

Acronis

acronis.com

Acronis Cyber Cloud

Integration with WHMCS

REVISION: FRIDAY, JUNE 20,
2025

Table of contents

- Overview** **4**
 - Module features 4
- Supported services** **5**
- Supported languages** **7**
- Installing and activating the Acronis Cyber Cloud module** **8**
 - Prerequisites 8
 - Installation and activation 8
- Configuring the Acronis Cyber Cloud module** **10**
 - Adding a new server 10
- Configuring the product** **12**
 - Creating a template 12
 - Creating a product 14
 - Adding a configurable option group 15
 - Configuring usage billing 18
 - WHMCS configuration 18
 - Usage reports 19
 - Product configuration 22
 - Configuring product upgrades 23
 - Setting up product upgrades 24
 - Switching customers to new licensing 25
 - Overview 25
 - Partner Tenants (detailed instructions) 25
 - Customer Tenants Upgrade (detailed instructions) 27
 - Setting up resource upsell 30
 - Enabling resource overage 30
- Module upgrade from previous versions** **32**
 - Upgrade from version 1.0 32
 - Preparation for upgrade from version 1.0 32
 - Cleaning up after the upgrade 32
 - Upgrade from version 2.0 33
 - Preparation for upgrade from version 2.x 33
 - Procedure for upgrade from version 2.x 33
- Uninstalling Cyber Cloud module** **35**
 - Removing products 35
 - Removing configurable options 35

Removing templates	35
Removing servers and server groups	36
Deactivating addon	36
Removing tables and files	36
Troubleshooting	37
Logs	37
Known errors	37

Overview

The Acronis Cyber Cloud Module for WHMCS automates provisioning and billing of Acronis Cyber Protect Cloud services, including Cyber Protection, File Sync & Share, Physical Data Shipping.

This document describes the installation and configuration procedures of the Acronis Cyber Cloud module.

Module features

- Create new partner-type tenants (suitable for service providers and resellers). Partner tenants can manage their own customers in the Acronis Management console, configure their own brand for the Cyber protection services, and use their own storage to keep customers' data.
- Create new customer-type tenants (suitable for end customers) and provision services for them. Customers can manage the purchased services using the Acronis Cloud console.
- Manage created tenants: suspend and unsuspend, terminate with all their content.
- "Build your own" Acronis Product offering by choosing which offering items to include, defining the limits and the pricing.
- Sell Acronis Cyber Protection as add-on to other services (for more information, refer to https://docs.whmcs.com/Product_Addons).
- Upgrade/downgrade the provisioned subscription by purchasing additional offering items or switching to another Acronis product offering.
- Get the current usage metrics, invoice and bill the customers based on service consumption.
- See current usage statistics in the admin and client area.
- Manage notifications from the client area.

Check the latest release notes for Acronis Cyber Cloud plugin for WHMCS at <https://marketplace.whmcs.com/product/1246>.

Supported services

The Acronis Cyber Cloud module for WHMCS supports the following services:

- **Cyber Protect**

All-in-one cyber protection solution that integrates advanced data protection, file sync and share, file notarization and eSigning, and physical data shipping functionality.

- **Protection**

Provides all aspects of cyber protection, including backup, antivirus, antimalware, antiransomware, monitoring, management, and disaster recovery functionalities to satisfy most user needs. Available in per gigabyte and per workload billing modes. The standard protection can be extended with the following advanced protection packs:

- **Advanced Backup**

Enables backup of Microsoft SQL in a cluster, Microsoft Exchange in a cluster, Oracle Database, and SAP HANA. It also allows direct backup to Microsoft Azure, Amazon S3, and S3-compatible public cloud storage, and provides features such as continuous data protection (CDP) and data protection map. [Find out more.](#)

- **RMM**

Enables an advanced level of monitoring and management for endpoints and Microsoft 365 seats. For endpoints, it enables patch management, remote desktop and assistance, monitoring based on machine learning, software deployment, cyber scripting, and software inventory. For Microsoft 365 seats, it enables automatic remediation of security posture baseline deviations. [Find out more.](#)

- **Advanced Security + XDR**

Enables comprehensive cybersecurity through antivirus, antimalware, URL filtering, and real-time threat detection via Advanced Security. Utilizes Endpoint Detection and Response for event correlation, identifying advanced attacks on endpoints, or Extended Detection and Response for identifying advanced threats across endpoints, email, identity, and beyond. Compatible with workstations, servers, virtual machines, and web hosting servers. [Find out more.](#)

- **Advanced Email Security**

Enables real-time protection for your Microsoft 365 and Gmail mailboxes: antimalware, antispam, URL scan in emails, DMARC analysis, antiphishing, impersonation protection, attachments scan, content disarm and reconstruction, and graph of trust. [Find out more.](#)

- Mailboxes: Allows protection of mailboxes against phishing attacks.

- Microsoft 365 collaboration apps seats: Allows protection of M365 OneDrive, SharePoint and Teams against content-borne threats.

- **Advanced Security Awareness Training**

Enables teaching for individuals about the risks and threats associated with information security; training on simulated phishing emails; and providing the knowledge and skills necessary to protect themselves and their organization from cyberattacks. [Find out more.](#)

- **Advanced Disaster Recovery**

Makes disaster recovery painless and increases efficiency with orchestration, runbooks, and automatic failover.

- **Advanced Data Loss Prevention**

Prevents the leakage of sensitive information from workstations, servers, and virtual machines by inspecting the content of data transferred through local and network channels, applying pre-defined data classifications, and fine-tuning the organization-specific data flow policy in the enforcement mode. [Find out more.](#)

- **Advanced Automation (PSA)**

Enables MSPs to automate day-to-day operations and improve operational efficiency with CRM, service desk, billing and invoicing, analytics, and reporting tools. Natively integrates with Acronis services (including device control with RMM), and can also integrate with external remote monitoring and management (RMM) software.

- **File Sync & Share**

Provides file sharing that allows users to store and share encrypted content in the Cloud, and to synchronize it across their devices. Available in per gigabyte and per user billing modes.

- **Advanced File Sync & Share**

Extends the integrated secure file sharing capabilities of Acronis Cyber Protect Cloud with fully remote notarization, verification and online signing.

Enables users to notarize and verify files by using the Blockchain technology, and sign files electronically

- **Physical Data Shipping**

Enables users to send data to the Cloud data center on a hard disk drive, instead of transferring it over the Internet.

- **Cyber Infrastructure SPLA**

Enables service providers to use a Service Provider License Agreement (SPLA) for Acronis Cyber Infrastructure, instead of a license key.

Additionally, the Acronis Cyber Cloud module for WHMCS supports services and editions that were available as part of the licensing model in Acronis Cyber Protect Cloud 21.02 and earlier, including:

- **(Legacy) Cyber Protect Edition**
- **(Legacy) Cyber Backup Edition**
- **(Legacy) Cyber Protect - Standard Edition**
- **(Legacy) Cyber Protect - Advanced Edition**
- **(Legacy) Cyber Protect - Disaster Recovery Edition**
- **(Legacy) Cyber Backup - Standard Edition**
- **(Legacy) Cyber Backup - Advanced Edition**
- **(Legacy) Cyber Backup - Disaster Recovery Edition**
- **(Legacy) File Sync & Share**

These services and editions are still supported and can be configured in WHMCS but now considered legacy. We recommend to upgrade your customers to the new Acronis Cyber Protect in order to enable the new functionality and flexible licensing.

Supported languages

The Acronis Cyber Cloud module for WHMCS supports the following languages:

LANGUAGE	CODE
Chinese	zh_TW
Czech	cs_CZ
Danish	da_DK
Dutch	nl_NL
French	fr_FR
German	de_DE
Hungarian	hu_HU
Italian	it_IT
Japanese	ja_JP
Norwegian	no_NO
Brazilian Portuguese	pt_BR
Portuguese	pt_PT
Russian	ru_RU
Spanish	es_ES
Swedish	sv_SE
Turkish	tr_TR

Installing and activating the Acronis Cyber Cloud module

Prerequisites

The following system requirements must be met before installing the Acronis Cyber Cloud module version 2.8:

- Acronis Cyber Cloud 22.0 or later
- Supported WHMCS versions, see <https://marketplace.whmcs.com/product/1246>
- MySQL 5.5 or later
- PHP 7.2 or later
- PHP extensions:
 - php
 - php-common
 - php-cli
 - php-pdo
 - php-mbstring
 - php-mysqlnd
 - php-xml
 - php-xmlrpc
 - php-soap
 - php-imap
 - php-gd
 - php-pecl-apcu (recommended)

Installation and activation

To get and install the Acronis Cyber Cloud module for WHMCS, do the following:

1. Go to the WHMCS Marketplace and download the Acronis Cyber Cloud Provisioning module:
<https://marketplace.whmcs.com/product/1246>
2. Extract the module into the main WHMCS directory, for example:

```
#unzip -o ./AcronisModulesForWHMCS-2.9.0-XXX.zip -d <WHMCS_DIR>
```

Note

Make sure to verify the destination directory on your WHMCS installation.

Your next step is to activate the Acronis Cyber Cloud module in the WHMCS system.

3. If a WHMCS database user doesn't have permissions to create new tables in MySQL, you will need to grant the CREATE permission to this user for the whole period of new module activation.

a. Get the MySQL user name from the configuration file:

```
# grep db_username <WHMCS_DIR>/configuration.php
$db_username = 'whmcs-admin';
# grep db_name <WHMCS_DIR>/configuration.php
$db_name = 'whmcs';
```

b. Connect to the MySQL server and grant this user the necessary permissions:

```
> GRANT CREATE ON whmcs.* TO 'whmcs-admin';
```

4. Log in to your WHMCS admin area and go to **Configuration > System Settings > Addon Modules**.

5. Click **Activate** for the Acronis Cyber Cloud module.

6. Click **Configure** for the Acronis Cyber Cloud module and define the below setting:

- **Access Control:** select a role that will allow you to manage the module, for example, **Full Administrator**.

7. Save your changes.

8. When the module activation is completed, it is recommended to revoke the CREATE permission:

```
> REVOKE CREATE ON whmcs.* FROM 'whmcs_admin';
```

Configuring the Acronis Cyber Cloud module

After you have installed the module, you must configure servers for Acronis Cyber Cloud.

Adding a new server

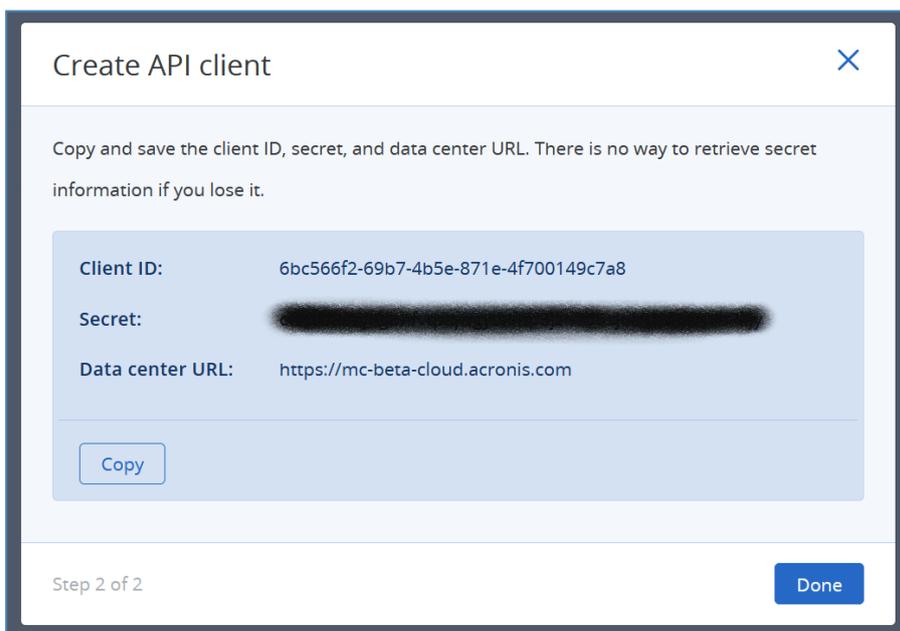
1. In the admin area, go to **Configuration > System Settings > Servers**.
2. Click **Add New Server**.

The screenshot shows a configuration form for adding a new server. At the top right, there is a blue button labeled "Go to Advanced Mode". The form includes the following fields and options:

- Module:** A dropdown menu with "Acronis Cyber Cloud" selected. Below it is the text "Choose the control panel the server uses".
- URL, Hostname or IP:** A text input field.
- Authentication method:** Radio buttons for "Client ID (recommended)" (which is selected) and "Username".
- Client ID:** A text input field.
- Client Secret:** A text input field.

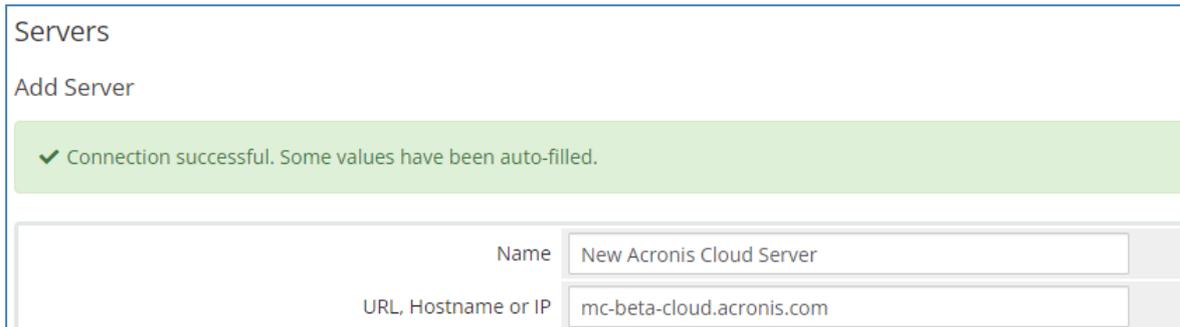
At the bottom of the form, there are four buttons: "Paste API Client Credentials »" (highlighted in blue), "Start Acronis 30 days trial" (highlighted in blue), "Test Connection »", and "Continue Anyway".

- **Module:** Acronis Cyber Cloud
 - **Authentication Method:** Client ID (recommended)
3. Go to Acronis Management Portal > **Settings > API Clients** and create a new client in advance. Use the available button to copy the credentials displayed.



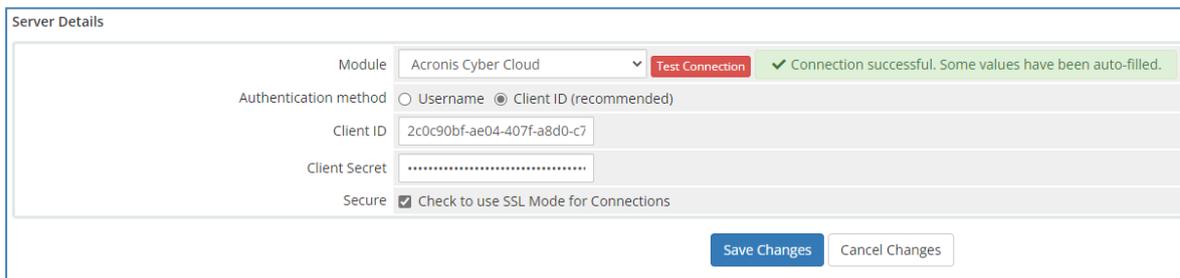
4. Click **Paste API Client Credentials**.
If the connection is successful, the next wizard page will open.

5. Enter the **Name** that will be displayed in the servers list, for example, "Acronis EU2."



The screenshot shows the 'Servers' section of a configuration interface. At the top, there is a green notification bar with a checkmark and the text: 'Connection successful. Some values have been auto-filled.' Below this, there is an 'Add Server' section with two input fields. The first field is labeled 'Name' and contains the text 'New Acronis Cloud Server'. The second field is labeled 'URL, Hostname or IP' and contains the text 'mc-beta-cloud.acronis.com'.

6. Verify that the **Secure** checkbox is selected in the **Server Details** section and click **Save Changes**.



The screenshot shows the 'Server Details' section of a configuration interface. It includes a 'Module' dropdown menu set to 'Acronis Cyber Cloud', a 'Test Connection' button, and a green notification bar with a checkmark and the text: 'Connection successful. Some values have been auto-filled.' Below this, there are radio buttons for 'Authentication method' with 'Client ID (recommended)' selected. The 'Client ID' field contains the text '2c0c90bf-ae04-407f-a8d0-c7'. The 'Client Secret' field is masked with dots. At the bottom, there is a 'Secure' checkbox which is checked, with the label 'Check to use SSL Mode for Connections'. There are two buttons at the bottom right: 'Save Changes' and 'Cancel Changes'.

The option to paste API credentials will only be available when using an HTTPS connection.

Reverting to a manual server configuration is possible by copy-pasting the API client details one by one. You will have to specify the exact data center in Acronis Cyber Cloud, for example "eu2-cloud.acronis.com".

If two-factor authentication is enabled for your Acronis Cyber Protect Cloud tenant, use the Client ID authentication method or you won't be able to establish a connection.

Starting from Acronis Cyber Cloud Module 2.0, the selection of authentication method will be automatically changed from Username to Client ID type, once you save the settings. The Client ID and Secret key will be also generated automatically, based on the provided username/password. The hostname you specified will be replaced with a specific data center that corresponds to the username in Acronis Cyber Cloud.

Configuring the product

Creating a template

1. In the admin area, go to **Addons > Acronis Cyber Cloud**.
2. Click **Create new template**.
3. Specify the template name (should be at least 3 characters long) and optionally, provide a description.
4. In the **Server** option, choose one of your Acronis Cyber Cloud servers to use for this template.
5. In the **Account type** option, select **Partner** if you want to provision only the partner tenants using this template, or select **Customer** to provision only the customer tenants.
6. To simplify the template configuration process, select a pre-configured service template sourced from the internal library of frequently used templates. In the subsequent step of the wizard, you'll have the flexibility to modify the assortment of available services and their corresponding quotas to align precisely with your needs.
7. (For Customer type only) In the **Pricing mode** option, select if you want to provision customer account in **Trial** or **Production** mode. If provisioned in trial mode, the customer will be automatically switched to production after 30 days (unless it is switched manually before).
8. (For Customer type only) Enable/disable the **Administrator** option. It defines if the first tenant user will be created in the Acronis Cloud with the Company Administrator role assigned or not. The role grants the user rights to manage all purchased services and access Management Portal to manage users within the entire company.
9. In the **Management mode** options, select **Self-Service** if the Acronis services will be managed by a partner/customer on their own completely or **Managed by Service Provider** if full access to the tenant is necessary.
10. Enable/Disable **Security** options.
 - **Two-factor authentication** enables 2FA for the tenant. If turned on, all users will require two-factor authentication setup.
 - (For Customer type only) **Enhanced security mode** defines whether to use encryption for all backups.
11. When all settings are defined, click **Next** step.
12. On the **Select Services** step, define a list of services that will be available to your partners or customers provisioned through this template:
 - Cyber Protection (per workload or per gigabyte billing modes), including the following advanced packs:
 - Advanced Backup
 - RMM
 - Advanced Security
 - Advanced Email Security

- Advanced Data Loss Prevention
 - Advanced Disaster Recovery
 - File Sync & Share (per user and per gigabyte billing modes)
 - Advanced File Sync & Share
 - Physical Data Shipping
 - Cyber Infrastructure SPLA (available only to partners)
- For the customer template type, you can choose only one billing mode (per gigabyte or per workload for Cyber Protection, per user or per gigabyte for File Sync & Share). For partner template type, all billing modes can be selected.

Legacy editions are supported to backward compatibility, including the following:

- (Legacy) Cyber Protect Edition
 - (Legacy) Cyber Backup Edition
 - (Legacy) Cyber Protect - Standard Edition
 - (Legacy) Cyber Protect - Advanced Edition
 - (Legacy) Cyber Protect - Disaster Recovery Edition
 - (Legacy) Cyber Backup - Standard Edition
 - (Legacy) Cyber Backup - Advanced Edition
 - (Legacy) Cyber Backup - Disaster Recovery Edition
 - (Legacy) File Sync & Share
13. The list of available services depends on your tenant, Acronis Cyber Cloud version and WHMCS module version. Select the required service(s), and then click **Next step**. On the **Configure services** step, you can enable/disable particular offering items for the selected services and specify a quota.
- For partner template type, we recommend to have all services enabled with unlimited quotas. For customer template type, choose services and quotas that best suit your customer.
14. When done, click **Save** to finish.

Creating a product

1. In the admin area, go to **Configuration > System Settings > Products/Services**.
2. Click **Create a New Group** to add a product group for Acronis Cyber Cloud and specify group details:
 - **Product Group Name:** for example, Acronis Cyber Cloud.
 - **Order Form Template:** select a layout to display products for customers, for example, Standard Cart.
 - **Available Payment Gateways:** select payment gateways to be available upon purchase.

The screenshot shows the 'Create Group' form in the 'Products/Services' section. The form includes the following fields and options:

- Product Group Name:** Acronis Cyber Protect Cloud
- URL:** /index.php?rp=/store/ acronis-cyber-protect-cloud (with a copy icon and 'OK' confirmation)
- Product Group Headline:** Buy Acronis Cyber Protect Cloud
- Product Group Tagline:** Modernize your cybersecurity and backup with integrated cyber protection
- Group Features:** You must save the product group for the first time before you can add features
- Order Form Template:** A grid of eight templates is shown, with 'Standard Cart (Default)' selected. Other templates include Premium Comparison, Pure Comparison, Supreme Comparison, Universal Slider, Cloud Slider, Legacy Boxes, and Legacy Modern.
- Available Payment Gateways:** A section for selecting payment gateways.
- Hidden:** A checkbox labeled 'Check this box if this is a hidden group'.

At the bottom of the form are two buttons: 'Save Changes' and 'Cancel Changes'.

3. Click **Save Changes**. A new product group was created and can be assigned now to products.
4. Click **Create a New Product** to create a new product or click  to configure an existing product.
5. On the **Product Details** page, configure the following parameters for your product:
 - **Product Type:** Other
 - **Product Group:** Acronis Cyber Cloud
 - **Product Name:** specify a product display name
 - **Module:** Acronis Cyber Cloud
 - **Create as Hidden:** select OFF if you want the product to be visible to your customers, or ON if not.
6. Then, click **Continue**.
7. In the **Edit Product** wizard, switch to the **Pricing** tab.
8. Depending on what product you want to offer to your customers (trial or production), configure one of the available pricing options.
For production, specify:

- **Payment Type:** Recurring
 - Click **Enable** for one of the available billing models – One Time/Monthly, Quarterly, Semi-Annually, Annually, Biennially, Triennially, and then specify **Setup fee** and **Price**.
9. Switch to the **Module Settings** tab and specify the settings below:
 - **Module Name:** Acronis Cyber Cloud
 - **Template Name:** select the Acronis Cyber Cloud template to use for this product
 - Choose the **Automatically setup the product as soon as an order is placed** option
 10. When done, click **Save Changes**.

Adding a configurable option group

If you want to allow your customers to purchase additional resources, you should set up the configurable option groups. The configuration process consists of the following steps:

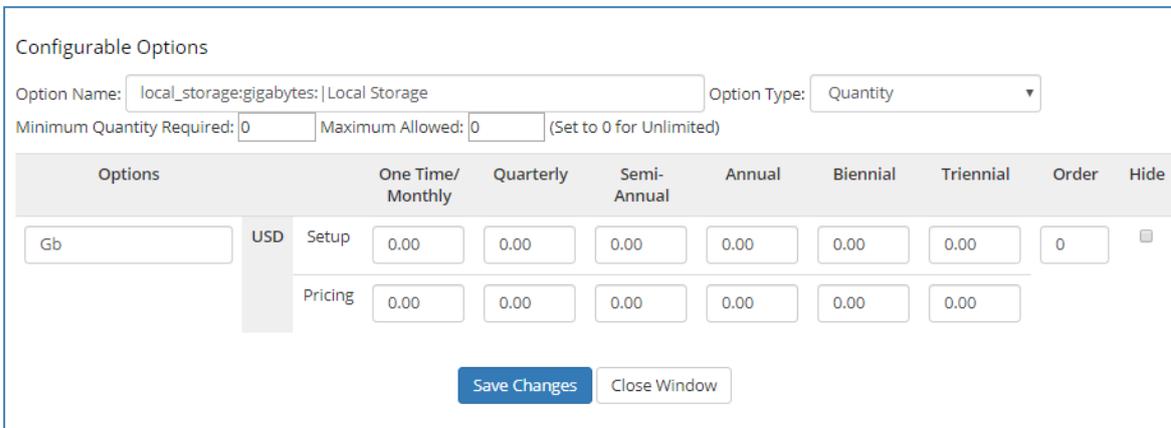
1. Use the wizard on the **Addons** page to create a new group.
2. To configure this new group, limit the number of offering items in the groups, define prices, etc.
3. Assign the configurable option group to a product by taking into account the following rules:
 - Use the customer-type template rather than the partner-type one, because by default partners have all services enabled and hence, some of billing metrics may not be applicable to the main product.
 - Products must be based on a template, created on the same server as the configurable option group.
 - Products must be based on a template with the same services and billing mode as selected in the configurable option group.

The steps to create a configurable option group for your product are the following:

1. In the admin area, go to **Addons > Acronis Cyber Cloud**.
2. Click **Add configurable options**.
3. Specify the following group parameters:
 - **Group name:** a name to display in the list of groups.
 - **Group description:** a description for the group of configurable options.
 - **Server:** selecting a specific server from the drop-down list will allow to retrieve only services, editions, and offering items available to the particular partner connected with the server.
 - **Service:** select a required edition.
4. Save the configuration.
The new group was created. Now you can proceed with setting up offering items within that group.
5. Go to **Configuration > System Settings > Configurable Options**.
6. Click the **Edit** icon for the new group.
7. In the **Assigned Products** field, select the product you created before.
Make sure the selected product was created on a template, targeted to the same server as the existing configurable option group, and for the same edition.

8. In the **Configurable Options** section, a full list of offering items, available for the selected server and edition, can be seen.

If you click the **Edit** icon  for an item, you can configure its settings as shown below:



- a. **Option Name:** This field has a special syntax and contains some item system information, separated by a colon, like:
- an internal name - for example, local_storage
 - an item attribute - for example, gigabytes, quantity or feature
 - a user-friendly name, visible to the customer - for example, Local Storage. Only this part can be modified, the internal name or other system attributes in this field should not be changed.

Files Cloud Storage requires an infrastructure component, therefore if you include this option into the configurable options group, ensure that the File Sync & Share service is enabled in the template. Otherwise, you should specify an infrastructure component for **Files Cloud Storage** explicitly. For more information, refer to the following article: <https://kb.acronis.com/content/63536>.

- b. **Option Type:** Depending on the specific item attribute, you can either select the **Quantity** or **Yes/No** option type from the drop-down list. See their relation in the table below:

	OPTION TYPE		
	Quantity	Yes/No	Dropdown
gigabytes	X		X
quantity	X	X	X
features		X	

The **Quantity** option type allows the customer to specify a number of items to purchase, while **Yes/No** is represented as a checkbox to activate/deactivate a particular item.

If you select the **Yes/No** type for the item of the quantity type, then upon purchase the customer will be asked to enable/disable it without the ability to manage the limit. The limit will be automatically set in accordance with the quota defined in the template.

Those items which, by default, use the **Quantity** option type can also use the **Dropdown** option to define service tiers that work as bundles and allow to configure different prices per service tier:

Configurable Options

Option Name: Option Type:

Options	One Time/ Monthly	Quarterly	Semi- Annual	Annual	Biennial	Triennial	Order	Hide
10 10GB	Setup 0.00	0.00	0.00	0.00	0.00	0.00	0	<input type="checkbox"/>
	Pricing 0.20	0.00	0.00	2.00	0.00	0.00		
20 20GB	Setup 0.00	0.00	0.00	0.00	0.00	0.00	0	<input type="checkbox"/>
	Pricing 0.18	0.00	0.00	0.00	0.00	0.00		
30 30GB	Setup 0.00	0.00	0.00	0.00	0.00	0.00	0	<input type="checkbox"/>
	Pricing 0.10	0.00	0.00	0.00	0.00	0.00		
Add Option:							0	<input type="checkbox"/>

In order to define service tiers, each item name has a special syntax that includes two parts, separated by a colon, like this:

- an internal value - for example, 20, meaning the item will add 20 units to the specific item.
- a user-friendly name, visible to the customer - for example, 20GB.

Configurable Options

PW - Workstations

5 workstations \$7.00 USD

PW - Microsoft 365 seats

0 x Seats \$0.50 USD

PW - Advanced Backup - Workstations

0 x Workstations \$1.00 USD

PW - Cloud Storage

10GB \$0.20 USD

10GB \$0.20 USD

20GB \$0.18 USD

30GB \$0.10 USD

Additional Information

Items are marked with *)

- Minimum Quantity Required:** minimum amount the customer will be asked to purchase.
- Maximum Allowed:** maximum amount of the item allowed for purchase.

- e. **Options:** units of measure visible to the customer.
- f. For the **Quantity** item type, you can specify **Unlimited** and select **Option Type = Yes/No**. In this case, the offering item will be allowed for activation in the marketplace and it will have the **Unlimited** quantity.
- g. **Setup fee** and **Pricing:** define prices for selected billing periods.
In this way, you will need to configure the list of offering items carefully and leave only those items that you want to offer to your customers additionally for the selected product. The rest of unnecessary offering items should be removed from this list.
- h. When done, click **Save Changes** to finish creating the group.

The table below explains how the total number of purchased items is calculated, depending on the limits in the product and in the configurable options group.

Countable offering items

Value in Configurable Options	Value in Template			
	Disabled	Limit = 0	Limit = x	Unlimited
Disabled	Disabled	0	X	Unlimited
Enabled	Unlimited	0	X	Unlimited
0	Disabled	0	X	Unlimited
Limit = Y	Y	Y	X+Y	Unlimited

Uncountable offering items

Value in Configurable Options	Value in Template	
	Disabled	Enabled
Disabled	Disabled	Enabled
Enabled	Enabled	Enabled

Configuring usage billing

WHMCS configuration

The Usage Billing feature uses WHMCS Crons (<https://docs.whmcs.com/Crons>) to collect usage reports from Acronis Cyber Cloud, so to be able to use it, crons should be set up.

1. If WHMCS is installed in a directory, different from /var/www/html/, you have to specify that directory in \$whmcs_path in the <whmcs-dir>/crons/config.php file.
2. If the config file doesn't exist yet, rename <whmcs-dir>/crons/config.php.new to <whmcs-

dir>/crons/config.php and then edit it.

3. Check the cron status at **WHMCS > System Settings > Automation Settings**.

For more information, go to https://docs.whmcs.com/Custom_Crons_Directory.

Usage reports

By default, the usage reports are stored at the following location:

```
/home/whmcs/downloads/acronis/reports
```

To store in a different category, edit the usage_report section in the <whmcs-dir>/includes/acronisccloud/config.yaml file. If there is no such section, you should add it in the following way:

```
usage_report:
download_path: tmp/reports
downloaded_files_ttl_in_days: 2
retries_limit: 2
retry_timeout: 300
```

Usage reports process

Usage report calculations are fully automatic and executed as part of the WHMCS cron jobs by using job hooks.

The process is the following:

1. A check is made for any Billing Metrics enabled for an Acronis product. If there are no such, cron jobs for usage reports are skipped.
Metrics are enabled in the **Module Settings** product.
2. After a cron job call in WHMCS is done, a reports' check is triggered (see the master command bellow).
 - For each Acronis server, if today's usage report is missing, it will be downloaded from the Acronis Cloud API.
 - The reports are stored in the configured Downloads location in the **WHMCSStorage Settings**. By default, an acronis/reports/ subfolder is created, where the reports are downloaded and grouped by date.
3. Twice a day, the metrics usage is gathered by WHMCS (see the TenantUsageMetrics cron task in https://docs.whmcs.com/Usage_Billing)
The usage calculation for Acronis reports is cached in the acronisccloud_service_report_storage database. You can reset the cache through the flushall manual command.
4. Once a day (as part of the daily cron job), the erase command is called to delete any outdated reports (to pass their TTL).

The cron status can be checked in **WHMCS > System Settings > Automation Settings**.

Usage report automation setup

Usage report jobs are automatically added to cron job hooks, but the commands are executed only if an Acronis product with Billing Metrics enabled exists. If not, the Acronis logs will show hooks triggered and skipped.

The above-described automatic usage report process, starts once a Billing Metric is enabled in an Acronis product and is done as part of WHMCS cron jobs execution.

By default, the usage report jobs use hardcoded values that match the ones in `config.yaml.sample`, which you can overwrite in the `config.yaml` file (see "Usage report configurations" (p. 21)).

The usage reports use the same folder as the one set in WHMCS > **Storage Settings** > **Downloads** to store the downloaded reports. A subfolder is also created there and its path can be overwritten in `config.yaml`.

The master command uses the `php` command by default, which must be CLI. If your `php` command isn't a CLI one, then you should set a path to the `php cli` interpreter in the `config.yaml` file.

Usage report manual commands

As part of the package, a command line tool is added to the WHMCS directory (`manage.php`), which can be used together with:

```
> php <whmcs-dir>/manage.php usage-report:<COMMMAND>
```

The `manage.php` script requires `php CLI` to run.

Available commands:

- `erase` - forces run of the "after daily cronjob" hook action that deletes expired reports.
- `flushall` - deletes all usage reports from the disk and database, including the metrics cache stored in the database.
- `process <SERVER_ID>` - downloads the usage report of a server with the provided id unless such report has been already downloaded for the same day.
- `master` - forces the "after each cron job" hook that downloads the usage reports for all Acronis servers using the `process` command. This happens automatically after each cron job.
- `metrics` - for each tenant id and offering item, check today's calculated metrics. This does not refresh the metrics in the WHMCS orders.
- `view-list` - for each server, view a table with usage reports status, including download date and location.
- `precheck` - checks the configuration before a module upgrade; provides a list of billing metrics to be removed or changed as well as a list of currently used billing metrics.

Executing any of the above actions from `manage.php` will run even if no billing usage metrics are enabled in any product. Cron job hooks (after each or daily cron job) will be triggered only if usage metrics are enabled for an Acronis product in WHMCS.

To force a metrics update in WHMCS, you can trigger manually the WHMCS cron job to fetch metrics for orders. Otherwise, it will be triggered automatically twice a day. For more information, see <https://docs.whmcs.com/Crons>:

```
php /path/to/cron.php do --TenantUsageMetrics
```

Usage report configurations

- `php_cli_interpreter` - an interpreter cli command, used by the master command to process reports (php by default)
- `download_path` - a subfolder created in the Downloads location for storage of downloaded reports (acronis/reports by default)
- `downloaded_files_ttl_in_days` - days to keep a downloaded report, before the erase command deletes it (2 by default)
- `retries_limit` - number of checks by the process command if a report download has finished successfully (2 by default)
- `retry_timeout` - halt time (in seconds) between each check done by the process command (300 by default)

Product configuration

Metrics are enabled from the product's **Module Settings**.

To enable a metric for billing or display purposes, slide the respective toggle to On position.

To configure the metric pricing, click **Configure Pricing**.

Enabled metrics are visible in the admin and client areas when viewing a service that belongs to a product.

The following metrics are supported:

Service/Billing Mode	Billing Metric Prefix	Metric Type
Cyber Protection (per gigabyte billing mode)	Cyber Protection (per GB) - *	Storage metrics for base offering items
	<Advanced Pack Name> - *	Metrics for advanced licensing packs
Cyber Protection (per workload billing mode)	Cyber Protection (per workload) - *	Storage metrics for base offering items
	Cyber Protection (per workload) - *	All other metrics for base offering items
	<Advanced Pack Name> - *	Metrics for advanced licensing packs
File Sync & Share	File Sync & Share (per user) - *	All metrics
Physical Data Shipping	Physical Data Shipping - *	All metrics

Service/Billing Mode	Billing Metric Prefix	Metric Type
Cyber Infrastructure	Cyber Infrastructure - *	All metrics
(Legacy) Cyber Protect Edition	(Legacy) Cyber Protect -*	All metrics
(Legacy) Cyber Backup Edition	(Legacy) Cyber Backup Standard - *	Storage metrics for (Legacy) Cyber Backup
(Legacy) Cyber Files	(Legacy) Cyber Files Cloud - *	All metrics

To sell a product to end customers, use the " * - Cloud storage" metric to charge for Cloud storage.

To sell a product to partners, using Acronis-hosted Cloud storages, use the following metrics:

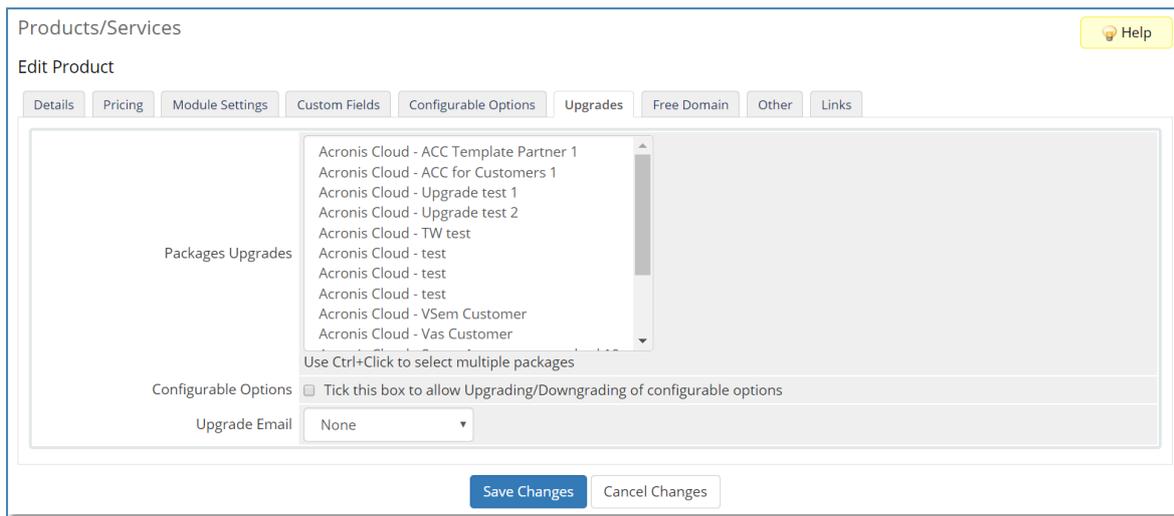
1. * - Acronis-hosted storage
2. * - Google-hosted storage
3. * - Azure-hosted storage
4. * - Partner storage

To sell a product for partners that use own Cloud storages, use the below-listed metrics:

1. * - Cloud storage
2. * - Partner storage
3. * - Service Provider storage

Configuring product upgrades

1. In the admin area, go to **Configuration > System Settings > Products/Services**.
2. Click on the product that you want to configure.
3. Switch to the **Upgrades** tab.
4. Select the alternative products to which your product can be upgraded or downgraded.



5. Click **Save Changes**.

Setting up product upgrades

1. Log in to your admin area in WHMCS, go to **Configuration > System Settings > Products/Services**.
2. Click the product that you want to configure.
3. Switch to the **Upgrades** tab.
4. Select the alternative products to which your product can be upgraded or downgraded, and click **Save Changes**.

For successful product upgrade, both products and service templates must meet the following requirements:

Object	Requirements
Template	<ul style="list-style-type: none"> - The same tenant type - The same edition - The same location and storage(s) selected
Server	The same server
Configurable Options Group	If there are different groups, assigned to source and target products, then after the upgrade, the source group will be unprovided, but the target group will not be provided. It can be purchased additionally later.

Switching customers to new licensing

Overview

1. To switch partner tenants created via WHMCS to the advanced licensing (21.03):
 - a. Stop selling legacy offerings to new partners.
 - b. Enable new offerings for the existing partner by adding them to existing partner templates and product, and updating the partners to new product version.
 - c. Ask your partners to switch their end customers to the advanced licensing.
 - d. Move the partners to the product without legacy offerings.
2. To switch customers' tenants created via WHMCS to the new licensing:
 - a. Stop selling legacy offerings for new customers.
 - b. Configure upgrade path from products based on legacy editions to products based on advanced licensing.
 - c. Upgrade all your customers to the products without legacy offerings.

Partner Tenants (detailed instructions)

Step 1. Stop selling legacy offerings to new partners

1. Hide the existing Acronis Cyber Cloud partner template from order form: **Products/Services** > **<Acronis Cyber Cloud for Partners>** > **Edit** > **Details** > Check **Hidden** box > **Save** the changes. This will ensure that old licensing is not available for the customers in the Client Area.
2. Create a new template based on the new licensing: **Addons** > **Acronis Cyber Cloud** > **Create New Template**. Make sure that legacy editions (**Cyber Protection** > **Legacy Editions and File Sync & Share** > **Inherited from partner contract**) are not selected.
3. Create a new product based on this template. Use this product to provision Acronis Cyber Cloud to new partners.

Step 2. Enable new offerings for the existing partners

1. Add advanced licensing offerings to the existing partner template: **Addons** > **Acronis Cyber Cloud** > **<Acronis Cyber Cloud Template for Partners>** > **Edit** > **Select Services** > **Enable Cyber Protection (per workload/per gigabyte)** and **File Sync & Share (per user/per gigabyte)**, as well as all Advanced packs available.
Do not de-select any legacy services yet.

Note

We recommend keeping all the quotas unlimited for the partner tenants, but if you used quotas in partner templates before, you can configure them on the **Configure Service** step of the template wizard.

2. Save the updated template.

3. If you used Pay-As-You-Go (usage-based billing) model for partner tenants, you need to enable usage billing for new offering items: **Products/Services > <Acronis Cyber Cloud for Partners> > Edit > Module Settings > Enable new offering items and set the price per unit > Save** the changes.
See the list of billing metrics available in "Product configuration" (p. 22).
4. In case you have used quotas and configurable options for partner products before, you might want to set up new configurable options based on advanced licensing offerings and add them to the product:
 - a. **Addons > Acronis Cyber Cloud > Add Configurable Options > Select non-legacy edition you need > Save** the changes.
 - b. **Products/Services > <Acronis Cyber Cloud for Partners> > Edit > Configurable Options > Select required configurable options > Save** the change.

Note

In general, we recommend using a simple PAYG (usage-based billing) model for partners and not using configurable options for them.

5. Update your existing partners to a new version of the Acronis Cyber Cloud product (you can do so by placing an upgrade order for partner for the same product).

After that advanced licensing will be available for the partner tenant in Acronis Cyber Cloud.

Step 3. Ask partners to switch their customers to new licensing

Ask your partners to switch their end customers to the new licensing.

If a partner doesn't use any integration to manage their customers, they can do the switch either directly in the Acronis Cyber Cloud portal or using mass edition switch script:

<https://kb.acronis.com/de/node/67942>.

If the partner uses some integration to manage their customers, they should follow the guidelines of the corresponding integration.

Step 4. Move the partners to the product without legacy offering

When all the end customers are switched to the new licensing, and there is no usage for legacy offering items, you can switch your partner to a new product that contains only new licensing (e.g. the one you've configured in Step 1). This can be done by placing an upgrade order for a new product in WHMCS.

Note

Do not switch the partner, if some of their end customers still use legacy products. If there is non-zero usage for legacy products, the upgrade order will either fail or some of the end customer services will be de-provisioned (depending on the way product/template is configured in WHMCS and which services are still in use).

After all partners are switched, you can disable/remove the old offering in WHMCS.

Customer Tenants Upgrade (detailed instructions)

Step 1. Stop selling legacy offerings to new customers

1. Hide the existing Acronis Cyber Cloud customer template(s) from order form: **Products/Services** > <**Acronis Cyber Cloud for Customers**> > **Edit** > **Details** > Check **Hidden** box > **Save** the changes.
This will ensure that old licensing is not available for the customers in the Client Area.
2. Create a new template based on the new licensing: **Addons** > **Acronis Cyber Cloud** > **Create New Template**. Make sure you do not use any legacy edition (**Cyber Protection** > **Legacy Editions and File Sync & Share** > **Inherited from partner contract**).
3. If you use quotas for customer products, define them on the **Configure Service** step of the template wizard.
4. Create a new product(s) based on this template. If you use PAYG (usage-based billing) model, refer to the billing metrics list in "Product configuration" (p. 22) to see which metrics should be enabled in the product configuration (**Module Settings** section).
5. Use new products to provision Acronis Cyber Cloud to new customers.

Step 2. Configure upgrade path from products based on legacy editions to products based on advanced licensing

To allow your customer to switch to a licensing offering, you have to configure an upgrade path from the product(s) based on the legacy edition to the product(s) based on new advanced licensing. This can be done from **Products/Services** > <**Acronis Cyber Cloud for Customers**> > **Edit** > **Upgrades**.

For a successful upgrade, make sure that you have proper services and advanced packs with correct quotas in new products (templates). The table below shows the upgrade paths that have been tested for WHMCS as well as guidelines on how to set the quotas. If you use configurable options in legacy and new products, verify that the same set of offering items is available, otherwise, the upgrade order can fail or some services could be disabled during upgrade.

Service	Legacy Licensing	New licensing	How to set Quotas
Protect	(Legacy) Cyber Backup (per gigabyte)	Cyber Protect (per gigabyte)	same as in the source edition
	(Legacy) Cyber Protect (per workload)	Cyber Protect (per workload) + RMM + Advanced Security + Advanced Backup + Advanced Disaster Recovery	for base - same as in the source editions, for packs see below
	(Legacy) Cyber Backup - Standard Edition	Cyber Protect (per workload/per gigabyte)	same as in the source edition
	(Legacy) Cyber	Cyber Protect (per workload/per gigabyte) +	for base - same as in

Service	Legacy Licensing	New licensing	How to set Quotas
	Backup - Advanced Edition	Advanced Backup + RMM	the source editions, for packs see below
	(Legacy) Cyber Backup - Disaster Recovery Edition	Cyber Protect (per workload/per gigabyte) + Advanced Backup + RMM + Advanced Disaster Recovery	for base - same as in the source editions, for packs see below
	(Legacy) Cyber Protect - Standard Edition	Cyber Protect (per workload/per gigabyte) + RMM + Advanced Security	for base - same as in the source editions, for packs see below
	(Legacy) Cyber Protect - Advanced Edition	Cyber Protect (per workload/per gigabyte) + Advanced Backup + RMM + Advanced Security	for base - same as in the source editions, for packs see below
	(Legacy) Cyber Protect - Disaster Recovery Edition	Cyber Protect (per workload/per gigabyte) + Advanced Backup + RMM + Advanced Disaster Recovery + Advanced Security	for base - same as in the source editions, for packs see below
File Sync & Share	File Sync & Share (Legacy):	File Sync & Share (per user/per gigabyte)	same as in the source edition
Data Shipping	Physical Data Shipping	Physical Data Shipping	same as in the source edition

How to set quotas:

Pack Offering Item	Quota
Advanced Data Loss Prevention	equals the sum of all quotas (Workstations, Servers, Virtual Machines, Web Hosting Servers) from the source editions
Advanced Data Loss Prevention Quotas	equals the sum of all quotas (Workstations, Servers, Virtual Machines, Web Hosting Servers) from the source editions
Advanced Security	equals the sum of all quotas (Workstations, Servers, Virtual Machines, Web Hosting Servers) from the source editions
Acronis RMM	equals the sum of all quotas (Workstations, Servers, Virtual Machines, Web Hosting Servers) from the source editions
Advanced Backup - Workstations	equals to Workstations' quotas in the source edition
Advanced Backup - Servers	equals to Servers' quotas in the source edition
Advanced Backup - Virtual Machines	equals to Virtual Machines' quotas in the source edition
Advanced Backup - Web Hosting Servers	equals to Web Hosting quotas in the source edition
Advanced Disaster Recovery - Storage	equals to DR Storage quotas in the source edition
Advanced Disaster Recovery - Compute points	equals to Compute points' quotas in the source edition
Advanced Disaster Recovery - Public IPs	equals to Public IPs' quotas in the source edition
Advanced Disaster Recovery - Cloud Servers	equals to Cloud Servers' quotas in the source edition

Step 3. Upgrade your customers to new products

When the upgrade path is configured, customers can switch to the new licensing on their own, by placing upgrade order for the new product. Alternatively, place upgrade orders on behalf of your customers.

When the upgrade order is completed, the customer will be switched from legacy to new services in Acronis Cyber Cloud. The quotas will be set accordingly to the new product configuration. The usage will be recalculated automatically in Acronis Cyber Cloud and updated in WHMCS next time after the cron job for usage collection is processed.

Once all customers are upgraded to a new product, you can disable/remove the old products from WHMCS.

Setting up resource upsell

To enable buying additional resources to the existing subscriptions via configurable options, do the following:

1. In the admin area, go to **Configuration > System Settings > Products/Services**.
2. Click the product you want to configure.
3. Switch to the **Upgrades** tab.
4. Enable the **Allow Upgrading/Downgrading of configurable options** checkbox.
5. Click **Save Changes**.

Enabling resource overage

To activate the overage feature, you need to create a `config.yaml` from a sample or modify the existing file, then set up the `overage_ratio` variable. This variable is a multiplier, used to calculate resource overage, according to the below formula:

$Hard\ quota = soft\ quota * overage_ratio$

$Overage = soft\ quota * (overage_ratio - 1)$

where the soft quota is a limit defined for the offering item in a template.

For example, suppose you defined the `overage_ratio = 1.5`. You also have a template with a quota set up for Workstations = 10. As a result, a customer subscribed to that product will get the following quota for Workstations in Acronis Cyber Cloud:

$Quota = 10$

$Overage = 5$

When the limit of 10 is reached, the customer will receive a notification about the exceeded quota, but will still be allowed to use the Workstations resource up to 15.

When the limit of 15 is reached, this resource usage will be restricted.

The `overage_ratio` is a server-wide setting, which means it will be automatically applied to each offering item in the order, placed for any of the Acronis Cyber Cloud products. It is not instantly applied to templates, only to the client subscriptions.

To configure the `overage_ratio`, do the following:

1. Create the `config.yaml` file from a sample (if you have not done it yet):

```
# cd <WHMCS_DIR>/includes/acroniscloud
# cp config.yaml.sample config.yaml
```

2. Open `config.yaml` for editing and define a value for `overage_ratio`, for example:

```
overage_ratio: 1.5
```

- The default value is 1.0, which means that the overage is equal to 0. You can set up any value greater than 1 as long as it suits your needs.

Module upgrade from previous versions

The Acronis Cyber Cloud module 2.8 supports upgrade from the following versions:

- Acronis Cyber Cloud Provisioning Module 1.0: build 1.0.177
- Acronis Cyber Cloud 2.0: build 2.0.127

Depending on the version installed, follow the corresponding chapter down below for upgrade instructions.

Upgrade from version 1.0

Preparation for upgrade from version 1.0

Make sure that the following requirements are met:

- Acronis Backup Cloud Provisioning Module v1.0.177 is installed
- Acronis Cyber Cloud platform 8.0 is installed
- Logging to the file is enabled on the WHMCS server
- Check the module configuration, especially the following settings:
 - Acronis servers have valid connection settings.
 - The offering items' parameters at **Module Settings** like unit of measure, storage and account type are correctly configured for Acronis products.
 - For each of the options included into configurable options groups, the name and unit of measure in the **Add Option** field should be defined.

If you have a lower version of Acronis Backup Cloud Provisioning Module installed, you should proceed with the upgrade to v1.0.177 first.

If you still work on Acronis Cyber Cloud platform lower than 8.0, you will not be able to activate a new version of the module. We recommend you to proceed with the upgrade only after platform update to 8.0 at the Acronis site.

We strongly recommend you to create a backup of your WHMCS installation directory and WHMCS system database before starting the upgrade procedure.

Cleaning up after the upgrade

Once a new Acronis Cyber Cloud module is installed and upgraded, you can remove the old one from the WHMCS system, following the instructions below.

1. Connect and log in to the WHMCS server.
2. Go to the WHMCS system installation directory and remove the directories with the following files from the system:

```
<WHMCS_DIR>/includes/Acronis  
<WHMCS_DIR>/modules/servers/AcronisBackupService  
<WHMCS_DIR>/templates/orderforms/acronis_backupservice
```

Verify the WHMCS directory on your installation and replace the <WHMCS_DIR> example in the path.

Once you remove these directories from the server, the old Acronis Backup Cloud module will disappear from the WHMCS portal.

Upgrade from version 2.0

Preparation for upgrade from version 2.x

1. Verify that the following requirements are met:
 - Previous version of Acronis Cyber Cloud Module is installed, e.g. if you want to install version 2.3.x you need to have 2.2.x available.
 - Acronis Cyber Cloud platform 8.0 or higher is used.
 - Logging in to the file is enabled on the WHMCS server.
 - Check the module configuration, especially the following details:
 - Acronis servers have valid connection settings.
If you have a lower version of Acronis Cyber Cloud Module 2.0 installed, please proceed with the upgrade to 2.0.127 first.

Note

We strongly recommend you to create a backup of your WHMCS installation directory and WHMCS system database before starting the upgrade procedure.

2. Provide ALTER permissions to the WHMCS database user.
3. Get the MySQL user name from the configuration file:

```
# grep db_username <WHMCS_DIR>/configuration.php  
$db_username = 'whmcs-admin';
```

4. Grant the necessary permissions to this user:

```
> GRANT ALTER ON whmcs.* TO 'whmcs-admin';
```

When this is done, you can proceed with updating the module.

Procedure for upgrade from version 2.x

To upgrade the module, do the following:

1. Go to the WHMCS Marketplace and download the new version of Acronis Cyber Cloud

Provisioning module: <https://marketplace.whmcs.com/product/1246>

2. Extract the new version into the main WHMCS directory, for instance:

```
# unzip -o ./AcronisModulesForWHMCS-2.9.0-XXX.zip -d <WHMCS_DIR>
```

Verify the destination directory on your WHMCS installation.

3. After the module update, revoke the ALTER permission:

```
> REVOKE ALTER ON whmcs.* FROM 'whmcs_admin';
```

Uninstalling Cyber Cloud module

This chapter provides instructions on how to uninstall the Acronis Cyber Cloud module of version 2.x.

Before you start the uninstall procedure of this module from the WHMCS system, make sure that there are no client orders for Acronis Cyber Cloud services left in WHMCS. Cancel and remove these orders if there are any, otherwise the system will not let you uninstall the module.

Then you can proceed with uninstalling the Acronis Cyber Cloud module in the following sequence.

Important

We can guarantee smooth product uninstallation only if there are no client orders placed for Acronis products in the WHMCS system. Otherwise, there is a chance that the system will not process the uninstallation procedure correctly due to some internal dependencies, and assistance from Support might be required.

Removing products

1. In the admin area, go to **Configuration > System Settings > Products/Services**.
2. Click the delete icon for the product you want to remove from the system and then confirm the operation.

Repeat step 2 for all the products, related to the Acronis Cyber Cloud service.

Removing configurable options

1. In the admin area, go to **Configuration > System Settings > Configurable Options**.
2. Click the delete icon for the configurable option group you want to remove from the system and then confirm the operation.

Repeat step 2 for all groups, related to the Acronis Cyber Cloud service.

Removing templates

1. In the admin area, go to **Addons > Acronis Cyber Cloud**.
2. Click the delete icon for a template that you want to remove from the system and confirm the operation.

Repeat step 2 for all the templates, related to the Acronis Cyber Cloud service.

Note

It is forbidden to delete a template used by a product. You should always delete the product first.

Removing servers and server groups

1. In the admin area, go to **Configuration > System Settings > Servers**.
2. You have to delete all of the server groups first. Click the delete icon for such server group and confirm the operation.

Repeat this action for all server groups, created for the Acronis Cyber Cloud service.

3. Then click the delete icon for a server that you want to remove from the system and then confirm the operation.

Repeat step 3 for all servers, related to the Acronis Cyber Cloud service.

Deactivating addon

1. In the admin area, go to **Setup > Addon Modules**.
2. Click **Deactivate** for the Acronis Cyber Cloud module and then confirm the action.



Removing tables and files

1. Log in to the WHMCS server and remove the module directories with all files from the WHMCS installation directory:

```
<WHMCS_DIR>/includes/acroniscloud/  
<WHMCS_DIR>/modules/addons/acroniscloud/  
<WHMCS_DIR>/includes/hooks/acroniscloud.php  
<WHMCS_DIR>/modules/servers/acroniscloud/
```

2. The last step is to clean up the WHMCS database from the tables named by acroniscloud*.

Troubleshooting

Logs

The most useful logs that will help you to identify and track the technical issues, related to the Acronis Cyber Cloud module can be found in the following ways:

1. The logs in WHMCS > **Utilities** > **Logs**:
 - **Module Log**: to enable it, open **Setup** > **Addon Modules**, click **Configure** for Acronis Cyber Cloud and select types of calls that will be logged by the system:
 - API calls to Acronis Cyber Cloud
 - API calls to the WHMCS platform
 - Queries to the WHMCS database
 - **Activity Log**
2. Logging in to the acronis-cloud.log file

Create a destination directory:

```
# mkdir /var/log/acroniscloud
# touch /var/log/acroniscloud/acronis-cloud.log
# chmod 777 /var/log/acroniscloud/acronis-cloud.log
```

Modify the config.yaml configuration file. If it doesn't exist yet, create it from the sample config:

```
# cd <WHMCS_DIR>/includes/acroniscloud/
# cp config.yaml.sample config.yaml
# vim config.yaml
logger:
enabled: true
filename: /var/log/acroniscloud/acronis-cloud.log
level: DEBUG
```

Note

The text logs can affect the performance, therefore we recommend you to enable it temporarily for debugging purposes only.

Known errors

Error	Scenario	Steps to resolve
Current database user has missing rights: CREATE	Activating addon module	Allow the MySQL database user to create tables in the WHMCS database. See "Module upgrade from previous versions" (p. 32) for instructions on how to grant permissions.

Error	Scenario	Steps to resolve
Error: Logging is not enabled for the module. To enable it, please refer to the Upgrade section in the module documentation.	Activating addon module	This error arises because logging to the file is required for the upgrade, but it is not enabled on the WHMCS server. The upgrade procedure is not allowed without it. See "Logs" (p. 37) and enable text logs.
Error: Cannot find group XX at server YY. Please check server ID for service ID or empty/update custom field "GroupID" if the group was manually deleted.	Activating addon module	Group ID specified in the client service was not found due to some inconsistency with a customer tenant. To continue the upgrade: Open the client service with ID from the error. Clean up the custom fields: GroupID, Login, AdminID.
Cannot upgrade products and services. Error: Cannot find an infrastructure component with name "XX". Please update module setting "Storage" in product YY.	Activating addon module	Product inconsistency: Infrastructure component with the name "XX" no longer exists in Acronis Cyber Cloud. Open the issued product and select another storage in the module settings. Then, save the changes.
Cannot upgrade products and services. Error: The platform version of the server XX is earlier than the minimum supported version "8.0"	Activating addon module	The minimum required version of Acronis Cyber Cloud is 8.0 (see "Module upgrade from previous versions" (p. 32)). If you work with an earlier version, you will not be able to activate a new version of the module. We recommend that you proceed with the module upgrade only after the platform will be updated up to 8.0 at Acronis site.
Cannot upgrade products and services. Error: Cannot find a server with name "XX". Please update module setting "YY" in product ZZ.	Activating addon module	Product inconsistency: server defined in the product setting does not exist. Open the issued product and specify another server in the module settings. Then, save the changes.
Cannot turn on offering items from multiple editions at the same time	Order provisioning	Verify Configurable Options Group assigned to the product: ensure all of the offering items inside the group correspond to the edition and services from the template. Verify the client order and set 0 for the items that are not compatible with that template.
Cannot delete template because it is still used by the following products: ..	Removing template	You cannot delete a template that is assigned to existing products. You need to assign another template to these products or delete the product if it is no longer required.