

# Management Portal

## Version 21.02

# Table of contents

<b>1 About this document</b>	<b>4</b>
<b>2 About the management portal</b>	<b>5</b>
2.1 Accounts and units	5
2.2 Quota management	6
2.2.1 Viewing quotas for your organization	7
2.2.2 Defining quotas for your users	10
2.3 Supported web browsers	12
<b>3 Step-by-step instructions</b>	<b>13</b>
3.1 Activating an administrator account	13
3.2 Accessing the management portal and the services	13
3.2.1 Switching between the management portal and the service consoles	13
3.3 Navigation in the management portal	13
3.4 Creating a unit	14
3.5 Creating a user account	14
3.6 User roles available for each service	16
3.6.1 Read-only administrator role	17
3.7 Changing the notification settings for a user	18
3.7.1 Notifications received by user role	18
3.8 Disabling and enabling a user account	18
3.9 Deleting a user account	19
3.10 Transferring ownership of a user account	19
3.11 Setting up two-factor authentication	20
3.11.1 How it works	20
3.11.2 Two-factor setup propagation across tenant levels	21
3.11.3 Setting up two-factor authentication for your tenant	22
3.11.4 Managing two-factor configuration for users	23
3.11.5 Resetting two-factor authentication in case of lost second-factor device	24
3.11.6 Brute-force protection	24
<b>4 Monitoring</b>	<b>26</b>
4.1 Usage	26
4.2 Operations	26
4.2.1 Protection status	27
4.2.2 #CyberFit Score by machine	28
4.2.3 Disk health forecast	29
4.2.4 Data protection map	33

4.2.5 Vulnerability assessment widgets .....	34
4.2.6 Patch installation widgets .....	35
4.2.7 Backup scanning details .....	37
4.2.8 Recently affected .....	37
4.2.9 Blocked URLs .....	38
4.2.10 Software inventory widgets .....	39
4.2.11 Hardware inventory widgets .....	39
<b>5 Reporting .....</b>	<b>41</b>
5.1 Usage .....	41
5.1.1 Report type .....	41
5.1.2 Report scope .....	41
5.1.3 Scheduled reports .....	41
5.1.4 Custom reports .....	42
5.1.5 Usage reports .....	42
5.2 Operations .....	43
5.3 Time zones in reports .....	47
<b>6 Audit log .....</b>	<b>49</b>
6.1 Audit log fields .....	49
6.2 Filtering and search .....	50
<b>7 Advanced scenarios .....</b>	<b>51</b>
7.1 Limiting access to the web interface .....	51
7.2 Limiting access to your company .....	51
7.3 Managing API clients .....	51
7.3.1 What is an API client? .....	52
7.3.2 Typical integration procedure .....	52
7.3.3 Creating an API client .....	52
7.3.4 Resetting the secret value of an API client .....	53
7.3.5 Disabling an API client .....	53
7.3.6 Enabling a disabled API client .....	53
7.3.7 Deleting an API client .....	54
<b>Index .....</b>	<b>55</b>

# 1 About this document

This document is intended for Customer administrators who want to use the cloud management portal to create and manage user accounts, units, and quotas, to configure and control the access to, and monitor the usage and operations in their cloud organization.

## 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

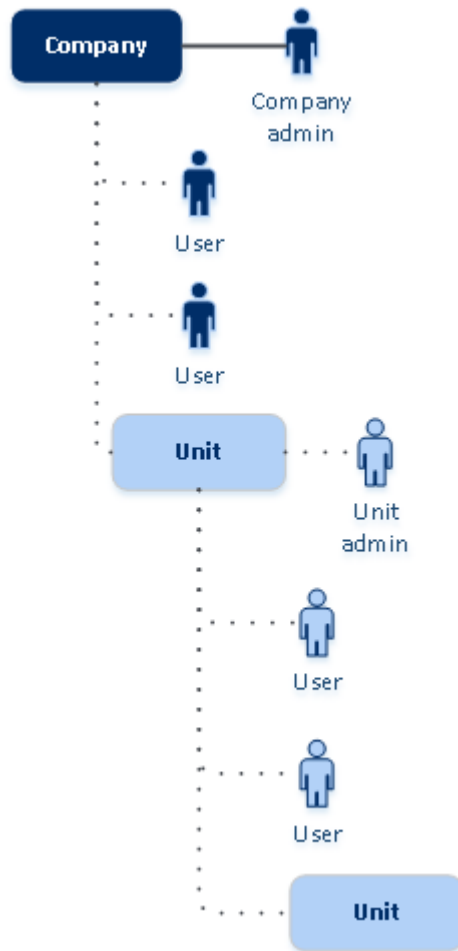
There are two user account types: administrator accounts and user accounts.

- **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.

### 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 protection 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 protection 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.

---

**Note**

Public folders consume licenses from your backup quota for Office 365 seats.

---

- **Office 365 Teams**

This quota is applied by the service provider to the entire company. This quota enables or disables the ability to protect Office 365 Teams and sets the maximum number of teams that can be protected. For protection of one team, regardless of the number of its members or channels, one quota is required. Company administrators can view the quota and the usage in the management portal.

- **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 and sets the maximum number of site collections and group sites that can be protected.

Company administrators can view the quota in the management portal. They can also view the quota, together with the amount of storage occupied by the 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.

- **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.

Backing up G Suite Shared drives is only available to customers who have at least one G Suite seats quota in addition. This quota is only verified and will not be taken up.

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

## Disaster Recovery quotas

---

### Note

The Disaster Recovery offering items are available only with the Disaster Recovery add-on.

---

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 service 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.

## 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.

## 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 number of drives to be transferred to the cloud data-center.

## 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 Cyber Protection 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 Cyber Protection 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 Cyber Protection service will be disabled when the number reaches 25.

## 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 protection 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 protection 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.

## 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.

## 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. Ensure that your password is at least eight characters long. 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 **Next**.
3. Type the password, and then click **Next**.
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.

The timeout period for the management portal is 24 hours for active sessions and 1 hour for idle sessions.

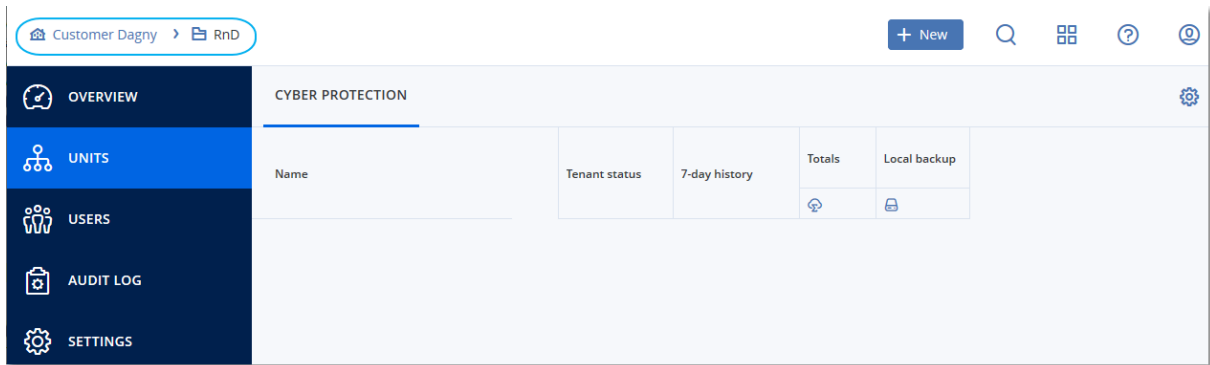
#### 3.2.1 Switching between the management portal and the service consoles

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](#)", 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:

- **Login**

---

**Important**

Each account must have a unique login.

---


- **Email**

- [Optional] **First name**
  - [Optional] **Last name**
  - In **Language**, change the default language of notifications, reports, and the software that will be used for this account.
5. 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 may 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](#).
  6. 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.

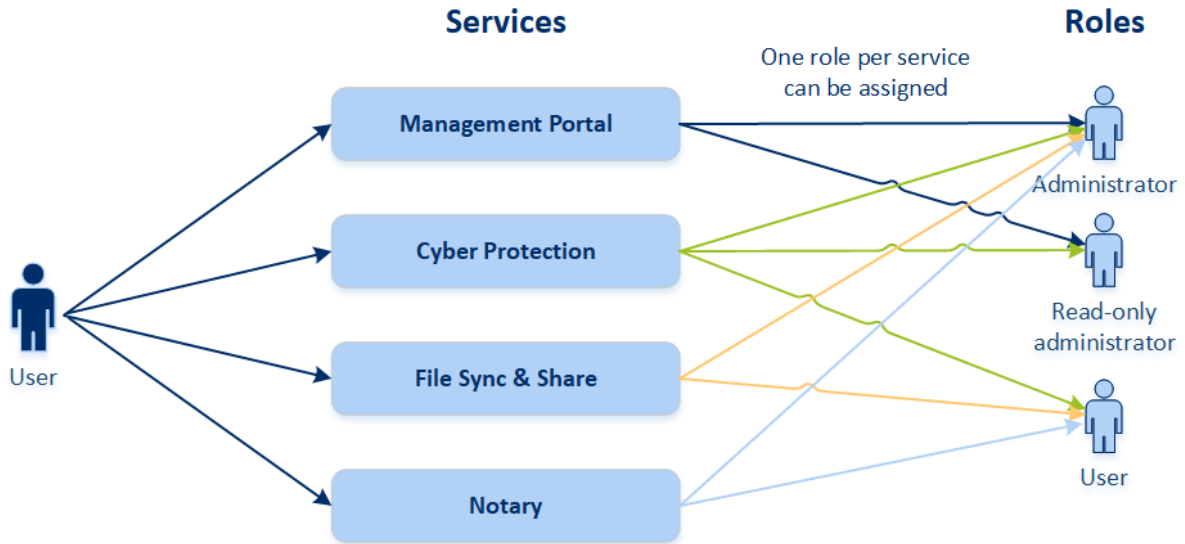
### **To reset a user's password**

1. In the management portal, go to **Users**.
2. Select the user whose password you want to reset, and then click the ellipsis icon  > **Reset password**.
3. Confirm your action by clicking **Reset**.

The user can now complete the resetting process by following the instructions in the email received.

### 3.6 User roles available for each service

One user can have several roles but only one role per service.



For each service, you can define which role will be assigned to a user.

Service	Role	Description
n/a	Company administrator	This role grants administrator rights for all services.  This role grants access to the corporate whitelist. If the Disaster Recovery add-on of the Cyber Protection service is enabled for the company, this role also grants access to the disaster recovery functionality.
Management Portal	Administrator	This role grants access to the management portal where the administrator can manage users within the entire organization.
	Read-only administrator	The role provides read-only access to all objects in the management portal. Such users can access data of other users of the organization in the read-only mode.
Cyber Protection	Administrator	This role enables configuring and managing Cyber Protection for your customers. The role is required for configuring and managing the Disaster Recovery functionality and the corporate whitelist.
	Read-only administrator	The role provides read-only access to all objects of the Cyber Protection service. Such users can access data of other users of the organization in the read-only mode. The read-only administrator cannot configure and manage the Disaster Recovery functionality or the corporate whitelist.



	User	This role enables using the Cyber Protection service but without administrative privileges. Such users cannot access data of other users of the organization.
File Sync & Share	Administrator	This role enables configuring and managing File Sync & Share for your users.
	User	This role enables using the File Sync & Share service. Such users cannot access data of other users of the organization.
Notary	Administrator	This role enables configuring and managing Notary for your users.
	User	This role enables using the Notary service but without administrative privileges. Such users cannot access data of other users of the organization.

### 3.6.1 Read-only administrator role

An account with this role has read-only access to the Cyber Protection web console and can:

- Collect diagnostic data, such as system reports.
- See the recovery points of a backup, but cannot drill down into the backup contents and cannot see files, folders, or emails.

A read-only administrator cannot:

- Start or stop any tasks.  
For example, a read-only administrator cannot start a recovery or stop a running backup.
- Access the file system on source or target machines.  
For example, a read-only administrator cannot see files, folders, or emails on a backed-up machine.
- Change any settings.  
For example, a read-only administrator cannot create a protection plan or change any of its settings.
- Create, update, or delete any data.  
For example, a read-only administrator cannot delete backups.

All UI objects that are not accessible for a read-only administrator are hidden, except for the default settings of the protection plan. These settings are shown, but the **Save** button is not active.

Any changes related to the accounts and roles are shown on the **Activities** tab with the following details:

- What was changed
- Who did the changes
- Date and time of changes

## 3.7 Changing the notification settings for a user

To change the notifications settings for a user, select the user on the **Users** tab, and then click the pencil icon in the **Settings** section. The following notifications settings are available:

- **Quota overuse notifications** (enabled by default)  
The notifications about exceeded quotas.
- **Scheduled usage reports**  
The usage reports described below that are sent on the first day of each month.
- **Failure notifications, Warning notifications, and Success notifications** (disabled by default)  
The notifications about the execution results of protection plans and the results of disaster recovery operations for each device.
- **Daily recap about active alerts** (enabled by default)  
The daily recap is generated based on the list of active alerts that are present in the service console at the moment when the recap is generated. The recap is generated and sent once a day, between 10:00 and 23:59 UTC. The time when the recap is generated and sent depends on the workload in the data center. If there are no active alerts at that time, the recap contains a note that everything is in order. The recap does not include information for past alerts that are no longer active. For example, if a user finds a failed backup and clears the alert, or the backup is retried and succeeds before the recap is generated, the alert will no longer be present and the recap will not include it.
- **Device control notifications** (disabled by default)  
The notifications about attempts to use peripheral devices and ports that are restricted by protection plans with the device control module enabled.

All notifications are sent to the user's email address.

### 3.7.1 Notifications received by user role


The notifications that Cyber Protection sends depend on the user role.

Notification type\User role	User	Customer Administrator
Notifications for own devices	Yes	Yes
Notifications for all devices in the organization	n/a	Yes
Notifications for Office 365, G-Suite, and other cloud-based backups	n/a	Yes


## 3.8 Disabling and enabling a user account

You may need to disable a user account in order to temporarily restrict its access to the cloud platform.

### ***To disable a user account***

1. In the management portal, go to **Users**.
2. Select the user account that you want to disable, and then click the ellipsis icon  > **Disable**.
3. Confirm your action by clicking **Disable**.

As a result, this user will not be able to use the cloud platform or to receive any notifications.

To enable a disabled user account, select it in the users list, and then click the ellipsis icon  > **Enable**.

## 3.9 Deleting a user account

You may need to delete a user account permanently in order to free up the resources it uses — such as storage space or license. The usage statistics will be updated within a day after deletion. For accounts with a lot of data, it might take longer.

Before deleting a user account, you have to disable it. For more information on how to do this, refer to [Disabling and enabling a user account](#).


---

### Important

Deleting a user account is irreversible!

---

#### *To delete a user account*

1. In the management portal, go to **Users**.
2. Select the disabled user account, and then click the ellipsis icon  > **Delete**.
3. To confirm your action, enter your login, and then click **Delete**.

As a result:

- This user account will be deleted.
- All data that belongs to this user account will be deleted.
- All machines associated with this user account will be unregistered.

## 3.10 Transferring ownership of a user account

You may need to transfer the ownership of a user account if you want to keep the access to a restricted user's data.


---

### Important

You cannot reassign the content of a deleted account.

---

#### *To transfer the ownership of a user account:*

1. In the management portal, go to **Users**.
2. Select the user account whose ownership you want to transfer, and then click the pencil icon in the **General information** section.
3. Replace the existing email with the email of the future account owner, and then click **Done**.
4. Confirm your action by clicking **Yes**.
5. Let the future account owner verify their email address by following the instructions sent there.
6. Select the user account whose ownership you are transferring, and then click the ellipsis icon  > **Reset password**.
7. Confirm your action by clicking **Reset**.
8. Let the future account owner reset the password by following the instructions sent to their email address.

The new owner can now access this account.

## 3.11 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.

### 3.11.1 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](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](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](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.

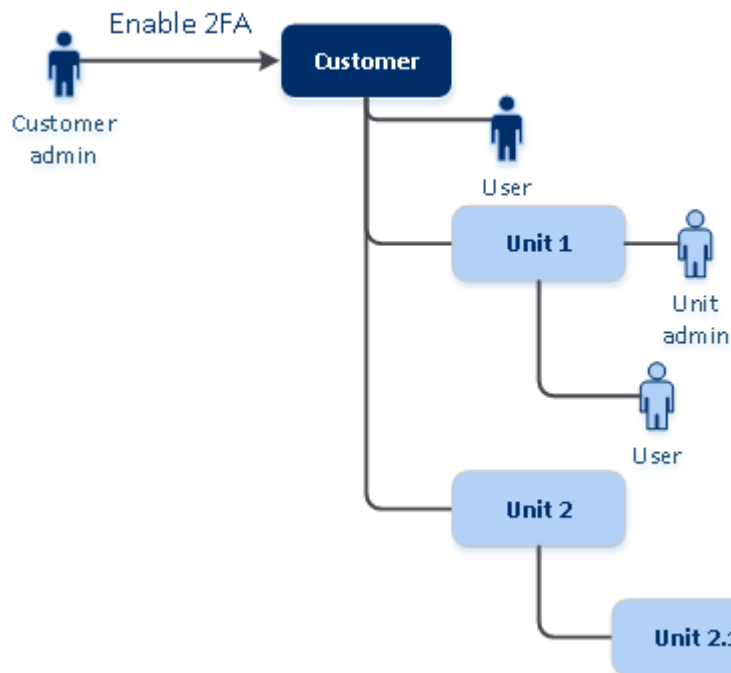
### 3.11.2 Two-factor setup propagation across tenant levels

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:

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

## 2FA setting propagation from a customer level



---

### Note

1. It is not possible to set up two-factor authentication on the unit level.
2. You can manage the two-factor authentication settings for users of the child organizations (units).

## 3.11.3 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. [If at least one user configured two-factor authentication within the organization] 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 secrets are deleted, and all trusted browsers are forgotten. 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.

### 3.11.4 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.

Users can reset all trusted browsers and reset two-factor authentication settings by themselves. This can be done when they log in to the system, by clicking the respective link and entering the TOTP code to confirm the operation.

#### 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.

### 3.11.5 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](#).

### 3.11.6 Brute-force protection

A brute-force attack is an attack when an intruder tries to get access to the system by submitting many passwords, with the hope of guessing one correctly.

The brute-force protection mechanism of the platform is based on [device cookies](#).

The settings for brute-force protection that are used in the platform are pre-defined:

Parameter	Entering the password	Entering the TOTP code
Attempt limit	10	5
Attempt limit period (the limit is reset after timeout)	15 min (900 sec)	15 min (900 sec)
Lockout happens on	Attempt limit + 1 (11th attempt)	Attempt limit
Lockout period	5 min (300 sec)	5 min (300 sec)



If you have enabled two-factor authentication, a device cookie is issued to a client (browser) only after successful authentication using both factors (password and TOTP code).

For trusted browsers, the device cookie is issued after successful authentication using only one factor (password).

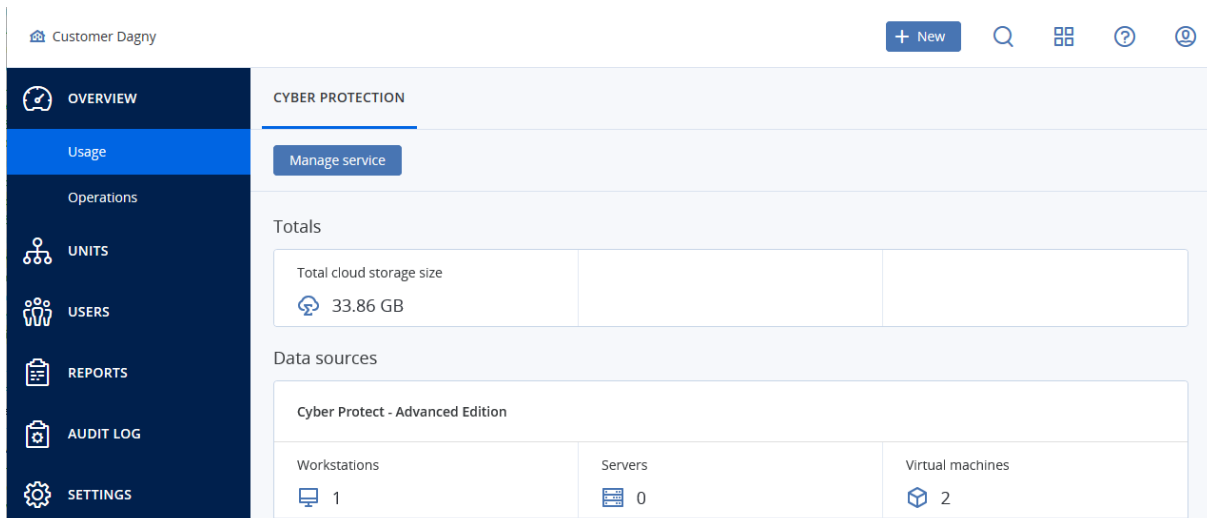
The TOTP code entering attempts are registered per user, not per device. This means that even if a user attempts to enter the TOTP code by using different devices, they will still be blocked out.

## 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.



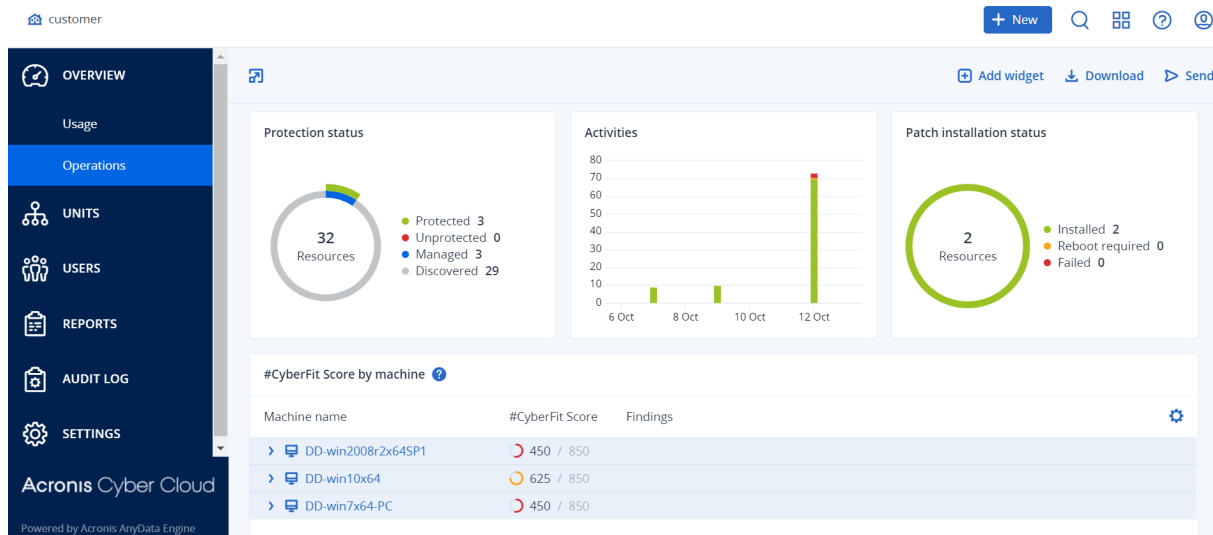
### 4.2 Operations

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 Cyber Protection service. Widgets for other services will be available in future releases.

The widgets are updated every two minutes. 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, pie charts, bar charts, lists, and tree maps. 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 pencil 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.

## 4.2.1 Protection status

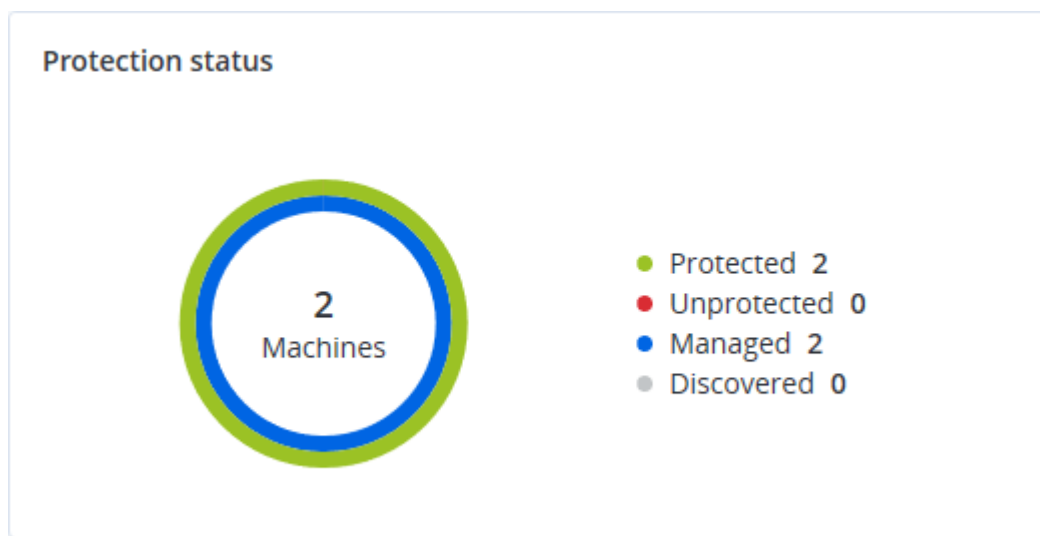
### Protection status

This widget shows the current protection status for all machines.

A machine can be in one of the following statuses:

- **Protected** – machines with applied protection plan.
- **Unprotected** – machines without applied protection plan. These include both discovered machines and managed machines with no protection plan applied.
- **Managed** – machines with installed protection agent.
- **Discovered** – machines without installed protection agent.

If you click on the machine status, you will be redirected to the list of machines with this status for more details.



## Discovered machines

This widget shows the list of discovered machines during the specified time range.

Discovered machines					
Device name ↑	IP address	OS	Organizational unit	Discovery type	⚙️
▼ Windows Server 2012 R2					
win-6g34mv70qa3	10.248.90.221	Windows Server 2012 R2	-	Local Network	
▼ Windows 10 Enterprise 2016 LTSB					
device1	10.248.90.238	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Local Network	
device2	-	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory	
device3	10.248.91.243	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Manual, Loc...	
device4	10.248.91.125	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Local Network	
device5	-	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Manual	
▼ -					
-	10.250.41.189	-	-	Manual	
-	10.248.44.199	-	-	Manual	

### 4.2.2 #CyberFit Score by machine

This widget shows for each machine the total #CyberFit Score, its compound scores, and findings for each of the assessed metrics:

- Antimalware
- Backup
- Firewall
- VPN

- Encryption
- NTLM traffic

To improve the score of each of the metrics, you can view the recommendations that are available in the report.

For more details about the #CyberFit Score, refer to "[#CyberFit Score for machines](#)".

#CyberFit Score by machine <span>?</span>			
Metric	#CyberFit Score	Findings	
<span>▼</span> DESKTOP-2N2TRE8	625 / 850		
Anti-malware	275 / 275	You have anti-malware protection enabled	
Backup	175 / 175	You have a backup solution protecting your data	
Firewall	175 / 175	You have a firewall enabled for public and private networks	
VPN	0 / 75	No VPN solution was found, your connection to public and shared networks is n...	
Encryption	0 / 125	No disk encryption was found, your device is at risk from physical tampering	
NTLM traffic	0 / 25	Outgoing NTLM traffic to remote servers is not denied, your credentials may be ...	

### 4.2.3 Disk health forecast

The disk health control feature allows you to monitor the current disk health status and get a forecast of disk health. This information allows you to prevent any problems with data loss related to disk crashes. Both HDD and SSD types of disk are supported.

#### Limitations:

1. Disk health forecast is supported only for Windows machines.
2. Only the disks of physical machines can be monitored. The disks of virtual machines cannot be monitored and shown in the widget.

Disk health can be in one of the following statuses:

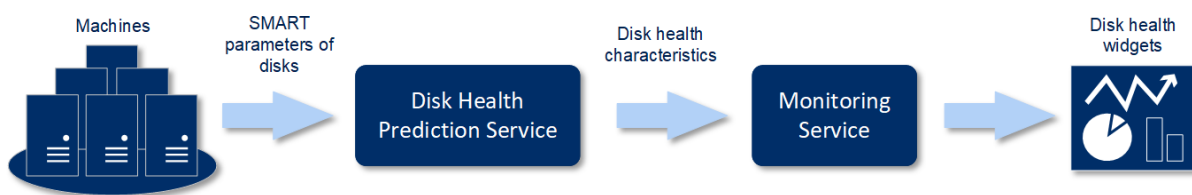
- **OK** – disk health is 70-100%
- **Warning** – disk health is 30-70%
- **Critical** – disk health is 0-30%
- **Calculating disk data** – the current disk status and forecast are being calculated

#### How it works

The Disk Health Prediction Service uses the artificial intelligence based prediction model.

1. The agent collects the SMART parameters of disks and passes this data to Disk Health Prediction Service:
  - SMART 5 – reallocated sectors count
  - SMART 9 – power-on hours
  - SMART 187 – reported uncorrectable errors
  - SMART 188 – command timeout

- SMART 197 – current pending sector count
  - SMART 198 – offline uncorrectable sector count
  - SMART 200 – write error rate
2. Disk Health Prediction Service processes the received SMART parameters, makes forecasts, and provides the following disk health characteristics:
    - Disk health current state: OK, Warning, Critical.
    - Disk health forecast: negative, stable, positive.
    - Disk health forecast probability in percentage.
 The prediction period is always one month.
  3. The Monitoring Service gets the disk health characteristics and use this data in disk health widgets shown to a user in the console.



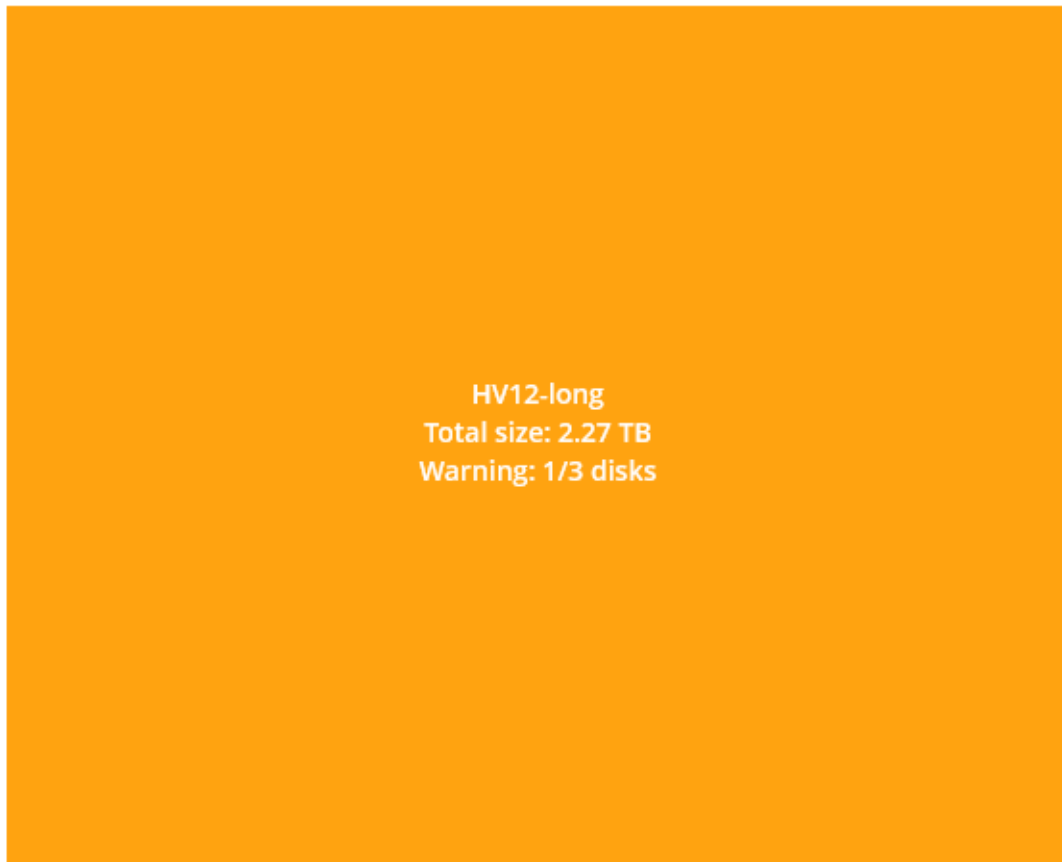
## Disk health widgets

The results of the disk health monitoring can be found on the dashboard in the disk health related widgets:

- **Disk health overview** – a treemap widget that has two levels of details that can be switched by drilling down:
  - Machine level – shows summarized information about disk status per the selected customer machines. The widget represents the most critical disk status data, other statuses are shown in the tooltip when you hover over the particular block. The machine block size depends on the total size of all disks of this machine. The machine block color depends on the most critical disk status found.

## Disk health overview

### Resources

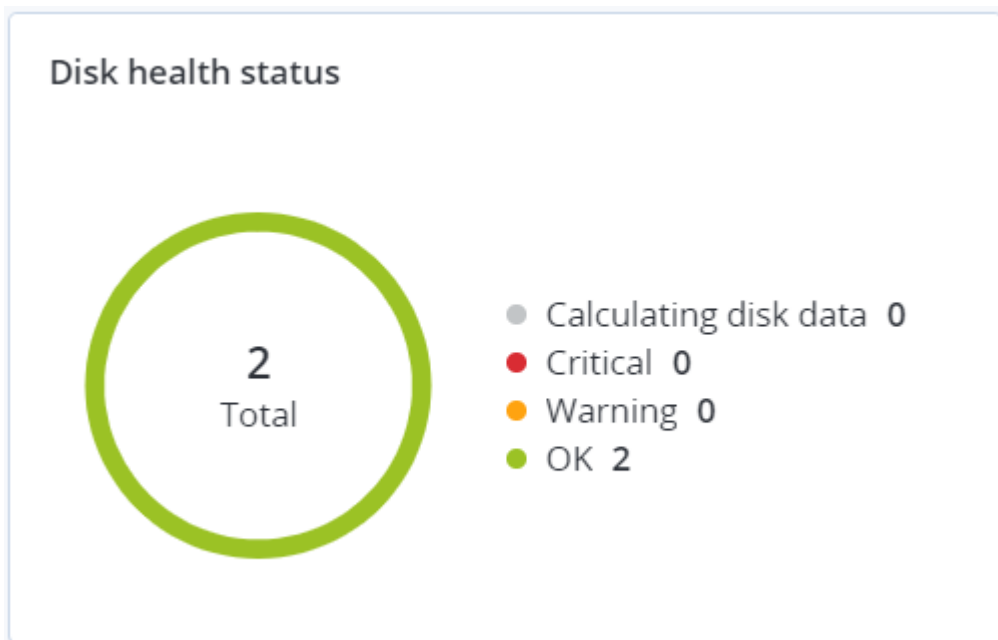


- Disk level – shows the current disk status of all disks for the selected machine. Each disk block shows a forecast of disk status change:
  - Will be degraded (disk health forecast probability in %)
  - Will stay stable (disk health forecast probability in %)

- Will be improved (disk health forecast probability in %)



- **Disk health status** – a pie chart widget showing the number of disks for each status.





## Disk health status alerts

Disk health check runs every 30 minutes while the corresponding alert is generated once a day. When the disk health has changed from Warning to Critical, you will also get the alert even if you already got another alert during a day.

Alert name	Severity	Disk health status	Description
Disk failure is possible	Warning	(30;70)	The [disk_name] disk on [machine_name] machine is likely to fail in the future. Please run a full image backup of this disk as soon as possible, replace it and then recover the image to the new disk.
Disk failure is imminent	Critical	(0;30)	The [disk_name] disk on [machine_name] machine is in a critical state and will most likely fail very soon. An image backup of this disk is not recommended at this point as the added stress can cause the disk to fail. Please back up all the most important files on this disk right now and replace it.

### 4.2.4 Data protection map

The data protection map feature allows you to discover all data that are important for you and get detailed information about number, size, location, protection status of all important files in a treemap scalable view.

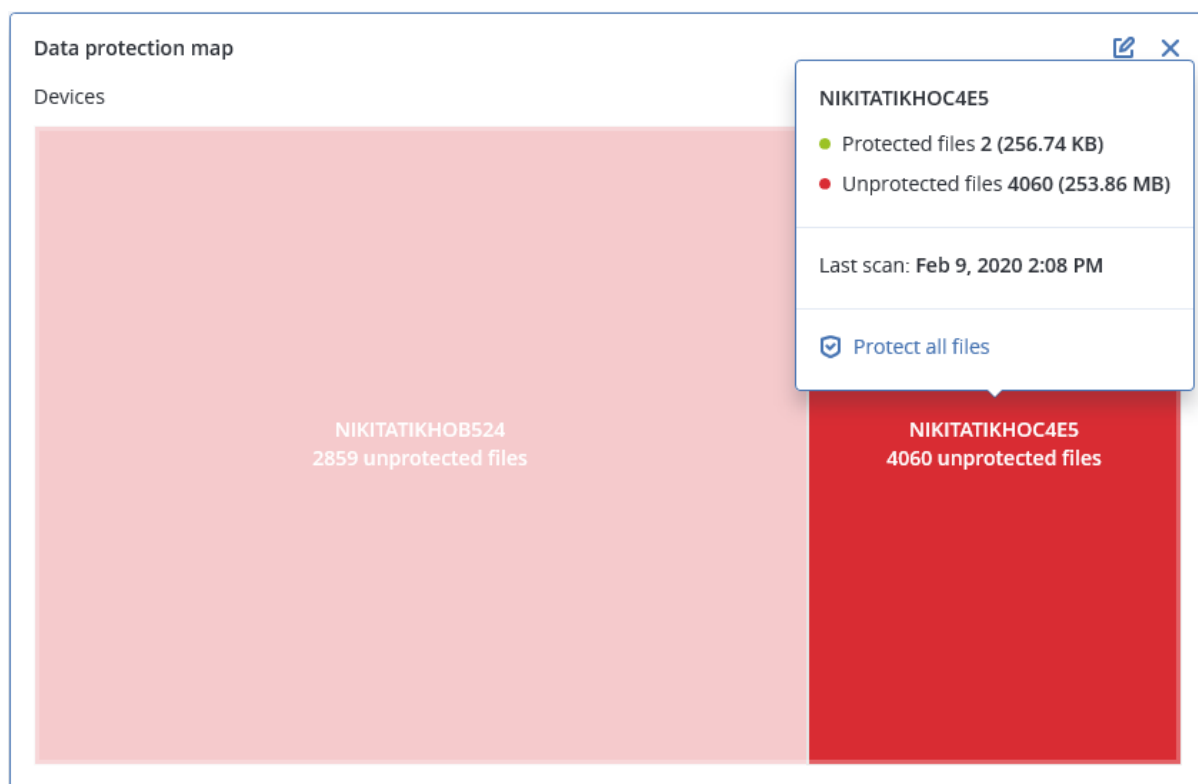
Each block size depends on the total number/size of all important files that belong to a customer/machine.

Files can have one of the following protection statuses:

- **Critical** – there are 51-100% of unprotected files with the extensions specified by you that are not being backed up and will not be backed up with the existing backup settings for the selected machine/location.
- **Low** – there are 21-50% of unprotected files with the extensions specified by you that are not being backed up and will not be backed up with the existing backup settings for the selected machine/location.
- **Medium** – there are 1-20% of unprotected files with the extensions specified by you that are not being backed up and will not be backed up with the existing backup settings for the selected machine/location.
- **High** – all files with the extensions specified by you are protected (backed up) for the selected machine/location.

The results of the data protection examination can be found on the dashboard in the Data Protection Map widget, a treemap widget that shows details on a machine level:

- Machine level – shows information about the protection status of important files per machines of the selected customer.



To protect files that are not protected, hover over the block and click **Protect all files**. In the dialog window, you can find information about the number of unprotected files and their location. To protect them, click **Protect all files**.

You can also download a detailed report in CSV format.

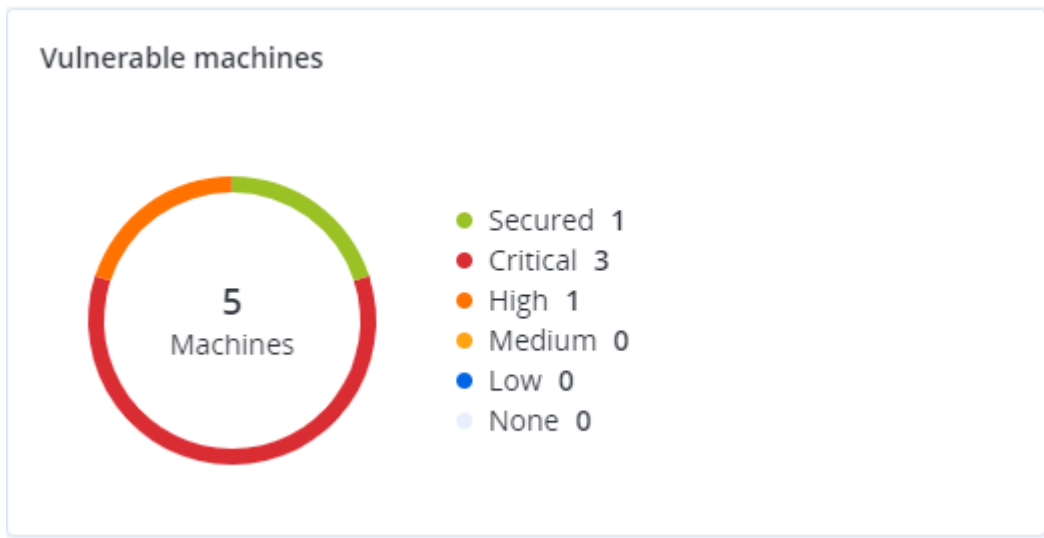
## 4.2.5 Vulnerability assessment widgets

### Vulnerable machines

This widget shows the vulnerable machines by the vulnerability severity.

The found vulnerability can have one of the following severity levels according to the [Common Vulnerability Scoring System \(CVSS\) v3.0](#):

- Secured: no vulnerabilities are found
- Critical: 9.0 - 10.0 CVSS
- High: 7.0 - 8.9 CVSS
- Medium: 4.0 - 6.9 CVSS
- Low: 0.1 - 3.9 CVSS
- None: 0.0 CVSS



## Existing vulnerabilities

This widget shows currently existing vulnerabilities on machines. In the **Existing vulnerabilities** widget, there are two columns showing timestamps:

- **First detected** – date and time when a vulnerability was detected initially on the machine.
- **Last detected** – date and time when a vulnerability was detected the last time on the machine.

Existing vulnerabilities							
Machine name	Vendor	Product	Vulnerability name/ID	Severity ↓	Last detected	First detected	⚙
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-7096	Critical	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0856	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0688	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0739	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0752	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0753	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0806	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0810	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0812	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU01945	Microsoft	Windows 10 LTSB	CVE-2019-0829	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	

[More](#)

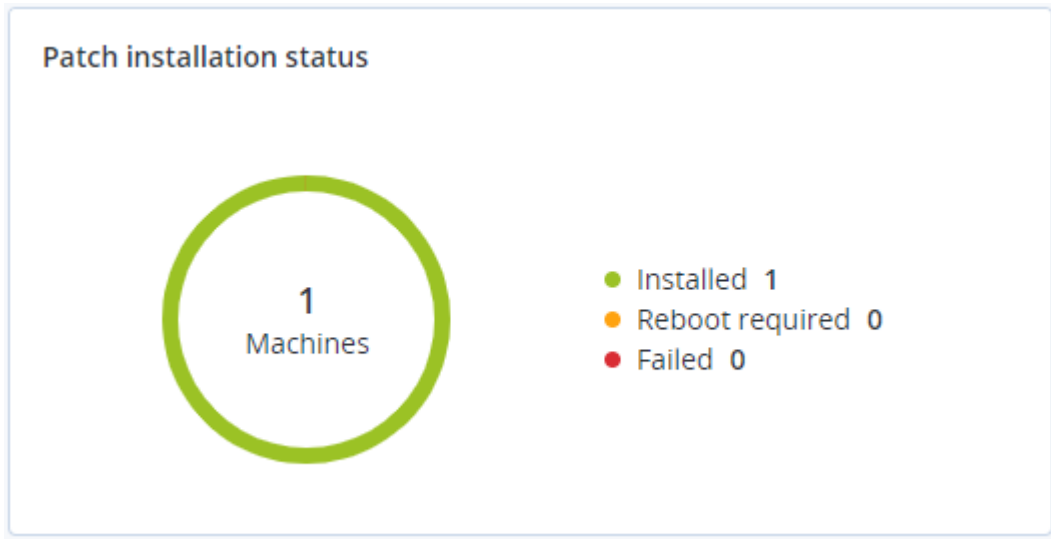
## 4.2.6 Patch installation widgets

There are four widgets related to the patch management functionality.

### Patch installation status

This widget shows the number of machines grouped by the patch installation status.

- **Installed** – all available patches are installed on a machine
- **Reboot required** – after patch installation reboot is required for a machine
- **Failed** – patch installation failed on a machine



## Patch installation summary

This widget shows the summary of patches on machines by the patch installation status.

Patch installation summary							
Installation status	Total number of machines	Total number of updates	Microsoft updates	Application updates	Critical severity	High severity	Medium severity
● Installed	1	2	1	1	2	0	0

## Patch installation history

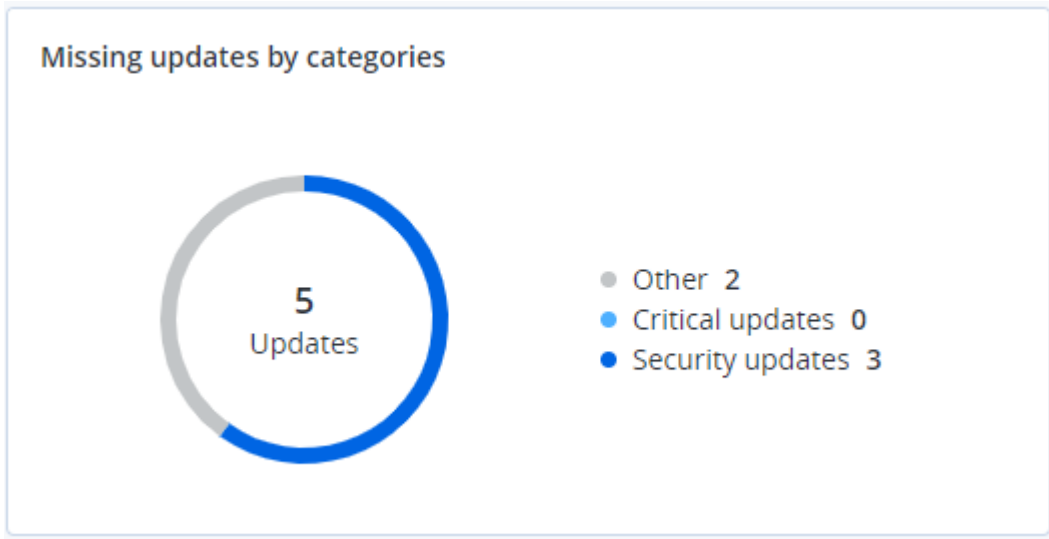
This widget shows the detailed information about patches on machines.

Patch installation history							
Machine name	Update name	Version	Severity	Approval status	Installation status	Installation date ↓	
NIKITATIKHOC4E5	FastStone Soft FastStone I...	5.9	Medium	New	● Installed	02/05/2020	
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	● Failed	02/04/2020	
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	● Installed	02/04/2020	
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	● Failed	02/04/2020	
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	● Installed	02/04/2020	
NIKITATIKHOC4E5	Oracle Java Runtime Envir...	8.0.2410.7	High	New	● Failed	02/04/2020	
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	● Installed	02/04/2020	
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	● Installed	02/04/2020	
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	● Failed	02/04/2020	
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	● Failed	02/04/2020	

## Missing updates by categories

This widget shows the number of missing updates per category. The following categories are shown:

- Security updates
- Critical updates
- Other



## 4.2.7 Backup scanning details

This widget shows the detailed information about the detected threats in backups.

Backup scanning details (threats)							
Device name	Plan name	Backup Date and time	Contents type	Location	Threat name	Affected files	Date and time
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	████████	Gen:Heur.PonyStealer.Im0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	████████	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	████████	Gen:Heur.PonyStealer.Im0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	████████	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	████████	Gen:Heur.PonyStealer.Im0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	████████	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	████████	Gen:Heur.PonyStealer.Im0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	████████	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	████████	Gen:Heur.PonyStealer.Im0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:33 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	████████	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:33 PM

[More](#)

## 4.2.8 Recently affected

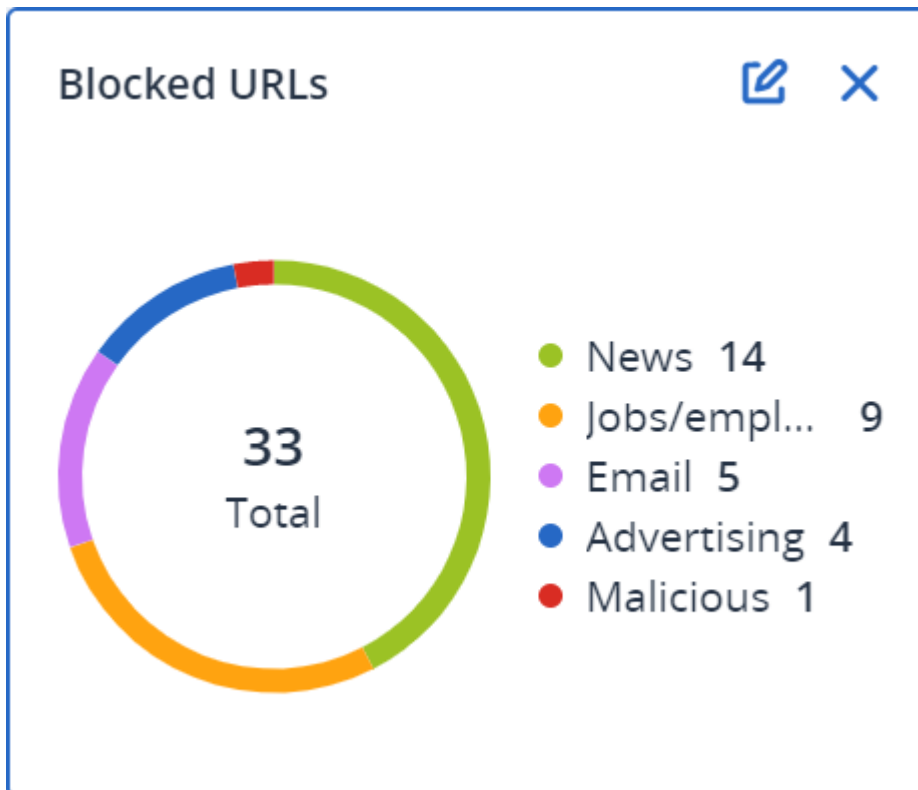
This widget shows the detailed information about recently infected machines. You can find information about what threat was detected and how many files were infected.

Recently affected					
Machine name	Protection plan	Threat	Affected files	Detection time	
Ubuntu_14.04_x64-1	Total protection	Adware.DealPlyIgen2	15	27.12.2017 11:23 AM	Folder
Ubuntu_14.04_x64-1	Protection plan	Bloodhound.MalMacroIg1	274	27.12.2017 11:23 AM	Customer
dc_w2k12_r2	Protection plan	Backdoor:Win32/Caphaw...	13	27.12.2017 11:23 AM	✓ Machine name
Win2012_r2-Hyper-V	Protection plan	W97M.DownloaderIg32	5	27.12.2017 11:23 AM	✓ Protection plan
HyperV_for12A	Total protection	Miner.XMRigIgen1	68	27.12.2017 11:23 AM	Detected by
vm-sql_2012	Total protection	Backdoor:Win32/Caphaw...	61	27.12.2017 11:23 AM	✓ Threat
vm-sql_2012	Protection plan	Adware.DealPlyIgen2	9	27.12.2017 11:23 AM	File name
MF_2012_R2	Total protection	MSH.DownloaderIgen8	73	27.12.2017 11:23 AM	File path
MF_2012_R2	Total protection	Bloodhound.MalMacroIg1	182	27.12.2017 11:23 AM	✓ Affected files
MF_2012_R2	Protection plan	Bloodhound.MalMacroIg1	18	27.12.2017 11:23 AM	✓ Detection time
ESXirestore	Protection plan	MSH.DownloaderIgen8	682	27.12.2017 11:23 AM	
MF_2012_R2	Protection plan	Miner.XMRigIgen1	13	27.12.2017 11:23 AM	
Ubuntu_14.04_x64-1	Total protection	Adware.DealPlyIgen2	3	27.12.2017 11:23 AM	
Win2012_r2-Hyper-V	Total protection	W97M.DownloaderIg32	27	27.12.2017 11:23 AM	

[More](#) | [Show all 556](#)

## 4.2.9 Blocked URLs

The widget shows the statistics of blocked URLs by category. For more information about URL filtering and categorization, see the Cyber Protection user guide.



## 4.2.10 Software inventory widgets

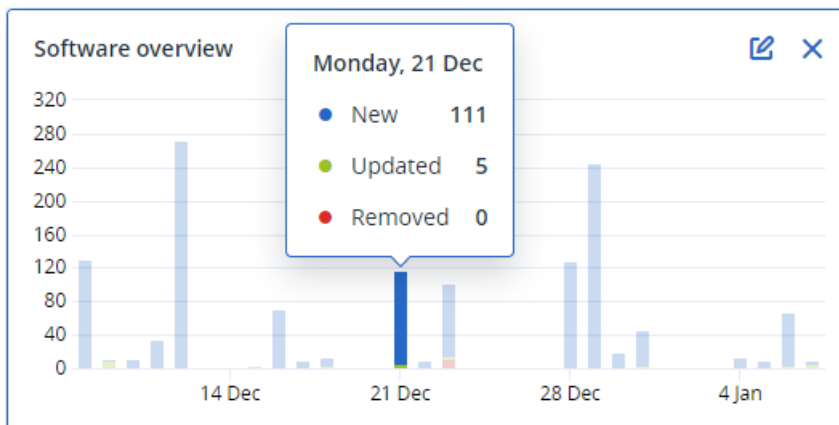
The **Software inventory** table widget shows detailed information about the all the software that is installed on Windows and macOS devices in your organization.

Software inventory

Machine name	Software name	Software version	Vendor name	Status	Date installed	Last run	Scan time	Location	User
00003079	Microsoft Policy Platform	68.1.1010.0	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
00003079	Microsoft PowerPoint MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	C:\Program Files\Microso...	System
00003079	Microsoft PowerPoint MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
00003079	Microsoft Publisher MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	C:\Program Files\Microso...	System
00003079	Microsoft Publisher MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
00003079	Microsoft Silverlight	5.1.50918.0	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	c:\Program Files\Microsof...	System
00003079	Microsoft Skype for Busin...	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
00003079	Microsoft Skype for Busin...	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	C:\Program Files\Microso...	System
00003079	Microsoft VC++ redistribu...	12.0.0.0	Intel Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
00003079	Microsoft Visual C++ 200...	8.0.61000	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
00003079	Microsoft Visual C++ 200...	9.0.30729	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
00003079	Microsoft Visual C++ 2010	10.0.40219	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
00003079	Microsoft Visual C++ 201...	11.0.61030.0	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System

More Less Show 248

The **Software overview** widget shows the number of new, updated, and deleted applications on Windows and macOS devices in your organization for a specified time period (7 days, 30 days, or the current month).



When you hover over a certain bar on the chart, a tooltip with the following information shows:

**New** - the number of newly installed applications.

**Updated** - the number of updated applications.

**Removed** - the number of removed applications.

When you click the part of the bar for a certain status, you are redirected to the **Software Management** -> **Software Inventory** page. The information in the page is filtered for the corresponding date and status.

## 4.2.11 Hardware inventory widgets

The **Hardware inventory** and **Hardware details** table widgets show information about the all the hardware that is installed on physical Windows and macOS devices in your organization.

Hardware inventory

Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (GB)	Motherboard name	Motherboard seria...	BIOS version	Domain	Registered owner	Registered organiz...	Scan date and time
Ivelins-Mac-mini...	macOS 11.0.1	10.16	6	233.47 GB	8.00 GB			0.1	-	-	-	12/14/2020 10:23 ...
O0003079.corp...	Microsoft Window...	10.0.16299	2	476.94 GB	11.83 GB	Base Board	L1HF6AC08PY	N1CET81W(1.49)	corp.acronis.com	User	Acronis Inc.	12/13/2020 8:18 PM

Hardware details

Machine name	Hardware category	Hardware name	Hardware details	Manufacturer	Status	Scan date
Ivelins-Mac-mini-2.local						
Ivelins-Mac-mini-2.local	CPU	To Be Filled By O.E.M.	Core i5, 3000, 6	Intel(R) Core(TM) i5-8500B CPU @ 3.00GHz	OK	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	RAM	4ATF51264HZ-2G6E3	9876543210, 4294...	1FACDD62	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	RAM	4ATF51264HZ-2G6E3	9876543210, 4294...	1FB057DA	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Ethernet	Ethernet, 00:00:00:...	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Wi-Fi	IEEE80211, 00:00:00:...	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Bluetooth PAN	Ethernet, 00:00:00:...	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 1	Ethernet, 00:00:00:...	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 2	Ethernet, 00:00:00:...	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 3	Ethernet, 00:00:00:...	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 4	Ethernet, 00:00:00:...	-	-	12/14/2020, 10:23 AM

More

The **Hardware changes** table widget shows information about the added, removed, and changed hardware on physical Windows and macOS devices in your organization for a specified time period (7 days, 30 days, or the current month).

Hardware changes

Machine name	Hardware category	Status	Old value	New value	Modification date and time
DESKTOP-0FF9TTF					
DESKTOP-0FF9TTF	Network adapter	Changed	Oracle Corporation, Ethernet 802.3,...	Oracle Corporation, Ethernet 802.3, ...	01/11/2021 9:28 AM
DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor Corp., Ether...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Toronto 5C1, PF0PJB10	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), WDC WD10JP...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 802.3, 00:0...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ethernet 802.3, ...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00 GB	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows Provider V9...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM

More



# 5 Reporting

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

---

## Note

This functionality is not available in the Standard editions of the Cyber Protection service.

---

## 5.1 Usage

Usage reports provide historical data about use of the services.

### 5.1.1 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.

### 5.1.2 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.

### 5.1.3 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.

### 5.1.4 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](#) 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**.

### 5.1.5 Usage reports

The report about using the Cyber Protection service includes the following data about a company or a unit:

- Size of backups by unit, by user, by device type.
- Number of protected devices by unit, by user, by device type.
- Price value by unit, by user, by device type.
- The total size of backups.
- The total amount of protected devices.
- Total price value.

---

#### **Note**

If the Cyber Protection service cannot detect a device type, that device appears as **untyped** in the report.

---

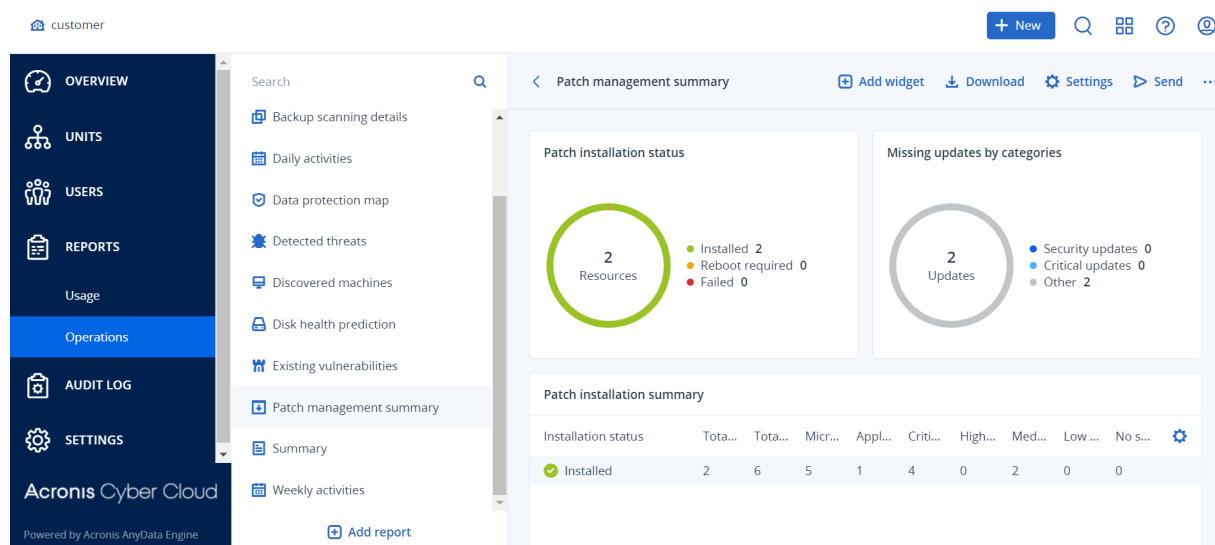
## 5.2 Operations

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**. 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 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.

The default reports are listed below:

Report name	Description	Available in service edition
#CyberFit Score by machine	Shows the #CyberFit Score, based on the evaluation of security metrics and configurations for each machine, and recommendations for improvements.	Cyber Protect
Alerts	Shows alerts that occurred during a specified time period.	Cyber Backup, Cyber Protect
Backup scanning details	Shows the detailed information about detected threats in the backups.	Cyber Protect

Daily activities	Shows the summary information about activities performed during a specified time period.	Cyber Backup, Cyber Protect
Data protection map	Shows the detailed information about the number, size, location, protection status of all important files on machines.	Cyber Protect
Detected threats	Shows the details of the affected machines by number of blocked threats and the healthy and vulnerable machines.	Cyber Backup, Cyber Protect
Discovered machines	Shows all found machines in the organization network.	Cyber Backup, Cyber Protect
Disk health prediction	Shows predictions when your HDD/SSD will break down and current disk status.	Cyber Protect
Existing vulnerabilities	Shows the existing vulnerabilities for OS and applications in your organization. The report also displays the details of the affected machines in your network for every product that is listed.	Cyber Backup, Cyber Protect
Patch management summary	Shows the number of missing patches, installed patches, and applicable patches. You can drill down the reports to get the missing/installed patch information and details of all the systems.	Cyber Protect
Summary	Shows the summary information about the protected devices for a specified time period.	Cyber Backup, Cyber Protect
Weekly activities	Shows the summary information about activities performed during a specified time period.	Cyber Backup, Cyber Protect
Software inventory	Shows detailed information about the all the software that is installed on Windows and macOS machines in your organization.	Cyber Protect
Hardware Inventory	Shows detailed information about the all the hardware that is available on physical Windows and macOS machines in your organization.	Cyber Protect

## 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

## General

Name

Backup scanning details

Set one tenant for all widgets

Range

7 days

## Scheduled

Recipients

user1@example.com; user2@example.com

File format

Excel and PDF

Language

English

Days of week

Monthly

SUN

MON

TUE

WED

THU

FRI

SAT

Send at

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 ellipsis icon in the top-right corner, and then click **Export**.

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

## Downloading a report

You can download a report, click **Download** and select the formats needed:

- Excel and PDF
- Excel
- PDF

---

### Note

For both formats, you can download up to 1000 rows for table-based widgets.

---

## 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 timestamps in CSV reports are in the UTC format. The timestamps in Excel and PDF reports are in the current system time zone.

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 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.

The raw historical data is kept permanently, but some limitations of the target export format might apply.

5. Click **Send**.

## 5.3 Time zones in reports

The time zones used in reports vary depending on the report type. The following table contains information for your reference.

Report location and type	Time zone used in the report
Management portal> Overview > Operations (widgets)	The time of report generation is in the time zone of the machine where the browser is running.
Management portal> Overview > Operations (exported to PDF or xlsx)	<ul style="list-style-type: none"> <li>The time stamp of the exported report is in the time zone of the machine that was used to export the report.</li> <li>The time zone of the activities displayed in the report is UTC.</li> </ul>
Management portal> Reports > Usage > Scheduled reports	<ul style="list-style-type: none"> <li>The report is generated at 23:59:59 UTC on the first day of the month.</li> <li>The report is sent on the second day of the month.</li> </ul>
Management portal> Reports > Usage > Custom reports	The time zone and date of the report is UTC.
Management portal> Reports > Operations (widgets)	<ul style="list-style-type: none"> <li>The time of report generation is in the time zone of the machine where the browser is running.</li> <li>The time zone of the activities displayed in the report is UTC.</li> </ul>
Management portal> Reports > Operations (exported to PDF or xlsx)	<ul style="list-style-type: none"> <li>The time stamp of the exported report is in the time zone of the machine that was used to export the report.</li> <li>The time zone of the activities displayed in the report is UTC.</li> </ul>
Management portal> Reports > Operations (scheduled delivery)	<ul style="list-style-type: none"> <li>The time zone of the report delivery is UTC.</li> <li>The time zone of the activities displayed in the report is UTC.</li> </ul>
Management portal> Users > Daily recap about active alerts	<ul style="list-style-type: none"> <li>This report is sent once a day between 10:00 and 23:59 UTC. The time when the report is sent depends on the workload in the datacenter.</li> <li>The time zone of the activities displayed in the report is UTC.</li> </ul>
Management portal> Users > Cyber Protection status notifications	<ul style="list-style-type: none"> <li>This report is sent when an activity is completed.</li> </ul> <hr/> <p><b>Note</b> Depending on the workload in the datacenter, some reports might be sent with delays.</p> <hr/> <ul style="list-style-type: none"> <li>The time zone of the activity in the report is UTC.</li> </ul>



## 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.

### 6.1 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.

## 6.2 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](#) 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. Disable the **Support access** option.
4. Click **Save**.

### 7.3 Managing API clients

Third-party systems can be integrated with Acronis Cyber Cloud by using its application programming interfaces (APIs). Access to these APIs is enabled via API clients, an integral part of [the OAuth 2.0 authorization framework](#) of the platform.

### 7.3.1 What is an API client?

An API client is a special platform account intended to represent a third-party system that needs to authenticate and be authorized to access data in the APIs of the platform and its services.

The client's access is limited to a tenant, where an administrator creates the client, and its sub-tenants.

When being created, the client inherits the service roles of the administrator account and these roles cannot be changed later. Changing roles of the administrator account or disabling it does not affect the client.

The client credentials consist of the unique identifier (ID) and secret value. The credentials do not expire and cannot be used to log in to the management portal or any service console. The secret value can be reset.

It is not possible to enable two-factor authentication for the client.

### 7.3.2 Typical integration procedure

1. An administrator creates an API client in a tenant that a third-party system will manage.
2. The administrator enables [the OAuth 2.0 client credentials flow](#) in the third-party system.  
According to this flow, before accessing the tenant and its services via the API, the system should first send the credentials of the created client to the platform by using the authorization API. The platform generates and sends back a security token, the unique cryptic string assigned to this specific client. Then, the system must add this token to all API requests.  
A security token eliminates the need for passing the client credentials with API requests. For additional security, the token expires in two hours. After this time, all API requests with the expired token will fail and the system will need to request a new token from the platform.

For more information about using the authorization and platform APIs, refer to the developer's guide at <https://developer.acronis.com/doc/account-management/v2/guide/index>.

### 7.3.3 Creating an API client

1. Log in to the management portal.
2. Click **Settings** > **API clients** > **Create API client**.
3. Enter a name for the API client.
4. Click **Next**.  
The API client is created with the **Active** status by default.
5. Copy and save the ID and secret value of the client and the data center URL. You will need them when enabling [the OAuth 2.0 client credentials flow](#) in a third-party system.

---


**Important**

For security reasons, the secret value is displayed only once. There is no way to retrieve this value if you lose it - only reset it.

---

6. Click **Done**.

### 7.3.4 Resetting the secret value of an API client

1. Log in to the management portal.
2. Click **Settings > API clients**.
3. Find the required client in the list.
4. Click , and then click **Reset secret**.
5. Confirm your decision by clicking **Next**.

A new secret value will be generated. The client ID and data center URL will not change.

All security tokens assigned to this client will become immediately expired and API requests with these tokens will fail.

6. Copy and save the new secret value of the client.

---


**Important**

For security reasons, the secret value is displayed only once. There is no way to retrieve this value if you lose it - only reset it.

---

7. Click **Done**.

### 7.3.5 Disabling an API client

1. Log in to the management portal.
2. Click **Settings > API clients**.
3. Find the required client in the list.
4. Click , and then click **Disable**.
5. Confirm your decision.


The status of the client will change to **Disabled**.

API requests with security tokens that are assigned to this client will fail but the tokens will not become immediately expired. Disabling the client does not affect tokens' expiration time.

It will be possible to re-enable the client at any time.

### 7.3.6 Enabling a disabled API client


1. Log in to the management portal.
2. Click **Settings > API clients**.
3. Find the required client in the list.

4. Click , and then click **Enable**.

The status of the client will change to **Active**.

API requests with security tokens that are assigned to this client will succeed if these tokens have not expired yet.

### 7.3.7 Deleting an API client

1. Log in to the management portal.
2. Click **Settings > API clients**.
3. Find the required client in the list.
4. Click , and then click **Delete**.
5. Confirm your decision.

All security tokens assigned to this client will become immediately expired and API requests with these tokens will fail.

---

#### **Important**

There is no way to recover a deleted client.

---

# Index

## #

#CyberFit Score by machine 28

## A

About the management portal 5

About this document 4

Accessing the management portal and the services 13

Accounts and units 5

Activating an administrator account 13

Adding a report 44

Advanced scenarios 51

Audit log 49

Audit log fields 49

## B

Backup quotas 7, 11

Backup scanning details 37

Blocked URLs 38

Brute-force protection 24

## C

Changing the notification settings for a user 18

Creating a unit 14

Creating a user account 14

Creating an API client 52

Custom reports 42

## D

Data protection map 33

Defining quotas for your users 10

Deleting a user account 19

Deleting an API client 54

Disabling an API client 53

Disabling and enabling a user account 18

Disaster Recovery quotas 8

Discovered machines 28

Disk health forecast 29

Disk health status alerts 33

Disk health widgets 30

Downloading a report 47

Dumping the report data 47

## E

Editing a report 45

Enabling a disabled API client 53

Existing vulnerabilities 35

Exporting and importing the report structure 47

## F

File Sync & Share quotas 9, 11

Filtering and search 50

## H

Hardware inventory widgets 39

How it works 20, 29

## L

Limiting access to the web interface 51

Limiting access to your company 51

## **M**

Managing API clients 51  
Managing two-factor configuration for users 23  
Missing updates by categories 36  
Monitoring 23, 26

## **N**

Navigation in the management portal 13  
Notary quotas 10-11  
Notifications received by user role 18

## **O**

Operations 26, 43

## **P**

Patch installation history 36  
Patch installation status 35  
Patch installation summary 36  
Patch installation widgets 35  
Physical Data Shipping quotas 9  
Protection status 27

## **Q**

Quota for storage 11  
Quota management 6  
Quotas for devices 11

## **R**

Recently affected 37  
Report scope 41  
Report type 41

Reporting 41

Resetting the secret value of an API client 53  
Resetting two-factor authentication in case of  
lost second-factor device 24

## **S**

Scheduled reports 41  
Scheduling a report 46  
Setting up two-factor authentication 20  
Setting up two-factor authentication for your  
tenant 22  
Software inventory widgets 39  
Step-by-step instructions 13  
Supported web browsers 12  
Switching between the management portal and  
the service consoles 13

## **T**

Time zones in reports 47  
To add a widget 27  
To create a unit 14  
To create a user account 15  
To delete a user account 19  
To disable a user account 18  
To disable two-factor authentication for a  
user 23  
To disable two-factor authentication for your  
tenant 22  
To dump the report data 47  
To edit a widget 27  
To enable or disable a scheduled report 41  
To enable two-factor authentication for a  
user 24



To enable two-factor authentication for your tenant 22

To generate a custom report 42

To limit access to the company 51

To limit access to the web interface 51

To rearrange the widgets on the dashboard 27

To remove a widget 27

To reset the trusted browsers for a user 23

To reset two-factor authentication for a user 23

To transfer the ownership of a user account 19

Transferring ownership of a user account 19

Two-factor setup propagation across tenant levels 21

Typical integration procedure 52

## **U**

Usage 26, 41

Usage reports 42

User roles available for each service 16

## **V**

Viewing quotas for your organization 7

Vulnerability assessment widgets 34

Vulnerable machines 34

## **W**

What is an API client? 52