

Acronis Cyber Cloud

Integration with Jamf Pro

Table of contents

Introduction	3
Terminology	4
Prerequisites	5
Configuration	6
How the integration works	7
Setup	8
Permissions and roles	8
Creating an integration user	8
Enabling the integration	9
Deploying Acronis on macOS computers	11
Monitoring protected computers	12
Editing accounts	13
Editing accounts	13
Removing accounts	13
Reporting open alerts	15
Example of how to monitor failed backup alerts	16
Disabling the integration	17

Introduction

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

Once setup, the integration enables MSPs to:

- Deploy Acronis on macOS computers
- Monitor protected computers based on Jamf's Extension Attributes

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

As an MSP, you can manage any number of Jamf Pro accounts, using a single Acronis account. Each Jamf Pro account will be mapped to a separate customer tenant under your Partner account and will appear connected in the integration Account list.

Terminology

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

Prerequisites

To use this integration, you should have:

- At least a single fully configured Jamf Pro account
- At least one smart or static group for queuing computers for deployment
- An Acronis Cyber Cloud account with the following characteristics:
 - at least a single setup customer tenant
 - optionally, a minimum of one protection plan, configured to be used as the default one
- Optionally, Acronis deployment on any macOS computers you want to protect

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

Configuration

The Jamf Pro integration is entirely Acronis-hosted. You don't need to install or manage any additional software but only to enable and configure it.

The following items will be created in your Jamf Pro instance:

- Computer Policy - required for installation and registration of the Acronis agent on macOS computers
 - Acronis - Install Acronis Cyber Protection Agent
- Scripts - required for installation, uninstallation and plan management
 - Acronis - Install Acronis Cyber Protection Agent
 - Acronis - Uninstall Acronis Cyber Protection Agent
 - Acronis - Update Acronis Cyber Protection Agent
- Configuration Profiles - required for installation and registration of the Acronis agent on macOS computers
 - Acronis Cyber Protection Profile v1
 - Acronis Cyber Protection Profile v2
- Extension attributes - used for monitoring of the computer status and alerts
 - Acronis - Agent status* - used for agent installation and registration
 - Acronis - Agent version
 - Acronis - Last antimalware scan
 - Acronis - Last backup
 - Acronis - Next antimalware scan
 - Acronis - Next backup
 - Acronis - Protection Plan
 - Acronis - Protection Status
- Smart groups - required to automate installation of the Acronis agent on macOS computers
 - Acronis - Awaiting Agent Installation
 - Acronis - Configuration Profile v1
 - Acronis - Configuration Profile v2
- Advanced computer searches in Search inventory - these are preconfigured groups for monitoring of computer statuses
 - Acronis Protected Computers
 - Acronis - Backups missed for more than 3 days

All artefacts, created by the integration, are clearly labelled as Acronis-owned and their names start with the company name.

Policies, scripts, configuration profiles, smart groups and *Agent status* extension attributes are required by the integration, whereas Advanced computer searches and remainder of extension attributes are provided only for your convenience and can be edited or even removed as necessary.

How the integration works

The integration requires a single smart or static group that queues computers for deployment of the Acronis agent. The choice of a group type depends on your deployment strategy.

The integration then creates an Acronis - Awaiting Agent Installation smart group, which queues computers for deployment of the agent using the Acronis - Agent status Extension Attribute as criteria.

The Acronis - Install Acronis Cyber Protection Agent policy will execute the agent installation script for all computers in the queue on each recurring check-in.

During installation, the Acronis agent will be deployed on the computer, the computer - registered with the Acronis Cloud and, if configured, a default protection plan will be applied.

Once the installation is successful, an inventory recon will be performed and the Acronis - Agent status Extension Attribute will be populated. This removes the computer from the installation queue.

Once Acronis is deployed to a computer, the integration will periodically update a set of Extension Attributes with status information for every protected device.

These extension attributes can be used to search, filter and group computers, according to your monitoring and troubleshooting needs.

Setup

The integration setup consists of two main parts:

- Creating a user in your Jamf Pro account to be used by the integration to access Jamf Pro
- Enabling and configuring the integration

Permissions and roles

Only partner tenant users with Company Administrator roles are allowed to enable/disable or edit the integration.

All other users have Read-only access. This means that they can view, but not modify the integration settings.

Creating an integration user

First, you have to create a dedicated Jamf Pro user for the integration. This user will serve only for the purposes of the integration and should have only the following permissions enabled:

Jamf Pro Server Object	Create	Read	Update	Delete
Advanced Computer Searches	✓	✓	✓	✗
Computers	✗	✓	✓	✗
Computer Extension Attributes	✓	✓	✓	✓
macOS Configuration Profiles	✓	✓	✓	✗
Policies	✓	✓	✓	✗
Scripts	✓	✓	✓	✗
Smart Computer Groups	✓	✓	✓	✗
Static Computer Groups	✓	✓	✓	✗
User	✗	✗	✓	✗
User Extension Attributes	✓	✓	✓	✓

Enabling the integration

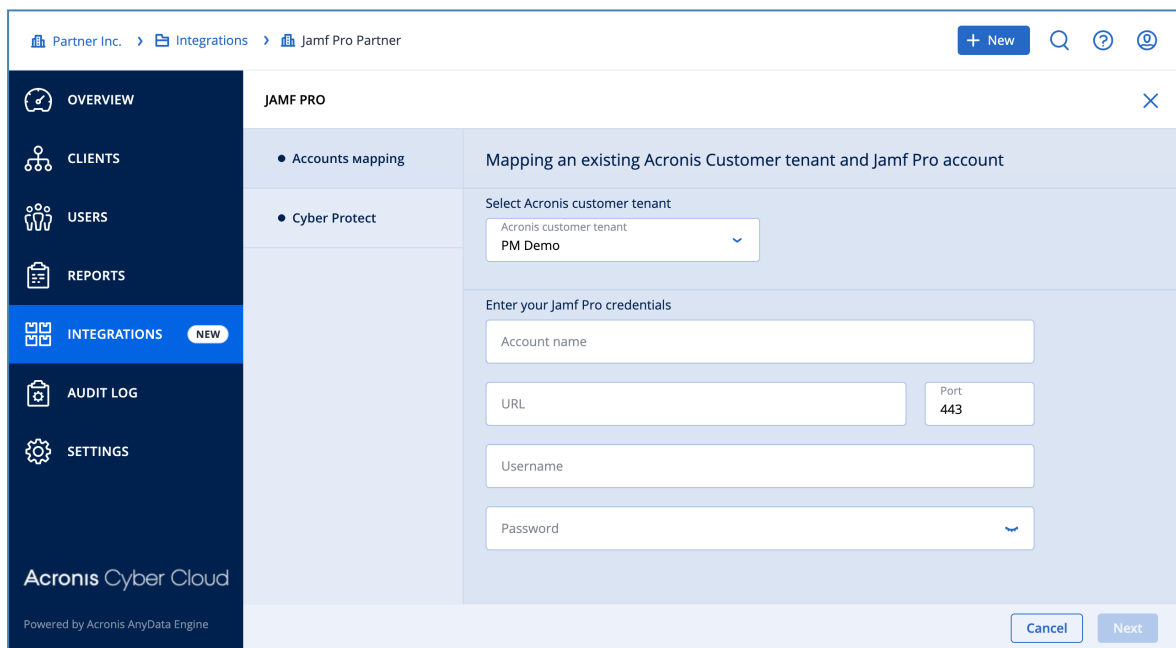
To enable the integration:

1. Go to the **Acronis Management portal** > **Integrations** and click on the **Jamf Pro** tile.
See [more information](#) about enabling and managing integrations.
2. You will be asked to select an existing Acronis customer tenant and user.

Note

Create a new customer tenant by clicking **New** at the top of any Acronis Management portal screen. Then select a customer and follow the steps to create a new customer tenant.

3. On the same screen, provide the following:
 - a. **Account name** - (for your own reference only) serves to identify the Jamf Pro account in the integration UI.
 - b. **URL** - provide url for your Jamf Pro instance.
 - c. **Port** - the port number of your Jamf Pro instance API. By default, this is port 443, but may be altered by the Jamf Pro Administrator.
 - d. **Username** and **password** to authenticate with.



4. Click **Next** to enter the Cyber Protect setup.
5. On the screen that opens, select a user for the customer tenant you selected on the previous screen. This customer will be used to register endpoints.
6. From the drop-down menu, select a smart or static group in your Jamf Pro account. Any computer that is a member of this group will have the Acronis agent installed.

7. Select a default protection plan. The list of available ones contains all protection plans, configured in the selected Acronis customer tenant. The selected plan will be applied to any computer where the integration deploys the Acronis agent.

The screenshot displays the Acronis management console interface. The breadcrumb navigation at the top reads: Partner Inc. > Integrations > Jamf Pro Integration Partner. The left sidebar contains a menu with the following items: OVERVIEW, CLIENTS, USERS, REPORTS, AUDIT LOG, SETTINGS (with sub-items: Locations, Branding, Security), and Integration (which is highlighted in blue). The main content area is titled 'JAMF PRO' and features a sub-menu with 'Accounts mapping' (selected) and 'Cyber protect'. The 'Accounts mapping' section contains the following configuration options:

- Select Acronis user and Cyber protection plan for computers**
- Select Acronis user**: A dropdown menu showing 'Acronis user' and 'John Smith'.
- Acronis Cyber Protect agent will be installed automatically on all devices in the selected Jamf Pro computer group and the selected protection plan will be applied.**
- Select Jamf Pro Computer group**: A dropdown menu showing 'Computer group' and 'Second Computer Smart Group'.
- Select cyber protection plan for devices**: A dropdown menu showing 'Cyber protection plan' and 'iOS default Cyber protection plan for devices'.

At the bottom right of the configuration area, there are 'Cancel' and 'Save' buttons.

8. Click **Save** to complete setup.

Once you have completed the setup, you will see a list of configured Jamf Pro accounts.

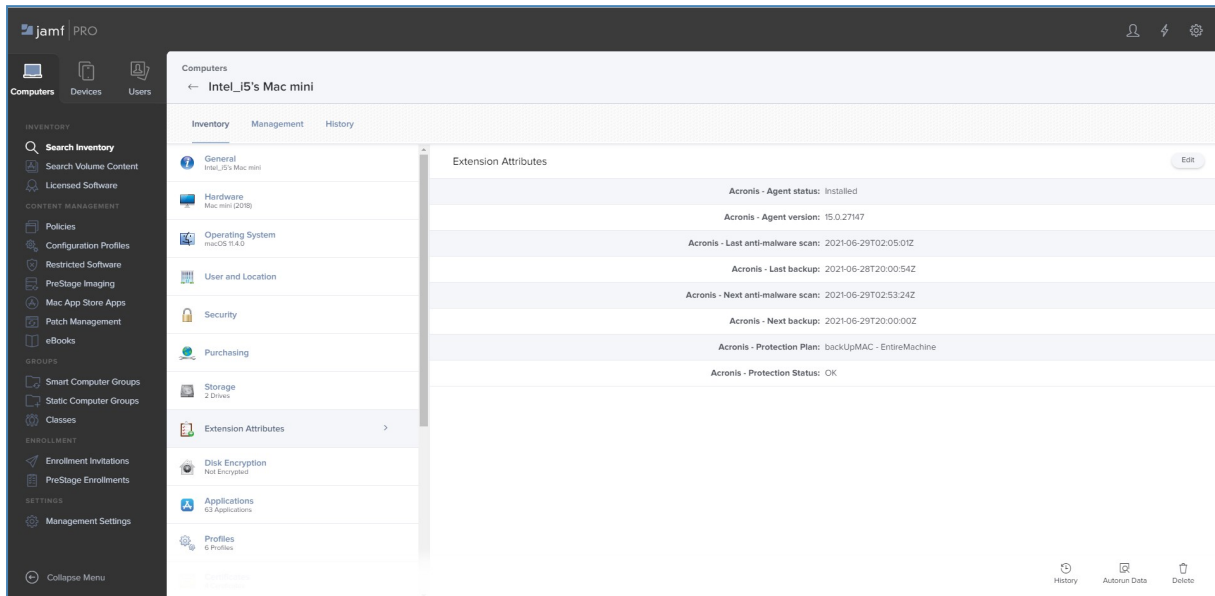
You can manage as many such accounts as necessary under a single Acronis Partner tenant account.

Deploying Acronis on macOS computers

Once you have set up the integration, all you have to do is to deploy Acronis to any computer and assign that particular computer to the group selected in step 6 of "Enabling the integration" (p. 9).

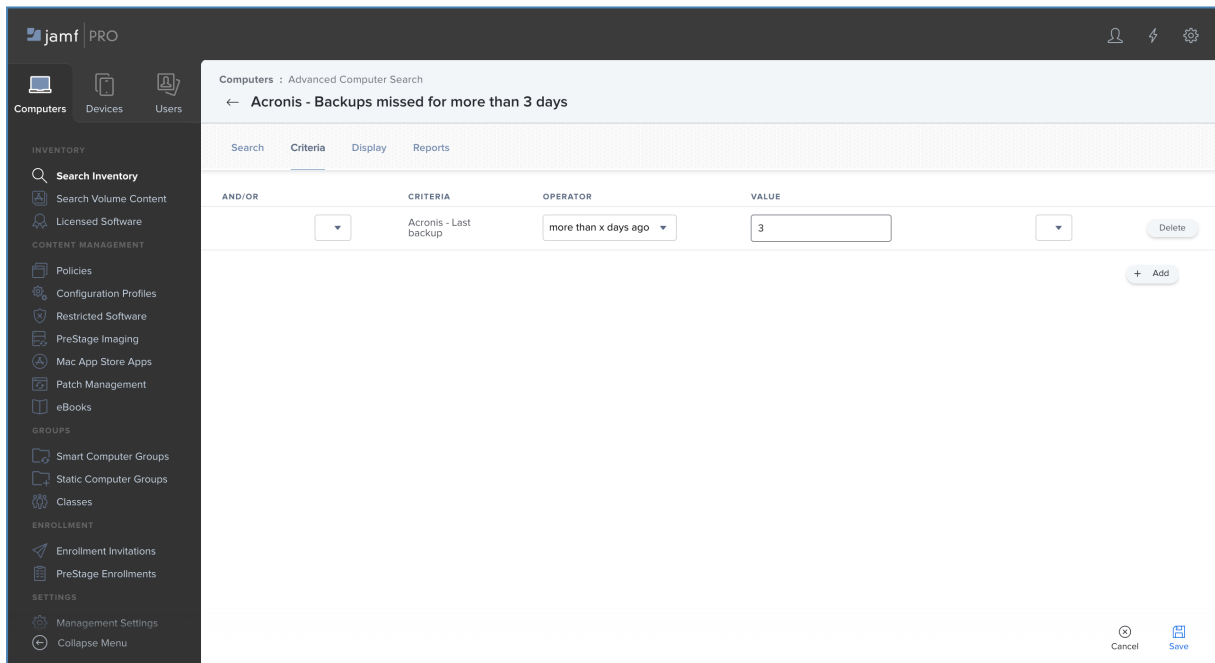
Monitoring protected computers

Any Acronis-deployed computer will have its associated Acronis extension attributes updated.



You can use these attributes the same way as any device property in Jamf Pro.

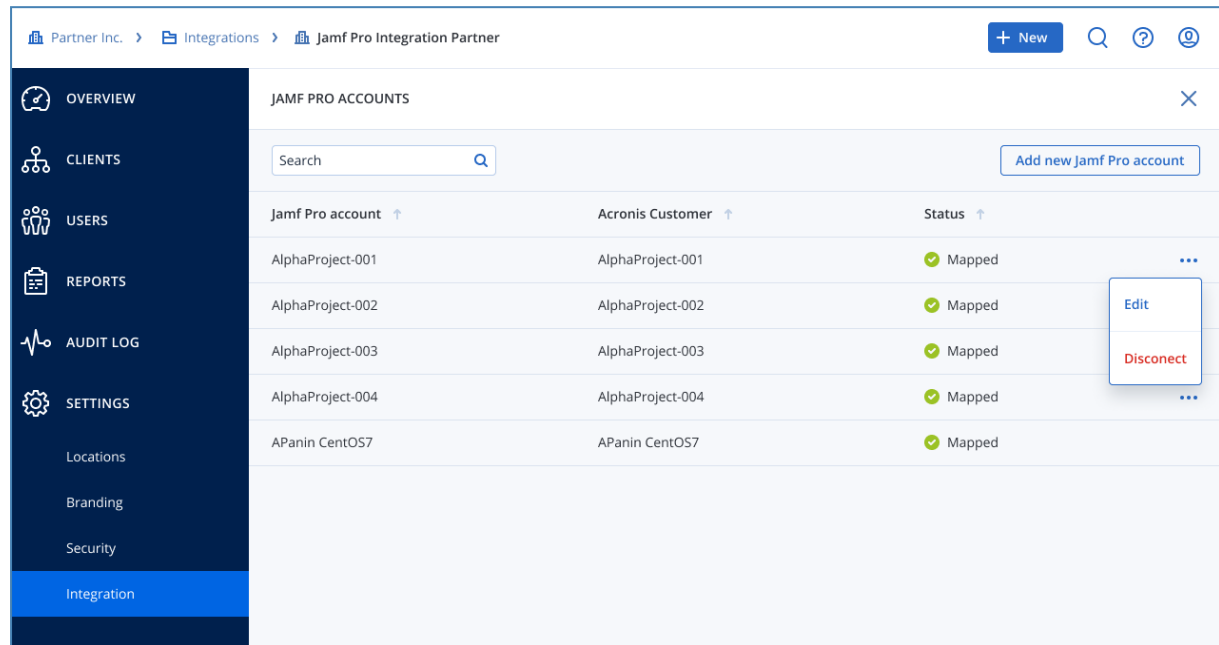
To start with, the integration has already created an Advanced Search, set up to find computers that have not completed a backup within the last 3 days.



You can modify and extend the Search and Display criteria as needed, or add Reporting options.

Editing accounts

Once you have set up any Jamf Pro account, you can go back and edit its settings or remove this account.



Editing accounts

To edit one or more mapped Jamf Pro accounts, do the following:

1. Go to **Acronis Management portal > Integrations**.
2. Click on the three dots (...) at the top-right of the **Jamf Pro integration** tile and select **Edit** from the drop-down menu.
3. On the next screen, find the Jamf Pro account you would like to edit and click on the three dots (...) at the end of the row.
4. Select **Edit** from the drop-down menu.
5. You will be taken to the **Account setup** screen with the following options:
 - **Account settings**
 - **Cyber protect**
6. Navigate to the section you want to edit and update the corresponding settings.

Removing accounts

To remove one or more mapped Jamf Pro accounts:

1. Go to **Acronis Management portal > Integrations**.
2. Click on the three dots (...) at the top-right of the **Jamf Pro integration** tile and select **Edit** from the drop-down menu.

3. On the next screen, find the Jamf Pro account you would like to remove and click on the three dots (...) at the end of the row.
4. Select **Disconnect** from the drop-down menu.
5. Confirm your selection.
6. The selected account has now been disconnected.

Repeat these steps for every Jamf Pro account that you want to disconnect.

Note

The Acronis customer tenant, including its associated workloads and usage, will not be affected by this change. The same applies to any scripts, groups, policies and extension attributes that have been created in your Jamf Pro account.

Reporting open alerts

For each protected workload, the Acronis integration for Jamf Pro can report the number of open alerts of specific types.

Reporting is enabled per alert type. Each alert type will create a corresponding Extension Attribute, where the number of currently open alerts is reported.

To enable alerts reporting, do the following:

1. In the Acronis Management panel, **Integrations > Jamf Pro Settings**.
2. On the Jamf account row, enable or edit the alert reporting by clicking on the three dots (...) at the end of the row and selecting **Edit**.
3. Next, navigate to the **Alerts Mapping** tab.
4. Click **Edit Mapping** to create new or modify the existing mapping.
5. Select any alert type you would like to have reported into Jamf Pro by clicking on the respective checkbox at the beginning of the row.

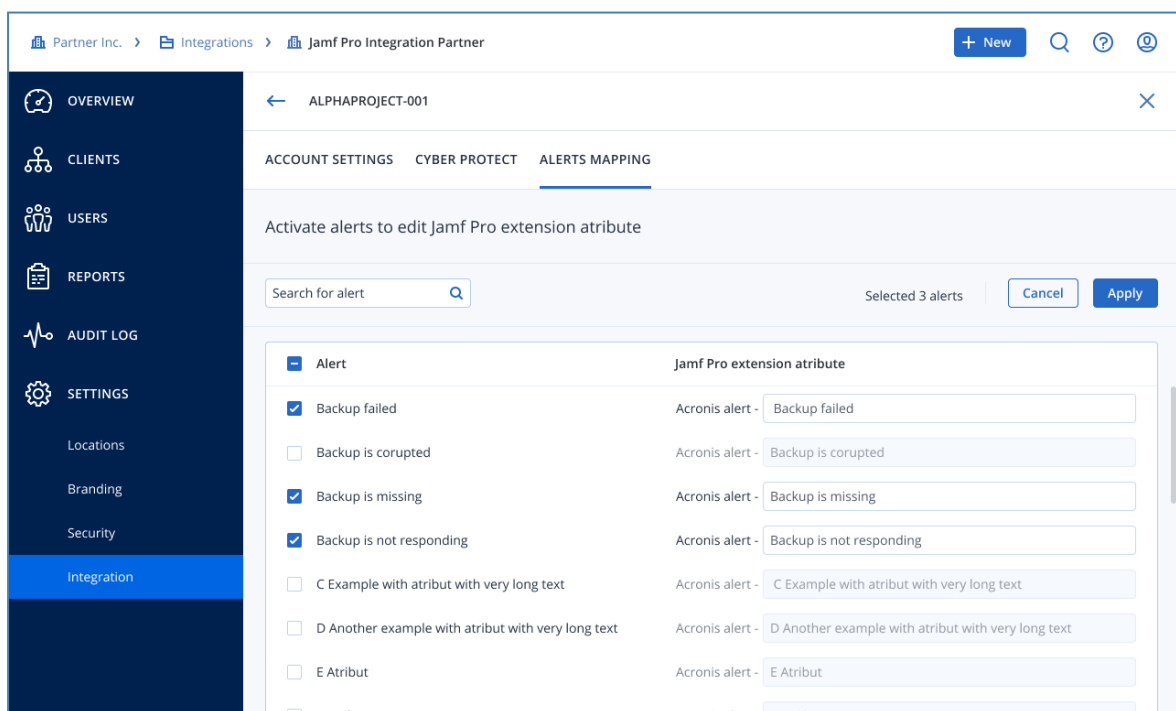
Note

Use the search bar (above the table with alert types) to quickly find any alert type or groups of such.

6. Optionally, modify the name of the Extension Attribute that will be used for this alert type.

Note

You cannot modify the name prefix, so that it is easier in Jamf Pro to distinguish between the different Extension Attributes used by the Acronis integration.



The Extension Attributes for any enabled alert types will be created.

7. When done editing, click **Apply**.

If necessary, any new Extension Attributes will be automatically created and will start populating. It may take up to 20 minutes for the first values to appear.

Example of how to monitor failed backup alerts

To monitor failed backups:

1. Enable the **Backup failed** alert type.
2. Set up a search for devices where the **Acronis alert - Backup failed** Extension Attribute is greater than 0.

Disabling the integration

To completely disable the integration:

1. Go to **Acronis Management portal > Integrations**.
2. On the **Jamf Pro integration** tile, click on the three dots (...) in the top-right and select **Delete** from the drop-down menu.
3. Confirm your selection.

The integration will be disabled and all mapped accounts - disconnected.

Note

Any Acronis customer tenants, including their related workloads and usages, will not be affected by this action.
