

Management Portal

Version 7.8

Table of contents

- 1 About this document3**
- 2 About the management portal3**
 - 2.1 Accounts and units.....3
 - 2.2 Supported web browsers.....4
- 3 Step-by-step instructions5**
 - 3.1 Activating an administrator account5
 - 3.2 Accessing the management portal and the services5
 - 3.3 Navigation in the management portal5
 - 3.4 Creating a unit6
 - 3.5 Creating a user account6
- 4 Monitoring7**
 - 4.1 Usage8
 - 4.2 Operations8
- 5 Reporting9**
 - 5.1 Usage9
 - 5.2 Operations11
- 6 Audit log.....13**
- 7 Advanced scenarios14**
 - 7.1 Limiting access to the web interface14
 - 7.2 Limiting access to your company.....14

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

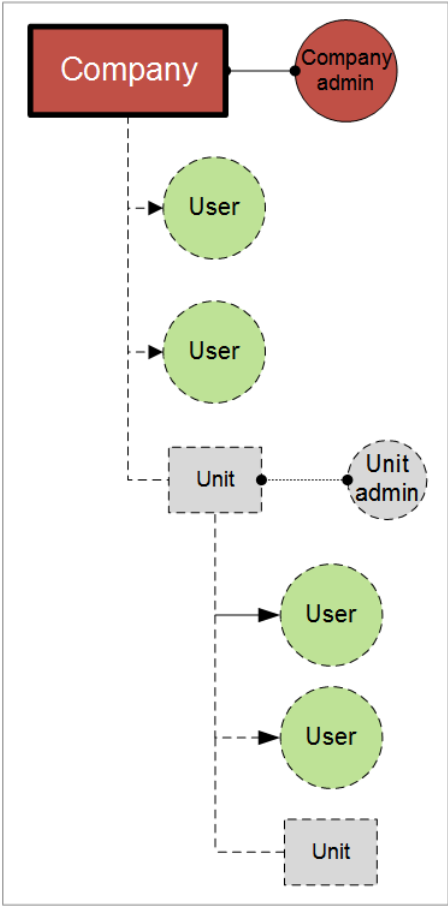
There are two user account types: administrator accounts and user accounts.

- **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 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

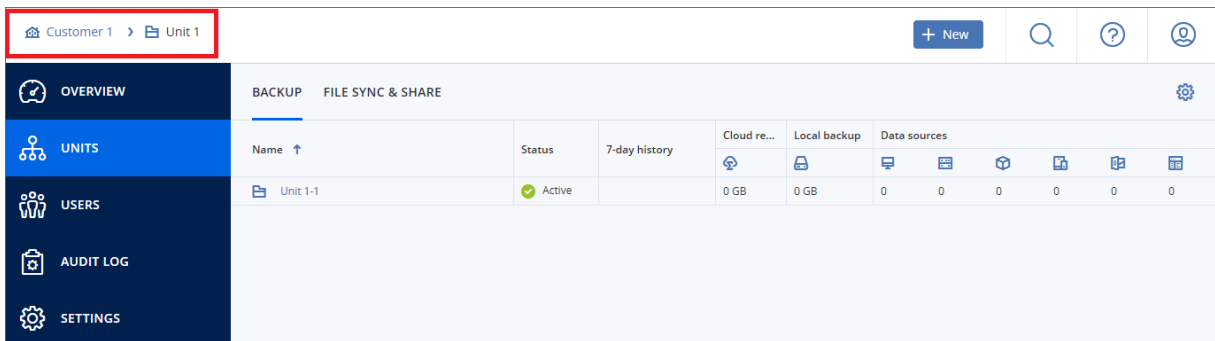
1. Go to the login page. The login page address was included in the activation email message.
2. Type the login, and then click **Continue**.
3. Type the password, and then click **Sign in**.
4. Do one of the following:
 - To log in to the management portal, click **Management Portal**.
 - To log in 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. 6), 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.

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.

Data sources		
Workstations 0	Servers 0	Virtual machines 0
Mobile devices 0	Office 365 seats 0	Websites 0

Local backup		
Local backup 0 GB		

Cloud resources		
Total cloud storage size 0 GB		

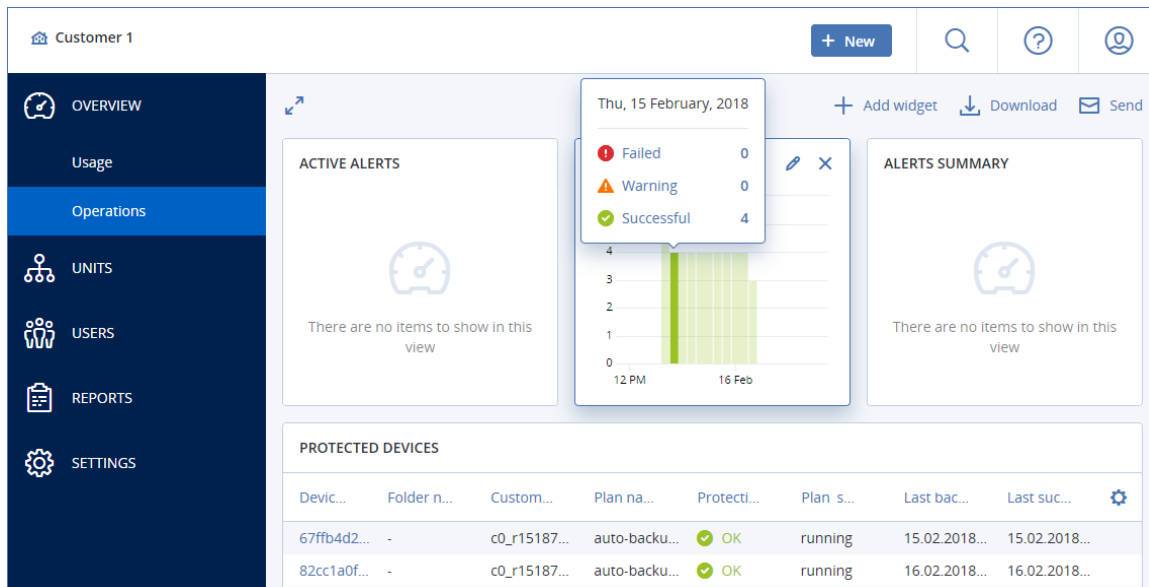
4.2 Operations

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. 5) 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**.

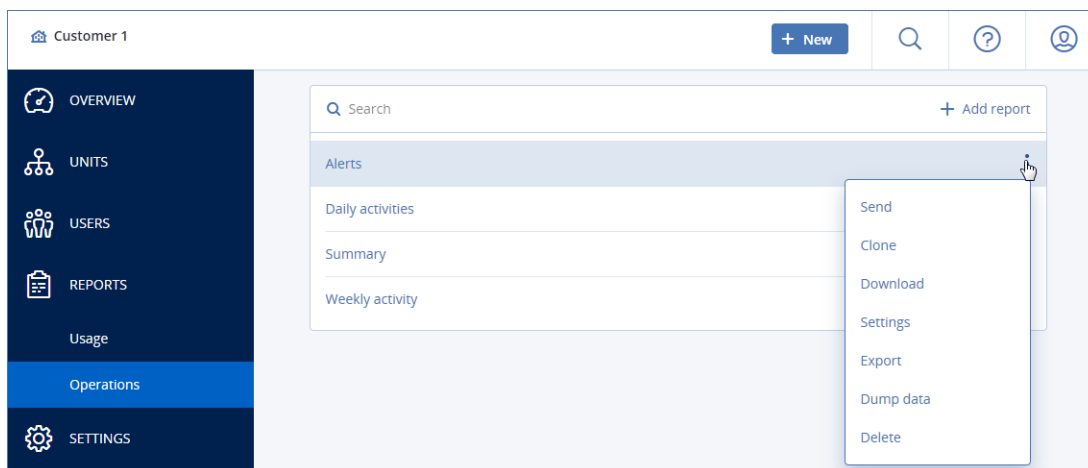
5.2 Operations

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. 8). 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 shows a web interface for configuring report settings. It is divided into two main sections: 'General' and 'Scheduled'.
In the 'General' section, there is a text input field for 'Name' containing the word 'Alerts', and a dropdown menu for 'Range' set to '7 days'.
The 'Scheduled' section has a green toggle switch that is turned on. Below it, there is a text input field for 'Recipients' containing 'user1@example.com; user2@example.com'. A dropdown menu for 'File format' is set to 'Excel and PDF'. There are two tabs: 'Days of week' (which is selected) and 'Monthly'. Under the 'Days of week' tab, there are seven buttons labeled 'SUN', 'MON', 'TUE', 'WED', 'THU', 'FRI', and 'SAT'. To the right of these buttons is a dropdown menu for 'Send at' 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. 5) 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**.