Acronis

Acronis Cyber Cloud

Version 8.0

PARTNER'S GUIDE

Revision: 7/12/2019

Table of contents

1 About this document

This document is intended for partner administrators who want to use Acronis Cyber Cloud to provide services to their clients.

This document describes how to set up and manage the services available in Acronis Cyber Cloud.

2 About Acronis Cyber Cloud

Acronis Cyber Cloud is a cloud platform that enables service providers, resellers, and distributors to deliver data protection services to their partners and customers.

The services are provided at the partner level, down to the customer company level and the end-user level.

The services management is available through web applications called the **service consoles**. The tenant and user account management is available through a web application called the **management portal**.

The management portal enables administrators to:

- Monitor the service usage and access the service consoles
- Manage tenants
- Manage user accounts
- Configure services and quotas for tenants
- Manage storage
- Manage branding
- Generate reports about the service usage

3 Offering items and quota management

This section describes the following:

- What are services, offerings, and offering items?
- How are offering items enabled or disabled?
- What are the soft and hard quotas?
- When can the hard quota be exceeded?
- What is backup quota transformation?
- How does the offering item availability affect the installer availability in the backup console?

3.1.1 Services, offerings, and offering items

Services

The following services are available in Acronis Cyber Cloud:

- **Backup & Disaster Recovery**
- **File Sync & Share**
- **Cyber Infrastructure SPLA**
- **Notary**
- **Physical Data Shipping**

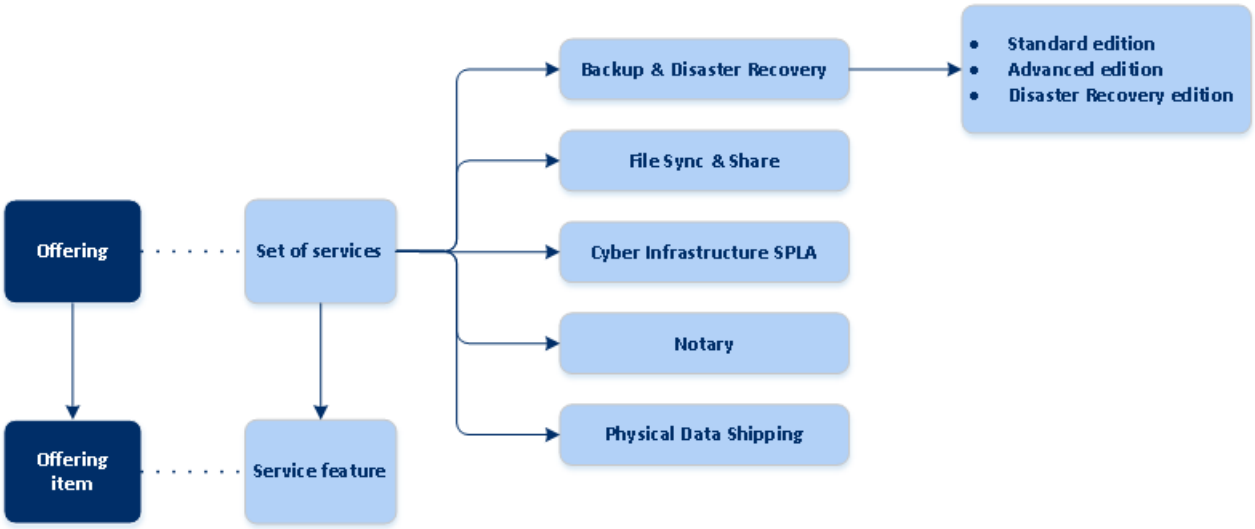
You can define which of these services will be available to your partners and customers by enabling or disabling them.

Offerings and offering items

Acronis Cyber Cloud enables you to customize the offering (the set of services and service features, called **offering items**) that you deliver to your customers and partners.

The **offering** defines which services and functionality will be available in the management portal and the service consoles to the partners, customers, and their end users. All functionality that is excluded from the offering will be hidden from them.

To further refine their offerings, you can define quotas for the specific offering items.



Backup service editions

The Backup service has three editions which determine the functionality that is provided to customers.

- **Standard** – provides backup and recovery functionality that covers small environment needs.
- **Advanced** – provides backup and recovery functionality designed for big environments. It is dedicated to protect advanced workloads such as Microsoft Exchange and Microsoft SQL cluster, and provides group management and plan management.
- **Disaster Recovery** – provides the disaster recovery functionality along with the advanced backup and recovery functionality. It is designed for companies that have high requirements for the Recovery Time Objective and needs in advanced backup and recovery functionality.

The edition allows you to differentiate the backup offerings for your partners and customers, and provide the backup functionality that meets their needs and budgets.

You can decide which of the editions will be available for your partner by enabling or disabling them while creating a partner. Each edition can be adjusted by configuring its offering items.

You can assign one edition per customer. Afterward, you can switch customers between the editions, on demand.

3.1.2 Enabling or disabling offering items

To learn how to enable or disable the offering items for a tenant, refer to "Creating a tenant (p. 17)".

The capability to disable the offering items and the result of these actions are listed in the table below.

Offering item	Disabling	Result
Backup storage	Can be disabled when the usage is equal to zero.	The cloud storage will become unavailable as a destination for backups within a customer tenant.

Local backup	Can be disabled when the usage is equal to zero.	The local storage will become unavailable as a destination for backups within a customer tenant.
Data sources (including Office 365 and G Suite)	Can be disabled when the usage is equal to zero.	The backup and recovery of data sources (including Office 365 and G Suite) will become unavailable within a customer tenant.
All Disaster Recovery offering items	Can be disabled when the usage is more than zero.	See the details in "Soft and hard quotas (p. 6)".
All Notary offering items	Can be disabled when the usage is equal to zero.	The Notary service will be unavailable within a customer tenant.
All File Sync & Share offering items	Offering items cannot be enabled or disabled separately.	The File Sync & Share service will be unavailable within a customer tenant.
All Physical Data Shipping offering items	Can be disabled when the usage is equal to zero.	The Physical Data Shipping service will be unavailable within a customer tenant.

For an offering item that cannot be disabled when its usage is more than zero, you can manually remove usage, and then disable the corresponding offering item.

3.1.3 Soft and hard quotas

Quotas enable you to limit a tenant's ability to use the service. To set the quotas, select the client on the **Clients** tab, select the service tab, and then click **Edit**.

When a quota is exceeded, a notification is sent to the user's email address. If you do not set a quota overage, the quota is considered "**soft.**" This means that restrictions on using the backup service are not applied.

When you specify the quota overage, then the quota is considered "**hard.**" An **overage** allows the user to exceed the quota by the specified value. When the overage is exceeded, restrictions on using the service are applied.

Example

Soft quota: You have set the quota for workstations equal to 20. When the number of the customer's protected workstations reaches 20, the customer will get a notification by email, but the backup service will be still available.

Hard quota: If you have set the quota for workstations equal to 20 and the overage is 5, then your customer will get the notification by email when the number of protected workstations reaches 20, and the backup service will be disabled when the number reaches 25.

Levels on which quotas can be defined

The quotas can be set on the levels listed in the table below.

Tenant/User	Soft quota (only quota)	Hard quota (quota and overage)
Partner	yes	no
Folder	yes	no
Customer	yes	yes
Unit	no	no
User	yes	yes

The soft quotas can be set on the partner and folder levels. On the unit level no quotas can be set. The hard quotas can be set on the customer and user levels.

The total amount of hard quotas that are set on the user level cannot exceed the related customer hard quota.

3.1.3.1 Backup quotas

You can specify the cloud storage quota, the quota for local backup, and the maximum number of machines/devices/websites a user is allowed to protect. The following quotas are available.

Quotas for devices

- **Workstations**
- **Servers**
- **Virtual machines**
- **Mobile devices**
- **Web hosting servers**
- **Websites**

A machine/device/website is considered protected as long as at least one backup plan is applied to it. A mobile device becomes protected after the first backup.

When the overage for a number of devices is exceeded, the user cannot apply a backup plan to more devices.

Quotas for cloud data sources

- **Office 365 seats**

  This quota is applied by the service provider to the entire company. The company can be allowed to protect **Mailboxes**, **OneDrive** files, or both. Company administrators can view the quota and the usage in the management portal, but cannot set the quota for a user.

- **Office 365 SharePoint Online**

  This quota is applied by the service provider to the entire company. This quota enables or disables the ability to protect SharePoint Online sites. If the quota is enabled, any number of SharePoint Online sites can be protected. Company administrators cannot view the quota in the management portal, but can view the amount of storage occupied by SharePoint Online backups in the usage reports.

- **G Suite seats**

  This quota is applied by the service provider to the entire company. The company can be allowed to protect **Gmail** mailboxes (including calendar and contacts), **Google Drive** files, or both.

Company administrators can view the quota and the usage in the management portal, but cannot set the quota for a user.

- **G Suite Shared drive**

  This quota is applied by the service provider to the entire company. This quota enables or disables the ability to protect G Suite Shared drives. If the quota is enabled, any number of Shared drives can be protected. Company administrators cannot view the quota in the management portal, but can view the amount of storage occupied by Shared drive backups in the usage reports.

An Office 365 seat is considered protected as long as at least one backup plan is applied to the user's mailbox or OneDrive. A G Suite seat is considered protected as long as at least one backup plan is applied to the user's mailbox or Google Drive.

When the overage for a number of seats is exceeded, a company administrator cannot apply a backup plan to more seats.

Quotas for storage

- **Local backup**

  The **Local backup** quota limits the total size of local backups that are created by using the cloud infrastructure. An overage cannot be set for this quota.

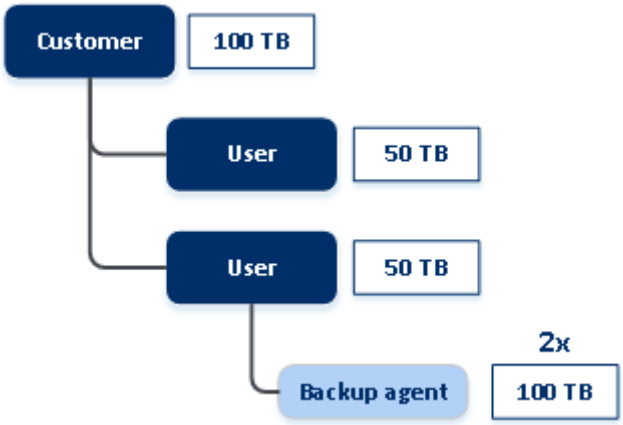
- **Cloud resources**

The **Cloud resources** quota combines the quota for backup storage and quotas for disaster recovery. The backup storage quota limits the total size of backups located in the cloud storage. When the backup storage quota overage is exceeded, backups fail.

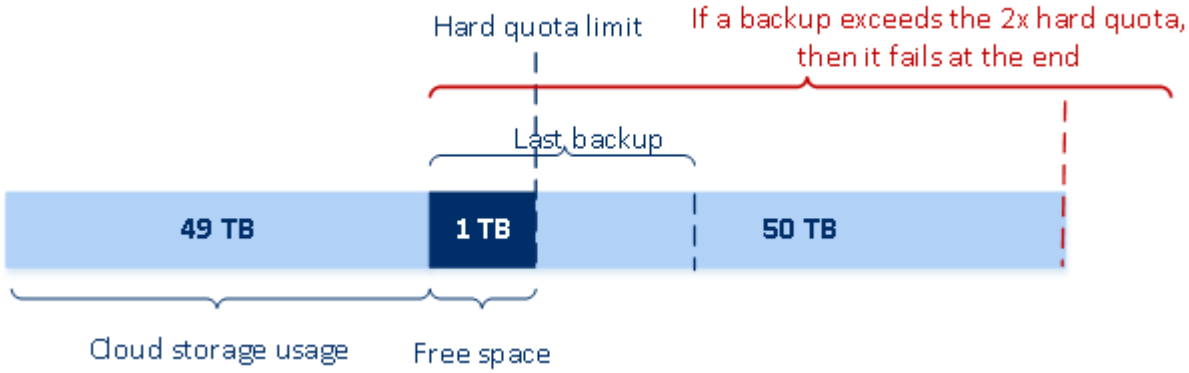
Exceeding the hard quota for backup storage

Regarding the backup storage, its hard quota can be exceeded to two times the defined hard quota. The backup agent certificate has the 2x technical quota that allows an agent to overcome the tenant's hard quota when it is not yet reached during a running backup. The next backup will not be possible if the tenant quota is exceeded. If the 2x multiplied value of the quota (in the certificate) is reached during backup creation, then the backup will fail.

Example: You have defined the cloud storage hard quota of 100 TB for a customer tenant which means that the total sum of hard quotas allocated to the tenant's users cannot exceed 100 TB. You decided to split the hard quota for the two users equally. This means that technically each user's agent has a 100 TB technical quota. But it does not mean that the agent can back up machines until all 100 TB are reached. It means only that if the hard quota is almost reached when the backup creation started, then the backup will be completed unless its size is too big that even the 2x hard quota is not enough.



On the scheme below, a user has 1 TB of free space, but the backup size is larger, for example, 3 TB. In this case, the backup will be successfully completed even though the hard quota limit of the cloud storage space is exceeded by 2 TB. If the backup size was 53 TB, then the backup creation would start but fail when the cloud storage limit (100 TB) is reached.



Backup quota transformation

In general, this is how acquiring a backup quota and offering item mapping to resource type works: the system compares the available offering items with the resource type, and then acquires the quota for the matched offering item.

There is also a capability to assign another offering item quota, even if it does not exactly match the resource type. This is called the **backup quota transformation**. If there is no matching offering item, the system tries to find a more expensive appropriate quota for the resource type (automatic backup quota transformation). If nothing appropriate is found, then you can manually assign the service quota to the resource type in the backup console.

Example

You want to back up a virtual machine (workstation, agent-based).

First, the system will check if there is an allocated **Virtual machines** quota. If it is not found, then the system automatically tries to acquire the **Workstations** quota. If that is also not found, the other quota will not be automatically acquired. If you have enough quota that is more expensive than the **Virtual machines** quota and it is applicable to a virtual machine, then you can log in to the backup console and assign the **Servers** quota manually.

3.1.3.2 Disaster Recovery quotas

Note *The Disaster Recovery offering items are available only in the Disaster Recovery edition.*

These quotas are applied by the service provider to the entire company. Company administrators can view the quotas and the usage in the management portal, but cannot set quotas for a user.

- **Disaster recovery storage**

  This storage is used by primary and recovery servers. If the overage for this quota is reached, it is not possible to create primary and recovery servers, or add/extend disks of the existing primary servers. If the overage for this quota is exceeded, it is not possible to initiate a failover or just start a stopped server. Running servers continue to run.
- **Compute points**

  This quota limits the CPU and RAM resources that are consumed by primary and recovery servers during a billing period. If the overage for this quota is reached, all primary and recovery servers are shut down. It is not possible to use these servers until the beginning of the next billing period. The default billing period is a full calendar month.

  When the quota is disabled, the servers cannot be used regardless of the billing period.
- **Public IP addresses**

  This quota limits the number of public IP addresses that can be assigned to the primary and recovery servers. If the overage for this quota is reached, it is not possible to enable public IP addresses for more servers. You can disallow a server to use a public IP address, by clearing the **Public IP address** check box in the server settings. After that, you can allow another server to use a public IP address, which usually will not be the same one.

  When the quota is disabled, all of the servers stop using public IP addresses, and thus become not reachable from the Internet.
- **Cloud servers**

  This quota limits the total number of primary and recovery servers. If the overage for this quota is reached, it is not possible to create primary or recovery servers.

  When the quota is disabled, the servers are visible in the backup console, but the only available operation is **Delete**.
- **Internet access**

  This quota enables or disables the Internet access from the primary and recovery servers.

  When the quota is disabled, the primary and recovery servers will not be able to establish connections to the Internet.

3.1.3.3 File Sync & Share quotas

You can define the following File Sync & Share quotas for a tenant:

- **Users**

  The quota defines a number of users that can access this service.
- **Cloud storage**

This is a cloud storage for storing users' files. The quota defines the allocated space for a tenant in the cloud storage.

3.1.3.4 Physical Data Shipping quotas

The Physical Data Shipping service quotas are consumed on a per-drive basis. You can save initial backups of multiple machines on one hard drive.

You can define the following Physical Data Shipping quotas for a tenant:

- **To the cloud**

  Allows sending an initial backup to the cloud data-center by using a hard disk drive. This quota defines the maximum amount of data on the hard disk drive to be transferred to the cloud data-center.

3.1.3.5 Notary quotas

You can define the following Notary quotas for a tenant:

- **Notary storage**

  The notary storage is the cloud storage where the notarized files, signed files, and files whose notarization or signing is in progress are stored. This quota defines the maximum space that can be occupied by these files.

  To decrease this quota usage, you can delete the already notarized or signed files from the notary storage.

- **Notarizations**

  This quota defines the maximum number of files that can be notarized by using the notary service. A file is considered notarized as soon as it is uploaded to the notary storage and its notarization status changes to In progress.

  If the same file is notarized multiple times, each notarization counts as a new one.

- **eSignatures**

  This quota defines the maximum number of files that can be signed by using the notary service. A file is considered signed as soon as it is sent for signature.

3.1.4 Agent installer dependency on offering items

Depending on the allowed offering items, the corresponding agent installer will be available in the **Add devices** section in the backup console. In the table below, you can see the agent installers and their availability in the backup console depending on the enabled offering items.

Enabled offering item / Agent installer	Servers	Workstations	Virtual machines	Office 365 seats	G Suite seats	Mobile devices	Web hosting servers	Websites
Workstations – Agent for Windows		+	+					+
Workstations – Agent for Mac OS		+	+					+

Servers – Agent for Windows	+		+				+	+
Servers – Agent for Linux	+		+				+	+
Agent for Hyper-V			+					
Agent for VMware			+					
Agent for Virtuozzo			+					
Agent for SQL	+		+					
Agent for Exchange	+		+					
Agent for Active Directory	+		+					
Agent for Office 365				+				
Agent for G Suite					+			
Full installer for Windows	+	+	+				+	+
Mobile (iOS and Android)						+		

3.2 User accounts and tenants

There are two user account types: administrator accounts and user accounts.

- **Administrators** have access to the management portal. They have the administrator role in all services.
- **Users** do not have access to the management portal. Their access to the services and their roles in the services are defined by an administrator.

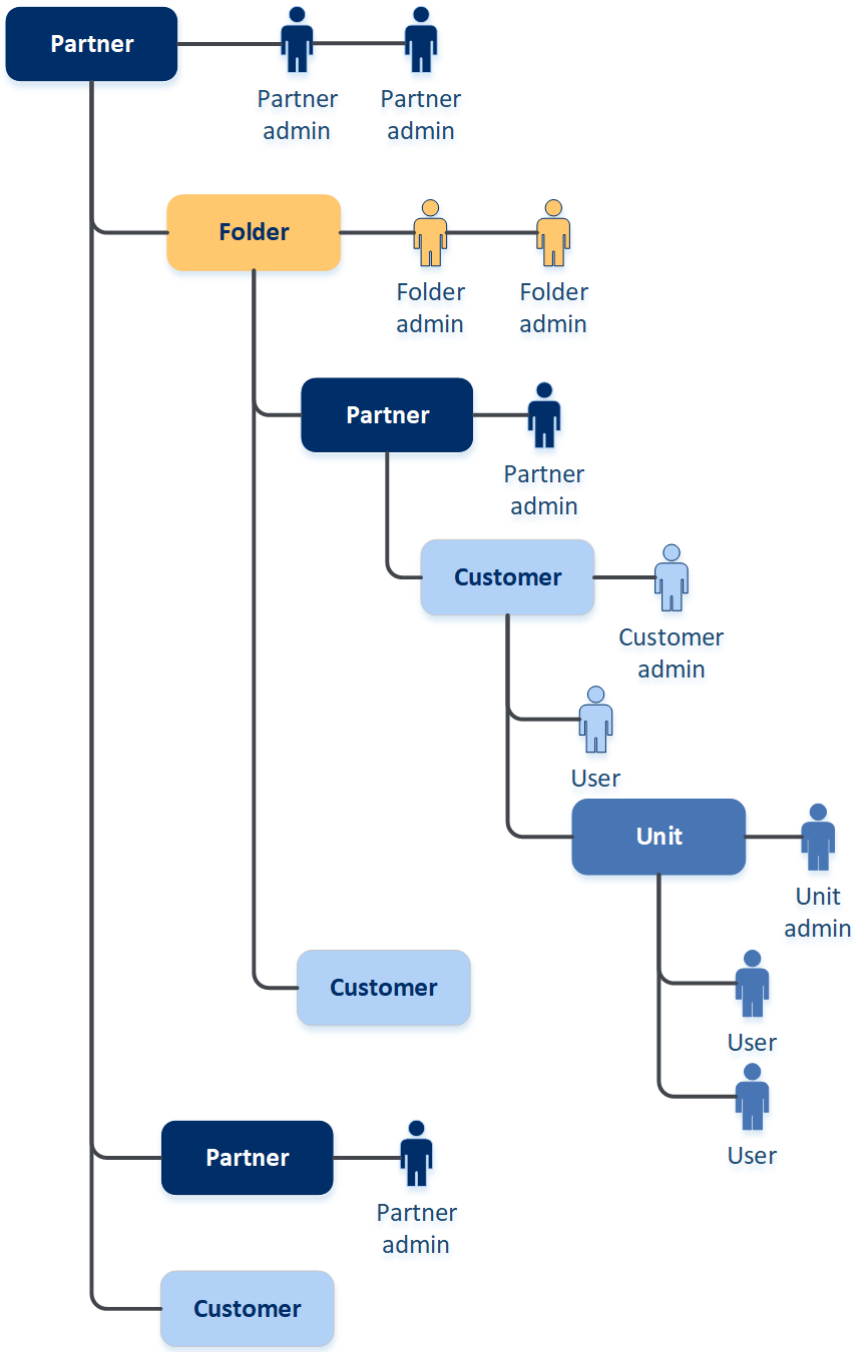
Each account belongs to a tenant. A tenant is a part of the management portal resources (such as user accounts and child tenants) and service offerings (enabled services and offering items within them) dedicated to partner or a customer. The tenant hierarchy is supposed to match the client/vendor relationships between the service users and providers.

- A tenant type of **Partner** typically corresponds to service providers that resell the services.
- A tenant type of **Folder** is a supplementary tenant that is typically used by partner administrators to group partners and customers to configure separate offerings and/or different branding.
- A tenant type of **Customer** typically corresponds to organizations that use the services.
- A tenant type of **Unit** typically corresponds to units or departments within the organization.

An administrator can create and manage tenants, administrator accounts, and user accounts on or below their level in the hierarchy.

Administrators at the customer level and higher can limit access to their tenant for higher-level administrators (p. 35).

The following diagram illustrates an example hierarchy of the partner, folder, customer, and unit tenants.



The following table summarizes operations that can be performed by the administrators and users.

Operation	Users	Customer and unit administrators	Partner and folder administrators
Create tenants	No	Yes	Yes
Create accounts	No	Yes	Yes
Download and install the software	Yes	Yes	No*
Manage services	Yes	Yes	Yes

Operation	Users	Customer and unit administrators	Partner and folder administrators
Create reports about the service usage	No	Yes	Yes
Configure branding	No	No	Yes

*A partner administrator who needs to perform these operations can create a customer administrator or user account for themselves.

3.3 Supported web browsers

The web interface supports the following web browsers:

- Google Chrome 29 or later
- Mozilla Firefox 23 or later
- Opera 16 or later
- Windows Internet Explorer 11 or later
- Microsoft Edge 25 or later
- Safari 8 or later running in the macOS and iOS operating systems

In other web browsers (including Safari browsers running in other operating systems), the user interface might be displayed incorrectly or some functions may be unavailable.

4 Using the management portal

The following steps will guide you through the basic use of the management portal.

4.1 Activating the administrator account

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 the administrator account. Remember the login that is shown on the account activation page.
- **A link to the login page**. The login and password are the same as in the previous step.

4.2 Accessing the management portal

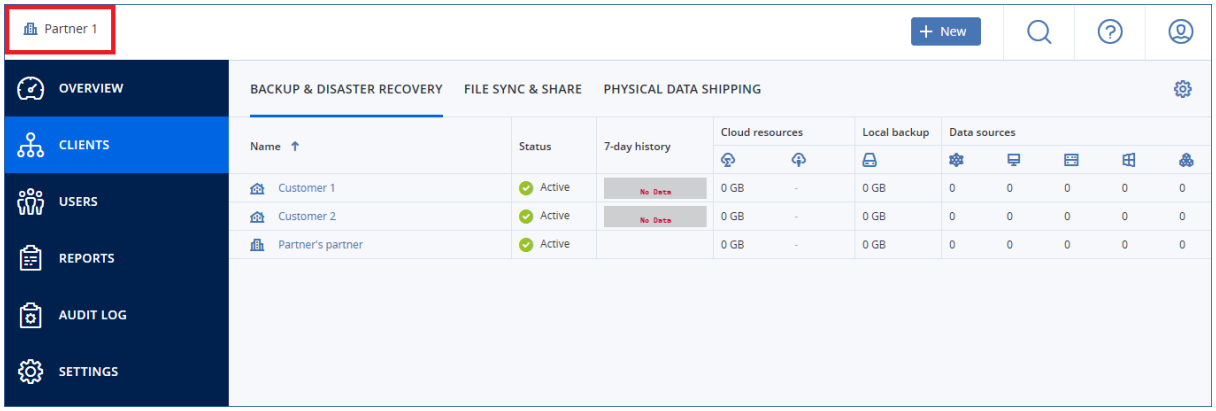
1. Go to the service login page. The login page address was included in the activation email message.
2. Type the login, and then click **Continue**.
3. Type the password, and then click **Sign in**.
4. Click **Management Portal**.

Some services include the capability to switch to the management portal from the service console.

4.3 Navigation in the management portal

When using the management portal, at any given time you are operating within a tenant. This is indicated in the top-left corner.

By default, the top-most hierarchy level available to you is selected. Click the tenant name to drill down the hierarchy. To navigate back to an upper level, click its name in the top-left corner.



All parts of the user interface display and affect only the tenant in which you are currently operating. For example:

- The **Clients** tab displays only the tenants that are direct children of the tenant in which you are currently operating.
- The **Users** tab displays only the user accounts that exist in the tenant in which you are currently operating.
- By using the **New** button, you can create a tenant or a new user account only in the tenant in which you are currently operating.

4.4 Accessing the services

Overview tab

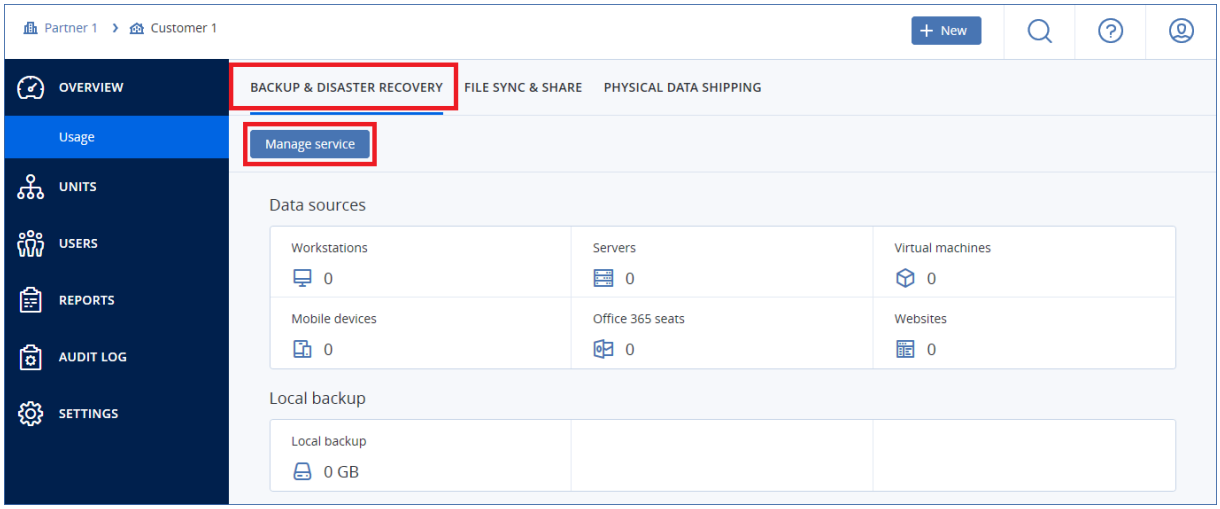
The **Overview** > **Usage** section provides an overview of the service usage and enables you to access the services within the tenant in which you are operating.

To manage a service for a tenant by using the Overview tab

1. Navigate to the tenant (p. 14) for which you want to manage a service, and then click **Overview** > **Usage**.

   Note that some services can be managed at the partner tenant and at the customer tenant levels, while other services can be managed only at the customer tenant level.
2. Click the name of the service that you want to manage, and then click **Manage service** or **Configure service**.

For information about using the services, refer to the user guides that are available in the service consoles.

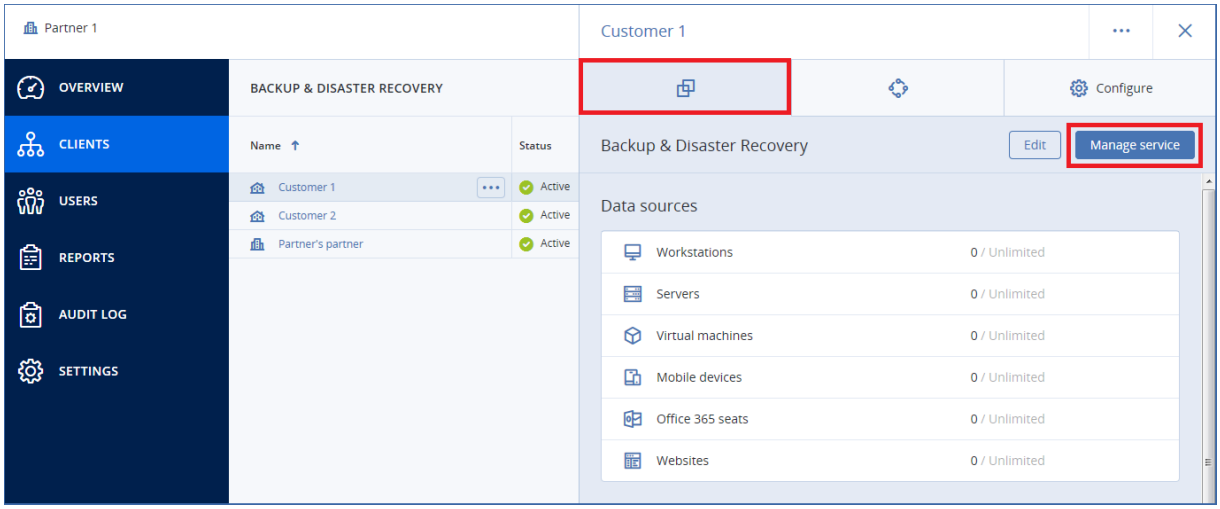


Clients tab

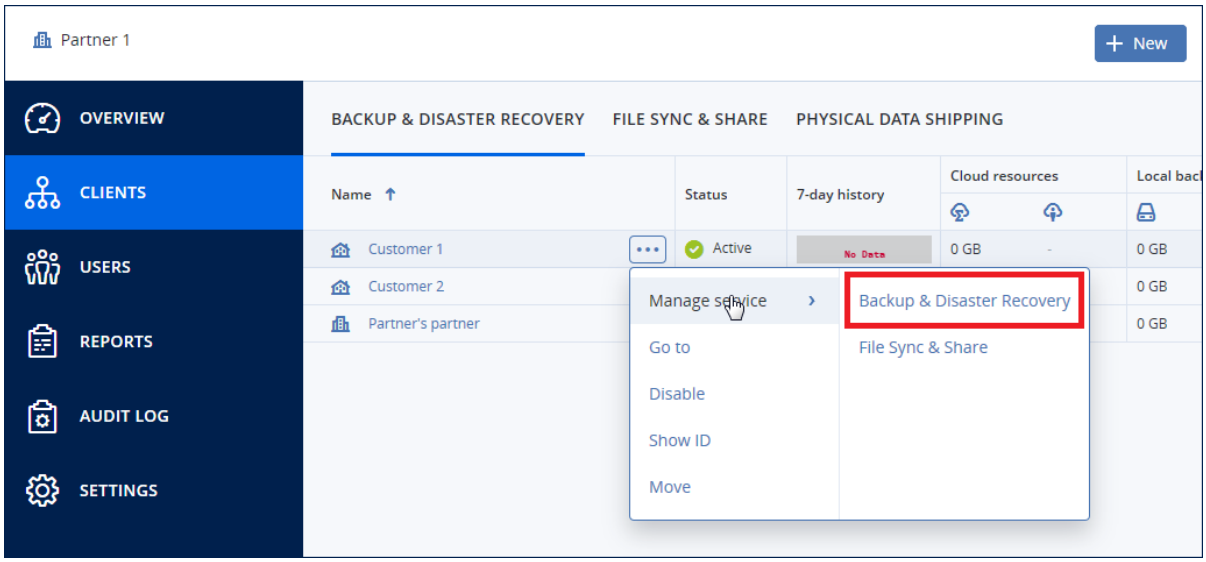
The **Clients** tab displays the child tenants of the tenant in which you are operating and enables you to access the services within them.

To manage a service for a tenant by using the Clients tab

1. Do one of the following:
   - Click **Clients**, select the tenant for which you want to manage a service, click the name or icon of the service that you want to manage, and then click **Manage service** or **Configure service**.



- Click **Clients**, click the ellipsis icon next to the name of the tenant for which you want to manage a service, click **Manage service**, and then select the service that you want to manage.



Note that some services can be managed at the partner tenant and at the customer tenant levels, while other services can be managed only at the customer tenant level.

For information about using the services, refer to the user guides that are available in the service consoles.

4.5 Creating a tenant

A **Partner** tenant is normally created for each partner that signs the partnership agreement.

A **Folder** tenant is normally created to group partners and customers to configure separate offerings and/or different branding.

A **Customer** tenant is normally created for each organization that signs up for a service.

You may want to create a new **Unit** tenant within a customer tenant when expanding the service to a new organizational unit.

To create a tenant

1. Log in to the management portal.
2. Navigate to the tenant (p. 14) in which you want to create a tenant.
3. In the top-right corner, click **New**, and then click one of the following, depending on the type of the tenant that you want to create:
   - **Customer**
   - **Partner**
   - **Folder**
   - **Unit**

   The available types depend on the parent tenant type.
4. In **Name**, specify a name for the new tenant.
5. [Only when creating a customer tenant] In **Mode**, select whether the tenant is using services in the trial mode or in the production mode. Monthly service usage reports do not include usage data for trial-mode tenants.

Important *If you switch the mode from trial to production in the middle of a month, the entire month will be included in the monthly service usage report. For this reason, we recommend that you switch the mode on the first day of a month. The mode is automatically switched to production when a tenant remains in the trial mode for one full month.*

6. [Optional] In **Language**, change the default language of notifications, reports, and the software that will be used within this tenant.
7. Do one of the following:
   - To finish the tenant creation, click **Save and close**. In this case, all services will be enabled for the tenant. The tenant will not have an administrator until you create one.
   - To configure services for the tenant and to create a tenant administrator, click **Next**.
8. [Optional, not applicable to a unit tenant] Disable the switches for the services that you want to disable for the tenant. Disabled services will be hidden from the users within the tenant and its child tenants.

   [If you create a partner] For the Backup & Disaster Recovery service, select which editions will be available.

   [If you create a customer] For the the Backup & Disaster Recovery service, select one of the editions that will be available.

   When ready, click **Next**.
9. [Optional, not applicable to a unit tenant] Configure the offering items for the tenant:
   a. Within each service, clear the check boxes for the offering items that you want to disable. The functionality that corresponds to the disabled offering items will be unavailable for the users within the tenant and its child tenants.
   b. Some services enable you to select storages that will be available to the new tenant. Storages are grouped by locations. You can select from the list of locations and storages that are available to your tenant.
      - When creating a parent/folder tenant, you can select multiple locations and storages for each service.
      - When creating a customer tenant, you must select one location, and then select one storage per service within this location. The storages assigned to the customer can be changed at a later time, but only before the customer starts using them.

      For more information about storages, refer to "Managing locations and storage" (p. 25).
   c. To specify the quota for an item, click on the **Unlimited** link next to the offering item. These quotas are "soft". If any of these values are exceeded, an email notification is sent to the tenant administrators and the administrators of the parent tenant. Restrictions on using the services are not applied.
   d. [Only when creating a customer tenant] Specify the quota overages. An overage allows a customer tenant to exceed the quota by the specified value. When the overage is exceeded, restrictions on using the corresponding service are applied.
10. Do one of the following:
    - To create a tenant administrator, click **Next**, and then follow the steps described in "Creating a user account" (p. 19), starting from step 4. If you change your mind, you can click **Skip and close** to cancel creating an administrator.
    - To create a tenant without an administrator, click **Save and close**. You can add administrators to the tenant later.

The newly created tenant appears on the **Clients** tab.

If you want to edit the tenant settings or specify the contact information, select the tenant on the **Clients** tab, and then click the pencil icon in the section that you want to edit.

4.6 Creating a user account

You may want to create additional accounts in the following cases:

- Partner/folder administrator accounts — to share the services management duties with other people.
- Customer/unit administrator accounts — to delegate the service management to other people whose access permissions will be strictly limited to the corresponding customer/unit.
- User accounts within the customer or a unit tenant — to enable the users to access only a subset of the services.

Please be aware that existing accounts cannot be moved between tenants. First, you need to create a tenant, and then populate it with accounts.

To create a user account

1. Log in to the management portal.
2. Navigate to the tenant (p. 14) in which you want to create a user account.
3. In the top-right corner, click **New** > **User**.
4. Specify the following contact information for the account:
   - **Email address**
   - [Optional] **First name**
   - [Optional] **Last name**
   - [Optional] To specify a login that is different from the specified email address, clear the **Use email address as login** check box, and then specify the login.

     Important *Each account must have a unique login.*
5. [Optional] In **Language**, change the default language of notifications, reports, and the software that will be used for this account.
6. [Not available when creating an account in a partner/folder tenant] Select the services to which the user will have access and the roles in each service.

   Available services depend on the services that are enabled for the tenant in which the user account is created.
   - If you select the **Company administrator** check box, the user will have access to the management portal and the administrator role in all services that are currently enabled for the tenant. The user will also have the administrator role in all services that will be enabled for the tenant in the future.
   - If you select the **Unit administrator** check box, the user will have access to the management portal, but may or not have the service administrator role, depending on the service.
   - Otherwise, the user will have the roles that you select in the services that you select.
7. Click **Create**.

The newly created user account appears on the **Users** tab.

If you want to edit the user settings or specify notification settings and quotas (not available for partner/folder administrators) for the user, select the user on the **Users** tab, and then click the pencil icon in the section that you want to edit.

4.7 Setting up two-factor authentication

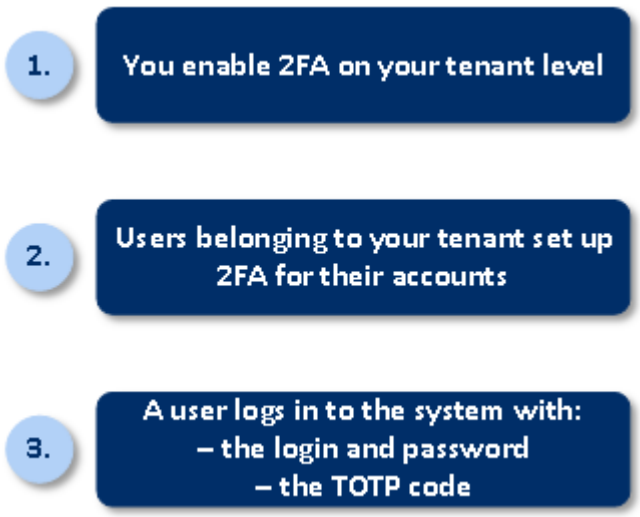
Two-factor authentication (2FA) is a type of multi-factor authentication that checks a user identity by using a combination of two different factors:

- Something that a user knows (PIN or password)
- Something that a user has (token)
- Something that a user is (biometrics)

Two-factor authentication provides extra protection from unauthorized access to your account.

The platform supports **Time-based One-Time Password (TOTP)** authentication. If the TOTP authentication is enabled in the system, users must enter their traditional password and the one-time TOTP code in order to access the system. In other words, a user provides the password (the first factor) and the TOTP code (the second factor). The TOTP code is generated in the authentication application on a user second-factor device on the basis of the current time and the secret (QR-code or alphanumeric code) provided by the platform.

How it works



1. You enable two-factor authentication on your organization level.
2. All of your organization users must install an authentication application on their second-factor devices (mobile phones, laptops, desktops, or tablets). This application will be used for generating one-time TOTP codes. The recommended authenticators:
   - Google Authenticator

     iOS app version (https://itunes.apple.com/sg/app/google-authenticator/id388497605?mt=8)

     Android version (https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en_SG)
   - Microsoft Authenticator

     iOS app version (https://app.adjust.com/n094ls?campaign=appstore_ios&fallback=https://itunes.apple.com/app/microsoft-authenticator/id983156458)

     Android version (https://app.adjust.com/n094ls?campaign=appstore_android&fallback=https://play.google.com/store/apps/details?id=com.azure.authenticator)

Important *Users must ensure that the time on the device where the authentication application is installed is set correctly and reflects the actual current time.*

3. Your organization users must re-log in to the system.
4. After entering their login and password, they will be prompted to set up two-factor authentication for their user account.
5. They must scan the QR code by using their authentication application. If the QR code cannot be scanned, they can use the TOTP secret shown below the QR code and add it manually in the authentication application.

Important *It is highly recommended to save it (print the QR-code, write down the TOTP secret, use the application that supports backing up codes in a cloud). You will need the TOTP secret to reset two-factor authentication in case of lost second-factor device.*

6. The one-time TOTP code will be generated in the authentication application. It is automatically regenerated every 30 seconds.
7. The users must enter the TOTP code on the "Set up two-factor authentication" screen after entering their password.
8. As a result, two-factor authentication for the users will be set up.

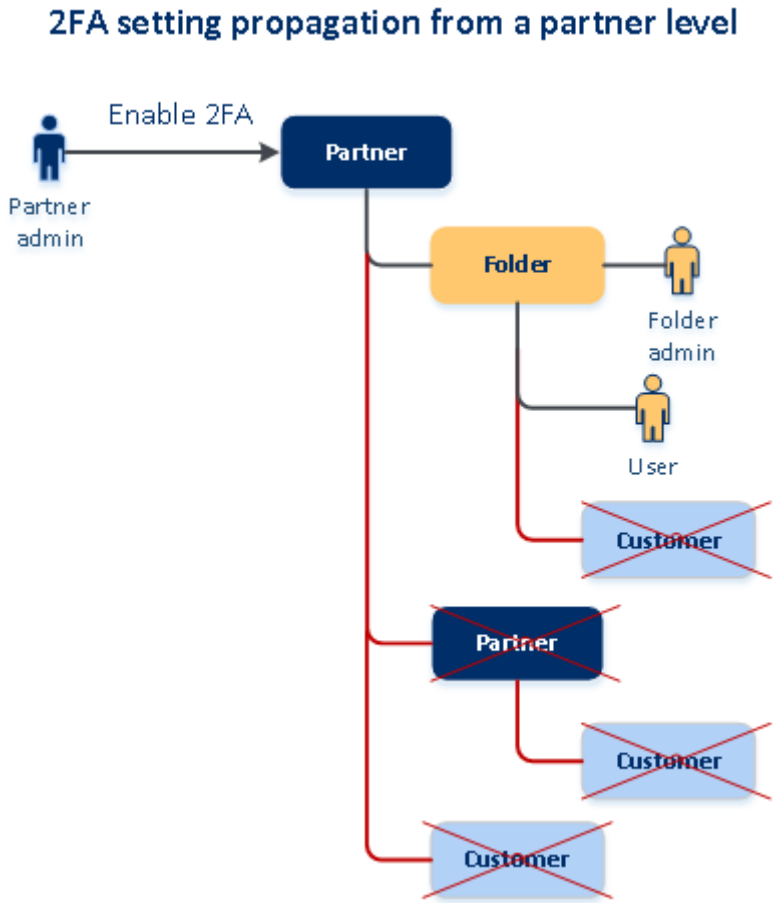
Now when users log in to the system, they will be asked to provide the login and password, and the one-time TOTP code generated in the authentication application. Users can mark the browser as trusted when they log in to the system, then the TOTP code will not be requested on subsequent logins via this browser.

4.7.1 Two-factor setup propagation across tenant levels

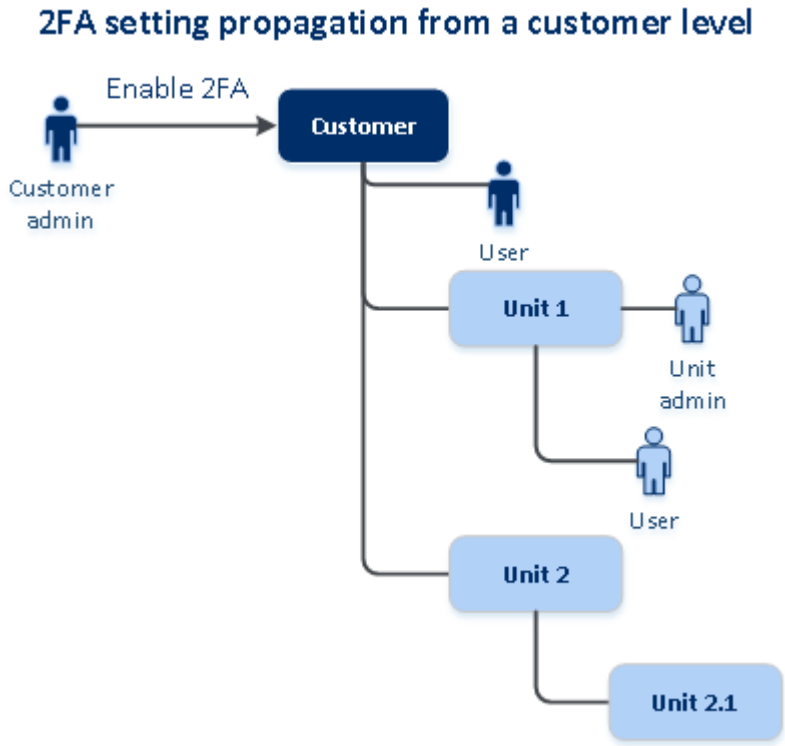
Two-factor authentication is set up on the **organization** level. You can set up two-factor authentication only for your own organization.

The two-factor authentication settings are propagated across tenant levels as follows:

- Folders auto-inherit the two-factor authentication settings from their partner organization. On the scheme below, the red lines mean that the propagation of two-factor authentication settings is not possible.



- Units auto-inherit the two-factor authentication settings from their customer organization.



Note
1. You can view the two-factor authentication settings of your child organizations, but you cannot configure them.
2. It is not possible to set up two-factor authentication on the folder or unit level.
3. You can configure the two-factor authentication setting even if your parent organization does not have this setting enabled.

4.7.2 Setting up two-factor authentication for your tenant

To enable two-factor authentication for your tenant

1. In the Management Portal, go to **Settings** > **Security**.
2. To enable two-factor authentication, turn on the slider. To confirm, click **Enable**.

The progress bar shows how many users have set up two-factor authentication for their accounts. As a result, two-factor authentication is enabled for your organization. Now all users of the organization must set up two-factor authentication in their accounts. After that, the users will be prompted to enter the login and password, and the TOTP code to log in to the system.

On the **Users** tab, the **2FA status** column will appear. You can track which users have set up two-factor authentication for their accounts.

To disable two-factor authentication for your tenant

1. In the Management Portal, go to **Settings** > **Security**.
2. To disable two-factor authentication, turn off the slider. To confirm, click **Disable**.
3. Enter the TOTP code generated in your authentication application on the mobile device.

As a result, two-factor authentication is disabled for your organization. All users will log in to the system by using only their login and password. On the **Users** tab, the **2FA status** column will be hidden.

4.7.3 Managing two-factor configuration for users

You can monitor two-factor authentication settings for all your users and reset the settings on the **Users** tab in the management portal.

Monitoring

In the Management Portal on the **Users** tab, you can see a list of all your organization users. The **2FA status** reflects if the two-factor configuration is set up for a user.

To reset two-factor authentication for a user

1. In the Management Portal on the **Users** tab, find a user for whom you want to change the settings, and then click the ellipsis icon.
2. Click **Reset two-factor authentication**.
3. Enter the TOTP code generated in the authentication application on your second-factor device and click **Reset**.

As a result, the user will be able to set up two-factor authentication again.

To reset the trusted browsers for a user

1. In the Management Portal on the **Users** tab, find a user for whom you want to change the settings, and then click the ellipsis icon.
2. Click **Reset all trusted browsers**.
3. Enter the TOTP code generated in the authentication application on your second-factor device, and then click **Reset**.

The user for whom you have reset all trusted browsers will have to provide the TOTP code on the next login.

To disable two-factor authentication for a user

You may need to disable two-factor authentication for a user while the rest users of the account will use two-factor authentication. This is needed in case this user is used to access the API.

Important *Do not switch normal users to service users in order to disable two-factor authentication, otherwise the users may not be able to log in.*

1. In the Management Portal on the **Users** tab, find a user for whom you want to change the settings, and then click the ellipsis icon.
2. Click **Mark as service account**. As a result, a user gets a special two-factor authentication status called **Service account.**
3. [If at least one user within a tenant has configured two-factor authentication] Enter the TOTP code generated in the authentication application on your second-factor device to confirm disabling.

To enable two-factor authentication for a user

You may need to enable two-factor authentication for a particular user for whom you have disabled it previously.

1. In the Management Portal on the **Users** tab, find a user for whom you want to change the settings, and then click the ellipsis icon.
2. Click **Mark as regular account**. As a result, a user will have to set up two-factor authentication or provide the TOTP code when entering the system.

4.7.4 Resetting two-factor authentication in case of lost second-factor device

To reset access to your account in case of lost second-factor device, follow one of the suggested approaches:

- Restore your TOTP secret (QR-code or alphanumeric code) from a backup.

  Use another second-factor device and add the saved TOTP secret in the authentication application installed on this device.
- Ask your administrator to reset the two-factor authentication settings for you (p. 24).

4.8 Managing locations and storage

The **Settings** > **Locations** section shows the cloud storages and disaster recovery infrastructures that you can use to provide the **Backup & Disaster Recovery** and the **File Sync & Share** services to your partners and customers.

Storages configured for other services will be shown on the **Locations** section in the future releases.

Locations

A location is a container that enables you to conveniently group the cloud storages and disaster recovery infrastructures. It can represent anything of your choice, like a specific data center or a geographical location of your infrastructure components.

You can create any number of locations and populate them with backup storages, disaster recovery infrastructures, and **File Sync & Share** storages. A location can contain multiple cloud storages but only one disaster recovery infrastructure.

For information about operations with storages, refer to "Managing storage" (p. 26).

Choosing locations and storages for partners and customers

When creating a partner/folder tenant (p. 17), you can select multiple locations and multiple storages per service within them that will be available in the new tenant.

When creating a customer tenant (p. 17), you must select one location, and then select one storage per service within this location. The storage assigned to the customer can be changed at a later time, but only before the customer starts using it.

The information about the storages that are assigned to a customer tenant is shown on the tenant details panel when the tenant is selected on the **Clients** tab. Information about the storage space usage is not updated in real time. Please allow up to 24 hours for the information to be updated.

Operations with locations

To create a new location, click **Add location**, and then specify the location name.

To move a storage or a disaster recovery infrastructure to another location, select the storage or the infrastructure, click the pencil icon in the **Location** field, and then select the target location.

To rename a location, click the ellipsis icon next to the location name, click **Rename**, and then specify the new location name.

To delete a location, click the ellipsis icon next to the location name, click **Delete**, and then confirm your decision. Only empty locations can be deleted.

4.8.1 Managing storage

Adding new storages

- **Backup & Disaster Recovery** service:
  - By default, the backup storages are located in Acronis data centers.
  - If the **Partner-owned backup storage** offering item is enabled for a partner tenant by an upper-level administrator, the partner administrators can organize the storage in the partner's own data center, by using the Acronis Cyber Infrastructure software. Click **Add backup storage** on the **Locations** section to find information about organizing a backup storage in your own data center.
  - If the **Partner-owned disaster recovery infrastructure** offering item is enabled for a partner tenant by an upper-level administrator, the partner administrators can organize a disaster recovery infrastructure in the partner's own data center. For information about adding a disaster recovery infrastructure, contact Acronis technical support at https://www.acronis.com/support.
- For information about adding storages that will be used by other services, contact Acronis technical support at https://www.acronis.com/support.

Deleting storages

You can delete storages that were added by you or your child tenants.

If the storage is assigned to any customer tenants, you must disable the service that uses the storage for all customer tenants, before deleting the storage.

To delete a storage

1. Log in to the management portal.
2. Navigate to the tenant (p. 14) in which the storage was added.
3. Click **Settings** > **Locations**.
4. Select the storage that you want to delete.
5. On the storage properties panel, click the ellipsis icon, and then click **Delete storage**.
6. Confirm your decision.

4.9 Configuring branding

The **Settings** > **Branding** section enables partner administrators to customize the user interface of the management portal and the **Backup & Disaster Recovery** service to remove any association with Acronis or the higher-level partners.

Branding can be configured on the partner and the folder levels. The branding is applied to all direct and indirect child partners/folders and customers of the tenant where the branding is configured.

The capability to configure branding for all services will be available in the future releases. Some services provide separate branding capability. For more information, refer to the user guides that are available in the service consoles.

Branding items

Appearance

- **Service name**. This name is used in all email messages that are sent by the management portal (account activation messages, business notification email messages), on the **Welcome** screen after the first login, and as the management portal browser tab name.
- **Logo**. The logo is displayed in the management portal and the services. Click the logo to upload an image file.
- **Color scheme**. The color scheme defines the combination of colors that is used for all user interface elements. Click the scheme, and then choose one of the predefined schemes that best fits your needs.

  Tip *Click* ***Preview scheme in a new tab*** *to preview what the interface will look like to your child tenants. The branding will not be applied until you click* ***Done*** *on the* ***Choose color scheme*** *panel.*

Documentation and support

- **Home URL**. This page is opened when a user clicks the company name on the **About** panel.
- **Support URL**. This page is opened when a user clicks the **Contact support** link on the **About** panel or in an email message that is sent by the management portal.
- **Support phone**. This phone number is shown on the **About** panel.
- **Knowledge base URL**. This page is opened when a user clicks the **Knowledge base** link in an error message.
- **Management portal administrator's guide**. This page is opened when a user clicks the question mark icon in the top-right corner of the management portal user interface, and then clicks **About** > **Administrator guide**.
- **Management portal administrator's help**. This page is opened when a user clicks the question mark icon in the top-right corner of the management portal user interface, and then clicks **Help**.

Legal

- **End-user License agreement (EULA) URL**. This page is opened when a user clicks the **End-user license agreement** link on the **About** panel or on the **Welcome** screen after the first login.
- **Platform terms URL**. This page is opened when a partner administrator clicks the **Platform terms** link on the **About** panel or the **Welcome** screen after the first login.
- **Privacy statement URL**. This page is opened when a user clicks the **Privacy statement** link on the **Welcome** screen after the first login.

Mobile apps

- **App Store**. This page is opened when the user clicks **Add** > **iOS** in the **Backup & Disaster Recovery** service.
- **Google Play**. This page is opened when the user clicks **Add** > **Android** in the **Backup & Disaster Recovery** service.

Email server settings

You can specify a custom email server that will be used to send email notifications from the management portal and the services. To specify a custom email server, click **Customize**, and then specify the following settings:

- In **From**, enter the name that will be shown in the **From** field of the email notifications.
- In **SMTP**, enter the name of the outgoing mail server (SMTP).
- In **Port**, enter the port of the outgoing mail server. By default, the port is set to 25.

- In **Encryption**, select whether to use SSL or TLS encryption. Select **None** to disable encryption.
- In **User name** and **Password**, specify the credentials of an account that will be used to send messages.

Configuring branding

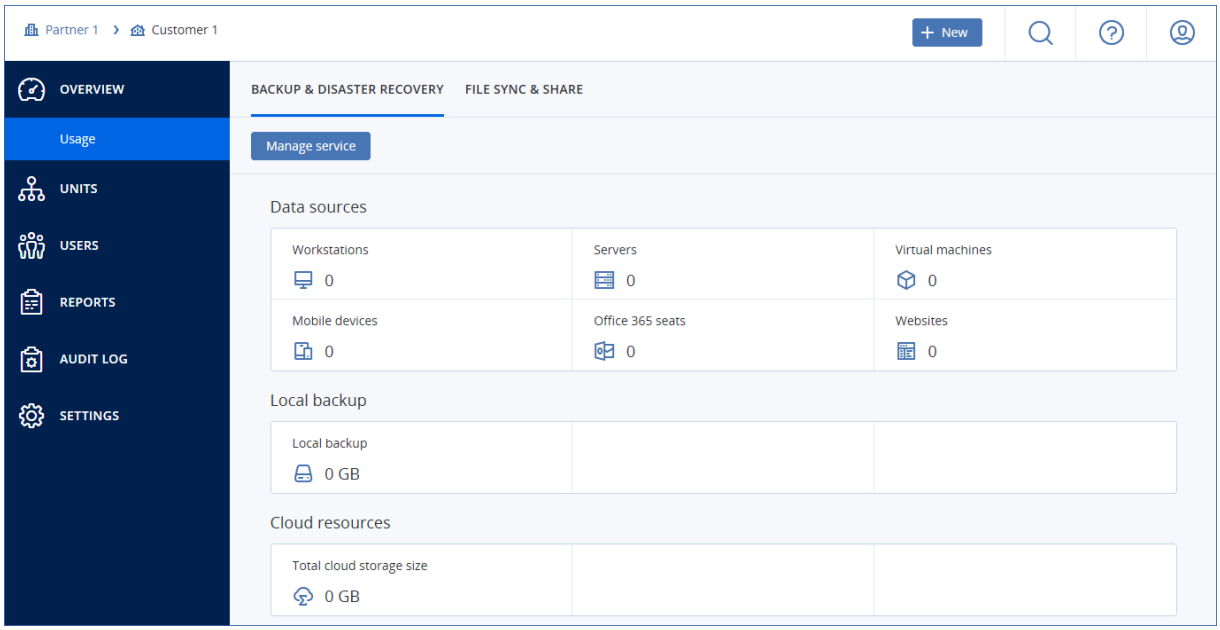
1. Log in to the management portal.
2. Navigate to the tenant (p. 14) in which you want to configure branding.
3. Click **Settings** > **Branding**.
4. Click **Enable branding**.
5. Do one of the following:
   - Configure the branding items described above.
   - Click **White label** to clear all branding items, except for **Service name**, **End-user License agreement (EULA) URL**, **Management portal administrator's guide**, **Management portal administrator's help**, and **Email server settings**.
   - Click **Restore to defaults** to reset all branding items to their default values.

4.10 Monitoring

To access information about services usage and operations, click **Overview**.

4.10.1 Usage

The **Usage** tab provides an overview of the service usage and enables you to access the services within the tenant in which you are operating.



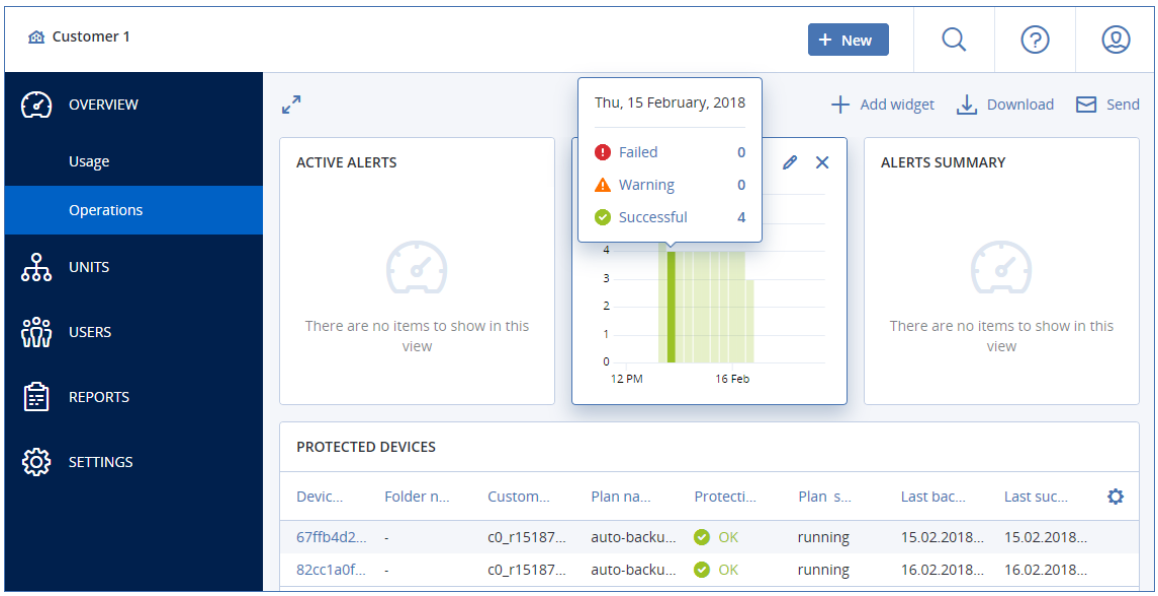
4.10.2 Operations

The **Operations** dashboard provides a number of customizable widgets that give an overview of operations related to the backup service. Widgets for other services will be available in future releases.

By default, the data is displayed for the tenant in which you are operating (p. 14). You can change the displayed tenant individually for each widget by editing it. Aggregated information about the direct child customer tenants of the selected tenant is also shown, including those that are located in folders. The dashboard does *not* display information about child partners and their child tenants; you must drill-down into the specific partner to see its dashboard. However, if you convert a child partner tenant to a folder tenant (p. 35), the information about this tenant's child customers will appear on the parent tenant's dashboard.

The widgets are updated in real time. The widgets have clickable elements that enable you to investigate and troubleshoot issues. You can download the current state of the dashboard in the .pdf or/and .xlsx format, or send it via email to any address, including external recipients.

You can choose from a variety of widgets, presented as tables, bar charts, and lists. You can add multiple widgets of the same type for different tenants or with different filters.



To rearrange the widgets on the dashboard

Drag and drop the widgets by clicking on their names.

To edit a widget

Click the pencil icon next to the widget name. Editing a widget enables you to rename it, change the period of time, select the tenant for which the data is displayed, and set filters.

To add a widget

Click **Add widget**, and then do one of the following:

- Click the widget that you want to add. The widget will be added with the default settings.
- To edit the widget before adding it, click the gear icon when the widget is selected. After editing the widget, click **Done**.

To remove a widget

Click the X sign next to the widget name.

4.11 Reporting

To create reports about services usage and operations, click **Reports**.

4.11.1 Usage

Usage reports provide historical data about use of the services.

Report type

You can select one of the following report types:

- **Current usage**

  The report contains the current service usage metrics.

  The usage metrics are calculated within each of the child tenants' billing periods. If the tenants included in the report have different billing periods, the parent tenant's usage may differ from the sum of the child tenants' usages.
- **Current usage distribution**

  This report is available only for partner tenants that are managed by an external provisioning system. This report is useful when the billing periods of child tenants do not match the billing period of the parent tenant. The report contains the service usage metrics for child tenants calculated within the current billing period of the parent tenant. The parent tenant's usage is guaranteed to be equal to the sum of the child tenants' usages.
- **Summary for period**

  The report contains the service usage metrics for the end of the specified period, and the difference between the metrics in the beginning and at the end of the specified period.
- **Day-by-day for period**

  The report contains the service usage metrics and their changes for each day of the specified period.

Report scope

You can select the scope of the report from the following values:

- **Direct customers and partners**

  The report will include the service usage metrics only for the immediate child tenants of the tenant in which you are operating.
- **All customers and partners**

  The report will include the service usage metrics for all child tenants of the tenant in which you are operating.
- **All customers, partners, and users**

  The report will include the service usage metrics for all child tenants of the tenant in which you are operating and for all users within the tenants.

Scheduled reports

A scheduled report covers service usage metrics for the last full calendar month. The reports are generated at 23:59:59 UTC on the first day of a month and sent on the second day of that month. The reports are sent to all administrators of your tenant who have the **Scheduled usage reports** check box selected in the user settings.

To enable or disable a scheduled report

1. Log in to the management portal.
2. Ensure that you operate in the top-most tenant available to you.
3. Click **Reports** > **Usage**.
4. Click **Scheduled**.

5. Select or clear the **Send a monthly summary** report check box.
6. In **Level of detail**, select the report scope as described above.

Custom reports

This type of report can be generated on demand and cannot be scheduled. The report will be sent to your email address.

To generate a custom report

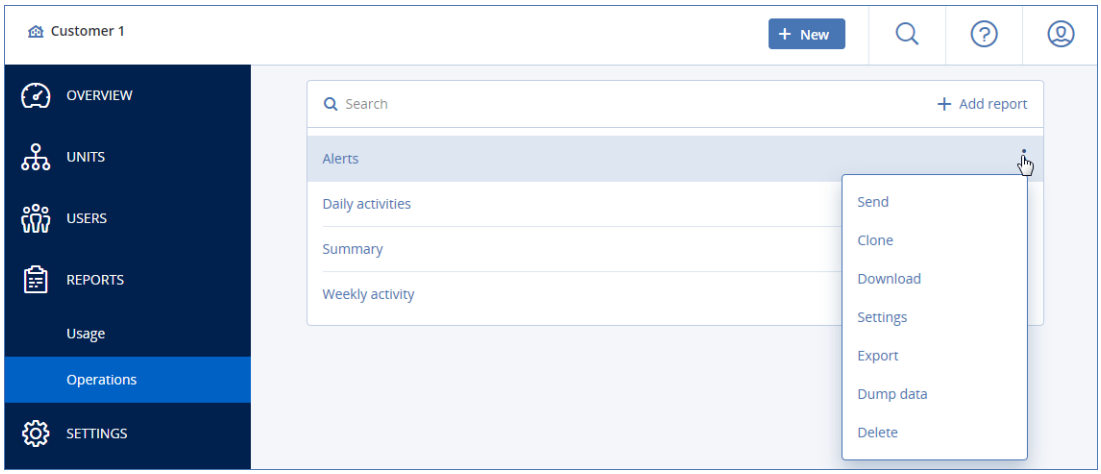
1. Log in to the management portal.
2. Navigate to the tenant (p. 14) for which you want to create a report.
3. Click **Reports** > **Usage**.
4. Select the **Custom** tab.
5. In **Type**, select the report type as described above.
6. [Not available for the **Current usage** report type] In **Period**, select the reporting period:
   - **Current calendar month**
   - **Previous calendar month**
   - **Custom**
7. [Not available for the **Current usage** report type] If you want to specify a custom reporting period, select the start and the end dates. Otherwise, skip this step.
8. In **Level of detail**, select the report scope as described above.
9. To generate the report, click **Generate and send**.

4.11.2 Operations

A report about operations can include any set of the **Operations** dashboard widgets (p. 28). By default, all of the widgets show the summary information for the tenant in which you are operating. You can change this individually for each widget by editing it, or for all widgets in the report settings. All of the widgets show the parameters for the same time range. You can change this range in the report settings.

To view a report, click its name.

To access operations with a report, click the vertical ellipsis icon on the report line. The same operations are available from within the report.



You can use predefined reports or create a custom report.

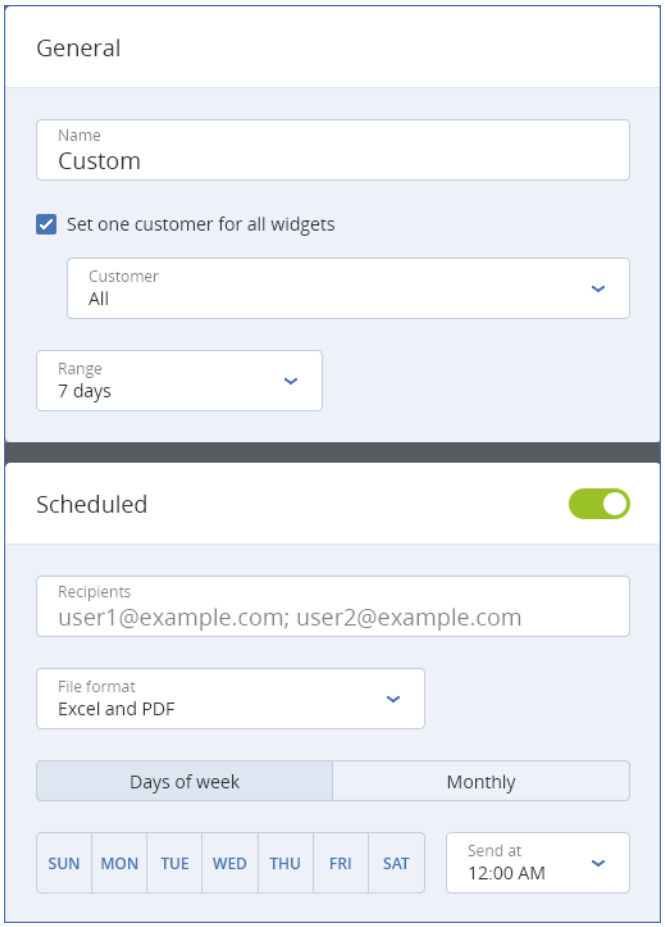
Adding a report

1. Click **Add report**.
2. Do one of the following:
   - To add a predefined report, click its name.
   - To add a custom report, click **Custom**, click the report name (the names assigned by default look like **Custom(1)**), and then add widgets to the report.
3. [Optional] Drag and drop the widgets to rearrange them.
4. [Optional] Edit the report as described below.

Editing a report

To edit a report, click its name, and then click **Settings**. When editing a report, you can:

- Rename the report
- Change the displayed tenant for all widgets included in the report
- Change the time range for all widgets included in the report
- Schedule sending the report via email in the .pdf or/and .xlsx format.



Scheduling a report

1. Click the report name, and then click **Settings**.
2. Enable the **Scheduled** switch.
3. Specify the recipients' email addresses.
4. Select the report format: .pdf, .xlsx, or both.
5. Select the days and the time when the report will be sent.

6. Click **Save** in the upper-right corner.

Exporting and importing the report structure

You can export and import the report structure (the set of widgets and the report settings) to a .json file. This may be useful for copying the report structure from one tenant to another tenant.

To export the report structure, click the report name, click the vertical ellipsis icon in the top-right corner, and then click **Export**.

To import the report structure, click **Add report**, and then click **Import**.

Dumping the report data

You can send a dump of the report data in a .csv file via email. The dump includes all of the report data (without filtering) for a custom time range.

The software generates the data dump on the fly. If you specify a long period of time, this action may take a long time.

To dump the report data

1. Click the report name.
2. Click the vertical ellipsis icon in the top-right corner, and then click **Dump data**.
3. Specify the recipients' email addresses.
4. In **Time range**, specify the time range.
5. Click **Send**.

4.12 Audit log

To view the audit log, click **Audit log**.

The audit log provides a chronological record of the following events:

- Operations performed by users in the management portal
- System messages about reached quotas and quota usage

The log shows events in the tenant in which you are currently operating and its child tenants. You can click an event to view more information about it.

The log is cleaned up on a daily basis. The events are removed after 180 days.

Audit log fields

For each event, the log shows:

- **Event**

  Short description of the event. For example, **Tenant was created**, **Tenant was deleted**, **User was created**, **User was deleted**, **Quota was reached**.
- **Severity**

  Can be one of the following:
  - **Error**

    Indicates an error.
  - **Warning**

    Indicates a potentially negative action. For example, **Tenant was deleted**, **User was deleted**, **Quota was reached**.

  - **Notice**

    Indicates an event that might need attention. For example, **Tenant was updated**, **User was updated**.
  - **Informational**

    Indicates a neutral informative change or action. For example, **Tenant was created**, **User was created**, **Quota was updated**.
- **Date**

  The date and time when the event occurred.
- **Object name**

  The object with which the operation was performed. For example, the object of the **User was updated** event is the user whose properties were changed. For events related to a quota, the quota is the object.
- **Tenant**

  The name of the tenant that the object belongs to.
- **Initiator**

  The login of the user who initiated the event. For system messages and events initiated by upper-level administrators, the initiator is shown as **System**.
- **Initiator's tenant**

  The name of the tenant that the initiator belongs to. For system messages and events initiated by upper-level administrators, this field is empty.
- **Method**

  Shows whether the event was initiated via the web interface or via API.
- **IP**

  The IP address of the machine from which the event was initiated.

Filtering and search

You can filter the events by description, severity, or date. You can also search the events by object, unit, initiator, and initiator's unit.

5 Advanced scenarios

5.1 Moving a tenant to another tenant

The management portal enables you to move a tenant from one parent tenant to another parent tenant. This may be useful if you want to transfer a customer from one partner to another partner, or if you created a folder tenant to organize your clients and want to move some of them to the newly created folder tenant.

Restrictions

- A partner/folder tenant can be moved only to a partner/folder tenant.
- A customer tenant can be moved only to a partner/folder tenant.
- A tenant cannot be moved to its child tenant.
- A unit tenant cannot be moved.

- A tenant can be moved only if the target parent tenant has the same or a larger set of services and offering items as the original parent tenant.
- When moving a customer tenant, all storages assigned to the customer tenant in the original parent tenant must exist in the target parent tenant. This is required because the customer service-related data cannot be moved from one storage to another storage.

How to move a tenant

1. Log in to the management portal.
2. On the **Clients** tab, select the target tenant to which you want to move a tenant.
3. On the tenant properties panel, click the vertical ellipsis icon, and then click **View ID**.
4. Copy the text string shown in the **Internal ID** field, and then click **Cancel**.
5. On the **Clients** tab, select the tenant which you want to move.
6. On the tenant properties panel, click the vertical ellipsis icon, and then click **Move**.
7. Paste the internal identifier of the target tenant, and then click **Move**.

5.2 Converting a partner tenant to a folder tenant and vice versa

The management portal enables you to convert a partner tenant to a folder tenant.

This may be useful if you used a partner tenant for grouping purposes and now want to organize your tenant infrastructure properly. This is also useful if you want the operational dashboard (p. 28) to include aggregated information about the tenant.

You can also convert a folder tenant to a partner tenant.

Note *The conversion is a safe operation and does not affect the users within the tenant and any service-related data.*

To convert a tenant

1. Log in to the management portal.
2. On the **Clients** tab, select the tenant that you want to convert.
3. Do one of the following:
   - Click the ellipsis icon next to the tenant name.
   - Select the tenant, and then click the ellipsis icon on the tenant properties panel.
4. Click **Convert to folder** or **Convert to partner**.
5. Confirm your decision.

5.3 Limiting access to the web interface

Administrators can limit access to the web interface by specifying a list of IP addresses from which the members of a tenant are allowed to log in.

This restriction also applies to accessing the management portal via API.

This restriction applies only at the level where it is set. It is *not* applied to the members of the child tenants.

To limit access to the web interface

1. Log in to the management portal.

2. Navigate to the tenant (p. 14) in which you want to limit the access.
3. Click **Settings** > **Security**.
4. Select the **Enable logon control** check box.
5. In **Allowed IP addresses**, specify the allowed IP addresses.

   You can enter any of the following parameters, separated by a semicolon:

   - IP addresses, for example: 192.0.2.0
   - IP ranges, for example: 192.0.2.0-192.0.2.255
   - Subnets, for example: 192.0.2.0/24
6. Click **Save**.

5.4 Limiting access to your tenant

Administrators at the customer level and higher can limit access to their tenants for higher-level administrators.

If access to the tenant is limited, the parent tenant administrators can only modify the tenant properties. They do not see the accounts and child tenants at all.

To prevent higher-level administrators from accessing your tenant

1. Log in to the management portal.
2. Click **Settings** > **Security**.
3. Clear the **Allow administrators from parent tenants to manage this tenant** check box.
4. Click **Save**.

5.5 Integration with third-party systems

Acronis Cyber Cloud enables service providers to configure integration with a variety of third-party Professional Services Automations (PSA) and Remote Monitoring and Management (RMM) systems.

To configure integration with a third-party system

1. Log in to the management portal.
2. Click **Settings** > **Integration**.
3. Click the name of the system with which you want to enable the integration.
4. Follow the on-screen instructions.

More information about integration with third-party systems is available in the integration references section on the Acronis website.