Acronis

Acronis Cyber Cloud

Integration with CloudBlue PSA

INTEGRATION GUIDE

Revision: 6/18/2021

Table of contents

© Acronis International GmbH, 2003-2021

1 Introduction

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

Once setup, the integration enables the following actions:

- Linking CloudBlue PSA customers to Acronis customer tenants
- Getting tickets in CloudBlue PSA, based on alerts from Acronis
- Configuring automatic ticket resolution and reopening in CloudBlue PSA
- Configuring automatic alert clearing in Acronis

© Acronis International GmbH, 2003-2021

2 Prerequisites and Supported Systems

To use this integration, you should have:

- A setup and configured CloudBlue PSA instance
- An account in CloudBlue PSA
- A setup Acronis Cyber Cloud partner account

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

The Acronis integration can work with:

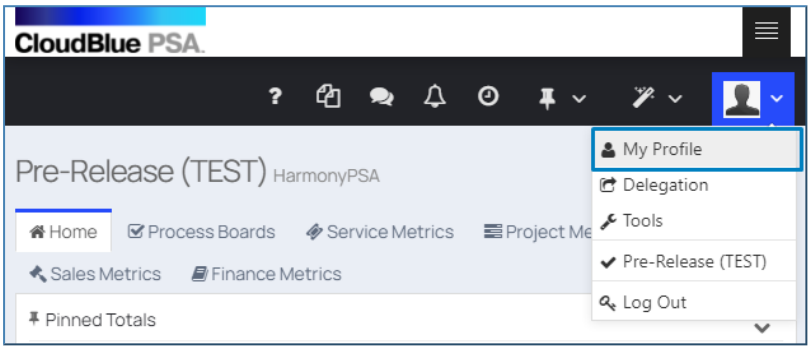
- CloudBlue PSA 4.25 or higher
- Acronis Cyber Cloud 21.06 or higher

© Acronis International GmbH, 2003-2021

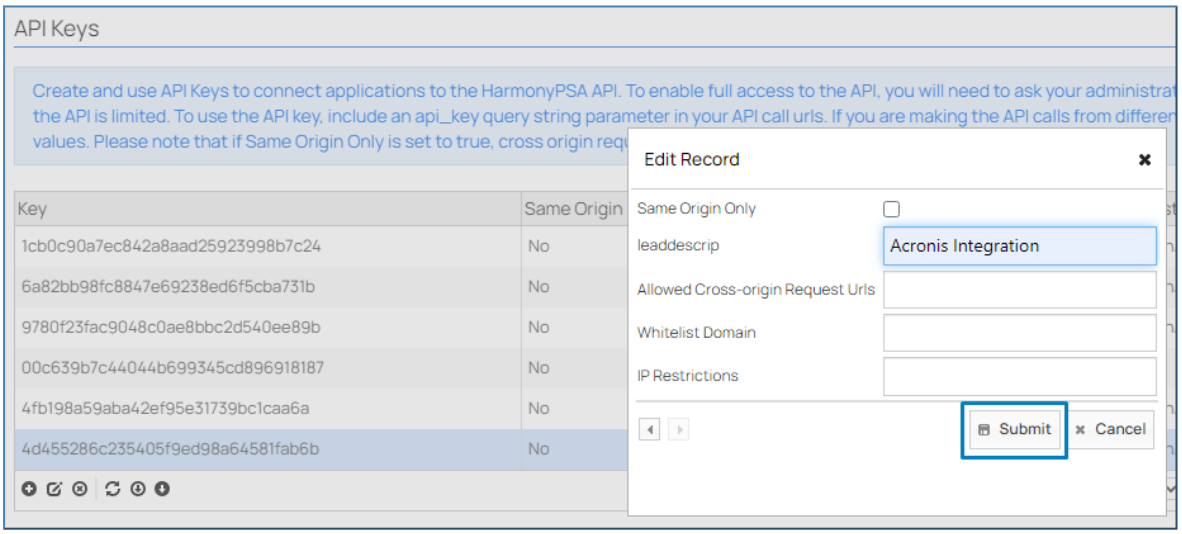
3 Setting up the Integration

3.1 Generating an API Key in CloudBlue PSA

1. Log in to the CloudBlue PSA app.
2. Click on the user name in the top right corner and select **My Profile**.



3. Scroll down to the **API Keys** section of the **Profile** page.
4. Click on the **+** sign at the bottom of the **API keys** table to open the new **API key** window.
5. Provide a name for the new API key and click **Submit**.



6. Copy the new API key generated and displayed in the list.

3.2 Setting up Integration with CloudBlue PSA

1. Log in to the Acronis Cyber Cloud Management portal.
2. Go to **Settings** > **Integration** > **CloudBlue PSA**.
3. Provide your **CloudBlue PSA** site and **API key**.
4. Click **Save**.

© Acronis International GmbH, 2003-2021

As a result, you should have configured the integration between Acronis Cyber Cloud and CloudBlue PSA.

After the integration is setup successfully, the following three major sections will be visible and accessible:

- **Integration Settings**
  Provides all configuration options for the integration:
  - Enable/disable ticket creation feature
  - Configure the way customer tenants are provisioned in Acronis
  - Configure the synchronization between Acronis alerts and CloudBlue PSA tickets
- **Customer Mapping**
  Provides functionality to map CloudBlue PSA customers to new or existing Acronis customer tenants
- **Ticket Creation**
  Provides functionality that configures which alerts raised in Acronis should have tickets created in CloudBlue PSA

© Acronis International GmbH, 2003-2021

4 Configuring the Integration

4.1 Mapping CloudBlue PSA Customers

The **Customer Mapping** tab displays the mapping between the CloudBlue PSA customers and the Acronis customer tenants.
It lists all the customers that can be currently found in CloudBlue PSA. For every such customer, the table displays:

- Customer status in CloudBlue PSA
- Mapping status
- Name of the Acronis customer tenant for those customers that are linked.

The mapping status can have one of the following values:

- **Not mapped** indicates that the current CloudBlue PSA customer is *not* linked to Acronis.
- **Mapped** indicates that the current CloudBlue PSA customer is linked to the Acronis customer tenant, displayed in the next column.
- **Mapping failed** means that an error occurred with the existing or while trying to apply a new mapping. For error details, click on the information icon right next to the status. Mapping errors will be cleared automatically on the next list reload.

Use the **Search** box to quickly find CloudBlue PSA customers by their name or part of it. The **Filter** button can be used also to filter the content of the mapping list.

There are two ways to map CloudBlue PSA customers to Acronis customer tenants:

- Map the CloudBlue PSA customer to existing Acronis customer tenants, already created under the current partner account. Each Acronis customer tenant can be mapped only to a single CloudBlue PSA customer.
- If an Acronis customer tenant, suitable for mapping to a CloudBlue PSA customer, is missing, then you can create a new one and map it automatically.

Mapped customers can be unlinked at anytime. CloudBlue PSA tickets, already created for the unlinked customers, will not be affected.

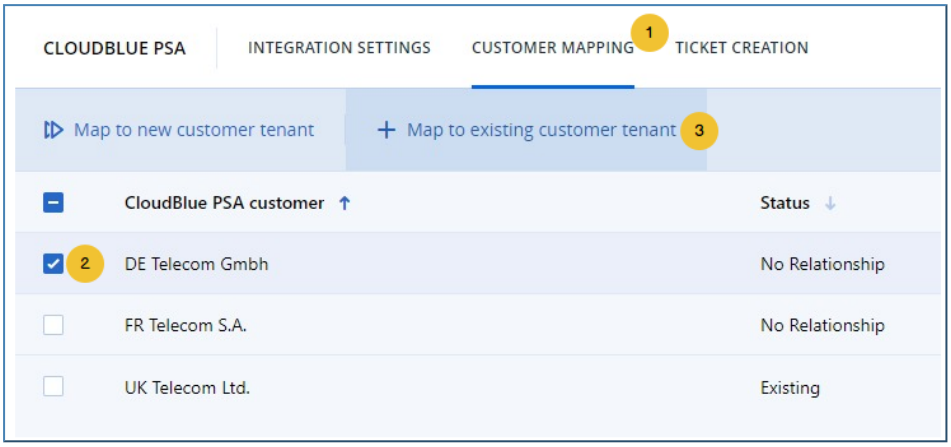
4.1.1 Map to Existing Acronis Customer Tenants

To link a CloudBlue PSA customer to an existing Acronis customer tenant, do the following:

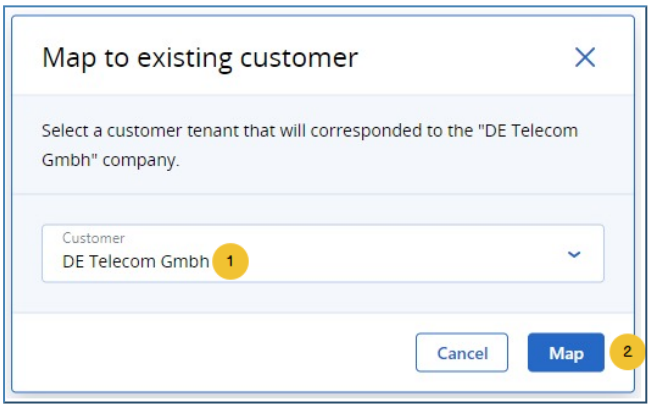
1. Go to the **Customer Mapping** tab.
2. Locate and select the row with the CloudBlue customer you want to link.

© Acronis International GmbH, 2003-2021

3. Click the **Map to existing customer tenant** button in the action bar.

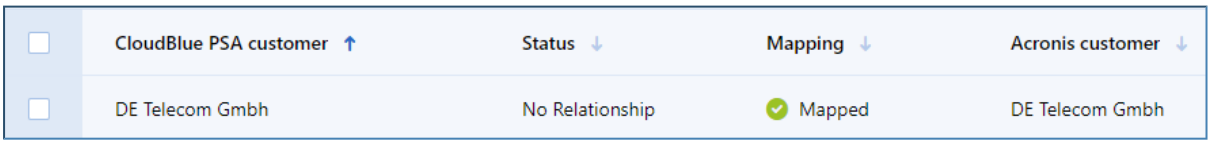


4. In the window that opens next, select the Acronis customer tenant you want to link.



5. Click **Map**.

The mapping will be applied and its status changed to **Mapped**. The **Acronis customer** column will display the name of the linked Acronis customer tenant.



4.1.2 Provision New Acronis Customer Tenants

To link a CloudBlue PSA customer to a new Acronis customer tenant:

1. Go to the **Customer Mapping** tab.
2. Locate and select the row with the CloudBlue customer you want to link.
3. Click the **Map to new customer tenant** button in the action bar.

The integration will display the following message: "**The mapping has been saved**". A request to create a new customer tenant will be issued to the Acronis Cyber Cloud platform. When this

© Acronis International GmbH, 2003-2021

operation is completed, the list will be refreshed to show the current mapping status as well as the linked customer tenant.

There are different options to create new Acronis customer tenants, explained in the next chapter.

4.1.3 Configuration Options for Provisioning New Acronis Customer Tenants

To configure the way administrator accounts of Acronis customer tenants are created:

1. Go to **Customer Provisioning** section > **Integration Settings** tab to change options.
2. The following choices are available:

- **Create accounts based on** can have one of two values:
  - ***Company primary contact*** *(default)*
  - ***Company name***
- **Activation email** is visible only when accounts are created based on the company name (option 2 above)
- **How to set account password** can have two possible values:
  - ***Send activation email*** *(default)*
  - ***Define manually***
- **Two-factor authentication** is disabled by default

Depending on the combination of the above options, when new customer tenant is created in Acronis, the associated administrator account (login) can be created in any of the below-listed different ways:

- If the **Create accounts based on** option is set to **Company primary contact**, then the created account will have details extracted from the primary contact of the mapped CloudBlue PSA customer as follows:
  - User login is set to the CloudBlue PSA primary contact first+last name
  - User email is set to CloudBlue PSA primary contact email
  - First name is set to CloudBlue PSA primary contact first name
  - Last name is set to CloudBlue PSA primary contact last name
- If the **Create accounts based on** option is set to **Company name**, then the created account will have details as follows:
  - User login is set to the company name
  - User email is set to Activation email value
  - First and last name are left empty
- If **How to set account password** is set to **Send activation email**, then the account password will be defined by the user after responding to the activation email sent by Acronis.
- If **How to set account password** is set to **Define manually**, then the account password will be set to the values, defined in the password fields.

© Acronis International GmbH, 2003-2021

Note
Using this option means all new accounts will have the same password.

- If **Two-factor authentication** is ON, then the new tenant will have 2FA enabled.
- If **Two-factor authentication** is OFF, then the new tenant will have 2FA disabled.

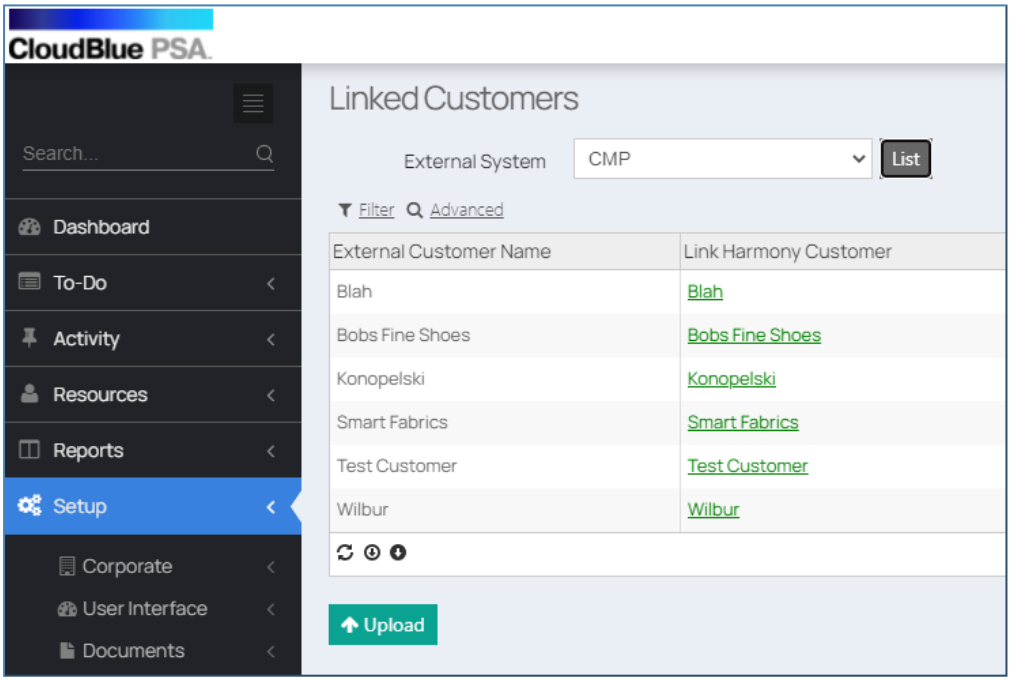
4.1.4 Ingram Cloud MarketPlace Customer Synchronization

It is very likely for Partners to use Ingram Cloud Marketplace to provision their customers and Acronis services.

Another Acronis integration is responsible for the provisioning flow, which ends up with Acronis customer tenants created and their services configured on Acronis side.

To identify customers provisioned in Ingram Cloud MarketPlace on CloudBlue PSA side:

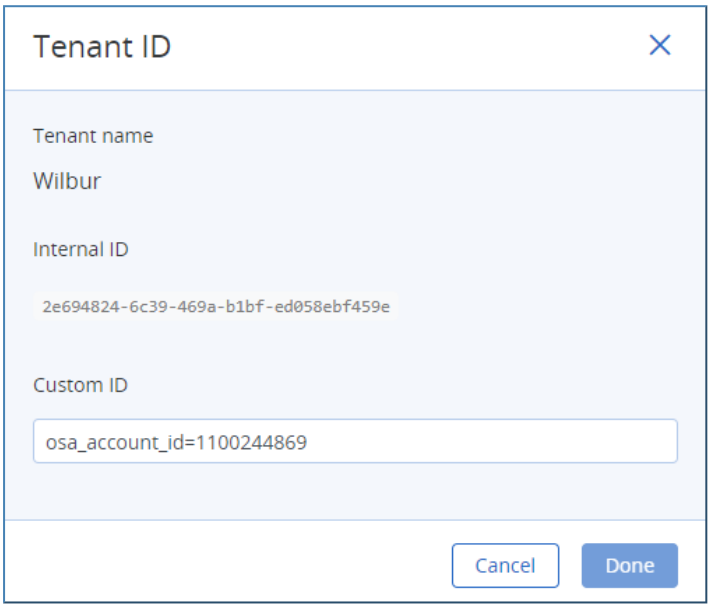
1. Go to **Setup** > **External System** > **Customers** > **Linked**.
2. From the **External System** drop-down, select **CMP** and click **List**.



© Acronis International GmbH, 2003-2021

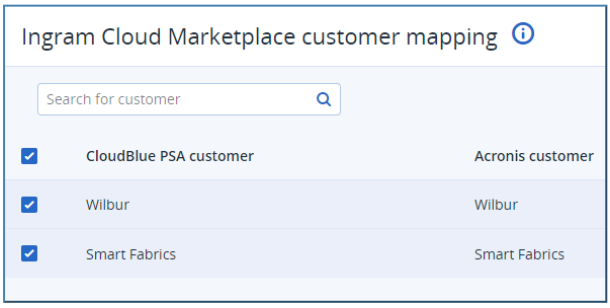
On Acronis side, you can identify whether customers are provisioned from Ingram Cloud MarketPlace by checking the **Custom ID** property of the respective customer tenant. For that purpose:

1. Right-click on the tenant.
2. Select **Show ID**.



If the **Custom ID** field has a value with pattern of the following type: osa_account_id=[some number], this means the customer tenant has been provisioned from the Ingram Cloud Marketplace.

Acronis CloudBlue PSA integration can detect such provisioning scenario. In this case, the integration provides additional wizard to help in mapping customers provisioned through this path. This is indicated by a **Map through Ingram Marketplace** button, available in the action toolbar, which starts the customer synchronization wizard. It does automatic matching between CloudBlue PSA customers and Acronis customer tenants, based on their associated Ingram IDs. The partner can review the proposed matching and confirm it.



The wizard also starts automatically right after completing the integration installation.

© Acronis International GmbH, 2003-2021

4.2 Mapping Alerts to Tickets

4.2.1 Enabling Ticket Creation Feature

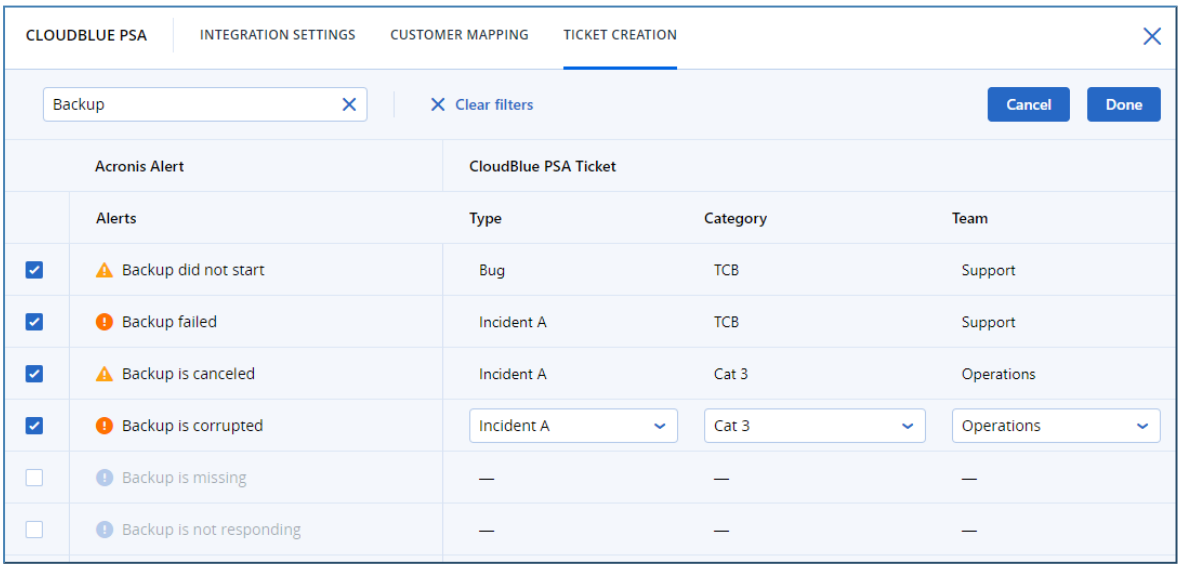
By default, the ticket creation feature is disabled after CloudBlue PSA installation. To enable it:

1. Go to the **Integration settings** tab.
2. Locate the ticket creation feature switch button.
3. Turn the feature on.

4.2.2 Choosing Acronis Alerts that Generate Tickets

To configure which alerts should generate tickets in CloudBlue PSA:

1. Go to the **Ticket creation** tab.
2. Locate the alert you want to configure. You can use the Filter box at the top to sort the alerts by their name.
3. Enable ticket generation for a particular alert by selecting its associated checkbox.
4. Specify values for **Type**, **Category** and **Team** to be used when creating the ticket in CloudBlue PSA. The values of these properties depend on the CloudBlue PSA ticket configuration.



5. Click **Done**.

© Acronis International GmbH, 2003-2021

5 CloudBlue Ticket Synchronization Flow

Once you finish mapping customers and configuring alert mapping, the integration takes care of ticket creation and synchronization between Acronis and CloudBlue PSA. The minimum requirement is to have at least one linked customer and one linked alert in order to have functional ticket generation.

There can be different synchronization flows, depending on the integration configuration. The next sections describe the possible scenarios.

5.1 Generating Tickets in CloudBlue PSA

This scenario is active as long as the ticket creation feature is enabled on the **Integration settings** tab. Generating tickets in CloudBlue PSA has the following preconditions:

- Acronis alerts are enabled and mapped from the **Ticket creation** tab.
- Acronis customer tenants are mapped to CloudBlue PSA customers.
- The mapped Acronis customer tenants always have at least a single protected workload.
- The protected workload encounters a problem, which raises the alert, mapped in step 1.

When these conditions are satisfied, the integration does the following:

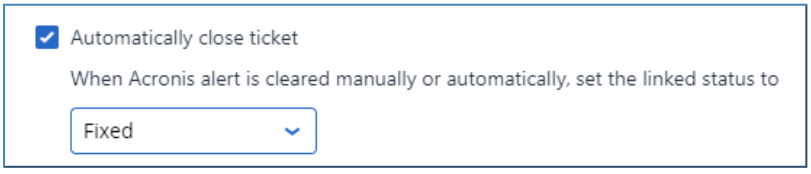
- Creates a ticket in CloudBlue PSA.
- Ticket status is set to **New**.
- The **Type**, **Category** and **Team** ticket fields are set according to the mapped alert configuration.
- The **Customer** ticket field is set to the mapped CloudBlue PSA customer.

5.2 Resolving Tickets in CloudBlue PSA

In this scenario, the integration can resolve a linked ticket in CloudBlue PSA when the originating Acronis alert is cleared.

By default, this option is disabled. To turn it on:

1. Go to **Integration settings** tab.
2. Locate the **Tickets** section and click on **Edit** in the top right.
3. Enable the **Automatically close ticket** option.
4. Use the **Status** drop-down list to select the desired value for setting the ticket to resolved state.



Once enabled, the following conditions are satisfied:

© Acronis International GmbH, 2003-2021

- An alert is raised on Acronis side.
- A ticket has been created in CloudBlue PSA.
- The alert is cleared in Acronis (manually or automatically).

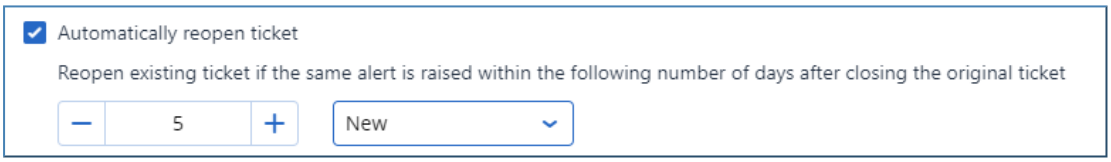
In this case, the integration resolves the ticket automatically by setting the **Status** field to the value selected from the drop-down.

5.3 Reopening Tickets in CloudBlue PSA

In this scenario, the integration can reopen an already resolved ticket within a certain period of time after the resolution.

By default, this option is disabled. To turn it on:

1. Go to the **Integration settings** tab.
2. Locate the **Tickets** section and click on **Edit** in the top right.
3. Enable the **Automatically reopen ticket** option.
4. In the **Days** numeric field, set maximum number of days that should have passed after closing the ticket and before the integration creates a new one.
5. Use the **Status** drop-down list to select desired value for setting the ticket to reopen state.



Once enabled, the following conditions are met:

1. An alert is raised in Acronis.
2. A ticket has been created in CloudBlue PSA.
3. The ticket has been resolved and the alert - cleared on Acronis side.
4. The same alert is raised again.
5. The number of days passed since the original ticket has been resolved are less than those configured in the above option.

In this case, the integration will not create a new ticket for the alert, but rather reopen the original ticket, setting the **Status** field to the drop-down option value. If the number of days passed since the original ticket has been resolved are more than the number configured in the option above, then a new ticket will be created.

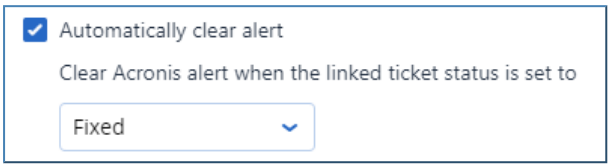
5.4 Clearing Alerts in Acronis

In this scenario, the integration can clear an originating Acronis alert by detecting if linked CloudBlue PSA ticket has been resolved.

By default, this option is disabled. To turn it on:

© Acronis International GmbH, 2003-2021

1. Go to the **Integration settings** tab.
2. Locate the **Tickets** section and click **Edit** in the top right.
3. Enable the **Automatically clear alert** option.
4. Use the **Status** drop-down list to select value for the ticket to clear the Acronis alert.



Once enabled, the following conditions are true:

- An alert is raised in Acronis.
- A ticket has been created in CloudBlue PSA.
- The ticket status has been changed to the value, configured in the drop-down above.

In this case, the integration will clear the originating Acronis alert.

© Acronis International GmbH, 2003-2021