acronis.com

Acronis Cyber Cloud

Integration with ConnectWise ScreenConnect (Control)

Integration Guide

REVISION: 5/26/2023

Table of contents

Introduction

This document describes how to configure the integration of Acronis Cyber Cloud with ConnectWise ScreenConnect (former ConnectWise Control). ConnectWise ScreenConnect is the solution that allows you to remotely access and control devices, and helps your customers to resolve IT issues.

By integrating Acronis Cyber Cloud with ConnectWise ScreenConnect, you will be able to provide the Acronis Cyber Protection service to existing customers and create new Cyber Cloud customers on the fly.

About ConnectWise ScreenConnect

The typical audience of ConnectWise ScreenConnect is Managed Service Providers (MSPs) that provide IT services to small and medium businesses. An MSP manages all their customers and corresponding machines within one ConnectWise ScreenConnect console. Some large MSPs use a separate ConnectWise ScreenConnect console per customer. When the ConnectWise agent is installed, machines are added to the ConnectWise ScreenConnect console as sessions. Sessions can be dynamically grouped based on certain parameters and the two most often used are name (required) and organization (optional). The grouping of sessions allows MSPs to apply modifications to a number of machines at once.

About Acronis Cyber Cloud extension

The Acronis Cyber Cloud extension for ConnectWise ScreenConnect provides the ability to back up machines from the ConnectWise ScreenConnect console. A user can:

- Remotely install and update the Cyber Protection agent on a single or a group of machines.
- Apply a protection plan with enabled backup module to a machine.
- Monitor a device status by means of alerts and the monitoring dashboard.

Prerequisites

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

Activating your account

Prior to installing the extension, please obtain an Acronis Cyber Cloud account from an Acronis or partner sales representative. To obtain the account from Acronis, visit https://www.acronis.com/provider/backup-cloud/ and click **Contact Us**.

After signing the partnership agreement, you will receive an email message containing the following information:

- **An account activation link**. Click the link and set the password for your account. Remember your login that is shown on the account activation page.
- **A link to the login page**. By using this link, you can access the cyber protection console directly from a browser. The login and password are the same as in the previous step.

An API Client is necessary in order to configure the Acronis Cyber Cloud extension in ConnectWise ScreenConnect.

To setup an API Client, do the following:

1. Log into your Acronis account.
2. Go to **Settings** > **API clients**.
3. Click on **Create new API client**.
4. Enter a name for the client and click **Next**.
5. The next screen will show your Client ID and Secret. Make sure that you treat this information safely. The Secret will not be displayed again and your API key will be useless without it.

Roles and Permissions

Three different types of users exist for the purposes of the Acronis integration:

- **Admin**: grants full access to the integration, including its settings and the Acronis Dashboard.
- **Technician**: access to all integration functionalities, except for the integration settings and the Acronis Dashboard. Those users do have access to the Acronis Management portal for each customer.
- **View-only**: can only view data, but can't interact with the integration.

The Acronis extension makes use of permissions already given to users.
The **Admin** user should have at least Administer global permissions.
The **Technician** user should have at least Editsessions permissions.
The **View-only** user needs at least ViewSessionGroup, but not Editsessions or Administer global permissions.

You don't have to create new roles for the integration.

Any user that has these permissions, automatically receives the appropriate access to the integration.

System requirements

The integration requires a recent version of the ConnectWise ScreenConnect solution, already installed and configured.

The following operating systems are currently supported by the Cyber Protection agent:

Windows

Windows XP Professional SP1 (x64), SP2 (x64), SP3 (x86)

Windows Server 2003 SP1/2003 R2 and later – Standard and Enterprise editions (x86, x64)

Windows Small Business Server 2003/2003 R2

Windows Vista – all editions

Windows Server 2008 – Standard, Enterprise, Datacenter, Foundation and Web editions (x86, x64)

Windows Small Business Server 2008

Windows 7 – all editions

Windows Server 2008 R2 – Standard, Enterprise, Datacenter, Foundation and Web editions

Windows Home Server 2011

Windows MultiPoint Server 2010/2011/2012

Windows Small Business Server 2011 – all editions

Windows 8/8.1 – all editions (x86, x64), except for the Windows RT editions

Windows Server 2012/2012 R2 – all editions

Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016

Windows 10 – Home, Pro, Education, Enterprise, IoT Enterprise and LTSC (formerly LTSB) editions

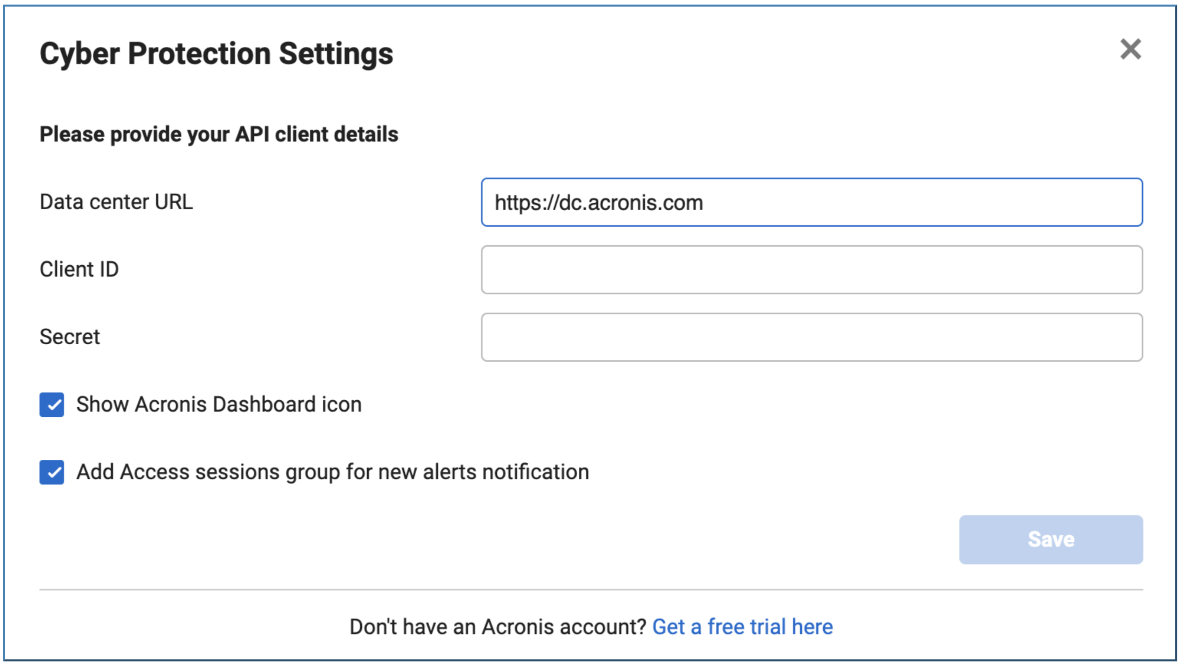
Windows Server 2016 – all installation options, except for Nano Server

Windows Server 2019 – all installation options, except for Nano Server

Installing the Acronis Cyber Cloud extension

To install the Acronis Cyber Cloud extension and configure integration between Acronis Cyber Cloud and ConnectWise ScreenConnect, do the following:

1. Log in to the ConnectWise ScreenConnect console.
2. In the left navigation menu, go to **Admin** > **Extensions**.
3. To open the Extension Marketplace, click **Browse Online Extensions**.
4. Find the Acronis Cyber Cloud extension and click **Install**. The extension will be automatically installed.
5. Close the **Extension Marketplace** window to go back to the list of installed extensions. Then find Acronis Cyber Cloud and click **Options** > **Cyber Protection Settings**.
6. Specify the following integration settings:



Cyber Protection Settings

Please provide your API client details

Data center URL: https://dc.acronis.com

Client ID:

Secret:

☑ Show Acronis Dashboard icon

☑ Add Access sessions group for new alerts notification

Don't have an Acronis account? Get a free trial here

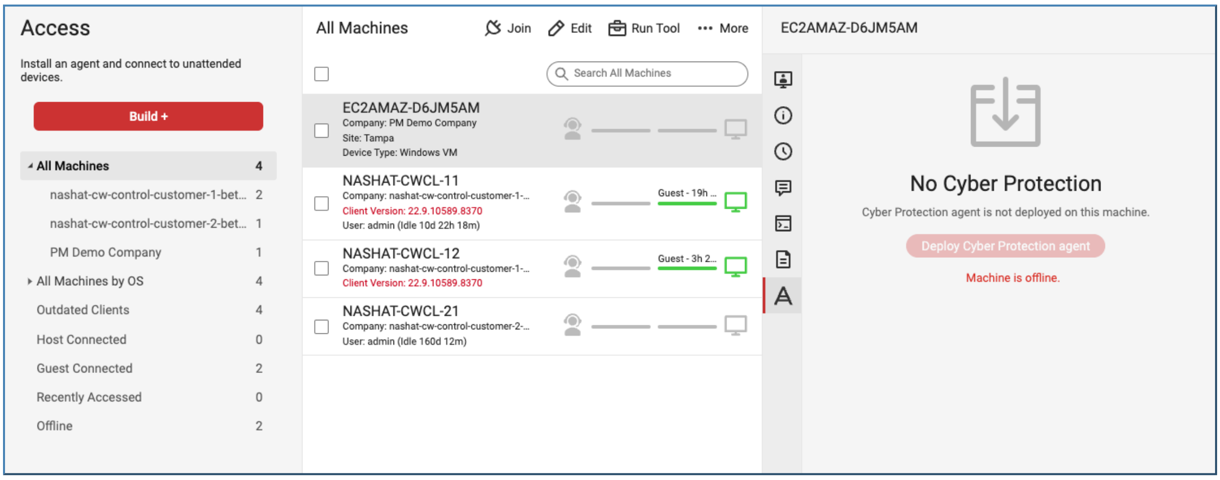
- **Data center URL** – URL of Acronis Cyber Cloud
- **Client ID** – your Acronis Cyber Cloud API Client ID
- **Secret** – your Acronis Cyber Cloud API Client Secret
- **Show Acronis Dashboard icon** checkbox:

  On – select this option to show an **Acronis Dashboard** icon in the left-hand panel of your ConnectWise ScreenConnect console. Click it to open the Acronis Management portal for detailed monitoring and management of your customers' machines.

  Off – clear this option to not show the **Acronis Dashboard** icon in the left-hand panel of your ConnectWise ScreenConnect console.
- **Add Access sessions group for new alerts notification** - use this checkbox to turn on/off the appearance of the session group in the left menu.

7. When ready, click **Save**.

If the Acronis Cyber Cloud extension installation was successful, the device view will be extended with the **Acronis** tab (Go to **Access** > **All Machines** and select a device from the list):



Install an agent and connect to unattended devices.

All Machines	4
nashat-cw-control-customer-1-bet...	2
nashat-cw-control-customer-2-bet...	1
PM Demo Company	1
All Machines by OS	4
Outdated Clients	4
Host Connected	0
Guest Connected	2
Recently Accessed	0
Offline	2

EC2AMAZ-D6JM5AM
Company: PM Demo Company
Site: Tampa
Device Type: Windows VM

NASHAT-CWCL-11
Company: nashat-cw-control-customer-1-...
Client Version: 22.9.10589.8370
User: admin (Idle 10d 22h 18m)

NASHAT-CWCL-12
Company: nashat-cw-control-customer-1-...
Client Version: 22.9.10589.8370

NASHAT-CWCL-21
Company: nashat-cw-control-customer-2-...
User: admin (Idle 160d 12m)

No Cyber Protection

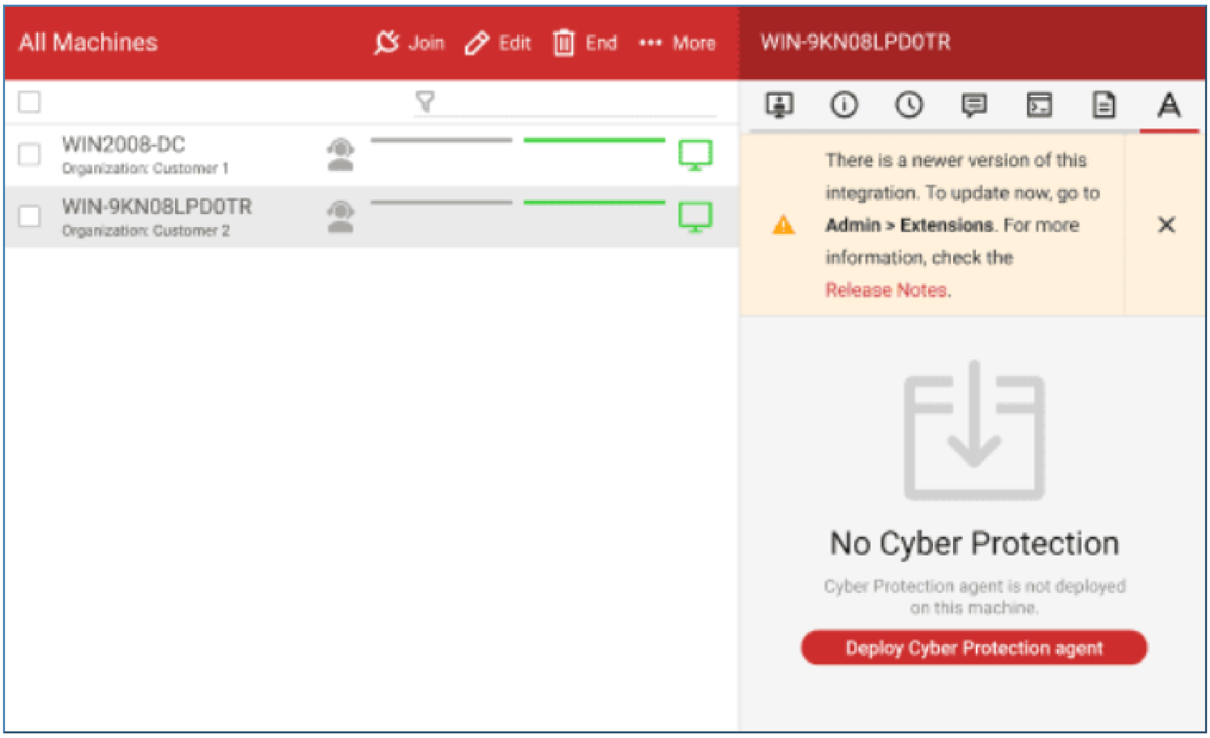
Cyber Protection agent is not deployed on this machine.

Deploy Cyber Protection agent

Machine is offline.

Now you can proceed with installing the Acronis Cyber Protection agent.

If the integration plugin is already out-of-date, the **Acronis** tab will inform you to make an update:



There is a newer version of this integration. To update now, go to **Admin > Extensions**. For more information, check the Release Notes.

No Cyber Protection

Cyber Protection agent is not deployed on this machine.

Deploy Cyber Protection agent

Automapping of devices and customers

The below scenario is intended for the cases when the Acronis agent is installed on a device outside the integration. Remapping is necessary in order for the Acronis agent info to appear on the Acronis tab.

Go to **Extensions parameters** form and click **Save**.

Installing, updating and unlinking the Cyber Protection agent for Windows, Mac and Linux

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.

Installing the Cyber Protection agent

The Acronis Cyber Protection agent can be deployed on Windows, Linux or macOS remote machines that have a ConnectWise ScreenConnect agent installation and have been already added to the ScreenConnect instance.

Note

The integration automatically detects which operating system is used and installs the corresponding agent.

For macOS specifically, depending on the particular version you deploy to:

- KEXTs or System extensions should be allowed
- the agent should have full disk access to be able to make backups.

To set up a protection plan on your machine(s), do the following:

1. In the left navigation menu, go to **Access** > **All Machines by Company** or select a session group.
2. Select at least one machine in the list, open the **Acronis** tab and click **Deploy Cyber Protection Agent**. Make sure that the machines are turned on.
3. When installing the agent, the machine will be assigned to either a new or existing customer in your Acronis account. Switching between the two installation methods is done by selecting one of the following two options: **Create a new Acronis customer** or **Use an existing Acronis customer**.
   - To install the Cyber Protection agent on a machine of a new customer, specify the following:

     Partner – the partner that your newly created customer will belong to.

     Customer – the customer account name.

     Login – the customer account login.

     Email – the email for the customer account.

     Password – the password for the customer account.

     Enable two-factor authentication check box – optionally, select to turn on this authentication method.

     Cyber Protection section – set Cyber Protection options by making selections from the drop-down lists: **Protection**, **Location**, **Backup storage** and **Disaster Recovery storage.**

     Protection can be set to one of the following billing modes:

    - **Standard protection per workload**
    - **Standard protection per GB**
    - **Legacy editions**
        - **Cyber Protect (all features, per workload)**
        - **Cyber Backup (backup only, per gigabyte)**

    All features available in both Standard and Advanced protection packs can be enabled for the selected billing mode but only the Advanced version supports multiple offering items at once.

    If you select either **per gb** or **per workload** editions, all Advanced packs will also be enabled for that customer tenant. Then you will only be charged based on your usage. Advanced packs can be disabled from the Acronis Management portal.

    You can optionally and separately enable **File Sync & Share** (make selections from the **Location** and **File Sync & Share storage** drop-down lists), **Physical Data Shipping** and **Notary** by marking those check boxes.

- To install the Cyber Protection agent on a machine of an existing customer, specify the following:

    Customer – select an existing customer from the drop-down list; partner accounts cannot be selected and appear disabled.

    Login – select an existing user under the selected customer account.

4. When ready, click **Deploy**.

It may take several minutes to deploy the Cyber Protection agent. During the installation, you cannot join the machine. To track the installation process, switch to the **Commands** tab.

As a result, the agent is installed on the selected machine(s).

The **Acronis Cyber Cloud** tab allows you to:

- Review machine protection details, including device status, last and next backup
- Apply a protection plan to the machine
- View and clear alerts
- Go to the Cyber Protection console
- Unlink the Cyber Protection agent

Updating the Cyber Protection agent

When the version of the Cyber Protection agent becomes outdated, an **Update Cyber Protection agent** button will become available.

To update the agent for your machine(s), do the following:

1. In the left navigation menu, go to **Access** > **All Machines** or select a session group.
2. Select one or several machines in the list, then go the **Acronis Cyber Cloud** tab > **General info** tab.
3. Scroll to the bottom to navigate to the **Update available** section. You will be able to check the

exact version, to which you can upgrade.

4. Click the **Update Cyber Protection Agent** button.

   As a result, the Cyber Protection agent will be updated on the selected machine(s).

Linking the session to the Cyber Protection agent

When setting up the integration, every workload in the instance is automatically checked for the following:

- Acronis agent installation
- whether it belongs to a customer tenant within the scope of the current partner tenant.

The ones that match these requirements become linked by default.

> **Note**
> Automatic session linking to the Cyber Protection agent can be done even after setting up the integration. This may be necessary if the agent was installed on a device outside the integration. In this case, opening the **Acronis** tab for the corresponding session displays the following message:
> "No Cyber Protection / Cyber Protection agent is not deployed on this machine."
> To link such sessions for all machines currently online:
>
> 1. Go to **Admin** > **Extensions** > **Acronis Cyber Cloud extension** > ... > **Edit settings**.
> 2. Click **Save settings**.

For any workloads that cannot be linked this way:

1. Use the **Deploy agent** button to first make the necessary installation.
2. Verify that the Acronis agent is installed successfully.
3. Link to new or existing customer tenant.

Unlinking the session from the Cyber Protection agent

Unlinking will remove the link between the ConnectWise session and the Acronis tenant. The Cyber Protection agent will not be uninstalled from the machine and unregistered from the cloud. Backups will continue to be created, but you won't see the **Acronis Cyber Cloud** tab in the ConnectWise control panel for this machine. You can re-create the link by clicking **Deploy Cyber Protection Agent**.

To unlink the Cyber Protection agent for your machine, do the following:

1. In the left navigation menu, go to **Access** > **All Machines**.
2. Select a machine for which you want to check the status.
3. Go to the **Acronis Cyber Cloud** tab, then select the **General info** tab and click **Unlink**.

As a result, the session will be unlinked from the Cyber Protection agent.

Uninstalling the Cyber Protection agent

To uninstall the Cyber Protection agent, do the following:

1. In the left navigation menu, go to **Access** > **All Machines** or select a session group.
2. Select one or several machines in the list, then go the **Acronis Cyber Cloud** tab > **General info** tab.
3. Click **Uninstall agent**.

Note
Uninstalling is permanent and can't be undone.

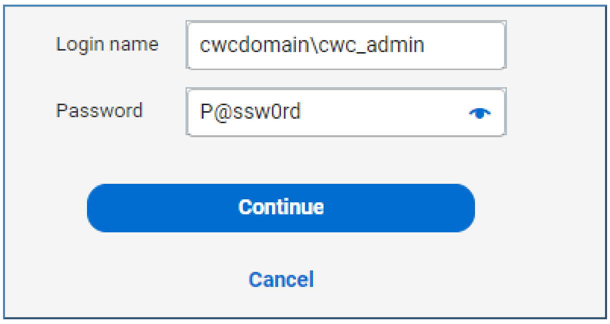
Domain Controller deployment

To deploy Acronis to a Windows Domain Controller, credentials are required for the agent installation.

When the installation is complete, the Domain Controller should have also been registered. You have to apply a protection plan yourself.

Installation on a workload

1. Select a workload that doesn't have an Acronis installation yet.
2. On the page that opens, click **Install agent**.
3. The integration checks if the workload is a Domain Controller.
4. You will be asked to provide credentials.



Login name: cwcdomain\cwc_admin

Password: P@ssw0rd

5. When the credentials have been entered, click **Continue** to proceed with the installation.

Configuring protection for machines

Protection plans are created in the Cyber Protection console. Plans are available immediately in ConnectWise ScreenConnect. Here you manage which plan is applied to the current machine.

The following operations can be performed with protection plans:

- View protection plan settings from the list of available plans
- Apply a plan
- Revoke an applied plan
- Run a backup or a scan

For more advanced operations and setup of new plans, click **Go to Cyber Protection console**.

Apply a protection plan

ConnectWise ScreenConnect lets you apply default protection plan to your machines.

For that purpose, do the following:

1. In the left navigation menu, go to **Access** > **All Machines** or select a session group.
2. Select a machine, switch to the **Acronis Cyber Cloud** tab, then go to the **Protection plans** tab.
3. Find the default protection plan or use the **+ Add plan** button to see a list of other available choices. You can view each plan details.

   Note
   If you have already set up protection plans in Acronis, you will see those here, instead of the default plan.

   You can also navigate back to the **Protection plans** tab by clicking "**Back to applied protection plans**".
4. Click **Apply** for the selected plan. As a result, it will be applied to the selected machine.

   Note
   The **Apply default protection plan** option is available on Windows workloads only.
5. Then you will be returned back to the **Protection plans** tab, which is now updated to show the plan you just applied. A green notification displays if the plan was successfully applied. Complete plan information is available as well.

Revoke a plan

1. In the left navigation menu, go to **Access** > **All Machines** or select a session group.
2. Select a machine, switch to the **Acronis Cyber Cloud** tab, then go to the **Protection plans** tab.
3. You will see a list of your currently **Applied Protection plans**. Click the **Revoke** button for the one you want to recall.

4. The **Protection plans** tab will refresh to show an updated view of the available protection plans ready to be applied.

Start a backup or anti-malware scan

1. In the left navigation menu, go to **Access** > **All Machines** or select a session group.
2. Select a machine, switch to the **Acronis Cyber Cloud** tab, then go to the **Protection plans** tab.
3. Select an already applied plan from the ones listed, click on its arrow **>** to expand the section for details.
4. Then for the **Backup** or **Vulnerability assessment** subsections, click again the arrow **>** at the end of the line to reveal more information.
5. You should be able to see details about each activity:
   - **Backup** - what and where to backup, for how long ahead to do it, for when it is scheduled
   - **Vulnerability assessment** - scope and schedule
6. Click the **Run now** button individually for each item.

Monitor the protection status

To view the Cyber Protection status of your machine, do the following:

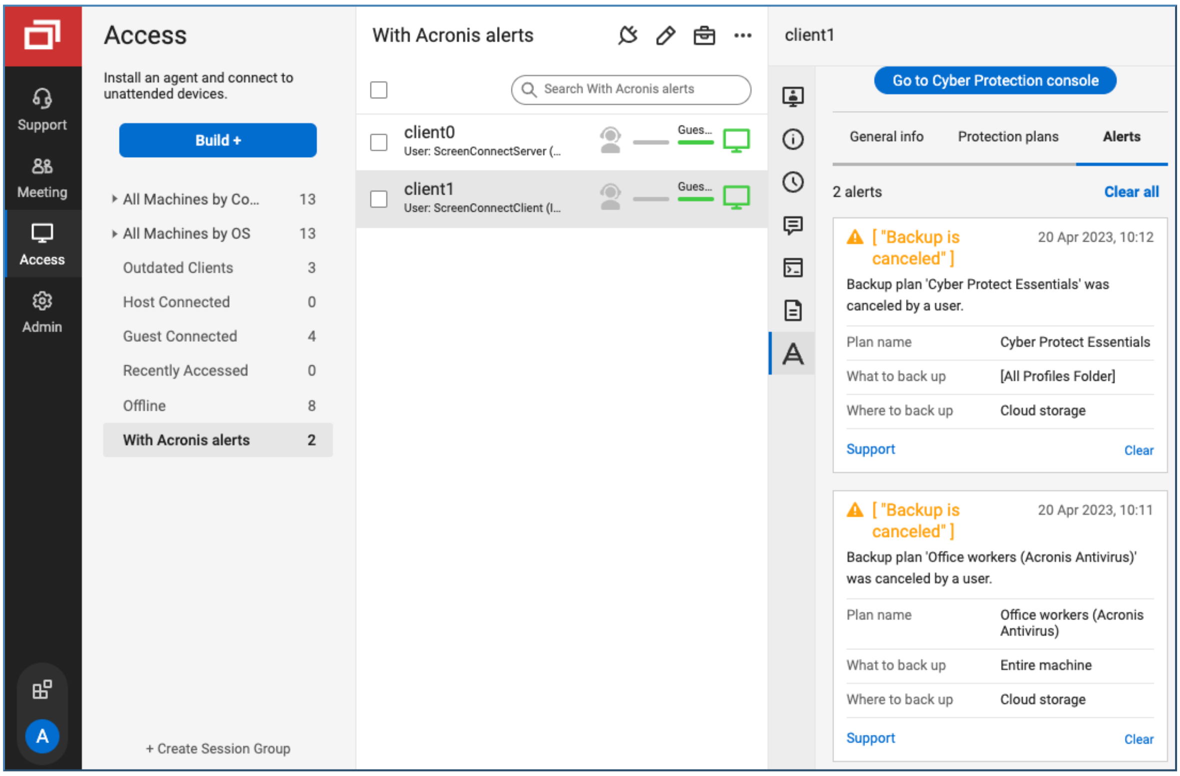
1. In the left navigation menu, go to **Access** > **All Machines**.
2. Select a machine, for which you want to check the status. On the **Acronis Cyber Cloud** tab > **General info** tab you can find information about the:
   - customer, user and agent
   - machine status, last and next backup details
   - any updates available

Monitoring dashboard and alerts

Viewing Alerts

Any Cyber Protection issues will appear as alerts, displayed in your ConnectWise ScreenConnect console. To view them:

1. In the left navigation menu, go to **Access** > **All Machines** or select the **With Acronis alerts** session group to view all devices that currently have open alerts.
2. Browse the list of machines and select one that has active alerts notification (these messages are updated on each product sync).
3. Navigate to the **Acronis Cyber Cloud** tab > **Alerts** tab to view the alert list of this particular device.



2 alerts Clear all

⚠ ["Backup is canceled"] 20 Apr 2023, 10:12

Backup plan 'Cyber Protect Essentials' was canceled by a user.

Plan name	Cyber Protect Essentials
What to back up	[All Profiles Folder]
Where to back up	Cloud storage

Support Clear

⚠ ["Backup is canceled"] 20 Apr 2023, 10:11

Backup plan 'Office workers (Acronis Antivirus)' was canceled by a user.

Plan name	Office workers (Acronis Antivirus)
What to back up	Entire machine
Where to back up	Cloud storage

Support Clear

Clicking **Support** will redirect you to the Acronis knowledge base. If there is a respective article on how to fix the issue, it will be opened.

4. Click **Clear** for each individual alert to close it. **Clear all** will close all alerts for the selected machine. Cleared alerts will no longer appear and the corresponding devices will be taken out from the **With Acronis alerts** session group.

The Acronis dashboard

If you select the **Show Acronis Dashboard icon** option while setting up the integration, then in the leftmost column you will find the **Acronis Dashboard** icon. It will redirect you to the Acronis dashboard where you can monitor your customers' machines, cloud resource usage and much more.

Sending your feedback

Send your feedback about the integration by using the form, located at:
Admin > **Extensions** > **Acronis Cyber Cloud** > **Options** > **Feedback**.

The following information is sent via the feedback form:

- The current ConnectWise ScreenConnect user login
- The feedback text
- The mapping file
- The log file
- The extension settings

Troubleshooting

If you have any issues with the integration, please follow the link available on the feedback screen, to download the log file and send it to the Support team.

Fix corrupted mapping

If your mapping file becomes corrupted or even deleted, you will receive the following notification:

"**Mapping is corrupted. A possible configuration issue with your Cyber Cloud setup has been detected. Please contact support or fix the issue automatically.**"

This situation can be easily resolved using the **Fix mapping automatically** option.

When clicking this button, you will see the following message:
"**This operation will verify and fix the setup for all online machines. For further assistance, please contact support.**"

Finally, click **Fix setup** to confirm and complete this adjustment.

Index