

Management Portal

25.06

Table of contents

About this document	6
About the management portal	7
Supported web browsers	7
My Inbox	7
Overview	7
Checking your notifications	7
Searching My Inbox	8
Accounts and units	8
Quota management	9
Viewing quotas for your organization	10
Defining quotas for your users	17
Step-by-step instructions	19
Activating an administrator account	19
Password requirements	19
Accessing the management portal and the services	19
Switching between the management portal and the service consoles	20
Navigation in the management portal	20
Creating a unit	20
Creating a user account	21
User roles available for each service	23
Read-only administrator role	27
Restore operator role	28
Changing the notification settings for a user	29
Default notification settings enabled by notification type and user role	31
Notifications enabled by default per device type and user role	32
Disabling and enabling a user account	32
Deleting a user account	32
Transferring ownership of a user account	33
Setting up two-factor authentication	34
How it works	34
Two-factor setup propagation across tenant levels	36
Setting up two-factor authentication for your tenants	37
Managing two-factor authentication for users	37
Resetting two-factor authentication in case of lost second-factor device	39
Brute-force protection	39

Configuring the updates of the Cyber Protection agent	40
Immutable storage	43
Immutable storage modes	44
Supported storages and agents	44
Configuring immutable storage	44
Viewing immutable storage usage	46
Billing example for immutable storage	47
Enabling the Advanced Security Awareness Training for users in your organization	47
Limiting access to the web interface	48
Limiting access to your company	48
Task management	50
Viewing service desk tickets	50
Creating a service desk ticket	50
Updating service desk tickets	52
Submitting service desk tickets via the ticket portal	53
Monitoring	54
Usage	54
Operations dashboard	54
Protection status	55
#CyberFit Score by machine	57
Endpoint Detection and Response (EDR) widgets	57
Disk health monitoring	59
Data protection map	63
Vulnerability assessment widgets	65
Patch installation widgets	66
Backup scanning details	67
Recently affected	68
Blocked URLs	69
Software inventory widgets	69
Hardware inventory widgets	70
Session history	71
Geolocation tracking widget	71
Chat sessions widget	71
Technician performance widget	72
Audit log	72
Audit log fields	72
Filtering and search	73

Collecting performance data for Cyber Protection agents	74
Performance thresholds for ETL data collection	75
Reporting	78
Usage reports	78
Report type	78
Report scope	78
Metrics with zero usage	79
Configuring scheduled Usage reports	79
Configuring custom Usage reports	79
Data in Usage reports	80
Operations reports	80
Actions with reports	82
Executive summary	84
Executive summary widgets	84
Configuring the settings of the Executive summary report	93
Creating an Executive summary report	93
Customizing the Executive summary report	94
Sending Executive summary reports	95
Time zones in reports	96
Reported data according to widget type	97
Integrations	100
Integration catalogs	100
Catalog entries	100
Opening your data center integration catalog	101
Opening Application Catalog	102
Activating an integration	106
Configuring an active integration	106
Deactivating an active integration	106
API clients	107
API client credentials	107
API client flow	107
Creating an API client	107
Resetting an API client secret value	108
Disabling an API client	108
Enabling a disabled API client	109
Deleting an API client	109
Creating an integration	109

Index	111
-------------	-----

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.

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.

My Inbox

The My Inbox page is designed to streamline your communication within the application. By following this guide, you can effectively manage your messages, stay organized, and enhance your productivity. The product inbox is your central hub for receiving and managing communications within the application. It lets you stay informed about important updates, messages, and alerts within your workflow.

Overview

The **My Inbox** tab features a notification counter that displays the number of unread notifications. Clicking on this counter reveals the unread notifications, making it easy to track pending items. Additionally, counters next to each filter (category, importance, action) show the number of notifications available under that specific filter, helping you understand how many notifications fall into each category.

In your Inbox, you will receive various notifications, each designed for specific purposes based on your account settings and context: feature announcements, new trainings available, invitations to events and webinars, certificate expiration reminders, promotions, maintenance notices, surveys, and other.

Checking your notifications

Checking your notification section

1. Sign in with to the Cyber Protect Cloud console.
2. In the navigation pane, select the **My Inbox** menu item.

Searching My Inbox

To search for unread messages

1. Click the **My Inbox** menu item.
2. In the upper right corner, switch the **Show only unread** toggle.

To search for important information in your inbox

1. Access **My Inbox** from the Cyber Protect Cloud dashboard.
2. In the inbox view, locate the **Search** bar at the top.
3. Enter relevant keywords or sender names to filter the messages.
4. Press **Enter** to view the search results.

The results will show all notifications that match your search criteria.

Accounts and units

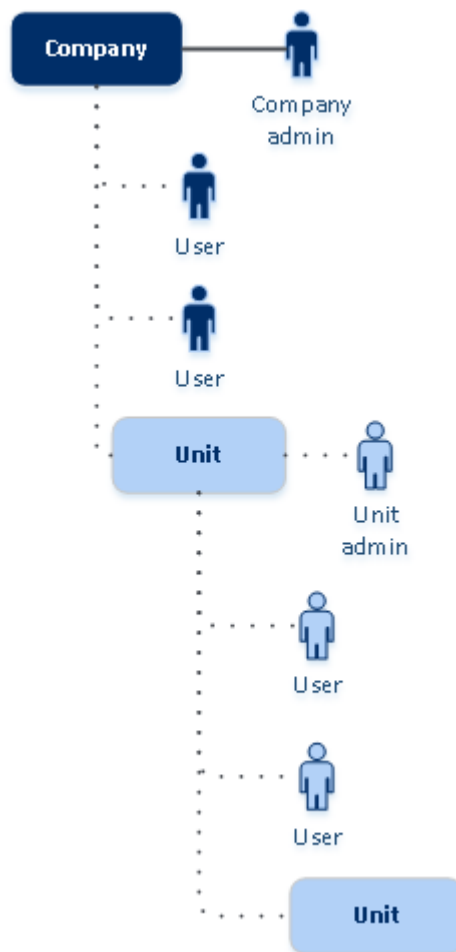
There are two user account types: administrator accounts and user accounts.

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

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

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

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



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

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

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.

Important

The values of storage usage displayed in the product UI are in binary byte units – mebibytes (MiB), gibibytes (GiB), and tebibytes (TiB) – even though the labels show MB, GB, and TB respectively. For example, if the actual usage is 3105886629888 bytes, the value displayed in the UI is correctly shown as 2.82, but is labeled with TB instead of TiB.

Viewing quotas for your organization

In the management portal, go to **Monitoring > 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 its usage in the management portal. When the hard quota is exceeded, backup plans cannot be applied to new seats.

The billing for this quota depends on the selected billing mode for Cyber Protection.

- In the **Per gigabyte** billing mode, the billing is based only on the storage usage and seats are not counted.
- In the **Per workload** billing mode, the billing is based on the number of protected Microsoft 365 seats. Storage usage is billed only for unprotected seats.

The following table summarizes the **Per workload** billing mode.

	Backup location	
	Acronis-hosted storage* Partner-hosted storage	Microsoft Azure storage Google storage
Protected seat	Billing is based on the number of protected seats. Storage space that is used by the backups of the protected seats is not billed.	Both protected seats and used storage are billed.
Unprotected seat	Unprotected seats are not billed. Storage space that is used by the backups of the unprotected seats is billed.	Unprotected seats are not billed. Storage space that is used by the backups of the unprotected seats is billed.

* Fair usage policy for Acronis storage applies. Terms and conditions are available at <https://www.acronis.com/company/licensing/#cyber-cloud-fair-usage>.

A seat is considered protected when a Microsoft 365 user has any of the following:

- Mailbox to which a backup plan is applied
- OneDrive to which a backup plan is applied
- Access to a protected company-level resource, such as 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, see [this knowledge base article](#).

A seat becomes unprotected in the following cases:

- The access to the protected company-level resource, such as Microsoft 365 SharePoint Online site or Microsoft 365 Teams, is revoked for a user.
- All backup plans are revoked from a user's mailbox or OneDrive.
- A user is deleted in the Microsoft 365 organization.

The following Microsoft 365 resources 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.

Note

Blocked Microsoft 365 users that do not have a protected personal mailbox or OneDrive, and can only access shared resources (shared mailboxes, SharePoint sites, and Microsoft Teams), are not charged. Blocked users are those who do not have a valid login and cannot access the Microsoft 365 services. To learn how to block all unlicensed users in a Microsoft 365 organization, see "Preventing unlicensed Microsoft 365 users from signing in" (p. 14).

Important

The local agent and the cloud agent consume separate quotas. If you back up the same workloads by using both agents, you will be charged twice. For example:

- If you back up the mailboxes of 120 users by using the local agent, and you back up the OneDrive files of the same users by using the cloud agent, you will be charged for 240 Microsoft 365 seats.
 - If you back up the mailboxes of 120 users by using the local agent, and you back up the same mailboxes also by using the cloud agent, you will be charged for 240 Microsoft 365 seats.
-

To check the frequently asked questions about the Microsoft 365 seats licensing, see [Cyber Protect Cloud: Microsoft 365 per GB licensing](#) and [Cyber Protect Cloud: Microsoft 365 licensing and pricing changes](#).

- **Microsoft 365 SharePoint Online**

This quota is applied by the service provider to the entire company. This quota enables the protection of 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 that is used by the SharePoint Online backups, in the usage reports.

- **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 email archiving seats**

The **Microsoft 365 email archiving seats** quota enables or disables the ability to create an email archive for Microsoft 365 mail servers and sets the maximum number of mailboxes that can be added to the archive.

- **Email archiving seats (obsolete)**

This quota is deprecated and you cannot enable it when creating new tenants in Management Portal.

For existing tenants, you can only disable the quota if it was already enabled, but you can no longer enable it.

Important

When creating new customer tenants, use the **Microsoft 365 archiving seats** quota.

For existing customers, the **Email archiving seats (obsolete)** quota will be automatically replaced by the **Microsoft 365 archiving seats** quota. Any existing usage under **Email archiving seats (obsolete)** will be transferred to **Microsoft 365 archiving seats**.

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.

A Google Workspace seat is considered protected if at least one backup plan is applied to the user's mailbox or Google Drive.

When the hard quota is exceeded, a company administrator cannot apply a backup plan to new seats.

- **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.

Quotas for storage

Important

The values of storage usage displayed in the product UI are in binary byte units – mebibytes (MiB), gibibytes (GiB), and tebibytes (TiB) – even though the labels show MB, GB, and TB respectively. For example, if the actual usage is 3105886629888 bytes, the value displayed in the UI is correctly shown as 2.82, but is labeled with TB instead of TiB.

- **Cloud resources**

- **Backup storage**

- **Backup storage**

This quota limits the total size of backups that are located in the cloud storage. When the backup storage hard quota is exceeded, the backup operation will not start.

In the **Per workload** billing mode, this quota applies only to backups of workloads that are different from Microsoft 365 and Google Workspace.

The backup storage for Microsoft 365 and Google Workspace workloads is unlimited*. If a seat quota, such as **Microsoft 365 seats** or **Google workspace seats**, is removed from a workload, the backup storage remains unlimited but its usage will be charged.

In the **Per gigabyte** billing mode, this quota applies to all backups, including backups of Microsoft 365 and Google Workspace workloads.

* Fair usage policy for Acronis storage applies. Terms and conditions are available at <https://www.acronis.com/company/licensing/#cyber-cloud-fair-usage>.

- **Archiving storage**

This quota limits the total size of the email archive in the cloud infrastructure.

- **Advanced Disaster Recovery**

This section contains disaster recovery-related quotas.

- **Local resources**

- **Local backup**

The **Local backup** quota limits the total size of backups to local disks, network shares, and public clouds, such as S3 compatible, Azure, AWS, Wasabi, and Impossible Cloud.

- An overage cannot be set for this quota.
- Hard quota cannot be applied for local backups.

Note

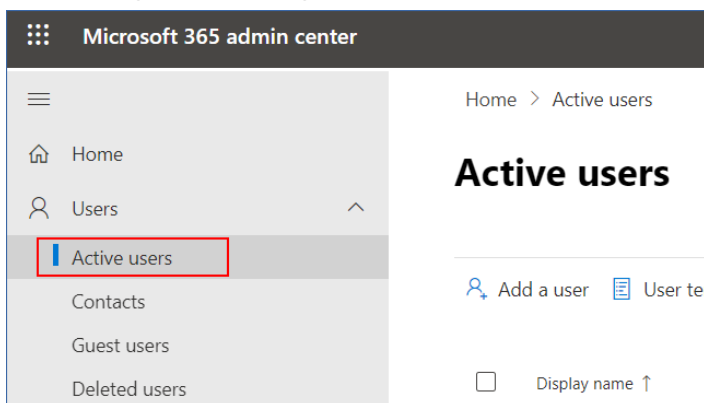
Disabling the **Local backup** quota will disable local backups, backups to network shares, and backups to public clouds.

Preventing unlicensed Microsoft 365 users from signing in

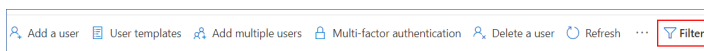
You can prevent all unlicensed users in your Microsoft 365 organization from signing in by editing their sign-in status.

To prevent unlicensed users from signing in

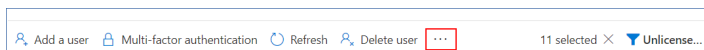
1. Log in to the Microsoft 365 admin center (<https://admin.microsoft.com>) as a global administrator.
2. In the navigation menu, go to **Users > Active Users**.



3. Click **Filter**, and then select **Unlicensed users**.



4. Select the check boxes next to the user names, and then click the ellipsis (...) icon.



5. From the menu, select **Edit sign-in status**.
6. Select the **Block users from signing in** check box, and then click **Save**.

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.

For Disaster Recovery to Microsoft Azure, the following offering items are available:

- **DR and direct backup to Azure**

Enables Advanced Disaster Recovery and direct backup to the customer's Azure subscription. One quota is assigned to each protected workload.

For Disaster Recovery to Cyber Protect Cloud, the following offering items are available:

- **Disaster recovery storage**

The Disaster recovery storage shows the backup storage size of the servers that are protected with disaster recovery. The usage of the Disaster recovery storage equals the usage of the backup storage of the workloads that are protected with disaster recovery servers. This storage is calculated starting from the time when a recovery server is created, regardless of whether the server is currently running. If the overage for this quota is reached, it will not be 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 will not be possible to initiate a failover or 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 Cyber Protect 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.

Administrator accounts are not counted as part of this quota.

- **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**

Defines the maximum cloud storage space for notarized files, signed files, and files whose notarization or signing is in progress.

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

- **Notarizations**

Defines the maximum number of files that can be notarized using the notary service.

A file is considered notarized as soon as it is uploaded to 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**

Defines the maximum number of digital eSignatures.

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 under **My Company**, 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

Important

The values of storage usage displayed in the product UI are in binary byte units – mebibytes (MiB), gibibytes (GiB), and tebibytes (TiB) – even though the labels show MB, GB, and TB respectively. For example, if the actual usage is 3105886629888 bytes, the value displayed in the UI is correctly shown as 2.82, but is labeled with TB instead of TiB.

- **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, the backups fail.

Important

The local agent and the cloud agent consume separate quotas. If you back up the same workloads by using both agents, you will be charged twice. For example:

- If you back up the mailboxes of 120 users by using the local agent, and you back up the OneDrive files of the same users by using the cloud agent, you will be charged for 240 Microsoft 365 seats.
- If you back up the mailboxes of 120 users by using the local agent, and you back up the same mailboxes also by using the cloud agent, you will be charged for 240 Microsoft 365 seats.

File Sync & Share quotas

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

- **Personal storage space**

Defines the allocated cloud storage space for a user's files.

Notary quotas

You can define the following Notary quotas for a user:

- **Notary storage**

Defines the maximum cloud storage space for notarized files, signed files, and files whose notarization or signing is in progress.

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

- **Notarizations**

Defines the maximum number of files that can be notarized using the notary service.

A file is considered notarized as soon as it is uploaded to 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**

Defines the maximum number of digital eSignatures.

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:

- **Your login.** This is the user name that you use to log in. Your login is also shown on the account activation page.
- **Activate account** button. Click the button and set the password for your account. Ensure that your password is at least nine characters long. For more information about the password, see "Password requirements" (p. 19).

Password requirements

Passwords are checked for complexity during user registration and are classified into one of the following categories:

- Weak
- Medium
- Strong

You cannot save a weak password, even though it might be long enough. Passwords that repeat the user name, the login, the user email, or the name of the tenant to which a user account belongs are always considered weak. Most common passwords are also considered weak.

Note

Password requirements are subject to change.

To strengthen a password, add more characters to it. Using different types of characters, such as digits, uppercase and lowercase letters, and special characters, is not mandatory but it results in stronger passwords that are also shorter.

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.

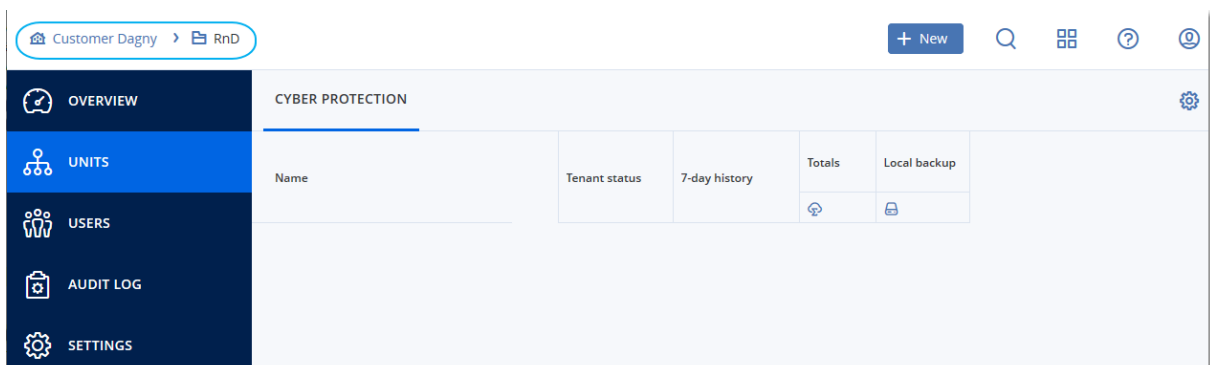
Switching between the management portal and the service consoles

To switch between the management portal and the service consoles, click the  icon in the upper-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 upper-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

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

- Company administrator account — to share the management duties with other people.
- Unit administrator accounts — to delegate the service management to other people whose access permissions will be strictly limited to the corresponding unit.
- User accounts within the customer or a unit tenant — 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 upper-right corner, click **New > User**.
Alternatively, go to **My Company > Users**, and click **+ New**.
4. Specify the following contact information for the account:
 - . If you prefer to use a login that is different from the email, select the check box **Use login that is different from email**, and then enter **Login** and **Email**.

Important

If the user is registered in the File Sync & Share service, please provide the email that was used for the File Sync & Share registration.

Please note that each customer user account must have a unique email address.

Important

Each account must have a unique login.

- [Optional] **First name**
 - [Optional] **Last name**
 - In the **Language** field, change the default language of notifications, reports, and the software that will be used for this account.
5. [Optional] Specify the company contacts.
- **Billing**—the contact that will get updates about important changes in usage reporting in the platform.
 - **Technical**—the contact that will get updates about important technical changes in the platform.
 - **Business**—the contact that will get updates about important business-related changes in the platform.

You can assign more than one company contact to a user.

You can view the assigned company contacts for a user in the **Users** list, in column **Company contacts**, and edit the user account to change the company contacts if needed.

6. [Not available when creating an account in a partner / folder tenant] Select the services to which the user will have access and the roles in each service.
- Available services depend on the services that are enabled for the tenant in which the user account is created.


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

7. Click **Create**.

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

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

To reset a user's password


1. In the management portal, go to **My Company > 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.

The account can now be used for services that do not support two-factor authentication (for example, registration in Cyber Infrastructure), you may need to convert a user account into a *Service account* — an account that does not require two-factor authentication.

For services that do not support two-factor authentication (for example, registration in Cyber Infrastructure), you might need to convert a user account to a service account. The service account does not require two-factor authentication.

To convert a user account to a service account

1. In the management portal, go to **My Company > Users**.
2. Select the user whose account you want to convert to the service account type, and then click the ellipsis icon  > **Mark as service account**.
3. In the confirmation window, enter the two-factor authentication code and confirm your action.

The account can now be used for services that do not support two-factor authentication.

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.

Note

The services that are available to you are configured by your service provider.

Service	Role	Description
n/a	Company administrator	This role grants full administrator rights for all services. This role grants access to the corporate allowlist. If the Disaster Recovery add-on to the Protection service is enabled for the company, this role also grants access to the disaster recovery functionality.
	Unit administrator Unit level	This role grants highest possible permissions to all applicable services in the unit. The role does not provide access to the disaster recovery functionality.
Management Portal	Administrator	This role grants access to the management portal where the administrator can manage users within the entire organization.
	Read-only administrator	This role provides read-only access to all objects in the Management Portal of the entire company. See "Read-only administrator role" (p. 27).

	Read-only administrator Unit level	This role provides read-only access to all objects in the Management Portal of the company unit and sub-units. See "Read-only administrator role" (p. 27).
Vendor Portal	Developer	This role provides full access to Vendor Portal. Developers can create and manage CyberApps, CyberApp Descriptions, and CyberApp Versions. They can also submit deployment requests and monitor CyberApp metrics.
	User	This role allows the user to create, manage, and request approvals of CyberApp Descriptions.
	Read-only user	This role provides read-only access to Vendor Portal.

Protection	
------------	--

	Administrator	<p>This role enables configuring and managing the Protection service for your customers.</p> <p>This role is required for:</p> <ul style="list-style-type: none"> • configuring and managing the Disaster Recovery functionality. • configuring and managing the corporate allowlist. • performing autodiscovery of devices. • performing all actions related to software deployment by using DeployPilot (working with software deployment plans, software repositories, software packages, and performing quick deploy actions).
	Cyber administrator	<p>In addition to the rights of the Administrator role, this role enables configuring and managing the Protection service, and approving actions in Cyber Scripting.</p> <p>The Cyber administrator role is only available for tenants with enabled RMM pack.</p>
	Read-only administrator	The role provides read-only access to all objects of the Protection service. See "Read-only administrator role" (p. 27).
	User	This role enables using the Protection service but without administrative privileges. Access is provided to functionality such as Endpoint Detection and Response, but users assigned this role cannot access the data of other users in the organization.
	Restore operator	Applicable to Microsoft 365 and Google Workspace organizations, the role provides access to backups and allows their recovery, while restricting the access to sensitive content inside the backups. See "Restore operator role" (p. 28).
	Security Analyst	The role can be assigned only in customer tenants for which the Advanced Security + EDR or Advanced Security + XDR pack is enabled. It provides access to the Cyber Protection console and enables the user to manage EDR incidents and perform response actions.
	DR support operator	This role provides read-only access to all objects of the Protection service in the organization and

		access to Disaster Recovery environment and allows to perform advanced troubleshooting.
File Sync & Share	Administrator	This role enables configuring and managing File Sync & Share for your users.
Cyber Infrastructure	Administrator	This role enables configuring and managing Cyber Infrastructure for your users.
Notary	Administrator	This role enables configuring and managing Notary for your users.
	User	This role enables using the Notary service but without administrative privileges. Such users cannot access data of other users of the organization.

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

Read-only administrator role

An account with this role has read-only access to the Cyber Protect console and can do the following:

- 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.
- When Advanced security + XDR is enabled, read-only administrators can access the Response Actions tab in the EDR incident screen, but cannot execute any actions.
- Access data of other users of the organization in the read-only mode.

A read-only administrator cannot do the following:

- Start or stop any tasks.
For example, a read-only administrator cannot start a recovery or stop a running backup.
- Configure and manage the Disaster Recovery functionality or the corporate allowlist, and has a read-only access to software deployment plans, software repositories, and software packages.
- 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 or delete, update, and rebuild search indexes for cloud-to-cloud backups.

Note

In the Management portal, read-only administrators can initiate the creation of new child tenants and configure all their properties for demonstration purposes, but cannot save them.

- Save any changes to scripting plans, monitoring plans, or agent plans.

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.

Restore operator role

Note

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

A restore operator can do the following:

- View alerts and activities.
- View and refresh the list of backups.
- View the list of recovery points.
- Browse backups without accessing their content.

Note

Restore operators can see the names of backed-up files and the subjects and senders of backed-up emails.

- Search backups (full text search is not supported).
- Recover cloud-to-cloud backups only to their original location 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.
- 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.
- Recover cloud-to-cloud backups to non-original locations, such as a different mailbox, OneDrive, Google Drive, or Microsoft 365 Team.

Changing the notification settings for a user

You can configure which notifications a user will receive by email, if the Cyber Protection service is enabled for the tenant where the user is created.

To configure the notifications for a user

1. Navigate to **My Company > Users**.
2. Click the user for which you want to configure the notifications, and then, on the **Services** tab, in the **Email notifications** section, click the pencil icon.
3. Select the checkboxes for the email notifications that you want to enable.

Notifications	Description
Maintenance notifications	Notifications that inform partner users, child tenants (partners, and customers), and individual users about upcoming maintenance activities on the Cyber Protect data center. These notifications can be enabled by partner users for their child tenants, and by partner users or company administrators for individual users within their organization.
Quota overuse notifications	Notifications about exceeded quotas.
Scheduled usage reports	Usage reports that are sent on the first day of each month.
URL branding notifications	Notifications about the upcoming expiration of the certificate used for the custom URL for the Cyber Protect Cloud services. The notifications are sent to all administrators of the selected tenant - 30 days, 15 days, 7 days, 3 days, and 1 day prior the expiration of the certificate.
Countdown to production switch notifications	Notifications about the customer trial expiration that will be sent 10 days before the trial expires and 3 days before the trial expires.
Production mode activation notification	Notifications about the activation of production mode.
Failure notifications	Notifications about the execution results of protection plans and the results of disaster recovery operations for each device.

Notifications	Description
Warning notifications	Notifications about the execution results of protection plans and the results of disaster recovery operations for each device.
Success notifications	Notifications about the execution results of protection plans and the results of disaster recovery operations for each device.
Daily recap about active alerts	The daily recap is generated based on the list of active alerts that are present in the Cyber Protect 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	Notifications about attempts to use peripheral devices and ports that are restricted by protection plans with the device control module enabled.
Notifications about newly discovered devices	Notifications about newly discovered devices. These notifications are sent every Monday and Thursday.
Recovery notifications	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.
Data loss prevention notifications	Notifications about data loss prevention alerts related to the activity of this user on the network.
Security incident notifications	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. There are two options available: Mitigated and Not mitigated . These options are relevant for Endpoint Detection and Response (EDR) incident alerts, EDR alerts from threat feeds, and individual alerts (for workloads that do not have EDR enabled on them). When an EDR alert is created, an email is sent to the relevant user. If the threat status of the incident changes, a new email is sent. The emails

Notifications	Description
	include action buttons that enable the user to see details of the incident (if it was mitigated), or to investigate and remediate the incident (if it was not mitigated).
Infrastructure notifications	Notifications about issues with the Disaster Recovery infrastructure: when the Disaster Recovery infrastructure is unavailable, or the VPN tunnels are unavailable.

Note

VMware Cloud Director users can receive the following notifications: quota overuse notifications, scheduled usage reports (if such reports are configured for the organization), and daily recap about active alerts.

Default notification settings enabled by notification type and user role

The notifications that are enabled or disabled by default depend on the notification type and user role.

Notification type\User role	Customer, unit administrators (Self-service)	Customer, unit administrators (Managed by Service Provider)
Maintenance notifications	No	No
Quota overuse notifications	Yes	No
Scheduled usage reports notifications	Yes	No
URL branding notifications	No	No
Failure notifications	No	No
Warning notifications	No	No
Success notifications	No	No
Daily recap about active alerts	Yes	No
Device Control notifications	No	No
Recovery notifications	No	No
Data Loss Prevention notifications	No	No
Security incident notifications: Mitigated	No	No

Security incident notifications: Not mitigated	No	No
Infrastructure notifications	No	No


Notifications enabled by default per device type and user role

Device type\User role	User	Customer Administrator
Notifications for own devices	Yes	Yes
Notifications for all devices in the organization	n/a	Yes
Notifications for Microsoft 365, Google Workspace, and other cloud-based backups	n/a	Yes

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.

Note

All devices associated to the disabled user will no longer be protected because no quota will be applied to them. To continue the protection of these devices, reassign them to an active user.

To enable a disabled user account

1. In the management portal, go to **Users**.
2. Select the disabled user 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.

Note

You can reuse the login of a deleted user after you delete the user.

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](#).

To delete a user account

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

As a result:

- All notifications configured for this account will be disabled.
- All data that belongs to this user account will be deleted.
- The administrator will not be able to access the management portal.
- All backups of workloads associated with this user will be deleted.
- All machines associated with this user account will be unregistered.
- All protection plans will be revoked from all workloads associated with this user.
- All File Sync & Share data that belongs to this user (for example, files and folders) will be deleted.
- Notary data that belongs to this user (for example, notarized files, eSigned files) will be deleted.
- You will see the user **Status** as **Deleted**. When you hover over the **Deleted** status, you will see the date when the user was deleted and the note that you can still recover all relevant user data and settings within 30 days of this deletion date.

Transferring ownership of a user account

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

Important

You cannot reassign the content of a deleted account.

To transfer the ownership of a user account:

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



> **Reset password**.

7. Confirm your action by clicking **Reset**.
8. Let the future account owner reset the password by following the instructions sent to their email address.

The new owner can now access this account.

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.

Note

For partner tenants in production mode, two-factor authentication is enabled by default and cannot be disabled.

For customer tenants, two-factor authentication is optional and can be disabled.

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>)
Android version (<https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2>)
 - Microsoft Authenticator
iOS app version (<https://apps.apple.com/app/microsoft-authenticator/id983156458>)
Android version (<https://play.google.com/store/apps/details?id=com.azure.authenticator>)

Important

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

3. Your organization users must re-log in to the system.
4. After entering their login and password, they will be prompted to set up two-factor authentication for their user account.
5. They must scan the QR code by using their authentication application. If the QR code cannot be scanned, they can use the 32-digit code 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 temporary one-time password (TOTP) secret, use the application that supports backing up codes in a cloud). You will need the temporary one-time password (TOTP) to reset two-factor authentication in case of lost second-factor device.

6. The temporary one-time password (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** window 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.

To restore two-factor authentication on a new device

If you have access to the previously set-up mobile authentication app:

1. Install an authenticator app on your new device.
2. Use the PDF file that you saved when you set up 2FA on your device. This file contains the 32-digit code that has to be entered in the authenticator app to link the authenticator app again to your Acronis account.

Important

If the code is correct but it is not working, make sure to sync the time in the authenticator mobile app.

3. If you missed saving the PDF file during the setup:
 - a. Click **Reset 2FA** and enter the one-time password shown in the previously set-up mobile authenticator app.
 - b. Follow the on-screen instructions.

If you have no access to previously set-up mobile authenticator app:

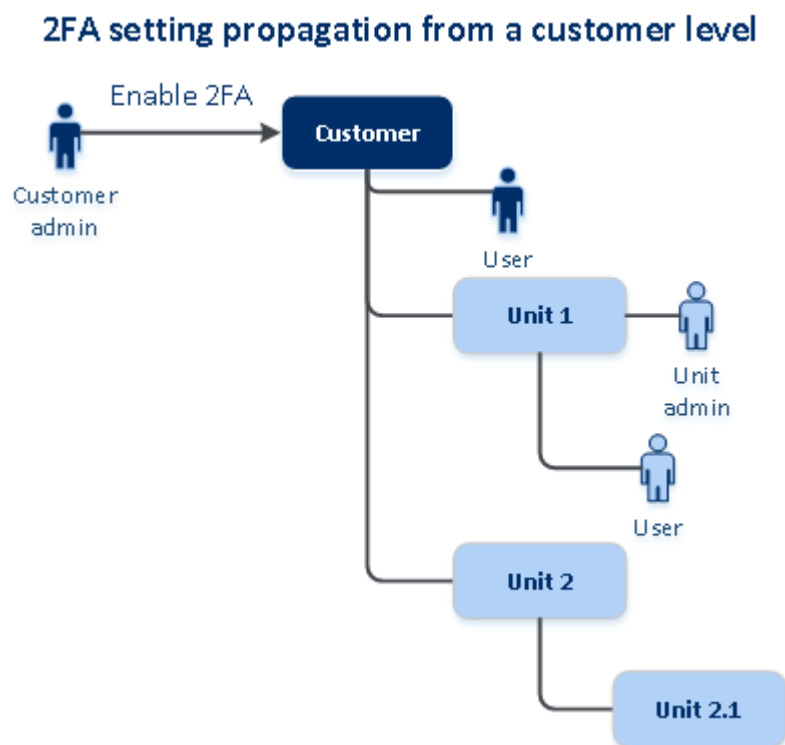
1. Take a new mobile device.
2. Use the stored PDF file to link a new device (default name of the file is cyberprotect-2fa-backupcode.pdf).
3. Restore access to your account from backup. Ensure that backups are supported by your mobile app.
4. Open the app under the same account from another mobile device if it is supported by the app.

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.



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 tenants

As a Company administrator, you can enable two-factor authentication for users in your organization.

To enable two-factor authentication

Required role: Company administrator

1. Log in to the management portal.
2. Go to **Settings > Security**.
3. 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 **My Company > 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

Required role: Company administrator

1. Log in to the management portal.
2. Go to **Settings > Security**.
3. To disable two-factor authentication, turn off the toggle, and then click **Disable**.
4. [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 the 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 **My Company > Users** tab, the **2FA status** column will be hidden.

Managing two-factor authentication for users

You can monitor two-factor authentication settings for all your users and reset the settings in the management portal, under **My Company > Users** tab.

Monitoring

In the management portal, under **My Company > Users**, you can see a list of all users in your organization. The **2FA status** indicates if the two-factor configuration is set up for a user.

To reset the two-factor authentication for a user

1. In the management portal, go to **My Company > Users**.
2. On the **Users** tab, find a user for whom you want to change the settings, and then click the ellipsis icon.
3. Click **Reset two-factor authentication**.
4. 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, go to **My Company > Users**.
2. On the **Users** tab, find a user for whom you want to change the settings, and then click the ellipsis icon.
3. Click **Reset all trusted browsers**.
4. 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, go to **My Company > Users**.
2. On the **Users** tab, find a user for whom you want to change the settings, and then click the ellipsis icon.
3. Click **Mark as service account**. As a result, a user gets a special two-factor authentication status called **Service account**.
4. [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, go to **My Company > Users**.
2. On the **Users** tab, find a user for whom you want to change the settings, and then click the ellipsis icon.
3. 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:

Parameter	Entering the password	Entering the TOTP code
Attempt limit	10	5
Attempt limit period (the limit is reset after timeout)	15 min (900 sec)	15 min (900 sec)

Lockout happens on	Attempt limit + 1 (11th attempt)	Attempt limit
Lockout period	5 min (300 sec)	5 min (300 sec)

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

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

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

Configuring the updates of the Cyber Protection agent

Important

You can access the agent update management functionality if you have the Protection service enabled.

This procedure applies to the updates of the following Cyber Protection agents: Agent for Windows, Agent for Linux, Agent for Mac, and Cyber Files Cloud Agent for File Sync & Share.

Cyber Files Cloud has a Windows version and a MacOS version of the desktop Agent for File Sync & Share, which allows synchronization of files and folders between a machine and a user's File Sync & Share cloud storage area to promote offline working, as well as WFH (Work From Home) and BYOD (Bring Your Own Device) working practices.

To facilitate the management of multiple workloads, you can configure manual or automatic, unattended updates for all agents on all machines or on individual machines.

Note

To manage agents on individual machines and customize auto-update settings from the Cyber Protect console, see section [Updating Agents](#) in the [Cyber Protect User Guide](#).

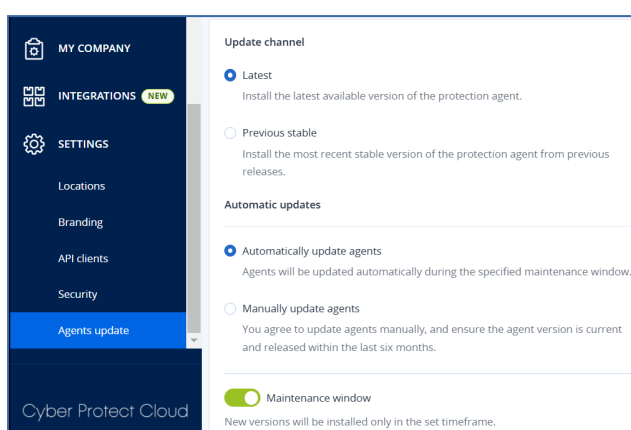
Automatic updates

Note

If you do not have the Protection service enabled, the settings for automatic updates of Agent for File Sync & Share are inherited from your service provider.

To configure the default settings for automatic updates of agents in Management Portal

1. Select **Settings > Agents update**.



2. Under **Update channel**, select which version to use for automatic updates.

Option	Description
Latest (selected by default)	Install the latest available version of the Cyber Protection agent.
Previous stable	Install the most recent stable version of the Cyber Protection agent from previous releases.

3. Verify that the option **Automatically update agents** is switched on.

Note

Automatic updates are only available for the following agents:

- Cyber Protect agent versions 26986 (released in May 2021) or later.
- Desktop Agent for File Sync & Share, version 15.0.30370 or later.

Older agents must be updated manually to the latest version before automatic updates can take effect.

4. [Optional] Set the maintenance window.

The default window is daily, from 23:00 to 08:00 on the machine where the agent is installed.

Note

Although agent updates are fast and seamless, we recommend that you choose a time frame that will cause minimum disruption for users, because users cannot prevent or postpone automatic updates.

5. Click **Save**.

Manual updates

Important

We strongly recommend that you enable automatic updates for your agents. Regular updates ensure your agents stay up to date, offering improved performance, bug fixes, and enhanced protection and security features.

To configure the default settings for manual updates of agents in Management Portal

1. Go to **Settings > Agents update**.
2. Under **Update channel**, select which version to use for automatic updates.

Option	Description
Latest (selected by default)	Install the latest available version of the Cyber Protection agent.
Previous stable	Install the most recent stable version of the Cyber Protection agent from previous releases.

3. Select **Manually update agents**.

Update channel

☒ Latest
Install the latest available version of the protection agent.

☐ Previous stable
Install the most recent stable version of the protection agent from previous releases.

Automatic updates

☐ Automatically update agents
Agents will be updated automatically during the specified maintenance window.

☒ Manually update agents
You agree to update agents manually, and ensure the agent version is current and released within the last six months.

☒ Enforce automatic updates for unsupported versions
Agents older than 6 months will be updated automatically during the specified maintenance window.

☒ Maintenance window
New versions will be installed only in the set timeframe.

From

To

4. [Optional] To prevent security risks, ensure access to the latest features, and minimize the technical issues caused by significantly outdated agents, enable the automated updates of agents that are older than 6 months.

- a. Select **Enforce automatic updates for unsupported versions**.

Important

If you have not enabled the automated updates of agents before the C25.02 release, this option will be enabled automatically for all tenants in your environment.

- b. [Optional] Set the maintenance window.

The default maintenance window is daily, from 23:00 to 08:00 on the machine where the agent is installed.

Note

Although agent updates are fast and seamless, we recommend that you choose a time frame that will cause minimum disruption for users, because users cannot prevent or postpone automatic updates.

5. Click **Save**.

Monitoring the agent updates

Important

Agent updates can only be monitored if you have the Protection module enabled.

To monitor agent updates, see sections [Alerts](#) and [Activities](#) of the [Cyber Protect User Guide](#).

Immutable storage

Immutable storage is a type of data storage that prevents backups from being altered, modified, or deleted for a defined period. It ensures that the data remains secure and tamper-proof, providing an extra layer of protection against unauthorized or unintended modification or ransomware attacks. Immutable storage is available for all cloud backups stored in a supported cloud storage instance. See "Supported storages and agents" (p. 44).

With immutable storage, you can access deleted backups during the specified retention period. You can recover content from these backups, but you cannot change, move, or delete them. When the retention period ends, the deleted backups are permanently deleted.

The immutable storage contains the following backups:

- Backups that are deleted manually.
- Backups that are deleted automatically, according to the settings in the **How long to keep** section in a protection plan or the **Retention rules** section in a cleanup plan.

Deleted backups in the immutable storage still use storage space and are charged accordingly.

Deleted tenants are not charged for any storage, including immutable storage.

Immutable storage modes

A Customer administrator can disable and re-enable immutable storage, and change its mode and retention period.

Immutable storage is available in the following modes:

- **Governance mode**

You can disable and re-enable the immutable storage. You can change the retention period or switch to Compliance mode.

Note

Starting in September 2024, immutable storage Governance mode with a retention period of 14 days might be enabled for your company automatically. Check with your service provider for details.

- **Compliance mode**

Warning!

Selecting Compliance mode is irreversible.

You cannot disable the immutable storage. You cannot change the retention period and cannot switch back to Governance mode.

Supported storages and agents

- Immutable storage is supported only on the cloud storage.
 - Immutable storage is available for Acronis-hosted and Partner-hosted cloud storages that use Cyber Infrastructure version 4.7.1 or later.
 - All storages that can be used with Cyber Infrastructure Backup Gateway are supported. For example, Cyber Infrastructure storage, Amazon S3 and EC2 storages, and Microsoft Azure storage.
 - Immutable storage requires that TCP port 40440 is open for the Backup Gateway service in Cyber Infrastructure. In version 4.7.1 and later, TCP port 40440 is automatically opened with the **Backup (ABGW) public** traffic type. For more information about the traffic types, see [Acronis Cyber Infrastructure documentation](#).
- Immutable storage requires a protection agent version 21.12 (build 15.0.28532) or later.
- Only TIBX (Version 12) backups are supported.

Configuring immutable storage

After September 2024, immutable storage Governance mode, with a retention period of 14 days, is enabled by default. You can modify the default settings for your organization, if needed.

Note

To allow access to deleted backups, port 40440 on the backup storage should be enabled for incoming connections.

To change the retention period or the mode of immutable storage

1. Log in to the management portal as an administrator, and then go to **Settings > Security**.
2. Verify that the **Immutable storage** switch is on.
3. Specify a retention period within the range of 14 to 3650 days.
The default retention period is 14 days. A longer retention period will result in increased storage usage.
4. Select the immutable storage mode and, if prompted, confirm your choice.
 - **Governance mode**
This mode ensures that ransomware or malicious actors cannot tamper with or erase backup data, because all deleted backups are kept in the immutable storage for the retention period that you specified. It also guarantees the integrity of backup data, which is critical for disaster recovery.
In this mode, you can disable and re-enable the immutable storage, change the retention period, or switch to Compliance mode.
 - **Compliance mode**
In addition to the benefits of the Governance mode, the Compliance mode helps organizations meet the regulatory requirements for data retention and security by preventing data tampering.

Warning!

Selecting Compliance mode is irreversible. After selecting this mode, you cannot disable the immutable storage, change the retention period, or switch back to Governance mode.

5. Click **Save**.

Warning!

Selecting **Compliance mode** is irreversible. After you select this mode, you will not be allowed to disable the immutable storage, or change its mode or retention period.

6. To add an existing archive to the immutable storage, create a new backup in that archive by running the corresponding protection plan manually or on a schedule.

Warning!

If you delete a backup before adding the archive to the immutable storage, the backup is deleted permanently.

To disable immutable storage

1. Log in to the management portal as an administrator, and then go to **Settings > Security**.
2. Disable the **Immutable storage** switch.

Note

You can disable immutable storage only in Governance mode.

Warning!

Disabling the immutable storage does not come into effect immediately. During a grace period of 14 days (336 hours), you can access the deleted backups according to their original retention period.

When the grace period ends, all backups in the immutable storage are permanently deleted. For example, if you disable the immutable storage on October 1 at 10:00 AM, all backups that are still in the immutable storage on October 15 at 10:00 AM will be permanently deleted.

3. Confirm your choice by clicking **Disable**.

Viewing immutable storage usage

You can view how much space the immutable storage uses in the Cyber Protect console or in the **Current usage** report that you can generate in Management Portal.

Limitations

- The reported value includes the total size of all deleted backups and the metadata of the backup archives in the storage. The metadata can be up to 10% of the reported value.
- The value shows usage data from up to 24 hours ago.
- If the actual usage is less than 0.01 GB, it is shown as 0.0 GB.

To view the immutable storage usage

In the Cyber Protect console

1. Log in to the Cyber Protect console.
2. Go to **Backup storage > Backups**, and then select a cloud storage location that supports immutable storage.
3. Check the **Immutable storage and metadata** column.

In the Current usage report

1. Log in to Management Portal as administrator.
2. Go to **Reports > Usage**.
3. Select **Current usage**, and then click **Generate and send**.
A report in CSV and HTML format is sent to your email address.
The HTML file is included in a ZIP archive.
4. In the report, check the **Metric name** column.
You can see the immutable storage usage in the **Cloud storage - Immutable** row.

Billing example for immutable storage

The example below shows a deleted backup that goes to the immutable storage for 14 days, which is the default retention period. During this period, the deleted backup uses storage space. When the retention period ends, the deleted backup is permanently deleted and storage usage decreases. Every month, the storage usage is charged accordingly.

Date	Backups	Storage usage	Billing
April, 1	Backup A (10 GB) is created Backup B (1 GB) is created	10 GB + 1 GB = 11 GB	
April, 20	Backup B is deleted, goes to Immutable storage (with retention period of 14 days)	10 GB + 1 GB = 11 GB	
April, 30			Billed 11 GB for April
May, 4	Backup B is permanently deleted because the retention period ended	11 GB - 1 GB = 10 GB	
May, 31			Billed 10 GB for May

Enabling the Advanced Security Awareness Training for users in your organization

The Security Awareness Training is provided by a third-party vendor, Wizer, as an integration in the Cyber Protect Cloud console. If your service provider has enabled the service for your organization, you must enable the integration to allow your users to access the training materials.

To enable the integration with Wizer for an Organization

Required role: Customer Administrator, Protection Administrator, or Cyber Administrator.

Note

This initial configuration is performed only once.

1. Log in to the Cyber Protect Cloud console.
2. In the navigation menu, click **Security Awareness Training > Awareness dashboard**.
3. Click **Enable integration**.
4. Click **Enable** to confirm.

Once the integration is enabled, a new tenant for the organization is provisioned in the Wizer platform. If you already have an account in Wizer and want to use that account instead of a new tenant, please contact your service provider.

You can access the Wizer Admin Panel and add users manually, by importing a CSV file, or by configuring SSO with Active Directory, Octa, Google, or another identity provider. See [How to add users](#).

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.

Important

Enabling login control prevents recovery from cloud storage by using unregistered bootable media. See [this KB article](#).

Note

- This restriction also applies to accessing the Management Portal [via API](#).
 - This restriction applies only at the level where it is set. It is not applied to members of the child tenants.
-

To limit access to the web interface

1. Log in to Management Portal.
2. [Navigate to the unit](#) for which you want to limit the access.
3. Click **Settings** > **Security**.
4. Enable the **Login control** switch.
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

You can limit access to your company for higher-level administrators.

If you, as Management Portal administrator, limit access to your company, administrators of your service provider partner can only modify your company's properties and quotas, and get usage reports for your company and your customers. They will not be able to access:

- Anything inside your tenant.
- Your customers, their users, services, backups, and other resources.

To limit access to your company

1. Log in to Management Portal.
2. Click **Settings** > **Security**.
3. Disable the **Support access** option.

Task management

If your account includes access to the Advanced Automation (PSA) service, click **Task management** to view and manage your service desk tickets.

Note

Users assigned with the Client manager role in Advanced Automation (PSA) can view and manage all service desk tickets within the organization; users assigned the Client role can only view and update their own tickets.

Viewing service desk tickets

To view existing service desk tickets, in the management portal go to **Task management > Service desk**. Information about each ticket is displayed, including:

- A link to the ticket.
- The ticket's current status.
- The total time spent on the ticket.
- The requestor of the ticket.
- The customer.
- The ticket's priority.
- The assigned support agent.
- The assigned service level agreement (SLA), when the SLA will be breached, and when to expect the next update from a ticket engineer.
- The date the ticket was last updated.

To export ticket data, click **Export**. An XSL file called **Tickets** is downloaded to your workload.

You can also filter and sort the displayed list to locate a specific ticket; for more advanced filtering, use the **Filter** tool to define which tickets should be displayed.

Filter <input type="text" value="Search"/>										
Quick filters: <input checked="" type="checkbox"/> My tickets <input type="checkbox"/> Closed <input type="checkbox"/> SLA breach <input type="checkbox"/> Unassigned tickets										
<input type="checkbox"/> Ticket ID	<input type="checkbox"/> Status	<input type="checkbox"/> Title	<input type="checkbox"/> Total time spent	<input type="checkbox"/> Requestor	<input type="checkbox"/> Customer	<input type="checkbox"/> Priority	<input type="checkbox"/> Support agent	<input type="checkbox"/> SLA	<input type="checkbox"/> SLA breach	<input type="checkbox"/> Last update
<input type="checkbox"/> 20160929-4	Activities scheduled	Workstation crashes	0 h 0 min	Olivia Brewer	Acme Corporation	High	Jane Cooper	24/7 SLA - all-in	15 Oct 2021, 11:26:35	15 Oct 2021, 11:26:35
<input type="checkbox"/> 20160929-5	In progress	Laptop was stolen	0 h 0 min	John Adams	Acme Corporation	Medium	Jane Cooper	24/7 SLA - all-in	10 Oct 2021, 11:26:35	10 Oct 2021, 11:26:35
<input type="checkbox"/> 20160929-6	New	Please help me	0 h 0 min	Silvester Hebert	Acme Corporation	Normal	Jane Cooper	Default SLA	10 Oct 2021, 11:16:35	10 Oct 2021, 11:16:35
<input type="checkbox"/> 20160929-7	New	Please upgrade my Office in...	0 h 0 min	Scott Cosgrove	Acme Corporation	Normal	Cameron Williamson	24/7 SLA - all-in	10 Oct 2021, 10:26:35	10 Oct 2021, 10:26:35
<input type="checkbox"/> 20160929-8	Waiting for response	Malware infection	0 h 0 min	Janet Fitzgerald	Acme Corporation	Low	Cameron Williamson	vFixed Price SLA - weekdays	9 Oct 2021, 11:26:35	9 Oct 2021, 11:26:35

Creating a service desk ticket

To create a new ticket

1. Go to **Task management > Service desk**. A list of open tickets is displayed.

Note

Users assigned with the Client manager role in Advanced Automation (PSA) will see all service desk tickets within the organization; users assigned the Client role will see only their own tickets.

2. Click **+ New**. The Create new ticket dialog is displayed.
3. Define the following:
 - In the **Ticket title** field, add the title for the ticket.
 - In the **Requestor** field (only enabled for users with the Client manager role), select the relevant user from the customer's list of active users and contacts. Note that the **Customer name** field is disabled for both Client manager and Client users.
 - (Optional) In the **Phone number** field, add a relevant phone number. Note that if you update the default number displayed, the new number is stored as that user's default phone number.
 - In the **Superior** field, select the relevant user from the list of active customer users (for example, users assigned the Client manager role).
 - In the **Configuration item or service** section, select one of **Managed service** or **IT service**:
 - **Managed service**: This option is selected and pre-filled with the relevant details if the Managed service product type is available in the relevant contract. Note that if there are no Managed service product types in the contract, this option is disabled.
 - **IT service**: This option is selected and pre-filled with the relevant details if the IT service product type is available in the relevant contract. Note that if there are no IT service product types in the contract, this option is disabled.
 - The **Configuration item** field shows devices that are linked to the selected Managed or IT service (**Unknown CI** is shown if the device is unknown); selecting a device after selecting a service is optional (when you select a device in this scenario, the SLA does not change but remains the SLA that belongs to the service).

Note

The listed devices include those provided by Cyber Protect. If Cyber Protection provides a remote control option for a listed device, you can connect remotely from the ticket using the RDP protocol or HTML5 client.

- You can also select a category in the **Category** field, and define a priority in the **Priority** field. The **SLA** field indicates the SLA agreement with your managed service provider.
- In the **Ticket update** section, you can add recipients in the **To** and **Cc** fields. You can also add rich text descriptions and comments (including images and other media files, up to a maximum of 25 MB; the supported formats and types are listed below under the **Attachments** section) in the displayed text box. Note that the ticket status is set to **New** by default and cannot be changed.
- Click to enable the **Send email to requestor** option switch to ensure any ticket updates will be emailed to the requestor. Note that when recipients are also added to the **To** and **Cc** fields,

notifications are only sent to these recipients when the ticket is updated, not when it is created.

- In the **Attachments** section, click (or drag and drop) to add any relevant attachments. Attachments can include any of the following formats and types (up to a maximum of 25 MB):
 - Media: .avi, .mp4, .mp3
 - Emails: .eml, .msg
 - Images: .png, .gif, .jpeg, .jpg, .heic, .bmp, .tiff, .svg
 - Document and log files: .doc, .docx, .xls, .xlsx, .ppt, .pptx, .txt, .log, .pdf
 - Archives: .zip, .rar

4. Click **Done**. When the ticket is generated, it is added to the list of open tickets.

Updating service desk tickets

To update a ticket

1. Go to **Task management > Service desk**. A list of currently open tickets is displayed.

Note

Users assigned with the Client manager role in Advanced Automation (PSA) will see all service desk tickets within the organization; users assigned the Client role will see only their own tickets.

2. (Optional) If you have a large number of tickets, use the filter to locate the relevant ticket(s). Click **Filter** (or **Saved filters** if you have previously defined a filter), and select the relevant values from the displayed fields. Note that you can click the **Add to Saved filters** option switch to save the defined filter for future use.

Alternatively, use the **Search** bar to locate the relevant ticket(s).

3. Click the relevant ticket row link and modify as required in the displayed tabs:
 - **Activities**: Displays recent activity on the ticket, including the current status, and comments made on the ticket.

Note

If you change the status of a ticket that was created by an alert in the Cyber Protect console to **Closed**, the alert in the Cyber Protect console is also closed.

- **Overview**: Displays general ticket settings that can be modified as required; for more information, see "Creating a service desk ticket" (p. 50).

Note that in this tab you can change the status of the ticket; for example, change it to **In progress** when you start working on it, or move it to **Closed** when it can be closed. You can also change devices linked to a ticket; for example, if a ticket is created that does not include the correct device, you can click on the **Configuration item** drop-down list to select the relevant device.

For more information about the various fields available when editing a ticket, see "Creating a service desk ticket" (p. 50).

4. Click **Save changes**.

Note that if the **Send email to requestor** toggle switch is enabled, an email is sent to the relevant user, and any recipients defined in the **To** and **Cc** fields.

Submitting service desk tickets via the ticket portal

The portal for submitting tickets enables customers to report issues or request support by submitting a simple, publicly available form, without registering or signing in to the system.

When submitted, a new ticket is created and assigned automatically to a support agent of the provider.

Note

The form is enabled or disabled by the provider, and can be accessed by registered or non-registered users. Note that the provider can also choose to restrict and not process requests from unregistered users.

To submit a ticket via the public ticket portal

1. Navigate to the public ticket portal URL shared by the provider.
2. In the Create new ticket dialog, define the following:
 - In the **Ticket title** field, add the title for the ticket.
 - In the **Email address** field, add your email address.

If the email address is recognized by the system, or the provider has selected not to restrict requests from unregistered users, the ticket will be created.

If the email address is not recognized, and the provider has selected to not process requests from unregistered users, the ticket will not be created.
 - [Optional] In the **Phone number** field, add a relevant phone number.
 - In the **Ticket details** section, add a description and comments (including images and other media files, up to a maximum of 25 MB; the supported formats and types are listed under the **Attachments** section) in the displayed text box.
 - [Optional] In the **Attachments** section, click (or drag and drop) to add any relevant attachments.

Attachments can include any of the following formats and types (up to a maximum of 25 MB):

 - Media: .avi, .mp4, .mp3
 - Emails: .eml, .msg
 - Images: .png, .gif, .jpeg, .jpg, .heic, .bmp, .tiff, .svg
 - Document and log files: .doc, .docx, .xls, .xlsx, .ppt, .pptx, .txt, .log, .pdf
 - Archives: .zip, .rar
3. Click **Submit**.

A confirmation message that your ticket was created is displayed. You will also be notified by email that a ticket was created.

Monitoring

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

Usage

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

The usage data includes both standard features and advanced features.

Important

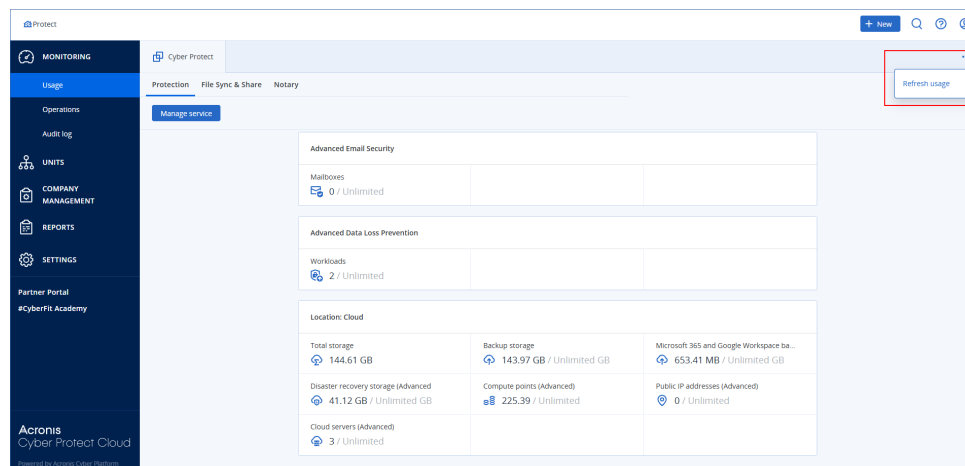
The values of storage usage displayed in the product UI are in binary byte units – mebibytes (MiB), gibibytes (GiB), and tebibytes (TiB) – even though the labels show MB, GB, and TB respectively. For example, if the actual usage is 3105886629888 bytes, the value displayed in the UI is correctly shown as 2.82, but is labeled with TB instead of TiB.

The storage usage for Microsoft 365 and Google Workspace workloads is reported separately from the general backup storage, and is shown under the section **Microsoft 365 and Google Workspace backups**.

To refresh the usage data that is displayed on the tab, click the ellipsis icon (...) in the upper-right of the screen, and then select **Refresh usage**.

Note

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



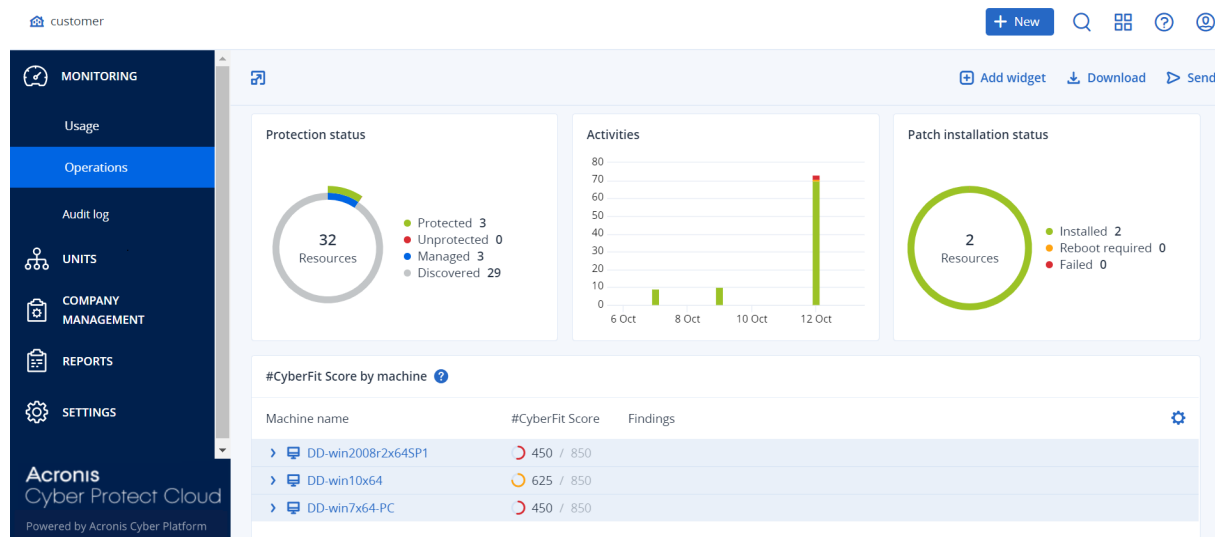
Operations dashboard

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

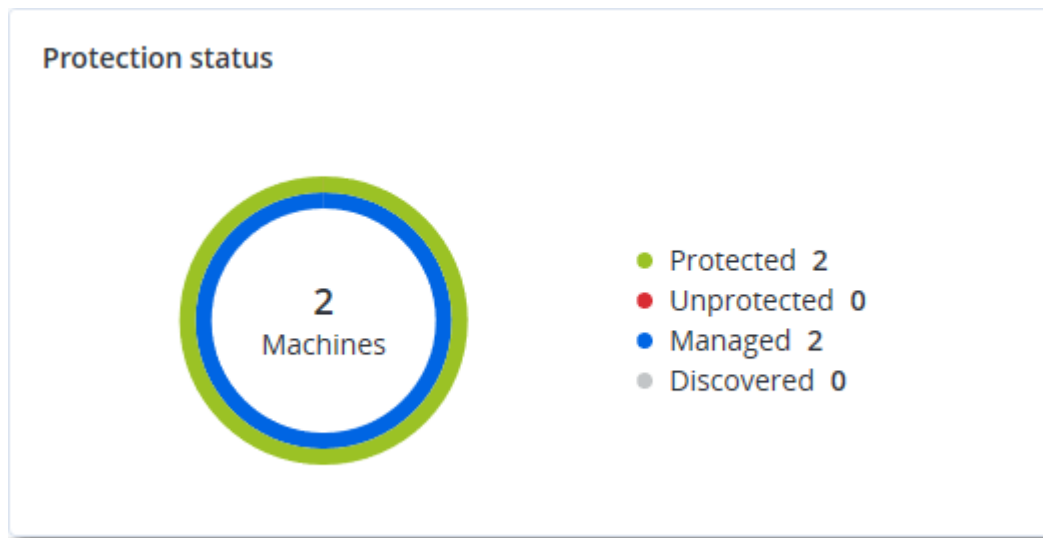
Protection status

This widget shows the current protection status for all machines.

A machine can be in one of the following statuses:

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

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



Discovered devices

This widget shows detailed information about the devices that were discovered in the organization's networks. The device information includes device type, manufacturer, operating system, IP address, MAC address, discovery date, and others.

Discovered devices										
Device name	Device type	Operating ...	Manuf...	Model	IP ad...	MAC ...	Organi... ↓	First discov...	Last discovered	Discovery type
win-2016-ad	Windows Computer	Windows	-	-	10. ...	56: ...	OU=Dom...	May 21, 20...	May 22, 2024 1...	Active Directory, Local network pas
DESKTOP-2BEV...	Windows Computer	Windows	-	-	10. ...	56: ...	-	May 21, 20...	May 22, 2024 1...	Local network passive
DESKTOP-J7S77IV	Windows Computer	Windows	-	-	10. ...	56: ...	-	May 21, 20...	May 22, 2024 1...	Local network passive
acp-win2016	Unknown	-	-	-	10. ...	56: ...	-	May 21, 20...	May 22, 2024 1...	Local network passive
win-2k19	Unknown	Windows	-	-	10. ...	56: ...	-	May 21, 20...	May 22, 2024 1...	Local network passive
acp-virtual-mac...	Windows Computer	Windows	VMware	-	10. ...	00: ...	-	May 21, 20...	May 22, 2024 1...	Local network active, Local network
DESKTOP-8FFA...	Windows Computer	Windows	VMware	-	10. ...	00: ...	-	May 21, 20...	May 22, 2024 1...	Local network active, Local network
acp-win	Unknown	Windows	-	-	10. ...	fa: ...	-	May 21, 20...	May 22, 2024 1...	Local network passive
DESKTOP-QCIK...	Windows Computer	Windows	-	-	10. ...	fa: ...	-	May 21, 20...	May 22, 2024 1...	Local network passive
DESKTOP-QCIK...	Windows Computer	Windows	-	-	10. ...	fa: ...	-	May 21, 20...	May 22, 2024 1...	Local network passive

[More](#)










#CyberFit Score by machine

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

- Antimalware
- Backup
- Firewall
- VPN
- Encryption
- NTLM traffic

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

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

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

Endpoint Detection and Response (EDR) widgets

Endpoint Detection and Response (EDR) includes a number of widgets which can be accessed from the **Operations** dashboard.

The widgets available are:



- Top incident distribution per workload
- Incident MTTR
- Security incident burndown
- Workload network status

Top incident distribution per workload

This widget displays the top five workloads with the most incidents (click **Show all** to redirect to the incident list, which is filtered according to the widget settings).

Hover over a workload row to view a breakdown of the current investigation state for the incidents; the investigation states are **Not started**, **Investigating**, **Closed**, and **False positive**. Then click on

the workload you want to analyze further, and select the relevant customer in the displayed popup; the incident list is refreshed according to the widget settings.

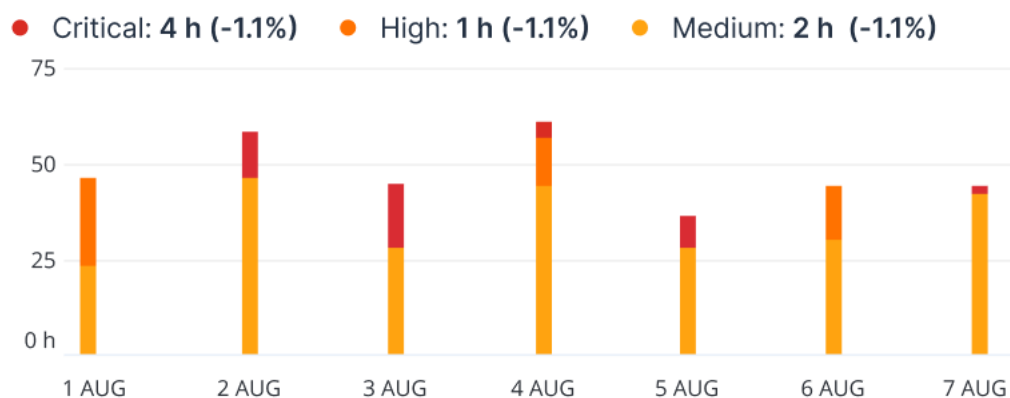
Top Incident distribution per workload		
SCRANTON		123
qa-gw3t68hh		41
RG_345		32
Georgy_Win_64		11
w_35jf_4		12
Show all		

Incident MTTR

This widget displays the average resolution time for security incidents. It indicates how quickly incidents are being investigated and resolved.

Click on a column to view a breakdown of the incidents according to severity (**Critical**, **High**, and **Medium**), and an indication of how long it took to resolve the different severity levels. The % value shown in parentheses indicates the increase or decrease in comparison to the previous time period.

Incident MTTR



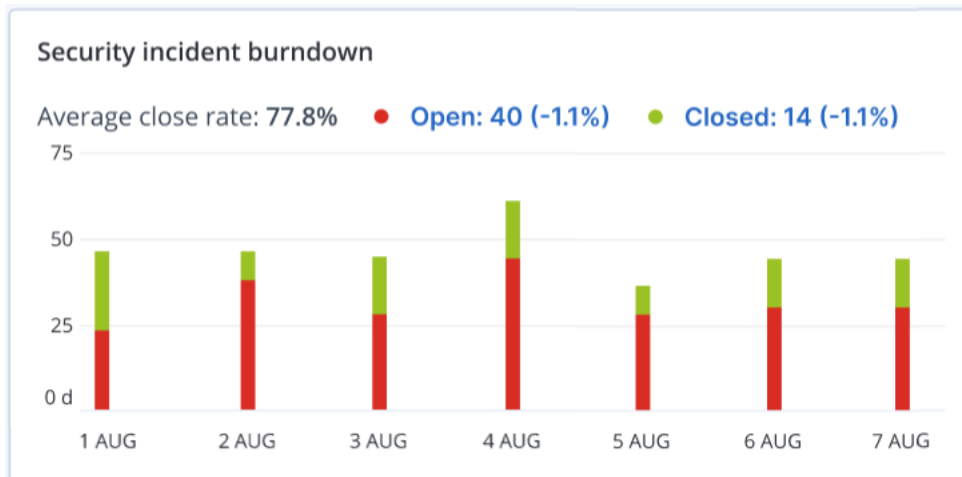
Security incident burndown

This widget shows the efficiency rate in closing incidents; the number of open incidents are measured against the number of closed incidents over a period of time.

Hover over a column to view a breakdown of the closed and open incidents for the selected day. If you click the Open value, a popup is displayed in which you select the relevant tenant; the filtered incident list for the selected tenant is displayed, to display incidents currently open (in the

Investigating or **Not started** states). If you click the Closed value, the incident list is displayed for the selected tenant, and filtered to display incidents that are no longer open (in the **Closed** or **False positive** states).

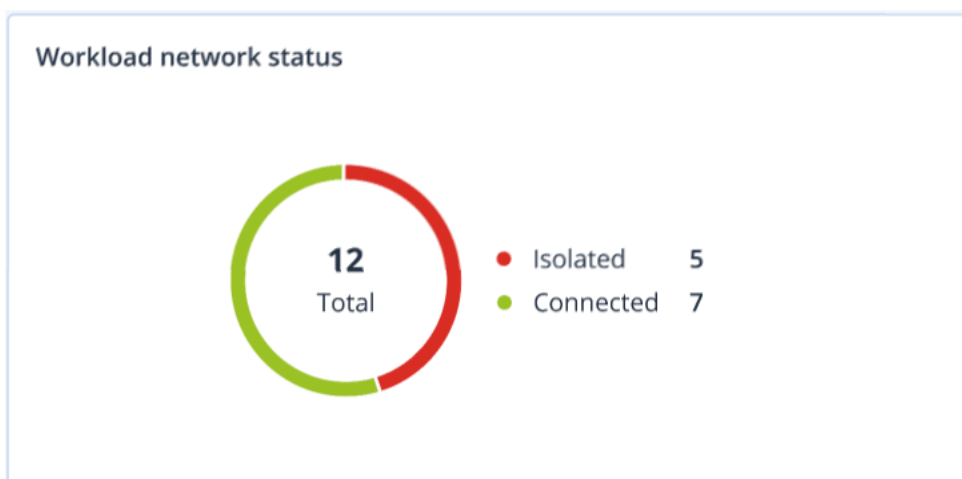
The % value shown in parentheses indicates the increase or decrease in comparison to the previous time period.



Workload network status

This widget displays the current network status of your workloads, and indicates how many workloads are isolated and how many are connected.

Click the Isolated value; a popup is displayed in which you select the relevant tenant. The displayed workload view is filtered to display isolated workloads. Click the Connected value to view the Workload with agents list filtered to display connected workloads (for the selected tenant).



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. The disk health widgets do not include any information about machines with RAID implementation.
- NVMe SSDs are not supported.
- External storage devices are not supported.

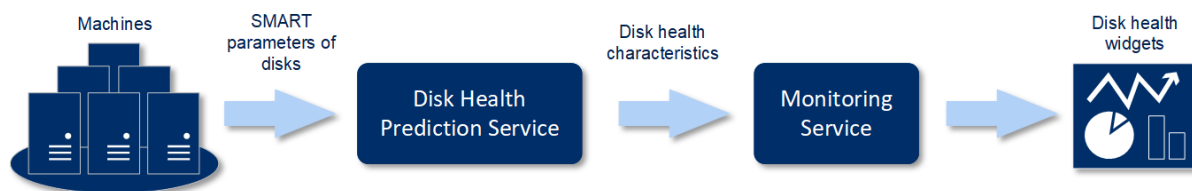
The disk health is represented by one of the following statuses:

- **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.

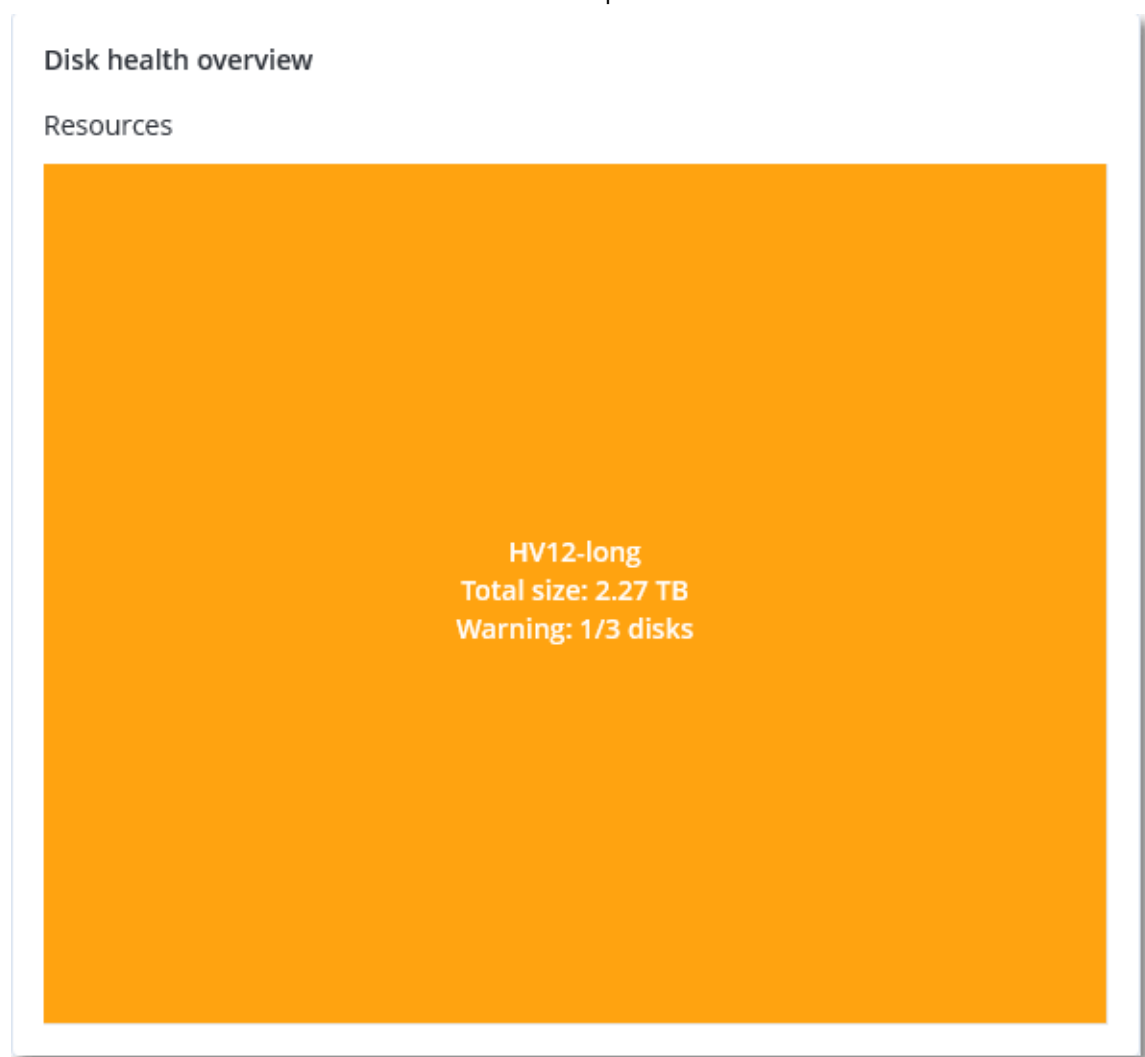
1. The protection agent collects the SMART parameters of the disks and passes this data to the Disk Health Prediction Service:
 - SMART 5 – Reallocated sectors count.
 - SMART 9 – Power-on hours.
 - SMART 187 – Reported uncorrectable errors.
 - SMART 188 – Command timeout.
 - SMART 197 – Current pending 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 Cyber Protect console.



Disk health widgets

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

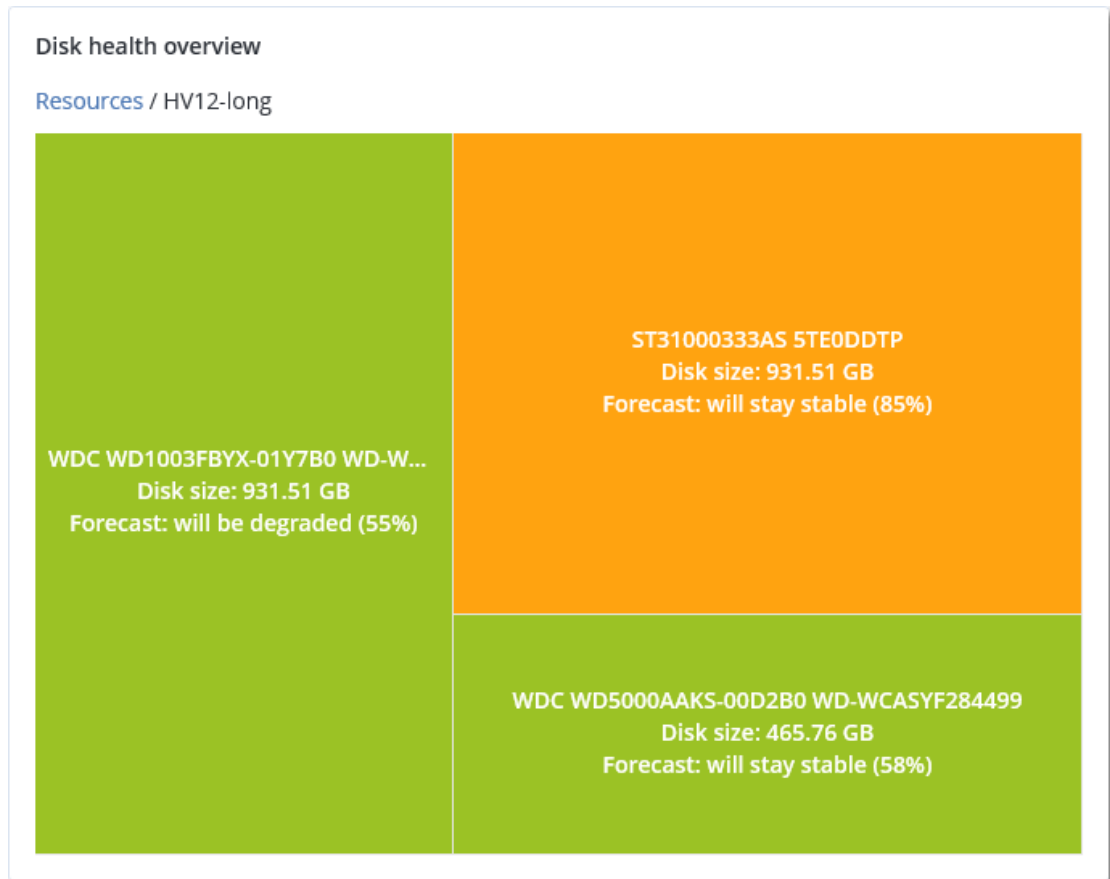
- **Disk health overview** is a treemap widget with two levels of detail that can be switched by drilling down.
 - **Machine level**
Shows summarized information about the disk health status of the selected customer machines. Only the most critical disk status is shown. The other statuses are shown in 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.



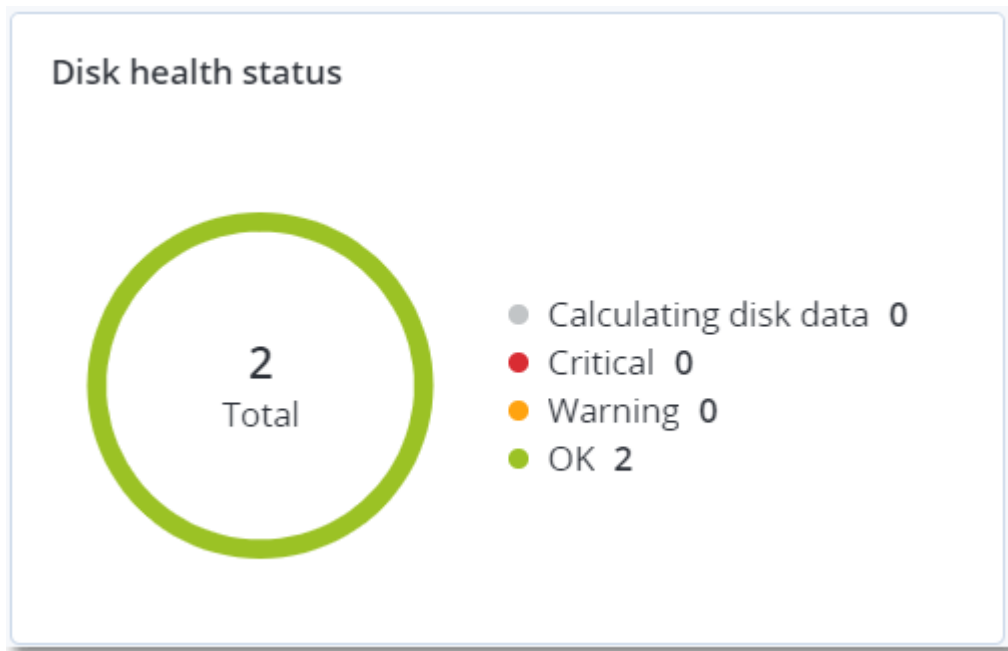
- Disk level

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
- 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.

Alert name	Severity	Disk health status	Description
Disk failure is possible	Warning	(30 – 70)	The <disk name> 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.
Disk failure is imminent	Critical	(0 – 30)	The <disk name> disk on this machine is in a critical state, and will most likely fail very soon. We do not recommend an image backup of this disk 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.

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.

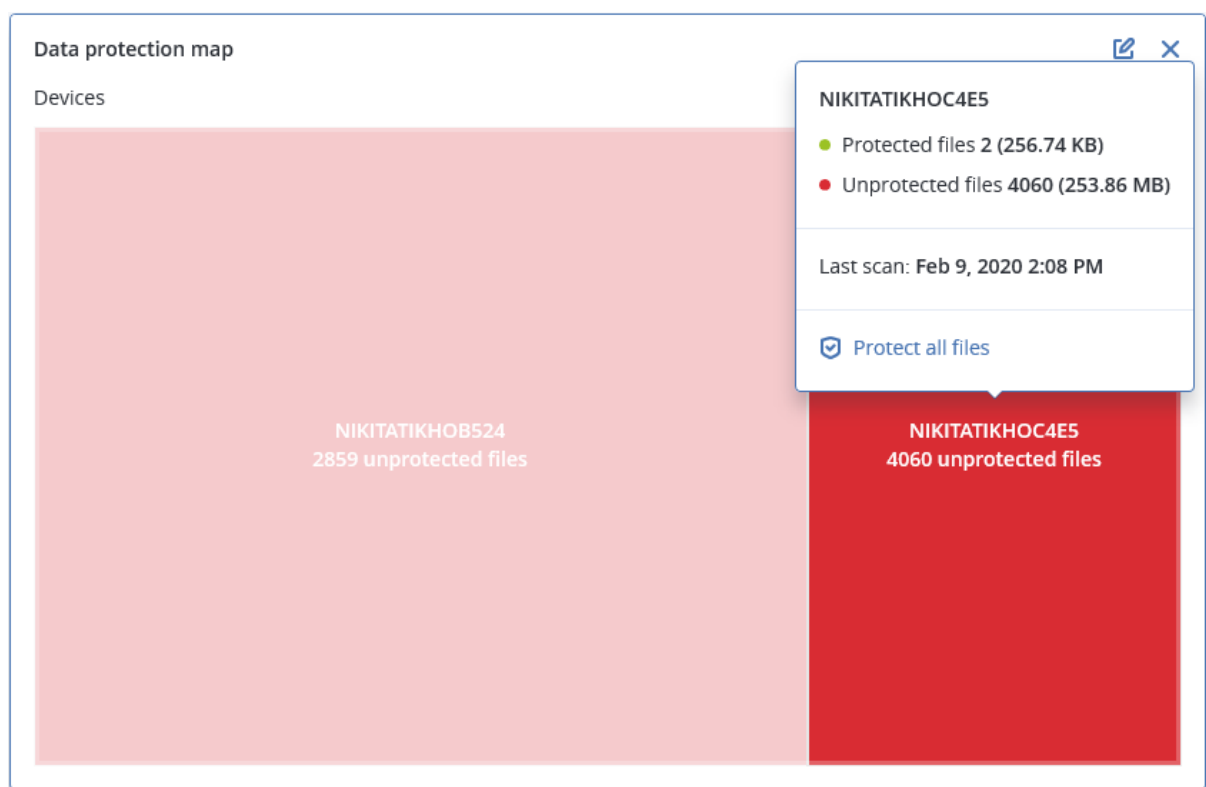
Each block size depends on the total number/size of all important files that belong to a customer/machine.

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.

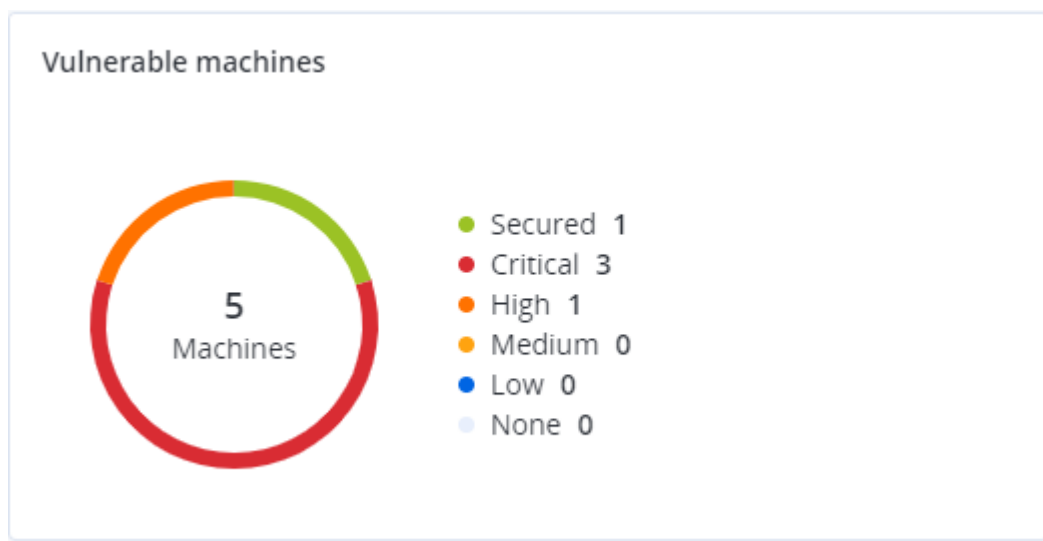
Vulnerability assessment widgets

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](#):

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



Existing vulnerabilities

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

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

Existing vulnerabilities							
Machine name	Vendor	Product	Vulnerability name/ID	Severity ↓	Last detected	First detected	⚙
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-7096	● Critical	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0856	● High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0688	● High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0739	● High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0752	● High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0753	● High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0806	● High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0810	● High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0812	● High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0829	● High	06/12/2020 5:16 PM	06/12/2020 5:15 PM	
More							

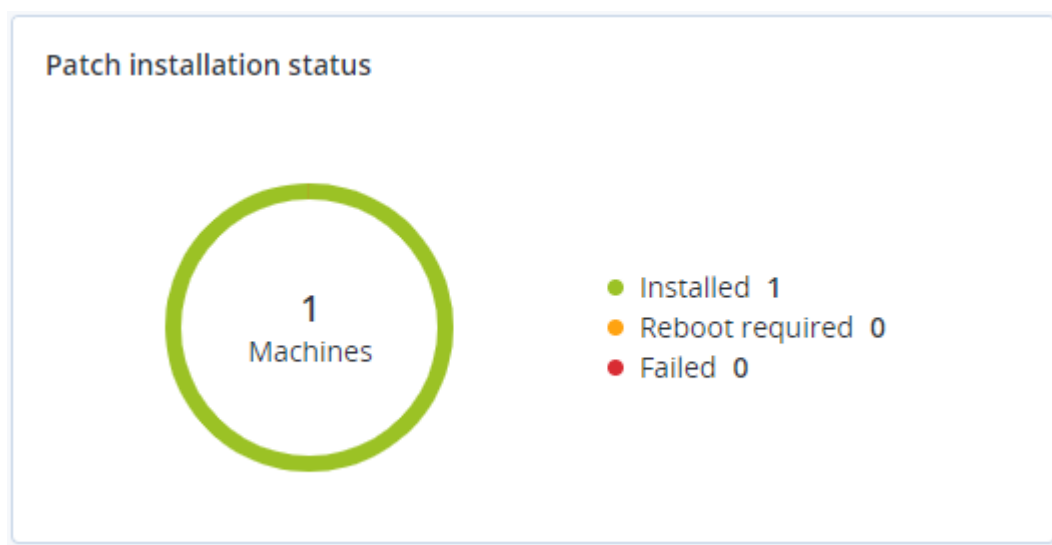
Patch installation widgets

There are four widgets related to the patch management functionality.

Patch installation status

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

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



Patch installation summary

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

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

Patch installation history

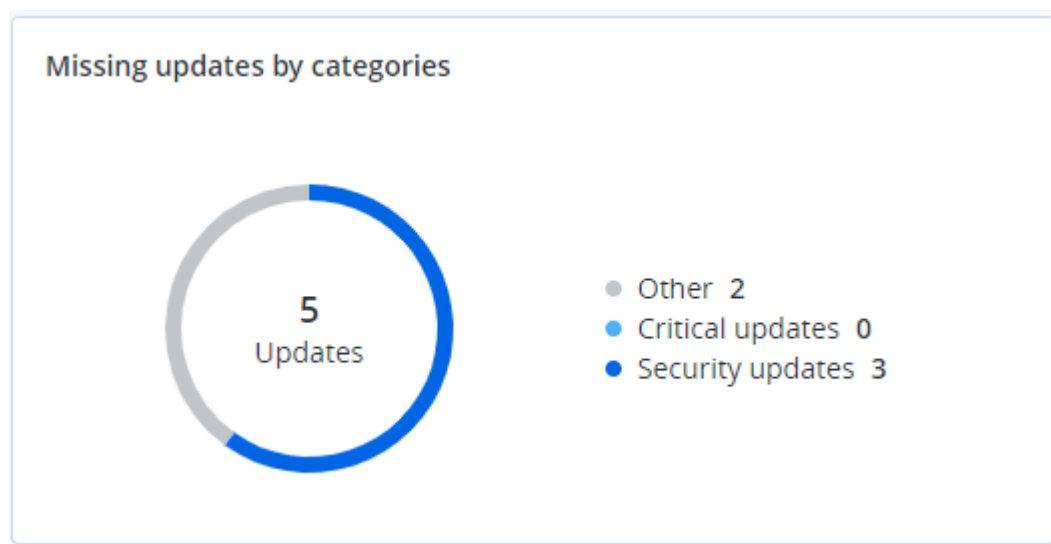
This widget shows the detailed information about patches on machines.

Patch installation history										30 days
Machine name	Update name	Version	Severity	Stability	Protection plan ↑	Size	Approval status	Release date	Installation status	⚙
Win11-10-35-112-141	Mozilla Firefox	138.0.3	⚠ Medium	-	New protection plan	68.76 MB	Not defined	05/16/2025	✅ Installed	
Win10-10-35-114-67	2024-10 Update for Wind...	-	⚠ Medium	⚠ Caution	New protection plan	0	Not defined	10/10/2024	✅ Installed	
Win11-10-35-112-141	Notepad++ Team Notepa...	8.8.1	⚠ Medium	✅ Stable	New protection plan	6.51 MB	Not defined	05/05/2025	✅ Installed	
Win11-10-35-112-141	Notepad++ Team Notepa...	8.8.1	⚠ Medium	✅ Stable	New protection plan	6.51 MB	Not defined	05/05/2025	❌ Failed	
Win11-10-35-112-141	Notepad++ Team Notepa...	8.8.1	⚠ Medium	✅ Stable	New protection plan	6.35 MB	Approved	05/05/2025	✅ Installed	

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.

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

More

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.

Recently affected					
Machine name	Protection plan	Threat	Affected files	Detection time	⚙
Ubuntu_14.04_x64-1	Total protection	Adware.DealPlylgen2	15	27.12.2	<ul style="list-style-type: none"> Folder Customer ✓ Machine name ✓ Protection plan Detected by ✓ Threat File name File path ✓ Affected files ✓ Detection time
Ubuntu_14.04_x64-1	Protection plan	Bloodhound.MalMacrolg1	274	27.12.2	
dc_w2k12_r2	Protection plan	Backdoor:Win32/Caphaw...	13	27.12.2	
Win2012_r2-Hyper-V	Protection plan	W97M.Downloaderlg32	5	27.12.2	
HyperV_for12A	Total protection	Miner.XMRiglg1	68	27.12.2	
vm-sql_2012	Total protection	Backdoor:Win32/Caphaw...	61	27.12.2	
vm-sql_2012	Protection plan	Adware.DealPlylgen2	9	27.12.2	
MF_2012_R2	Total protection	MSH.Downloaderlg8	73	27.12.2	
MF_2012_R2	Total protection	Bloodhound.MalMacrolg1	182	27.12.2	
MF_2012_R2	Protection plan	Bloodhound.MalMacrolg1	18	27.12.2	
ESXirestore	Protection plan	MSH.Downloaderlg8	682	27.12.2017 11:23 AM	
MF_2012_R2	Protection plan	Miner.XMRiglg1	13	27.12.2017 11:23 AM	
Ubuntu_14.04_x64-1	Total protection	Adware.DealPlylgen2	3	27.12.2017 11:23 AM	
Win2012_r2-Hyper-V	Total protection	W97M.Downloaderlg32	27	27.12.2017 11:23 AM	
More Show all 556					

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.

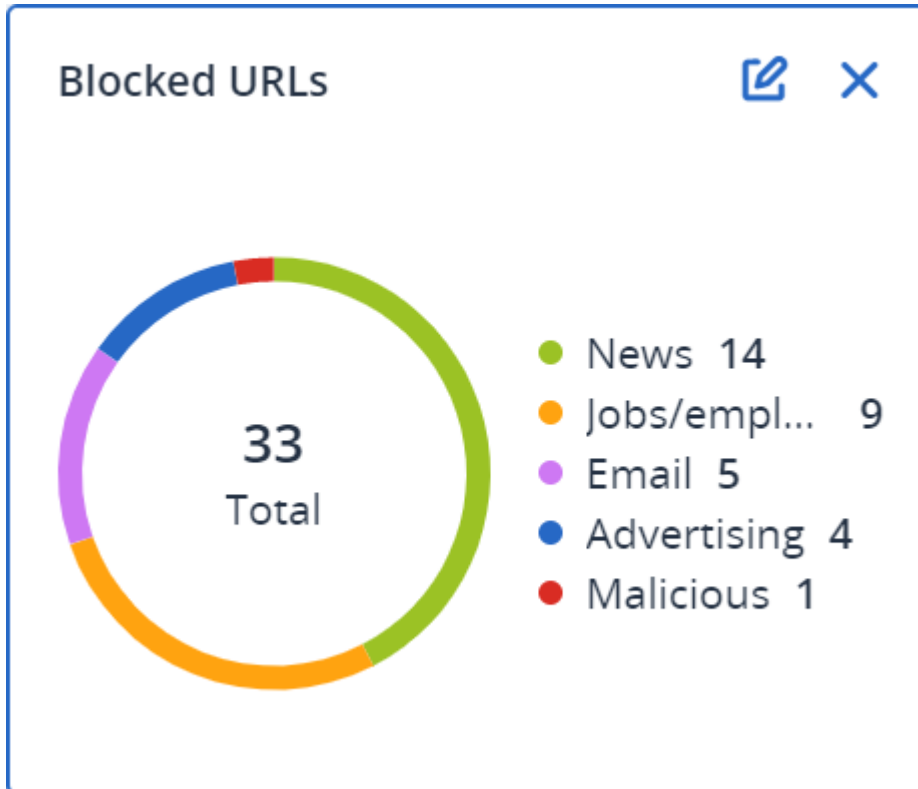
To download the data for the recently affected workloads

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](#).



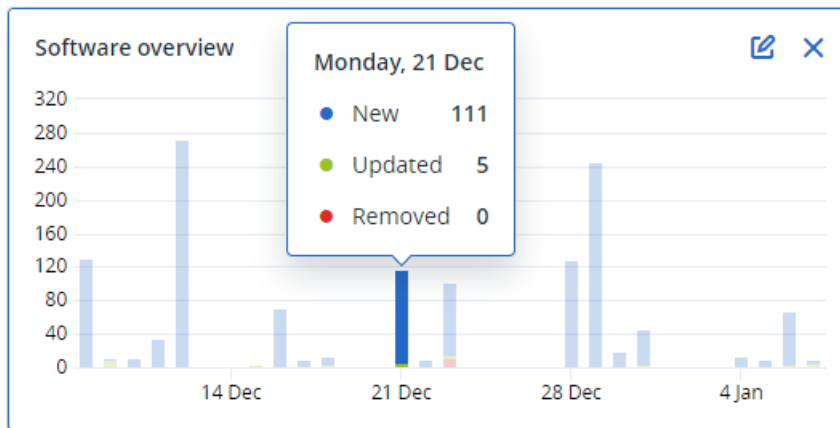
Software inventory widgets

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

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

More Less Show 248

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



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

New - the number of newly installed applications.

Updated - the number of updated applications.

Removed - the number of removed applications.

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

Hardware inventory widgets

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

Hardware inventory												
Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (GB)	Motherboard name	Motherboard serial	BIOS version	Domain	Registered owner	Registered organiz...	Scan date and time
Ivelins-Mac-mini...	macOS 11.0.1	10.16	6	233.47 GB	8.00 GB			0.1	-	-	-	12/14/2020 10:23 ...
O0003079.corp...	Microsoft Window...	10.0.16299	2	476.94 GB	11.83 GB	Base Board	L1HF6AC08PY	NICET81W(1.49)	corp.acronis.com	User	Acronis Inc.	12/13/2020 8:18 PM

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

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).

Hardware changes						
Machine name	Hardware category	Status	Old value	New value	Modification date and time ↓	⚙
▼ DESKTOP-0FF9TTF						
DESKTOP-0FF9TTF	Network adapter	Changed	Oracle Corporation, Ethernet 802.3, ...	Oracle Corporation, Ethernet 802.3, ...	01/11/2021 9:28 AM	
DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor Corp., Ether...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Toronto 5C1, PF0PJ810	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), WDC WD10JP...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 802.3, 00:0...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ethernet 802.3, ...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00 GB	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows Provider V9...	01/04/2021 2:37 PM	
DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM	
More						

Session history

The widget shows the detailed information about the remote desktop and file transfer sessions that were conducted in your organization during a specified time period.

Remote sessions							
Start time	End time	Duration	Connection type	Protocol	Connection sou...	Accessed by	Connection des... ⚙
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. l.1.4
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...
12/15/2022 4:...	12/15/2022 4:4...	2 minutes	Cloud	NEAR	RU-PC0YHMZL	sk-part	ACPM-Sveta
12/15/2022 4:...	12/15/2022 4:1...	16 minutes	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 4:0...	a minute	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 3:5...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. l.1.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 1...	12/15/2022 12:...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 1...	12/15/2022 12:...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...
More							



Geolocation tracking widget

On the **Geolocation tracking** widget, you can see details about the location of your organization's workloads, such as country, city or town, coordinates, last seen time, and the geolocation tracking method.

Geolocation tracking						1 day
Workload name ↑	Method	Details	Country	City/Town	Last seen	⚙
Long	OS	Lat. -34.5810, Long. -...	Argentina	Ciudad Autónoma de ...	02/11/2025 3:01 PM	
Chucks-Laptop	OS	Lat. 42.6826, Long. 2...	Bulgaria	Sofia City	02/11/2025 3:06 PM	



Chat sessions widget

In the **Chat sessions** widget, you can view details about of the remote chat sessions in your organization for a specified period.

Chat sessions								30 days
Start time	End time	Waiting time	Active time	Hold time	Total time	Technician name	Technician login	Workload ...  
Mar 11, 2025 2:55 PM	Mar 11, 2025 3:11 PM	-	00:15:58	-	00:15:58	D Z	dz-con	WIN-PMJ2B9....
Mar 4, 2025 12:31 PM	Mar 11, 2025 10:09 AM	21:12:24	21:38:13	00:00:04	00:25:53	Igor	igor	WIN-PMJ2B9....
Mar 11, 2025 2:54 PM	Mar 11, 2025 2:55 PM	-	00:01:10	-	00:01:10	Borya	boryana	WIN-PMJ2B9....
Mar 11, 2025 3:11 PM	Mar 11, 2025 6:24 PM	02:57:58	03:12:59	-	00:15:01	D Z	dz-con	WIN-PMJ2B9....
Mar 11, 2025 6:24 PM	Mar 11, 2025 7:10 PM	00:30:31	00:46:00	-	00:15:28	D Z	dz-con	WIN-PMJ2B9....
Feb 28, 2025 7:22 PM	Mar 3, 2025 5:16 PM	00:00:19	21:53:46	-	21:53:27	Igor	igor	WIN-PMJ2B9....

Technician performance widget

In the **Technician performance** widget, you can view details about the performance of each technician in your organization for a specified period.

Technician performance						30 days
Technician name	Technician login	Total sessions	Total session time	Average pick-up time	Average session duration 	
Igor	igor	2	19:32:04	10:36:21	21:46:02	

Audit log

To view the audit log, go to **Monitoring > Audit log**.

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

- Operations that are performed by users in the management portal
- Operations with cloud-to-cloud resources that are performed by users in the Cyber Protect console
- Cyber Scripting operations that are performed by users in the Cyber Protect console
- Operations related to email archiving
- 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.

Audit logs are stored in the data center and their availability cannot be affected by issues on end-user machines.

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**, **Script was changed**.

- **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**, **Scripting plan was deleted**.

- **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 type, severity, or date. You can also search the events by their name, object, tenant, initiator, and initiator's tenant.

Collecting performance data for Cyber Protection agents

For the protected Windows machines in your environment, you can collect performance logs manually or enable the automatic collection of diagnostic data if the system performance drops below the factory-defined thresholds. See "Performance thresholds for ETL data collection" (p. 75).

Collected logs are anonymized before they are sent for analysis to the vendor. The following data will be deleted from all logs, messages, alerts, and error messages:

- User account
- Company name
- Name of the protected workload

As a Company administrator, you can enable the automatic collection of logs for randomly selected agents or for specific agents in your organization.

Note

- Automated data collection on individual workloads is supported on Cyber Protection agent for Windows version 24.4.37758 or later.
 - Performance data collection on the tenant level is supported on Cyber Protection agent for Windows version 25.03.XXXXX or later.
-

To ensure that our support recommendations are well-informed, we gather data from approximately 10% of the agents in the environment for analysis.

This does not override the settings on individual workloads. For example, if the automated data collection is disabled on a specific workload, that workload will not be included in the bulk data collection.

Automated collection for multiple agents

To enable the automated collection of performance data for multiple agents in a tenant

Required role: Customer administrator

1. In the Cyber Protect Cloud console, navigate to **Settings > Agents**.
2. In the **Actions** menu to the right, click **Edit performance monitor settings**.
3. In the **Performance monitor** section, enable the toggle **Automatic collection and upload of performance logs**.

The automatically collected data is stored on the local disks of the protected machines, in folder C:\ProgramData\Acronis\ETLTool\ETL\, anonymized, and sent to the service provider for analysis.

Note

The limit for sending ETL logs to cloud is 3 times in 24 hours.

Automated collection for a single agent

To enable the automated collection of performance data for a specific agent

1. At the company level in the Cyber Protect Cloud console, navigate to **Settings > Agents**.
2. In the **Agents** list, select the agent for which you want to enable the performance monitor.
3. In the **Actions** menu to the right, click **Details**.
4. Scroll down to the **Performance monitor** section, and enable the **Allow this agent to collect performance logs automatically** toggle.

The automatically collected data is stored on the local disk of the protected machine in folder
C:\ProgramData\Acronis\ETLTool\ETL\.

Manual collection

To collect performance data manually

You can collect performance data on demand. In this case, it is not necessary to enable the performance monitor and automated collection of performance data.

1. Log in to the protected machine as an administrator user.
2. On the command prompt, run one of the following commands:
 - "C:\Program Files\Common Files\Acronis\ETLTool\etl-tool.exe" -o
The collection of ETL traces will run until you press the S key on the keyboard, or when the maximum time limit of 3600 seconds elapses.
 - "C:\Program Files\Common Files\Acronis\ETLTool\etl-tool.exe" -o -i X
Where X is the time limit for data collection in seconds, and the maximum value is 3600. You can stop the collection at any time by pressing the S key on the keyboard.

The manually collected data is stored on the local disk of the protected machine, in folder
C:\ProgramData\Acronis\ETLTool\OnDemandCollect\ETL\

To collect the performance logs

1. Log in to the protected machine as an administrator user.
2. Locate the data that you need:
 - Automatically collected performance data is located in folder
C:\ProgramData\Acronis\ETLTool\ETL\
 - Performance data collected on demand is located in folder
C:\ProgramData\Acronis\ETLTool\OnDemandCollect\ETL\

The ETL traces are also included in the sysinfo package.

Performance thresholds for ETL data collection

You can enable the automatic collection of performance data for the protected Windows machines in your environment. The monitoring is configured in the Cyber Protect Cloud console per agent, and enables the automatic collection of diagnostic data if the system performance drops below predefined thresholds.

The automated data collection starts when one of the thresholds is exceeded.

Default thresholds for ETL data collection

The following table describes the thresholds that trigger the automated collection of ETL data.

Parameter	Description	Default value
"process-memory-consumption"	Threshold for memory overuse	
"allocated-memory-percent"		15
"minimum-allocated-memory-duration-seconds"		10
"allocated-memory-free-limit-seconds"		300
"process-disk-io"	Threshold for high disk I/O usage	
"maximum-operations-number"		10000
"maximum-transferred-bytes"		100000000
"estimation-period-seconds"		5
"process-file-io"	Threshold for high file I/O usage	
"maximum-operations-number"		30000
"maximum-transferred-bytes"		100000000
"estimation-period-seconds"		5
"process-cpu-usage"	Threshold for high CPU consumption	
"cpu-percent"		15
"estimation-period-seconds"		10
"acronis-component-thresholds"	Performance of protection agent components	
"behavioral-engine"	Threshold for the Behavior engine	
"average-system-utilization-percent"		50
"be-stats-event-number"		10
"avc-scan"	Threshold for the Antivirus and	

Parameter	Description	Default value
	Antimalware protection component	
"average-scan-duration-seconds"	Maximum average scan duration	3
"estimation-period-seconds"		10
"maximum-scan-duration-seconds"	Maximum scan duration for a single scan	5

Reporting

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

Note

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

Usage reports

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

Important

The values of storage usage displayed in the product UI are in binary byte units – mebibytes (MiB), gibibytes (GiB), and tebibytes (TiB) – even though the labels show MB, GB, and TB respectively. For example, if the actual usage is 3105886629888 bytes, the value displayed in the UI is correctly shown as 2.82, but is labeled with TB instead of TiB.

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.

Note

Local storage usage data is reported only at the unit and customer tenant levels. Users do not receive information about the local storage usage in the Summary reports.

- **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 tenants of the tenant in which you are operating and for all users within the tenants.

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 by unit, by user, by device type.
- Total size of backups.
- Total number of protected devices.
- Total price.

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

Important

The values of storage usage displayed in the product UI are in binary byte units – mebibytes (MiB), gibibytes (GiB), and tebibytes (TiB) – even though the labels show MB, GB, and TB respectively. For example, if the actual usage is 3105886629888 bytes, the value displayed in the UI is correctly shown as 2.82, but is labeled with TB instead of TiB.

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. 97).

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

You can use default reports or create a custom report.

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

The default reports are listed below:

Report name	Description
#CyberFit Score by machine	Shows the #CyberFit Score, based on the evaluation of security metrics and configurations for each machine, and recommendations for improvements.
Alerts	Shows alerts that occurred during a specified time period.
Backup scanning details	Shows the detailed information about detected threats in the backups.
Daily activities	Shows the summary information about activities performed during a specified time period.
Data protection map	Shows the detailed information about the number, size, location, protection status of all important files on machines.
Detected threats	Shows the details of the affected machines by number of blocked threats and the healthy and vulnerable machines.
Discovered devices	Shows all devices that were discovered in your organization's networks.
Disk health prediction	Shows predictions when your HDD/SSD will break down and current disk status.
Existing vulnerabilities	Shows the existing vulnerabilities for OS and applications in your organization. The report also displays the details of the affected machines in your network for every product that is listed.
Patch management summary	Shows the number of missing patches, installed patches, and applicable patches. You can drill down the reports to get the missing/installed patch information and details of all the systems.
Summary	Shows the summary information about the protected devices for a specified time period.
Weekly activities	Shows the summary information about activities performed during a specified time period.
Software inventory	Shows detailed information about the all the software that is installed on Windows and macOS machines in your organization.
Hardware Inventory	Shows detailed information about the all the hardware that is available on physical and virtual Windows and macOS machines in your organization.
Remote sessions	Shows detailed information about the remote desktop and file transfer sessions that were conducted in your organization during a specified time period.

Actions with reports

Add

To add a new report

1. In the Cyber Protect console, go to **Reports**.
2. Under the list of available reports, click **Add report**.
3. [To add a predefined report] Click the name of the predefined report.
4. [To add a custom report] Click **Custom**, and then add widgets to the report.
5. [Optional] Drag and drop the widgets to rearrange them.

View

To view a report

- To view a report, click its name.

Edit

To edit a report

1. In the Cyber Protect console, go to **Reports**.
2. In the list of reports, select the report that you want to edit.
3. In the upper-right corner of the screen, click **Settings**.
4. Edit the report, and then click **Save**.

Delete

To delete a report

1. In the Cyber Protect console, go to **Reports**.
2. In the list of reports, select the report that you want to delete.
3. In the upper-right corner of the screen, click the ellipsis icon (...), and then click **Delete report**.
4. In the confirmation window, click **Delete**.

Schedule

To schedule a report

1. In the Cyber Protect console, go to **Reports**.
2. In the list of reports, select the report that you want to schedule.
3. In the upper-right corner of the screen, click **Settings**.
4. Next to **Scheduled**, enable the switch.
 - Specify the email addresses of the recipients.
 - Select the format of the report.

- **Note**

You can export up to 1,000 items in a PDF file, and up to 10,000 items in a XLSX file. The timestamps in the PDF and XLSX files use the local time of your machine.

- Select the language of the report.
- Configure the schedule.

5. Click **Save**.

Download

To download a report

1. In the Cyber Protect console, go to **Reports**.
2. In the list of reports, select the report.
3. In the upper-right corner of the screen, click **Download**.
4. Select the format of the report.

As a result, a file in the selected format is downloaded to your machine.

If you selected **Excel and PDF**, a ZIP file is downloaded to your machine.

Send

To send a report

1. In the Cyber Protect console, go to **Reports**.
2. In the list of reports, select the report.
3. In the upper-right corner of the screen, click **Send**.
4. Specify the email addresses of the recipients.
5. Select the format of the report.
6. Click **Send**.

Export structure

To export the report structure

1. In the Cyber Protect console, go to **Reports**.
2. In the list of reports, select the report.
3. In the upper-right corner of the screen, click the ellipsis icon (...), and then click **Export**.

As a result, the report structure is saved on your machine as a JSON file.

Dump data

To dump the report data

You can export all data for a custom period, without filtering it, to a CSV file and send the CSV file to an email recipient. The CSV file contains only data about the widgets that are included in the report.

Note

You can export up to 150,000 items in a CSV file. The timestamps in the CSV file use Coordinated Universal Time (UTC).

1. In the Cyber Protect console, go to **Reports**.
 2. In the list of reports, select the report whose data you want to dump.
 3. In the upper-right corner of the screen, click the ellipsis icon (...), and then click **Dump data**.
 4. Specify the email addresses of the recipients.
 5. In **Time range**, specify the custom period for which you want to dump data.
-

Note

Preparing CSV files for longer periods takes more time.

6. 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.

Widget	Description
Cloud workloads protection status	<p>This 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):</p> <ul style="list-style-type: none"> • 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 <p>For some workload types, the following workload groups are used:</p> <ul style="list-style-type: none"> • Microsoft 365: Users, Groups, Public Folders, Teams, and Site Collections • Google Workspace: Users, and Shared Drives • Hosted Exchange: Users <p>If in one workload group there are more than 10 000 workloads, the widget does not display any data for the corresponding workloads.</p> <p>For example, if your organization 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.</p>
Cyber protection summary	<p>The widget shows the key metrics of the Cyber protection performance for the specified time range.</p> <p>Data backed up - the total size of the archives that were created in the cloud and local storages.</p> <p>Mitigated threats - the total number of malware blocked across all devices.</p> <p>Malicious URLs blocked - the total number of URLs blocked on all devices.</p> <p>Patched vulnerabilities - the total number of vulnerabilities that were fixed</p>

Widget	Description
	<p>through installation of software patches on all devices.</p> <p>Installed patches - the total number of installed patches on all devices.</p> <p>Servers protected by DR - the total number of servers protected by Disaster Recovery.</p> <p>File Sync & Share users - the total number of end and guest users who use Cyber Files.</p> <p>Notarized files - the total number of notarized files.</p> <p>eSigned documents - the total number of eSigned documents.</p> <p>Blocked peripheral devices - the total number of blocked peripheral devices.</p>
Workload network status	<p>This widget indicates how many workloads are isolated and how many are connected (the normal state of the workload).</p>
Workloads protection status	<p>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:</p> <p>Servers - physical servers, and Domain Controller servers.</p> <p>Workstations - physical workstations.</p> <p>Virtual machines - both agent-based and agentless virtual machines.</p> <p>Web hosting servers - virtual or physical server with installed cPanel or Plesk.</p> <p>Mobile devices - physical mobile devices.</p> <p>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.</p>
Discovered devices	<p>The widget shows the following information about the devices that were discovered in your organization's networks in a specified period:</p> <p>Device name</p> <p>Device type</p> <p>Operating system</p> <p>Manufacturer</p> <p>Model</p> <p>IP address</p> <p>MAC address</p>

Widget	Description
	Organizational unit You can edit the widget and filter the displayed information by organizational unit, device type, discovery type, first discovered date, last discovered date, IP address, MAC address, and discovery type.

Antimalware protection widgets

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

Widget	Description
Antimalware scan of files	<p>The widget shows the results of on-demand antimalware scanning of the devices for the specified date range.</p> <p>Files - the total number of scanned files</p> <p>Clean - the total number of clean files</p> <p>Detected, quarantined - the total number of infected files that were quarantined</p> <p>Detected, not quarantined - the total number of infected files that were not quarantined</p> <p>Devices protected - The total number of devices with applied antimalware protection policy</p> <p>Total number of registered devices - The total number of registered devices at the time of the report's generation</p>
Antimalware scan of backups	<p>The widget shows the results from the antimalware scanning of the backups for the specified date range, using the following metrics:</p> <ul style="list-style-type: none"> • 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.
Blocked URLs	<p>For the specified date range, the widget shows the number of blocked URLs grouped by website category.</p> <p>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.</p> <p>For more information about the website categories, see the URL filtering topic in Cyber Protection.</p>
Security incident burndown	<p>This widget shows the efficiency rate in closing incidents for the selected company; the number of open incidents are measured against the number of closed incidents over a period of time.</p>

Widget	Description
	Hover over a column to view a breakdown of the closed and open incidents for the selected day. The % value shown in parentheses indicates the increase or decrease in comparison to the previous time period.
Incident MTTR	<p>This widget displays the average resolution time for security incidents. It indicates how quickly incidents are being investigated and resolved.</p> <p>Click on a column to view a breakdown of the incidents according to severity (Critical, High, and Medium), and an indication of how long it took to resolve the different severity levels. The % value shown in parentheses indicates the increase or decrease in comparison to the previous time period.</p>
Threat status	This widget displays the current threat status for a company's workloads (regardless of the number of workloads), highlighting the current number of incidents that are not mitigated and that need investigating. The widget also indicates the number of incidents that were mitigated (manually and/or automatically by the system).
Threats detected by protection technology	<p>For the specified date range, the widget shows the number of detected threats grouped by the following protection technologies:</p> <ul style="list-style-type: none"> • Antimalware scanning • Behavior engine • Cryptomining protection • Exploit prevention • Ransomware active protection • Real-time protection • URL filtering

Backup widgets

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

Widget	Description
Workloads backed up	<p>The widget shows the total number of registered workloads by backup status.</p> <p>Backed up - number of workloads that were backed up (at least one successful backup was performed) during the report date range.</p> <p>Not backed up - number of workloads which were not backed up (no successful backup was performed) during the report date range.</p>
Disk health status by physical device	<p>The widget shows the aggregated health status of physical devices based on the health statuses of their disks.</p> <p>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.</p>

Widget	Description
	<p>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.</p> <p>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.</p> <p>Calculating disk data - The status of the device is Calculating disk data when the statuses of its disks are not calculated yet.</p>
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.

Widget	Description
Patched vulnerabilities	<p>The widget shows the vulnerability assessment performance results for the specified date range.</p> <p>Total- the total number of patched vulnerabilities.</p> <p>Microsoft software vulnerabilities- total number of fixed Microsoft vulnerabilities on all Windows devices.</p> <p>Windows third-party software vulnerabilities - the total number of fixed Windows third-party vulnerabilities on all Windows devices.</p> <p>Workloads scanned - the total number of devices which were successfully scanned for vulnerabilities at least once within the specified date range.</p>
Patches installed	<p>The widget shows the patch management performance results for the specified date range.</p> <p>Installed - the total number of patches that were successfully installed on all devices.</p> <p>Microsoft software patches - the total number of Microsoft software patches that were installed on all Windows devices.</p> <p>Windows third-party software patches - the total number of Windows third-party software patches that were installed on all Windows devices.</p> <p>Workloads patched - the total number of devices which were successfully patched (at least one patch was successfully installed during the specified date range).</p>

Software widgets

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

Widget	Description
Installation status	This widget shows the total number of installation activities, grouped by status. Clicking a segment of the donut chart redirects you to the Activities page, where only activities with the corresponding status are shown, ordered chronologically.
Uninstallation status	The widget shows the total number of uninstallation activities, grouped by status. Clicking a segment of the donut chart redirects you to the Activities page, where only activities with the corresponding status are shown, ordered chronologically.
Software installation history	This widget provides detailed status information about remote software installations on your managed devices. Clicking a status in the Installation status column redirects you to the Activities page, where activities with the corresponding status are displayed in chronological order.
Software uninstallation history	The widget provides detailed status information about remote software uninstallations from your managed devices. Clicking a status in the Uninstallation status column redirects you to the Activities page, where activities with the corresponding status are displayed in chronological order.

Disaster Recovery widgets

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

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

Widget	Description
	Total compute points consumed - the total number of compute points consumed during the specified time range.
Disaster Recovery servers tested	<p>The widget shows information about the servers that are protected by Disaster Recovery and tested with test failover.</p> <p>The widget shows the following metrics:</p> <p>Server protected - the number of servers protected by Disaster Recovery (servers which have at last one recovery server) at the moment of the report's generation.</p> <p>Tested - 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.</p> <p>Not tested - 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.</p> <p>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.</p>
Servers protected with Disaster Recovery	<p>The widget shows information about the servers protected with Disaster Recovery and the unprotected servers.</p> <p>The widget shows the following metrics:</p> <p>The total number of servers registered in customer tenant at the moment of the report's generation.</p> <p>Protected - 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.</p> <p>Unprotected - the total number of unprotected servers out of all registered servers at the moment of the report's generation.</p>

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.

Widget	Description
File Sync & Share statistics	<p>The widget shows the following metrics:</p> <p>Total cloud storage used - The total storage usage of all users.</p> <p>End users - the total number of end users.</p> <p>Average storage used per end user - the average storage usage per end user.</p> <p>Guest users - the total number of guest users.</p>
File Sync & Share storage usage by end users	<p>The widget shows the total number of File Sync & Share end users who have a storage usage in the following ranges:</p> <ul style="list-style-type: none"> • 0 - 1 GB • 1 - 5 GB • 5 - 10 GB • 10 - 50 GB • 50 - 100 GB • 100 - 500 GB • 500 - 1 TB • 1+ TB

Notary widgets

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

Widget	Description
Cyber Notary	The widget shows the following Notary metrics:

Widget	Description
statistics	<p>Notary cloud storage used - the total size of the storage used for Notary services.</p> <p>Notarized files - the total number of notarized files.</p> <p>eSigned documents - the total number of eSigned documents and eSigned files.</p>
Notarized files across end users	<p>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.</p> <ul style="list-style-type: none"> • Up to 10 files • 11 - 100 files • 101 - 500 files • 501 - 1000 files • 1000+ files
eSigned documents across end users	<p>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.</p> <ul style="list-style-type: none"> • 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. 93).

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.

Report location and type	Time zone used in the report
Management portal > Monitoring > Operations (widgets)	The time of report generation is in the time zone of the machine where the browser is running.
Management portal > Monitoring > Operations (exported to PDF or xlsx)	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • 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 xlsx)	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 >	<ul style="list-style-type: none"> • This report is sent when an activity is completed.

Cyber Protection status notifications	<p>Note Depending on the workload in the datacenter, some reports might be sent with delays.</p> <ul style="list-style-type: none"> 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.

Widget name	Data displayed in widget and reports
#CyberFit Score by machine	Actual
5 latest alerts	Actual
Active alerts details	Actual
Active alerts summary	Actual
Activities	Historical
Activity list	Historical
Alerts history	Historical
Antimalware scan of backups	Historical
Antimalware scan of files	Historical
Backup scanning details (threats)	Historical
Backup status	Historical - in columns Total runs and Number of successful runs Actual - in all other columns
Backup storage usage	Historical
Blocked peripheral devices	Historical
Blocked URLs	Actual
Cloud applications	Actual

Cloud workloads protection status	Actual
Cyber protection	Actual
Cyber protection summary	Historical
Data protection map	Historical
Devices	Actual
Disaster recovery servers tested	Historical
Disaster recovery statistics	Historical
Discovered devices	Actual
Disk health overview	Actual
Disk health status	Actual
Disk health status by physical devices	Actual
eSigned documents across end users	Actual
Existing vulnerabilities	Historical
File Sync & Share statistics	Actual
File Sync & Share storage usage by end users	Actual
Hardware changes	Historical
Hardware details	Actual
Hardware inventory	Actual
Historical alerts summary	Historical
Locations summary	Actual
Missing updates by categories	Actual
Not protected	Actual
Notarized files across end users	Actual
Notary statistics	Actual
Patch installation history	Historical
Patch installation status	Historical
Patch installation summary	Historical
Patched vulnerabilities	Historical

Patches installed	Historical
Protection status	Actual
Recently affected	Historical
Remote sessions	Historical
Security incident burndown	Historical
Security incident MTTR	Historical
Servers protected with disaster recovery	Actual
Software inventory	Actual
Software overview	Historical
Threat status	Actual
Threats detected by protection technology	Historical
Top incident distribution per workload	Actual
Vulnerable machines	Actual
Workload network status	Actual
Workloads backed up	Historical
Workloads protection status	Actual

Integrations

This chapter provides the information you need to find and activate integrations.

Integrations offer third-party cyber protection, endpoint management, customer management, monitoring, analytics, etc., right alongside the standard Cyber Protect console products and, likewise, offer our solutions through third-party software platforms. Over 200 integrations currently automate daily routines and increase efficiency for our partners and their customers.

Integrations are listed on [the integration catalogs](#).

Note

Some integrations require [an API client](#) to access the application programming interfaces (APIs).

Integration catalogs

The integration catalogs list the available integrations:

- [The Application Catalog](#).

This catalog is publicly available. Integrations cannot be activated from this catalog.

If you see an integration you want to use, contact your partner to activate it for you.

- [Data center \(DC\) catalogs](#).

These catalogs are data center-specific. Integrations can be activated from these catalogs.

Partner-level Management Portal administrators can:

- See all of the integrations deployed on the data center.
- Activate all of the integrations deployed on the data center, either for themselves or for their customers.

Customer-level Management Portal administrators can:

- Only see integrations which the integration developer explicitly sets as visible for customers.
- Only activate integrations which the integration developer explicitly allows to be activated by customers.

Note

The partner-level Management Portal administrator must activate the integration at the partner level before it can be activated by a customer-level Management Portal administrator.

Catalog entries

Catalog entries consist of two parts:

- The catalog card provides an overview of the integration.
- [The catalog detail page](#) provides more information, such as a full functional description, screenshots, videos, a feature list, contact details, links to integration resources, etc.

Opening your data center integration catalog

In data center (DC) integration catalogs, hover over a catalog card to read a short product description, the **Configure** button, and a **Learn more** link:

- The **Learn more** link
Each integration catalog entry has a page with integration details including, for example, a full functional description, screenshots, videos, a feature list, contact details, links to integration resources, etc.
Click this link to open the integration detail page.
- The **Configure** button
Click this button to activate the integration.

Note

Catalog cards representing inactive integrations appear grayed out, and are disabled.

To open your DC integration catalog

1. [Open Management Portal](#).
2. Select **Integrations** from the main menu.
The **All integrations** tab is opened by default. This displays the catalog cards for the integrations which customer-level Management Portal administrators can enable.
3. [Optional] Choose a category and enter text in the search field to filter the catalog cards.

Opening an integration detail page

To open an integration detail page

1. [Open the integration catalog on your data center](#).
2. Locate the catalog card for the integration.
3. Hover over the catalog card.
4. Click **Learn more**.

The integration detail page opens.

Viewing your activated integrations

The **Integrations in use** tab of the integration catalog displays a card for each integration you have activated.

To view your actived integrations

1. [Open the integration catalog on your data center](#).
2. Select the **Integrations in use** tab.

Opening Application Catalog

Application Catalog lists all Cyber Protect Cloud integrations.

Note

If you identify an integration that you want to use, you must contact your partner to activate it for you.

To open Application Catalog

1. Visit solutions.acronis.com.
The initial view is a grid of all the catalog cards.
2. [Optional] Choose a category and enter text in the search field to filter the catalog cards.

Acronis

Products Solutions Partners Support Company

Start selling Try now

Acronis Cyber Protect Cloud
FOR SERVICE PROVIDERS

Application Catalog

Integrations with the tools and services you know and trust

Contact us Try Acronis

All categories acronis

- Security
- Data Protection
- Management
- Automation

CloudBlue

Acronis Cyber Cloud Connect for Resellers

Ingram Micro

Acronis Cyber Protect Cloud for resellers provides full subscription live-cycle management.

Learn more

CloudBlue

Acronis Cyber Cloud Connect for End Customers

Acronis

Acronis Cyber Protect Cloud for end-customers provides full subscription live-cycle management.

Learn more

Acronis

Acronis Generic SIEM Connector

Acronis

Simplify security posture by integrating with SIEM platforms.

Learn more

Can't find your favorite tool or service?

With the Acronis Cyber Protect Cloud platform, developers, software vendors and service providers can build new applications and share them with the Acronis community. Building a new application is fast and easy with a powerful low-code CyberApp Standard development framework. You can build a new integration or nominate your favorite tool for integration.

Build Integration
Nominate a tool

Opening an integration detail page

Each catalog entry also has a page with integration details, such as a full functional description, screenshots, videos, a feature list, contact details, links to integration resources, etc.

To open an integration detail page

1. Visit solutions.acronis.com.
2. Locate the catalog card for the integration in which you are interested.
3. Click **Learn more** on the catalog card.

Acronis

[Products](#)
[Solutions](#)
[Partners](#)
[Support](#)
[Company](#)

[Start selling](#)
[Try now](#)

Acronis Cyber Protect Cloud

FOR SERVICE PROVIDERS

Application Catalog

Integrations with the tools and services you know and trust

[Contact us](#)
[Try Acronis](#)

[← Back to Integrations](#)
[Have a question or need help?](#)

Acronis

Integration: Acronis Generic SIEM Connector

Category: SIEM

Company: Acronis

Website

Acronis Generic SIEM Connector

SIEM (Security Information and Event Management) platforms are used by many MSPs for security incident investigation and remediation, threat hunting, and compliance. Acronis Generic SIEM Connector allows MSPs to forward Acronis Cyber Protect Cloud alerts to any SIEM system that supports the CEF event format over SYSLOG for further correlation and analysis to reveal patterns of activity that may indicate an attempt of intrusion.

[Integration Overview](#)

Simplify security posture by integrating with SIEM platforms.

SIEMs empower MSPs security specialists to identify attack rout across the network and get visibility into compromised files. Now with Acronis Generic SIEM connector, MSPs will gain extra visibility into customers networks, will be able to search for threats across all managed workloads, and correlate events from both security and data protection applications, and run response actions.

Features

Support of core event format

Acronis supports core event format - CEF (Common Event Format), enabling MSPs to work with any SIEM that supports CEF format out of the box. Alerts are transferred to SIEM via syslog server.

Threat hunting across all managed companies

Integration allows MSPs to select which customer tenants in Acronis should send alerts to SIEM. Since alerts are sent to the same SIEM instance, it's possible to run correlation, threat hunting and perform investigation for all customers in the same console. It also empowers MSPs to search for threats, that were discovered on one workload in one customer tenant, in other customers environments.

Simple integration enablement

It's very easy to enable the integration by obtaining server and client certificates, establishing connection to the server and specifying the server port.

Select data you want to see

It is possible to select which alerts should be sent to SIEM. With this functionality, MSPs benefit from reducing the amount of sent to SIEM data and, therefore, lower SIEM invoice. MSPs can select and work only with the data that is necessary.

Acronis

Acronis Generic SIEM Connector

Need help or support with an integration?

Contact Support

Can't find your favorite tool or service?

With the Acronis Cyber Protect Cloud platform, developers, software vendors and service providers can build new applications and share them with the Acronis community. Building a new application is fast and easy with a powerful low-code CyberApp Standard development framework. You can build a new integration or nominate your favorite tool for integration.

[Build integration](#)
[Nominate a tool](#)

Engage with Acronis

[f](#)
[X](#)
[in](#)
[v](#)
[u](#)

Acronis

© 2003–2024 Acronis International GmbH. [Legal information](#) | [Privacy policy](#)

105

Activating an integration

Note

The partner-level Management Portal administrator must activate the integration at the partner level before it can be activated by a customer-level Management Portal administrator.

To activate an integration

1. [Open the integration catalog on your data center.](#)
2. Locate the catalog card for the integration you want to activate.
To filter the integrations:
 - [Optional] Select a category.
 - [Optional] Type a string in the search field.
3. Hover over the catalog card.
4. Click **Configure**.
5. Follow the on-screen instructions.

Configuring an active integration

To configure an active integration

1. [Open the integration catalog on your data center.](#)
2. Select the **Integrations in use** tab.
3. Locate the catalog card for the integration you want to configure.
4. Click **Manage**.
The integration configuration screen opens.
5. Follow the on-screen instructions or consult the integration documentation.

Note

Documentation is usually available in the catalog detail page. For more information, see [Opening an integration detail page](#).

Deactivating an active integration

To deactivate an integration

1. [Open the integration catalog on your data center.](#)
2. Select the **Integrations in use** tab.
3. Locate the catalog card for the integration you want to disable.
4. Click **Deactivate**.
5. Click **Delete**.

API clients

Third-party system integrations can use the application programming interfaces (APIs). Access to the APIs is enabled via API clients, which are an integral part of [the OAuth 2.0 authorization framework](#) of the platform.

An API client is a special platform account which represents the third-party system that must authenticate and be authorized to access platform data and services data. API client access is limited to the tenant whose Management Portal administrator creates the client, and any sub-tenants.

Note

The API 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.

API client credentials

The API client credentials consist of the unique identifier (ID) and a secret value. These credentials do not expire, and cannot be used to log in to Management Portal or any other service console.

Note

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

API client flow

1. A Management Portal administrator creates an API client.
2. An administrator enables [the OAuth 2.0 client credentials flow](#) in the third-party system.
3. According to this flow, before accessing the tenant and its services via the API, the system must first send the API client credentials to the platform, using the authorization API.
4. The platform generates and sends back a security token- the unique cryptic string assigned to this specific client.
5. The third-party system must add this token to all API requests.

Note

The security token eliminates the need for passing client credentials with API requests.

For additional security, the security token expires in two hours.

After this time, all API requests with the expired token will fail, and the system must request a new token from the platform.

Creating an API client

To create an API client

1. Log in to 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 **Active** status by default.
5. Copy and save the ID and secret value of the API client and the data center URL. You will need them when enabling [the OAuth 2.0 client credentials flow](#) in the 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. It can be reset.

6. Click **Done**.


Resetting an API client secret value

If you lose your API client secret value, you can generate a new one. The client ID and data center URL do not change.

Important

If you reset the secret value, all security tokens assigned to the client will immediately expire, and API requests with these tokens will fail.

To reset an API client secret value

1. Log in to Management Portal.
2. Click **Settings** > **API clients**.
3. Find the required client in the list.
4. Click , and then click **Reset secret**.
5. Click **Next** to confirm your decision.
6. Copy and save the new API client secret value.

Note

For security reasons, the secret value is displayed only once. There is no way to retrieve this value if you lose it. It can be reset by repeating these steps.

7. Click **Done**.

Disabling an API client


You can disable API clients. If you do, API requests with security tokens that are assigned to the client will fail, but the tokens will not immediately become expired.

Note

Disabling the client does not affect tokens' expiration time.

You can [re-enable the API client](#) at any time.


To disable an API client

1. Log in to 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.

Enabling a disabled API client

If you enable a previously disabled API client, API requests with security tokens that are assigned to the client will succeed **if these tokens have not expired yet**.

To enable a disabled API client

1. Log in to 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 API client will change to **Active**.


Deleting an API client

If you delete an API client, all security tokens assigned to this client will immediately expire, and API requests with these tokens will fail.

Important

There is no way to recover a deleted client.

To delete an API client

1. Log in to 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.

Creating an integration

If you have data or services that you want to integrate with Cyber Protect Cloud, you can either create a native CyberApp using Vendor Portal or use API calls.

CyberApp

Vendor Portal is an online platform that allows third-party software vendors to integrate products and services natively within Cyber Protect Cloud, in accordance with our CyberApp Standard best practices. Vendor Portal integrations are called CyberApps.

Note

For more information about CyberApps and Vendor Portal, see [the Integration Guide](#).

API integrations

There is a full suite of APIs for integrations.

Note

For more information about APIs, see [the platform APIs chapter of the Integration Guide](#).

Index

#

#CyberFit Score by machine 57

A

About the management portal 7

About this document 6

Accessing the management portal and the services 19

Accounts and units 8

Activating an administrator account 19

Activating an integration 106

Antimalware protection widgets 87

API client credentials 107

API client flow 107

API clients 107

API integrations 110

Audit log 72

Audit log fields 72

B

Backup quotas 10, 17

Backup scanning details 67

Backup widgets 88

Billing example for immutable storage 47

Blocked URLs 69

Brute-force protection 39

C

Catalog entries 100

Changing the notification settings for a user 29

Chat sessions widget 71

Checking your notifications 7

Collecting performance data for Cyber Protection agents 74

Configuring an active integration 106

Configuring custom Usage reports 79

Configuring immutable storage 44

Configuring scheduled Usage reports 79

Configuring the settings of the Executive summary report 93

Configuring the updates of the Cyber Protection agent 40

Creating a service desk ticket 50

Creating a unit 20

Creating a user account 21

Creating an API client 107

Creating an Executive summary report 93

Creating an integration 109

Customizing the Executive summary report 94

CyberApp 110

D

Data in Usage reports 80

Data Loss Prevention widget 91

Data protection map 63

Deactivating an active integration 106

Default notification settings enabled by notification type and user role 31

Default thresholds for ETL data collection 76

Defining quotas for your users 17

Deleting a user account 32

Deleting an API client 109

Disabling an API client 108

Disabling and enabling a user account 32

Disaster Recovery quotas 14

Disaster Recovery widgets 90

Discovered devices 56

Disk health monitoring 59

Disk health status alerts 63

Disk health widgets 61

Downloading data for recently affected
workloads 68

E

Enabling a disabled API client 109

Enabling the Advanced Security Awareness
Training for users in your
organization 47

Endpoint Detection and Response (EDR)
widgets 57

Executive summary 84

Executive summary widgets 84

Existing vulnerabilities 65

F

File Sync & Share quotas 16, 18

File Sync & Share widgets 92

Filtering and search 73

G

Geolocation tracking widget 71

H

Hardware inventory widgets 70

How it works 34, 60

I

Immutable storage 43

Immutable storage modes 44

Incident MTTR 58

Integration catalogs 100

Integrations 100

L

Limitations 46, 60

Limiting access to the web interface 48

Limiting access to your company 48

M

Managing two-factor authentication for
users 37

Metrics with zero usage 79

Missing updates by categories 67

Monitoring 37, 54

My Inbox 7

N

Navigation in the management portal 20

Notary quotas 16, 18

Notary widgets 92

Notifications enabled by default per device
type and user role 32

O

Opening an integration detail page 101, 103

Opening Application Catalog 102

Opening your data center integration

catalog 101

Operations dashboard 54

Operations reports 80

Overview 7

P

Password requirements 19

Patch installation history 67

Patch installation status 66

Patch installation summary 66

Patch installation widgets 66

Performance thresholds for ETL data
collection 75

Physical Data Shipping quotas 16

Preventing unlicensed Microsoft 365 users
from signing in 14

Protection status 55

Q

Quota for storage 18

Quota management 9

Quotas for cloud data sources 10

Quotas for storage 13

R

Read-only administrator role 27

Recently affected 68

Report scope 78

Report type 78

Reported data according to widget type 97

Reporting 78

Resetting an API client secret value 108

Resetting two-factor authentication in case of
lost second-factor device 39

Restore operator role 28

S

Searching My Inbox 8

Security incident burndown 58

Sending Executive summary reports 95

Session history 71

Setting up two-factor authentication 34

Setting up two-factor authentication for your
tenants 37

Software inventory widgets 69

Software widgets 90

Step-by-step instructions 19

Submitting service desk tickets via the ticket
portal 53

Supported storages and agents 44

Supported web browsers 7

Switching between the management portal and
the service consoles 20

T

Task management 50

Technician performance widget 72

Time zones in reports 96

To disable two-factor authentication 37

To disable two-factor authentication for a
user 38

To enable two-factor authentication for a
user 39

To reset the trusted browsers for a user 38

To reset the two-factor authentication for a

user 38

Top incident distribution per workload 57

Transferring ownership of a user account 33

Two-factor setup propagation across tenant
levels 36

U

Updating service desk tickets 52

Usage 54

Usage reports 78

User roles available for each service 23

V

Viewing immutable storage usage 46

Viewing quotas for your organization 10

Viewing service desk tickets 50

Viewing your activated integrations 101

Vulnerability assessment and patch
management widgets 89

Vulnerability assessment widgets 65

Vulnerable machines 65

W

Workload network status 59

Workloads overview widgets 85