

Acronis Cyber Cloud

Integration with ConnectWise Asio

Table of contents

Introduction	3
Future functionality	3
Terminology	3
Prerequisites	4
Enabling the integration	5
Mapping customers	8
Installing the Cyber Protection agent for Windows and Linux	10
Uninstalling the Acronis Cyber Protection agent	14
Monitoring	15
Ticketing	16
View ticket details	17
DR runbooks	18
Prerequisites	18
Steps in Asio	18
Disabling the integration	19
Index	20

Introduction

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

The integration enables Managed Service Providers (MSPs) to:

- Deploy agents to Windows x32/x64 and Linux devices.
- Monitor protected devices from the Acronis integration dashboard.
- Get tickets based on Acronis alerts.
- Schedule a DR failover test and review the results.

This functionality belongs to ConnectWise Asio, so you don't have to use the Acronis Cyber Protect web interface.

The Acronis integration for ConnectWise Asio is vital for MSPs who want to use ConnectWise Asio's NOC functionality. Tickets created by the integration can be set up to be automatically assigned to and processed by the NOC team.

Future functionality

The following scenarios are not (yet) supported by the current integration version. They will be covered in future versions of ConnectWise Asio.

- Agent deployment to macOS devices and Domain Controllers.
- Protection plans management.
- Task management.
- Customer provisioning.

Terminology

- **MSP** - a Managed Service Provider, who uses both ConnectWise Asio and Acronis Cyber Protect
- **Customer** - a client of the MSP
- **Customer tenant** - the account of a Customer in Acronis Cyber Cloud
- **Site** - the account of a Customer in ConnectWise Asio

Prerequisites

ConnectWise Asio prerequisites

- A ConnectWise Asio account, fully configured with sites and endpoints.

Acronis prerequisites

- [Optional] Acronis deployed on the endpoints you want to protect.
- At least one fully configured Acronis Cyber Cloud account, with at least one customer tenant.
- The user account that you use to configure the integration must be a Company Administrator.
- 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

- You must not have disabled support access.

Note

For more information, see [the Management Portal Partner Administrator guide](#).

Enabling the integration

For integrations that have never been enabled before, find instructions on how to do this at:

Acronis Cyber Cloud > Management portal > Integrations catalog page > CW Asio tile > Configure button:

The ConnectWise Asio integration is currently not active. To enable it, follow the below steps:

- 1 Set up the API Client:**
 - Go to Acronis > Settings > API Clients.
 - Create an API Client for the integration.
 - Copy and save the Client ID, Secret and Datacenter URL.
- 2 Go to the ConnectWise Asio site and log in as an administrator.**
- 3 Activate the Acronis integration:**
 - Go to ConnectWise Asio > Settings > Integrations.
 - Click Acronis Cyber Protect.
 - Complete the Acronis Cyber Protect activation wizard. Use the API Client credentials generated in step 1c.

Full documentation with step-by-step guide is available at:
<https://www.acronis.com/en-us/support/documentation/ConnectWiseAsio>

To activate the integration, follow the below steps:

- Go to **Acronis Cyber Cloud > Settings > API Clients**.
- Click **Create API Client** in the top right corner.
- In the **Create API client** window, provide a name of your choice and click **Next**.

Create API client

Name

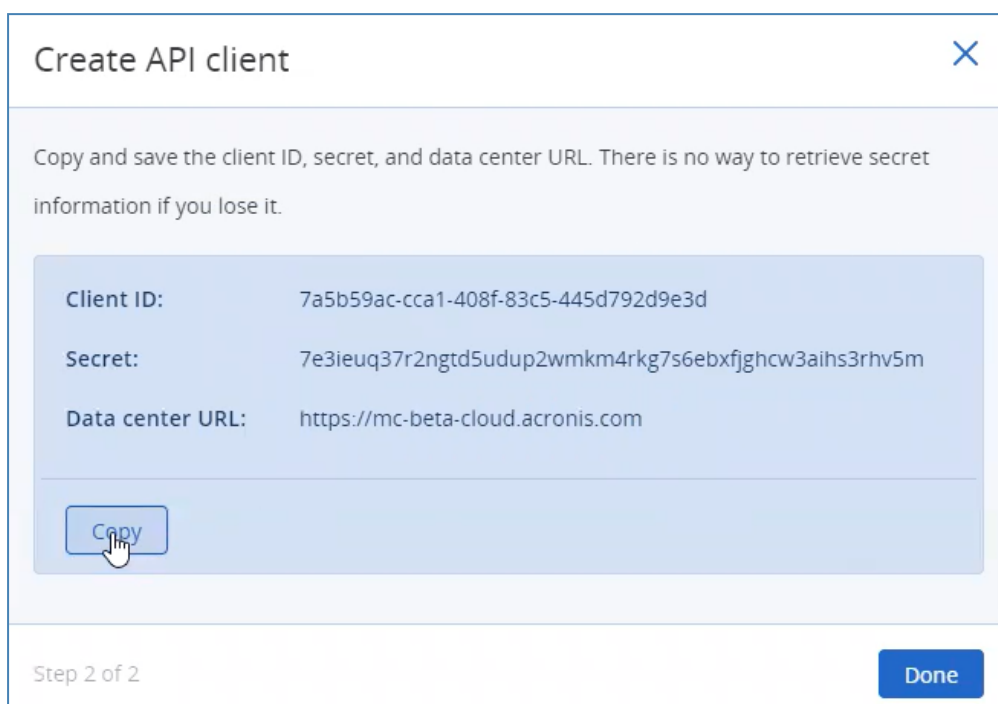
Asio demo

The API client will have the same privileges as your account has

Step 1 of 2

CancelNext

4. The newly generated credentials will be displayed:

A screenshot of a 'Create API client' window. The window has a title bar with a close button (X). Below the title bar, there is a light blue box with the text: 'Copy and save the client ID, secret, and data center URL. There is no way to retrieve secret information if you lose it.' Below this box, there is a light blue box containing the following information: 'Client ID: 7a5b59ac-cca1-408f-83c5-445d792d9e3d', 'Secret: 7e3ieuq37r2ngtd5udup2wmkm4rkg7s6ebxfjghcw3aihs3rhv5m', and 'Data center URL: https://mc-beta-cloud.acronis.com'. Below this box, there is a 'Copy' button with a hand icon pointing to it. At the bottom of the window, there is a 'Step 2 of 2' indicator and a 'Done' button.

Create API client

Copy and save the client ID, secret, and data center URL. There is no way to retrieve secret information if you lose it.

Client ID: 7a5b59ac-cca1-408f-83c5-445d792d9e3d

Secret: 7e3ieuq37r2ngtd5udup2wmkm4rkg7s6ebxfjghcw3aihs3rhv5m

Data center URL: https://mc-beta-cloud.acronis.com

Copy

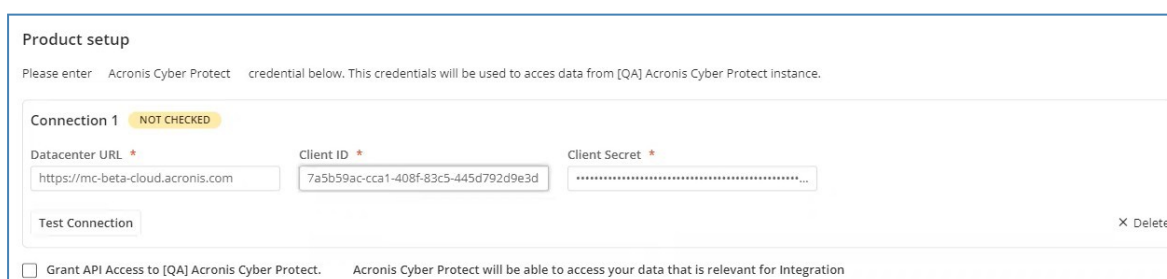
Step 2 of 2 Done

In the same window, click **Copy**, then **Done**. This will save the **Client ID**, **Secret** and **Datacenter URL**.

Note

The Client secret will not be displayed anymore once you close this window.

5. Use these credentials to log in to the CW Asio site as an administrator.
6. Go to **ConnectWise Asio > Settings > Integrations**.
7. Click **Acronis Cyber Protect**.
8. On the **Product setup** page, complete the activation wizard with the credentials from step 4:

A screenshot of the 'Product setup' window. The window has a title bar. Below the title bar, there is a light blue box with the text: 'Please enter Acronis Cyber Protect credential below. This credentials will be used to access data from [QA] Acronis Cyber Protect instance.' Below this box, there is a 'Connection 1' section with a 'NOT CHECKED' status. This section contains three input fields: 'Datacenter URL' with the value 'https://mc-beta-cloud.acronis.com', 'Client ID' with the value '7a5b59ac-cca1-408f-83c5-445d792d9e3d', and 'Client Secret' with a masked value '*****'. Below these fields, there is a 'Test Connection' button and a 'Delete' button (X Delete). At the bottom of the window, there is a checkbox labeled 'Grant API Access to [QA] Acronis Cyber Protect.' and a text label 'Acronis Cyber Protect will be able to access your data that is relevant for Integration'.

Enter **Datacenter URL**, **Client ID** and **Client Secret**.

9. Use the **Test Connection** button to verify that connection can be established successfully. Click **Delete** to break this connection without deleting the already generated API Client credentials. Clicking **Cancel** will only close this window.

10. Select the **Grant API access to Acronis Cyber Protect** checkbox. This will generate API Asio credentials in the backend and enable Acronis Cyber Protect to access the relevant data. If reset for some reason, new credentials of this type can be easily obtained by using the **Regenerate** option.
11. Click **Save and Proceed**.

After enabling the integration, you will be able to see the following page in the Acronis platform:

General	
Integration status	✔ Success
Activation date	9/22/2022, 4:11:15 PM
ConnectWise Asio site	https://openapi.use1.cwvendorintprod.cwnet.io
ConnectWise Asio Client ID	4d45e791c89afe79becbacf8a54347f6
Linked accounts	3

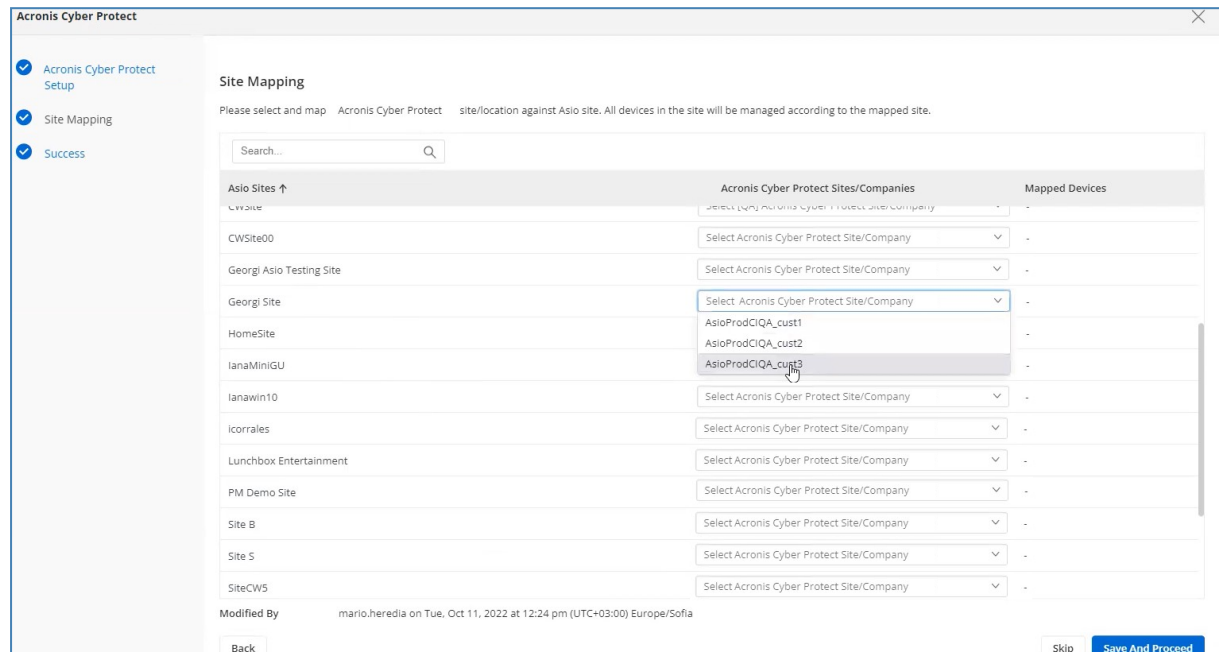
Ticket synchronization	
Last Sync	9/23/2022, 1:08:53 PM
Status	✔ Success

Device status synchronization	
Last Sync	9/23/2022, 1:08:40 PM
Status	✔ Success

It represents a summary where you can track the last synchronizations regarding device statuses and ticket creation. You can also check when the integration has been enabled. The Linked accounts are the number of Asio sites mapped to Acronis clients.

Mapping customers

The next step is to map existing Asio sites to Acronis Customer tenants.



1. Make sure that you are logged in with your Acronis partner tenant account.
2. After successful integration setup, you will be redirected to the Asio **Site Mapping** page to map existing sites to Acronis Customer tenants.

Important

Only service provider-managed customers are available for mapping i.e. ones with the **Enable self-managed customer profile** option turned off and with the **Support access** setting turned on.

3. On this page, find the below information, presented in a three-column table:
 - a. Existing Asio sites
 - b. Acronis Cyber Protect sites
 - c. Mapped devices
4. To map one or more sites to an Acronis Customer tenant, do the following:
 - a. Browse the list of sites in the table to locate the one(s) you want to map.
 - b. Expand their corresponding drop-down lists and make your selections.
5. Click **Save and Proceed**.

If the mapping is correct, you will see a success message.

To edit an existing mapping:

1. Return to the main **Integrations** page.
2. Click the same product again.
3. Click **Proceed** to navigate back to the **Site Mapping** page.
4. Edit the mapped row.
5. Click **Save and Proceed**.

Installing the Cyber Protection agent for Windows and Linux

To deploy the Acronis Cyber Protection agent on Windows and Linux machines, you have to create an Acronis **policy**, then a **package** with the policy created, assign this policy to sites and finally activate it.

Note

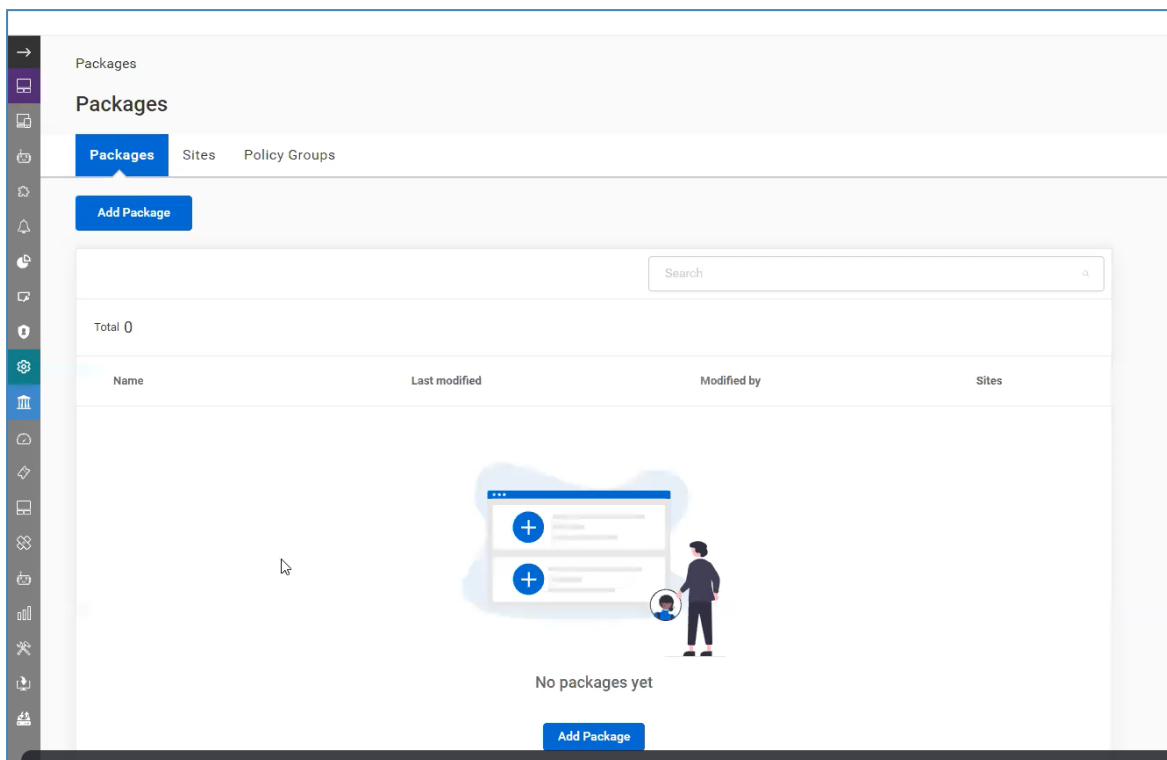
A package with the corresponding policy is created only once, so in order to install the Acronis Cyber Protection agent, next time it will be enough just to assign the respective site to the package.

1. On the Asio site, go to **Policies > Add Policy**.
2. Define the following parameters:
 - a. From the **Category** drop-down list, select **Devices**.
 - b. From the **Type** drop-down list, select **Acronis installation agent**.
 - c. In the **Name** field, enter **Acronis agent deploy**.

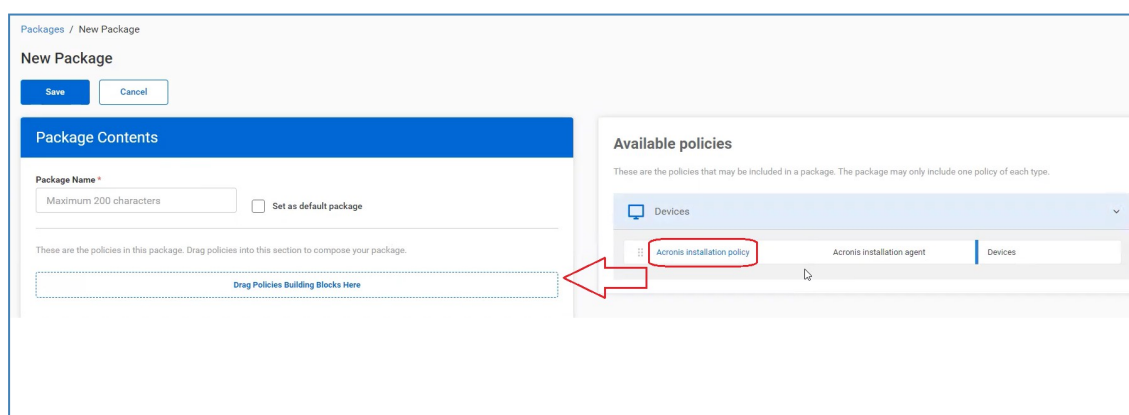
The screenshot shows the 'Policies / New policy' interface. The title is 'Acronis agent deploy'. There are 'Save' and 'Cancel' buttons. The 'Summary' section contains three fields: 'Category' (set to 'Devices'), 'Type' (set to 'Acronis installation agent'), and 'Name' (set to 'Acronis agent deploy'). To the right, the 'Acronis installation agent Settings' section shows 'Acronis Cyber Protect Agent Installation' with a toggle switch set to 'disabled'.

3. Click **Save**.
4. On the Asio site, go to **Settings > Packages**.

5. Open the **Packages** tab and click **Add Package**.

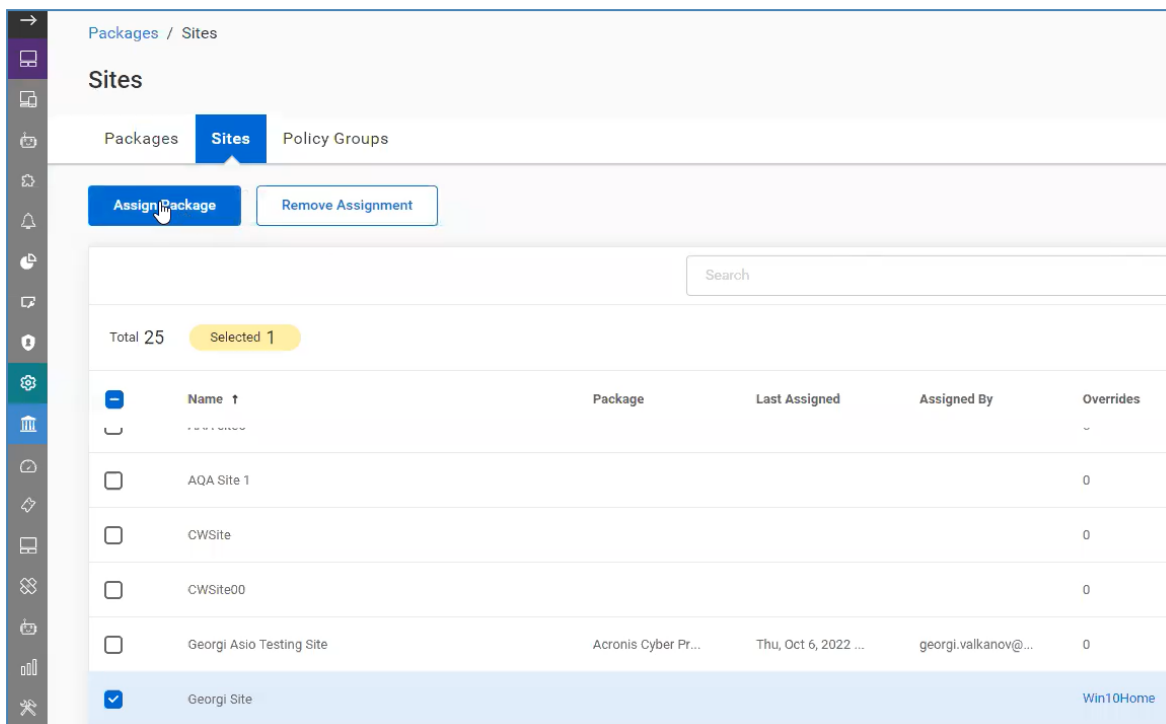


6. On the **New Package** page:
 - a. Provide a name for the new package.
 - b. Expand the **Devices** list in the **Available policies** block on the right. Then drag and drop the selected policy to the designated area on the left.

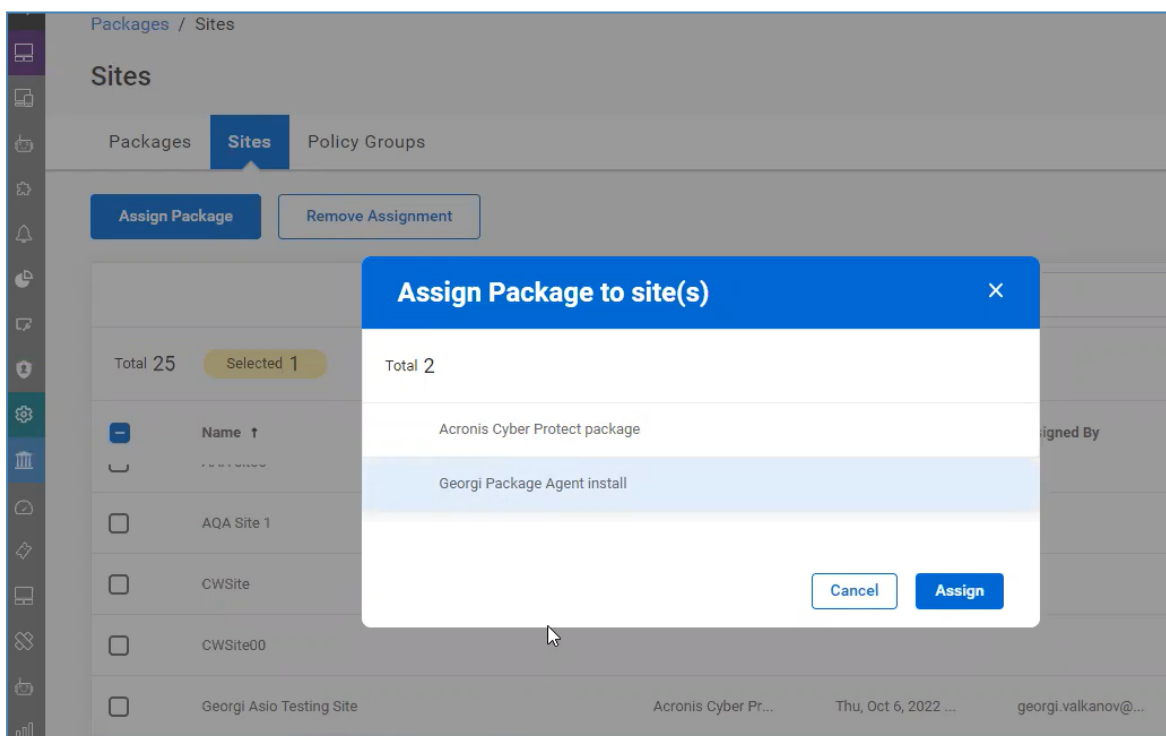


7. Click **Save**.
8. You should be able to see a "**Package was added successfully**" message.
9. On the **Packages** page, navigate to the **Sites** tab.

10. Select a site from the list and click **Assign Package**.

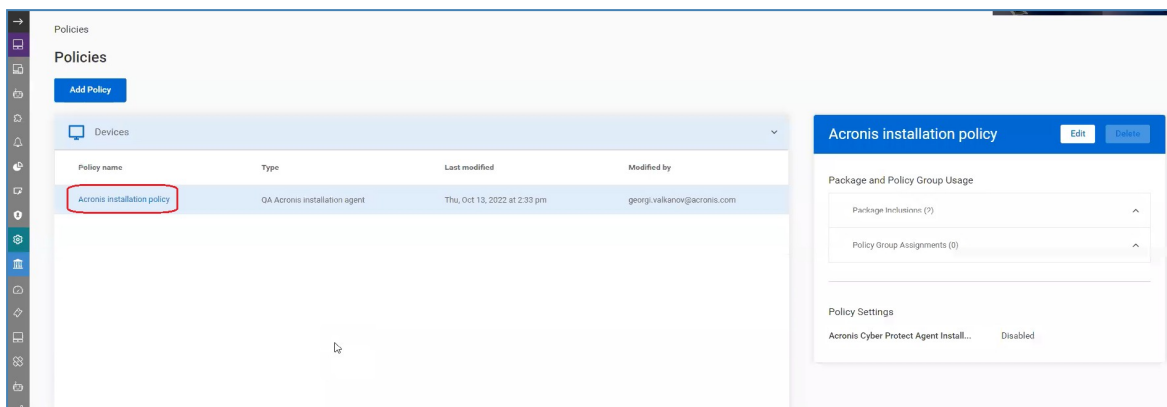


11. In the popup that opens, select a package and click **Assign**:



12. You should be able to see an "**Assignment(s) added successfully**" message.

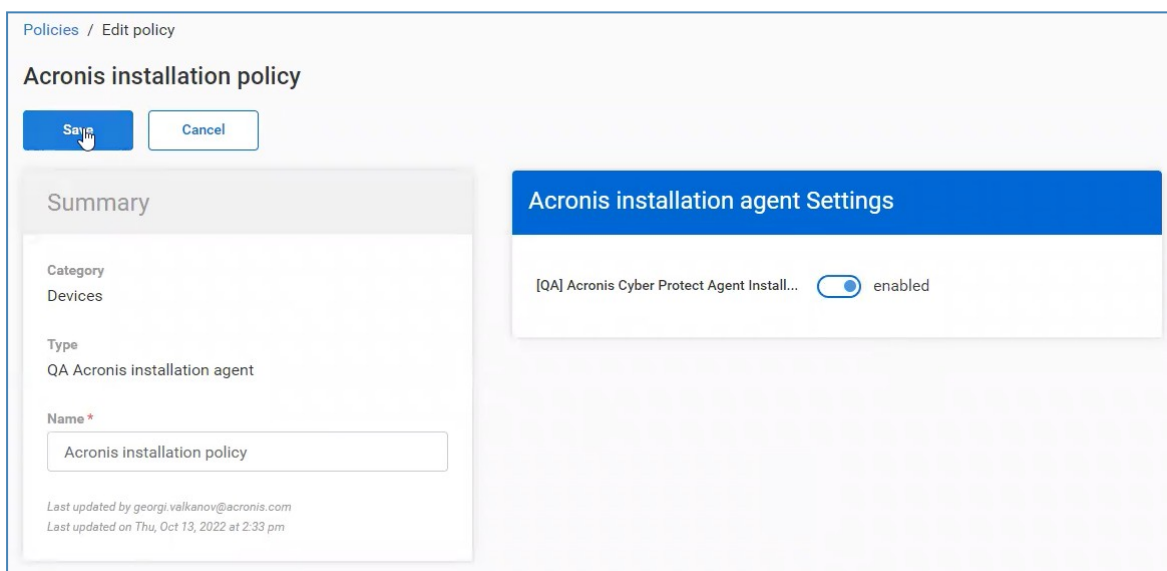
13. Go to **Policies**.



14. Click **Edit** on the policy you want to enable.

15. Switch the toggle button to **Enabled** mode.

16. Click **Save**.



17. A "**Policy was updated successfully**" message should be displayed.

This will trigger the installation of the Cyber Protection agent on all machines that belong to the selected site.

Uninstalling the Acronis Cyber Protection agent

To uninstall the Acronis Cyber Protection agent

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

1. Navigate to the Customer tenant > **Settings** > **Agents**.
2. Find the Acronis Cyber Protection agent in the list, and click on the row.
3. In the **Actions** panel that appears on the right, go to **Agent Update Settings**.
4. 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.

In ConnectWise Asio, disable the corresponding policy.

1. Go to **Policies** and select a policy to edit.
2. In the right panel, switch the toggle button to **disabled**:

Policies / Edit policy

Dev Acronis Cyber Protect Agent 1

Save Cancel

Summary

Category
Devices

Type
Dev Acronis Cyber Protect Agent

Name *
Dev Acronis Cyber Protect Agent 1

Dev Acronis Cyber Protect Agent Settings

Acronis Cyber Protect Agent Installation ☐ disabled

3. Click **Save**.

Note

To uninstall the Acronis Cyber Protection agent from all mapped devices, you can [disable the integration](#).

Monitoring

When you have mapped customers, the integration will automatically map endpoints in ConnectWise Asio to workloads in Acronis under the mapped Customer tenant.

For any mapped workload, you will see corresponding statuses in ConnectWise Asio.

The integration supports the following statuses:

STATUS NAME	VALUE
Agent version	Version of the currently installed agent
Protection status	<ul style="list-style-type: none"> <i>Unprotected</i> (Acronis agent is installed, but no protection plan applied) <i>Protected</i> (Acronis agent is installed and protection plan is applied)
Protection Plan	Name of the protection plan
Access Acronis Console	Link to the Acronis Management portal
Next backup	Date and time of next scheduled backup
Last backup	Date and time of last successful backup
Antivirus & Antimalware	Date and time of last antivirus scan

To view statuses, go to **Portal > Devices > Computers**, then open the drop-down menu under **Integrations** and choose **Acronis Cyber Cloud**.

Workstations & Servers								
Total 7 Filtered 0 Selected 0								
Run Manage								
Search for devices								
General Automation OS Patching Integrations BDR								
Acronis Cyber Protect								
	Name	Friendly Name	Device Type	Log In	Last User	Last Restart	Site Name	OS
<input type="checkbox"/>	SPP-WS-1	SPP-WS-1	Desktop (Virtual)		ja	Jul 22, 9:31 p...	AAA Design	10 Pro 2009
<input type="checkbox"/>	SPP-WS-3	SPP-WS-3	Desktop (Virtual)		ja	Jun 4, 10:34 a...	AAA Design	10 Pro 2004
<input type="checkbox"/>	DESKTOP-95P4HTP	DESKTOP-95P4HTP	Desktop		IRINA	Apr 30, 1:11 ...	PM Demo Site	10 Enterprise 2016 LTSB 16..
<input type="checkbox"/>	DD-win10x64-A	DD-win10x64-A	Desktop (Virtual)		admin	Jun 25, 9:22 a...	PM Demo Site	10 Pro 2009
<input type="checkbox"/>	DD-win10x64-C	DD-win10x64-C	Desktop (Virtual)		admin	Jun 18, 11:06 ...	PM Demo Site	10 Pro 2009
<input type="checkbox"/>	DESKTOP-4HV971T	DESKTOP-4HV971T	Desktop (Virtual)		Irina	Jun 30, 4:31 p...	PM Demo Site	10 Pro 2009
<input type="checkbox"/>	Virtual-PC	Virtual-PC	Desktop (Virtual)		Test-PC	Jun 30, 1:19 a...	PM Demo Site	8.1 Pro 6.3.9600

Ticketing

After [enabling the integration](#), tickets will be automatically generated in ConnectWise Asio for the following alert types:

- Activity failed
- Activity is not responding
- Active Protection service is not running
- An error occurred while setting up the disaster recovery infrastructure
- Agent is outdated
- Automatic update has failed
- Backup failed
- Backup recovery failed
- Backup is corrupted
- Backup is missing
- Backup is not responding
- Backup did not start
- Backup succeeded with warnings
- Backup status is unknown
- Backup stopped
- Cannot protect a device with assigned Quota
- Cannot protect a device with assigned license
- Cloud servers quota is exceeded
- Compute points quota is exceeded
- Continuous Data Protection failed
- Cryptomining activity is detected
- Cyber Protection (or Active Protection) service is not responding
- Device quota reached
- Disk failure is imminent
- Encryption password is missing
- Failback error
- Failback error: data transfer failed
- Failback error: switchover failed
- Failback confirmation failed
- Failed to reconnect the workload to the network
- Failed to isolate the workload from the networks
- Failed to migrate the backups in the cloud storage to the new format
- Failed to run machine from backup
- Hyper-V hosts configuration is not valid
- Incident detected

- Machine is offline for more than 20 days
- Machine is offline for more than 30 days
- Quota reached
- Storage quota exceeded
- Subscription license has expired
- The device has no quota to apply a protection plan
- Unauthorized operation is detected and blocked
- Validation failed

To be able to view the tickets, it is necessary for you to have selected at least the following:

RMM Setup > Sites using RMM > Site you want to view tickets for > Product Options > Essential service level.

View ticket details

To see more detailed information for a particular ticket:

1. Open the **Ticket** view of the Acronis backup console.
2. Go to **ConnectWise RMM > Tickets**.
3. Select a ticket, generated by Acronis.
4. Click the **Login on behalf of user** button.

Tickets will be automatically updated after alert resolution:

- If NOC services are enabled for the partner and depending on whether the NOC operator has accepted the corresponding ticket:
 - if yes, then the ticket will be marked as **NOC completed**;
 - if not yet, then the ticket will be closed.
- if NOC services are disabled for the partner:
 - the ticket will be closed.
- Before closing the ticket, the integration will check for running tasks:
 - if an alert is cleared and there are no running tasks, the integration will close the corresponding ticket.
 - if an alert has running tasks, the integration will not close the corresponding ticket during the current sync.

DR runbooks

DR runbooks support scheduling a DR failover test and reviewing the results from a scheduled failover test.

Important

- DR runbooks in Asio are independent from DR runbooks in Acronis.
 - Any DR runbook scheduled in Asio will run on the Acronis data center.
-

Prerequisites

- Acronis is deployed.
- Acronis Standard Disaster Recovery and/or Advanced Disaster Recovery services are enabled.
- Device is backed up.
- A recovery server is created.
- A recovery point is created.
- VPN is configured.

Steps in Asio

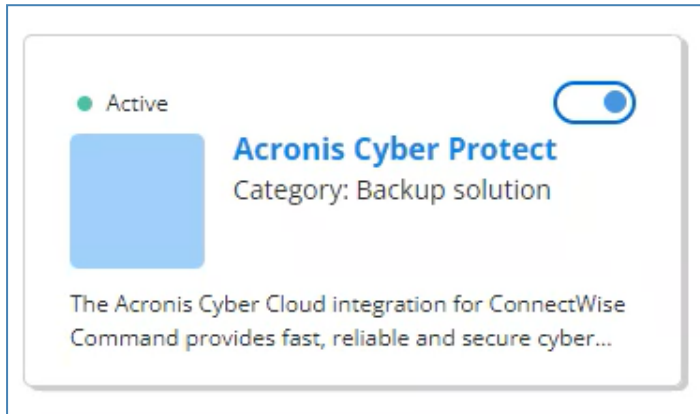
To schedule a DR runbook in Asio

1. In ConnectWise Asio, go to **DATA PROTECTION > DR Test**.
2. Click **Add DR Test**.
3. Configure the mandatory fields.
4. Click **Next** and follow the instructions on the wizard.
When the test is scheduled, it appears in the list. The status indicates progress.
5. When the test status changes to **Completed**, click the name of the test to review results.
6. Go to the Acronis console.
7. Go to the running DR server.
8. End the test and shut down the DR server.

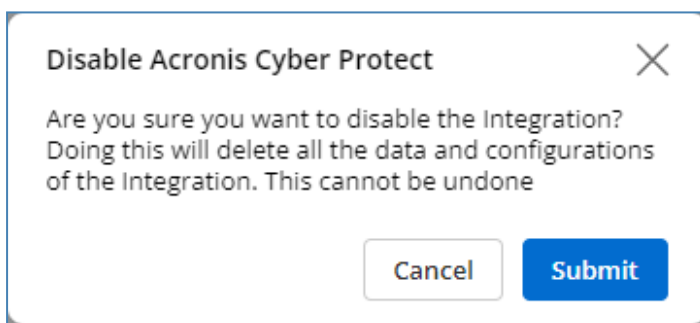
Disabling the integration

If you eventually decide that you don't need this integration anymore, you can disable it. To do so:

1. Go to **ConnectWise Asio > Settings > Integrations**.
2. Locate the **Acronis Cyber Protect** tile and switch off the toggle button in the upper right corner.



3. In the popup that opens, confirm the deactivation by clicking **Submit**:



As a result, the integration will be disabled.

Note

This action will uninstall the Acronis Cyber Protection agent from all devices set up in your Acronis account. You will also no longer be able to monitor workloads, deploy the Acronis agent automatically or receive tickets in Asio.

Index

D

Disabling the integration 19

DR runbooks 18

E

Enabling the integration 5

F

Future functionality 3

I

Installing the Cyber Protection agent for
Windows and Linux 10

Introduction 3

M

Mapping customers 8

Monitoring 15

P

Prerequisites 4, 18

S

Steps in Asio 18

T

Terminology 3

Ticketing 16

U

Uninstalling the Acronis Cyber Protection
agent 14

V

View ticket details 17