Acronis

acronis.com

Kaseya VSA 10 Integration

C25.05

Configuration Guide

REVISION: FRIDAY, JUNE 20, 2025

Table of contents

© Acronis International GmbH, 2003-2025

Introduction

This guide describes how to activate and configure the integration of Acronis Cyber Cloud with Kaseya VSA 10. It also covers the integration content package which is provisioned on the Kaseya VSA 10 platform.

Integration functionality

The integration lets you:

- Map Kaseya VSA 10 customer organizations to existing Acronis customer tenants.
- Provision Kaseya VSA 10 customers as new customer tenants in Acronis.
- Deprovision deleted Kaseya VSA 10 customers from Acronis.
- Select default protection plans for mapped Kaseya VSA 10 customer organizations.

Acronis functionality on Kaseya VSA 10 platform

When you activate the integration, a content package of scripts, workflows, and custom fields is provisoned on the Kaseya VSA 10 platform. With this package you can:

- Install the Acronis agent on devices.
- Scan protected devices.
- Check the Acronis agent version on protected devices.
- Check the CyberFit score of protected devices.
- Check the device protection status.
- Invoke and revoke default protection plans on protected devices.
- Scan protected devices for malware.
- Check the last and next backup details of protected devices.
- Check the last and next anti-malware scan details of protected devices.

Note
For more information, see Integration content package and Monitoring device status.

© Acronis International GmbH, 2003-2025

Prerequisites

Kaseya VSA 10 prerequisites

- An administrator account in Kaseya VSA 10.

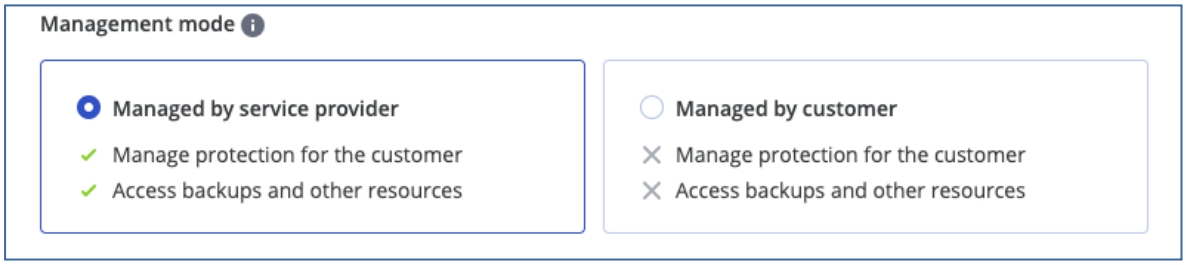
Acronis prerequisites

- You must have a fully configured Acronis Cyber Cloud partner tenant account.
- The user account that you use to activate and configure the integration must be a Company Administrator.
- You must not have disabled support access.

> **Note**
> For more information, see the Management Portal Partner Administrator guide.

- [Optional] One or more customer tenants.

> **Note**
> Only customer tenants that are provisioned as **Managed by service provider** will appear as active for mapping.



- [Optional] One or more protection plans.

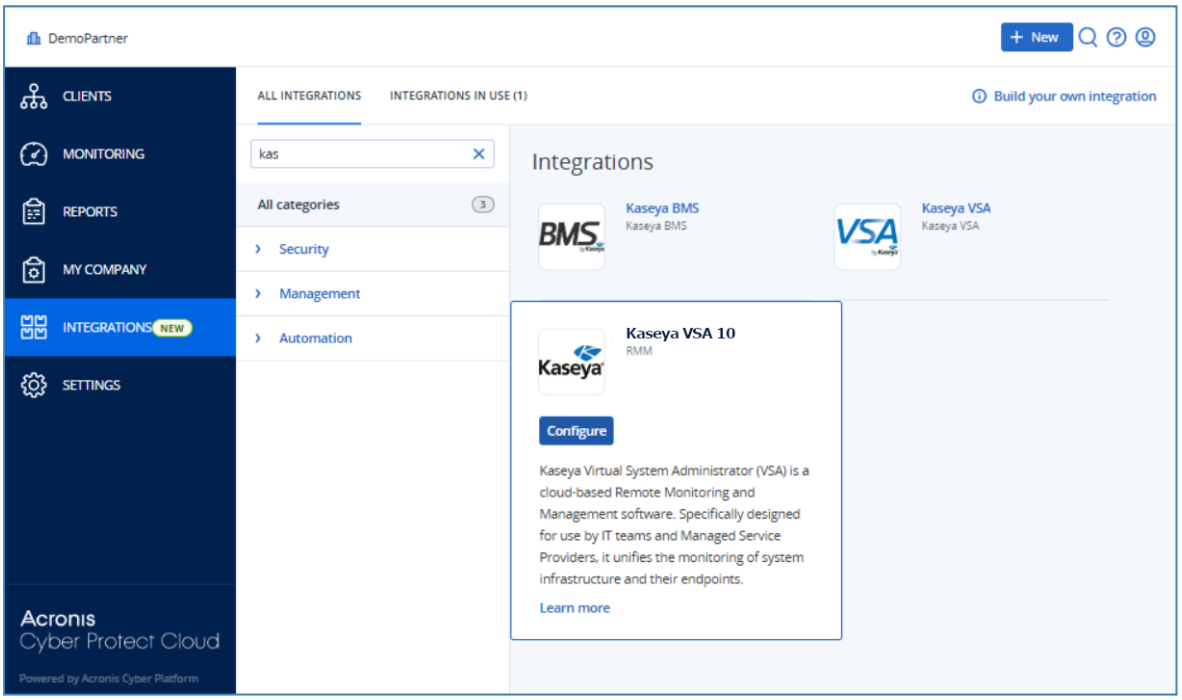
© Acronis International GmbH, 2003-2025

Activating the integration

To activate the integration

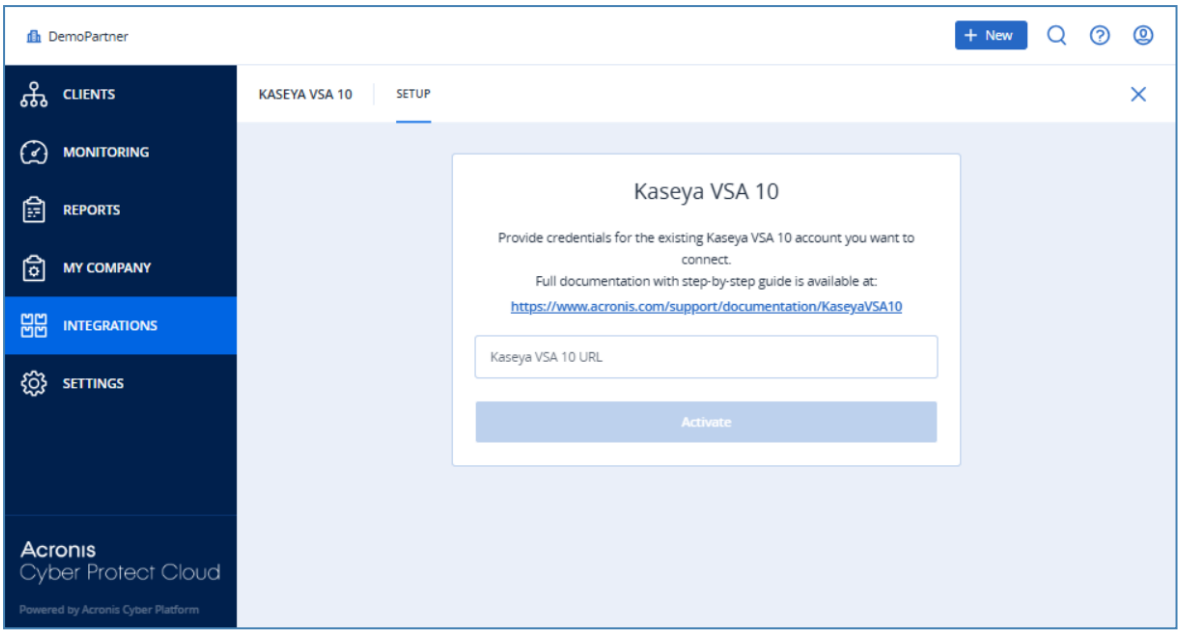
1. Log in to Acronis Management Portal as a Company Administrator.
2. Select **INTEGRATIONS** from the main menu.
3. Search for the Kaseya VSA 10 catalog card.

Note
For more information, see the Management Portal partner administrator guide.



4. Hover over the Kaseya VSA 10 catalog card and click **Configure**.

© Acronis International GmbH, 2003-2025

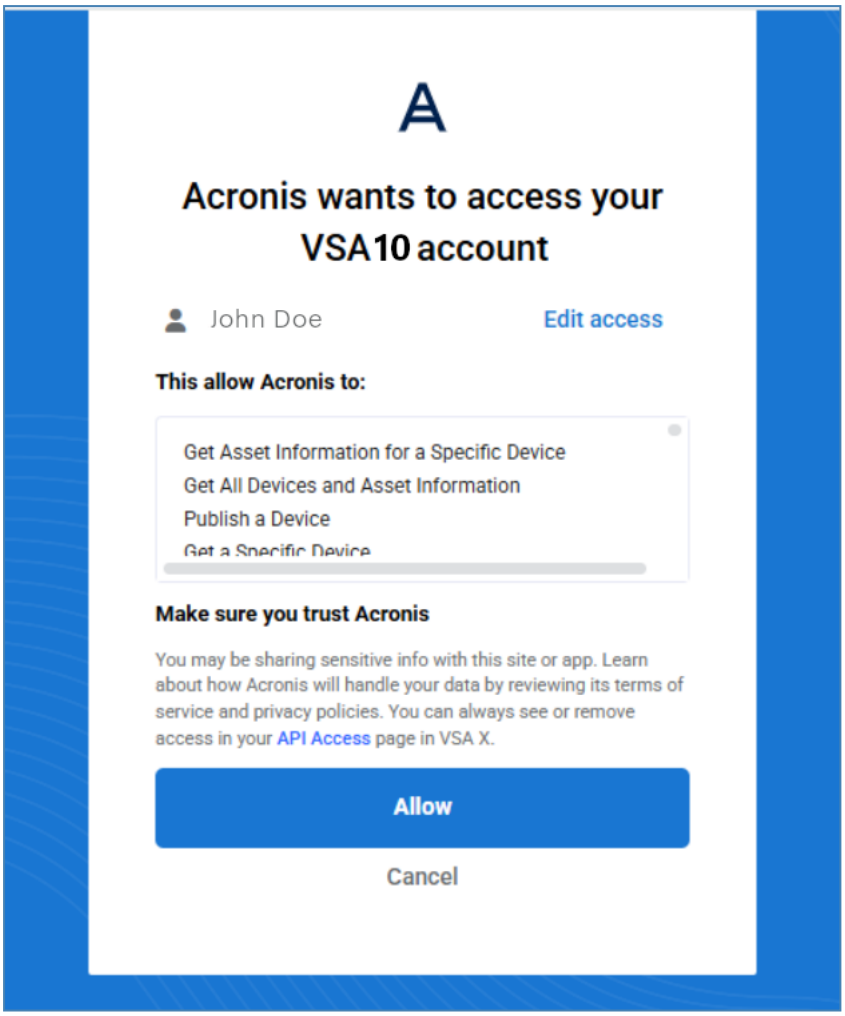


5. Enter the base URL of your Kaseya VSA 10 account, with no path.

Note
You cannot change this after activation. To change it, you must deactivate the integration and activate it again.

6. Click **Activate**.
7. Enter your Kaseya VSA 10 username and password.

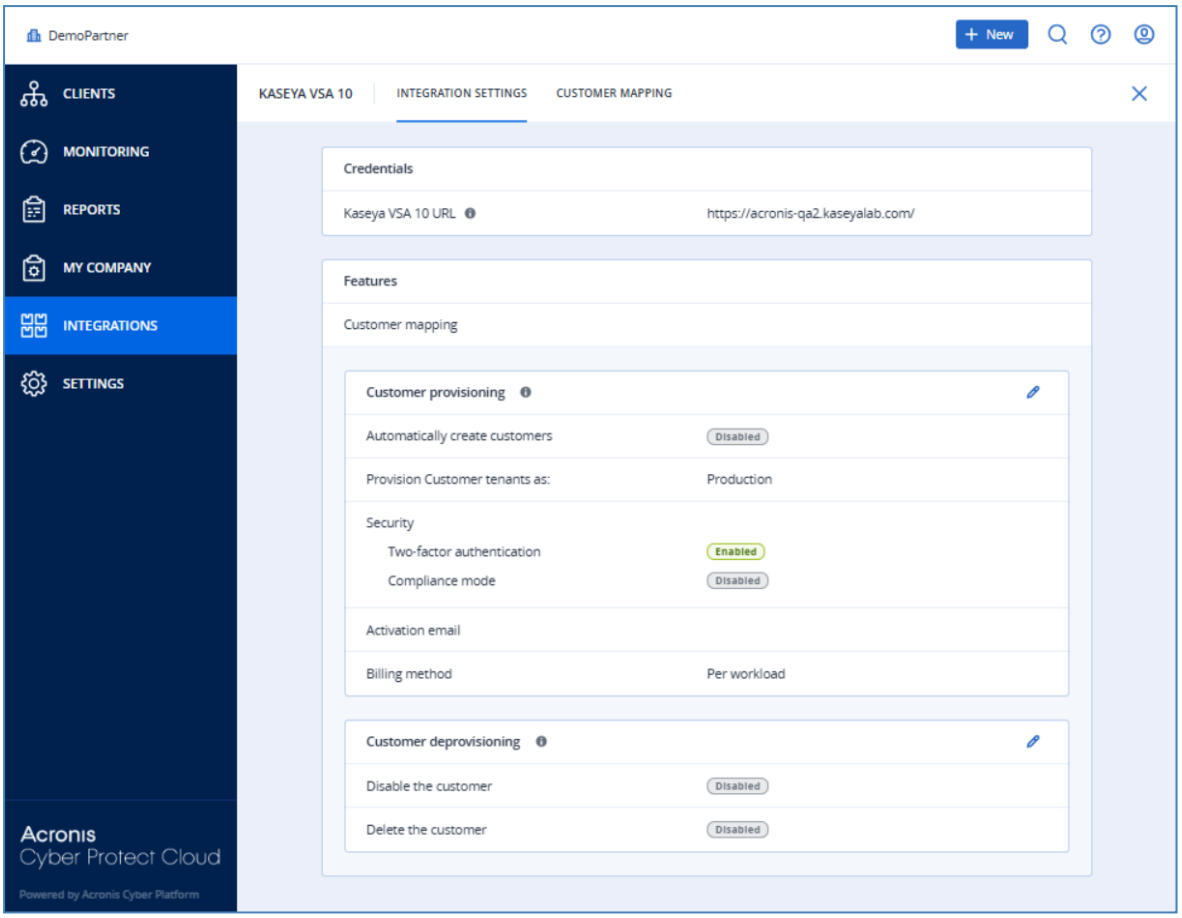
© Acronis International GmbH, 2003-2025



8. Click **Allow**.

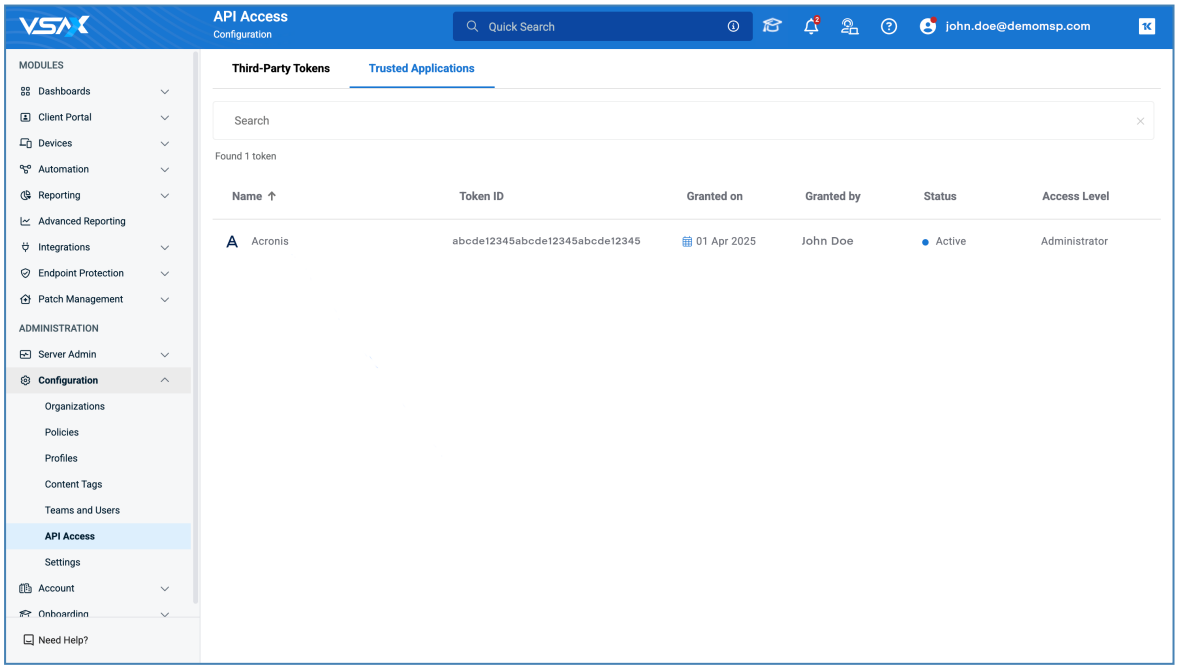
   The integration is activated, and opens on the **INTEGRATION SETTINGS** tab.

© Acronis International GmbH, 2003-2025



Note

To check that the integration is correctly activated, log in to Kaseya VSA 10 and navigate to **Configuration** > **API Access** > **Trusted Applications** tab. Check that Acronis appears in the list.



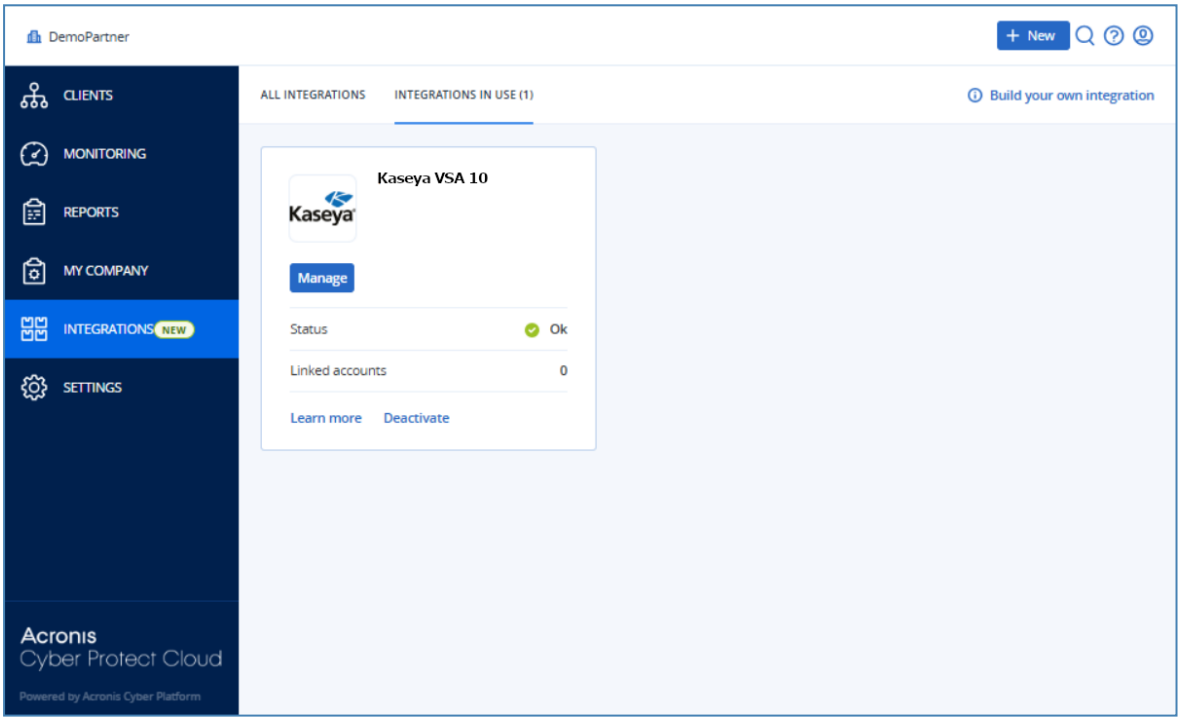
© Acronis International GmbH, 2003-2025

Opening the integration

To open the integration

1. Log in to Acronis Management Portal as administrator.
2. In the main menu, select **INTEGRATIONS**.
3. Select the **INTEGRATION IN USE** tab.
4. Locate the Kaseya VSA 10 integration catalog card.

Note
For more information, see the Management Portal partner administrator guide.



5. Click **Manage**.

© Acronis International GmbH, 2003-2025

Settings

The **INTEGRATION SETTINGS** tab contains sections for:

- Credentials
- Customer mapping

To manage integration settings

1. [If required] Open the integration.
2. Select the **INTEGRATION SETTINGS** tab.

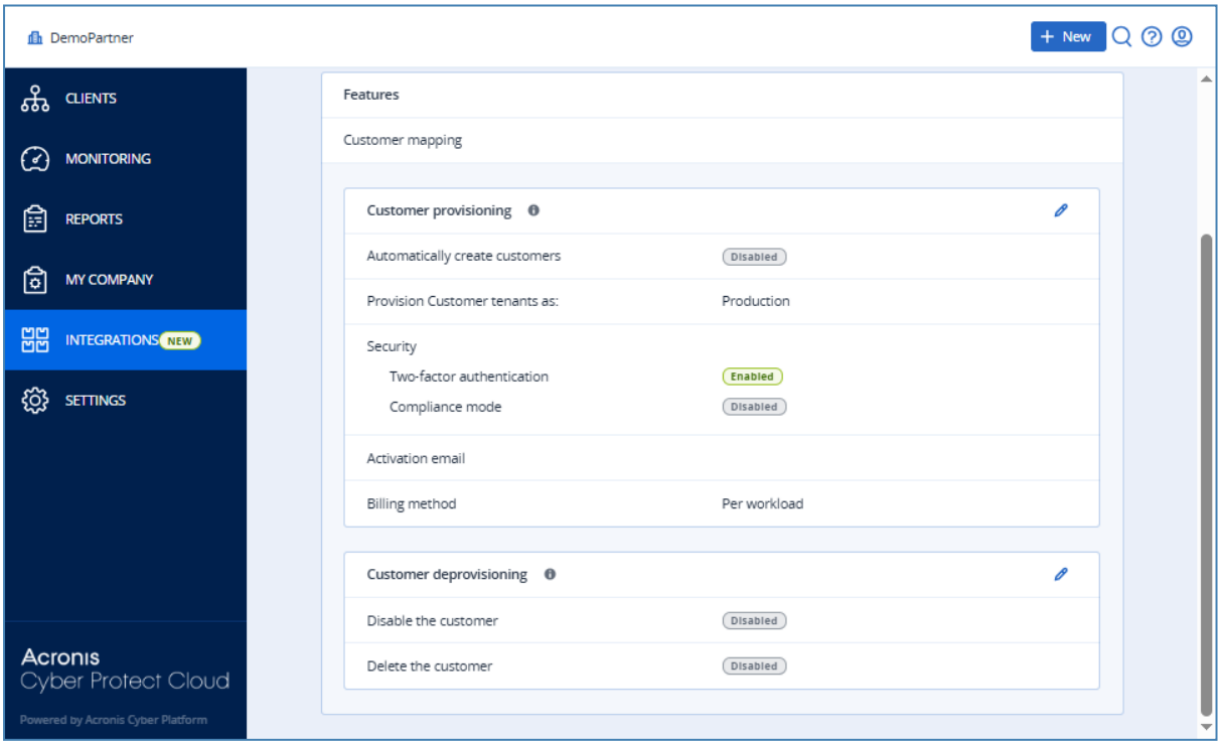
Credentials

Note
You cannot change the Kaseya VSA 10 URL after activation.
To change it, you must deactivate the integration and activate it again.

Customer mapping settings

In the Customer mapping section, you can define setting for:

- Customer provisioning
- Customer deprovisioning



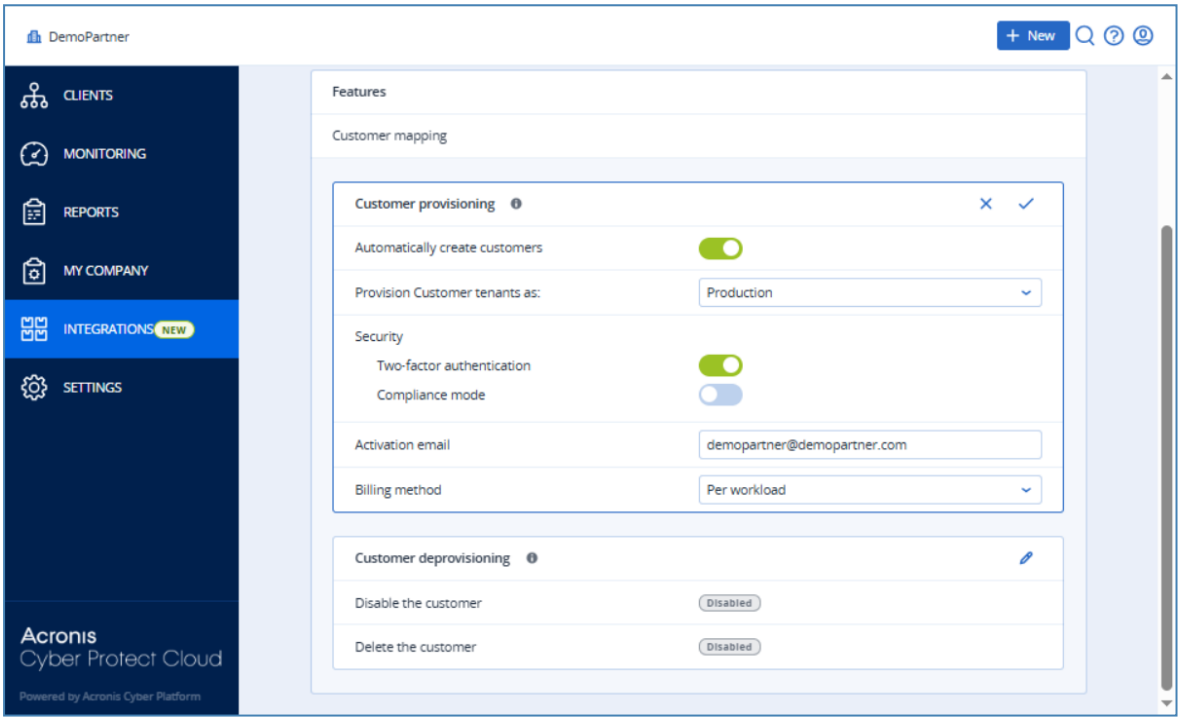
© Acronis International GmbH, 2003-2025

Customer provisioning

In the **Customer provisioning** section, you configure the parameters required to create new customers and accounts in Acronis Management Portal.

To configure customer provisioning

1. Open the integration.
2. Select the **INTEGRATION SETTINGS** tab.
3. In the **Customer provisioning** section, click .



4. Turn the **Automatically create customers** toggle switch on or off.
   If you enable this feature, newly created Kaseya VSA 10 organizations are provisioned in Acronis, and the new Acronis customer tenant is mapped to the corresponding Kaseya VSA 10 organization.

   Note
   By default, customers are provisioned in Acronis **Managed by service provider** mode, with the same services enabled as for the service provider and with all quotas set to unlimited.

   Important
   Make sure that you have mapped Kaseya VSA 10 organizations which are already registered as Acronis customer tenants. Otherwise, these customers will be duplicated after enabling automatic customer provisioning.

5. Select the **Provision customer tenants as** setting from the dropdown list:

© Acronis International GmbH, 2003-2025

- **Production** (default)
- **Trial**

> **Note**
> Customers in trial mode have full access to all integration functionality for the duration of the trial.
> They are automatically switched to production mode after 30 days.

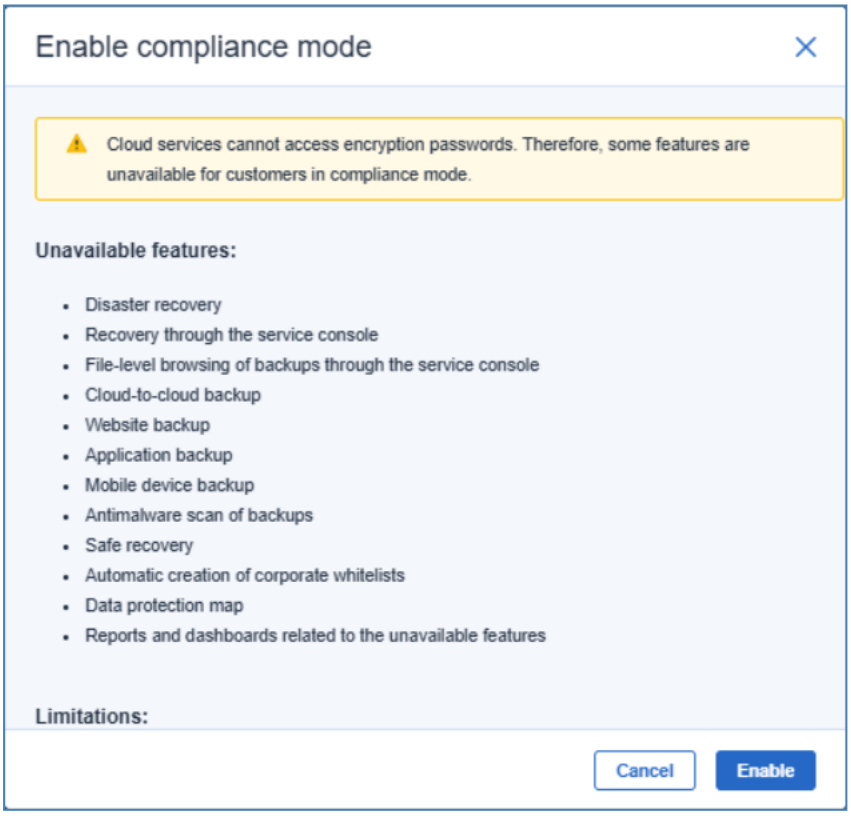
6. Turn the **Two-factor authentication** toggle switch on or off.
   If turned on, new customer tenants are provisioned with two-factor authentication.

> **Note**
> For more information, see the Management Portal Partner Administrator guide.

7. Turn the **Compliance mode** toggle switch on or off.
   Compliance mode is designed for higher security demands. It requires mandatory encryption for all backups and allows only locally set encryption passwords.

> **Note**
> For more information, see the Management Portal Partner Administrator guide.

   If you enable compliance mode, carefully review the information presented, then click either **Enable**.



8. Enter an **Administration email**.
   This is the administrator user email for provisioned Acronis customers.

© Acronis International GmbH, 2003-2025

Note
User activation links are sent to this email address.

9. Select the **Billing method** from the dropdown list.
   - **Per Workload**
     This billing method is based on the number of protected workloads. Cloud storage is charged separately.
   - **Per gigabyte**
     This billing method is based on the cloud and local storage used.
10. Click ✓.

Customer deprovisioning

When a mapped organization is removed from Kaseya VSA 10, the integration can deprovision the mapped Acronis customer.

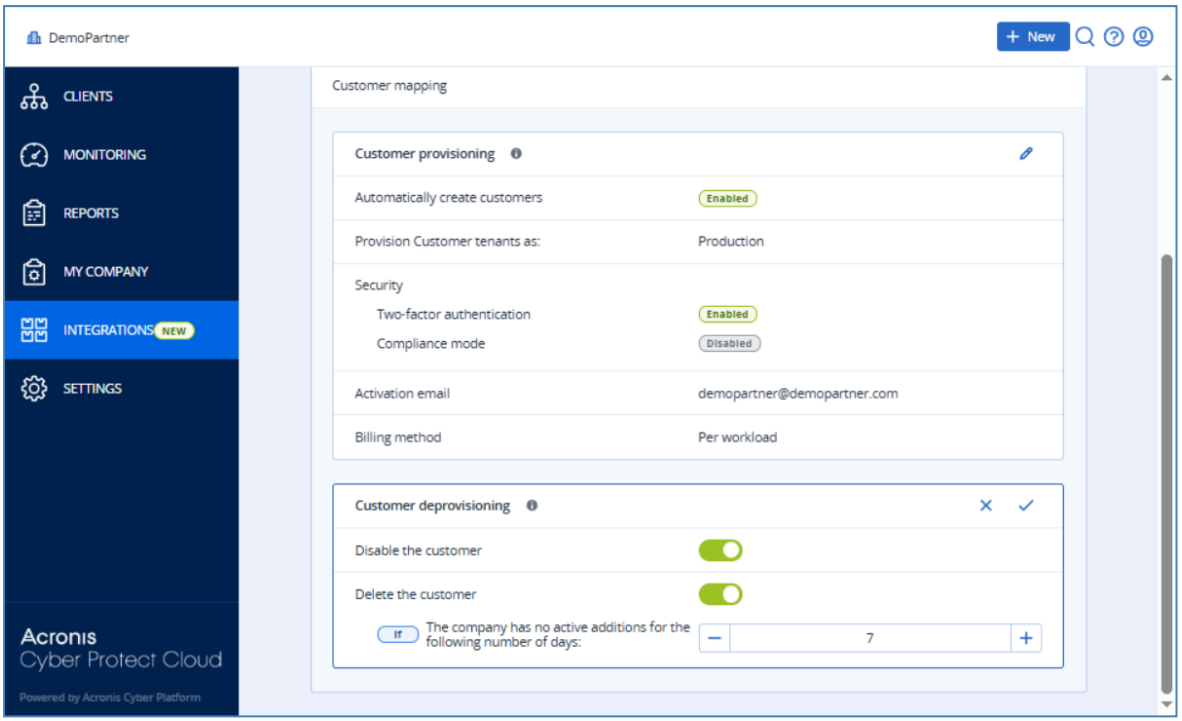
Note
Deprovisioning is a two-step process:

1. The integration disables the Acronis customer.
2. [After a specified number of days with no active additions] The integration deletes the Acronis customer and all related data.

To configure customer deprovisioning

1. Open the integration.
2. Select the **INTEGRATION SETTINGS** tab.
3. In the **Customer deprovisioning** section, click ✎.

© Acronis International GmbH, 2003-2025



4. Turn the **Disable the customer** toggle switch on of off.
   If you enable this functionality, when a Kaseya VSA 10 organization which you mapped to an Acronis customer is removed, the mapped Acronis customer is disabled.
5. [If you turn on the **Disable the customer** toggle switch] Turn the **Delete the customer** toggle switch on or off.
   If you enable this functionality, Acronis customers which have been disabled by the previous setting and all related data are subsequently deleted. You must use the number picker to specify how many days after disablement the deletion occurs.

   Note
   The Acronis customer is deleted if the company has no active additions during the specified period.

   Important
   You can prevent customer deletion by re-enabling the Acronis customer in Management Portal before the specified number of days have passed.

6. Click ✓.

© Acronis International GmbH, 2003-2025

Customers

You must map Kaseya VSA 10 organizations with Acronis customer tenants so that the integration can perform synchronization of monitoring statuses and alerts for those entities.

The CUSTOMER MAPPING tab

The **CUSTOMER MAPPING** tab lists all your Kaseya VSA 10 organizations. It displays:

- Kaseya VSA 10 customer name.
- The status of the integration mapping for the Kaseya VSA 10 customer.
  - **Not mapped** indicates that the Kaseya VSA 10 customer is not linked to an Acronis customer.
  - **Mapped** indicates that the Kaseya VSA 10 customer is linked to an Acronis customer tenant.
  - **Mapping error** means that an error occurred with the existing or while trying to apply a new mapping. For more details, click on the information icon right next to the status. Mapping errors will be cleared automatically on the next list reload, when the reason for the failure has been addressed.
- [For mapped Kaseya VSA 10 customers] The corresponding Acronis customer tenant.
- [If selected] The default protection plan for the mapped Kaseya VSA 10 customer organization.

Mapping customers

There are two ways to map Kaseya VSA 10 customers to Acronis customer tenants.

Mapping to existing Acronis customer tenants

If an appropriate Acronis customer tenant already exists, you can map a single Kaseya VSA 10 organization to it.

Note
For more information, see Mapping to an existing Acronis customer tenant.

Provisioning and mapping to new Acronis customer tenants

If there is no appropriate Acronis customer tenant, the integration can provision a new one and map the Kaseya VSA 10 organization to it.

Note
For more information, see Mapping to new Acronis customer tenants.

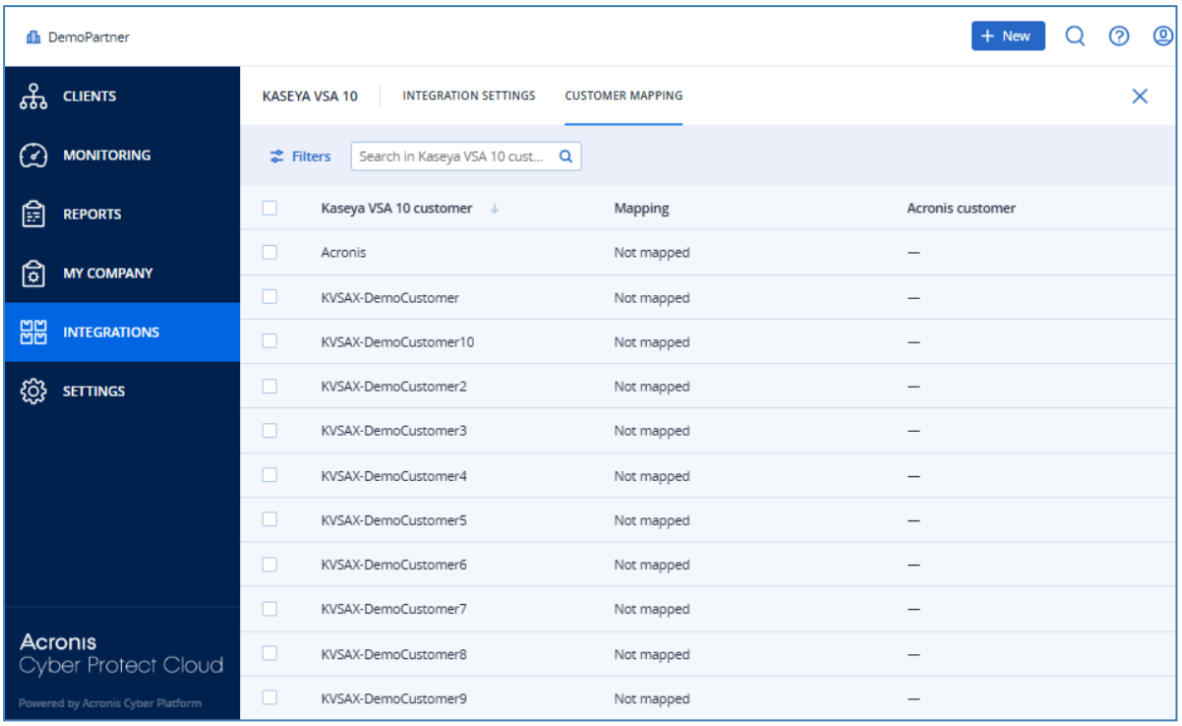
Mapping to an existing Acronis customer

If an appropriate Acronis customer already exists, you can map a Kaseya VSA 10 customer to it.

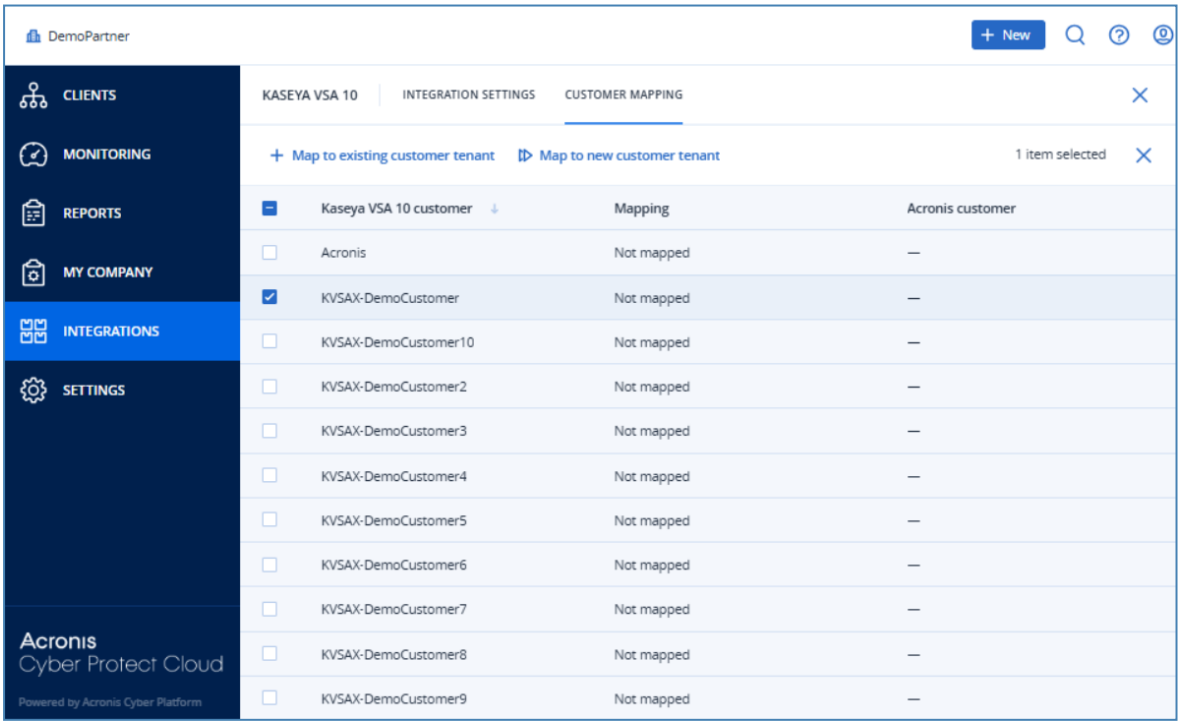
To map to an existing Acronis customer

© Acronis International GmbH, 2003-2025

1. Open the integration.
2. Select the **CUSTOMER MAPPING** tab.



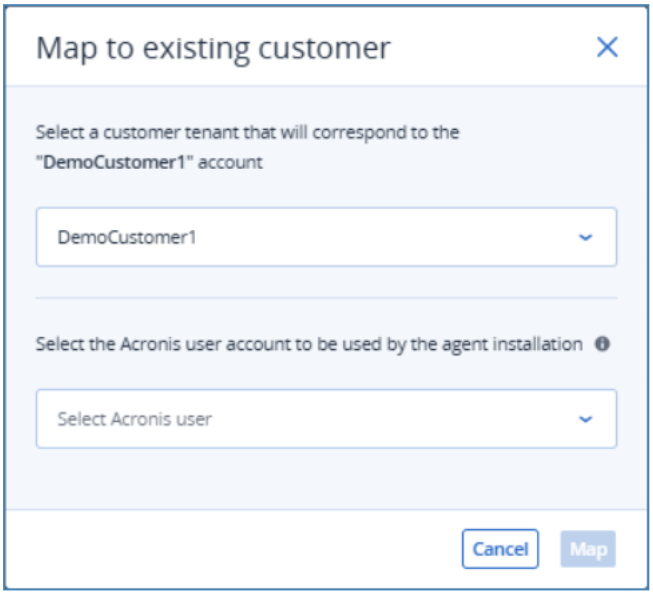
3. [Optional] Type in the **Search** field to filter the list based on the Kaseya VSA 10 organization names.
4. [Optional] Click Filters to refine the contents of the list by mapping status.
5. Select the Kaseya VSA 10 organization that you want to map.



6. Click **Map to existing customer tenant**.

© Acronis International GmbH, 2003-2025

Note
This button is only available if you select a single Kaseya VSA 10 organization.
You cannot map multiple Kaseya VSA 10 organizations to a single Acronis customer.



7. Select an Acronis customer tenant from the dropdown.

Note
Use the **Search** option to filter the list.

8. Select an Acronis user account from the dropdown.
   This is the user account that the agent installation will use.

Note
Only active users are available for selection.

9. Click **Map**.

Mapping to a new Acronis customer

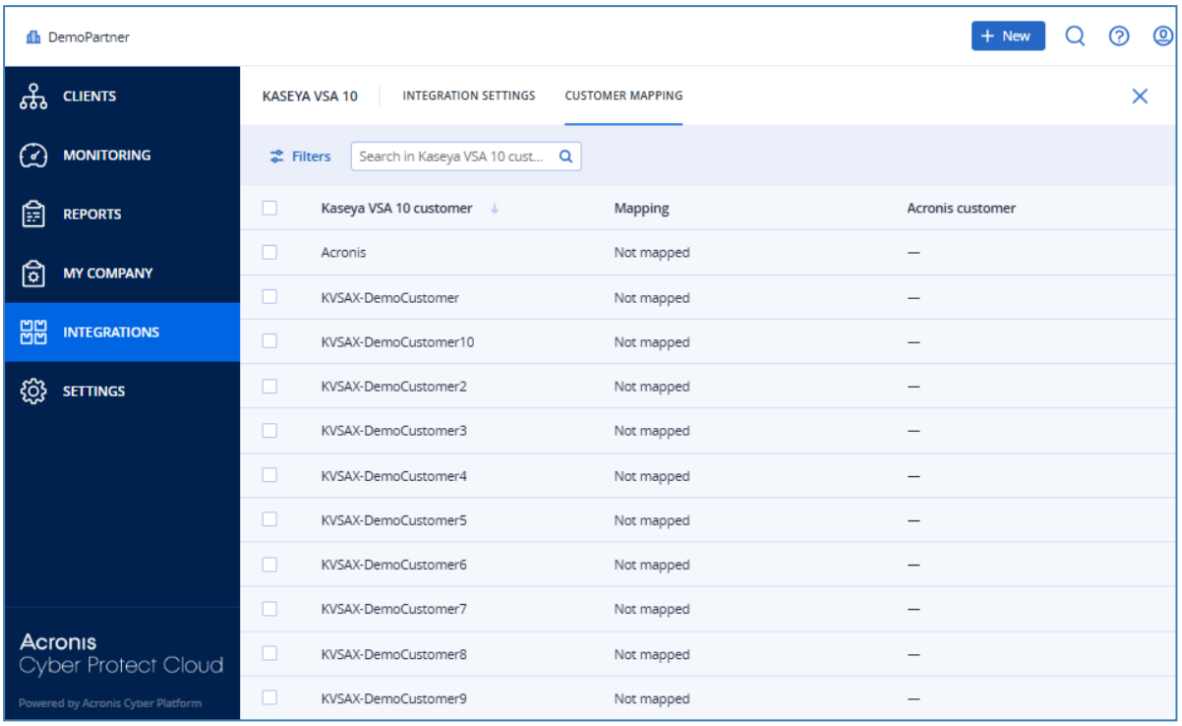
If there is no appropriate Acronis customer, the integration can provision a new customer tenant in Acronis and map the Kaseya VSA 10 organization to it.

The integration also creates an administrator user for the provisioned customer, because the Acronis agent can only be installed by an administrator. The activation email address for the new Acronis customer administrator user is specified in the Customer provisioning section of the INTEGRATION SETTINGS tab.

To map to a new Acronis customer

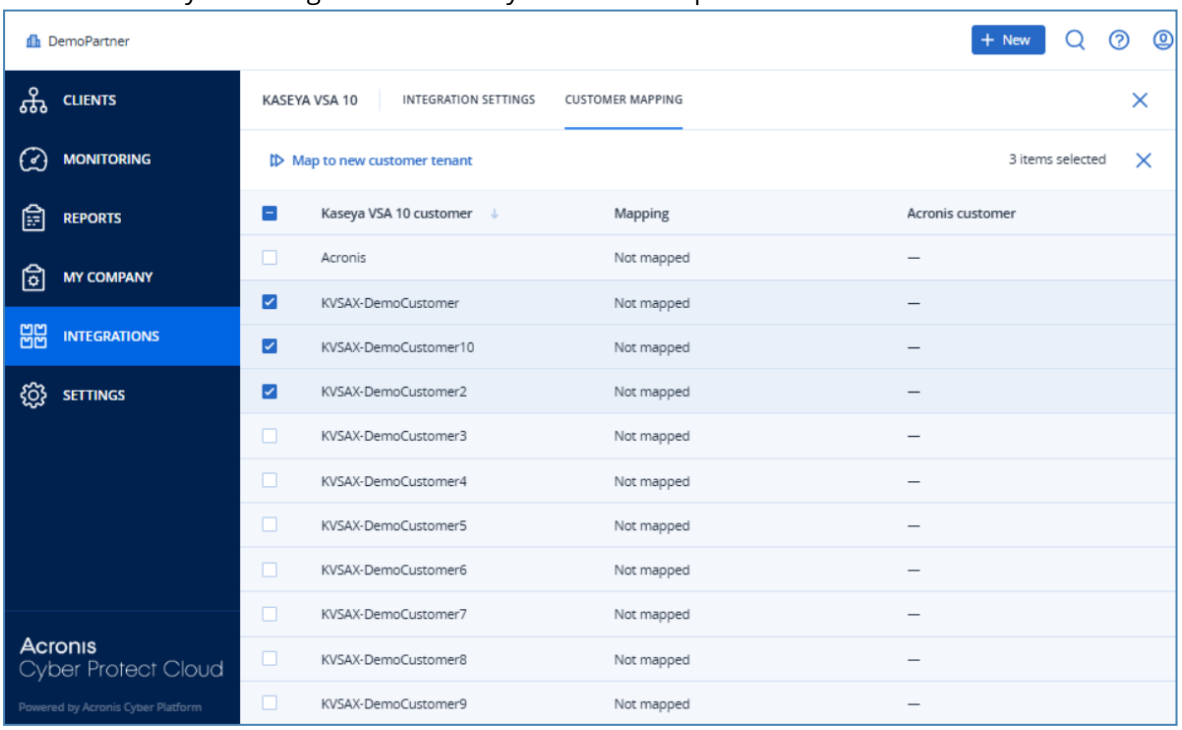
© Acronis International GmbH, 2003-2025

1. Open the integration.
2. Select the **CUSTOMER MAPPING** tab.



3. [Optional] Type in the **Search** field to filter the list based on the Kaseya VSA 10 organization names.
4. [Optional] Click Filters to refine the contents of the list by mapping status.

   Select the Kaseya BMS organizations that you want to map.

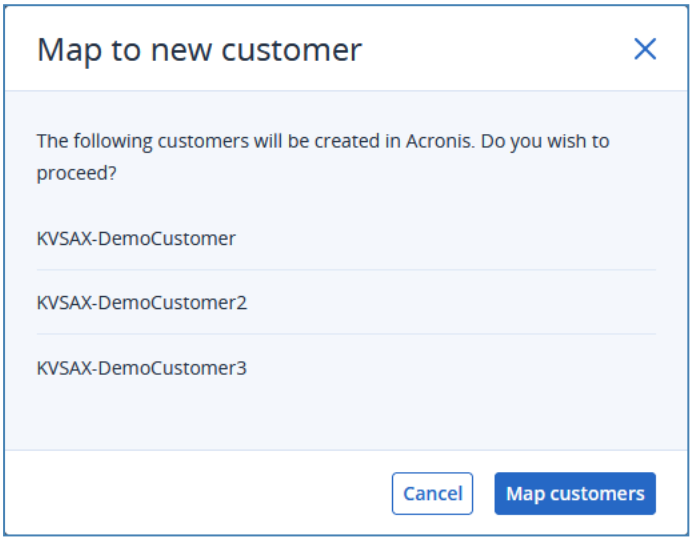


5. Select the Kaseya BMS organization you want to map.

© Acronis International GmbH, 2003-2025

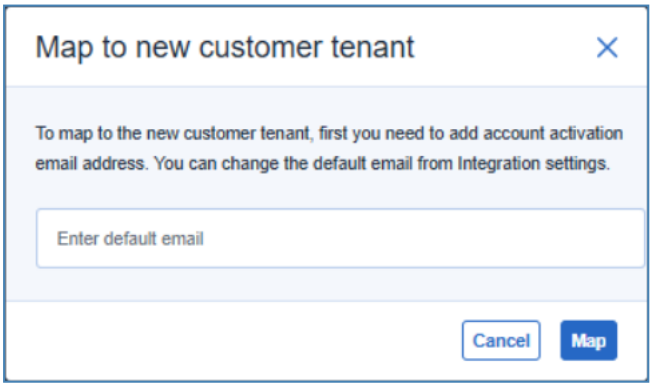
Note
You can select multiple Kaseya VSA 10 organizations for this action.

6. Click **Map to new customer tenant**.
7. [If you selected multiple customers] Verify the list of Kaseya VSA 10 customer organizations to provision and map, then click **Map customers**.



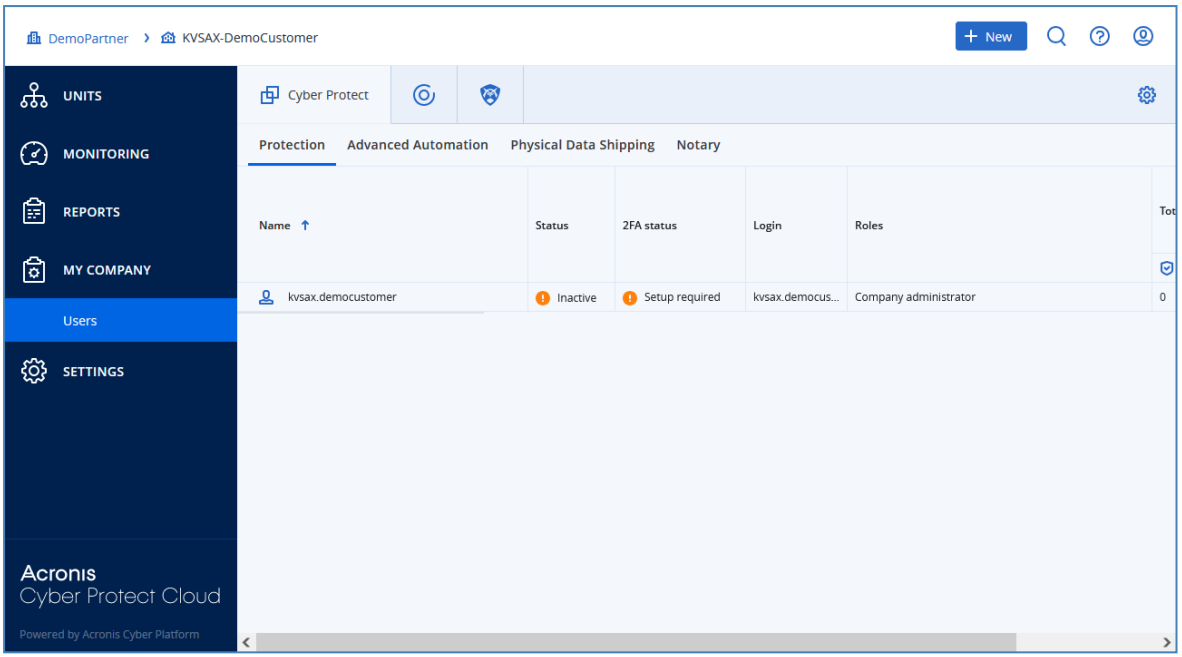
8. [If you have not yet specified the default **Activation email** in the **Customer provisioning** section of the **INTEGRATION SETTINGS** tab] Enter a default activation email.
   The email you enter here is assigned as the default **Activation email** value.

Note
For more information, see Customer provisioning.



9. Activate the newly provisioned Acronis customer administrator user.
   To do this, open the activation email, which is sent to the default customer provisioning activation email address and follow the instructions.

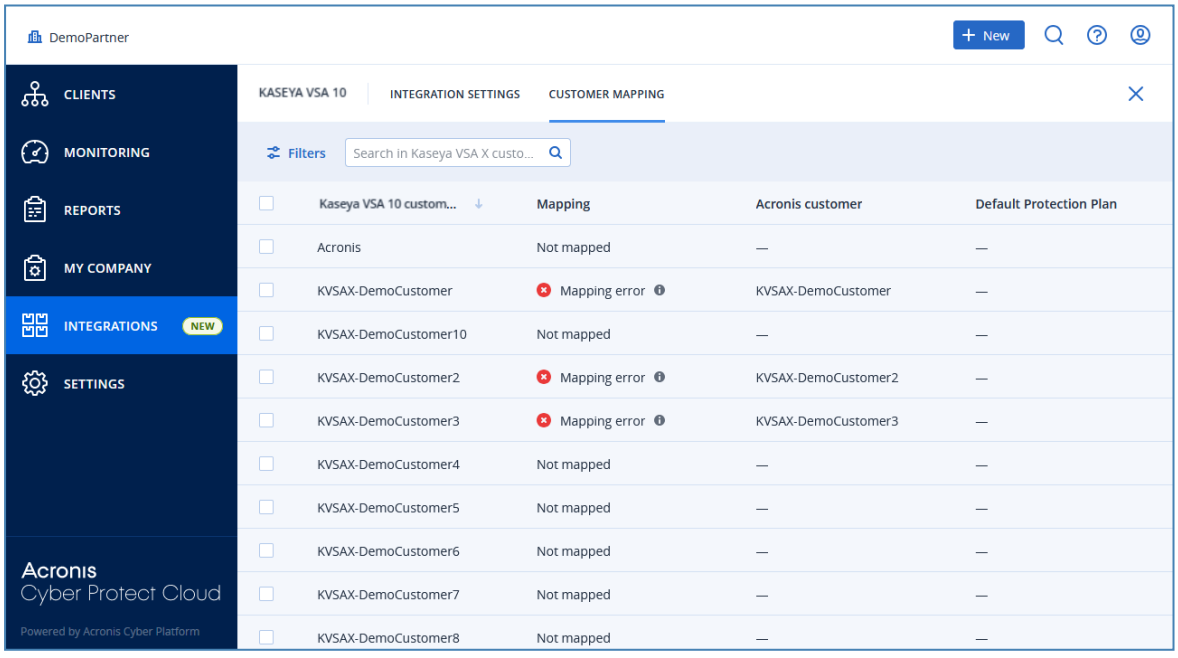
© Acronis International GmbH, 2003-2025



Note

When mapping is complete, the **Mapping** column entry for new customer mappings will display as mapped.

However, until you activate the newly provisioned Acronis customer administrator user, if you leave the **CUSTOMER MAPPING** tab and return to it, the **Mapping** column entry for new customer mappings will display a mapping error.



When you have activated the newly provisioned customer administrator user, the mapping error will clear at the next synchronization (synchronization occurs every 15 minutes).

© Acronis International GmbH, 2003-2025

Selecting a default protection plan

For each mapped customer tenant, you can select a default protection plan from the available protection plans for that customer.

If a default protection plan is selected for a mapped customer, the integration will create and refresh registration tokens that have extended scope to also apply or revoke protection plans.

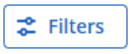
If no default protection plan is selected for a mapped customer, the integration will create and refresh registration tokens with normal scope.

The integration is then able to automatically apply the default protection plan to new workloads by workload type.

Note
For more information about protection plans, see Protection plans and modules.

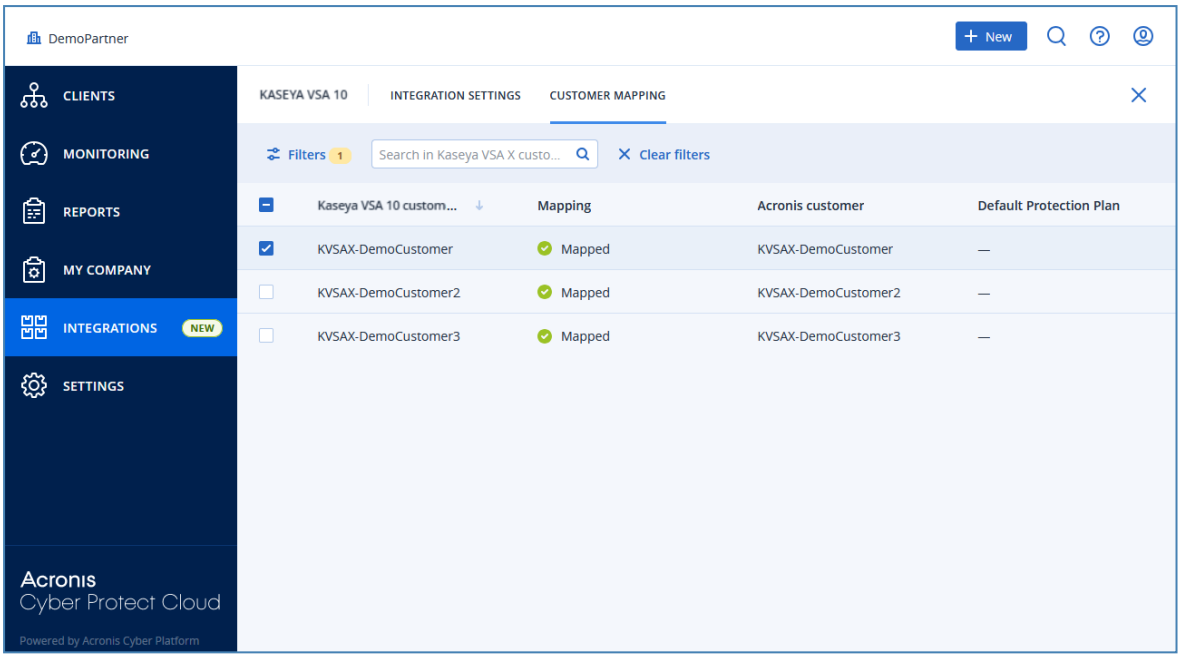
To select a default protection plan

Note
You must have already defined at least one protection plan for the mapped Acronis customer before you can perform this task.

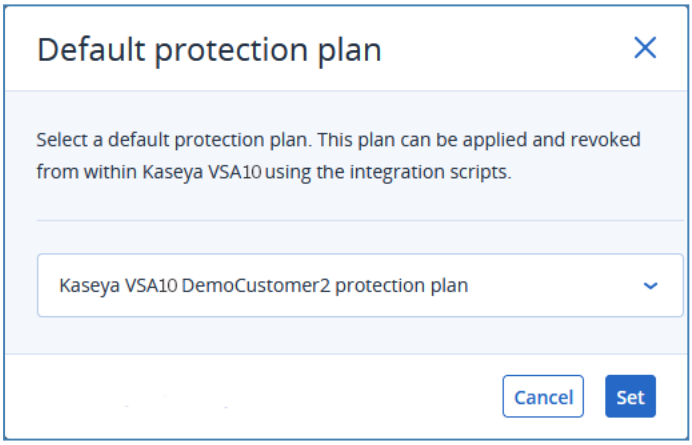
1. Open the integration.
2. Select the **CUSTOMER MAPPING** tab.
3. [Optional] Type in the **Search** field to filter the list.
4. [Optional] Click 

to refine the contents of the list by mapping status.
5. Select the Kaseya VSA 10 customer organization for which you want to select the default protection plan.

© Acronis International GmbH, 2003-2025



6. Click Default protection plan.



7. From the dropdown list, select the default protection plan for the mapped Kaseya VSA 10 customer.
8. Click **Set**.

Removing a default protection plan

You can remove the default protection plan for a mapped Kaseya VSA 10 customer organization.

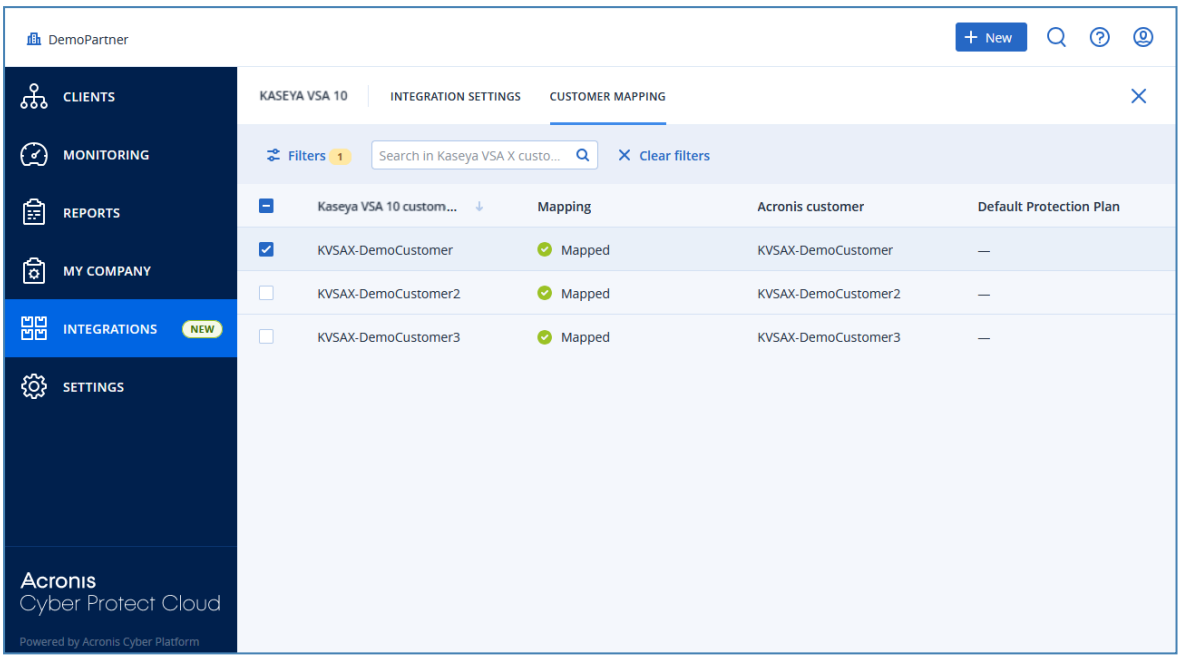
Note
For more information about protection plans, see Protection plans and modules.

To remove a default protection plan

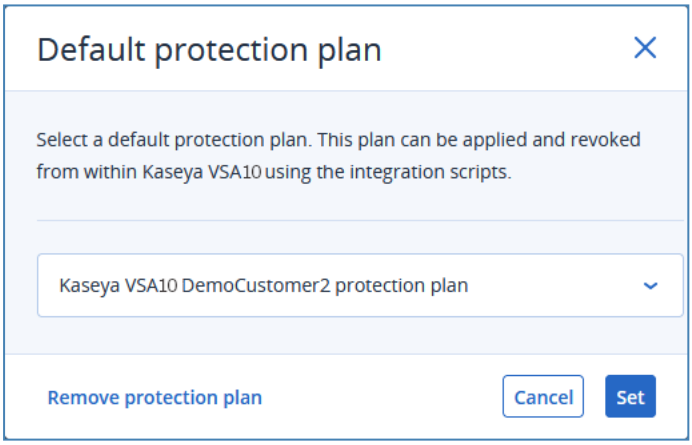
1. Open the integration.
2. Select the **CUSTOMER MAPPING** tab.
3. [Optional] Type in the **Search** field to filter the list.

© Acronis International GmbH, 2003-2025

4. Select the Kaseya VSA 10 customer organization for which you want to apply the default protection plan.



5. Click Default protection plan.



6. [If you have already selected a default protection plan for the Kaseya VSA 10 customer organization] Click **Remove protection plan**.

Removing a customer mapping

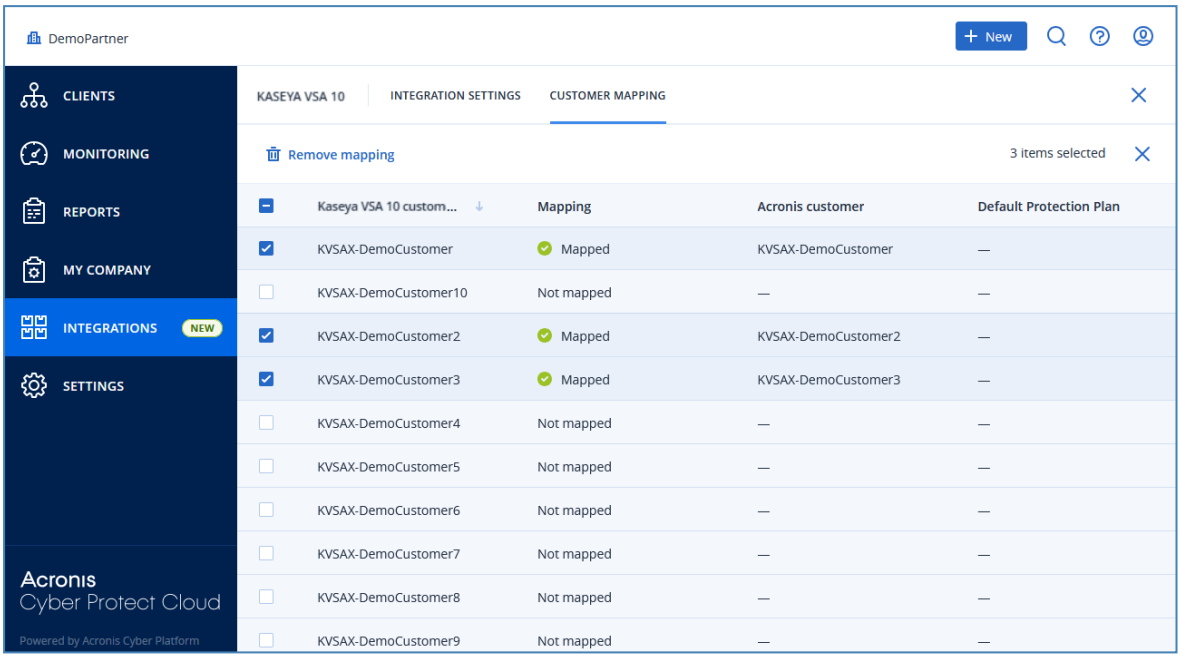
Note
The Acronis customer tenant and associated storage usage are not affected.

To remove a customer mapping

1. Open the integration.
2. Select the **CUSTOMER MAPPING** tab.
3. [Optional] Type in the **Search** field to filter the list.

© Acronis International GmbH, 2003-2025

4. [Optional] Click Filters to refine the contents of the list by **Mapping**.
5. Select the organizations for which you want to remove the mapping.



6. Click Remove mapping.
7. In the **Remove mapping** verification pop-up window, click **Remove**.

© Acronis International GmbH, 2003-2025

Acronis Content Package

When you activate the integration, Acronis provisions a content package on Kaseya VSA 10. The content package includes:

- Scripts

  Note
  For more information about Kaseya VSA 10 scripts, see the Kaseya VSA 10 help system.

- Workflows

  Note
  For more information about Kaseya VSA 10 workflows, see the Kaseya VSA 10 help system.

- Custom fields

  Note
  For more information about Kaseya VSA 10 custom fields, see the Kaseya VSA 10 help system.

Scripts

Important
Scripts will only run for Windows devices. You must use Acronis workflows to run scripts on multiple machine OS.
For more information, see Workflows.

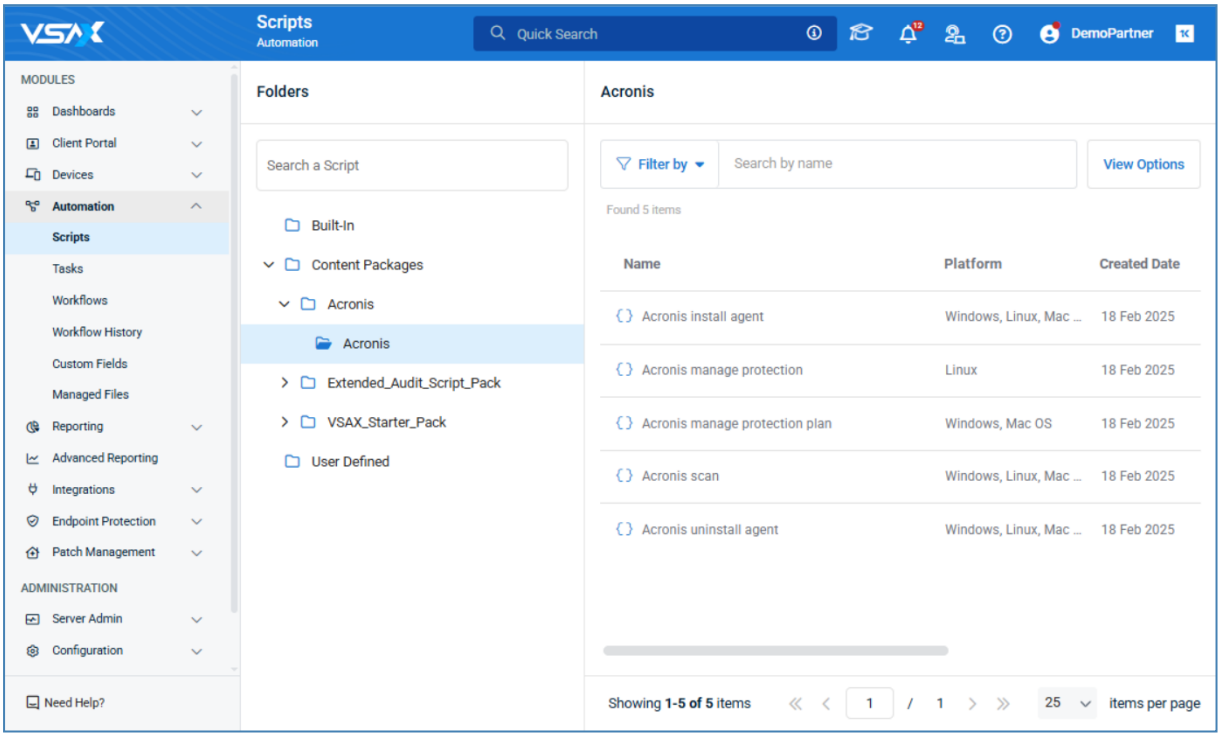
The Acronis content package provisions 5 Kaseya VSA 10 scripts:

- **Acronis install agent** (Windows, Linux, macOS)
  Installs the Acronis agent on Windows, Linux, and macOS devices. During installation of the Acronis agent, the integration registers the workload with Acronis and, if configured, applies a default protection plan.
- **Acronis manage protection** (Linux)
  Invokes or revokes the default Acronis protection plan on Linux devices.
- **Acronis manage protection plan** (Windows, macOS)
  Invokes or revokes the default Acronis protection plan on Windows and macOS devices.
- **Acronis scan** (Windows, Linux, macOS)
  Performs one of 5 Acronis scan tasks on Windows, Linux, and macOS devices:
  - backup
  - av_scan
  - malware_scan
  - vulnerability_assessment
  - patch_management

© Acronis International GmbH, 2003-2025

- **Acronis uninstall agent** (Windows, Linux, macOS)
  Uninstalls the Acronis agent from Windows, Linux, and macOS devices.

Note
For more information about Kaseya VSA 10 scripts, see the Kaseya VSA 10 help system.



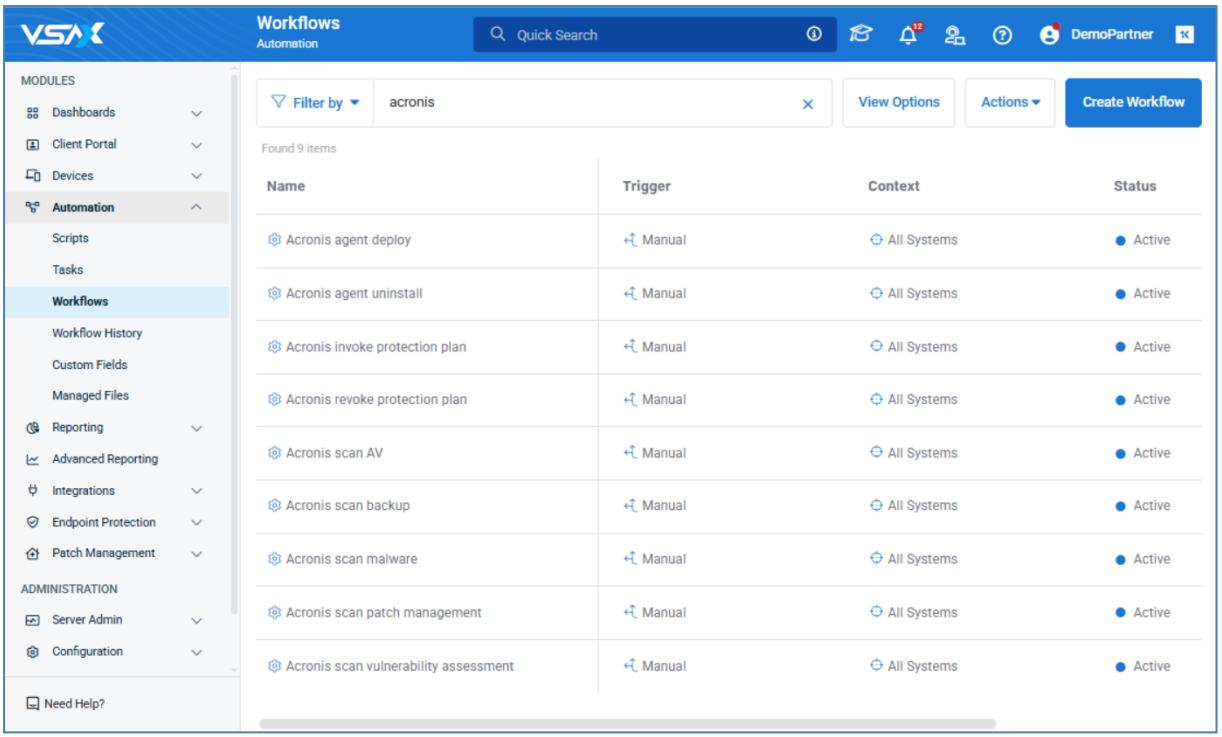
Workflows

Note
For more information about Kaseya VSA 10 workflows, see the Kaseya VSA 10 help system.

The Acronis content package provisions 10 Kaseya VSA 10 workflows:

- **Acronis agent deploy**
- **Acronis agent uninstall**
- **Acronis invoke protection plan**
- **Acronis revoke protection plan**
- **Acronis scan AV**
- **Acronis scan backup**
- **Acronis scan malware**
- **Acronis scan patch management**
- **Acronis scan vulnerability assessment**

© Acronis International GmbH, 2003-2025



Custom fields

Note
For more information about Kaseya VSA 10 custom fields, see the Kaseya VSA 10 help system.

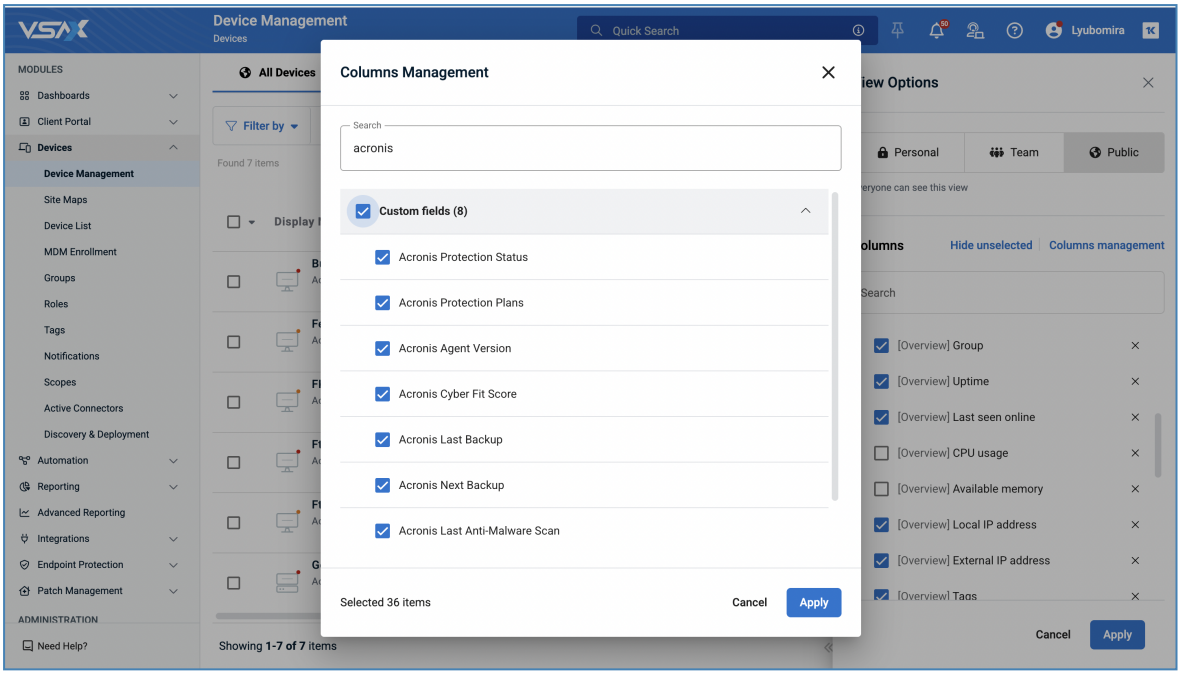
The Acronis content package provisions 10 Kaseya VSA 10 custom fields. These fields are used to display the status of devices with the Acronis agent installed.

You can add Acronis custom fields as columns in the Kaseya VSA 10 device management table, and then sort and filter with them.

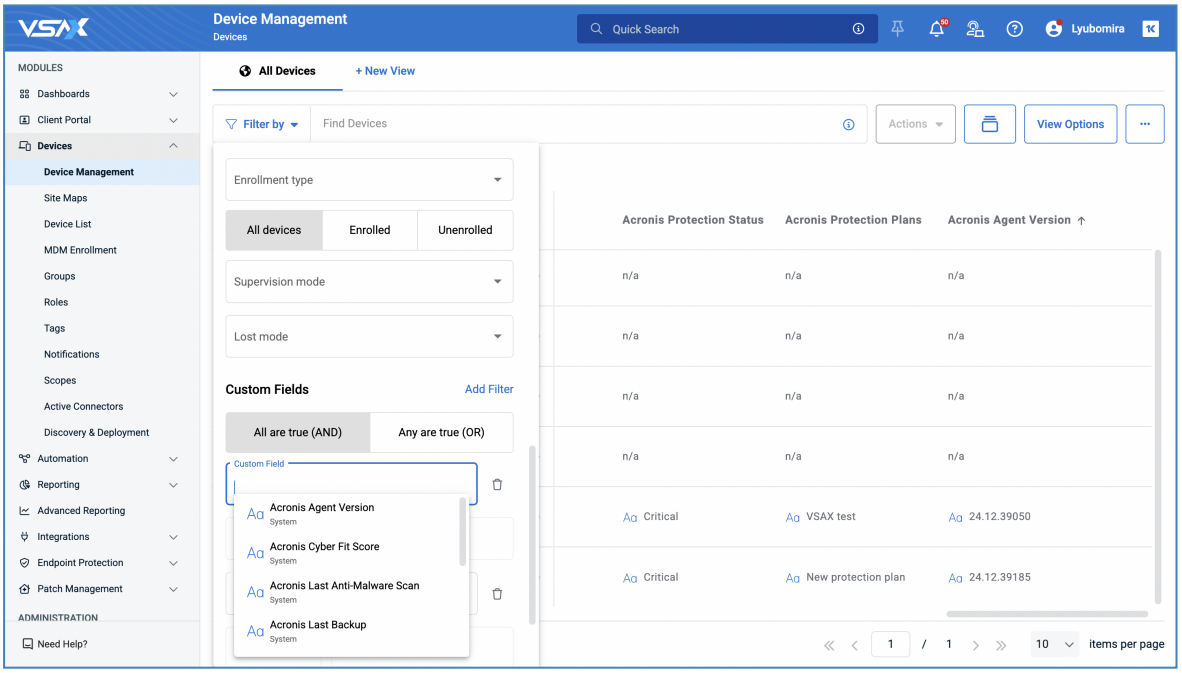
To do this:

1. Log in to Kaseya VSA 10.
2. Go to **Device Management** > **View Options** > **Columns Management**.

© Acronis International GmbH, 2003-2025



3. Search for 'Acronis' and add the custom fields in the list of columns.



List of provisioned custom fields

- **Acronis Protection Status**
- **Acronis Protection Plans**
- **Acronis Agent Version**
- **Acronis Cyber Fit Score**
- **Acronis Last Backup**
- **Acronis Next Backup**

© Acronis International GmbH, 2003-2025

- **Acronis Last Anti-Malware Scan**
- **Acronis Next Anti-Malware Scan**

  Organization custom fields:

  - **Acronis Data Center URL**
  - **Acronis Registration Token**

© Acronis International GmbH, 2003-2025

Monitoring device status

Note

Currently, Acronis custom fields are displayed in the **Custom fields** tab of the device details screen. In an upcoming release, Kaseya VSA 10 will allow users to include custom fields in the device management table. When this functionality is released, you will be able to add columns from Acronis custom fields, and sort and filter by the status of those custom fields.

Note

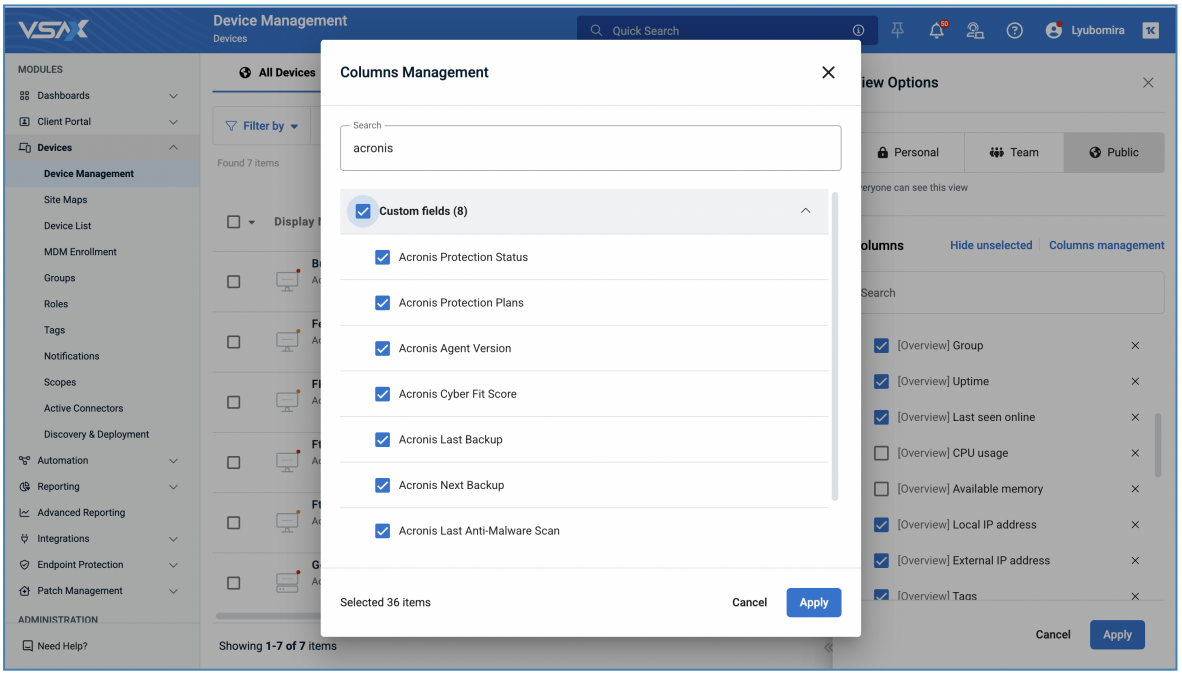
If an Acronis custom field has a value, it is displayed. If it has no value, it is hidden.

To monitor the status of devices with the Acronis agent installed

You can add Acronis custom fields as columns in the Kaseya VSA 10 device management table, and then sort and filter with them.

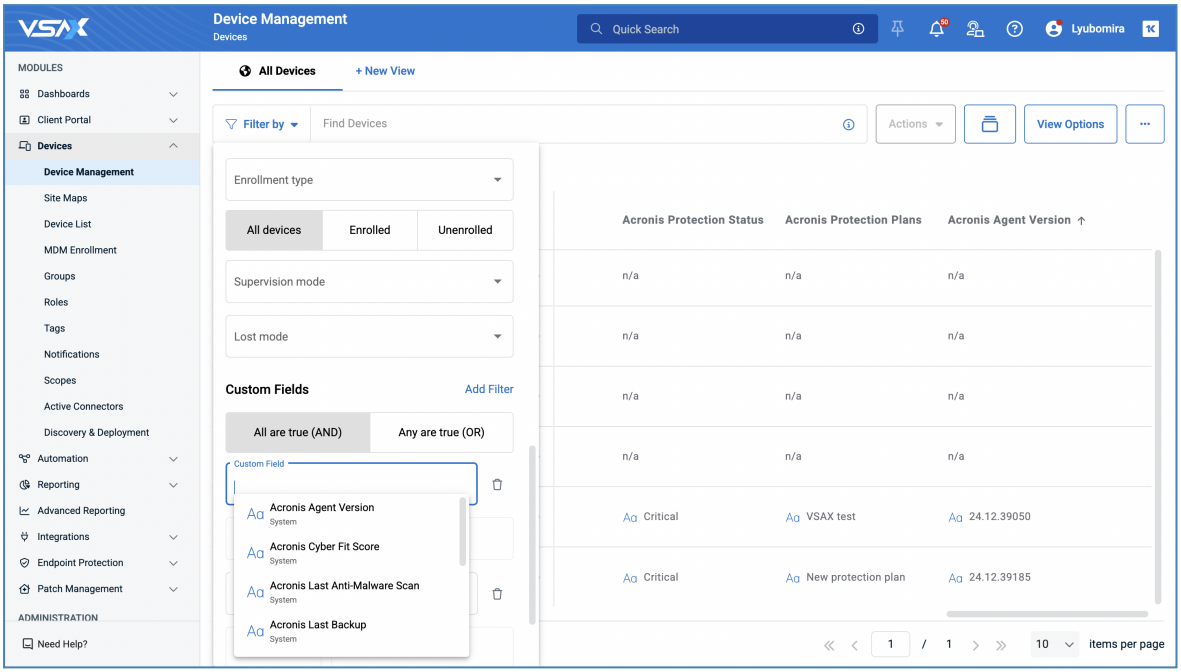
To do this:

1. Log in to Kaseya VSA 10.
2. Go to **Device Management** > **View Options** > **Columns Management**.



© Acronis International GmbH, 2003-2025

3. Search for 'Acronis' and add the custom fields in the list of columns.



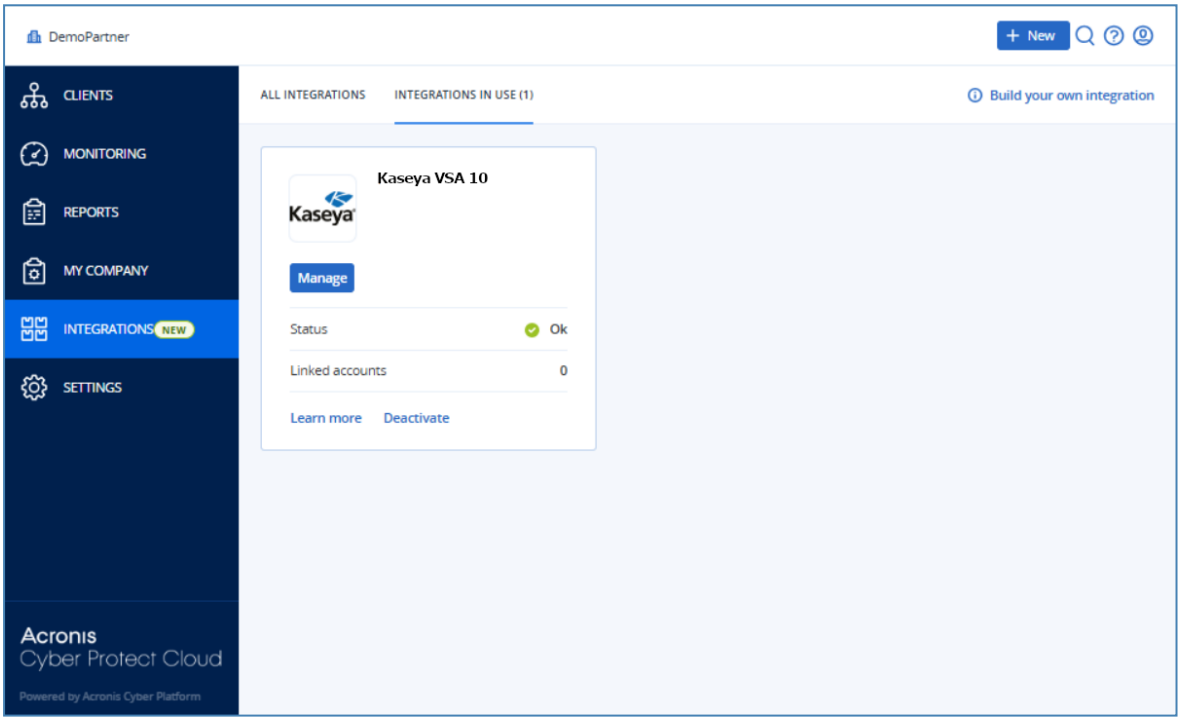
© Acronis International GmbH, 2003-2025

Deactivating the integration

To deactivate the integration

1. Log in to Acronis Management Portal as administrator.
2. In the main menu, select **INTEGRATIONS**.
3. Select the **INTEGRATION IN USE** tab.
4. Locate the Kaseya VSA 10 integration catalog card.

Note
For more information, see the Management Portal partner administrator guide.



5. Click **Deactivate**.
6. Click **Delete**.

© Acronis International GmbH, 2003-2025

Index

© Acronis International GmbH, 2003-2025