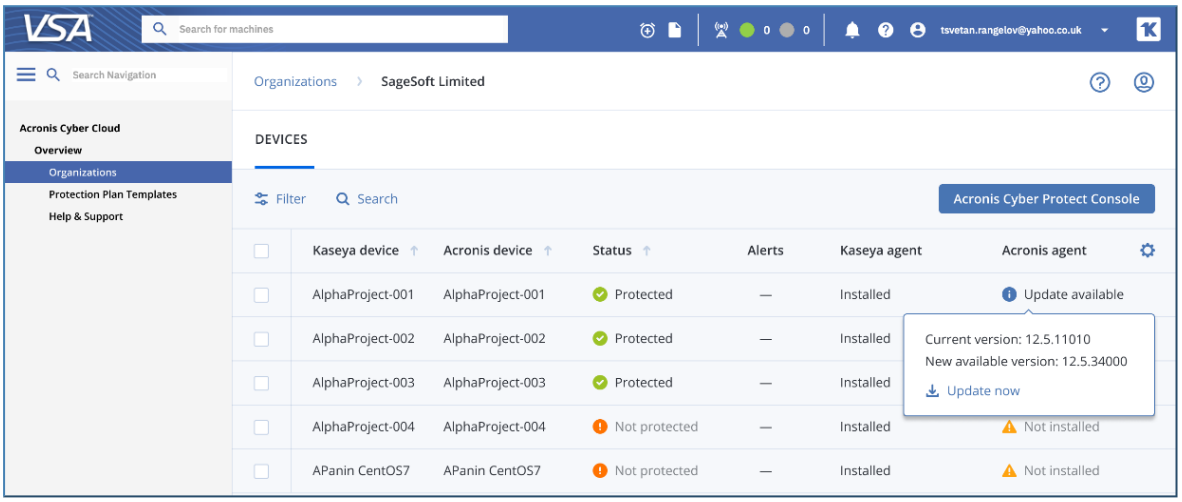


3. For those identified as Domain Controllers, you will be asked to provide user credentials with the following two options:
   a. apply the same credentials to all selected workloads
   b. use different credentials, in which case you have to enter each pair of username and password individually
4. Click **Install Acronis agent**.

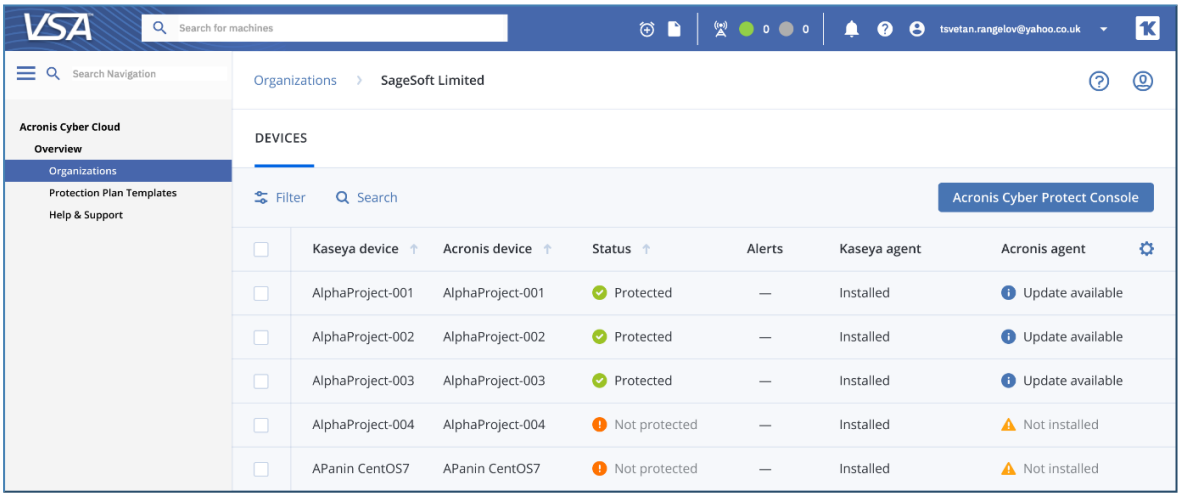
Updating cyber protection agents

Updating is done similarly to installation from the Acronis Cyber Protect module.

1. To identify the agents that require an update, the **Acronis Agent** column status in the **Devices** table should be marked as **Update Available**.



2. Select all machines, for which you want to update agents and click **Update Acronis agent** at the top left of the table.



Protecting devices

Acronis Cyber Protect provides backup and cyber protection for devices through the usage of protection plans.

A protection plan is a set of rules that specify how a device will be protected, as well as how the Acronis Cyber Protect agent will monitor for suspicious activities on the device, and act when a threat is detected.

A protection plan can be applied to a single or multiple devices.

An Active Protection plan is the currently assigned set of rules.

The Acronis Cyber Protect plugin for Kaseya comes with a built-in Default Protection Plan, but you can also configure and use your own protection plans.

The Default Protection Plan

The default plan shipped with the plugin is a general purpose backup and protection plan that will suit most situations and is provided to MSPs to be able to have devices working protected right away.

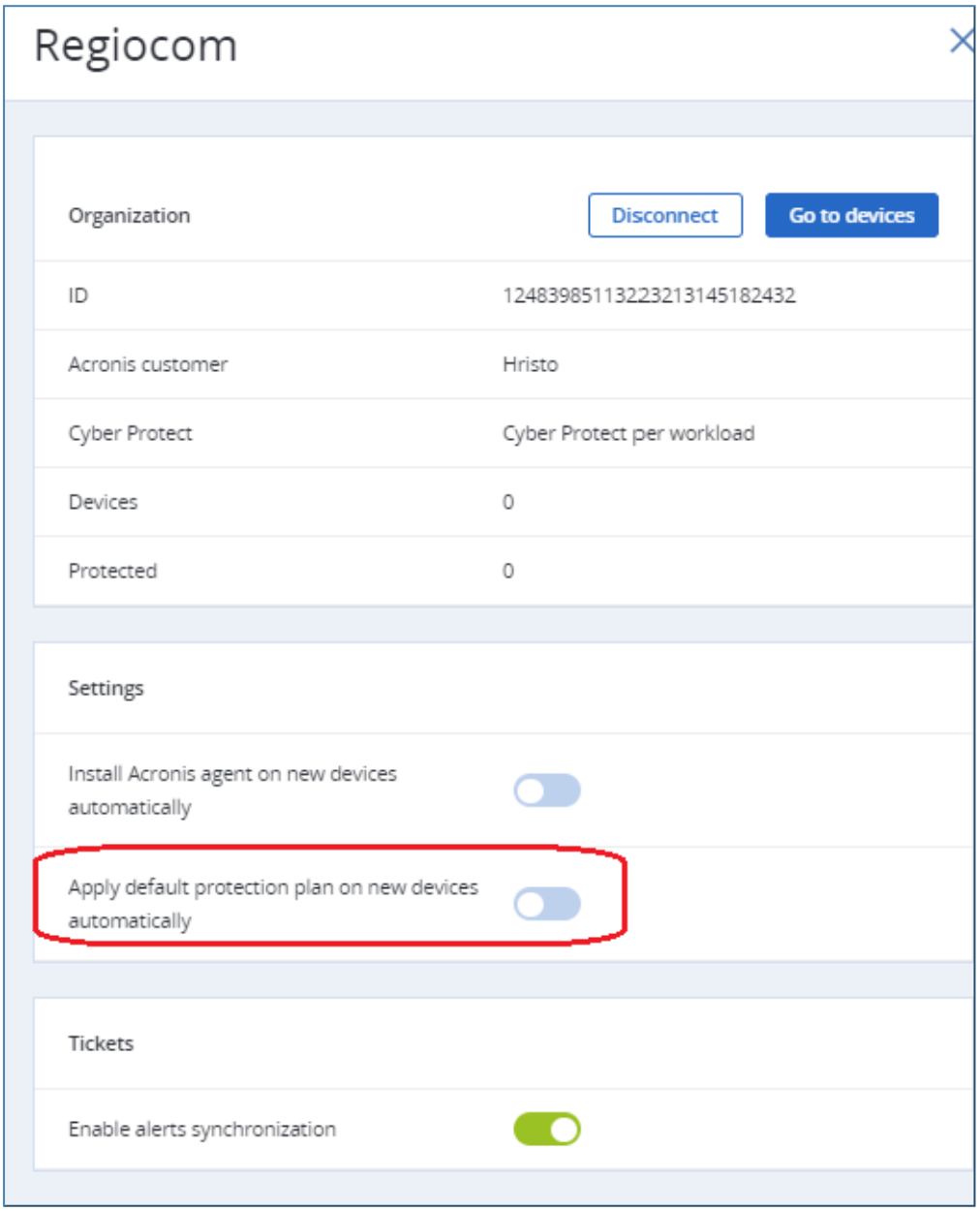
This built-in Default Protection Plan has the following settings:

- **Backup Module**
  Entire machine to Cloud Storage. According to this plan, a machine is backed up to the cloud storage daily from Monday to Friday at 11:00 pm.
- **Antivirus and Antimalware Protection**
  Self-protection, Real-time protection and Scheduled scan are turned on. Server-side protection is off. Quarantined files are removed after 30 days.
- **Microsoft Security Essentials Settings**
  Full scan at 12:00 pm only on Friday
- **Windows Defender Antivirus**
  Full scan at 12:00 pm only on Friday. Real-time protection is turned on.
- **URL Filtering**
  URL Filtering is on. Website access: always ask user
- **Vulnerability Assessment**
  Products to check every day at 10 am (UTC): Microsoft products, other third-party products
- **Patch Management**
  Patch Microsoft as well as other third-party products. Schedule: every Monday at 4:00 pm.
- **Data Protection Map**
  Run weekly at 3:30 pm, Monday through Friday for 66 extensions.

You can use this default plan or configure and apply your own variant as default one.

The default plan will be applied automatically on every device that does not have a protection plan yet, if you enable Apply default plan on new devices automatically by following these steps:

1. In your Acronis Cyber Protect module, choose an organization from the **Organizations list**.
2. In the side panel that appears next, under **Settings**, enable the **Apply default plan on new devices automatically** option.



Importing protection plans

In this section, find a description on how to import and apply a protection plan in Kaseya VSA.

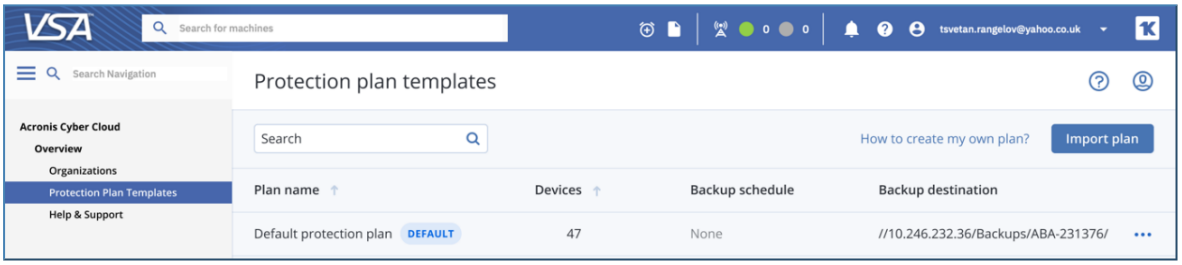
A custom protection plan appears in Kaseya VSA only after it has been imported from Acronis Cyber Cloud.

Important
Before importing a protection plan, verify that the **Using policy rules** selection method is chosen in the **Items to back up** section of this plan.

There are two ways to import a protection plan in Kaseya VSA.

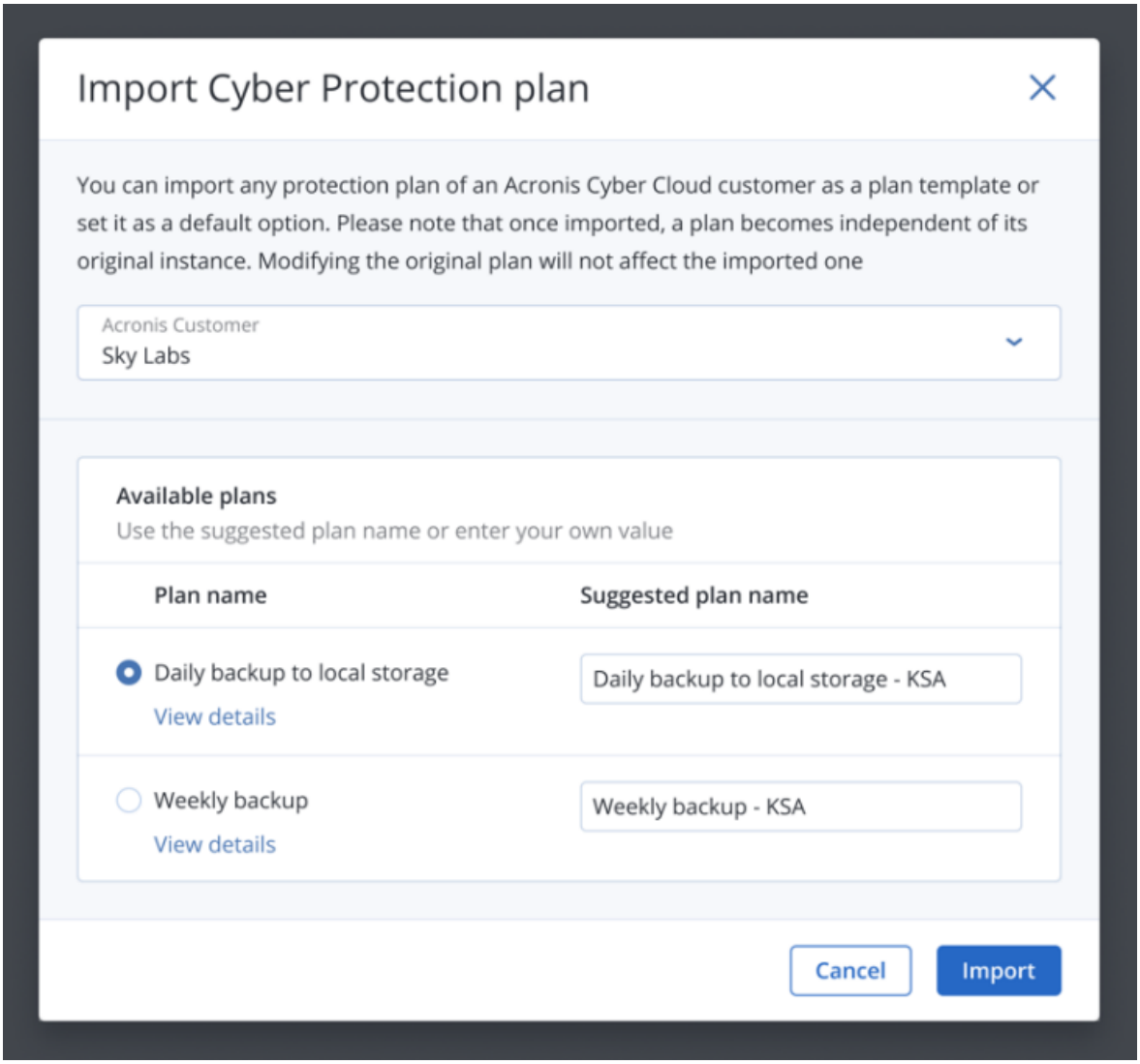
Importing plans from the Protection Plan Templates tab

1. Go to the **Acronis Cyber Protect** module in **Kaseya VSA** > **Protection Plan Templates**.
2. Click **Import plan**.

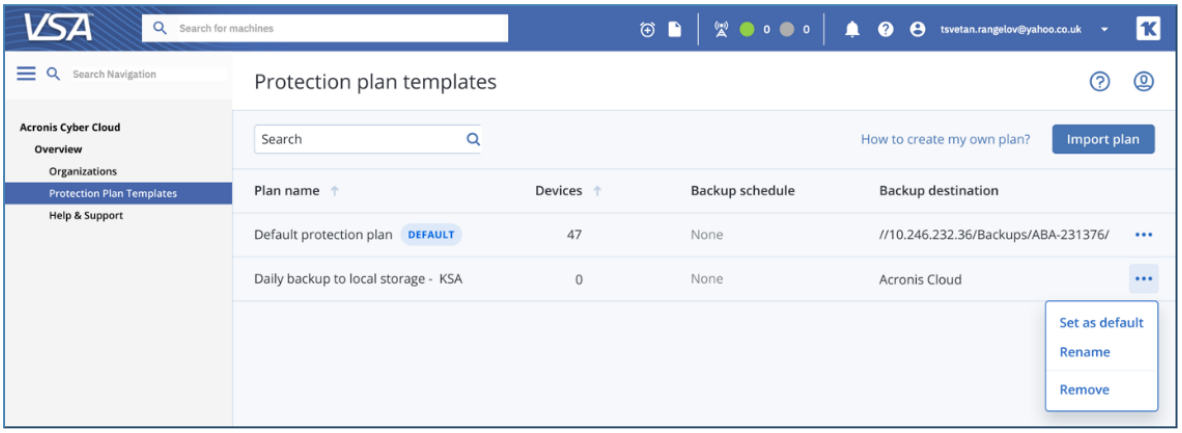


3. Select the Acronis customer from which you want to import a plan. All available plans for this customer will be displayed.

4. Choose the protection plan you want to import and optionally, rename it.

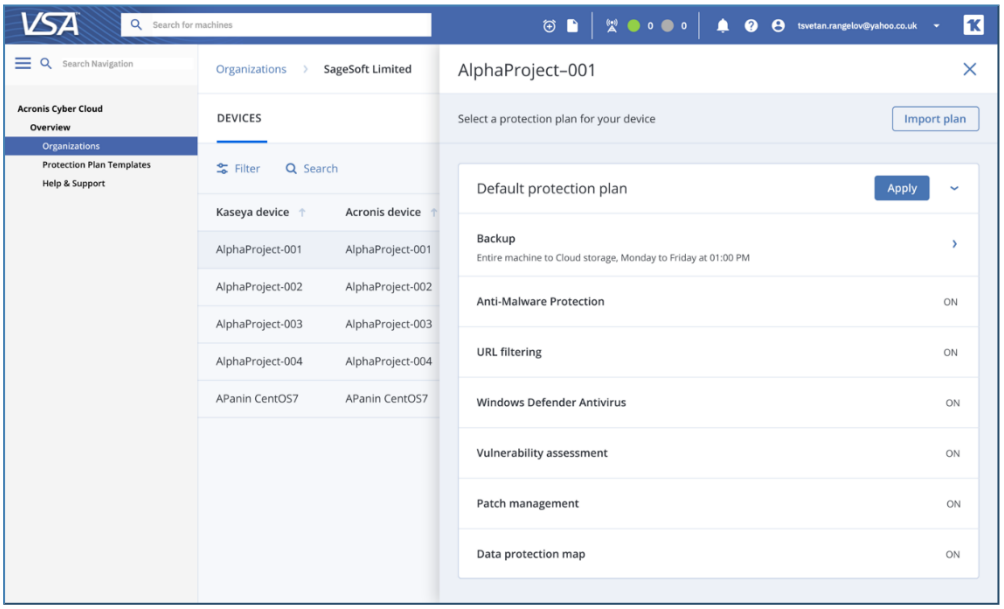


5. After you have imported the plan, you can make it the **Default Protection Plan**. Do this by clicking the ... three dots next to the plan row, then select **Set as default** from the pop-up menu. As described above, the default protection plan is the one applied when the **Apply default plan on new devices automatically** option in **Organizations** > **Settings** is activated.



Importing plans from the device side menu

1. Go to the **Acronis Cyber Protect** module in Kaseya VSA.
2. Navigate to **Organizations**.
3. Choose an organization, then select a device.
4. On the side panel that appears next, click **Import plan**.



5. Select an Acronis customer, then a protection plan.
6. After the plan is imported, it will be available for all organizations in your Kaseya VSA module.
7. You can set the plan as the default one by clicking on the ... three dots next to the plan row, then select **Set as default** from the pop-up menu.

As described above, the default protection plan is applied when the **Apply default plan on new devices automatically** option in **Organizations** > **Settings** is activated.

How to Create a Custom Protection Plan

You can create your own plans in the **Plans** section of the Acronis Management portal.

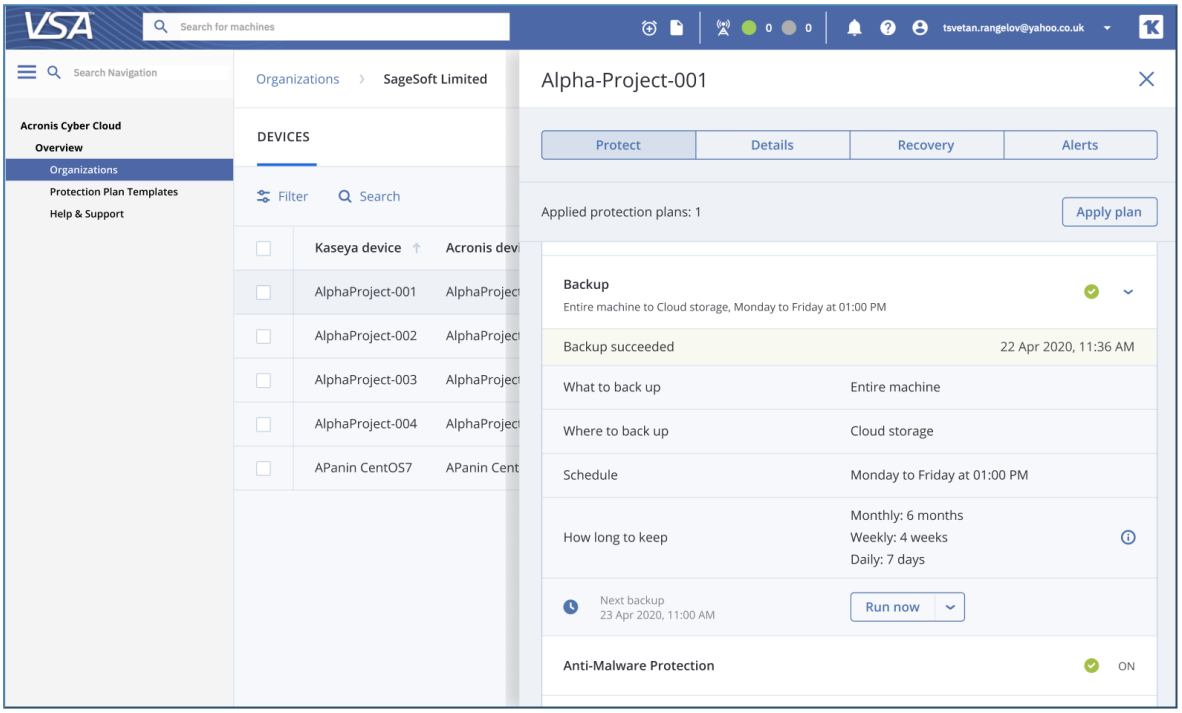
Any protection plan created in the portal becomes immediately available for import in the Kaseya VSA interface.

For more information about the protection capabilities, refer to the Acronis Cyber Protect documentation.

Operations with Protection Plans

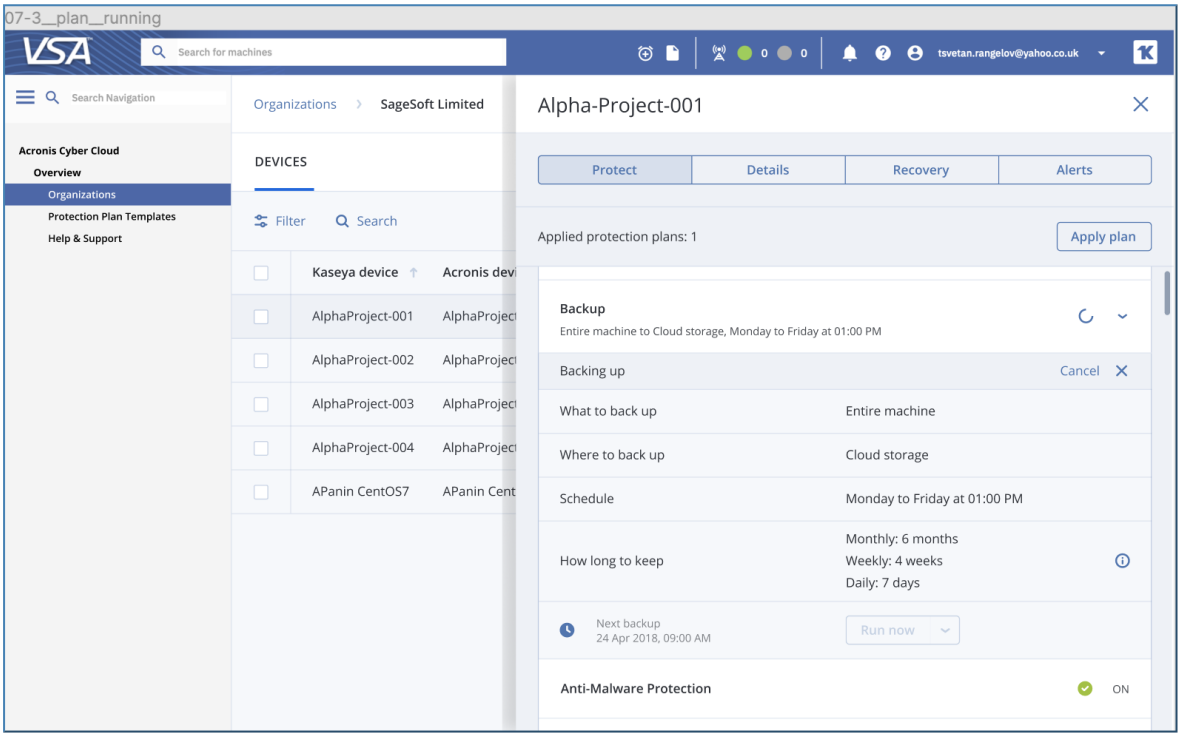
Manually start a non-scheduled backup

1. Click on the device you want to back up.
2. If more than one plan has been assigned to a device, you will need to select the one you want to manually run the backup for.
3. Expand the **Backup** section and click **Run now**.



Manually stop a running backup

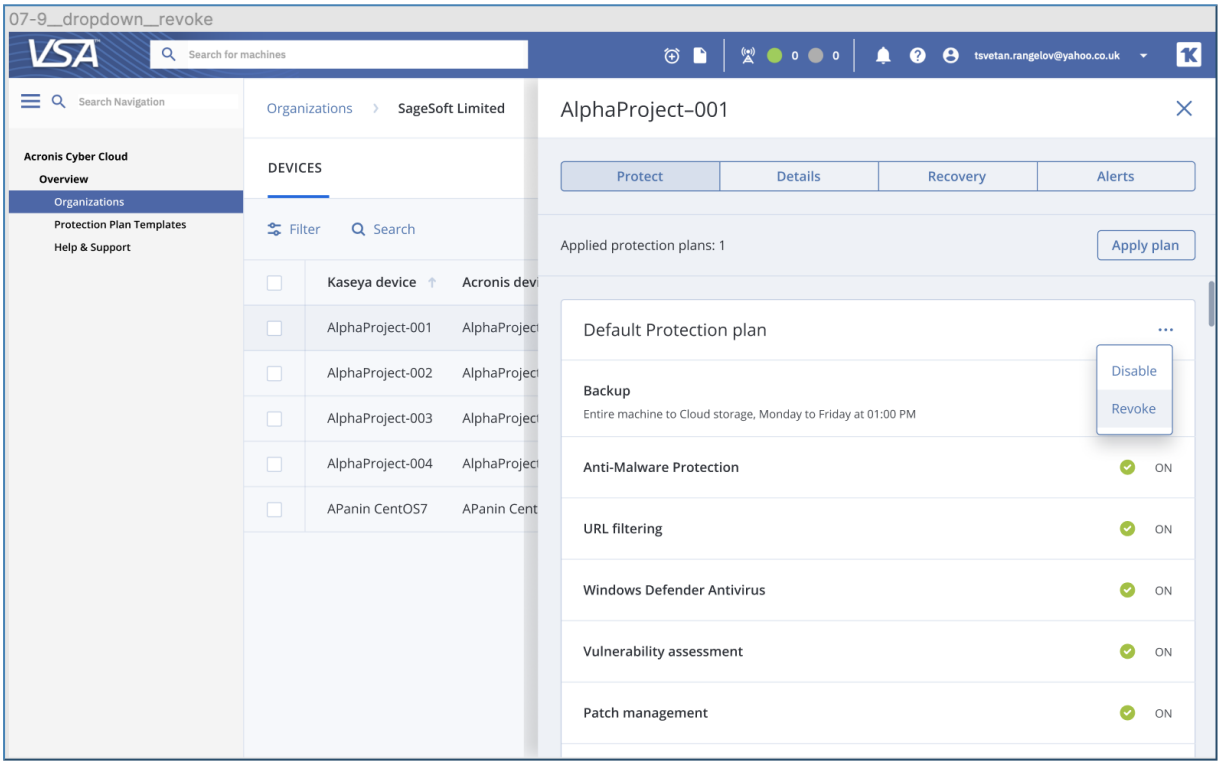
1. Double-click a device with a backup in progress.
2. Select the protection plan that shows a **Backing up** status.
3. Click **Cancel** to stop the currently running backup process and remove the incomplete backup file from storage. The next backup will run as scheduled.



Revoke a protection plan

1. Double-click the device you want to revoke the protection plan for.
2. Select the protection plan you want to revoke.
3. Click on the **...** three dots to invoke the pop-up menu.
4. Select **Revoke** from the available options.

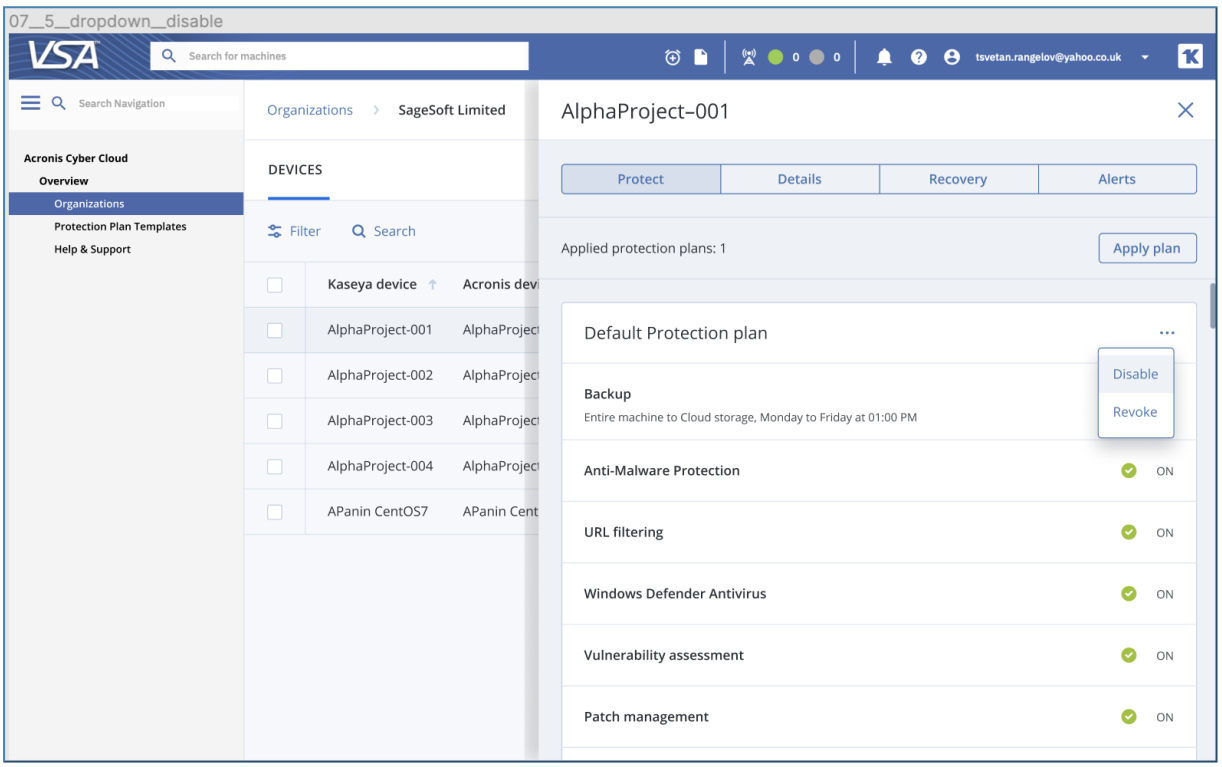
The selected plan will be revoked. Any other plans, applied to this device, will continue to run as scheduled.



Disable a protection plan

1. Double-click the machine.
2. Select the protection plan you want to revoke.
3. Click on the three dots **...** to invoke the pop-up menu.
4. Select **Disable** from the available options.

You can always enable a previously disabled plan.

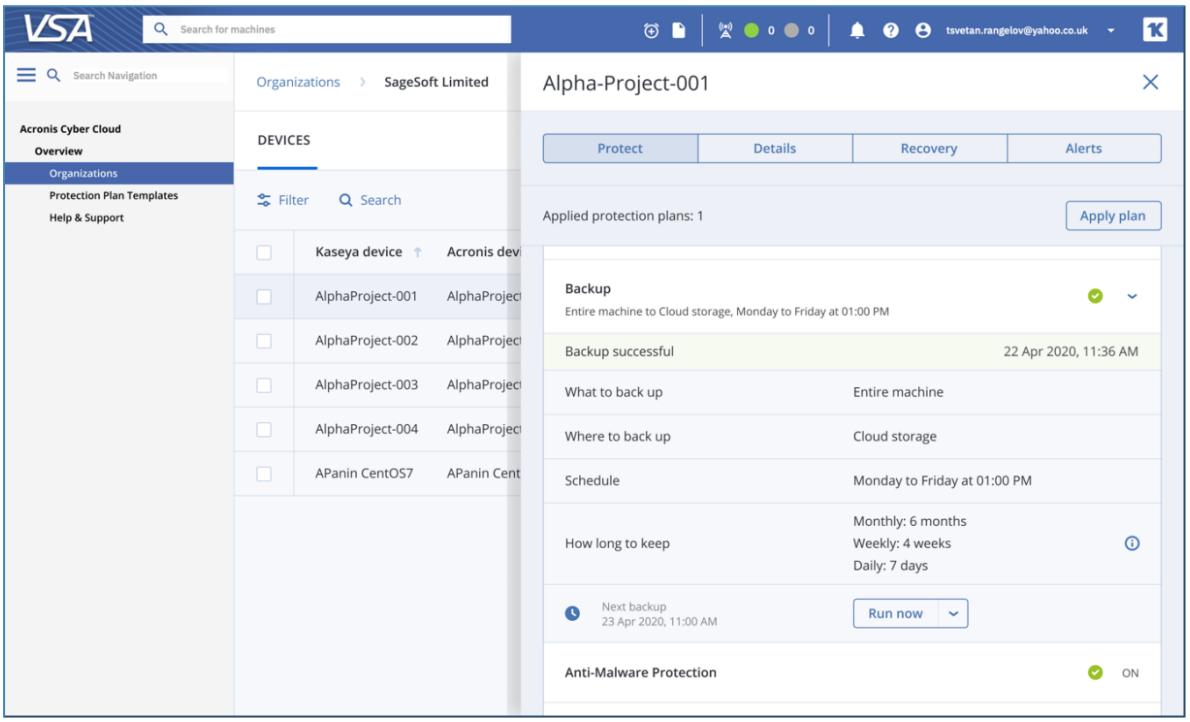


Monitoring Backup and Protection Status

Monitoring at customer or machine level

For each machine that has a backup module enabled in the protection plan, the following parameters can be tracked from the side menu **Protect** tab:

- The last backup date and time
- The next backup date and time

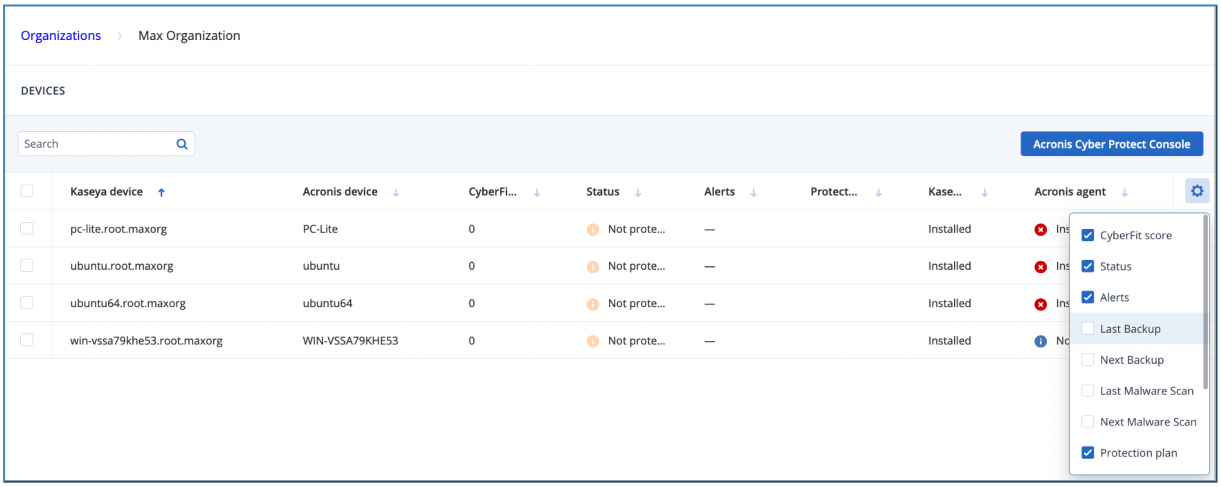


Monitoring in the Devices table

For every device that has a backup module enabled in the protection plan, some parameters can be monitored in the **Devices** table per customer.

To set which device protection statuses to be visible (and appear as columns in the table):

1. Click on the icon in the top right corner of the table.
2. In the drop-down list that opens, check the boxes of the parameters that you want to track:
   - **Kaseya device**
   - **Acronis device**
   - **CyberFit score**
   - **Status**
   - **Alerts** - number of active alerts for each device
   - **Last/Next backup** - last/next backup date and time
   - **Last/Next malware scan** - last/next malware scan date and time
   - **Protection plan** - name of currently applied protection plan
   - **Kaseya agent** - agent version
   - **Acronis agent** - agent version
   - **IP address**



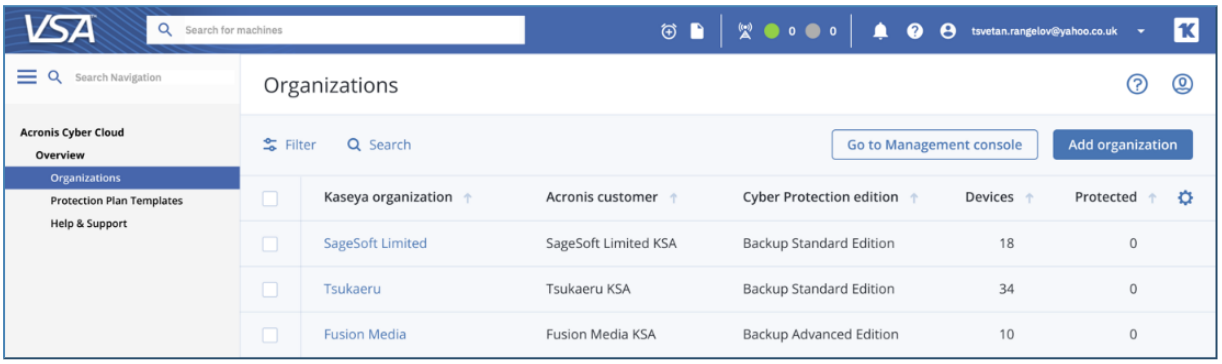
For further information, go to the **Acronis Cyber Protect Console** by clicking on the corresponding button. The console will then open on behalf of the Administrator user.

Important

For customer tenants created via the integration, an Administrator user account is created automatically with 2FA option switched off. If the existing customer tenant was mapped to a Kaseya VSA organization, verify that the 2FA option for its Administrator user account is turned off in order for the **Acronis Cyber Protect Console** link to work properly.

Monitoring in the Organizations table

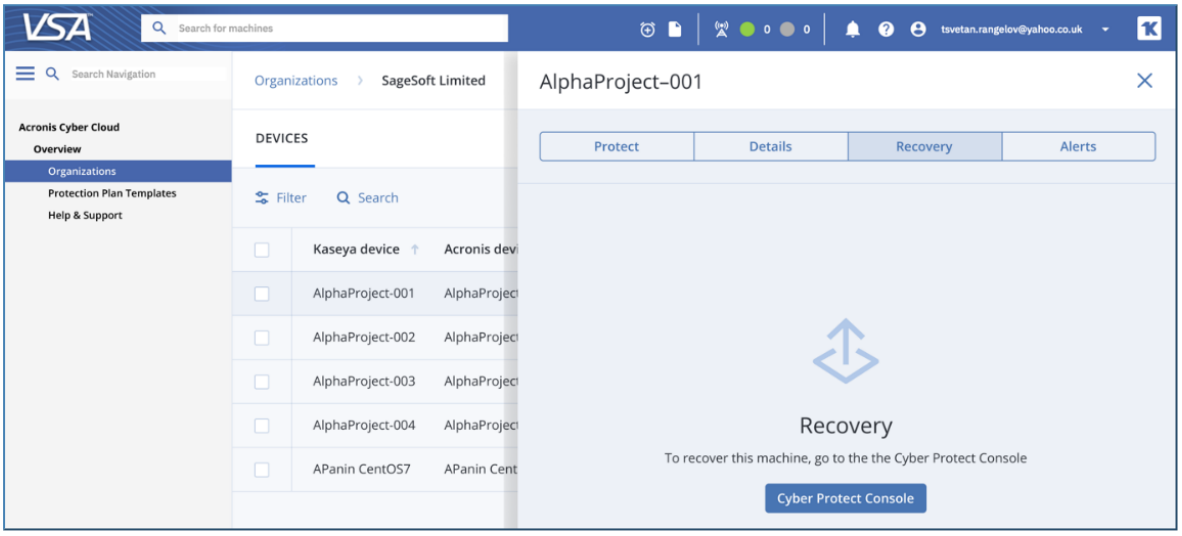
For each customer, you can see the total number of devices available as well as how many of them are **Protected**. A device is considered 'protected' if it has both an Acronis Cyber Protection agent installed and a protection plan applied.



Recovery

To recover data to a device:

1. Double-click the device you would like to recover.
2. On the side panel that opens next, click **Recovery**. This will take you to the Acronis Management portal and the recovery points for this device will be displayed.



3. Follow the instructions in the Acronis Cyber Protect Help about:
   a. File recovery
   b. Device recovery

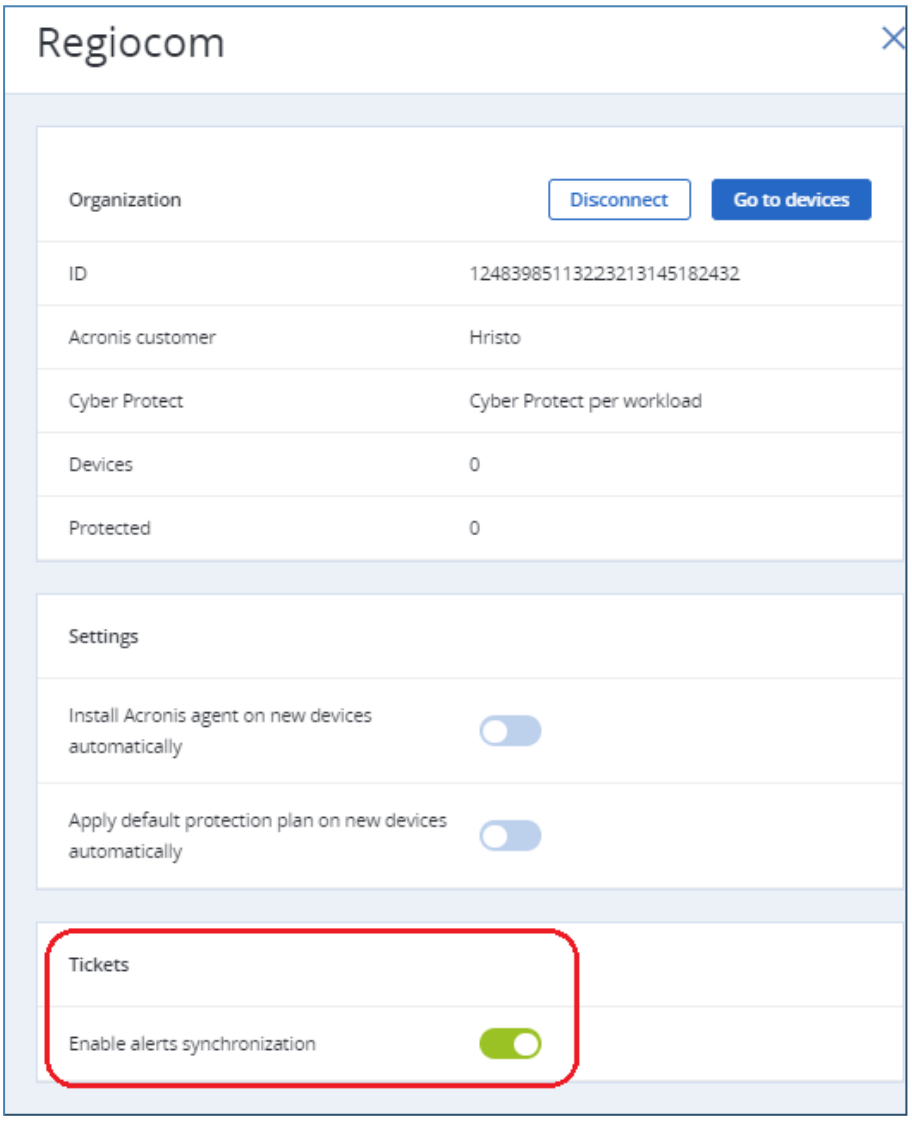
Ticketing

Acronis alerts generate tickets in your favorite Kaseya ticketing solution:

- **Ticketing** tab in Kaseya VSA
- **Service Desk** in Kaseya VSA
- **Service Desk** in Kaseya BMS

There are two ways to switch on and off the alerts synchronization:

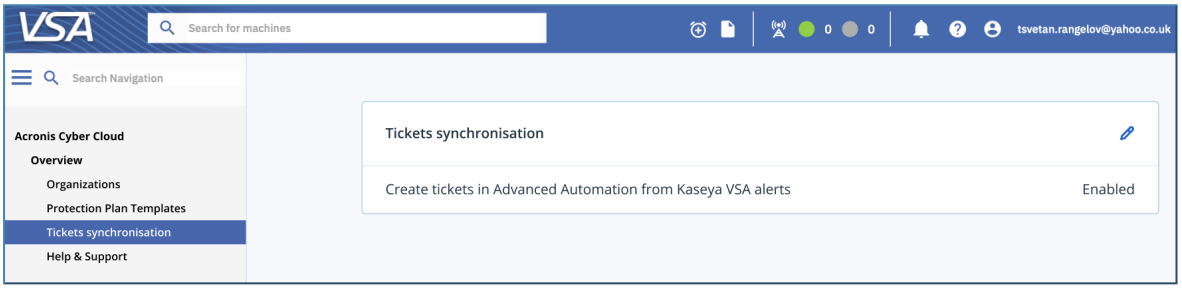
- when creating or linking Acronis customers
- by modifying the settings of an existing organization



Kaseya alerts to Advanced Automation tickets sync

Kaseya VSA alerts can be pushed into Advanced Automation tickets as long as the Advanced Automation service has been enabled for a partner:

1. From the Kaseya VSA left-pane menu, select the **Ticket synchronisation** tab.
2. Click the pencil icon in the top-right corner to enable editing of the **Ticket synchronisation** section.



3. Use the **Create tickets in Advanced Automation from Kaseya VSA alerts** checkbox to turn this option on and off.

Troubleshooting

If there is an issue that requires you to create a ticket:

1. Go to the **Help & Support** page and click on **Get support**.
2. You will be redirected to the Support portal, from where you can file your ticket.

In general, two types of logs may be necessary:

- Procedure logs
  To get those, hover the mouse pointer over the green dot in front of any device. A modal window will open where you'll find a link to the Procedure logs.
- Acronis agent logs
  The procedure that describes how to get these can be found at:
  https://kb.acronis.com/content/54608