

Management Portal

Version 8.0

Table of contents

1	About this document	3
2	About the management portal	3
2.1	Accounts and units.....	3
2.2	Quota management.....	4
2.2.1	Viewing quotas for your organization	5
2.2.2	Defining quotas for your users	7
2.3	Supported web browsers.....	9
3	Step-by-step instructions	9
3.1	Activating an administrator account	9
3.2	Accessing the management portal and the services	10
3.3	Navigation in the management portal	10
3.4	Creating a unit	10
3.5	Creating a user account	11
3.6	Setting up two-factor authentication	12
3.6.1	Two-factor setup propagation across tenant levels	13
3.6.2	Setting up two-factor authentication for your tenant	14
3.6.3	Managing two-factor configuration for users.....	15
3.6.4	Resetting two-factor authentication in case of lost second-factor device	16
4	Monitoring	16
4.1	Usage	16
4.2	Operations	16
5	Reporting	17
5.1	Usage	17
5.2	Operations	19
6	Audit log.....	21
7	Advanced scenarios	22
7.1	Limiting access to the web interface	22
7.2	Limiting access to your company.....	22

1 About this document

This document is intended for administrators who want to use the management portal.

2 About the management portal

The management portal is a web interface to the cloud platform that provides data protection services.

While each service has its own web interface, called the service console, the management portal enables administrators to control services usage, create user accounts and units, generate reports, and more.

2.1 Accounts and units

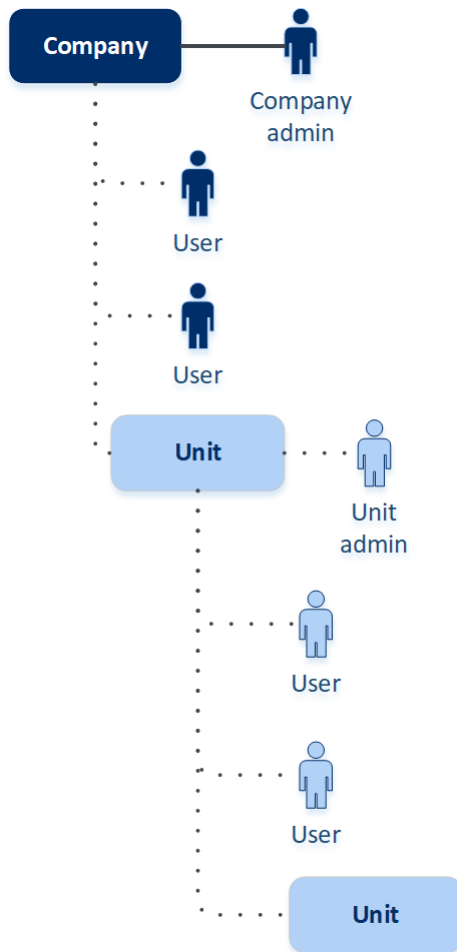
There are two user account types: administrator accounts and user accounts.

- **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.

Administrators can create units, which typically correspond to units or departments of the organization. Each account exists either on the company level or in a unit.

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

The following diagram illustrates three hierarchy levels – the company and two units. Optional units and accounts are shown by a dotted line.



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

Operation	Users	Administrators
Create units	No	Yes
Create accounts	No	Yes
Download and install the software	Yes	Yes
Use services	Yes	Yes
Create reports about the service usage	No	Yes

2.2 Quota management

Quotas limit a tenant's ability to use the service.

In the management portal, you can view the service quotas that were allocated to your organization by your service provider but you cannot manage them.

You can manage the service quotas for your users.

2.2.1 Viewing quotas for your organization

In the management portal, go to **Overview > Usage**. You will see a dashboard showing the allocated quotas for your organization. The quotas for each service are shown on a separate tab.

2.2.1.1 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.

2.2.1.2 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.

2.2.1.3 File Sync & Share quotas

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.

- **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.

2.2.1.4 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.

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.

- **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.

2.2.1.5 Notary quotas

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.

- **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.

2.2.2 Defining quotas for your users

Quotas enable you to limit a user's ability to use the service. To set the quotas for a user, select the user on the **Users** tab, and then click the pencil icon in the **Quotas** section.

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 user's protected workstations reaches 20, the user 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 the user 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.

2.2.2.1 Backup quotas

You can specify the backup storage quota 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** (Linux-based physical or virtual servers running Plesk or cPanel control panels)
- **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, a user cannot apply a backup plan to more devices.

Quota for storage

- **Backup storage**

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.

2.2.2.2 File Sync & Share quotas

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

- **Personal storage space**

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

2.2.2.3 Notary quotas

You can define the following Notary quotas for a user:

- **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.

2.3 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.

3 Step-by-step instructions

The following steps will guide you through the basic use of the management portal. They describe how to:

- Activate your administrator account
- Access the management portal and the services
- Create a unit
- Create a user account


3.1 Activating an administrator account

After signing up for a service, 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.

3.2 Accessing the management portal and the services

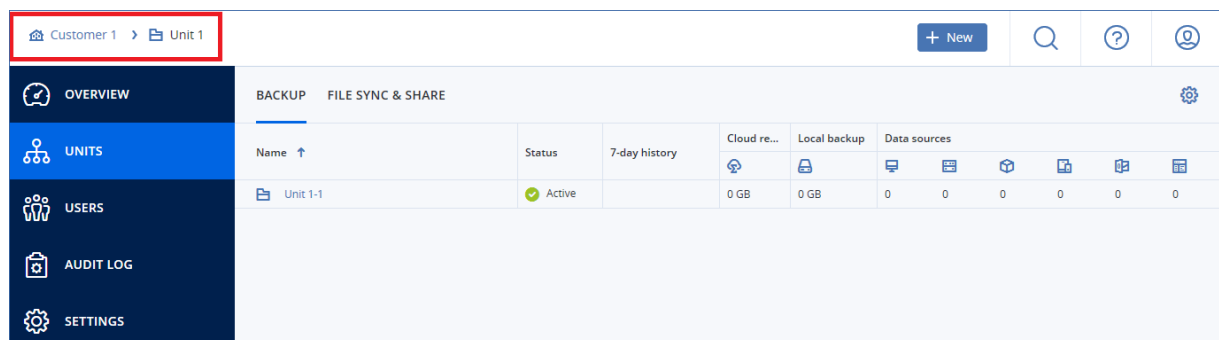
1. Go to the login page. The login page address was included in the activation email message.
2. Type the login, and then click **Continue**.
3. Type the password, and then click **Sign in**.
4. Do one of the following:
 - To log in to the management portal, click **Management Portal**.
 - To log in to a service, click the name of the service.

To switch between the management portal and the service consoles, click the  icon in the top-right corner, and then select **Management portal** or the service that you want to go to.

3.3 Navigation in the management portal

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

By default, the top-most hierarchy level available to you is selected. Click the unit 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 company or a unit in which you are currently operating. For example:

- By using the **New** button, you can create a unit or a user account only in this company or unit.
- The **Units** tab displays only the units that are direct children of this company or unit.
- The **Users** tab displays only the user accounts that exist in this company or unit.

3.4 Creating a unit

Skip this step if you do not want to organize accounts into units.

If you are planning to create units later, please be aware that existing accounts cannot be moved between units or between the company and units. First, you need to create a unit, and then populate it with accounts.

To create a unit

1. Log in to the management portal.

2. Navigate to the unit in which you want to create a new unit.
3. In the top-right corner, click **New > Unit**.
4. In **Name**, specify a name for the new unit.
5. [Optional] In **Language**, change the default language of notifications, reports, and the software that will be used within this unit.
6. Do one of the following:
 - To create a unit administrator, click **Next**, and then follow the steps described in "Creating a user account" (p. 11), starting from step 4.
 - To create a unit without an administrator, click **Save and close**. You can add administrators and users to the unit later.

The newly created unit appears on the **Units** tab.

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

3.5 Creating a user account

Skip this step if you do not want to create additional user accounts.

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

- Company administrator accounts — to share the management duties with other people.
- Unit administrator accounts — to delegate the management to other people whose access permissions will be limited to the corresponding units.
- User accounts — to enable the users to access only a subset of the services.

To create a user account

1. Log in to the management portal.
2. Navigate to the unit in which you want to create a new user account.
3. In the top-right corner, click **New > User**.
4. Specify the following 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. Select the services to which the user will have access and the roles in each service.
 - If you select the **Company administrator** check box, the user will have access to the management portal and the administrator role in all services.
 - 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 for the user, select the user on the **Users** tab, and then click the pencil icon in the section that you want to edit.

3.6 Setting up two-factor authentication

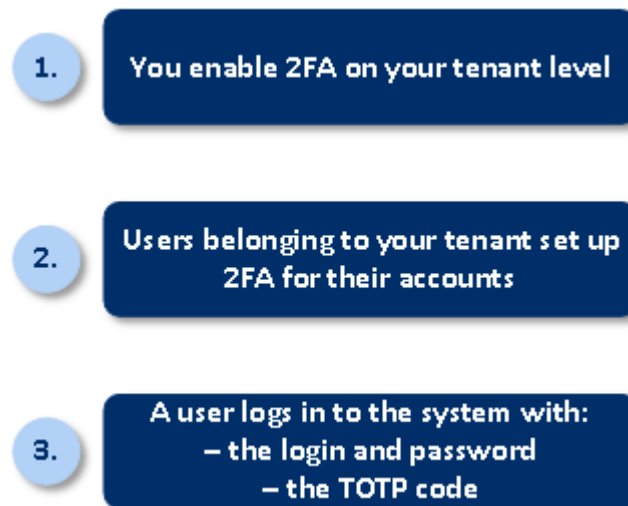
Two-factor authentication (2FA) is a type of multi-factor authentication that checks a user identity by using a combination of two different factors:

- 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 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 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 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.

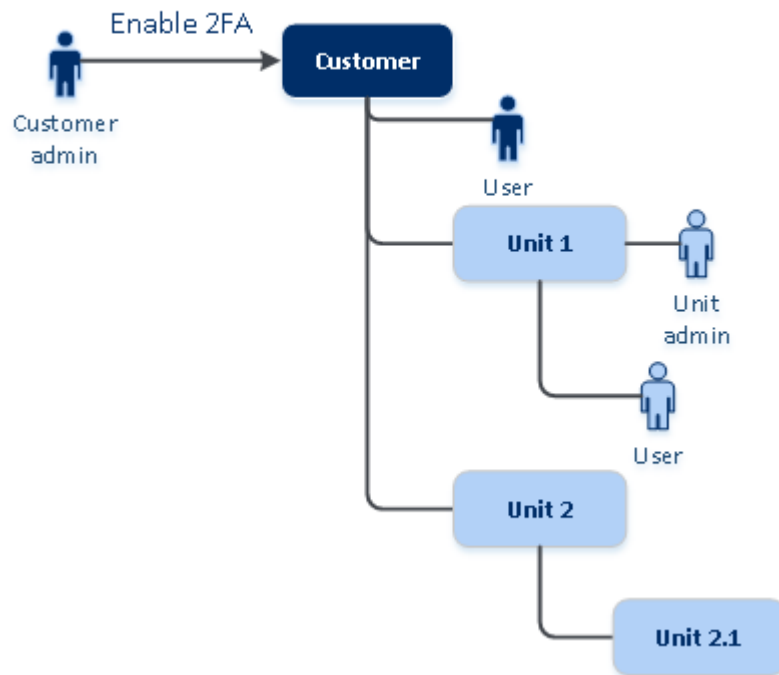
3.6.1 Two-factor setup propagation across tenant levels

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

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

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

2FA setting propagation from a customer level



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 unit level.
-

3.6.2 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.

3.6.3 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.

3.6.4 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:

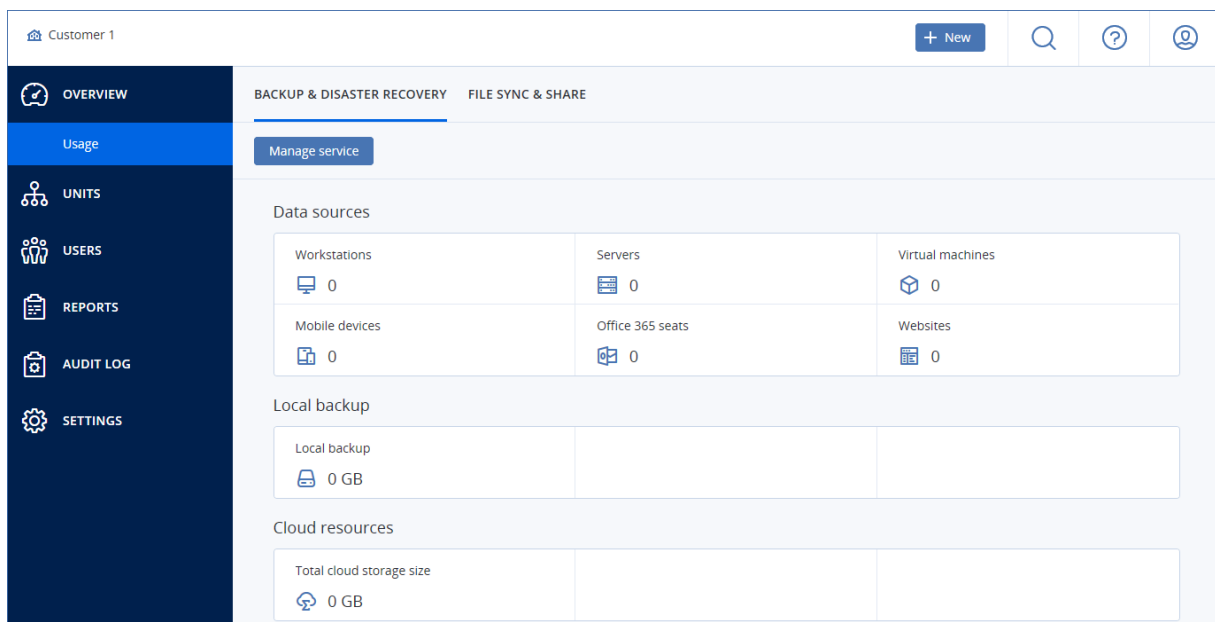
- Restore your TOTP secret (QR-code or alphanumeric code) from a backup.
Use another second-factor device and add the saved TOTP secret in the authentication application installed on this device.
- Ask your administrator to reset the two-factor authentication settings for you (p. 15).

4 Monitoring

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

4.1 Usage

The **Usage** tab provides an overview of the services usage (including the quotas, if any) and enables you to access the service consoles.



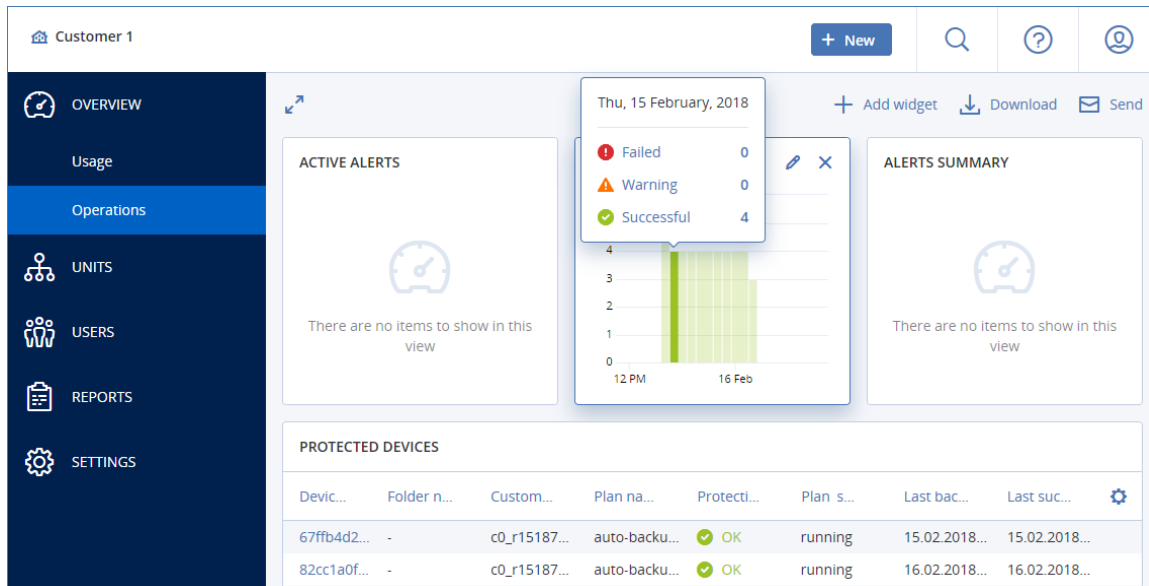
4.2 Operations

The **Operations** dashboard is available only to company administrators when operating on the company level.

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.

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 or send it via email in the .pdf or/and .xlsx format.

You can choose from a variety of widgets, presented as tables, bar charts, and lists. You can add multiple widgets of the same type 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 time range, 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.

5 Reporting

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

5.1 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.
- **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 units of the company or unit in which you are operating.
- **All customers and partners**
The report will include the service usage metrics for all child units of the company or unit in which you are operating.
- **All customers, partners, and users**
The report will include the service usage metrics for all child units of the company or unit in which you are operating, and for all users within the units.

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 company or unit 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 company or top-most unit 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

A custom report is 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 unit (p. 10) for which you want to create a report.
3. Click **Reports > Usage**.
4. Click **Custom**.
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**.

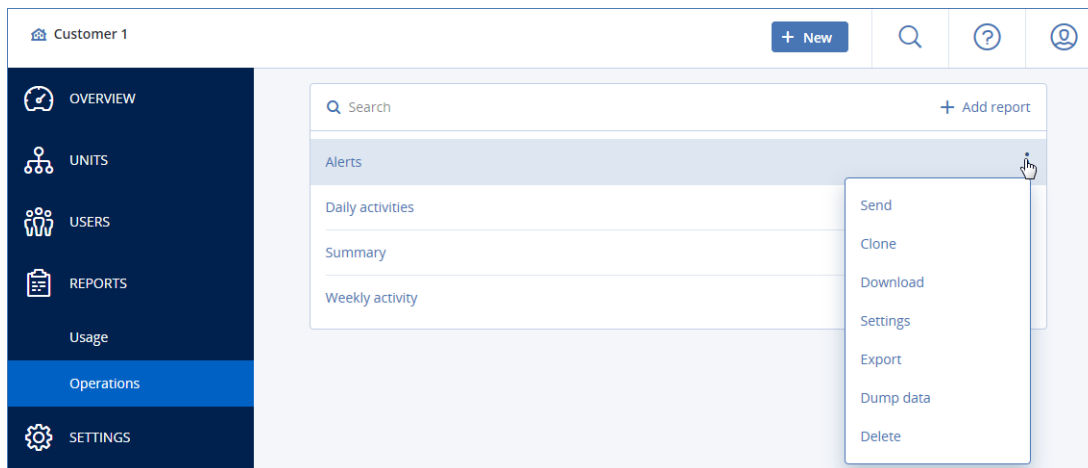
5.2 Operations

The **Operations** reports are available only to company administrators when operating on the company level.

A report about operations can include any set of the **Operations** dashboard widgets (p. 16). All of the widgets show the summary information for the entire company. 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 time range for all widgets included in the report
- Schedule sending the report via email in the .pdf or/and .xlsx format

The screenshot displays a configuration window for scheduling a report. It is divided into two main sections: 'General' and 'Scheduled'. In the 'General' section, the 'Name' field contains 'Alerts' and the 'Range' is set to '7 days'. The 'Scheduled' section features a green toggle switch that is turned on. Below the toggle, the 'Recipients' field contains 'user1@example.com; user2@example.com'. The 'File format' dropdown is set to 'Excel and PDF'. There are two tabs for scheduling: 'Days of week' and 'Monthly', with 'Monthly' currently selected. Under the 'Monthly' tab, there is a row of buttons for the days of the week: SUN, MON, TUE, WED, THU, FRI, and SAT. To the right of these buttons is a 'Send at' dropdown menu set to '12:00 AM'.

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.

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**.

6 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 organization or unit in which you are currently operating and its child units. 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 unit that the object belongs to. For example, the tenant of the **User was updated** event is the unit where the user is located. The tenant of the **Quota was reached** event is the user whose quota was reached.

- **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 unit 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 the 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.

7 Advanced scenarios

7.1 Limiting access to the web interface

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

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

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

To limit access to the web interface

1. Log in to the management portal.
2. Navigate to the unit (p. 10) for 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**.

7.2 Limiting access to your company

Company administrators can limit access to the company for higher-level administrators.

If access to the company is limited, the higher-level administrators can only modify the company properties. They do not see the user accounts and child units at all.

To limit access to the company

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**.