Acronis

acronis.com

Acronis Cyber Cloud

Integration with Matrix42

Integration Guide

REVISION: 9/12/2022

Table of contents

Introduction

This document describes how to enable and configure the integration of Acronis Cyber Cloud with Matrix42.

Once set up, the integration enables:

- Deployment of Acronis to and monitoring of endpoints from within the Matrix42 Unified Endpoint Manager
- Get tickets based on alerts from Acronis in the Matrix42 Service Desk

Prerequisites

To use this integration, you should have:

- A setup and configured Matrix42 instance
- A setup Acronis Cyber Cloud account

The Acronis account should have at least a single Customer tenant created, along with one admin user.

Dependencies

What needs to be preconfigured:

- Empirum SDK installed on the Workspace Management Server
- Empirum API enabled and configured

The following is required to optionally make use of the features provided in the Unified Endpoint Manager:

- Unified Endpoint Management Extension 21.0.0.4 or newer
- Secure Unified Endpoint Management Extension 21.0.0.3 or newer

Supported systems

The Acronis integration works with:

- Matrix42 Workspace Management 10.0.4 or newer
- Matrix42 Empirum SDK Extension 1.3.5 or newer
- Matrix42 Empirum 20.0.3 or newer
- Acronis Cyber Cloud 9

The Unified Endpoint integration currently supports Acronis deployment on Windows only.

What is installed

The integration basically represents the Matrix42 Workspace Management Extension.

This includes the Empirum Package and Variable configuration files, which have to be manually imported into Empirum.

After installation of the extension, the files can be found at: `Matrix42 Workspace Management\Acronis\Emp`.

The package itself is the `{1172650C-A175-4215-9658-B8FB4393ADC6}` folder and the `AcronisVariables.xml` file contains the variables that should be imported.

Installation

To fully install and configure the Acronis integration for Matrix42, you have to:

- Install the integration onto your Matrix42 instance
- Install the Empirum package
- Configure the integration
- Configure ticket mapping

The Acronis integration will add the following components to your Matrix42 instance:

- Acronis Cyber Protect package for Empirum
- Actions
- Workflows

Installation procedure

To start the installation of the Acronis integration:

1. Do either of the following:
   a. Log in to the Acronis Management portal, then go to **Integrations** and click on the **Matrix42** tile. You will be redirected to the Acronis integration on the Matrix42 Extensions Marketplace. See more information about enabling and managing integrations.
   b. Navigate directly to extensions.matrix42.com and locate the Acronis integration.
2. Review the on-screen information and click on **Install**.

If you have multiple instances, you can select the one to install the integration on, then click **Install** to actually trigger the installation process.

After completing these steps, the Acronis integration will be installed on your Matrix42 instance. Next step is to configure Empirum for deployment of Acronis to workloads as well as to configure the integration to work with your Acronis partner tenant account.

Importing the Empirum package

For a successful installation you will need:

- Package Folder (Name: {1172650C-A175-4215-9658-B8FB4393ADC6})

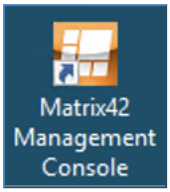
The package will be installed together with the Workspace Management package and can be found at: Matrix42 Workspace Management\Acronis\EmpirumPackage folder

- AcronisVariables.xml
- access to the physical Empirum Server and the Empirum Management Console
  - with an administrative User

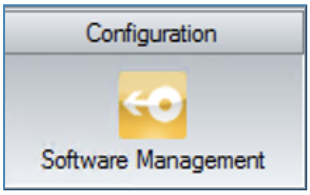
Follow these steps to import and configure Empirum to work with the Acronis integration.

Import the package

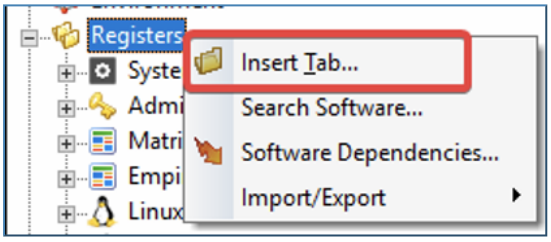
1. Open the Matrix42 Management Console as an administrator.



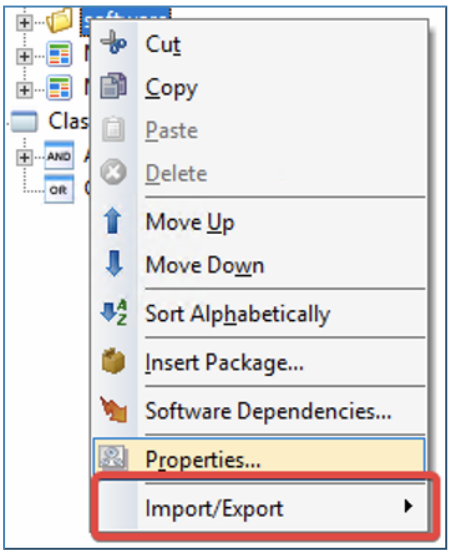
2. In the left pane, navigate to **Configuration** > **Software Management**



3. Right-click **Register** and choose **Insert Tab**. Give the tab an appropriate name, for example: “Acronis”.

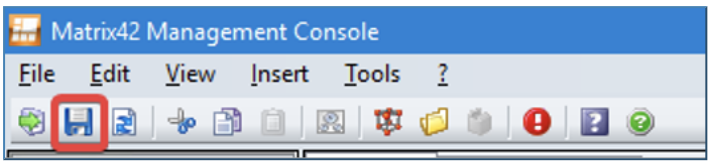


4. In the left pane, select and right-click the **Acronis** folder, then choose **Import/Export** > **Import Package**.



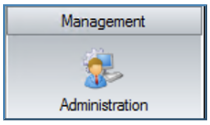
5. Click through the assistant, until you are asked to provide directory. Then choose the directory where your package is stored.
6. Click **Next** and choose the **Acronis Cyber Protection Agent** option, then click **Next** again.

7. The package will now be imported. When the import is done, save your changes by clicking on the **SAVE** icon just below the main menu options.

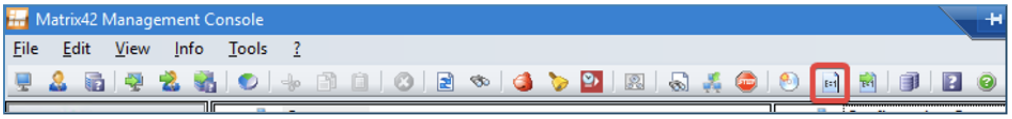


Import the variables

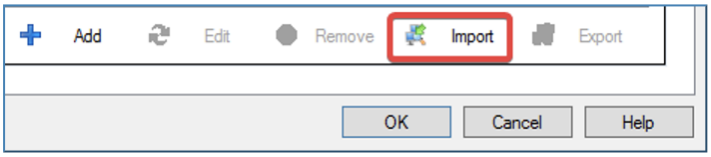
1. In the left pane, navigate to the **Management** > **Administration** section.



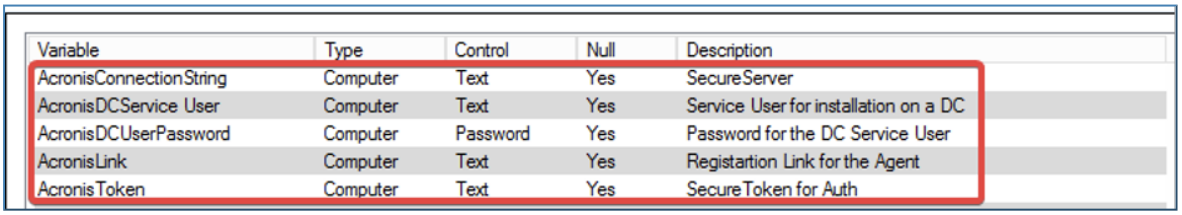
2. Choose **Define Variables** from the actions bar.



3. In the **Variable Definitions** window that opens next, choose the **Import** option.



4. Import both files.
5. After the import, the variables should appear in the list. It might be necessary to scroll to the bottom, before reloading, to be able to see them.



Variable	Type	Control	Null	Description
AcronisConnectionString	Computer	Text	Yes	SecureServer
AcronisDCService User	Computer	Text	Yes	Service User for installation on a DC
AcronisDCUserPassword	Computer	Password	Yes	Password for the DC Service User
AcronisLink	Computer	Text	Yes	Registartion Link for the Agent
AcronisToken	Computer	Text	Yes	SecureToken for Auth

Notes on deployment of Acronis to a Domain Controller

If you choose to install the Acronis agent on a Domain Controller, the installer will need the Service Account credentials for the Domain Controller. These credentials should be filled in the AcronisDCService User variables. The password will be stored in encrypted format.

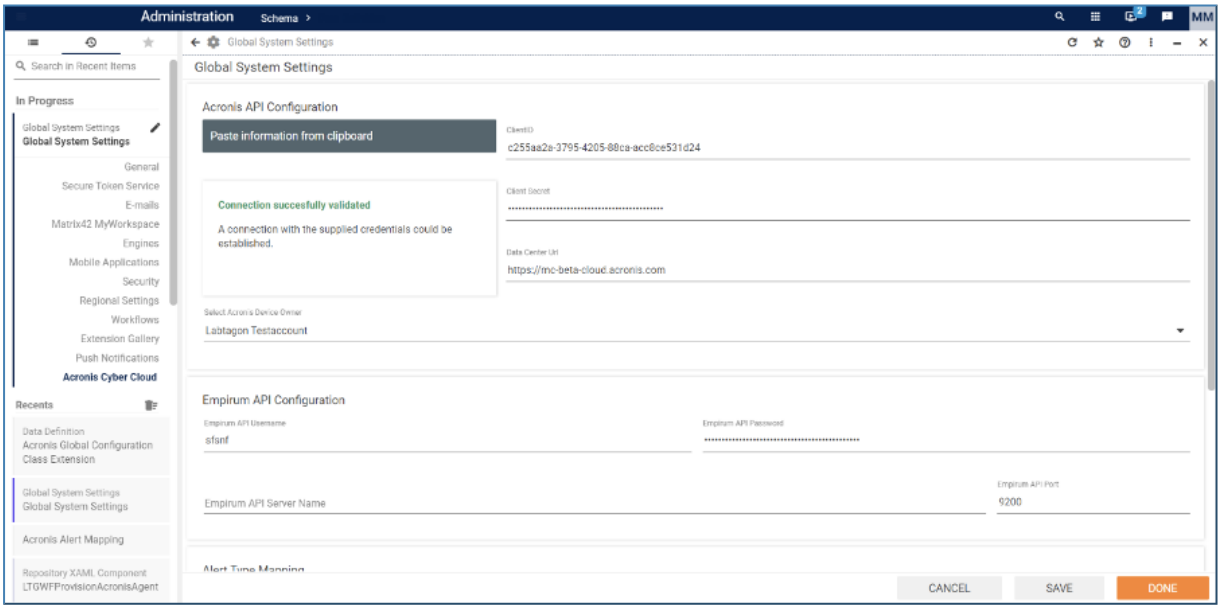
Integration configuration

Once the integration is installed, the following steps will let you configure it for usage with your Acronis account.

1. Log in to your Partner tenant account on the Acronis Management portal and go to **Settings** > **API clients**.
2. Click on **Create new client**, then provide a name for the new API client and click on **Next**.
3. On the next screen, copy the **Client ID**, **Secret** and **Data center URL**.

Note
After closing this screen, there will be no way to see the Secret key again, so make sure to store it safely.

4. In Matrix42, go to the **Administration module** > **Global System Settings** > **Edit** > **Acronis Cyber Cloud**.
5. Provide the credentials created in steps 2-3 above.
6. Select a Customer tenant and a user associated with it. On Acronis side, all your protected devices will be positioned under this Customer tenant.
7. In the **Empirum API Configuration** section, provide:
   a. **Empirum API user**
   b. **Empirum API Password**
   c. **Empirum API URL**



Once the integration is fully configured, a sync is scheduled where the endpoint devices on Matrix42 and Acronis are made to match each other. This is the moment when the **Acronis devices** tab in **Assets** and the **Unified Endpoint Manager** will start populating.

You can trigger this process manually by going to **Administration module** > **Services and Processes** > **Engine Activations** > **AcronisConnector Inventory**.

Acronis deployment to endpoint devices

Acronis can be deployed to endpoint devices from the **Endpoint devices** screens in the **Assets**, **Unified Endpoint Manager** and **Secure Unified Endpoint Manager** modules.

1. In the module, go to the **Endpoint devices** screen to select one or more endpoints from the list.
2. On the Action Bar, locate the **Install/Repair Acronis Agent** button and click it.
3. In the confirmation window, click **Yes** to deploy the Acronis agent to the selected endpoint device.

Devices are synchronised every 20 minutes.

Monitoring Acronis statuses on protected endpoint devices

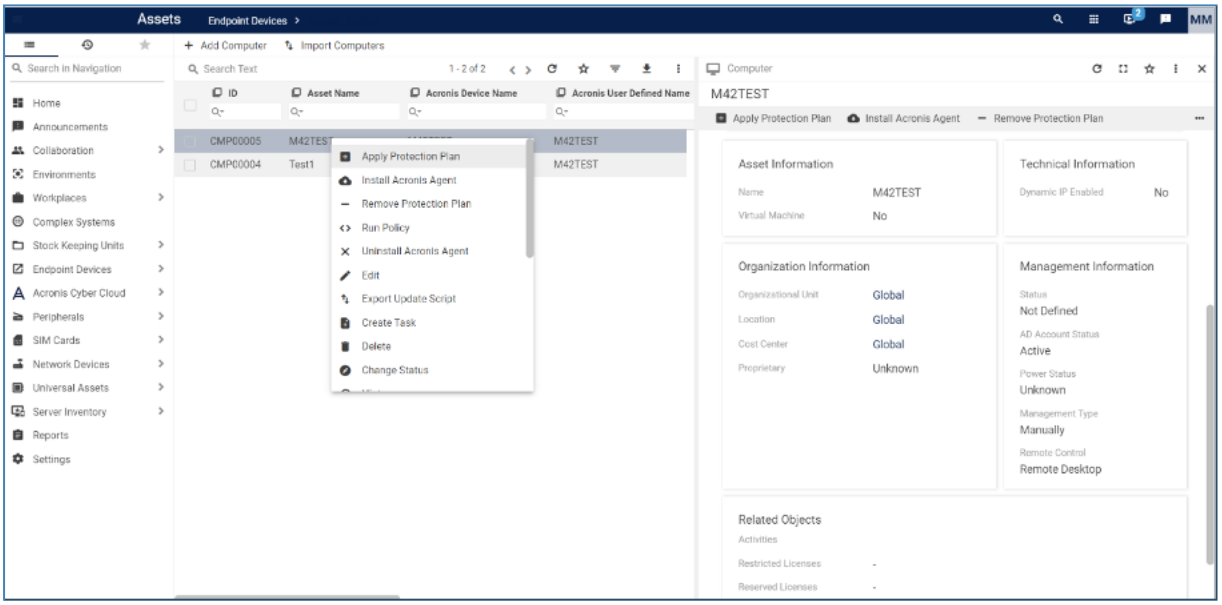
To monitor protected endpoint devices' statuses, go to **Assets**, **Unified Endpoint Manager** and **Secure Unified Endpoint Manager** modules.

Under **Endpoint devices**, you'll find a new filtered **Acronis devices** view. It lists all protected workloads along with their backup and protection statuses.

Manually running tasks

The integration provides actions and workflows that can be run manually.

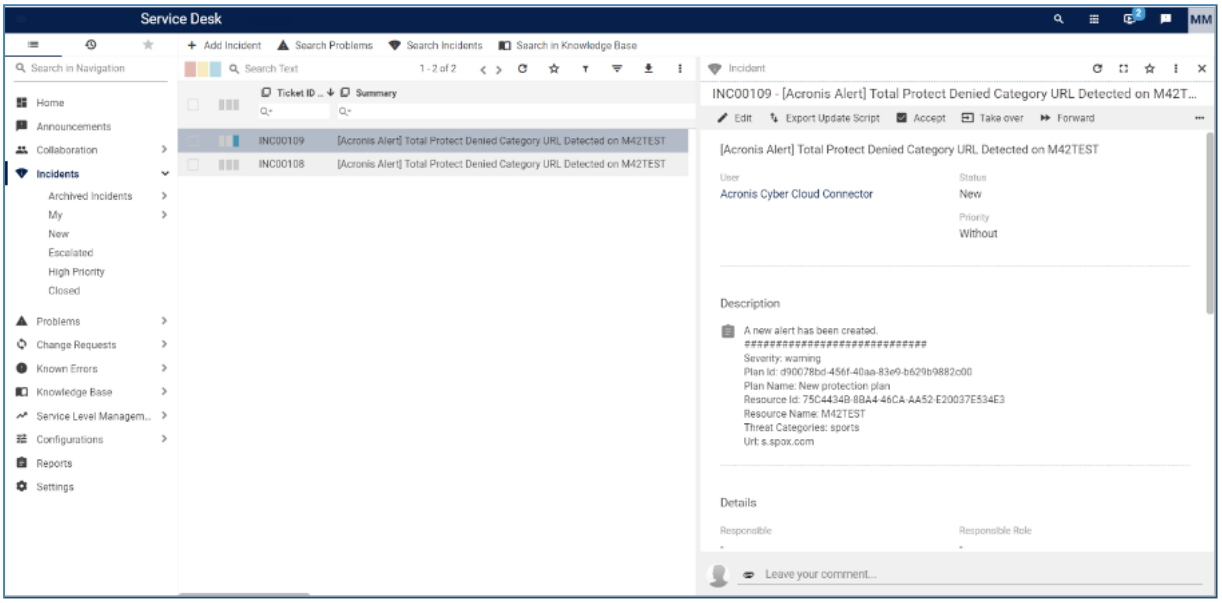
1. In **Assets**, **Unified Endpoint Manager** and **Secure Unified Endpoint Manager** modules, go to the **Acronis devices** view and select a device you want to run any manual task on.
2. Do either of the following:
   a. Right-click any device and run an action from the pop-up menu
   b. Select the desired action from the panel actions menu on the right.



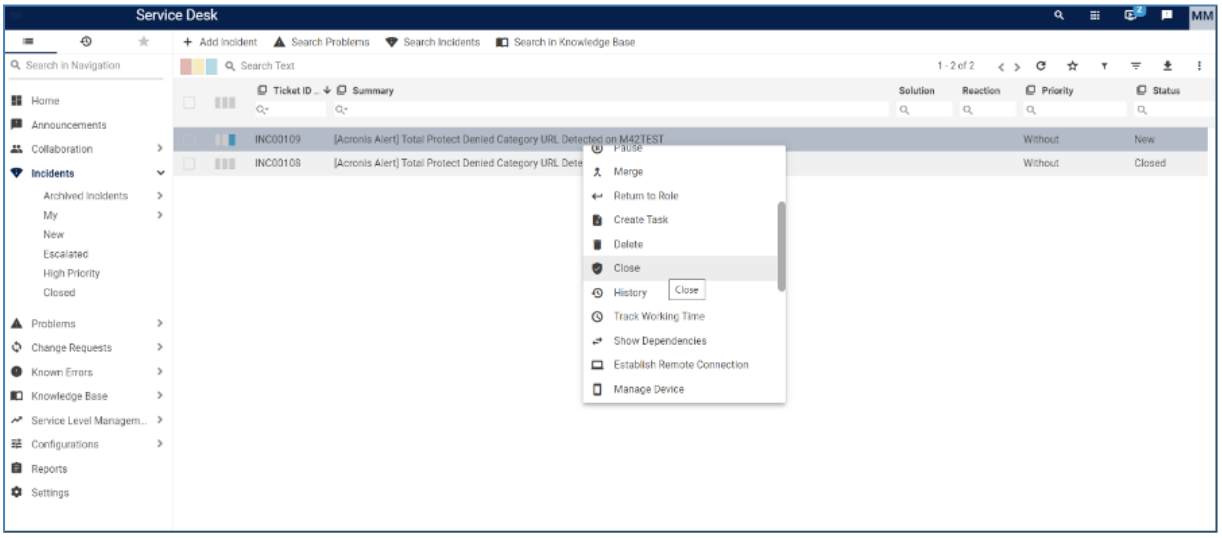
Tickets in Service Desk

Any Acronis alerts of type mapped in the ticketing settings, will create Incidents tickets in the Matrix42 Service Desk.

These can be viewed from **Service Desk** module > **Incidents** > **New**.



Closing an incident in Matrix42, will close also the corresponding alert in Acronis.



Configuring ticket mapping

Ticket mapping can be configured from two places:

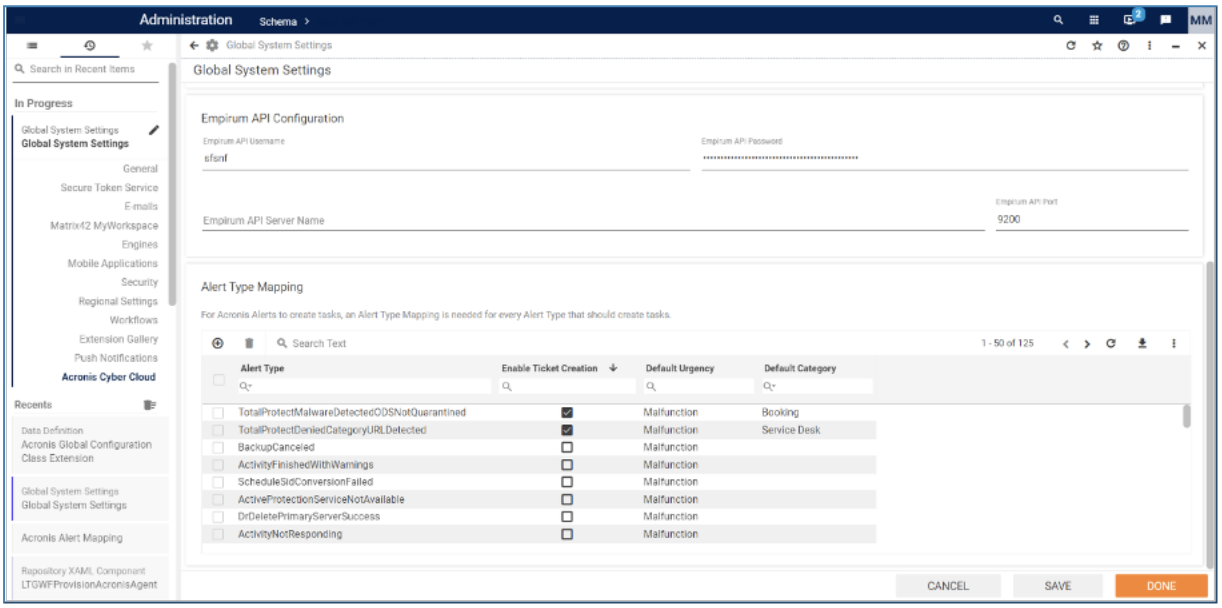
- **Administration** module > **Global System Settings** > **Edit** > **Acronis Cyber Cloud**. Scroll down to the **Alert Type Mapping** section.
- **Service Desk** module > **Settings** > **Global System Settings** > **Edit** > **Acronis Cyber Cloud**

Both of these locations list the available alert types, as follows:

1. For each alert type, for which you would like tickets to be created in Matrix42, select its checkbox on the **Enable Ticket Creation** screen.
2. For each enabled alert type, you can define a Default Urgency and a Default Category.

Whenever a new alert is generated on Acronis side, if the corresponding alert type has been already enabled in Matrix42, a new Incident ticket will be created with the specified Urgency and Category.

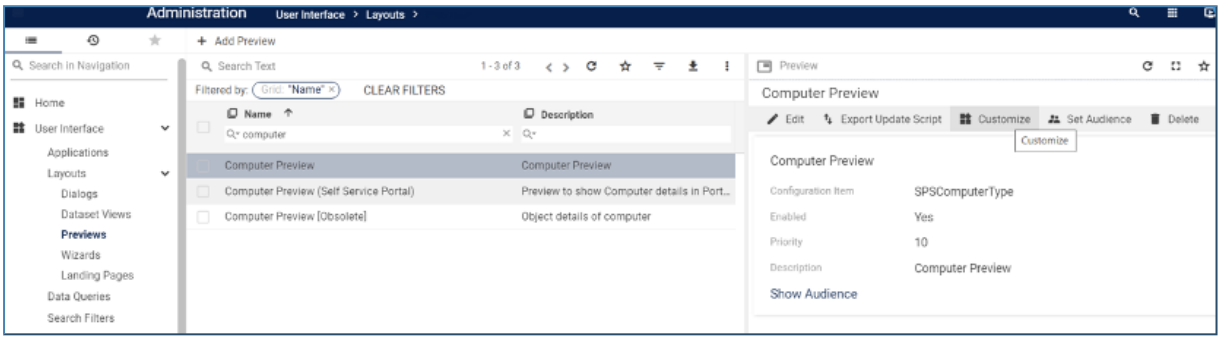
Alerts are updated every 10 minutes.



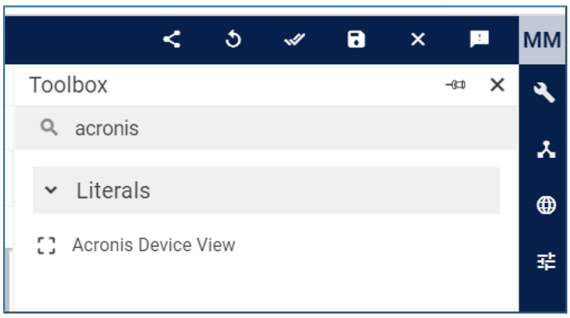
Customizing layouts

You can use standard Matrix42 layout methods to customize the way Acronis data is shown.

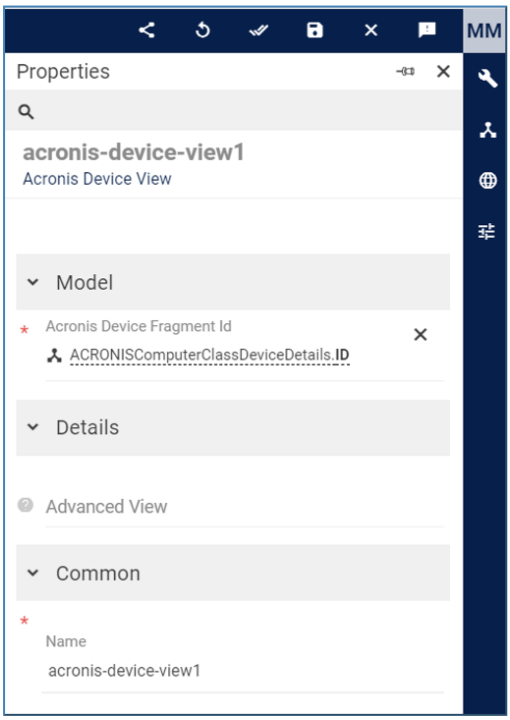
For example, to show the additional device data in a preview or dialog, use the Acronis device control in the Layout Designer. It can be opened by clicking the **Customize** action.



Locate the Acronis device view control and drag and drop it to the layout.

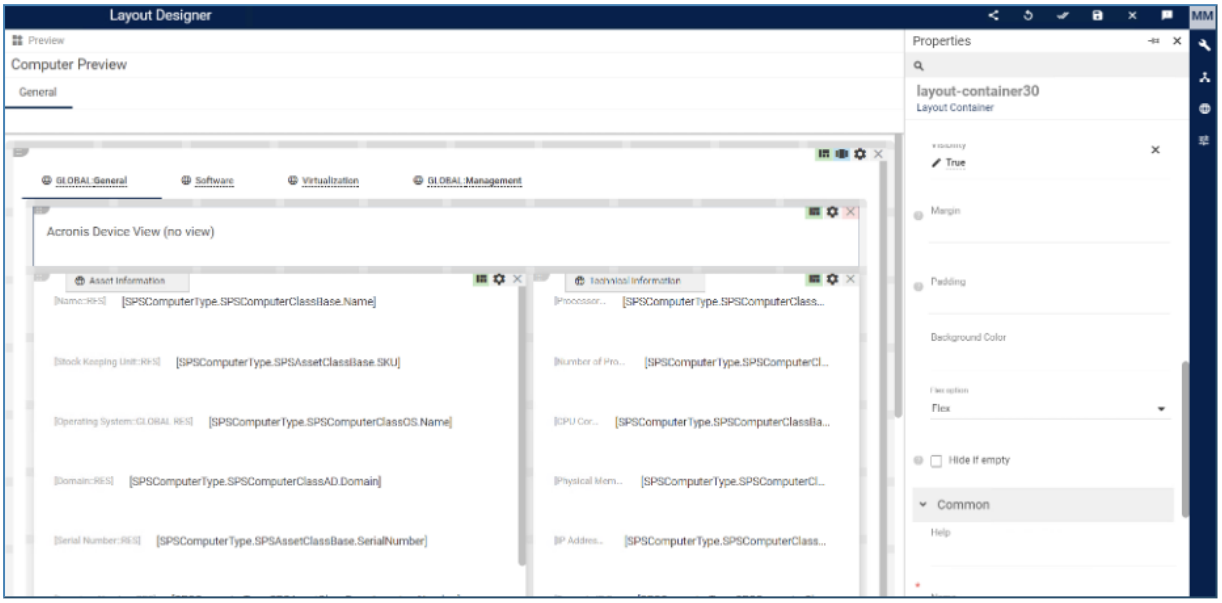


In the control properties, set the Fragment ID of the Device Data.



If the control doesn't appear, uncheck the controls container **Hide when empty** property.

(To select the container of the control, click the white area around the control.)



Uninstalling the integration

To uninstall the integration, follow these simple steps:

1. Open Matrix42 and go to **Administration menu** > **Installed Packages** > **Acronis Cyber Cloud Connector**.
2. In the menu that opens next, click **Uninstall Package**.

This will remove the following files:

```
Acronis.M42.CyberCloudConnector.Services.dll
```

from

```
C:\Program Files (x86)\Matrix42\Matrix42 Workplace Management\svc\bin
```

AND

```
Acronis.M42.CyberCloudConnector.Activities.dll

Acronis.M42.CyberCloudConnector.Client.dll

Acronis.M42.CyberCloudConnector.Contracts.dll
```

from

```
C:\Program Files (x86)\Matrix42\Matrix42 Workplace Management\ServiceRepository\BinaryComponents
```