# Table of contents

**About this document** .......................................................................................................................... 5

**About the management portal** ........................................................................................................... 6
  Accounts and units ................................................................................................................................. 6
  Quota management ............................................................................................................................... 7
    Viewing quotas for your organization ................................................................................................. 8
    Defining quotas for your users .......................................................................................................... 12
  Supported web browsers .................................................................................................................... 13

**Step-by-step instructions** .................................................................................................................. 14
  Activating an administrator account ..................................................................................................... 14
  Accessing the management portal and the services .............................................................................. 14
    Switching between the management portal and the service consoles ............................................... 14
  Navigation in the management portal .................................................................................................... 14
  Creating a unit ....................................................................................................................................... 15
  Creating a user account .......................................................................................................................... 15
  User roles available for each service .................................................................................................... 17
    Read-only administrator role .............................................................................................................. 18
    Restore operator role .......................................................................................................................... 18
  Changing the notification settings for a user .......................................................................................... 19
    Notifications received by user role ..................................................................................................... 20
  Disabling and enabling a user account .................................................................................................. 20
  Deleting a user account ........................................................................................................................ 20
  Transferring ownership of a user account .............................................................................................. 21
  Setting up two-factor authentication .................................................................................................... 22
    How it works ....................................................................................................................................... 22
    Two-factor setup propagation across tenant levels .............................................................................. 23
    Setting up two-factor authentication for your tenant ......................................................................... 24
  Managing two-factor configuration for users ......................................................................................... 24
  Resetting two-factor authentication in case of lost second-factor device ........................................... 26
  Brute-force protection ........................................................................................................................... 26

**Monitoring** ......................................................................................................................................... 28
  Usage ................................................................................................................................................... 28
  Operations dashboard ............................................................................................................................. 28
  Protection status ................................................................................................................................... 29
  #CyberFit Score by machine ............................................................................................................... 30
  Disk health monitoring ......................................................................................................................... 31
Enabling a disabled API client ........................................................................................................... 69
Deleting an API client ....................................................................................................................... 70
Index ................................................................................................................................................. 71
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.
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.

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.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Users</th>
<th>Administrators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create units</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Create accounts</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Download and install the software</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Use services</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Create reports about the service usage</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**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.
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 (Linux-based physical or virtual servers running Plesk, cPanel, DirectAdmin, VirtualMin, or ISPManager 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, the user cannot apply a protection plan to more devices.

Quotas for cloud data sources

- **Microsoft 365 seats**
  This quota is applied by the service provider to the entire company. Company administrators can view the quota and the usage in the management portal.

  Licensing of the Microsoft 365 seats depends on the selected billing mode for Cyber Protection.

  In the **Per workload** billing mode, the **Microsoft 365 seats** quota is counted per unique users. A unique user is a user who has at least one of the following:
  - Protected mailbox
  - Protected OneDrive
  - Access to at least one protected company-level resource: Microsoft 365 SharePoint Online site, or Microsoft 365 Teams.

  To learn how to check the number of members of a Microsoft 365 SharePoint or Teams site, refer to this knowledge base article.

  The following Microsoft 365 seats are not charged and do not require a per-seat license:
  - Shared mailboxes
  - Rooms and equipment
  - External users with access to backed up SharePoint sites and/or Microsoft Teams
For more information about the licensing options with the per gigabyte billing mode, refer to Cyber Protect Cloud: Microsoft 365 per GB licensing. For more information about the licensing options with the per workload billing mode, refer to Cyber Protect Cloud: Microsoft 365 licensing and pricing changes.

- **Microsoft 365 Teams**
  This quota is applied by the service provider to the entire company. This quota enables or disables the ability to protect Microsoft 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.

- **Microsoft 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.

- **Google Workspace 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.

- **Google Workspace Shared drive**
  This quota is applied by the service provider to the entire company. This quota enables or disables the ability to protect Google Workspace 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 Google Workspace Shared drives is only available to customers who have at least one Google Workspace seats quota in addition. This quota is only verified and will not be taken up.

A Microsoft 365 seat is considered protected as long as at least one protection plan is applied to the user’s mailbox or OneDrive. A Google Workspace 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.
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, cPanel, DirectAdmin, VirtualMin, or ISPManager 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, the 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.

**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
- 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.
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

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.

Accessing the management portal and the services

1. Go to the service console login page.
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.

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.

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.

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.

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.
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.

<table>
<thead>
<tr>
<th>Service</th>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>n/a</td>
<td>Company administrator</td>
<td>This role grants administrator rights for all services. This role grants access to the corporate allowlist. If the Disaster Recovery feature of the Protection service is enabled for the company, this role also grants access to the disaster recovery functionality.</td>
</tr>
<tr>
<td>Management Portal</td>
<td>Administrator</td>
<td>This role grants access to the management portal where the administrator can manage users within the entire organization.</td>
</tr>
<tr>
<td></td>
<td>Read-only administrator</td>
<td>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.</td>
</tr>
<tr>
<td>Protection</td>
<td>Administrator</td>
<td>This role enables configuring and managing Protection for your customers. The role is required for configuring and managing the Disaster Recovery functionality and the corporate allowlist.</td>
</tr>
<tr>
<td></td>
<td>Read-only administrator</td>
<td>The role provides read-only access to all objects of the 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 allowlist.</td>
</tr>
<tr>
<td></td>
<td>Restore operator</td>
<td>The role provides access to backups of Microsoft 365 and Google Workspace organizations and allows their recovery, while restricting the access to sensitive content.</td>
</tr>
<tr>
<td></td>
<td>User</td>
<td>This role enables using the Protection service but without administrative privileges. Such users cannot access data of other users of the organization.</td>
</tr>
<tr>
<td>File Sync &amp; Share</td>
<td>Administrator</td>
<td>This role enables configuring and managing File Sync &amp; Share for your users.</td>
</tr>
<tr>
<td></td>
<td>User</td>
<td>This role enables using the File Sync &amp; Share service. Such users cannot access data of other users of the organization.</td>
</tr>
<tr>
<td>Notary</td>
<td>Administrator</td>
<td>This role enables configuring and managing Notary for your users.</td>
</tr>
<tr>
<td>--------</td>
<td>---------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>User</td>
<td></td>
<td>This role enables using the Notary service but without administrative privileges. Such users cannot access data of other users of the organization.</td>
</tr>
</tbody>
</table>

**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

**Restore operator role**

This role is available only in the Cyber Protection service and is limited to Microsoft 365 and Google Workspace backups.

A restore operator can do the following:

- View alerts and activities.
- Browse and refresh the list of backups.
• Browse backups without accessing their content. The Restore operator can see the names of the backed-up files and the subjects and senders of the backed-up emails.
• Search backups (full text search is not supported).
• Recover cloud-to-cloud backups within the original Microsoft 365 or Google Workspace organization.

A restore operator cannot do the following:
• Delete alerts.
• Add or delete Microsoft 365 or Google Workspace organizations.
• Add, delete, or rename backup locations.
• Delete or rename backups.
• Create, delete, or rename folders when recovering a backup to a custom location.
• Apply a backup plan or run a backup.
• Access backed-up files or the content of backed-up emails.
• Download backed-up files or email attachments.
• Send backed-up cloud resources, such as emails or calendar items, as email.
• View or recover Microsoft 365 Teams conversations.

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 if the Cyber Protection service is enabled for the tenant where the user is created:

• Quota overuse notifications (enabled by default)
  Notifications about exceeded quotas.
• Scheduled usage reports (enabled by default)
  Usage reports that are sent on the first day of each month.
• Failure notifications, Warning notifications, and Success notifications (disabled by default)
  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 report is generated and sent depends on the workload in the data center. If there are no active alerts at that time, the recap is not sent. 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)
  Notifications about attempts to use peripheral devices and ports that are restricted by protection plans with the device control module enabled.
• **Recovery notifications** (disabled by default)
  
  Notifications about recovery actions on the following resources: user email messages and entire mailbox, public folders, OneDrive / GoogleDrive: entire OneDrive and files or folders, SharePoint files, Teams: Channels, entire Team, email messages, and Team site.

  In the context of these notifications, the following actions are considered recovery actions: send as email, download, or start a recovery operation.

• **Malware detection notifications** (enabled by default)
  
  Notifications about detected malware during on-access, on-execution, and on-demand scans, and about detections from the behavioral engine and the URL filtering engine.

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

**Notifications received by user role**

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

<table>
<thead>
<tr>
<th>Notification type\User role</th>
<th>User</th>
<th>Customer Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notifications for own devices</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Notifications for all devices in the organization</td>
<td>n/a</td>
<td>Yes</td>
</tr>
<tr>
<td>Notifications for Microsoft 365, Google Workspace, and other cloud-based backups</td>
<td>n/a</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**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**.

**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 \( \text{***} \) > **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.

**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 \( \text{***} \) > **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.
Setting up two-factor authentication

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

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

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

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

**How it works**

1. You enable two-factor authentication on your organization level.
2. All of your organization users must install an authentication application on their second-factor devices (mobile phones, laptops, desktops, or tablets). This application will be used for generating one-time TOTP codes. The recommended authenticators:
   - Google Authenticator
     - iOS app version ([https://apps.apple.com/app/google-authenticator/id388497605](https://apps.apple.com/app/google-authenticator/id388497605))
   - Microsoft Authenticator
     - iOS app version ([https://apps.apple.com/app/microsoft-authenticator/id983156458](https://apps.apple.com/app/microsoft-authenticator/id983156458))

   **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.

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).

Setting up two-factor authentication for your tenant

As an administrator, you can enable two-factor authentication for your organization.

To enable two-factor authentication for your tenant

1. In the management portal, go to Settings > Security.
2. Slide the Two-factor authentication toggle, and then click Enable.

Now, all users in the organization must set up two-factor authentication for their accounts. They will be prompted to do this the next time they try to sign in or when their current sessions expire.

The progress bar under the toggle shows how many users have set up two-factor authentication for their accounts. To check which users have configured their accounts, navigate to the Users tab and check the 2FA status column. The 2FA status of users who have not yet configured two-factor authentication for their accounts is Setup Required.

After the successful configuration of two-factor authentication, users will have to enter their login, password, and a TOTP code each time they log in to the service console.

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 toggle, and then 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.

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

We do not recommend disabling the two-factor authentication because this creates potential for breaches in the tenant security.

As an exception, you can disable the two-factor authentication for a user and keep the two-factor authentication for all other users of the tenant. This is a workaround for cases when two-factor authentication is enabled within a tenant where a cloud integration is configured, and this integration authorizes to the platform via the user account (login password). In order to continue using the integration, as a temporary solution, the user can be converted into a service account for which two-factor authentication is not applicable.

**Important**

Switching regular users to service users in order to disable two-factor authentication is not recommended because it poses risks to the tenant security.

The recommended secure solution for using cloud integrations without disabling the two-factor authentication for tenants is to create API clients and configure your cloud integrations to work with them.
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.

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.

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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Entering the password</th>
<th>Entering the TOTP code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attempt limit</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>Attempt limit period (the limit is reset after timeout)</td>
<td>15 min (900 sec)</td>
<td>15 min (900 sec)</td>
</tr>
<tr>
<td>Lockout happens on</td>
<td>Attempt limit + 1 (11th attempt)</td>
<td>Attempt limit</td>
</tr>
<tr>
<td>Lockout period</td>
<td>5 min (300 sec)</td>
<td>5 min (300 sec)</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
<td>----------------</td>
</tr>
</tbody>
</table>

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

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

To refresh the usage data displayed on the tab, click the ellipsis in the upper right of the screen and select **Refresh usage**.

**Note**
Fetching the data may take up to 10 minutes. Reload the page to view the updated data.

Operations dashboard
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.

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.

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.

![Machines](image)

**Discovered machines**

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

<table>
<thead>
<tr>
<th>Device name</th>
<th>IP address</th>
<th>OS</th>
<th>Organizational unit</th>
<th>Discovery type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2012 R2</td>
<td>10.248.90.221</td>
<td>Windows Server 2012 R2</td>
<td>-</td>
<td>Local Network</td>
</tr>
<tr>
<td>Windows 10 Enterprise 2016 LTSC</td>
<td>10.248.90.238</td>
<td>Windows 10 Enterprise 2016 LTSC</td>
<td>OU1</td>
<td>Active Directory, Local Network</td>
</tr>
<tr>
<td>device1</td>
<td>10.248.91.243</td>
<td>Windows 10 Enterprise 2016 LTSC</td>
<td>OU1</td>
<td>Active Directory</td>
</tr>
<tr>
<td>device2</td>
<td>10.248.91.125</td>
<td>Windows 10 Enterprise 2016 LTSC</td>
<td>OU1</td>
<td>Active Directory, Local Network</td>
</tr>
<tr>
<td>device3</td>
<td>10.250.41.189</td>
<td>-</td>
<td>-</td>
<td>Manual</td>
</tr>
<tr>
<td>device4</td>
<td>10.248.44.199</td>
<td>-</td>
<td>-</td>
<td>Manual</td>
</tr>
</tbody>
</table>

**#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”.

Disk health monitoring

Disk health monitoring provides information about the current disk health status and a forecast about it, so that you can prevent data loss that might be related to a disk failure. Both HDD and SSD disks are supported.

Limitations

• Disk health forecast is supported only for machines running Windows.
• Only disks of physical machines are monitored. Disks of virtual machines cannot be monitored and are not shown in the disk health widgets.
• RAID configurations are not supported.
• On NVMe drives, disk health monitoring is supported only for drives that communicate the SMART data via the Windows API. Disk health monitoring is not supported for NVMe drives that require reading the SMART data directly from the drive.

The disk health is represented by one of the following statuses:

• **OK**
  Disk health is between 70% and 100%.

• **Warning**
  Disk health is between 30% and 70%.

• **Critical**
  Disk health is between 0% and 30%.

• **Calculating disk data**
  The current disk status and forecast are being calculated.
How it works

The Disk Health Prediction Service uses an AI-based prediction model.

1. The protection agent collects the SMART parameters of the disks and passes this data to the 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. The Disk Health Prediction Service processes the received SMART parameters, makes forecasts, and then 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 one month.

3. The Monitoring Service receives these characteristics, and then shows the relevant information in the disk health widgets in the service console.

Disk health widgets

The results of the disk health monitoring are presented in the following widgets that are available in the service console.

- **Disk health overview** is a treemap widget with two levels of detail that can be switched by drilling down.
  - Machine level
    Shows summarized information about the disk health status of the selected customer machines. Only the most critical disk status is shown. The other statuses are shown in a tooltip when you hover over a particular block. The machine block size depends on the total size of all disks of the machine. The machine block color depends on the most critical disk status found.
Disk health overview

Resources

HV12-long
Total size: 2.27 TB
Warning: 1/3 disks

- Disk level
  Shows the current disk health status of all disks for the selected machine. Each disk block shows one of the following disk health forecasts and its probability in percentage:
  - Will be degraded
  - Will stay stable
- **Disk health status** is a pie chart widget that shows the number of disks for each status.

![Disk health overview]

- Will be improved

- **Disk health status** is a pie chart widget that shows the number of disks for each status.
Disk health status alerts

The disk health check runs every 30 minutes, while the corresponding alert is generated once a day. When the disk health changes from **Warning** to **Critical**, an alert always is generated.

<table>
<thead>
<tr>
<th>Alert name</th>
<th>Severity</th>
<th>Disk health status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk failure is possible</td>
<td>Warning</td>
<td>(30 – 70)</td>
<td>The &lt;disk name&gt; disk on this machine is likely to fail in the future. Run a full image backup of this disk as soon as possible, replace it, and then recover the image to the new disk.</td>
</tr>
<tr>
<td>Disk failure is imminent</td>
<td>Critical</td>
<td>(0 – 30)</td>
<td>The &lt;disk name&gt; disk on this 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. Back up the most important files on this disk immediately and replace it.</td>
</tr>
</tbody>
</table>

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.

**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](https://cvedetails.com/data-standard/cvss-standard):

- 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.

### 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 history

This widget shows the detailed information about patches on machines.

Missing updates by categories

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

- Security updates
- Critical updates
- Other
Backup scanning details

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

Recently affected

This widget shows detailed information about workloads that were affected by threats, such as viruses, malware, and ransomware. You can find information about the detected threats, the time when the threats were detected, and how many files were affected.
Downloading data for recently affected workloads

You can download the data for the recently affected workloads, generate a CSV file, and send it to the recipients that you specify.

**To download the data for the recently affected workloads**

1. In the **Recently affected** widget, click **Download data**.
2. In the **Time period** field, enter the number of days for which you want to download data. The maximum number of days that you can enter is 200.
3. In the **Recipients** field, enter the email addresses of all the people who will receive an email with a link for downloading the CSV file.
4. **Click Download**.

   The system starts generating the CSV file with the data for the workloads that were affected in the time period that you specified. When the CSV file is complete, the system sends an email to the recipients. Each recipient can then download the CSV file.

**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.
Software inventory widgets

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

<table>
<thead>
<tr>
<th>Machine name</th>
<th>Software name</th>
<th>Software version</th>
<th>Vendor name</th>
<th>Status</th>
<th>Date installed</th>
<th>Last run</th>
<th>Scan time</th>
<th>Location</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>40000079</td>
<td>Microsoft Excel</td>
<td>6.3.3.0.0</td>
<td>Microsoft Corporation</td>
<td>No change</td>
<td>12/16/2021, 10:29 AM</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>System</td>
</tr>
<tr>
<td>40000079</td>
<td>Microsoft PowerPoint</td>
<td>6.0.39.1301</td>
<td>Microsoft Corporation</td>
<td>No change</td>
<td>12/16/2021, 10:29 AM</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>System</td>
</tr>
<tr>
<td>40000079</td>
<td>Microsoft Word</td>
<td>16.0.12591.1001</td>
<td>Microsoft Corporation</td>
<td>No change</td>
<td>12/16/2021, 10:29 AM</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>System</td>
</tr>
<tr>
<td>40000079</td>
<td>Microsoft Publisher MUI</td>
<td>16.0.12591.1001</td>
<td>Microsoft Corporation</td>
<td>No change</td>
<td>12/16/2021, 10:29 AM</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>System</td>
</tr>
<tr>
<td>40000079</td>
<td>Microsoft Visio Standard MUI</td>
<td>16.0.12591.1001</td>
<td>Microsoft Corporation</td>
<td>No change</td>
<td>12/16/2021, 10:29 AM</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>System</td>
</tr>
<tr>
<td>40000079</td>
<td>Microsoft Outlook</td>
<td>16.0.12591.1001</td>
<td>Microsoft Corporation</td>
<td>No change</td>
<td>12/16/2021, 10:29 AM</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>System</td>
</tr>
<tr>
<td>40000079</td>
<td>Microsoft Project</td>
<td>16.0.12591.1001</td>
<td>Microsoft Corporation</td>
<td>No change</td>
<td>12/16/2021, 10:29 AM</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>System</td>
</tr>
<tr>
<td>40000079</td>
<td>Microsoft Access</td>
<td>16.0.12591.1001</td>
<td>Microsoft Corporation</td>
<td>No change</td>
<td>12/16/2021, 10:29 AM</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>System</td>
</tr>
<tr>
<td>40000079</td>
<td>Microsoft Word</td>
<td>16.0.12591.1001</td>
<td>Microsoft Corporation</td>
<td>No change</td>
<td>12/16/2021, 10:29 AM</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>System</td>
</tr>
</tbody>
</table>

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.

**Hardware inventory widgets**

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

The **Hardware changes** table widget shows information about the added, removed, and changed hardware on physical and virtual Windows and macOS devices in your organization for a specified time period (7 days, 30 days, or the current month).
<table>
<thead>
<tr>
<th>Machine name</th>
<th>Hardware category</th>
<th>Status</th>
<th>Old value</th>
<th>New value</th>
<th>Modification date and time</th>
</tr>
</thead>
<tbody>
<tr>
<td>DESKTOP-0997TF</td>
<td>Network adapter</td>
<td>Changed</td>
<td>Oracle Corporation, Ethernet 802.3...</td>
<td>Oracle Corporation, Ethernet 802.3...</td>
<td>01/11/2021 9:25 AM</td>
</tr>
<tr>
<td>DESKTOP-0997TF</td>
<td>Network adapter</td>
<td>New</td>
<td>-</td>
<td>Realtek Semiconductor Corp., Ethernet 802.3...</td>
<td>01/06/2021 3:37 PM</td>
</tr>
<tr>
<td>DESKTOP-0997TF</td>
<td>Motherboard</td>
<td>New</td>
<td>-</td>
<td>Lenovo, Toshiba SC1, J9DRB10</td>
<td>01/06/2021 3:37 PM</td>
</tr>
<tr>
<td>DESKTOP-0997TF</td>
<td>GPU</td>
<td>New</td>
<td>-</td>
<td>Intel(R) HD Graphics Family</td>
<td>01/06/2021 3:37 PM</td>
</tr>
<tr>
<td>DESKTOP-0997TF</td>
<td>Disk</td>
<td>New</td>
<td>-</td>
<td>(Standard disk drives), WD WD10EFRK</td>
<td>01/06/2021 3:37 PM</td>
</tr>
<tr>
<td>DESKTOP-0997TF</td>
<td>Network adapter</td>
<td>New</td>
<td>-</td>
<td>Cisco Systems, Ethernet 802.3, 10.0.0...</td>
<td>01/06/2021 3:37 PM</td>
</tr>
<tr>
<td>DESKTOP-0997TF</td>
<td>Network adapter</td>
<td>New</td>
<td>-</td>
<td>Oracle Corporation, Ethernet 802.3...</td>
<td>01/06/2021 3:37 PM</td>
</tr>
<tr>
<td>DESKTOP-0997TF</td>
<td>Raid1</td>
<td>New</td>
<td>-</td>
<td>Samsung, SSD725Q, 4.06 GB</td>
<td>01/06/2021 3:37 PM</td>
</tr>
<tr>
<td>DESKTOP-0997TF</td>
<td>Network adapter</td>
<td>New</td>
<td>-</td>
<td>T1H-NorthP4 Windows Provider V8...</td>
<td>01/06/2021 3:37 PM</td>
</tr>
<tr>
<td>DESKTOP-0997TF</td>
<td>RAID1</td>
<td>New</td>
<td>-</td>
<td>Micron, 90006500, 0.05 GB</td>
<td>01/06/2021 3:37 PM</td>
</tr>
</tbody>
</table>
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.

Usage reports

Usage reports provide historical data about use of the services. Usage reports are available in both CSV and HTML formats.

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 and partners (including user details)**
  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.

Metrics with zero usage

You can reduce the number of rows in the report by showing information about the metrics that have non-zero usage, and hiding information about the metrics that have zero usage.
Configuring scheduled Usage 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.
7. [Optional] Select Hide metrics with zero usage if you want to exclude metrics with zero usage from the report.

Configuring custom Usage 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.
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.
9. [Optional] Select Hide metrics with zero usage if you want to exclude metrics with zero usage from the report.
10. To generate the report, click Generate and send.
Data in 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.

Operations reports

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 widgets show summary information for the entire company.

Depending on the widget type, the report includes data for a time range or for the moment of browsing or report generation. See "Reported data according to widget type" (p. 62).

All historical widgets show data for the same time range. You can change this range in the report settings.

To view a report, click its name.

You can download a report about operations or send it via email in Excel (XLSX) or PDF format.

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:

<table>
<thead>
<tr>
<th>Report name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#CyberFit Score by machine</td>
<td>Shows the #CyberFit Score, based on the evaluation of security metrics and configurations for each machine, and recommendations for improvements.</td>
</tr>
<tr>
<td>Alerts</td>
<td>Shows alerts that occurred during a specified time period.</td>
</tr>
<tr>
<td>Backup scanning details</td>
<td>Shows the detailed information about detected threats in the backups.</td>
</tr>
<tr>
<td>Daily activities</td>
<td>Shows the summary information about activities performed during a specified time period.</td>
</tr>
<tr>
<td>Data protection map</td>
<td>Shows the detailed information about the number, size, location, protection status of all important files on machines.</td>
</tr>
<tr>
<td>Detected threats</td>
<td>Shows the details of the affected machines by number of blocked threats and the healthy and vulnerable machines.</td>
</tr>
<tr>
<td>Discovered machines</td>
<td>Shows all found machines in the organization network.</td>
</tr>
<tr>
<td>Disk health prediction</td>
<td>Shows predictions when your HDD/SSD will break down and current disk status.</td>
</tr>
<tr>
<td>Existing vulnerabilities</td>
<td>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.</td>
</tr>
<tr>
<td>Patch management summary</td>
<td>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.</td>
</tr>
</tbody>
</table>
### 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 Excel format
Scheduling a report

1. Click the report name, and then click **Settings**.
2. Enable the **Scheduled** switch.
3. Specify the recipients’ email addresses.
4. Select the report format: PDF, Excel, 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 ellipse 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 ellipse 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**.

**Executive summary**

The Executive summary report provides an overview of the protection status of your organization's environment and protected devices for a specified time range.
The Executive summary report includes customizable sections with dynamic widgets which show key performance metrics related to the usage of the following cloud services: Backup, Antimalware protection, Vulnerability assessment, Patch management, Notary, Disaster Recovery, and Files Sync & Share.

You can customize the report in several ways.

- Add or delete sections.
- Change the order of sections.
- Rename sections.
- Move widgets from one section to another.
- Change the order of the widgets in each section.
- Add or remove widgets.
- Customize widgets.

You can generate Executive summary reports in PDF and Excel format, and sent them to the stakeholders or owners of your organization, so that they can easily see the technical and business value of the provided services.

**Executive summary widgets**

You can add or remove the sections and widgets from the Executive summary report and thus control what information to include in it.

**Workloads overview widgets**

The following table provides more information about the widgets in the Workloads overview section.

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cyber protection summary</strong></td>
<td>The widget shows the key metrics of the Cyber protection performance for the specified time range.</td>
</tr>
<tr>
<td></td>
<td><strong>Data backed up</strong> - the total size of the archives that were created in the cloud and local storages.</td>
</tr>
<tr>
<td></td>
<td><strong>Mitigated threats</strong> - the total number of malware blocked across all devices.</td>
</tr>
<tr>
<td></td>
<td><strong>Malicious URLs blocked</strong> - the total number of URLs blocked on all devices.</td>
</tr>
<tr>
<td></td>
<td><strong>Patched vulnerabilities</strong> - the total number of vulnerabilities that were fixed through installation of software patches on all devices.</td>
</tr>
<tr>
<td></td>
<td><strong>Installed patches</strong> - the total number of installed patches on all devices.</td>
</tr>
<tr>
<td></td>
<td><strong>Servers protected by DR</strong> - the total number of servers protected by Disaster Recovery.</td>
</tr>
<tr>
<td></td>
<td><strong>File Sync &amp; Share users</strong> - the total number of end and guest users who use Cyber Files.</td>
</tr>
<tr>
<td>Widget</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Notarized files</td>
<td>the total number of notarized files.</td>
</tr>
<tr>
<td>eSigned documents</td>
<td>the total number of eSigned documents.</td>
</tr>
<tr>
<td>Blocked peripheral devices</td>
<td>the total number of blocked peripheral devices.</td>
</tr>
</tbody>
</table>

**Workloads protection status**
The widget shows the protected and unprotected workloads by type at the moment of the report's generation. Protected workloads are workloads on which at least one protection or backup plan is applied. Unprotected workloads are workloads on which no protection or backup plan is applied. The following workloads are counted:

- **Servers** - physical servers, and Domain Controller servers.
- **Workstations** - physical workstations.
- **Virtual machines** - both agent-based and agentless virtual machines.
- **Web hosting servers** - virtual or physical server with installed cPanel or Plesk.
- **Mobile devices** - physical mobile devices.

One workload can belong to more than one category. For example, a web hosting server is counted in two categories - **Servers**, and **Web hosting servers**.

**Cloud workloads protection status**
The widget shows the number of protected and unprotected cloud workloads by type at the moment of the report's generation. Protected cloud workloads are cloud workloads on which at least one backup plan is applied. Unprotected cloud workloads are cloud workloads on which no backup plan is applied. The following cloud workload types are shown in the chart (in alphabetical order from A to Z):

- Google Workspace Drive
- Google Workspace Gmail
- Google Workspace Shared Drive
- Hosted Exchange mailboxes
- Microsoft 365 mailboxes
- Microsoft 365 OneDrive
- Microsoft 365 SharePoint Online
- Microsoft Teams
- Websites

For some workload types, the following workload groups are used:

- Microsoft 365: Users, Groups, Public Folders, Teams, and Site Collections
- Google Workspace: Users, and Shared Drives
- Hosted Exchange: Users

If in one workload group there are more than 10 000 workloads, the widget does not display any data for the corresponding workloads.
For example, if the customer has a Microsoft 365 account with 10,000 mailboxes and OneDrive service for 500 users, they all belong to the Users workload group. The sum of these workloads is 10,500, which exceeds the 10,000 limitation of a workload group. Therefore, the widget will hide the corresponding workload types: Microsoft 365 mailboxes, and Microsoft 365 OneDrive.

### Antimalware protection widgets

The following table provides more information about the widgets in the **Antimalware protection** section.

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Antimalware scan of files** | The widget shows the results of on-demand antimalware scanning of the devices for the specified date range.  
Files - the total number of scanned files  
Clean - the total number of clean files  
Detected, quarantined - the total number of infected files that were quarantined  
Detected, not quarantined - the total number of infected files that were not quarantined  
Devices protected - The total number of devices with applied antimalware protection policy  
Total number of registered devices - The total number of registered devices at the time of the report's generation |
| **Blocked URLs**              | For the specified date range, the widget shows the number of blocked URLs grouped by website category.  
The widget lists the seven website categories that have the biggest number of blocked URLs, and combines the rest of the website categories into Other.  
For more information about the website categories, see the URL filtering topic in Cyber Protection. |
| **Threats detected by protection technology** | For the specified date range, the widget shows the number of detected threats grouped by the following protection technologies:  
- Antimalware scanning  
- Behavior engine  
- Cryptomining protection  
- Exploit prevention  
- Ransomware active protection |
<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
</table>
|                              | • Real-time protection  
|                              | • URL filtering  
| **Antimalware scan of backups** | The widget shows the results from the antimalware scanning of the backups for the specified date range, using the following metrics:  
|                              | • Total number of scanned recovery points  
|                              | • Number of clean recovery points  
|                              | • Number of clean recovery points with unsupported partitions  
|                              | • Number of infected recovery points. This metric includes the number of infected recovery points with unsupported partitions. |

### Backup widgets

The following table provides more information about the widgets in the **Backup** section.

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Workloads backed up**      | The widget shows the total number of registered workloads by backup status.  
|                              | **Backed up** - number of workloads that were backed up (at least one successful backup was performed) during the report date range.  
|                              | **Not backed up** - number of workloads which were not backed up (no successful backup was performed) during the report date range. |

| **Disk health status by physical device** | The widget shows the aggregated health status of physical devices based on the health statuses of their disks.  
| **OK** | This disk health status relates to values [70-100]. The status of the device is **OK** when all its disks are in status **OK**. |
| **Warning** | This disk health status relates to values [30-70]. The status of a device is **Warning** when the status of at least one of its disks is **Warning**, and when there are no disks in status **Error**.  
| **Error** | This disk health status relates to values [0-30]. The status of the device is **Error** when the status of at least one of its disks is **Error**.  
| **Calculating disk data** | The status of the device is **Calculating disk data** when the statuses of its disks are not calculated yet.  

| **Backup storage usage** | For the specified time range, the widget shows the total number and total size of the backups in the cloud and local storage. |

### Vulnerability assessment and patch management widgets

The following table provides more information about the widgets in the **Vulnerability assessment and patch management** section.
The widget shows the vulnerability assessment performance results for the specified date range.

**Total** - the total number of patched vulnerabilities.

**Microsoft software vulnerabilities** - total number of fixed Microsoft vulnerabilities on all Windows devices.

**Windows third-party software vulnerabilities** - the total number of fixed Windows third-party vulnerabilities on all Windows devices.

**Workloads scanned** - the total number of devices which were successfully scanned for vulnerabilities at least once within the specified date range.

The widget shows the patch management performance results for the specified date range.

**Installed** - the total number of patches that were successfully installed on all devices.

**Microsoft software patches** - the total number of Microsoft software patches that were installed on all Windows devices.

**Windows third-party software patches** - the total number of Windows third-party software patches that were installed on all Windows devices.

**Workloads patched** - the total number of devices which were successfully patched (at least one patch was successfully installed during the specified date range).

The following table provides more information about the widgets in the Disaster recovery section.

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Disaster Recovery statistics</strong></td>
<td>The widget shows Disaster Recovery key performance metrics for the specified date range.</td>
</tr>
<tr>
<td><strong>Production failovers</strong></td>
<td>- the number of production failover operations for the specified time range.</td>
</tr>
<tr>
<td><strong>Test failovers</strong></td>
<td>- the total number of test failover operations that were performed during the specified time range.</td>
</tr>
<tr>
<td><strong>Primary servers</strong></td>
<td>- the total number of primary servers at the moment of the report's generation.</td>
</tr>
<tr>
<td><strong>Recovery servers</strong></td>
<td>- the total number of recovery servers at the moment of the report's generation.</td>
</tr>
<tr>
<td><strong>Public IPs</strong></td>
<td>- the total number of public IP addresses (at the moment of the report's generation).</td>
</tr>
</tbody>
</table>
### Widget

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total compute points consumed</strong></td>
<td>the total number of compute points consumed during the specified time range.</td>
</tr>
<tr>
<td><strong>Disaster Recovery servers tested</strong></td>
<td>The widget shows information about the servers that are protected by Disaster Recovery and tested with test failover.</td>
</tr>
<tr>
<td></td>
<td>The widget shows the following metrics:</td>
</tr>
<tr>
<td><strong>Server protected</strong></td>
<td>the number of servers protected by Disaster Recovery (servers which have at least one recovery server) at the moment of the report's generation.</td>
</tr>
<tr>
<td><strong>Tested</strong></td>
<td>the number of servers protected by Disaster Recovery which were tested using test failover during the selected time range, out of all servers protected by Disaster Recovery.</td>
</tr>
<tr>
<td><strong>Not tested</strong></td>
<td>the number of servers protected by Disaster Recovery which were not tested using test failover during the selected time range, out of all servers protected by Disaster Recovery.</td>
</tr>
<tr>
<td></td>
<td>The widget also shows the size of the Disaster Recovery storage (in GB) at the moment of the report's generation. It is the sum of the backup sizes of the cloud servers.</td>
</tr>
<tr>
<td><strong>Servers protected with Disaster Recovery</strong></td>
<td>The widget shows information about the servers protected with Disaster Recovery and the unprotected servers.</td>
</tr>
<tr>
<td></td>
<td>The widget shows the following metrics:</td>
</tr>
<tr>
<td><strong>Protected</strong></td>
<td>the number of servers protected by Disaster Recovery (have at least one recovery server and an entire server backup) out of all registered servers at the moment of the report's generation.</td>
</tr>
<tr>
<td><strong>Unprotected</strong></td>
<td>the total number of unprotected servers out of all registered servers at the moment of the report's generation.</td>
</tr>
</tbody>
</table>

### Data Loss Prevention widget

The following topic provides more information about the Blocked peripheral devices in the **Data Loss Prevention** section.

The widget shows the total number of blocked devices and total number of blocked devices by device type for the specified date range.

- Removable storage
- Encrypted removable
- Printers
- Clipboard - includes the Clipboard and Screenshot capture device types.
• Mobile devices
• Bluetooth
• Optical drives
• Floppy drives
• USB - includes the USB port and Redirected USB port device types.
• FireWire
• Mapped drives
• Redirected clipboard - includes the Redirected clipboard incoming and Redirected clipboard outgoing device types.

The widget shows the first seven device types that have the highest number of blocked devices, and combines the rest of the device types into the Other device type.

**File Sync & Share widgets**

The following table provides more information about the widgets in the File Sync & Share section.

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File Sync &amp; Share statistics</strong></td>
<td>The widget shows the following metrics:</td>
</tr>
<tr>
<td></td>
<td><strong>Total cloud storage used</strong> - The total storage usage of all users.</td>
</tr>
<tr>
<td></td>
<td><strong>End users</strong> - the total number of end users.</td>
</tr>
<tr>
<td></td>
<td><strong>Average storage used per end user</strong> - the average storage usage per end user.</td>
</tr>
<tr>
<td></td>
<td><strong>Guest users</strong> - the total number of guest users.</td>
</tr>
<tr>
<td><strong>File Sync &amp; Share storage usage by end users</strong></td>
<td>The widget shows the total number of File Sync &amp; Share end users who have a storage usage in the following ranges:</td>
</tr>
<tr>
<td></td>
<td>• 0 - 1 GB</td>
</tr>
<tr>
<td></td>
<td>• 1 - 5 GB</td>
</tr>
<tr>
<td></td>
<td>• 5 - 10 GB</td>
</tr>
<tr>
<td></td>
<td>• 10 - 50 GB</td>
</tr>
<tr>
<td></td>
<td>• 50 - 100 GB</td>
</tr>
<tr>
<td></td>
<td>• 100 - 500 GB</td>
</tr>
<tr>
<td></td>
<td>• 500 - 1 TB</td>
</tr>
<tr>
<td></td>
<td>• 1+ TB</td>
</tr>
</tbody>
</table>

**Notary widgets**

The following table provides more information about the widgets in the Notary section.

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Notary</td>
<td>The widget shows the following Notary metrics:</td>
</tr>
<tr>
<td>Widget</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| statistics                | **Notary cloud storage used** - the total size of the storage used for Notary services.  
                              | **Notarized files** - the total number of notarized files.  
                              | **eSigned documents** - the total number of eSigned documents and eSigned files. |
| Notarized files across end users | Shows the total number of notarized files for all end users. The users are grouped based on the number of notarized files that they have.  
                              | • Up to 10 files  
                              | • 11 - 100 files  
                              | • 101 - 500 files  
                              | • 501 - 1000 files  
                              | • 1000+ files       |
| eSigned documents across end users | The widget shows the total number of eSigned documents and eSigned files for all end users. The users are grouped based on the number of eSigned documents and files that they have.  
                              | • Up to 10 files  
                              | • 11 - 100 files  
                              | • 101 - 500 files  
                              | • 501 - 1000 files  
                              | • 1000+ files       |

**Configuring the settings of the Executive summary report**

You can update the report settings that were configured when the Executive summary report was created.

*To update the settings of the executive summary report*

1. In the management console, go to Reports->Executive summary.
2. Click the name of the Executive summary report that want to update.
3. Click **Settings**.
4. Change the values of the fields as needed.
5. Click **Save**.

**Creating an Executive summary report**

You can create an Executive summary report, preview its content, configure the recipients of the report, and schedule when to send it automatically.

*To create an Executive summary report*
1. In the management console, go to Reports > Executive summary.
2. Click Create executive summary report.
3. In Report name, type the name of the report.
4. Select the Recipients of the report.
   - If you want to send the report to all contacts and users, select Send to all contacts and users.
   - If you want to send the report to specific contacts and users
     a. Clear the Send to all contacts and users.
     b. Click Select contacts.
     c. Select the specific contacts and users. You can use the Search to easily find a specific contact.
     d. Click Select.
5. Select Range: 30 days or This month
6. Select file format: PDF, Excel, or Excel and PDF.
7. Configure the scheduling settings.
   - If you want to send the report to the recipients at specific date and time:
     a. Enable the Scheduled option.
     b. Click the Day of the month field, clear the Last day field, and click the date that you want to set.
     c. In the Time field, enter the hour that you want to set.
     d. Click Apply.
   - If you want to create the report without sending it to the recipients, disable the Scheduled option.
8. Click Save.

Customizing the Executive summary report

You can determine what information to include in the Executive summary report. You can add or delete sections, add or delete widgets, rename sections, customize widgets, and drag and drop widgets and sections to change the order in which the information in the report appears.

To add a section

1. Click Add item > Add section.
2. In the Add section window, type a section name, or use the default section name.
3. Click Add to report.

To rename a section

1. In the section where you want to rename, click Edit.
2. In the Edit section window, type the new name.
3. Click **Save**.

**To delete a section**
1. In the section where you want to delete, click **Delete section**.
2. In the **Delete section** confirmation window, click **Delete**.

**To add a widget with default settings to a section**
1. In the section where you want to add the widget, click **Add widget**.
2. In the **Add widget** window, click the widget that you want to add.

**To add a customized widget to a section**
1. In the section where you want to add the widget, click **Add widget**.
2. In the **Add widget** window, find the widget that you want to add, and click **Customize**.
3. Configure the fields as necessary.
4. Click **Add widget**.

**To add a widget with default settings to the report**
1. Click **Add item > Add widget**.
2. In the **Add widget** window, click the widget that you want to add.

**To add a customized widget to the report**
1. Click **Add widget**.
2. In the **Add widget** window, find the widget that you want to add, and click **Customize**.
3. Configure the fields as necessary.
4. Click **Add widget**.

**To reset the default settings of a widget**
1. In the widget that you want to customize, click **Edit**.
2. Click **Reset to default**.
3. Click **Done**.

**To customize a widget**
1. In the widget that you want to customize, click **Edit**.
2. Edit the fields as necessary.
3. Click **Done**.

**Sending Executive summary reports**

You can send an Executive summary report on demand. In this case, the **Scheduled** setting is disregarded, and the report is sent immediately. When sending the report, the system uses the Recipients, Range, and File format values that are configured in **Settings**. You can manually change these settings before sending the report. For more information, see "Configuring the settings of the Executive summary report" (p. 58).
To send an Executive summary report

1. In the management portal, go to Reports>Executive summary.
2. Click the name of the Executive summary report that you want to send.
3. Click Send now.
   The system sends the Executive summary report to the selected recipients.

Time zones in reports

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

<table>
<thead>
<tr>
<th>Report location and type</th>
<th>Time zone used in the report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management portal&gt; Overview &gt; Operations (widgets)</td>
<td>The time of report generation is in the time zone of the machine where the browser is running.</td>
</tr>
</tbody>
</table>
| Management portal> Overview > Operations (exported to PDF or xslx) | • The time stamp of the exported report is in the time zone of the machine that was used to export the report.  
• The time zone of the activities displayed in the report is UTC. |
| Management portal> Reports > Usage > Scheduled reports | • The report is generated at 23:59:59 UTC on the first day of the month.  
• The report is sent on the second day of the month. |
| Management portal> Reports > Usage > Custom reports | The time zone and date of the report is UTC. |
| Management portal> Reports > Operations (widgets) | • The time of report generation is in the time zone of the machine where the browser is running.  
• The time zone of the activities displayed in the report is UTC. |
| Management portal> Reports > Operations (exported to PDF or xslx) | • The time stamp of the exported report is in the time zone of the machine that was used to export the report.  
• The time zone of the activities displayed in the report is UTC. |
| Management portal> Reports > Operations (scheduled delivery) | • The time zone of the report delivery is UTC.  
• The time zone of the activities displayed in the report is UTC. |
| Management portal> Users > Daily recap about active alerts | • 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.  
• The time zone of the activities displayed in the report is UTC. |
| Management portal> Users > | • This report is sent when an activity is completed. |
Cyber Protection status notifications

**Note**
Depending on the workload in the datacenter, some reports might be sent with delays.

- The time zone of the activity in the report is UTC.

### Reported data according to widget type

According to the data range that they display, widgets on the dashboard are two types:

- Widgets that display actual data at the moment of browsing or report generation.
- Widgets that display historical data.

When you configure a date range in the report settings to dump data for a certain period, the selected time range will apply only for widgets that display historical data. For widgets that display actual data at the moment of browsing, the time range parameter is not applicable.

The following table lists the available widgets and their data ranges.

<table>
<thead>
<tr>
<th>Widget name</th>
<th>Data displayed in widget and reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>#CyberFit Score by machine</td>
<td>Actual</td>
</tr>
<tr>
<td>5 latest alerts</td>
<td>Actual</td>
</tr>
<tr>
<td>Active alerts details</td>
<td>Actual</td>
</tr>
<tr>
<td>Active alerts summary</td>
<td>Actual</td>
</tr>
<tr>
<td>Activities</td>
<td>Historical</td>
</tr>
<tr>
<td>Activity list</td>
<td>Historical</td>
</tr>
<tr>
<td>Alerts history</td>
<td>Historical</td>
</tr>
<tr>
<td>Antimalware scan of backups</td>
<td>Historical</td>
</tr>
<tr>
<td>Antimalware scan of files</td>
<td>Historical</td>
</tr>
<tr>
<td>Backup scanning details (threats)</td>
<td>Historical</td>
</tr>
<tr>
<td>Backup status</td>
<td>Historical - in columns <strong>Total runs</strong> and <strong>Number of successful runs</strong></td>
</tr>
<tr>
<td></td>
<td>Actual - in all other columns</td>
</tr>
<tr>
<td>Backup storage usage</td>
<td>Historical</td>
</tr>
<tr>
<td>Blocked peripheral devices</td>
<td>Historical</td>
</tr>
<tr>
<td>Blocked URLs</td>
<td>Actual</td>
</tr>
<tr>
<td>Cloud applications</td>
<td>Actual</td>
</tr>
<tr>
<td>Feature</td>
<td>Type</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Cloud workloads protection status</td>
<td>Actual</td>
</tr>
<tr>
<td>Cyber protection</td>
<td>Actual</td>
</tr>
<tr>
<td>Cyber protection summary</td>
<td>Historical</td>
</tr>
<tr>
<td>Data protection map</td>
<td>Historical</td>
</tr>
<tr>
<td>Devices</td>
<td>Actual</td>
</tr>
<tr>
<td>Disaster recovery servers tested</td>
<td>Historical</td>
</tr>
<tr>
<td>Disaster recovery statistics</td>
<td>Historical</td>
</tr>
<tr>
<td>Discovered machines</td>
<td>Actual</td>
</tr>
<tr>
<td>Disk health overview</td>
<td>Actual</td>
</tr>
<tr>
<td>Disk health status</td>
<td>Actual</td>
</tr>
<tr>
<td>Disk health status by physical devices</td>
<td>Actual</td>
</tr>
<tr>
<td>eSigned documents across end users</td>
<td>Actual</td>
</tr>
<tr>
<td>Existing vulnerabilities</td>
<td>Historical</td>
</tr>
<tr>
<td>File Sync &amp; Share statistics</td>
<td>Actual</td>
</tr>
<tr>
<td>File Sync &amp; Share storage usage by end users</td>
<td>Actual</td>
</tr>
<tr>
<td>Hardware changes</td>
<td>Historical</td>
</tr>
<tr>
<td>Hardware details</td>
<td>Actual</td>
</tr>
<tr>
<td>Hardware inventory</td>
<td>Actual</td>
</tr>
<tr>
<td>Historical alerts summary</td>
<td>Historical</td>
</tr>
<tr>
<td>Locations summary</td>
<td>Actual</td>
</tr>
<tr>
<td>Missing updates by categories</td>
<td>Actual</td>
</tr>
<tr>
<td>Not protected</td>
<td>Actual</td>
</tr>
<tr>
<td>Notarized files across end users</td>
<td>Actual</td>
</tr>
<tr>
<td>Notary statistics</td>
<td>Actual</td>
</tr>
<tr>
<td>Patch installation history</td>
<td>Historical</td>
</tr>
<tr>
<td>Patch installation status</td>
<td>Historical</td>
</tr>
<tr>
<td>Patch installation summary</td>
<td>Historical</td>
</tr>
<tr>
<td>Patched vulnerabilities</td>
<td>Historical</td>
</tr>
<tr>
<td>Metric</td>
<td>Timeframe</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Patches installed</td>
<td>Historical</td>
</tr>
<tr>
<td>Protection status</td>
<td>Actual</td>
</tr>
<tr>
<td>Recently affected</td>
<td>Historical</td>
</tr>
<tr>
<td>Servers protected with disaster recovery</td>
<td>Actual</td>
</tr>
<tr>
<td>Software inventory</td>
<td>Actual</td>
</tr>
<tr>
<td>Software overview</td>
<td>Historical</td>
</tr>
<tr>
<td>Threats detected by protection technology</td>
<td>Historical</td>
</tr>
<tr>
<td>Vulnerable machines</td>
<td>Actual</td>
</tr>
<tr>
<td>Workloads backed up</td>
<td>Historical</td>
</tr>
<tr>
<td>Workloads protection status</td>
<td>Actual</td>
</tr>
</tbody>
</table>
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
- Operations with cloud-to-cloud resources that are performed by users in the Cyber Protection service console
- 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**, **Backup content was browsed**.

- **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.
Advanced scenarios

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.

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.

Managing API clients

Third-party systems can be integrated with 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.
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.

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.

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**.

**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**.

**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.

**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.

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  30

A
About the management portal  6
About this document  5
Accessing the management portal and the services  14
Accounts and units  6
Activating an administrator account  14
Adding a report  48
Advanced scenarios  67
Antimalware protection widgets  53
Audit log  65
Audit log fields  65

B
Backup quotas  8, 12
Backup scanning details  39
Backup widgets  54
Blocked URLs  40
Brute-force protection  26

C
Changing the notification settings for a user  19
Configuring custom Usage reports  45
Configuring scheduled Usage reports  45
Configuring the settings of the Executive summary report  58
Creating a unit  15
Creating a user account  15
Creating an API client  68
Creating an Executive summary report  58
Customizing the Executive summary report  59

D
Data in Usage reports  46
Data Loss Prevention widget  56
Data protection map  35
Defining quotas for your users  12
Deleting a user account  20
Deleting an API client  70
Disabling an API client  69
Disabling and enabling a user account  20
Disaster Recovery quotas  10
Disaster Recovery widgets  55
Discovered machines  30
Disaster Recovery widgets  55
Disk health monitoring  31
Disk health status alerts  35
Disk health widgets  32
Downloading a report  50
Downloading data for recently affected workloads  40
Dumping the report data  50

E
Editing a report  48
Enabling a disabled API client  69
Executive summary  50
Executive summary widgets  51
Existing vulnerabilities 37
Exporting and importing the report structure 50

F
File Sync & Share quotas 11, 13
File Sync & Share widgets 57
Filtering and search 66

H
Hardware inventory widgets 42
How it works 22, 32

L
Limitations 31
Limiting access to the web interface 67
Limiting access to your company 67

M
Managing API clients 67
Managing two-factor configuration for users 24
Metrics with zero usage 44
Missing updates by categories 38
Monitoring 24, 28

N
Navigation in the management portal 14
Notary quotas 11, 13
Notary widgets 57
Notifications received by user role 20

O
Operations dashboard 28
Operations reports 46

P
Patch installation history 38
Patch installation status 37
Patch installation summary 38
Patch installation widgets 37
Physical Data Shipping quotas 11
Protection status 29

Q
Quota for storage 12
Quota management 7
Quotas for cloud data sources 8
Quotas for storage 9

R
Recently affected 39
Report scope 44
Report type 44
Reported data according to widget type 62
Reporting 44
Resetting the secret value of an API client 69
Resetting two-factor authentication in case of lost second-factor device 26

S
Scheduling a report 49
Sending Executive summary reports 60
Setting up two-factor authentication 22
Setting up two-factor authentication for your tenant 24
Software inventory widgets 41
Step-by-step instructions 14
Supported web browsers 13
Switching between the management portal and the service consoles 14

Time zones in reports 61
To disable two-factor authentication for a user 25
To disable two-factor authentication for your tenant 24
To enable two-factor authentication for a user 26
To enable two-factor authentication for your tenant 24
To reset the trusted browsers for a user 25
To reset two-factor authentication for a user 25
Transferring ownership of a user account 21
Two-factor setup propagation across tenant levels 23
Typical integration procedure 68

Usage 28
Usage reports 44
User roles available for each service 17

Viewing quotas for your organization 8