Acronis

acronis.com

Acronis Cyber Cloud

Integration with ConnectWise Automate

Integration Guide

REVISION: 4/10/2023

Table of contents

Introduction

This document describes how to install and use the Acronis Cyber Cloud plugin for ConnectWise Automate. The integration with Acronis Cyber Cloud enables IT service providers to easily back up and protect against ransomware endpoints directly from the ConnectWise Automate interface without going to the Acronis Cyber Cloud web interface.

Once the plugin is installed and configured, the data protection properties are automatically available for all servers and workstations in any location.

The service providers can:

- Remotely install, update, and uninstall the cyber protection agent on protected machines
- Easily apply and revoke the pre-defined protection plan at the client, location, or machine level
- Monitor protection status for errors and warnings
- Leverage the native ConnectWise Automate reporting, ticketing, and alerting functionality for handling backup events
- Provision new Acronis Cyber Cloud customers

The service providers can go to the Acronis Cyber Cloud web interface if they want to configure unique backup settings. The backup plans created in the Acronis Cyber Cloud web interface are then synchronized and available for further use in the ConnectWise Automate interface.

Recovery is performed exclusively via the Acronis Cyber Cloud web interface.

Terminology conventions

We will refer to the Acronis Cyber Cloud plugin as "Acronis plugin" throughout this document and the Acronis Cyber Cloud web interface as "backup console" throughout this document.

Prerequisites

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

System requirements

Acronis plugin

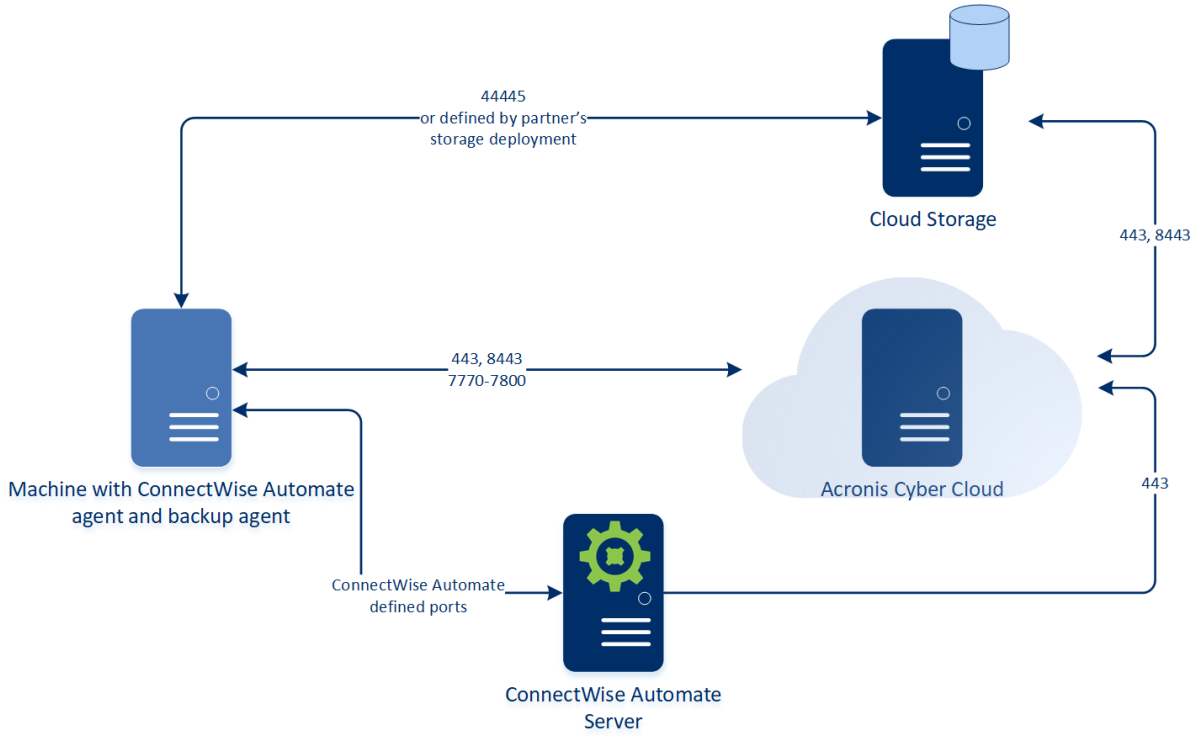
The Acronis plugin can be installed on a ConnectWise Automate server running ConnectWise Automate version 12 and .NET Framework 4.5.2 or later.

Acronis agents

Agents are applications that perform data backup, recovery, and other operations on the machines managed by Acronis. An agent can be installed in any Windows, Linux, or Mac operating system supported by ConnectWise Automate. For the exact list of supported operating systems, refer to the Acronis backup service documentation.

Network requirements

The diagram below illustrates the network connections that are necessary for the Acronis plugin to work.

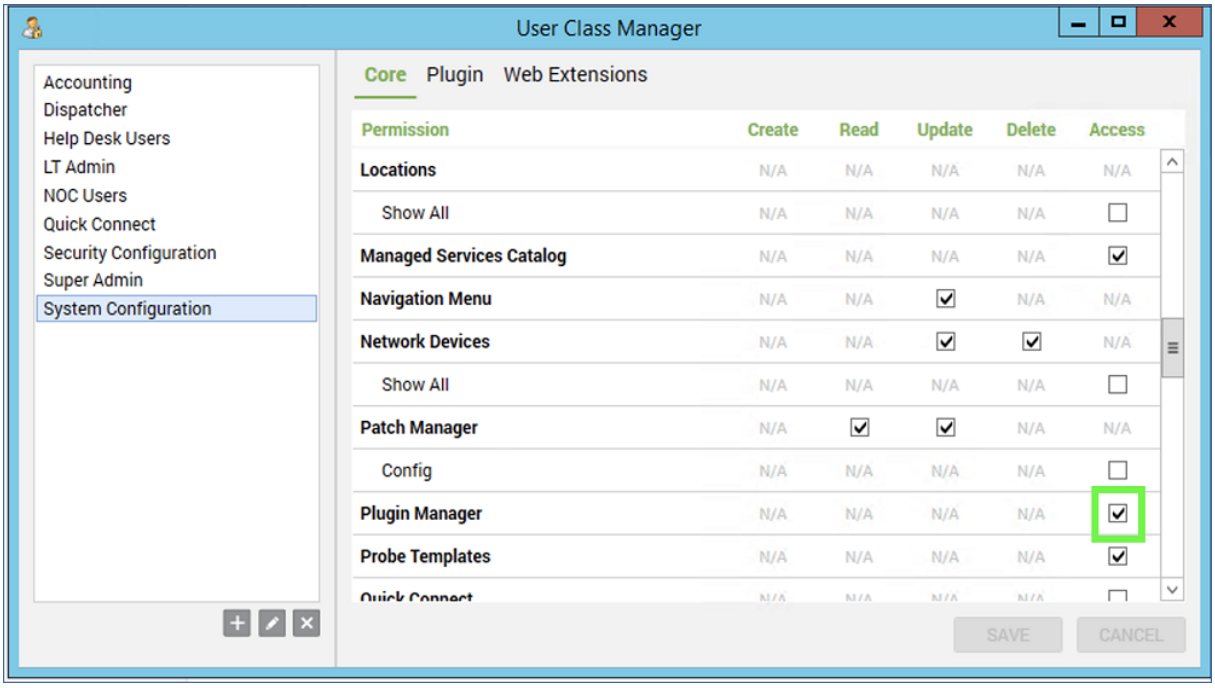


User rights

There are two levels of access rights in ConnectWise Automate, to differentiate between administrator and general technician users.

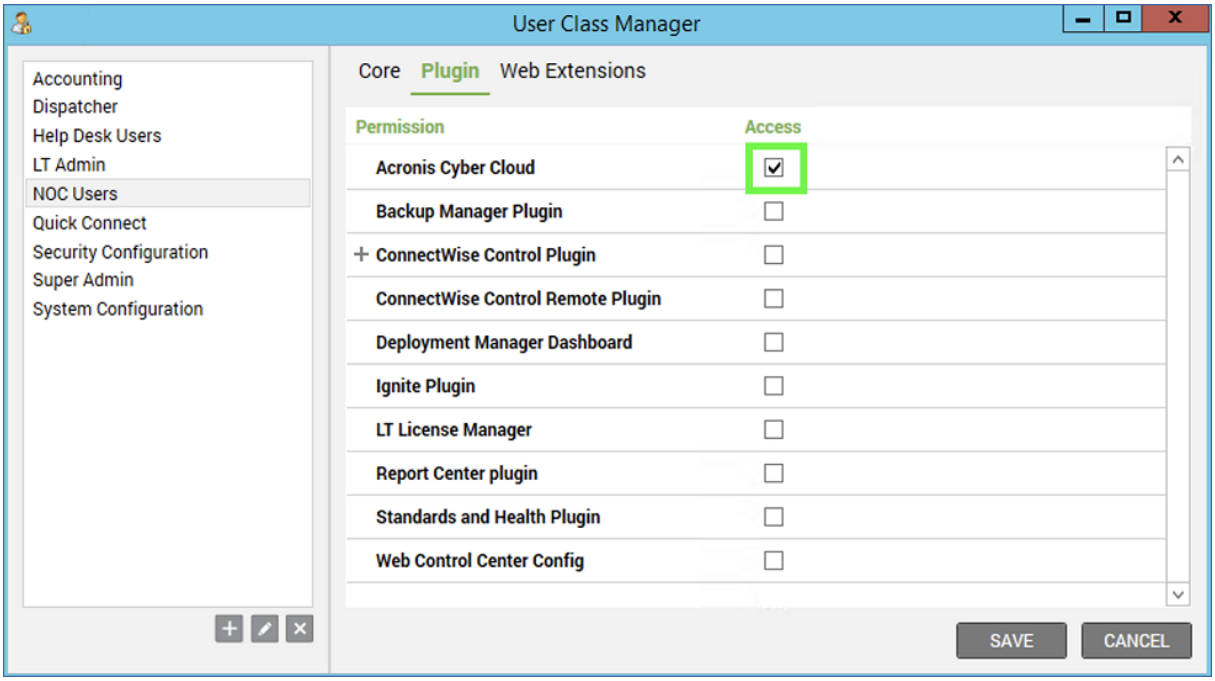
Administrator access

In order to have full access to the plugin, including installation, the administrator's ConnectWise Automate user class must have the **Core** > **Plugin Manager** permission set to **Access**.



Technician access

For technicians, who should not have access to the Plugin Manager, but do need the full functionality of the Acronis integration, make sure that their user class has the **Plugin** > **Acronis Cyber Cloud** permission set to **Access**.



Apart from the administrator, it is not necessary for any other user, to have Plugin Manager access in order to use the integration.

Installation or update of Acronis plugin

1. Download and install/update the Acronis plugin from the ConnectWise Automate **Solution Center**.

   For more information about how to use the **Solution Center**, refer to https://docs.connectwise.com/ConnectWise_Automate/ConnectWise_Automate_Documentation/070/270
2. Restart any open ConnectWise Automate Control Center instances.

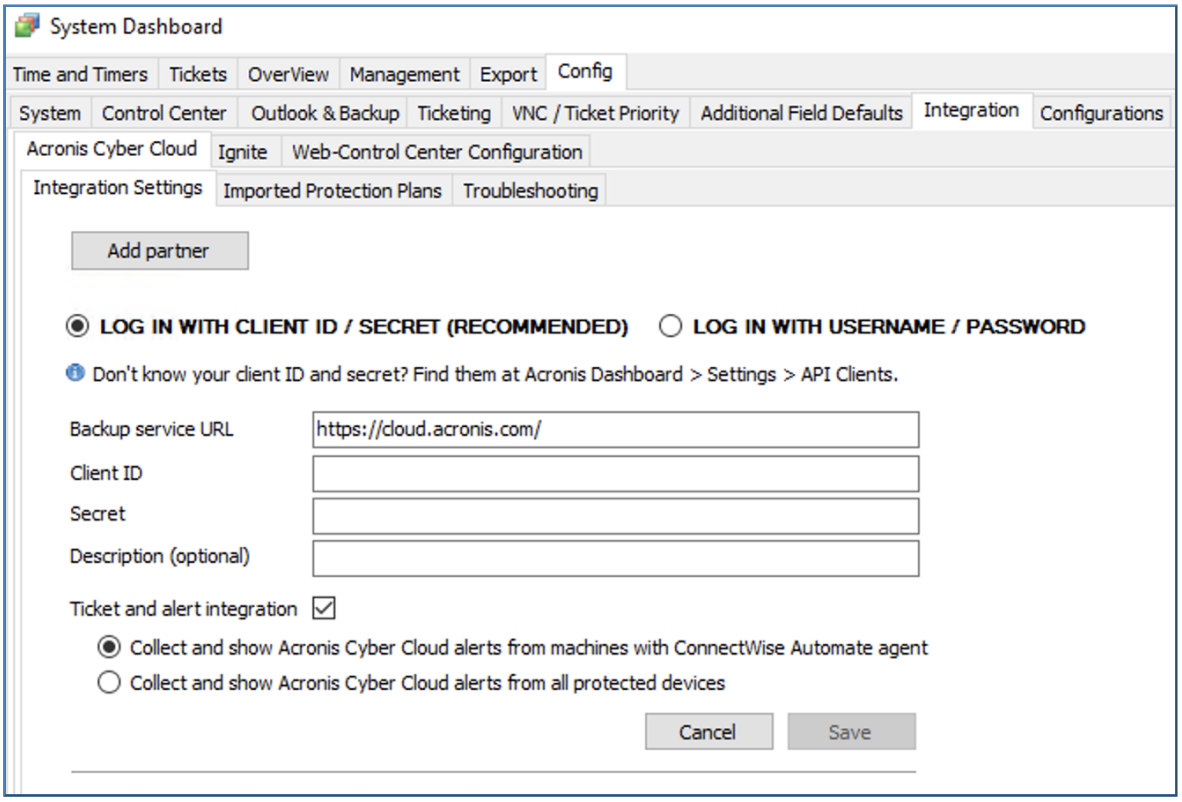
Configuring the integration

To configure integration with Acronis Cyber Cloud

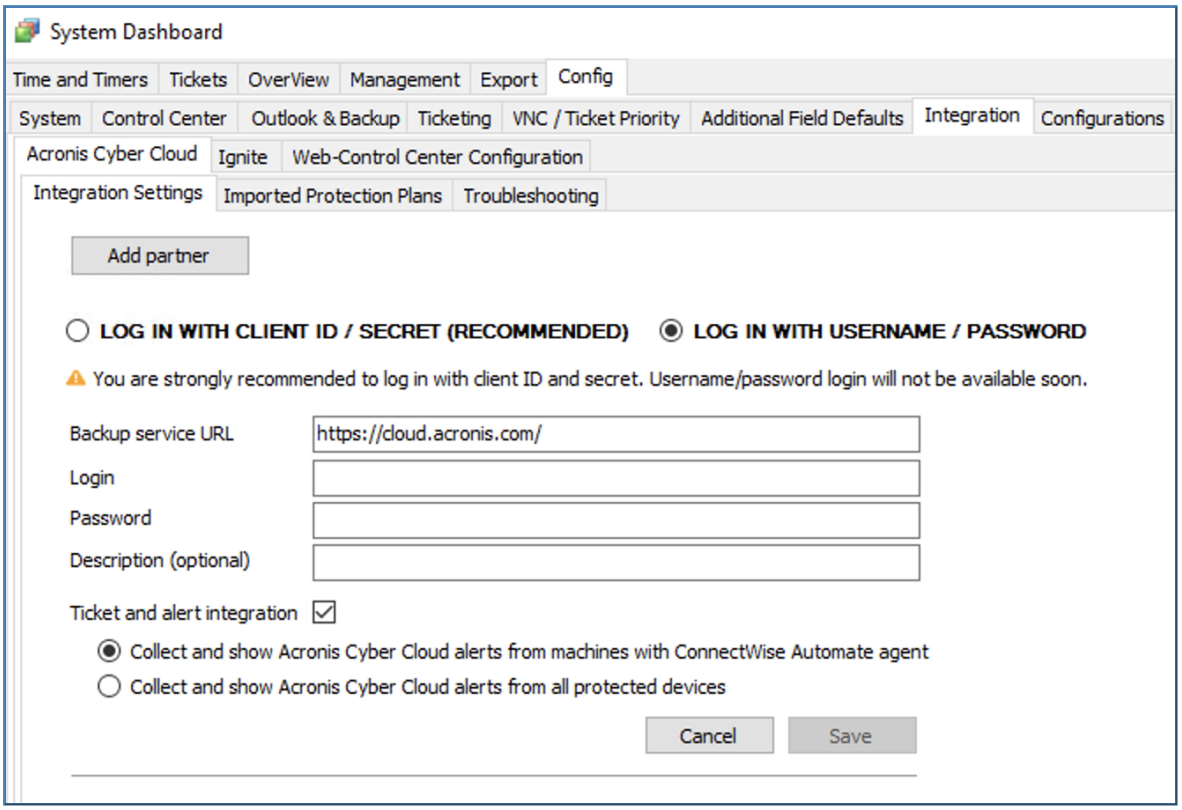
1. Open the Acronis Control panel and go to **Settings** > **API Clients**.
2. Click on **Create New API Client** and give your new client a name. It will be used for reference purposes only (so that you know later what the API keys are used for).
3. When done, click **Next**.
4. In the window that opens, copy the following information: **Client ID** and **Secret**.

   Note
   This is the only time the Secret key will be directly exposed to you. Make sure to copy and store it before closing this window.

5. In the ConnectWise Automate interface, go to **System** > **Configuration** > **Dashboard** > **Config** > **Integration** > **Acronis Cyber Cloud** > **Integration Settings**.
6. Enter the Acronis Cyber Cloud URL. You can copy this link from the account activation email.
7. Enter the **Client ID** and **Secret** from step 4.



Alternatively, if you do not have a **Client ID** and **Secret**, click on **Log in with username and password**, then enter the login and password you set when activating your account in Acronis Cyber Cloud.



Note

If you have two-factor authentication enabled for your Acronis account, you have to use Client ID and Secret.

8. Optionally, set up ticket and alert integration:
   - Clear the **Ticket and alert integration** check box, if you do not want ConnectWise Automate to create tickets and raise alerts, related to backup issues. For details, see "Monitoring backup status" (p. 25).
   - Select the **Ticket and alert integration** check box, if you want to collect and show Cyber Cloud alerts:
     - To monitor devices unavailable in ConnectWise Automate interface (Office 365, G-Suite, websites, etc.), select the **Collect** option and show Acronis Cyber Cloud alerts from all protected devices.
9. Optionally, add integration with one more data center, by clicking **Add partner** and specifying the integration parameters.
10. When ready, click **Save**.

To configure integration with several data centers, use the **Add Partner** button at the top of the window.

Managing clients

Cyber Protect features are available as part of either Standard or Advanced Protection packs. Advanced Protection extends the Standard version with further protection capabilities that can be added only on top of it and are charged additionally. Advanced Protection can support multiple workloads but only ones that already have Standard Protection assigned.

To configure device protection, you must link clients in ConnectWise Automate with customers in Acronis Cyber Cloud. You have two options:

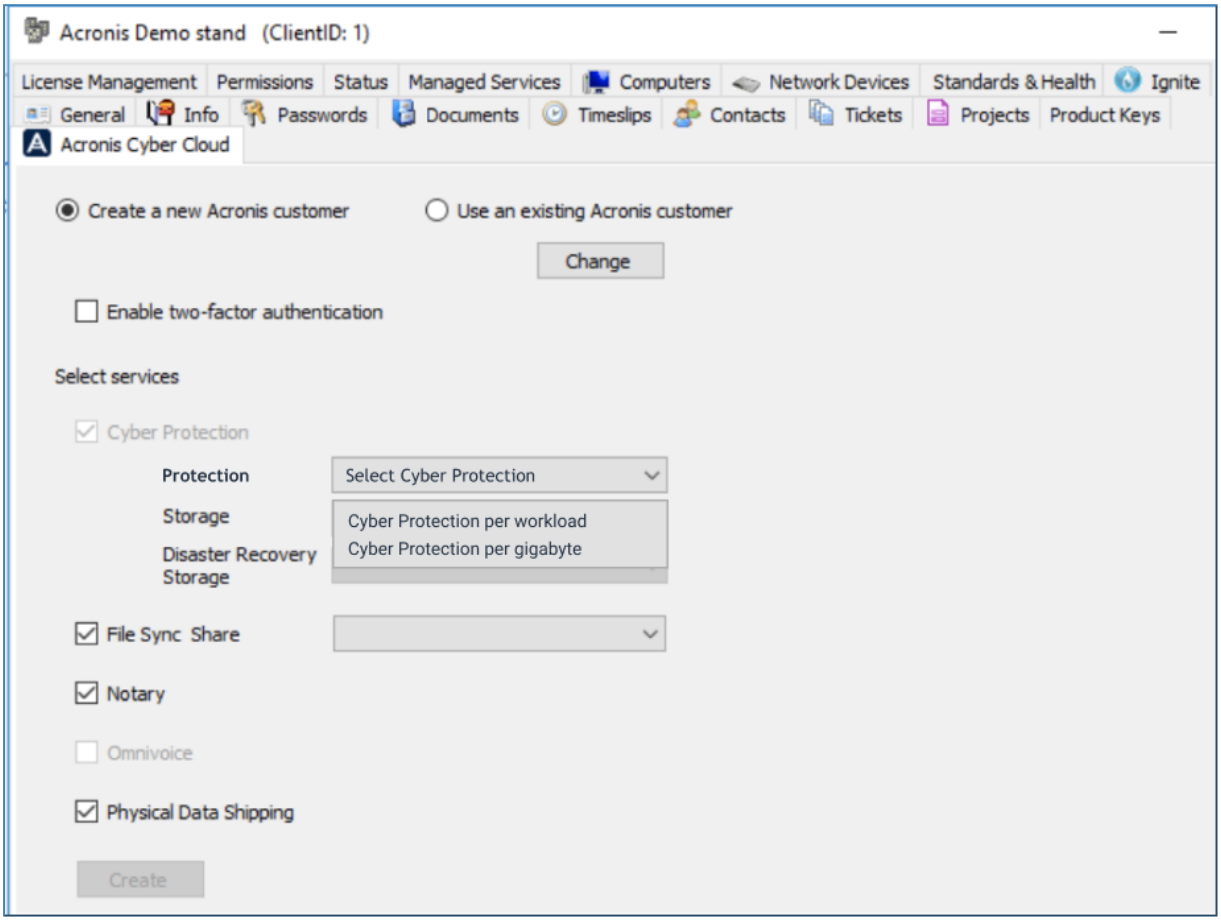
- If you do not have any customer tenant in Acronis Cyber Cloud to link with, then you can define the parameters of the customer tenant to be created on the Acronis Cyber Cloud side. The login and password of the created tenant will be used automatically when you click **Go to backup console** in the ConnectWise Automate interface.
- If you have a customer tenant in Acronis Cyber Cloud to link with, then select it and specify the backup user.

To link a ConnectWise Automate client with an Acronis Cyber Cloud customer

1. In the list of clients, double-click the client name, and then select the **Acronis Cyber Cloud** tab.
2. Specify whether to create a new Acronis customer or use a customer that already exists in Acronis Cyber Cloud.
3. [For a new customer] Enter the required parameters and click **Create**.
   - **Partner** – the partner name under which the customer will be created. The default setting is commonly used. You have a choice only if there are partners under your partner in Acronis Cyber Cloud.
   - **Customer** – the customer name. By default, this is the client name in ConnectWise Automate.
   - **Login** – the user name of the customer account. By default, it is combined from your account user name in ConnectWise Automate and the client name.
   - **Email** – the email address to which the notifications will be sent. By default, this is the email address of your account in ConnectWise Automate.
   - **Password** – the password of the customer account.
   - **Two-factor authentication** - enable two-factor authentication for the customer tenant.

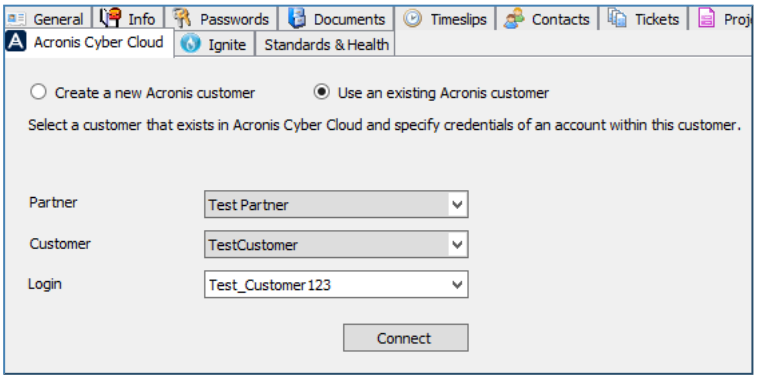
   Select which services will be provided to a customer. For the Backup, Disaster Recovery, and File Sync & Share services, define the storage.
   - **Protection** - select one of the following billing modes:
     - **Standard protection per workload**
     - **Standard protection per GB**

- **Storage** – the cloud storage for the customer. You have a choice only if you registered your own storage or have multiple storages inherited from parent groups. Please be aware that this setting cannot be changed after the customer is created.



You can optionally and separately enable **File Sync & Share**, **Physical Data Shipping** and **Notary** by marking those check boxes.

[For an existing customer] Select the **Partner** (if available), **Customer** or unit, and **Login** parameters.



If, for example, each client location should have different protection plan, individual locations can be linked to customers in Acronis Cyber Cloud in the following way:

1. In the list of clients and locations, double-click the location name, then select the **Acronis Cyber Cloud** tab.
2. Follow steps 2 and 3 above.

Note

Linking at client and location level is mutually exclusive. If linking to an Acronis customer tenant is set up for a single client location in ConnectWise Automate, it is not possible to link also at client level. You can still link all remaining locations individually or should remove the existing links at location level before adding the link at client level.

Installation of cyber protection agents

A cyber protection agent must be installed on every machine that you want to back up. There are two installation methods:

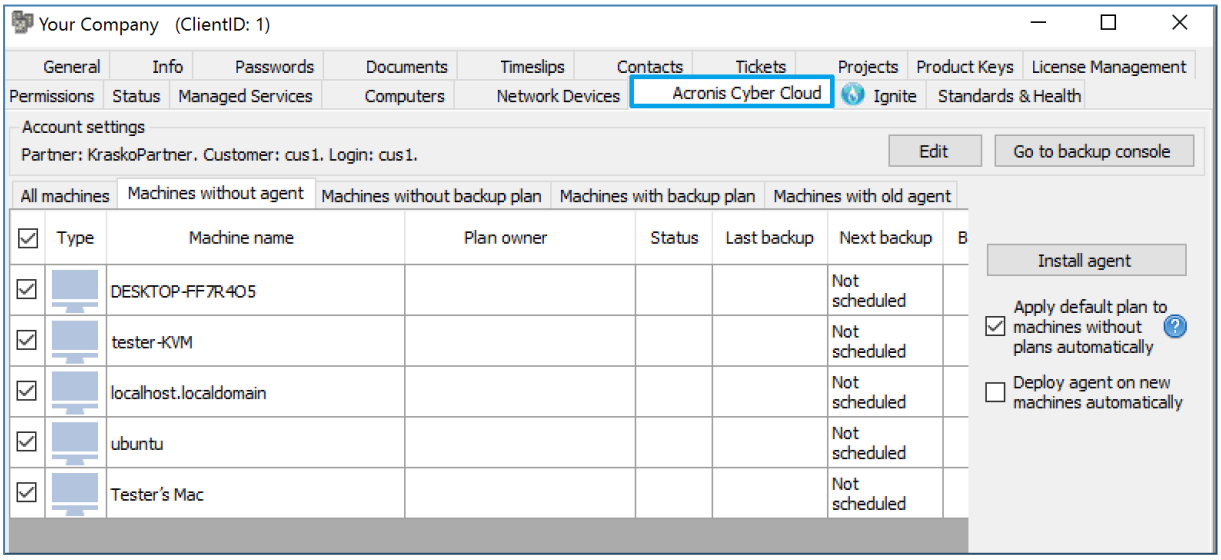
- Manual
  - Installing the agent at a client or location level
  - Installing the agent at a machine level
- Automatic
  - Installing the agent at a client or location level
  - Installing the agent by using the scripts provided with the plugin across multiple clients

Manual installation of a cyber protection agent

This method allows you to install agents on any machines within a client or location.

To install cyber protection agents at a client or location level

1. Double-click the client or location.
2. Select the **Acronis Cyber Cloud** tab.
3. Select the machines that you want to back up. To identify the machines that do not have cyber protection agents, use the **Machines without agent** tab.
4. [Optional] Select the **Apply default plan to machines without plans automatically** check box. The details of this setting are described in the next section.
5. Click **Install agent**.



To install a cyber protection agent at a machine level

1. Double-click the machine.
2. Click **Acronis Cyber Cloud**.
3. Click **Install agent**.

Automatic installation of a cyber protection agent

To install cyber protection agents at a client or location level

1. Perform the steps 1-4 as described in the section **Manual installation of a cyber protection agent**.
2. Select the **Deploy agent on new machines automatically** check box. If you do this, a cyber protection agent will be silently installed on any machine that will be added to the client or location at a later time.

Installation by using scripts

In addition to a client or a machine, an installation script can be applied to a group. You can group all machines that you need to back up, including those from multiple clients, and install agents on these machines at once, or schedule the installation procedure on a regular basis for new devices. There is a predefined search for this purpose at **Searches** > **Backup Software** > **Backup - Acronis Cyber Cloud (Machines Without Agent)**. This search works for Windows machines only.

Also, this installation method enables you to install the backup monitor. The backup monitor is a small utility for an end-user self-service that appears in the tray area and enables users to see the backup progress; start and stop backups; or prevent backups from running. There are two installation scripts for installing agents with or without the backup monitor.

To install cyber protection agents by using an installation script

1. Right-click the group that you want to apply the script to.
2. In the shortcut menu, select **Scripts** > **Computer Scripts**, and then choose one of the following scripts:
   - Acronis Cyber Cloud agent Install/Upgrade
   - Acronis Cyber Cloud agent Install/Upgrade with backup monitor
3. [Optional] Specify the schedule. Usually, you need to perform installation only once. You may want to set up a schedule if new machines will be added to the group at a later time.
4. Click **OK** to confirm the settings.

To install a cyber protection agent for Active Directory, SQL, Exchange, Office 365, or VMWare, double-click the client or location, select the **Acronis Cyber Cloud** tab, and then click **Go to backup console**.

Deploying agent to Domain Controllers

The installation of Acronis agent on Windows Domain Controller Server requires additional credentials. Installing the agent on non-DC workloads with these credentials will cause failure. To avoid this, group the workloads in two separate locations: one for domain controller servers and another - for the rest (non-domain controller) computers.

Apply the following steps on the location with a domain controller server:

Note
The process is basically the same as for standard agent deployment with the only difference of 3 additional pre-installation steps.

1. Create a special account on the Windows Domain Controller machine

For more information, see: https://www.acronis.com/en-us/support/documentation/BackupService/index.html#47301.html

The Acronis agent runs as a Managed Machine Service (MMS) on Windows Domain Controller machines. This means that in order for the agent to work correctly, the account under which it will run, must have specific rights. The MMS user should be assigned the following privileges:

1. Included in the Backup Operators and Administrators groups: the user must be included in the Domain Admins group on a domain controller.
2. Granted Full Control permission on the %PROGRAMDATA%\Acronis folder (in Windows XP and Server 2003: %ALLUSERSPROFILE%\Application Data\Acronis folder) as well as on its subfolders.
3. Granted Full Control permission on certain registry keys, in the below key: HKEY_LOCAL_MACHINE\SOFTWARE\Acronis
4. Assigned the following user rights:
   - Log on as a service
   - Adjust memory quotas for a process
   - Replace a process level token
   - Modify firmware environment values

How to assign user rights

Follow the instructions below to assign the user rights. This particular example uses **Log on as service**, however, the steps are the same for all the rest user rights:

1. Log on to the computer with an administrative privileges account.
2. Go to **Control panel** > **Administrative Tools** or click **Win+R**, type **control admintools** and click **Enter**. Then open **Local Security Policy**.
3. Expand **Local Policies** to click on **User Rights Assignment**.
4. In the right pane, right-click **Log on as a service** and select **Properties**.
5. To add a new user, click on the **Add User or Group...** button.
6. In the **Select Users, Computers, Service Accounts or Groups** window, find the user you want to enter and click **OK**.
7. To save the changes, click **OK** in the **Log on as a service** properties.

Important
Make sure that the user you have added to the **Log on as a service** user right is not listed in the **Deny log on as a service** policy in **Local Security Policy**.

Note
It is not recommended to change the logon accounts manually after the installation is completed.

2. Log into the Domain Controller Server at least once with the new account

This will create the user profile directory. The agent installation requires the profile folder to exist in order to put some files there.

3. Add the Domain Controller username and password to Automate

Automate documentation available on how to do this: https://docs.connectwise.com/ConnectWise_Automate_Documentation/070/040/010/030

4. Set the Deployment and Default Settings in Automate

Refer to the Automate documentation: https://docs.connectwise.com/ConnectWise_Automate_Documentation/070/040/020/030

Updating cyber protection agents

Updating is performed similarly to installation, either from the ConnectWise Automate interface or by using the installation script. To identify the agents that require an update, use the **Machines with old agent** tab at the client or location level.

Uninstalling cyber protection agents

Uninstallation is performed similarly to installation, either from the ConnectWise Automate interface or by using the uninstallation script.

Protection of machines

Acronis plugin provides with backup and anti-ransomware protection of your devices.

- A backup plan is a set of rules that specify how the given data will be protected on a given machine. A backup plan can be applied to one or multiple machines.
- An Active Protection plan is a set of rules that specify how the cyber protection agent will monitor for suspicious activities on the device and act when the threat is detected. An Active Protection plan can be applied to one or multiple machines.

Before a backup plan can be applied, it has to be created in Acronis Cyber Cloud and then imported to ConnectWise Automate. You can also use the default backup plan.

Importing and applying backup plans

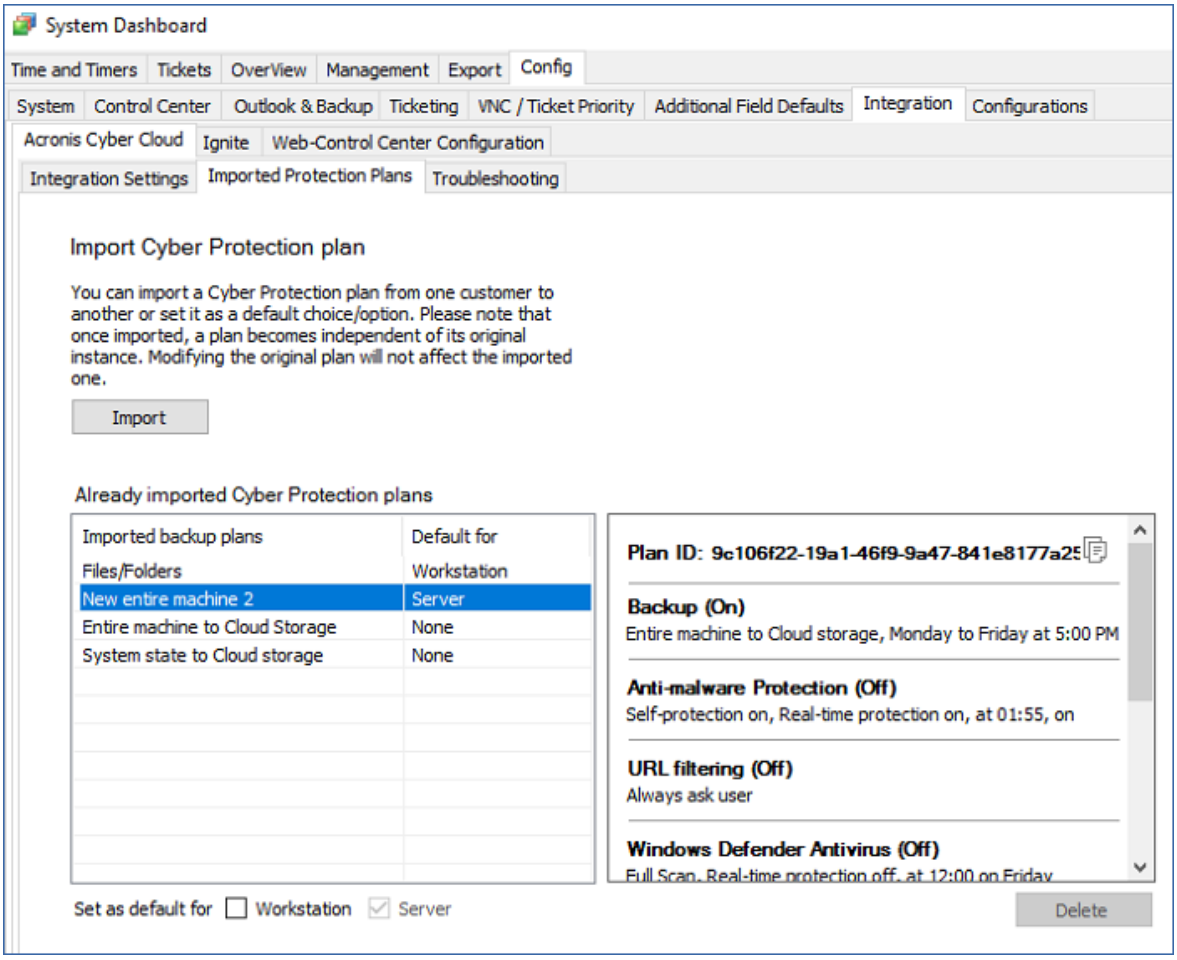
Importing backup plans

A custom backup plan appears in the ConnectWise Automate interface only for the client for whom the plan is created. If you want a custom backup plan to be available to all clients, import this plan to ConnectWise Automate. An imported plan becomes available for all clients at the client, location, and machine levels.

Important
Before importing a backup plan, ensure that the selection method in the **Items to back up** section of this plan is set to **Using policy rules**.

To import a backup plan to ConnectWise Automate

1. Select **System** > **Configuration** > **Dashboard** > **Config** > **Integration** > **Acronis Cyber Cloud** > **Imported Backup Plans**.
2. Click **Import**.



3. Select the customer. The software displays a list of backup plans available for this customer.
4. Select a plan. The software displays its details.
5. If according to the backup plan the backups should be encrypted, create the encryption password. Note that the same password will be used for all clients.

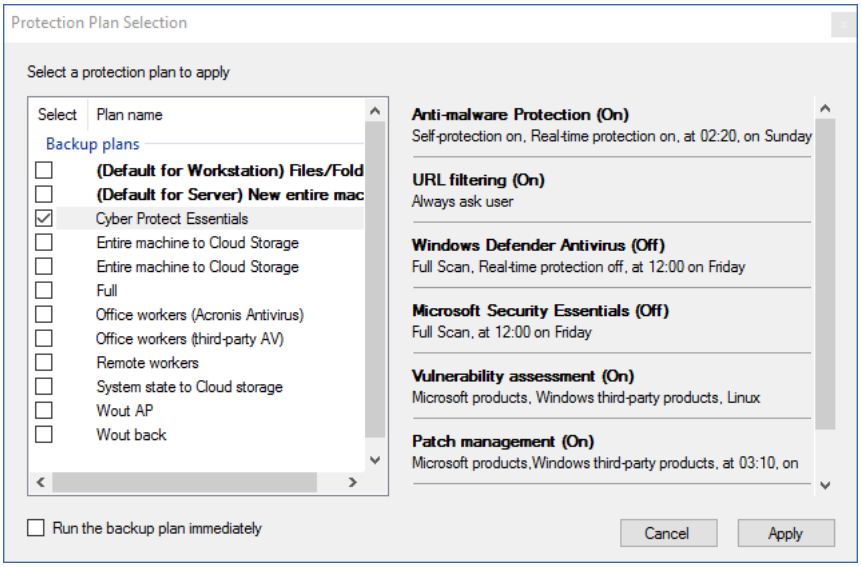
   Important
   There is no way to recover encrypted backups if you lose or forget the password.

6. Click **Import**. The plan appears in the **Imported backup plans** list.

You can click **Set as default for Workstations** or **Set as default for Servers** to make an imported plan the default for workstations or servers, respectively.

Applying backup plans manually

1. Double-click the client or location.
2. Click **Acronis Cyber Cloud**.
3. Select the machines that you want to back up. To identify the machines that do not have backup plans, use the **Machines without backup plan** tab.
4. Click **Apply plan**.
5. Select the backup plan. If no custom backup plans were created, only the default backup plan is available.
6. [Optional] Select the **Run the backup plan immediately** check box. If you do this, the backups will be started on all of the selected machines immediately.
7. Click **Apply**.



Applying backup plans automatically

Applying backup plans by using a script

If you want to apply a custom backup plan to all machines within one location, you can do this by using a pre-defined script, specifying the **Plan ID** in the script parameters.

1. Select **System** > **Configuration** > **Dashboard** > **Config** > **Integration** > **Acronis Cyber Cloud** > **Imported Backup Plans**.
2. In the **Imported backup plans** column, select the backup plan to be applied.
3. Click the **Copy to clipboard** icon next to the **Plan Id** in **Plan details** box. The ID of the plan is copied.
4. Close the **System Dashboard** window.
5. Right-click the client or location where you want to apply the backup plan, select **Scripts** > **Computer Scripts**> **Acronis Cyber Cloud** **Apply Backup Plan**. The **Run Script** window opens.

6. [Optional] Specify the schedule. Usually, you need to perform installation only once. You may want to set up a schedule if new machines will be added to the group at a later time.
7. Paste the copied plan ID to **backupPlanId** field.
8. Click **OK**.
9. Wait for the script to apply the backup plan.

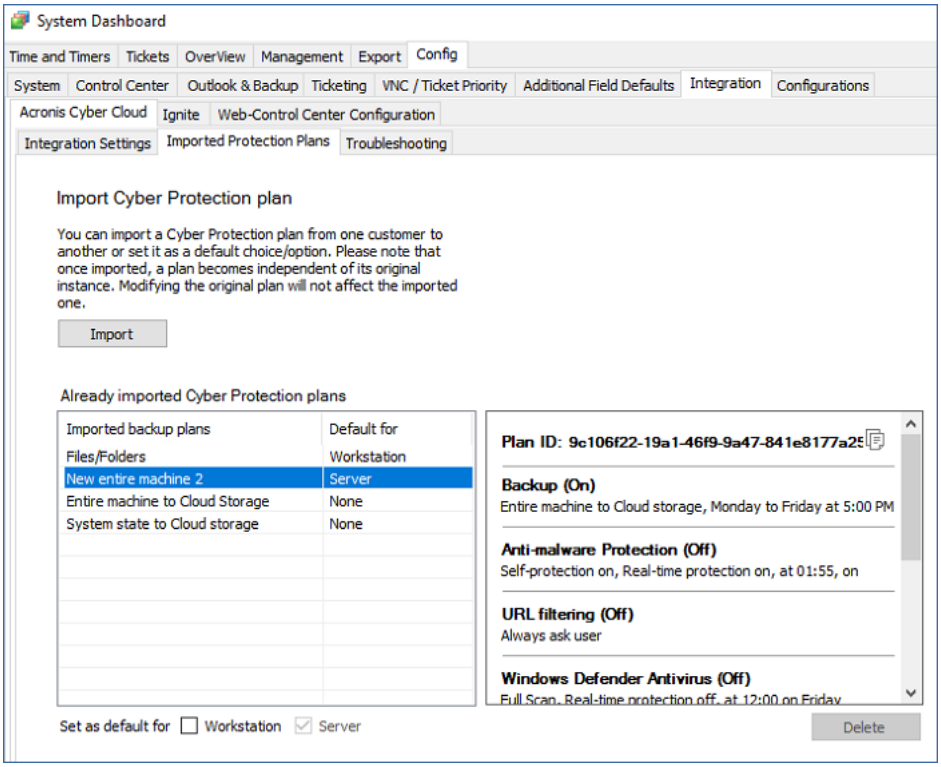
Default backup plan

The default backup plan is **Entire machine to Cloud Storage**. According to this plan, a machine is backed up to the cloud storage daily from Monday to Friday at 11:00 PM.

You can recover any files from this backup, as well as individual volumes or the entire machine.

The retention rules are applied to each backup set separately:

- A monthly backup is the first backup created after a month starts. Monthly backups are kept for six months.
- A weekly backup is the backup created on Monday. Weekly backups are kept for four weeks.
- All other backups are considered daily. Daily backups are kept for seven days.



After you import a backup plan following the steps described above, you can click **Set as default for Workstations** or **Set as default for Servers** to make an imported plan the default for workstations or servers, respectively. The parameter in ConnectWise Automate indicating the type of the machine (Server or Workstation) is located on the Client and Location tabs.

If you want the default backup plan to be applied automatically, select the **Apply default plan to machines without plans automatically** check box at the client or location level. The Acronis

plugin will scan the machine statuses every six minutes, and apply the default backup plan to machines that have an agent but do not have a backup plan.

Custom backup plans

If you need more flexibility in terms of backed-up items, schedule, or location, click **Go to backup console** and create a backup plan by using the numerous options offered by Acronis Cyber Cloud. The backup plans created in the Acronis Cyber Cloud web interface are then synchronized and available for further use in the ConnectWise Automate interface.

For the information about the backup capabilities, refer to the Acronis backup service documentation.

Operations with backup plans

To start a backup outside of its schedule

1. Double-click the machine that you want to back up.
2. Click **Acronis Cyber Cloud** .
3. Select the backup plan that you want to run.
4. Click **Start backups**.

After refreshing the status, you will see the backup progress in the **Status** column.

To stop a running backup

1. Double-click the machine.
2. Click **Acronis Cyber Cloud** .
3. Select the backup plan that has the **Backing up** status.
4. Click **Stop backups**.

This will stop the currently running backup and remove the incomplete backup file from the storage. The next backup will run as scheduled.

Unlike starting a backup, it is possible to stop a backup on multiple machines at once. Select the machines at a client or location level and click **Stop backups**.

To revoke a backup plan

1. Double-click the machine.
2. Click **Acronis Cyber Cloud** .
3. Select the backup plan that you want to revoke.
4. Click **Revoke plan**.

The backup created by this plan will be kept. Any other plans applied to this machine will run as scheduled.

To revoke a backup plan from multiple machines

1. Double-click the client or location.
2. Click **Acronis Cyber Cloud** .
3. Select the machines that you want to revoke the backup plan from.
4. Click **Revoke plan**.
5. Select the backup plan that you want to revoke.
6. Click **Revoke**.

Monitoring backup status

Monitoring at a client, location, or machine level

For each machine that has a backup plan, you can see the following parameters:

- The status, which is derived from the last backup result (**OK**, **Error**, **Warning**, **Not protected**)
- The last backup date and time
- The next backup date and time

Monitoring at the system level

The Acronis plugin installs the monitors that are listed below. These monitors enable ConnectWise Automate to create tickets and raise alerts related to backup issues. To access the monitors in the ConnectWise Automate console, go to **Automation** > **Monitors**, and then select the **Internal Monitors** tab.

Monitors for machines with ConnectWise Automate agent:

- Acronis Cyber Cloud - Clients - Critical Issues
- Acronis Cyber Cloud - Clients - Non Critical Issues
- Acronis Cyber Cloud - Clients - Warnings
- Acronis Cyber Cloud - Computers - Critical Issues
- Acronis Cyber Cloud - Computers - Non Critical Issues
- Acronis Cyber Cloud - Computers - Warnings
- Acronis Cyber Cloud - Computers - Missed Backups
- Acronis Cyber Cloud - Computers - Not protected

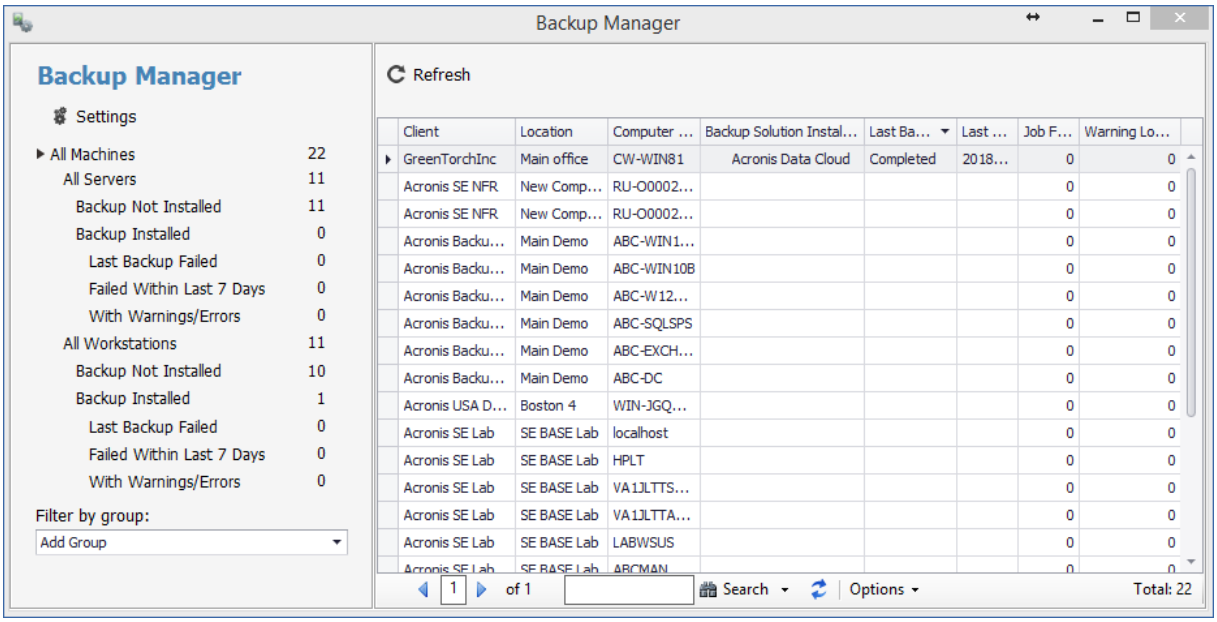
Monitors for devices without ConnectWise Automate agent:

- Acronis Cyber Cloud - Other - Critical Issues
- Acronis Cyber Cloud - Other - Non Critical Issues
- Acronis Cyber Cloud - Other - Warnings
- Acronis Cyber Cloud - Other - Missed Backups
- Acronis Cyber Cloud - Other - Not protected

To disable creating tickets and alerts related to Acronis Cyber Cloud, clear the **Ticket and alert integration** check box at **Dashboard** > **Config** > **Integration** > **Acronis Cyber Cloud** > **Integration Settings**. The monitors will continue working, but the table they check will no longer be updated. You can enable the ticket and alert integration again at any time.

Monitoring in Backup Manager

You can use the native ConnectWise Automate Backup Manager to monitor the backup status.

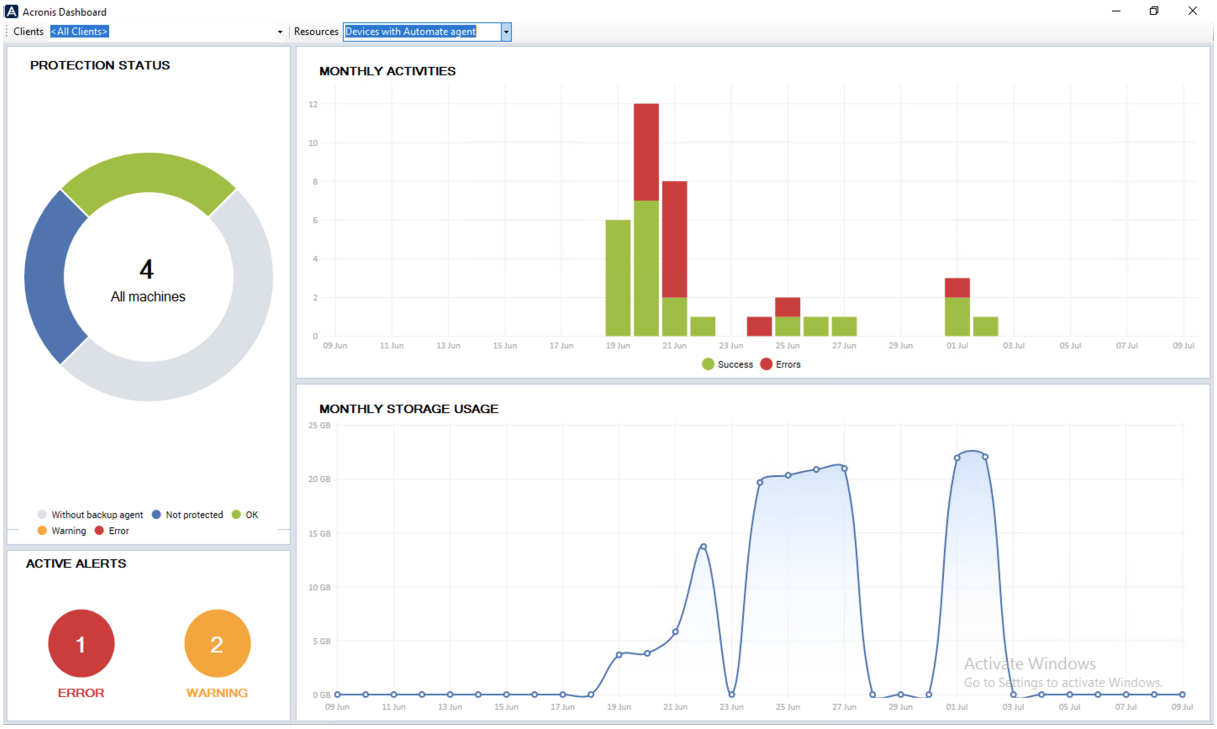


Monitoring with Acronis Dashboard

The Acronis plugin installs the dashboard that provides the following information:

- **Protection status** - shows the numbers of machines with the **OK**, **Error**, and **Warning** backup statuses; the number of machines without a backup plan; and the number of machines without a cyber protection agent.
- **Active alerts** - shows the numbers of Acronis Cyber Cloud alerts with the severity of **Error** or **Warning**.
- **Monthly activities** - shows the monthly statistics about successful and failed backups.
- **Monthly storage usage** - shows the monthly usage of the cloud storage.

To access the dashboard, go to **Tools** > **Acronis Dashboard** on the toolbar.



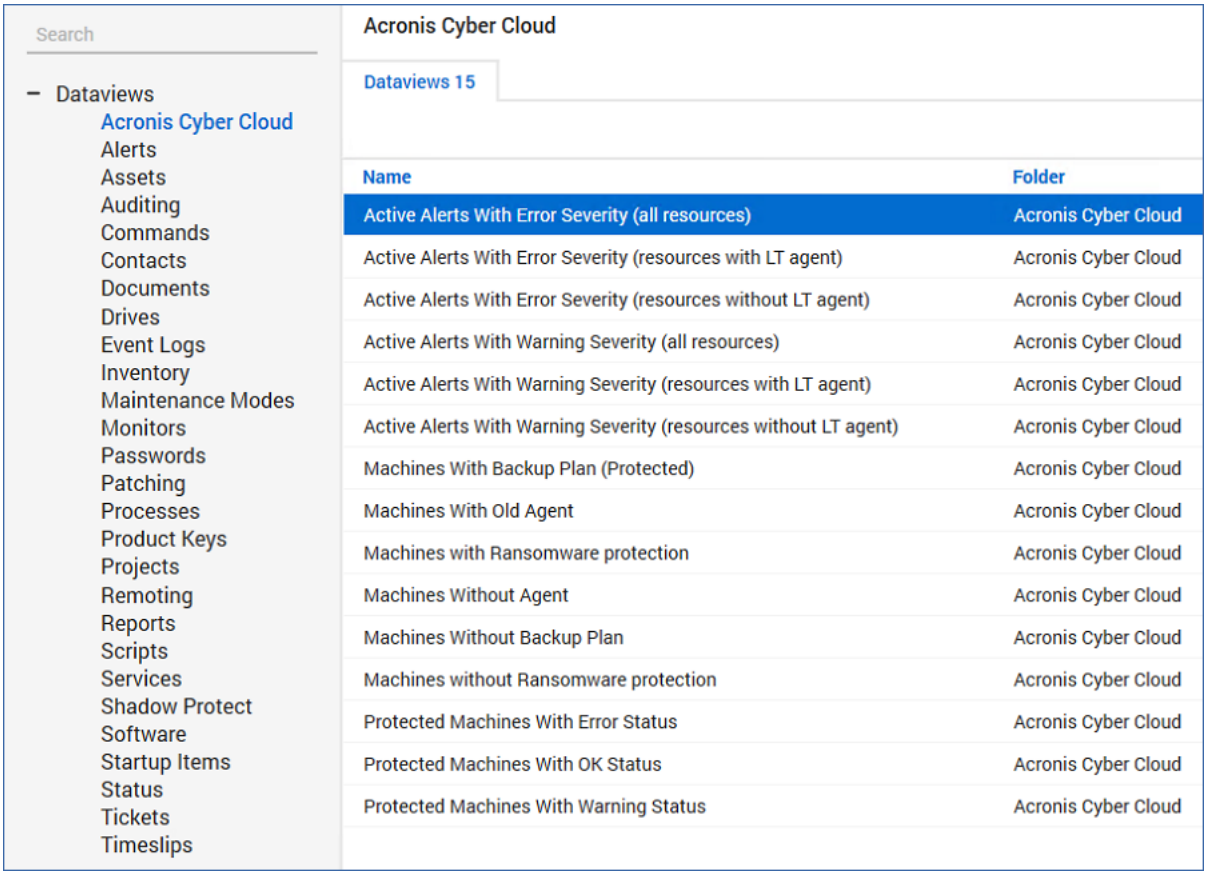
In order to generate the alerts for the missing backup activities, enable **Alert** option for the backup plan in Acronis Cyber Cloud, as described here:

https://dl.managed-protection.com/u/baas/help/20.08/user/index.html#46968.html

In this way, the alert with warning severity will be generated in Acronis Cyber Cloud and will be forwarded into Acronis **Monitors** in ConnectWise Automate. If ticket creation is enabled in ConnectWise Automate, then the new ticket will be created for the missing backup activities.

Monitoring with Acronis Dataviews

The Acronis plugin installs the dataviews that sort the Acronis Cyber Cloud statistics by the following criteria:



- **Active Alerts With Error Severity (all resources)**
- **Active Alerts With Error Severity (resources with LT agent)**
- **Active Alerts With Error Severity (resources without LT agent)**
- **Active Alerts With Warning Severity (all resources)**
- **Active Alerts With Warning Severity (all resources with LT agent)**
- **Active Alerts With Warning Severity (all resources without LT agent)**
- **Machines With Backup Plan (Protected)**
- **Machines With Old Agent**
- **Machines with Ransomware protection**
- **Machines Without Agent**
- **Machines Without Backup Plan**
- **Machines without Ransomware protection**
- **Protected Machines With Error Status**
- **Protected Machines With OK Status**
- **Protected Machines With Warning Status**

To access a dataview, click the corresponding item on the **Acronis Dashboard** or at **Automation** > **Dataviews** > **Acronis Cyber Cloud** .

Reporting

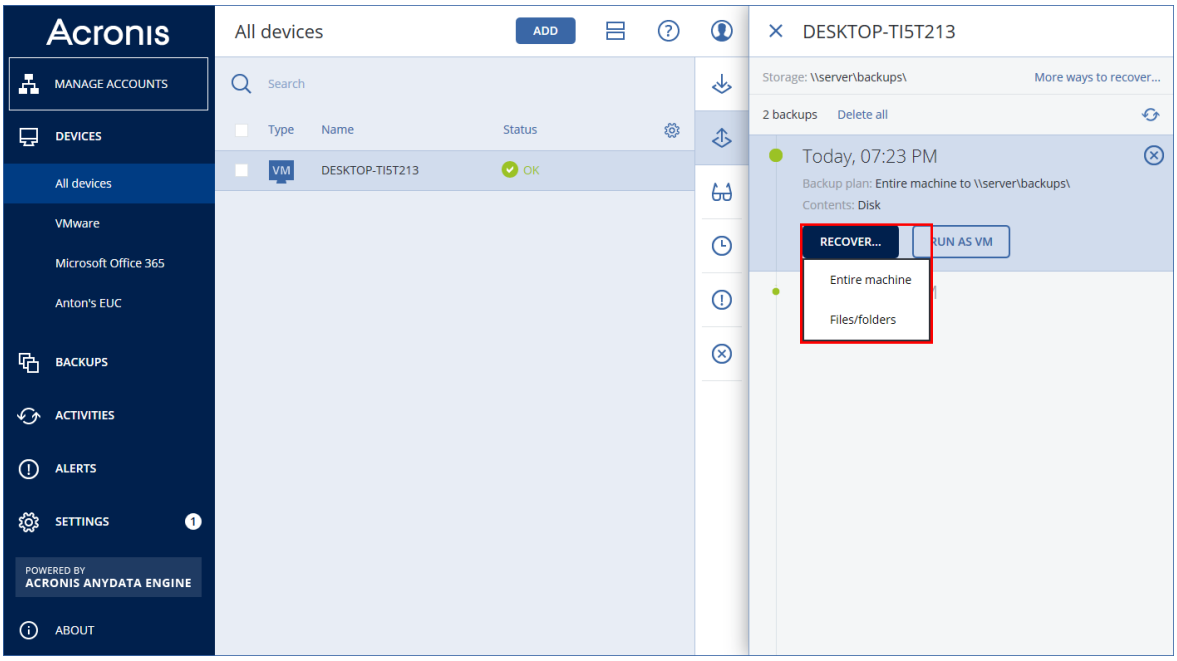
Information about backups performed by Acronis Cyber Cloud is present in the following ConnectWise Automate reports:

- **Backup Health**
- **Backup History**

Recovery

To recover data to a machine

1. Double-click the machine.
2. Click **Acronis Cyber Cloud** .
3. Click **Recover**. This will take you to the Acronis Cyber Cloud interface and the recovery points for this machine will be displayed.



4. Follow the instructions described in Acronis Cyber Cloud Help.
   - File recovery
   - Machine recovery

For full information about the recovery capabilities, refer to Acronis backup service documentation.

Troubleshooting

You can collect data for the Support team. It will contain one .zip file with information from plugin tables, settings, and logs:

To collect troubleshooting data for Acronis plugin for ConnectWise Automate

1. Select **System** > **Configuration** > **Dashboard** > **Config** > **Integration** > **Acronis Cyber Cloud** > **Troubleshooting**.
2. Select **Log level**.

   Important
   You must wait for a few minutes for the new log level to be applied.

3. Click **Collect data**.

Index

U

