Cyber Protect Cloud

23.02

Partner Administrator Guide

REVISION: 2/20/2023

Table of contents

About this document **5**

About Cyber Protect **6**

Cyber Protect services 6

Billing modes for Cyber Protect 7

Switching between editions and billing modes 9

Offering items and quota management 11

Services and offering items 11

Using the management portal **24**

Supported web browsers 24

Activating the administrator account 24

Password requirements 24

Accessing the management portal 25

Configuring contacts in the Company profile wizard 25

Accessing the Cyber Protection console from the management portal 26

Navigation in the management portal 26

Limiting the access to the web interface 27

Accessing the services 28

Overview tab 28

Clients tab 28

7-day history bar 29

User accounts and tenants 30

Managing tenants 32

Creating a tenant 32

Enhanced security mode 34

Selecting the services for a tenant 35

Configuring the offering items for a tenant 36

Enabling services for multiple existing tenants 37

Enabling maintenance notifications 39

Configuring self-managed customer profile 39

Configuring company contacts 40

Refreshing the usage data for a tenant 42

Disabling and enabling a tenant 42

Moving a tenant to another tenant 43

Converting a partner tenant to a folder tenant and vice versa 44

Limiting the access to your tenant 45

Deleting a tenant 45

Managing users 46

Creating a user account 46

User roles available for each service 48

Changing the notification settings for a user 53

Disabling and enabling a user account 54

Deleting a user account 55

Transferring ownership of a user account 55

Setting up two-factor authentication 56

How it works 56

Two-factor setup propagation across tenant levels 57

Setting up two-factor authentication for your tenant 59

Managing two-factor authentication for users 59

Resetting two-factor authentication in case of lost second-factor device 61

Brute-force protection 61

Configuring upsell scenarios for your customers 62

Upsell points shown to a customer 63

Managing locations and storage 64

Locations 64

Managing storage 65

Configuring immutable storage 66

Configuring branding and white labeling 68

Branding items 69

Configuring branding 71

Restoring the default branding settings 71

Disabling the branding 71

White labeling 71

Configuring custom web interface URLs 72

Updating agents automatically 73

To update agents automatically 73

To monitor agent updates 75

Monitoring 75

Usage 75

Operations 75

Reporting 94

Usage 94

Operations reports 96

Executive summary 100
Time zones in reports 112
Reported data according to widget type 113
Audit log 115
Audit log fields 116
Filtering and search 117
Advanced Protection packs 118
Included features and advanced packs in Cyber Protect services 118
Included and advanced features in the Protection service 119
Pay as you go and advanced features in the Protection service 122
Advanced Data Loss Prevention 122
Enabling Advanced Data Loss Prevention 123
Advanced Security + EDR 123
Enabling Advanced Security + EDR 123
Advanced Disaster Recovery 124
Advanced Email Security 125
Integrations 126
Integration with third-party systems 126
Setting up an integration for Cyber Protect Cloud 126
Managing API clients 126
Integration references 129
Integration with VMware Cloud Director 131
Limitations 131
Software requirements 132
Configuring RabbitMQ message broker 132
Installing the plug-in for VMware Cloud Director 133
Installing a management agent 133
Installing backup agents 136
Updating the agents 137
Accessing the Cyber Protection web console 138
Creating a backup administrator 139
System report, log files, and configuration files 140
Removing the integration with VMware Cloud Director 141
Privacy settings 142
Index 143

About this document

This document is intended for partner administrators who want to use Cyber Protect Cloud to provide services to their clients.

This document describes how to set up and manage the services available in Cyber Protect Cloud by using the management portal.

About Cyber Protect

Cyber Protect is a cloud platform that enables service providers, resellers, and distributors to deliver data protection services to their partners and customers.

The services are provided at the partner level, down to the customer company level and the end-user level.

The services management is available through web applications called the **service consoles**. The tenant and user account management is available through a web application called the **management portal**.

The management portal enables administrators to:

- Monitor the usage of services and access the service consoles
- Manage tenants
- Manage user accounts
- Configure services and quotas for tenants
- Manage storage
- Manage branding
- Generate reports about the service usage

Cyber Protect services

This section describes feature sets introduced in March 2021 with the new billing model. Read more about the advantages of the new billing model in the Cyber Protect data sheet.

The following services and feature sets are available in Cyber Protect Cloud:

- **Cyber Protect**
  - **Protection** - complete cyber protection with security and management functionality included in the base product, and disaster recovery, back up and recovery, automation, and email security available as pay as you go features. This functionality can be extended with advanced protection packs that are subject to additional charges.
    Advanced protection packs are sets of unique features that address more sophisticated scenarios in a specific functional area, for example, Advanced Backup, Advanced Security, and others. Advanced packs extend the functionality available in the standard Cyber Protect service.

    For more information on Advanced Protection packs, see "Advanced Protection packs" (p. 118).
  - **File Sync & Share** - a solution for secure sharing of corporate content from anywhere, at any time, and on any device.
  - **Physical Data Shipping** - a solution that helps you save time and network traffic by sending the data to the cloud data center on a hard drive.
  - **Notary** - a blockchain-based solution that ensures the authenticity of shared content.
- **Cyber Infrastructure SPLA**

In the management portal, you can select which services and feature sets will be available to your tenants. The configuration is done per tenant, when you provision or edit a tenant, as described in Creating a tenant.

Billing modes for Cyber Protect

A billing mode is a scheme for accounting and billing for the use of services and their features. The billing mode determines what units will be used as the base for pricing calculations. Billing modes can be set by partners at the Customer level.

The licensing engine automatically acquires the offering items depending on what features are requested in protection plans. Users can optimize the level of protection and cost by customizing their protection plans.

Note
You can use only one billing mode per Customer tenant.

Billing modes for the Protection component

The Protection has two billing modes:

- Per workload
- Per gigabyte

The feature set of both billing modes is identical.

In both billing modes, the Protection service includes standard protection features that covers the majority of cyber security risks. Users can use them at no additional charge. The use of included features will be accounted, but not billed for. For a complete list of included and billable offering items, see "Cyber Protect services" (p. 6).

Though an advanced pack is enabled for a customer, billing will start only after the customer starts using the features of that pack in a protection plan. When an advanced feature is applied in a protection plan, the licensing engine automatically assigns the required license to the protected workload.

When the advanced feature is no longer used, the license is revoked and the billing stops. The licensing engine assigns automatically the license that reflects the actual usage of the features.

You can assign licenses only for the standard Cyber Protect service features. Advanced features are billed based on the usage and their licenses cannot be modified manually. The licensing engine assigns and unassigns these licensed automatically. You can change the license type for a workload manually, but it will be reassigned when the protection plan for that workload is modified by a user.

Note
The billing for the advanced protection features does not start when you enable them. Billing starts only after a customer starts using the advanced features in a protection plan. Enabled feature sets will be accounted and included in usage reports, but will not be billed for, unless their features are used.

Billing modes for File Sync & Share

File Sync & Share has the following billing modes:

- Per user
- Per gigabyte

You can also apply the billing rules of the legacy File Sync & Share edition.

Note
The billing for Advanced File Sync & Share does not start when you enable it. Billing starts only after a customer starts using its advanced features. The enabled advanced feature set will be accounted for and included in usage reports, but will not be billed for, unless its features are used.

Billing for Physical Data Shipping

The billing for Physical Data Shipping follows the pay-as-you-go model.

Billing for Notary

The billing for Notary follows the pay-as-you-go model.

Using the billing modes with legacy editions

If you still have not migrated to the current billing model, use the offering items under one of the billing modes to replace the legacy editions. The licensing engine will automatically optimize the licenses that are assigned to the customer to minimize the billable amount.

Note
You cannot mix editions with billing modes.

Switching from legacy editions to the current licensing model

You can manually switch the offering items for your tenants by editing their profile and selecting offering items for them. For more information about the switching process, see "Switching between editions and billing modes" (p. 9).

To switch from editions to billing modes for multiple customers, see Mass edition switch for multiple customers (67942).

Switching between editions and billing modes

In the management portal, you can modify a tenant account to switch offering items between billing modes (per workload to per gigabyte and vice versa) and between legacy editions and billing modes.

For information about mass switching of tenants, see Mass edition switch for multiple customers (67942).

The switching process includes the following steps.

1. Provision the new offering items to a customer tenant (enabling of offering items and quota set up) to match the functionality that was available in the original offering item.
2. Unassign unused offering items and assign the offering items to workloads according to the features used in the protection plans (usage reconciliation).

The following table illustrates the process in both directions.

	Switch direction	
	Edition > Billing modes	**Billing mode > Billing mode**
Offering items switch	Enable offering items to fulfill the functionality that was available in the source edition.	The identical set of the offering items will be enabled.
Quota switch	Quota will be replicated from the source offering item to destination offering items. Source Standard → destination Standard product . Source Standard → destination packs. **Note** If you are switching from an edition with sub-editions (for example, "Cyber Protect (per workload)"), the quotas will be summarized.	Quotas will be replicated from the source offering item to the destination offering item.
Usage switch	Offering items will be reassigned to the workloads according to the features requested in the protection plans assigned on these workloads.	

Example: Switching Cyber Protect Advanced edition to Per workload billing

In this scenario, a customer tenant has Cyber Protect Advanced edition used on 8 workstations, and the quota is set to 10 workloads. 3 of the workstations are using software inventory and patch management in their protection plans, 2 of the workstations have URL filtering enabled in their protection plans, and one of the machines is using continuous data protection. The following table illustrates the conversion of the edition to new offering items.

Source offering items - usage/quota	**Destination offering items - usage/quota**
Cyber Protect Advanced workstation 8/10	• Workstation - 8/10

Source offering items - usage/quota	Destination offering items - usage/quota
	• Advanced Security - 2/10 • Advanced Backup workstation - 1/10 • Advanced Management - 3/10

The following steps were executed during the switch:

1. The offering items that cover the functionality that was available in the source edition were enabled automatically.
2. The quota was replicated on the new offering items.
3. The usage was reconciled according to the actual usage in protection plans: three workloads use features of the Advanced Management pack, two use features from the Advanced Security pack, and one uses features of the Advanced Backup pack.

Example: Cyber Protect per workload edition to Per workload billing

In this example, the customer has multiple editions assigned on workloads. Each workload can have only one edition or one billing mode assigned.

Source offering items - usage/quota	Destination offering items - usage/quota
Cyber Protect Essentials Workstation - 6/12	• Workstation - 14/42 • Advanced Backup workstation – 2/42 • Advanced Security - 13/42 • Advanced Management - 5/42
Cyber Protect Standard Workstation - 5/10	
Cyber Protect Advanced Workstation - 2/10	
Cyber Backup Standard Workstation - 1/10	

The following steps were executed during the switch:

1. The offering items that cover the functionality that was available in all source editions were enabled automatically. With billing modes, multiple offering items can be assigned to a workload as needed.
2. The quotas were summarized and replicated.
3. The usage was reconciled according to the protection plans.

Changing the billing mode for a partner tenant

To change the billing mode for a partner tenant

1. In the management portal, go to **Clients**.
2. Select the partner tenant whose billing mode you want to change, click the ellipsis icon ••• , and then click **Configure**.
3. On the **Cyber Protect** tab, select the service for which you want to change the billing mode and click **Edit**.

4. Select the desired billing mode and enable or disable the available offering items as needed.
5. Click **Save**.

Changing the billing mode for a customer tenant

You can change the billing for a customer tenant by:

- Editing the original billing mode, by enabling or disabling offering items.
- Switching to a completely new billing mode.

For more information about how to edit the available offering items, refer to Enabling or disabling offering items.

To switch the billing mode for a customer tenant

1. In the management portal, go to **Clients**.
2. Select the customer tenant whose edition you want to change, click the ellipsis icon •••, and then click **Configure**.
3. On the **Configure** tab, under **Service**, select the new billing mode.
   A dialog pops up to inform you about the consequences of the change to the new billing mode.
4. Enter your user name to confirm your choice.

Note
This change may take up to 10 minutes to complete.

Offering items and quota management

This section describes the following:

- What are services and offering items?
- How are offering items enabled or disabled?
- What are billing modes?
- What are Advanced protection packs?
- What are legacy editions and sub-editions?
- What are the soft and hard quotas?
- When can the hard quota be exceeded?
- What is backup quota transformation?
- How does the offering item availability affect the installer availability in the service console?

Services and offering items

Services

A cloud service is a set of functionality that is hosted by a partner, or at end customer's private cloud. Usually, services are sold as a subscription or on a pay-as-you-go basis.

The Cyber Protect service integrates cyber security, data protection, and management to protect your endpoints, systems, and data from cyber security threats. The Cyber Protect service consists of several components: Protection, File Sync & Share, Notary, and Physical Data Shipping. Some of them can be extended with advanced functionality by using Advanced protection packs. For detailed information about included and advanced features, see "Cyber Protect services" (p. 6).

Offering items

An offering item is a set of service features that are grouped by specific workload type or functionality, for example, storage, disaster recovery infrastructure, and others. By enabling specific offering items, you determine what workloads can be protected, how many workloads can be protected (by setting quotas), and the level of the protection that will be available to your partners, customers, and their end users (by enabling or disabling advanced protection packs).

The functionality that is not enabled will be hidden from customers and users, unless you configure an upsell scenario. For more information on upsell scenarios, see "Configuring upsell scenarios for your customers" (p. 62).

The feature usage is gathered from the services and reflected on the offering items, which is used in the reports and further billing.

Billing modes and editions

With legacy editions, you can enable one offering item per workload. With billing modes, the functionality is split, so you can enable multiple offering items (service features and advanced packs) per workload to better suit the needs of your customers and apply more precise billing, only for the features that your customers actually use.

For more information about the billing modes for Cyber Protect, see "Billing modes for Cyber Protect" (p. 7).

You can use billing modes or editions to configure the services available to your tenants. You can select one billing mode or one edition per Customer tenant. As a result, to apply different billing modes for different service features, you need to create multiple tenants for a customer. For example, if the customer wants to have Microsoft 365 mailboxes in Per gigabyte billing mode, and Teams in Per workload billing mode, you must create two different customer tenants for this customer.

To limit the use of services in an offering item, you can define quotas for that offering item. See "Soft and hard quotas" (p. 13).

Enabling or disabling offering items

You can enable all offering items available for a given edition or a billing mode, as described in Creating a tenant.

Note
Disabling all offering items of a service does not disable the service automatically.

There are some limitations to disabling offering items, listed in the table below.

Offering item	Disabling	Result
Backup storage	Can be disabled when the usage is equal to zero.	The cloud storage will become unavailable as a destination for backups within a customer tenant.
Local backup	Can be disabled when the usage is equal to zero.	The local storage will become unavailable as a destination for backups within a customer tenant.
Data sources (including Microsoft 365 and Google Workspace)	Can be disabled when the usage is equal to zero.	The backup and recovery of data sources (including Microsoft 365 and Google Workspace) will become unavailable within a customer tenant.
All Disaster Recovery offering items	Can be disabled when the usage is more than zero.	See the details in "Soft and hard quotas".
All Notary offering items	Can be disabled when the usage is equal to zero.	The Notary service will be unavailable within a customer tenant.
All File Sync & Share offering items	Offering items cannot be enabled or disabled separately.	The File Sync & Share service will be unavailable within a customer tenant.
All Physical Data Shipping offering items	Can be disabled when the usage is equal to zero.	The Physical Data Shipping service will be unavailable within a customer tenant.

For an offering item that cannot be disabled when its usage is more than zero, you can manually remove usage, and then disable the corresponding offering item.

Soft and hard quotas

Quotas enable you to limit a tenant's ability to use the service. To set the quotas, select the client on the **Clients** tab, select the service tab, and then click **Edit**.

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 customer's protected workstations reaches 20, the customer 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 your customer 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.

When a hard quota is reached, service gets limited (It is not possible to protect another workload or use more storage). When the hard quota is exceeded, a notification is sent to the user's email address.

Levels on which quotas can be defined

The quotas can be set on the levels listed in the table below.

Tenant/User	Soft quota (only quota)	Hard quota (quota and overage)
Partner	yes	no
Folder	yes	no
Customer	yes	yes
Unit	no	no
User	yes	yes

The soft quotas can be set on the partner and folder levels. On the unit level no quotas can be set. The hard quotas can be set on the customer and user levels.

The total amount of hard quotas that are set on the user level cannot exceed the related customer hard quota.

Setting up soft and hard quotas

To set up quotas for your clients

1. In the management portal, go to **Clients**.
2. Select the client for which you want to setup quotas.
3. Select the **Protection** tab, and then click **Edit**.
4. Select the type of quota that you want to set. For example, select **Workstations** or **Servers**.
5. Click the **Unlimited** link on the right to open the **Quota edit** window.
   - If you want to inform the client about the quota and do not want to limit the client's ability to use the service, set the quota value in the **Soft quota** field.

     The client will receive an email notification upon reaching the quota, but the Cyber Protection service will be still available.

   - If you want to limit the client's ability to use the service, select **Hard quota** and set the quota value in the field below **Hard quota**.

The client will receive an email notification upon reaching the quota, and the Cyber Protection service will be disabled.

6. In the **Quota edit** window, click **Done**, and then click **Save**.

Backup quotas

You can specify the cloud storage quota, the quota for local backup, and the maximum number of machines/devices/websites a user is allowed to protect. The following quotas are available.

Quotas for devices

- **Workstations**
- **Servers**
- **Virtual machines**
- **Mobile devices**
- **Web hosting servers** (Linux-based physical or virtual servers running Plesk, cPanel, DirectAdmin, VirtualMin , or ISPManager control panels)
- **Websites**

A machine/device/website is considered protected as long as at least one protection plan is applied to it. A mobile device becomes protected after the first backup.

When the overage for a number of devices is exceeded, the user cannot apply a protection plan to more devices.

Quotas for cloud data sources

- **Microsoft 365 seats**

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

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

  In the **Per workload** billing mode, the **Microsoft 365 seats** quota is counted per unique users. A unique user is a user who has at least one of the following:

  - Protected mailbox
  - Protected OneDrive
  - Access to at least one protected company-level resource: Microsoft 365 SharePoint Online site, or Microsoft 365 Teams.
    To learn how to check the number of members of a Microsoft 365 SharePoint or Teams site, refer to this knowledge base article.

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, refer to "Preventing unlicensed Microsoft 365 users from signing in" (p. 18).)

The following Microsoft 365 seats are not charged and do not require a per-seat license:

- Shared mailboxes
- Rooms and equipment
- External users with access to backed up SharePoint sites and/or Microsoft Teams

For more information about the licensing options with the per gigabyte billing mode, refer to Cyber Protect Cloud: Microsoft 365 per GB licensing.

For more information about the licensing options with the per workload billing mode, refer to Cyber Protect Cloud: Microsoft 365 licensing and pricing changes.

- **Microsoft 365 Teams**

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

- **Microsoft 365 SharePoint Online**

  This quota is applied by the service provider to the entire company. This quota enables or disables the ability to protect SharePoint Online sites and sets the maximum number of site collections and group sites that can be protected.

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

- **Google Workspace seats**

  This quota is applied by the service provider to the entire company. The company can be allowed to protect **Gmail** mailboxes (including calendar and contacts), **Google Drive** files, or both. Company administrators can view the quota and the usage in the management portal.

- **Google Workspace Shared drive**

  This quota is applied by the service provider to the entire company. This quota enables or disables the ability to protect Google Workspace Shared drives. If the quota is enabled, any number of Shared drives can be protected. Company administrators cannot view the quota in the management portal, but can view the amount of storage occupied by Shared drive backups in the usage reports.

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

A Microsoft 365 seat is considered protected as long as at least one protection plan is applied to the user's mailbox or OneDrive. A Google Workspace seat is considered protected as long as at least one protection plan is applied to the user's mailbox or Google Drive.

When the overage for a number of seats is exceeded, a company administrator cannot apply a protection plan to more seats.

Quotas for storage

- **Local backup**

  The **Local backup** quota limits the total size of local backups that are created by using the cloud infrastructure. An overage cannot be set for this quota.
- **Cloud resources**

  The **Cloud resources** quota combines the quota for backup storage and quotas for disaster recovery. The backup storage quota limits the total size of backups located in the cloud storage. When the backup storage quota overage is exceeded, backups fail.

Exceeding the quota for backup storage

The backup storage quota cannot be exceeded. The protection agent certificate has technical quota that equals the tenant's backup quota + overage. A backup cannot start if the quota is exceeded. If the quota in the certificate is reached during backup creation but the overage is not reached, the backup will complete successfully. If the overage is reached during backup creation, the backup will fail.

Example:

A user tenant has 1 TB of free space of their quota, and the overage configured for this user is 5 TB. The user starts a backup. If the size of the created backup is, for example, 3 TB, the backup will complete successfully because the overage is not exceeded. If the size of the created backup is larger than 6 TB, the backup will fail when the overage is exceeded.

Backup quota transformation

In general, this is how acquiring a backup quota and offering item mapping to resource type works: the system compares the available offering items with the resource type, and then acquires the quota for the matched offering item.

There is also a capability to assign another offering item quota, even if it does not exactly match the resource type. This is called the **backup quota transformation**. If there is no matching offering item, the system tries to find a more expensive appropriate quota for the resource type (automatic backup quota transformation). If nothing appropriate is found, then you can manually assign the service quota to the resource type in the service console.

Example

You want to back up a virtual machine (workstation, agent-based).

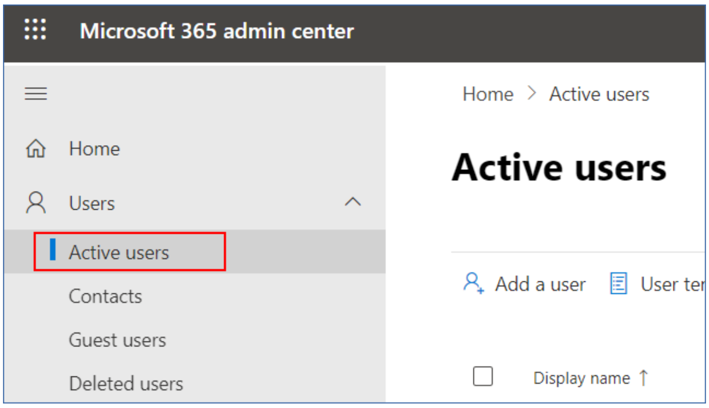
First, the system will check if there is an allocated **Virtual machines** quota. If it is not found, then the system automatically tries to acquire the **Workstations** quota. If that is also not found, the other quota will not be automatically acquired. If you have enough quota that is more expensive than the **Virtual machines** quota and it is applicable to a virtual machine, then you can log in to the service console and assign the **Servers** quota manually.

Preventing unlicensed Microsoft 365 users from signing in

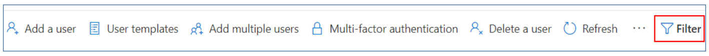
You can prevent all unlicensed users in your Microsoft 365 organization from signing in by editing their sign-in status.

To prevent unlicensed users from signing in

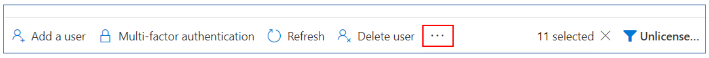
1. Log in to the Microsoft 365 admin center (https://admin.microsoft.com) as a global administrator.
2. In the navigation menu, go to **Users** > **Active Users**.



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.

- **Disaster recovery storage**

  The Disaster Recovery storage shows the cold storage size of the servers that are protected with Disaster Recovery. This storage is calculated starting from the time when a recovery server is created, regardless of whether the server is currently running or not. 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 just start a stopped server. Running servers continue to run.

- **Compute points**

  This quota limits the CPU and RAM resources that are consumed by primary and recovery servers during a billing period. If the overage for this quota is reached, all primary and recovery servers are shut down. It is not possible to use these servers until the beginning of the next billing period. The default billing period is a full calendar month.

  When the quota is disabled, the servers cannot be used regardless of the billing period.
- **Public IP addresses**

  This quota limits the number of public IP addresses that can be assigned to the primary and recovery servers. If the overage for this quota is reached, it is not possible to enable public IP addresses for more servers. You can disallow a server to use a public IP address, by clearing the **Public IP address** check box in the server settings. After that, you can allow another server to use a public IP address, which usually will not be the same one.

  When the quota is disabled, all of the servers stop using public IP addresses, and thus become not reachable from the Internet.
- **Cloud servers**

  This quota limits the total number of primary and recovery servers. If the overage for this quota is reached, it is not possible to create primary or recovery servers.

  When the quota is disabled, the servers are visible in the service console, but the only available operation is **Delete**.
- **Internet access**

  This quota enables or disables the Internet access from the primary and recovery servers.

  When the quota is disabled, the primary and recovery servers will not be able to establish connections to the Internet.

File Sync & Share quotas

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

- **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.

You can define the following Physical Data Shipping quotas for a tenant:

- **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

You can define the following Notary quotas for a tenant:

- **Notary storage**

  The notary storage is the cloud storage where the notarized files, signed files, and files whose notarization or signing is in progress are stored. This quota defines the maximum space that can be occupied by these files.

  To decrease this quota usage, you can delete the already notarized or signed files from the notary storage.
- **Notarizations**

  This quota defines the maximum number of files that can be notarized by using the notary service. A file is considered notarized as soon as it is uploaded to the notary storage and its notarization status changes to In progress.

  If the same file is notarized multiple times, each notarization counts as a new one.
- **eSignatures**

  This quota defines the maximum number of files that can be signed by using the notary service. A file is considered signed as soon as it is sent for signature.

Changing the service quota of machines

The protection level of a machine is defined by the service quota that is applied to it. Service quotas relate to the offering items available for the tenant in which the machine is registered.

A service quota is automatically assigned when a protection plan is applied to a machine for the first time.

The most appropriate quota is assigned, depending on the type of the protected machine, its operating system, required level of protection, and the quota availability. If the most appropriate quota is not available in your organization, the second-best quota is assigned. For example, if the most appropriate quota is **Web Hosting Server** but it is not available, the **Server** quota is assigned.

Examples of quota assignment:

- A physical machine that runs a Windows Server or a Linux operating system is assigned the **Server** quota.
- A physical machine that runs a desktop Windows operating system is assigned the **Workstation** quota.
- A physical machine that runs Windows 10 with enabled Hyper-V role is assigned the **Workstation** quota.
- A desktop machine that runs on a virtual desktop infrastructure and whose protection agent is installed inside the guest operating system (for example, Agent for Windows), is assigned the

Virtual machine quota. This type of machine can also use the **Workstation** quota if the **Virtual machine** quota is not available.

- A desktop machine that runs on a virtual desktop infrastructure and which is backed up in the agentless mode (for example, by Agent for VMware or Agent for Hyper-V), is assigned the **Virtual machine** quota.
- A Hyper-V or vSphere server is assigned the **Server** quota.
- A server with cPanel or Plesk is assigned the **Web Hosting Server** quota. It can also use the **Virtual machine** or the **Server** quota, depending on the type of machine on which the web server runs, if the **Web Hosting Server** quota is not available.
- The application-aware backup requires the **Server** quota, even for a workstation.

You can manually change the original assignment later. For example, to apply a more advanced protection plan to the same machine, you might need to upgrade the machine's service quota. If the features required by this protection plan are not supported by the currently assigned service quota, the protection plan will fail.

Alternatively, you can change the service quota if you purchase a more appropriate quota after the original one is assigned. For example, the **Workstation** quota is assigned to a virtual machine. After you purchase a **Virtual machines** quota, you can manually assign this quota to the machine, instead of the original **Workstation** quota.

You can also release the currently assigned service quota, and then assign this quota to another machine.

You can change the service quota of an individual machine or for a group of machines.

To change the service quota of an individual machine

1. In the Cyber Protection service console, go to **Devices**.
2. Select the desired machine, and then click **Details**.
3. In the **Service quota** section, click **Change**.
4. In the **Change license** window, select the desired service quota or **No quota**, and then click **Change**.

To change the service quota for a group of machines

1. In the Cyber Protection service console, go to **Devices**.
2. Select more than one machine, and then click **Assign quota**.
3. In the **Change license** window, select the desired service quota or **No quota**, and then click **Change**.

Agent installer dependency on offering items

Depending on the allowed offering items, the corresponding agent installer will be available in the **Add devices** section in the service console. In the table below, you can see the agent installers and their availability in the service console depending on the enabled offering items.

Enabled offering item	Servers	Workstations	Virtual machines	Microsoft 365 seats	Google Workspace seats	Mobile devices	Web hosting servers	Websites
Agent installer								
Workstations – Agent for Windows		+	+					+
Workstations – Agent for Mac OS		+	+					+
Servers – Agent for Windows	+		+				+	+
Servers – Agent for Linux	+		+				+	+
Agent for Hyper-V			+					
Agent for VMware			+					
Agent for Virtuozzo			+					
Agent for SQL	+		+					
Agent for Exchange	+		+					
Agent for Active Directory	+		+					
Agent for Microsoft 365				+				
Agent for Google Workspace					+			
Full	+	+	+				+	+

installer for Windows								
Mobile (iOS and Android)						+		

Using the management portal

The following steps will guide you through the basic use of the management portal.

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.

Activating the administrator account

After signing the partnership agreement, 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, refer to "Password requirements" (p. 24).

Password requirements

The password for a user account must be at least 9 characters long. Passwords are also checked for complexity, and fall into one of the following categories:

- Weak
- Medium
- Strong

You cannot save a weak password, even though it might contain 9 characters or more. 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.

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

1. Go to the service login page.

   The address of the login page was included in the activation email message that you received.
2. Type the login, and then click **Next**.
3. Type the password, and then click **Next**.

   > **Note**
   > To prevent   Cyber Protect Cloud from brute force attacks, the portal will lock you out after 10 unsuccessful login attempts. The lockout period is 5 minutes. The number of unsuccessful login attempts is reset after 15 minutes.

4. Use the menu to the right to navigate the management portal.

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

Some services include the capability to switch to the management portal from the service console.

Configuring contacts in the Company profile wizard

You can configure contact information for your company. We will send updates on new features and other important changes in the platform to the contacts you provide.

When you log in to the management portal for the first time, the Company profile wizard guides you through the basic information about the company and the contacts to be provided.

You can create contacts from users that exist in the Cyber Protect platform or add contact information of people who do not have access to the service.

To configure company contacts using the Company profile wizard

1. In the **Company information**, specify the following details of your company:
   - **Official (legal) company name**
   - **Company legal address (headquarters address)**
     - **Country**
     - **Zip code**
2. Click **Next**.
3. In the **Company contacts**, configure contacts for the following purposes:
   - **Billing contact** — the contact that will get updates about important changes in usage reporting in the platform.
   - **Business contact**—the contact that will get updates about important business-related changes in the platform.
   - **Technical contact**—the contact that will get updates about important technical changes in the platform.

   You can use a contact for more than one purpose.

   Select an option to create the contact.

   - **Create from existing user**. Select a user from the drop-down list.
   - **Create a new contact**. Provide the following contact information:
     - **First name** — First name of the contact person. This field is required.
     - **Last name** — Last name of the contact person. This field is required.
     - **Business email** — Email address of the contact person. This field is required.
     - **Business phone** — This field is optional.
     - **Job title** — This field is optional.

4. If you plan to use the Billing contact as a business or technical contact as well, select the corresponding flags in the **Billing contact** section:
   - **Use the same contact for Business contact**
   - **Use the same contact for Technical contact**
5. Click **Done**.

   As a result, the contacts are created. You can edit the information and configure other contacts in the **Company Management > Company profile** section of the management console, as described in Configuring company contacts.

Accessing the Cyber Protection console from the management portal

1. In the management portal, go to **Monitoring** > **Usage**.
2. Under **Cyber Protect**, select **Protection**, and then click **Manage service**.

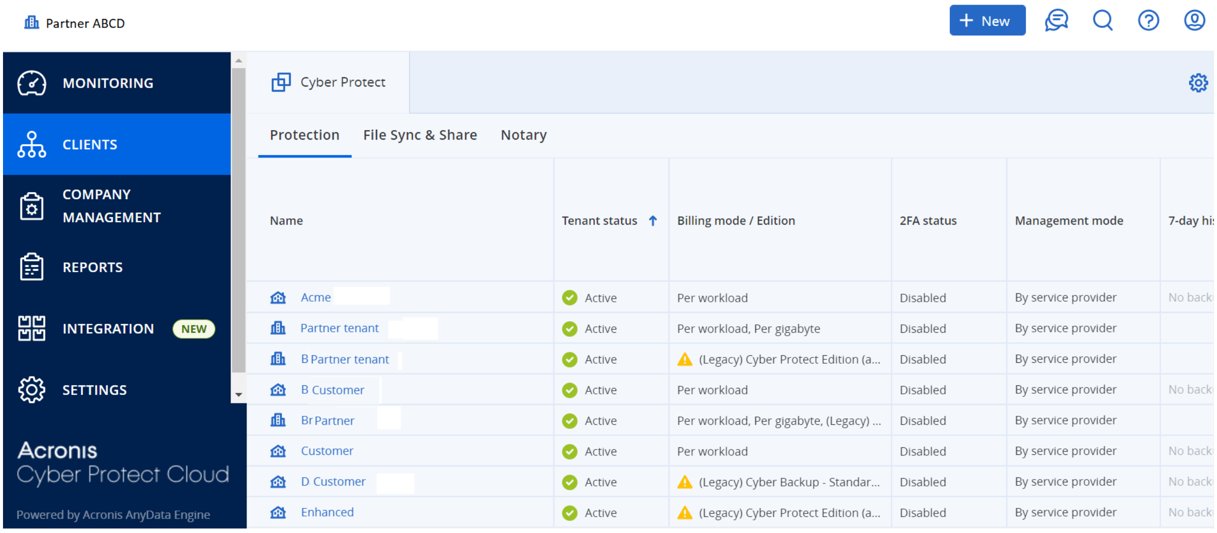
   Alternatively, under **Clients**, select a customer, and then click **Manage service**.

As a result, you are redirected to the Cyber Protection console.

Navigation in the management portal

When using the management portal, at any given time you are operating within a tenant. The name of this tenant is indicated in the top-left corner.

By default, the highest hierarchy level available to you is selected. Click a tenant name in the list to drill down the hierarchy. To navigate back to an upper level, click its name in the top-left corner.



Name	Tenant status ↑	Billing mode / Edition	2FA status	Management mode	7-day hi
Acme	✓ Active	Per workload	Disabled	By service provider	No back
Partner tenant	✓ Active	Per workload, Per gigabyte	Disabled	By service provider	
B Partner tenant	✓ Active	⚠ (Legacy) Cyber Protect Edition (a...	Disabled	By service provider	
B Customer	✓ Active	Per workload	Disabled	By service provider	No back
Br Partner	✓ Active	Per workload, Per gigabyte, (Legacy) ...	Disabled	By service provider	
Customer	✓ Active	Per workload	Disabled	By service provider	No back
D Customer	✓ Active	⚠ (Legacy) Cyber Backup - Standar...	Disabled	By service provider	No back
Enhanced	✓ Active	⚠ (Legacy) Cyber Protect Edition (a...	Disabled	By service provider	No back

All parts of the user interface display and affect only the tenant in which you are currently operating. For example:

- The **Clients** tab displays only the tenants that are direct children of the tenant in which you are currently operating.
- The **Company Management** tab displays the company profile and the user accounts that exist in the tenant in which you are currently operating.
- By using the **New** button, you can create a tenant or a new user account only in the tenant in which you are currently operating.

Limiting the access to the web interface

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

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 the members of the child tenants.

To limit access to the web interface

1. Log in to the management portal.
2. Navigate to the tenant in 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**.

Note

For service providers who use Cyber Infrastructure (hybrid model):

If the **Login control** switch is enabled under **Settings** > **Security** in the management portal, add the external public IP address (or addresses) of the Cyber Infrastructure nodes to the **Allowed IP addresses** list.

Accessing the services

Overview tab

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

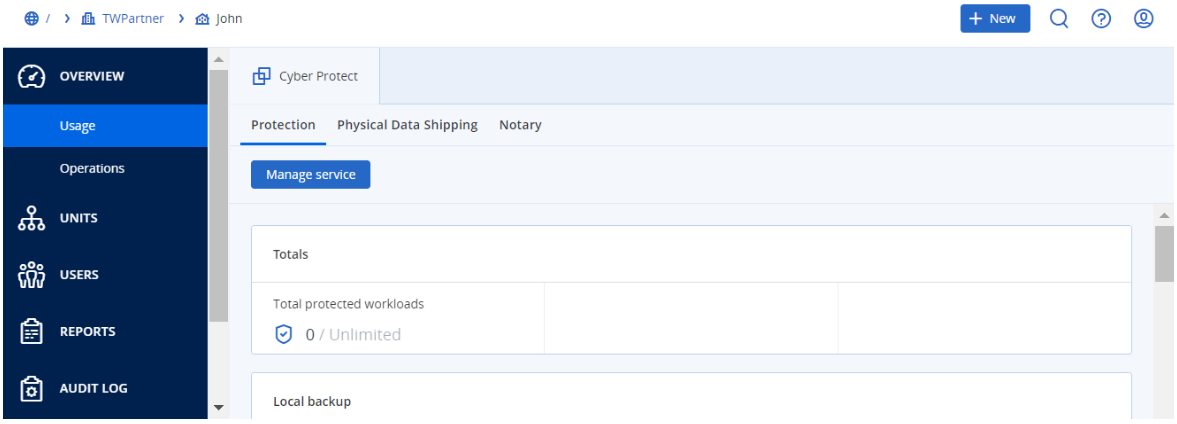
To manage a service for a tenant by using the Overview tab

1. Navigate to the tenant for which you want to manage a service, and then click **Overview** > **Usage**.

   Note that some services can be managed at the partner tenant and at the customer tenant levels, while other services can be managed only at the customer tenant level.

2. Click the name of the service that you want to manage, and then click **Manage service** or **Configure service**.

   For information about using the services, refer to the user guides that are available in the service consoles.

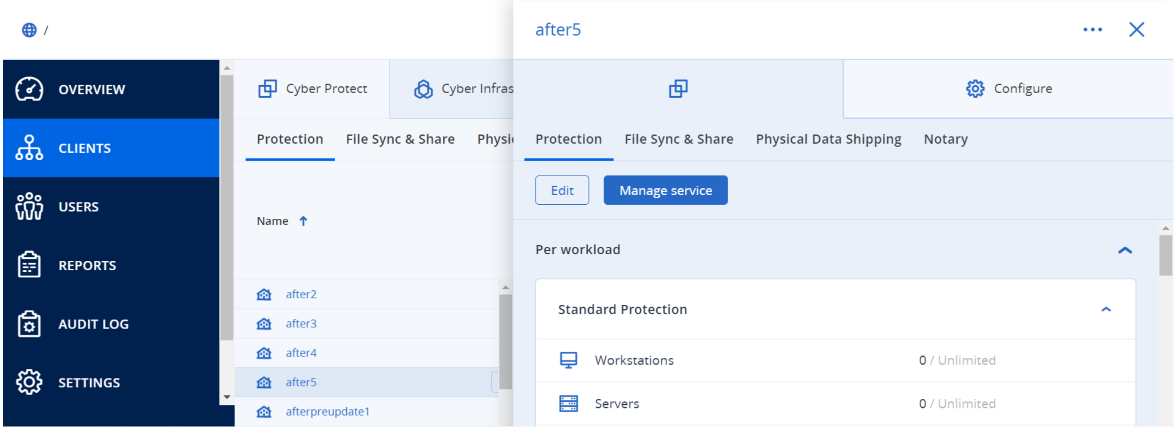


Clients tab

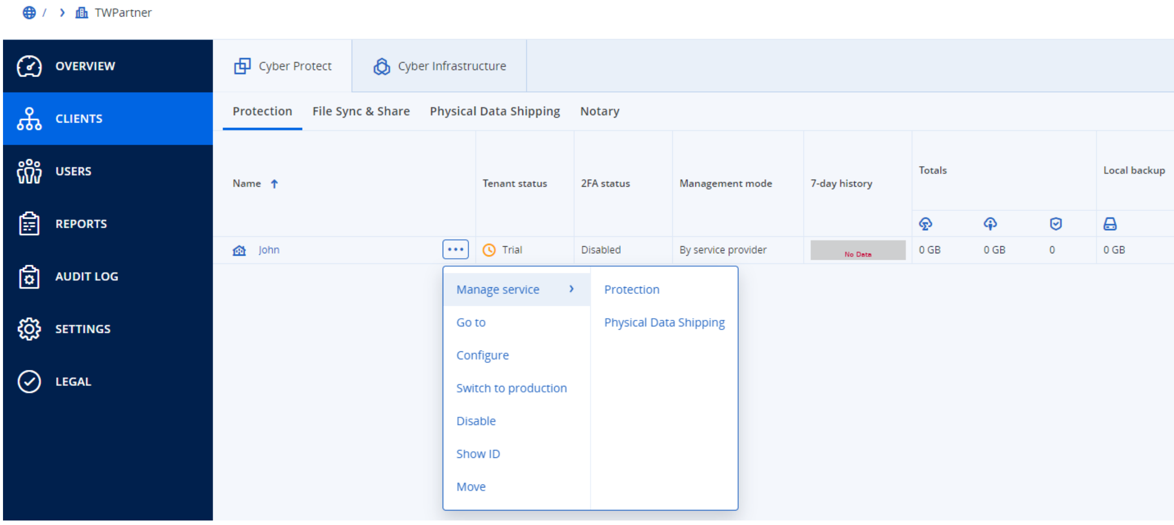
The **Clients** tab displays the child tenants of the tenant in which you are operating and enables you to access the services within them.

To manage a service for a tenant by using the Clients tab

1. Do one of the following:
   - Click **Clients**, select the tenant for which you want to manage a service, click the name or icon of the service that you want to manage, and then click **Manage service** or **Configure service**.



   - Click **Clients**, click the ellipsis icon next to the name of the tenant for which you want to manage a service, click **Manage service**, and then select the service that you want to manage.



Note that some services can be managed at the partner tenant and at the customer tenant levels, while other services can be managed only at the customer tenant level.

For information about using the services, refer to the user guides that are available in the service consoles.

7-day history bar

On the **Clients** screen, the **7-day history** bar shows the status of the workload backups for each customer tenant for the last seven days. The bar is divided into 168 colored lines. Each line represents a one-hour interval, and displays the worst status of a backup within the corresponding one-hour interval.

The following table provides information about the meaning of each color of the lines.

Color	Description
red	at least one of the backups during the one-hour period failed
orange	at least one of the backup during the one-hour period completed with a warning, but without any backup errors
green	there was at least one successful backup during the one-hour period, without any backup errors and warnings
grey	there were no completed backups during the one-hour period

The **7-day history** bar shows "No backups" until the corresponding statistics is gathered.

For partner tenants, the **7-day history** bar is empty, as the aggregated statistics is not supported.

User accounts and tenants

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.

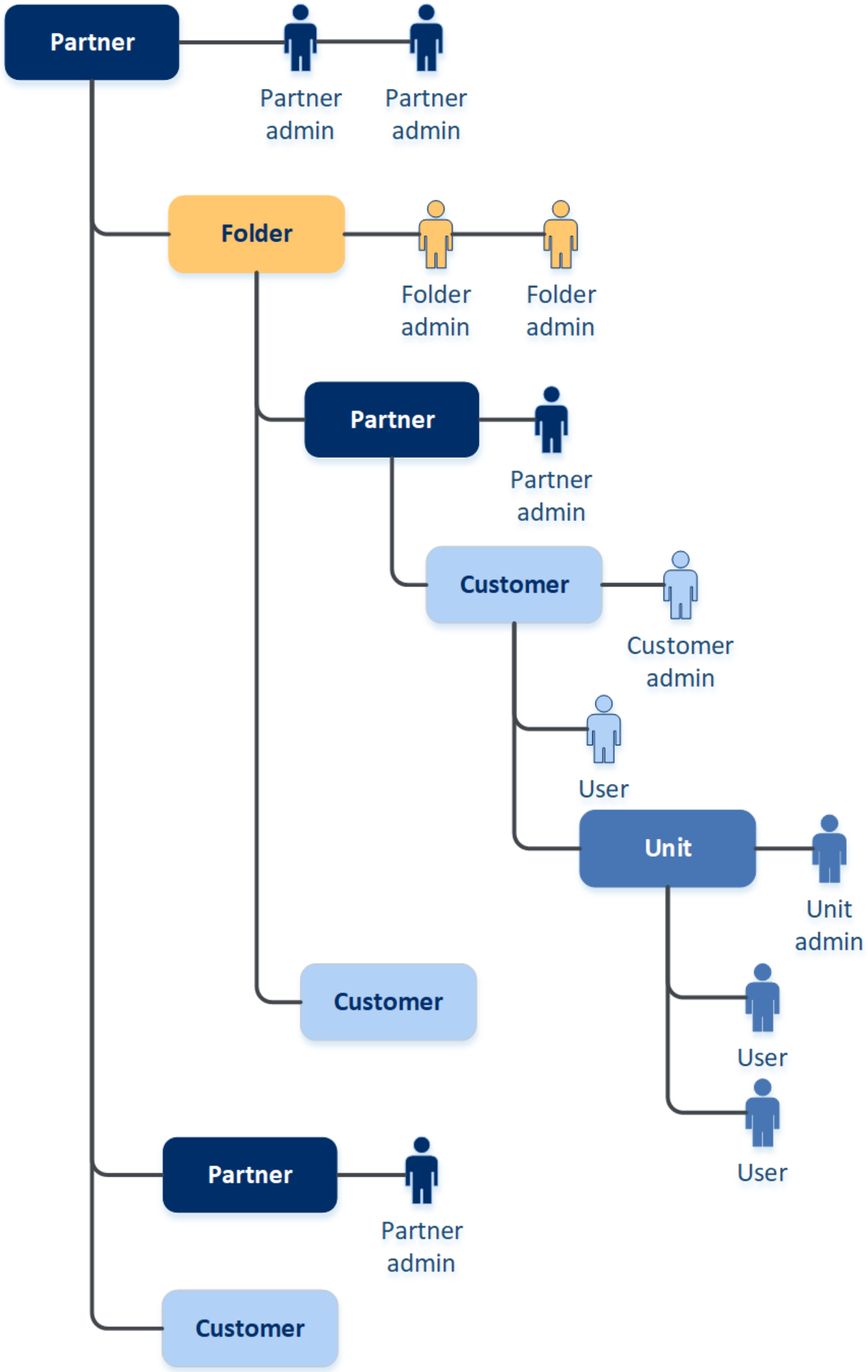
Each account belongs to a tenant. A tenant is a part of the management portal resources (such as user accounts and child tenants) and service offerings (enabled services and offering items within them) dedicated to partner or a customer. The tenant hierarchy is supposed to match the client/vendor relationships between the service users and providers.

- A tenant type of **Partner** typically corresponds to service providers that resell the services.
- A tenant type of **Folder** is a supplementary tenant that is typically used by partner administrators to group partners and customers to configure separate offerings and/or different branding.
- A tenant type of **Customer** typically corresponds to organizations that use the services.
- A tenant type of **Unit** typically corresponds to units or departments within the organization.

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

An administrator of parent tenant of type **Partner** can act as a lower-level administrator in tenants of type **Customer** or **Partner**, whose management mode is **Managed by service provider**. Thus, the partner-level administrator can, for example, manage user accounts and services, or access backups and other resources in the child tenant. However, the administrators at the lower level can limit the access to their tenant for higher-level administrators.

The following diagram illustrates an example hierarchy of the partner, folder, customer, and unit tenants.


Partner
Partner admin
Partner admin
Folder
Folder admin
Folder admin
Partner
Partner admin
Customer
Customer admin
User
Unit
Unit admin
User
User
Customer
Partner
Partner admin
Customer

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

Operation	Users	Customer and unit administrators	Partner and folder administrators
Create tenants	No	Yes	Yes
Create accounts	No	Yes	Yes
Download and install the software	Yes	Yes	No*
Manage services	Yes	Yes	Yes
Create reports about the service usage	No	Yes	Yes
Configure branding	No	No	Yes

*A partner administrator who needs to perform these operations can create a customer administrator or user account for themselves.

Managing tenants

The following tenants are available in Cyber Protect:

- A **Partner** tenant is normally created for each partner that signs the partnership agreement.
- A **Folder** tenant is normally created to group partners and customers to configure separate offerings and/or different branding.
- A **Customer** tenant is normally created for each organization that signs up for a service.
- A **Unit** tenant is created within a customer tenant to expand the service to a new organizational unit.

The steps for creating and configuring a tenant vary depending on the tenant that you create, but in general the process consists of the following steps:

1. Create the tenant.
2. Select services for the tenant.
3. Configure the offering items for the tenant.

Creating a tenant

1. Log in to the management portal.
2. Navigate to the tenant in which you want to create a tenant.
3. In the upper-right corner, click **New**, and then click one of the following, depending on the type of the tenant that you want to create:

- A **Partner** tenant is normally created for each partner that signs the partnership agreement.
- A **Folder** tenant is normally created to group partners and customers to configure separate offerings and/or different branding.
- A **Customer** tenant is normally created for each organization that signs up for a service.
- A **Unit** tenant is created within a customer tenant to expand the service to a new organizational unit.

4. In **Name**, specify a name for the new tenant.
5. [Only when creating a partner tenant] Enter **Official (legal) company name** (required) and **VAT number/TAX ID/Company registration number** (optional).
6. [Only when creating a customer tenant] In **Mode**, select whether the tenant is using services in the trial mode or in the production mode. Monthly service usage reports do not include usage data for trial-mode tenants.

Important

If you switch the mode from trial to production in the middle of a month, the entire month will be included in the monthly service usage report. For this reason, we recommend that you switch the mode on the first day of a month. The mode is automatically switched to production when a tenant remains in the trial mode for one full month.

There are two possible scenarios to automatically switch tenants' trial mode to production:

- In the middle of a month, in which case the entire ***next*** month will be also included in the monthly service usage report.
- [Recommended option] On the first day of a month – then only the current month will be counted.

7. In **Management mode**, select one of the following modes for managing access to the tenant:
   - **Self-service** – this mode limits access to this tenant for administrators of the parent tenant: they can only modify the tenant properties, but cannot access or manage anything inside (e.g. tenants, users, services, backups, and other resources).
   - **Managed by service provider** – this mode grants full access to the tenant for administrators of the parent tenant: modify properties, manage tenants, users, services; access backups and other resources.

   Only the administrator of the tenant created by you will be able to change the Management mode if it is **Self-service**. For this, the administrator of the created tenant can go to **Settings** > **Security** and set up the **Support access** switch.

   You can check the selected Management mode for your child tenants in the **Clients** tab.
8. In **Security**, enable or disable two-factor authentication for the tenant.
   If enabled, all users of this tenant will be required to set up two-factor authentication for their accounts for more secure access. Users must install the authentication application on their second-factor devices and use the one-time generated TOTP code along with the traditional login and password to log in to the console. For more details, refer to "Setting up two-factor authentication". To view the two-factor authentication status for your customers, go to **Clients**.

9. [Only when creating a customer tenant in the Enhanced security mode] In **Security**, select the **Enhanced security mode** check box.

   With this mode, only encrypted backups are allowed. The encryption password must be set on the protected device and without it, creating backups will fail. All operations that require providing the encryption password to a cloud service are not available. For more details, refer to "Enhanced security mode" (p. 34).

   Important
   You cannot disable the Enhanced security mode after the tenant is created.

10. In **Create administrator**, configure an administrator account.

    Note
    The creation of an administrator is mandatory for a customer tenant and for a partner tenant with **Management mode** set to **Self-service**.

    a. Enter a login name and email for the administrator account. The rest of the fields are optional, but provide more communication channels in case we need to contact the administrator.
    b. Select a language.
       If you do not select a language, English will be used by default.
    c. 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.
11. In **Language**, change the default language of notifications, reports, and the software that will be used within this tenant.
12. Do one of the following:
    - To finish the tenant creation, click **Save and close**. In this case, all services will be enabled for the tenant. The billing mode for the Protection service will be set to per workload.
    - To select services for the tenant, click **Next**. See "Selecting the services for a tenant" (p. 35).

Enhanced security mode

The Enhanced security mode provides special settings for clients with increased security demands. This mode requires mandatory encryption for all backups and allows only locally set encryption passwords.

A partner administrator can enable the Enhanced security mode only when creating a new customer tenant, and cannot disable this mode later. Enabling the Enhanced security mode for already existing tenants is not possible.

With the Enhanced security mode, all backups created in a customer tenant and its units are automatically encrypted with the AES algorithm and 256-bit key. Users can set their encryption passwords only on the protected devices, and cannot set the encryption passwords in the protection plans.

Cloud services cannot access the encryption passwords. Due to this limitation, the following features are not available for tenants in the Enhanced security mode:

- Recovery through the service console
- File-level browsing of backups through the service console
- Cloud-to-cloud backup
- Website backup
- Application backup
- Backup of mobile devices
- Antimalware scan of backups
- Safe recovery
- Automatic creation of corporate whitelists
- Data protection map
- Disaster recovery
- Reports and dashboards related to the unavailable features

Limitations

- The Enhanced security mode is compatible only with agents whose version is 15.0.26390 or higher.
- The Enhanced security mode is not available for devices running Red Hat Enterprise Linux 4.x or 5.x, and their derivatives.

Selecting the services for a tenant

By default, all services are enabled when you create a new tenant. You can select which services will be available to the users within the tenant and its child tenants.

You can also select and enable services for multiple existing tenants in one action. For more information, see "Enabling services for multiple existing tenants" (p. 37).

This procedure is not applicable to a unit tenant.

To select the services for a tenant

1. In the **Select services** section of the create/edit tenant dialog, select a billing mode or an edition.
    - Select **Per workload** or **Per gigabyte** billing mode, and then clear the check boxes for the services that you want to disable for the tenant.

  The set of services is identical for both billing modes.

  For Advanced Disaster Recovery, if you registered your own disaster recovery location under your account, you can select the location for disaster recovery from the drop-down list.

- To use a legacy edition, select the **Legacy Editions** radio button, and select an edition from the drop-down list.

Disabled services will be hidden from the users within the tenant and its child tenants.

2. Do one of the following:
   - To finish the tenant creation, click **Save and close**. In this case, all offering items for the selected services will be enabled for the tenant with unlimited quota.
   - To configure the offering items for the tenant, click **Next**. See "Configuring the offering items for a tenant" (p. 36).

Configuring the offering items for a tenant

When you create a new tenant, all offering items for the selected services are enabled. You can select which offering items will be available to the users within the tenant and its child tenants, and set quotas for them.

This procedure is not applicable to a unit tenant.

To configure the offering items for a tenant

1. On the **Configure services** section of the create/edit tenant dialog, under each service tab, clear the check boxes for the offering items that you want to disable.
   The functionality that corresponds to the disabled offering items will be unavailable for the users within the tenant and its child tenants.

   Note
   You can disable offering items that are related to advanced protection functionality, but they will be automatically re-enabled when a user enables an advanced feature in a protection plan.

2. For some services, you can select storages that will be available to the new tenant. Storages are grouped by locations. You can select from the list of locations and storages that are available to your tenant.
   - When creating a partner/folder tenant, you can select multiple locations and storages for each service.
   - When creating a customer tenant, you must select one location, and then select one storage per service within this location. The storages assigned to the customer can be changed later, but only if their usage is 0 GB – that is, either before the customer starts using the storage or after the customer removes all the backups from this storage. The information about the storage space usage is not updated in real time. Please allow up to 24 hours for the information to be updated.

   For details about storages, refer to "Managing locations and storage".

3. To specify the quota for an item, click on the **Unlimited** link next to the offering item.
   These quotas are "soft". If any of these values are exceeded, an email notification is sent to the tenant administrators and the administrators of the parent tenant. Restrictions on using the services are not applied. For a partner tenant it is expected that the offering item usage can exceed the quota because the overage cannot be set when creating a partner tenant.
4. [Only when creating a customer tenant] Specify the quota overages.
   An overage allows a customer tenant to exceed the quota by the specified value. When the overage is exceeded, restrictions on using the corresponding service are applied.
5. Click **Save and close**.

The newly created tenant appears on the **Clients** tab of the management console.

If you want to edit the tenant settings or change the administrator, select the tenant on the **Clients** tab, and then click the pencil icon in the section that you want to edit.

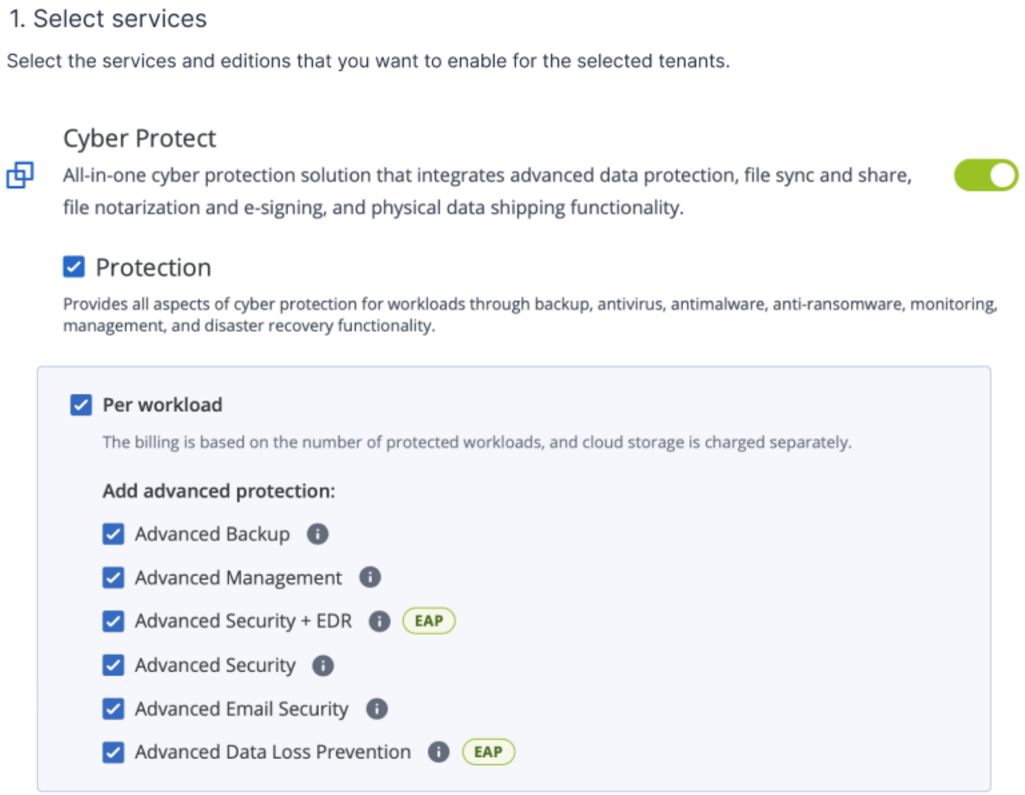
Enabling services for multiple existing tenants

You can mass-enable services, editions, packs, and offering items for multiple tenants (up to a maximum of 100 tenants in one session).

This procedure is applicable to sub-root, partner, folder, and customer tenants. Tenants of any of these different types can be selected simultaneously.

To enable services for multiple tenants

1. In the management portal, go to **Clients**.
2. In the top right corner, click **Configure services**.
3. Select each of the tenants you want to enable services for by selecting the check box next to the tenant name, and then click **Next**.
4. In the **Select services** section, select the relevant services you want to apply to all of the selected tenants, and then click **Next**.



1. Select services

Select the services and editions that you want to enable for the selected tenants.

Cyber Protect

All-in-one cyber protection solution that integrates advanced data protection, file sync and share, file notarization and e-signing, and physical data shipping functionality.

☑ Protection

Provides all aspects of cyber protection for workloads through backup, antivirus, antimalware, anti-ransomware, monitoring, management, and disaster recovery functionality.

☑ Per workload

The billing is based on the number of protected workloads, and cloud storage is charged separately.

Add advanced protection:

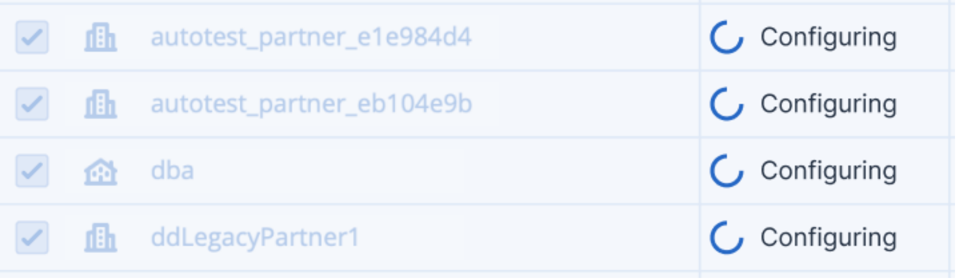
- ☑ Advanced Backup
- ☑ Advanced Management
- ☑ Advanced Security + EDR EAP
- ☑ Advanced Security
- ☑ Advanced Email Security
- ☑ Advanced Data Loss Prevention EAP

Note

You cannot disable a previously enabled service in this screen. All services, editions, and offering items that were selected before you began this procedure will remain enabled.

5. In the **Configure services** section, select the service features and offering items you want to enable for the selected tenants, and then click **Next**.
6. In the **Summary** section, review the changes that will be applied to the selected tenants.

   You can click **Expand all** to see all the tenants' selected services and offering items that will be applied. Alternatively, you can expand each tenant to view the selected services and offering items specific to that tenant.
7. Click **Apply changes**. While the services are configured for each tenant, the tenant is disabled, and the **Tenant status** column indicates the services and offering items are currently being configured, as shown below.



☑	autotest_partner_e1e984d4	Configuring
☑	autotest_partner_eb104e9b	Configuring
☑	dba	Configuring
☑	ddLegacyPartner1	Configuring

8. When the configuration of services and offering items is successfully applied to the selected tenants, a confirmation message is displayed.

If for some reason the services and offering items could not be applied to a tenant, the **Tenant status** column shows **Not applied**. Click **Try again** to review the configuration for the selected tenants.

Enabling maintenance notifications

As a Partner user, you can allow your child tenants (partners and customers) to receive maintenance notification emails directly from the Cyber Protect data center, and receive in-product maintenance notifications inside the Management portal. This will help you to reduce the number of maintenance-related support calls.

Note
The maintenance notification emails are branded by the data center. Custom branding is not supported for these notifications.

To enable the maintenance notifications for child partners or customers

1. Log in to the management portal as a Partner user, click **Clients**, and then click the name of a partner or customer tenant for whom you want to enable the maintenance notifications.
2. Click **Configure**.
3. On the **General settings** tab, locate the **Maintenance notifications** option and enable it.
   If you do not see the **Maintenance notifications** option, contact your service provider.

Note
Maintenance notifications are enabled, but will not be sent until the selected tenant enables the notifications for their users or further propagates this option to child partners or customers to enable notifications for their users.

To enable the maintenance notifications for a user

1. Log in to the management portal as a Partner user or a Company administrator.
   As Partner, you can access the users for all tenants that are managed by you.
2. Navigate to **Company Management** > **Users** , and then click the name of a user for whom you want to enable the maintenance notifications.
3. On the **Services** tab, in the **Settings** section, click the pencil to edit the options.
4. Select the **Maintenance notifications** check box and click **Done**.

The selected user will receive email notifications for upcoming maintenance activities on the data center.

Configuring self-managed customer profile

As a partner, you can configure self-managed customer profiles for the tenants managed by you. This option allows you to control visibility of tenants profile and contact information to each of your customers.

To configure self-managed customer profile

1. In the management portal, go to **Clients**.
2. Select the client for which you want to configure the self-managed customer profile.
3. Select the **Configure** tab, and then select the **General settings** tab.
4. Enable or disable the **Enable self-managed customer profile** switch.

When the self-managed customer profile is enabled, this client will see the **Company profile** section in the navigation menu and the contact-related fields in the user creation wizard (**Business phone**, **Company contact** and **Job title**).

When the self-managed customer profile is disabled, the **Company profile** section in the navigation menu and the contact-related fields in the user creation wizard will be hidden.

Configuring company contacts

As a partner, you can configure contact information for your company and for the tenants managed by you. We will send updates on new features and other important changes in the platform to the contacts in this list.

You can add multiple contacts and assign company contacts, depending on the user role. You can create contacts from users that exist in the Cyber Protect platform or add contact information of people who do not have access to the service.

To configure contacts for your company

1. In the management console, go to **Company Management** > **Company profile**.
2. In the **Contacts** section, click **+**.
3. Select an option to create the contact.
   - **Create from existing user**
     - Select a user from the drop-down list.
     - Select a company contact.
       - **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.

     If you delete a contact that is associated with a user from the list of contacts in the Company profile, the user will not be deleted. The system will unassign all company contacts for the user, so they will no longer appear in the **Company contacts** column of the **Users** list.

     If you want to change the email address of the contact that is associated with the user, the system will request verification of the newly defined address. An email will be sent to this address, and the user will need to confirm the change.

- **Create a new contact**
    - Provide the contact information.
        - **First name**—First name of the contact person. This field is required.
        - **Last name**—Last name of the contact person. This field is required.
        - **Business email**—Email address of the contact person. This field is required.
        - **Business phone**—This field is optional.
        - **Job title**—This field is optional.
    - Select 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.

4. Click **Add**.

To configure contacts for a tenant

Note
If you modify the contact information for a child tenant, your changes will be visible to the tenant.

1. In the management portal, go to **Clients**.
2. Click the tenant, and click **Configure**.
3. In the **Contacts** section, click **+**.
4. Select an option to create the contact.
    - **Create from existing user**
        - Select a user from the drop-down list.
        - Select a company contact.
            - **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.

          If you delete a contact that is associated with a user from the list of contacts in the Company profile, the user will not be deleted. The system will unassign all company contacts for the user, so they will no longer appear in the **Company contacts** column of the **Users** list.

    If you want to change the email address of the contact that is associated with the user, the system will request verification of the newly defined address. An email will be sent to this address, and the user will need to confirm the change.

- **Create a new contact**
    - Provide the contact information.
        - **First name**—First name of the contact person. This field is required.
        - **Last name**—Last name of the contact person. This field is required.
        - **Business email**—Email address of the contact person. This field is required.
        - **Business phone**—This field is optional.
        - **Job title**—This field is optional.
    - Select 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.

5. Click **Add**.

Refreshing the usage data for a tenant

By default, the usage data is refreshed at fixed intervals. You can refresh the usage data for a tenant manually.

1. In the management console, go to **Clients**.
2. Click the tenant, and click the ellipsis in the tenant row.
3. Select **Refresh usage**.

   Note
   Fetching the data may take up to 10 minutes.

4. Reload the page to view the updated data.

Disabling and enabling a tenant

You may need to disable a tenant temporarily. For example, in case your tenant has debts for using services.

To disable a tenant

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

As the result:

- The tenant and all its sub-tenants will be disabled, their services will be stopped.
- Billing of the tenant and its sub-tenants will be continued as their data will be preserved and stored in Cyber Protect Cloud.
- All API clients within the tenant and its sub-tenants will be disabled and all integrations using these clients will stop working.

To enable a tenant, select it in the client list, then click the ellipsis icon > **Enable**.

Moving a tenant to another tenant

The management portal enables you to move a tenant from one parent tenant to another parent tenant. This may be useful if you want to transfer a customer from one partner to another partner, or if you created a folder tenant to organize your clients and want to move some of them to the newly created folder tenant.

Type of tenants that can be moved

Type of tenant	Can be moved	Target tenant
Partner	Yes	Partner or Folder
Folder	Yes	Partner or Folder
Customer	Yes	Partner or Folder
Unit	No	None

Requirements and restrictions

- You can move a tenant only if the target parent tenant has the same or a larger set of services and offering items as the original parent tenant.
- When moving a customer tenant, all storages assigned to the customer tenant in the original parent tenant must exist in the target parent tenant. This is required because the customer service-related data cannot be moved from one storage to another storage.
- In customer tenants that are managed by service providers, there can be plans that are applied to customer workloads from the service provider level (for example, scripting plans).

  When moving such a customer tenant, the plans of the service provider will be revoked from the customer workloads and all services associated with these plans will stop working for this customer.
- You can move tenants inside your partner account hierarchy. You can also move some customer tenants to a target tenant outside your partner account hierarchy. To learn whether that operation is possible, contact your account manager in .
- Only administrators (for example, Administrator in Management Portal or Company administrator) can move tenants to different parent tenants.

How to move a tenant

1. Log in to the management portal.
2. Find and copy the **Internal ID** of the target partner or folder tenant to which you want to move a tenant. Do the following:
   a. On the **Clients** tab, select the target tenant to which you want to move a tenant.
   b. On the tenant properties panel, click the vertical ellipsis icon, and then click **Show ID**.
   c. Copy the text string that is shown in the **Internal ID** field, and then click **Cancel**.
3. Select the tenant that you want to move, and then move it to the target partner/folder. Do the following:
   a. On the **Clients** tab, select the tenant that you want to move.
   b. On the tenant properties panel, click the vertical ellipsis icon, and then click **Move**.
   c. Paste the internal identifier of the target tenant, and then click **Move**.

The operation starts immediately and takes up to 10 minutes.

If the tenant that you are moving has child tenants (for example, it is a partner or folder tenant with a customer tenant inside), the whole tenant sub-tree will be moved to the target tenant.

Converting a partner tenant to a folder tenant and vice versa

The management portal enables you to convert a partner tenant to a folder tenant.

This may be useful if you used a partner tenant for grouping purposes and now want to organize your tenant infrastructure properly. This is also useful if you want the operational dashboard to include aggregated information about the tenant.

You can also convert a folder tenant to a partner tenant.

Note
The conversion is a safe operation and does not affect the users within the tenant and any service-related data.

To convert a tenant

1. Log in to the management portal.
2. On the **Clients** tab, select the tenant that you want to convert.
3. Do one of the following:
   - Click the ellipsis icon next to the tenant name.
   - Select the tenant, and then click the ellipsis icon on the tenant properties panel.
4. Click **Convert to folder** or **Convert to partner**.
5. Confirm your decision.

Limiting the access to your tenant

Administrators at the customer level and higher can limit the access to their tenants for higher-level administrators.

If access to the tenant is limited, the parent tenant administrators can only modify the tenant properties. They do not see the accounts and child tenants at all.

To prevent higher-level administrators from accessing your tenant

1. Log in to the management portal.
2. Go to **Settings** > **Security**.
3. Disable the **Support access** switch.

As a result, the administrators of the parent tenants will have limited access to your tenant. They will only be able to modify the tenant properties, but won't be able to access or manage anything inside (e.g. tenants, users, services, backups and other resources).

If the **Support access** switch is enabled, then the administrators of the parent tenants will have full access to your tenant. They will be able to do the following: modify properties; manage tenants, users, and services; access backups, and other resources.

Deleting a tenant

You may want to delete a tenant in order to free up the resources that it uses. The usage statistics will be updated within a day after deletion. For large tenants it might take longer.

Before deleting a tenant, you have to disable it. For more information on how to do this, refer to Disabling and enabling a tenant.

Important
Deleting a tenant is irreversible!

To delete a tenant

1. In the management portal, go to **Clients**.
2. Select the disabled tenant that you want to delete, and then click the ellipsis icon ••• > **Delete**.
3. To confirm your action, enter your login, and then click **Delete**.

As a result:

- The tenant and its sub-tenants will be deleted.
- All services that were enabled within the tenant and its sub-tenants will be stopped.
- All users within the tenant and its sub-tenants will be deleted.
- All machines in the tenant and its sub-tenants will be unregistered.
- All service-related data, for example backups and synced files, in the tenant and its sub-tenants will be deleted.

- All API clients within the tenant and its sub-tenants will be deleted and all integrations using these clients will stop working.

Managing users

Partner administrators, Customer administrators, and Unit administrators can configure and manage user accounts under the tenants that are accessible to them.

Creating a user account

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

- Partner/folder administrator accounts — to share the services management duties with other people.
- Customer/prospect/unit administrator accounts — to delegate the service management to other people whose access permissions will be strictly limited to the corresponding customer/prospect/unit.
- User accounts within the customer or a unit tenant — to enable the users to access only a subset of the services.

Be aware that existing accounts cannot be moved between tenants. First, you need to create a tenant, and then populate it with accounts.

To create a user account

1. Log in to the management portal.
2. Navigate to the tenant in which you want to create a user account. See "Navigation in the management portal" (p. 26).
3. In the upper-right corner, click **New** > **User**.

   Alternatively, go to **Company management > Users**, and click **+ New**.
4. Specify the following contact information for the account:
   - **Login**

     Important
     Each account must have a unique login.

   - **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.

   - **First name**
   - **Last name**
   - [Optional] **Business phone**

> **Note**
> Fields like **Business phone**, **Job title** and **Company contact** are displayed in user creation wizard only if the parent partner has enabled the **Enable self-managed customer profile** option for the customer tenant. Otherwise, these fields are not displayed.

   - [Optional] **Job title**
   - In **Language**, 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 not have the service administrator role, depending on the service.
   - Otherwise, the user will have the roles that you select in the services that you select.
7. Click **Create**.

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

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 **Company Management** > **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.

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.

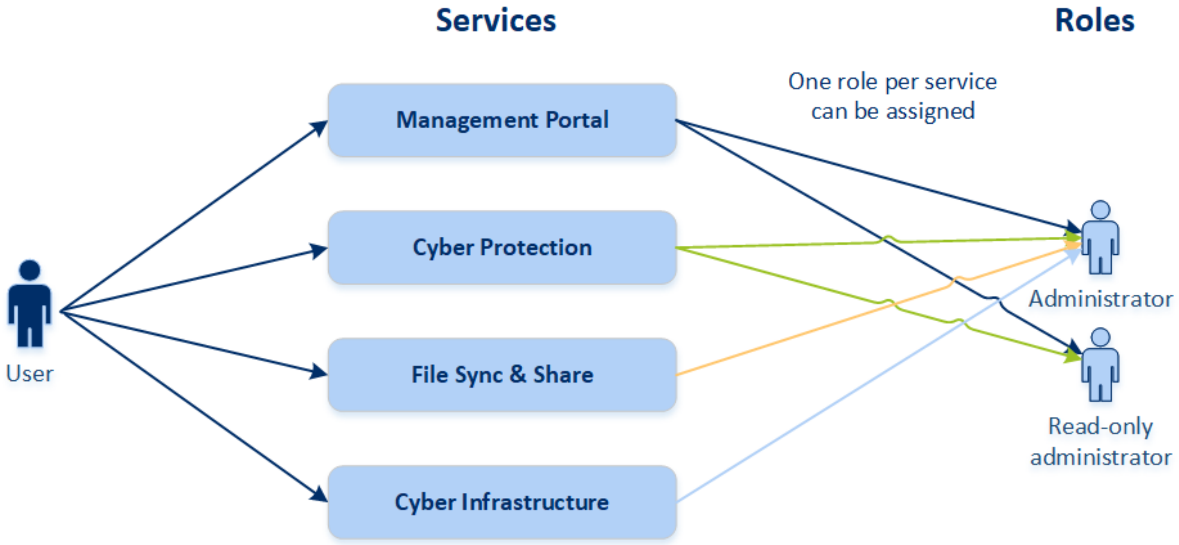
To convert a user account to the service account type

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

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 of the Cyber Protection service is enabled for the company, this role also grants access to the disaster recovery functionality.
Management Portal	Administrator	This role grants access to the management portal where the administrator can manage users within the entire organization.
	Read-only	This role provides read-only access to all objects in the partner's

	administrator Partner level	management portal and the management portal of all this partner's customers. Such users can access data of other users of the organizations in the read-only mode.
	Read-only administrator Customer level	This role provides read-only access to all objects in the management portal of the entire company. Such users can access data of other users of the organization in the read-only mode.
	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. Such users can access data of other users of the organization in the read-only mode.
Cyber Protection	Cyber administrator	In addition to the Administrator role rights, this role enables configuring and managing the Cyber Protection service, and approving actions in Cyber Scripting. The Cyber administrator role is only available for tenants with enabled Advanced Management pack.
	Administrator	This role enables configuring and managing Cyber Protection for your customers. This role is required for configuring and managing the Disaster Recovery functionality and the corporate allowlist.
	Read-only administrator	The role provides read-only access to all objects of the Cyber Protection service. Such users can access data of other users of the organization in the read-only mode. The read-only administrator cannot configure and manage the Disaster Recovery functionality or the corporate allowlist.
	Restore operator	The role provides access to backups of Microsoft 365 and Google Workspace organizations and allows their recovery, while restricting the access to sensitive content.
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.

Read-only administrator role

An account with this role has read-only access to the Cyber Protection web 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.

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.
- Access the file system on source or target machines.

  For example, a read-only administrator cannot see files, folders, or emails on a backed-up machine.
- Change any settings.

  For example, a read-only administrator cannot create a protection plan or change any of its settings.
- Create, update, or delete any data.

  For example, a read-only administrator cannot delete backups.

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

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

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

Restore operator role

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

A restore operator can do the following:

- View alerts and activities.
- Browse and refresh the list of backups.
- Browse backups without accessing their content. The Restore operator can see the names of the backed-up files and the subjects and senders of the backed-up emails.
- Search backups (full text search is not supported).
- Recover cloud-to-cloud backups 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 to a custom location.
- Apply a backup plan or run a backup.
- Access backed-up files or the content of backed-up emails.
- Download backed-up files or email attachments.

- Send backed-up cloud resources, such as emails or calendar items, as email.
- View or recover Microsoft 365 Teams conversations.
- Recover cloud-to-cloud backups to non-original locations, such as a different mailbox, OneDrive, Google Drive, or Microsoft 365 Team.

User roles and Cyber Scripting rights

The available actions with scripts and scripting plans depend on the script status and your user role.

Administrators can manage objects in their own tenant and in its child tenants. They cannot see or access objects on an upper administration level, if any.

Lower-level administrators have only read-only access to the scripting plans applied to their workloads by an upper-level administrator.

The following roles provide rights with regard to Cyber Scripting:

- Company administrator

  This role grants full administrator rights in all services. With regard to Cyber Scripting, it grants the same rights as the Cyber administrator role.

- Cyber administrator

  This role grants full permissions, including approval of scripts that can be used in the tenant, and the ability to run scripts with the **Testing** status.
- Administrator

  This role grants partial permissions, with the ability to run approved scripts as well as create and run scripting plans that use approved scripts.
- Read-only administrator

  This role grants limited permissions, with the ability to view scripts and protection plans that are used in the tenant.
- User

  This role grants partial permissions, with the ability to run approved scripts as well as create and run scripting plans that use approved scripts, but only on the user's own machine.

The following table summarizes all available actions, depending on the script status and the user role.

Role	**Object**	**Script status**		
		Draft	**Testing**	**Approved**
Cyber administrator Company administrator	Scripting plan	Edit (Remove a draft script from a plan) Delete Revoke	Create Edit Apply Enable	Create Edit Apply Enable

		Disable Stop	Run Delete Revoke Disable Stop	Run Delete Revoke Disable Stop
	Script	Create Edit Change status Clone Delete Cancel running	Create Edit Change status Run Clone Delete Cancel running	Create Edit Change status Run Clone Delete Cancel running
Administrator User (for their own workloads)	Scripting plan	View Revoke Disable Stop	View Cancel run	Create Edit Apply Enable Run Delete Revoke Disable Stop
	Script	Create Edit Clone Delete Cancel running	View Clone Cancel running	Run Clone Cancel running
Read-only administrator	Scripting plan	View	View	View
	Script	View	View	View

Changing the notification settings for a user

To change the notifications settings for a user, navigate to **Company Management** > **Users**. Select the user for which you want to configure the notifications, and then click the pencil icon in the **Settings** section. The following notifications settings are available if the Cyber Protection service is enabled for the tenant where the user is created:

- **Quota overuse notifications** (enabled by default)

  Notifications about exceeded quotas.
- **Scheduled usage reports** (enabled by default)

  Usage reports that are sent on the first day of each month.
- **URL branding notifications** (disabled by default)

  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.
- **Failure notifications**, **Warning notifications**, and **Success notifications** (disabled by default)

  Notifications about the execution results of protection plans and the results of disaster recovery operations for each device.
- **Daily recap about active alerts** (enabled by default)

  The daily recap is generated based on the list of active alerts that are present in the service console at the moment when the recap is generated. The recap is generated and sent once a day, between 10:00 and 23:59 UTC. The time when the report is generated and sent depends on the workload in the data center. If there are no active alerts at that time, the recap is not sent. The recap does not include information for past alerts that are no longer active. For example, if a user finds a failed backup and clears the alert, or the backup is retried and succeeds before the recap is generated, the alert will no longer be present and the recap will not include it.
- **Device control notifications** (disabled by default)

  Notifications about attempts to use peripheral devices and ports that are restricted by protection plans with the device control module enabled.
- **Recovery notifications** (disabled by default)

  Notifications about recovery actions on the following resources: user email messages and entire mailbox, public folders, OneDrive / GoogleDrive: entire OneDrive and files or folders, SharePoint files, Teams: Channels, entire Team, email messages, and Team site.

  In the context of these notifications, the following actions are considered recovery actions: send as email, download, or start a recovery operation.
- **Data loss prevention notifications** (disabled by default)

  Notifications about data loss prevention alerts related to the activity of this user on the network.
- **Security incident notifications** (disabled by default)

  Notifications about detected malware during on-access, on-execution, and on-demand scans, and about detections from the behavioral engine and the URL filtering engine.

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 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** (disabled by default)
  Notifications about issues with the Disaster Recovery infrastructure: when the Disaster Recovery infrastructure is unavailable, or the VPN tunnels are unavailable.

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

Notifications received by user role

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

Notification type\User role	User	Customer Administrator
Notifications for own devices	Yes	Yes
Notifications for all devices in the organization	n/a	Yes (except **Security incident notifications**)
Notifications for Microsoft 365, Google Workspace, and other cloud-based backups	n/a	Yes

Notification type\User role	User	Customer and unit administrators	Partner and folder administrator
Notifications for own devices	Yes	Yes	n/a*
Notifications for all devices of the child tenants	n/a	Yes	Yes
Notifications for Microsoft 365, Google Workspace, and other cloud-based backups	n/a	Yes	Yes

* Partner administrators cannot register own devices, but can create their own customer administrator accounts and use those accounts to add own devices. See User accounts and tenants.

Disabling and enabling a user account

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

To disable a user account

1. In the management portal, go to **Users**.
2. Select the user account that you want to disable, and then click the ellipsis icon ••• > **Disable**.

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

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

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

Deleting a user account

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

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

Important
Deleting a user account is irreversible!

To delete a user account

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

As a result:

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

Transferring ownership of a user account

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

Important
You cannot reassign the content of a deleted account.

To transfer the ownership of a user account:

1. In the management portal, go to **Users**.
2. Select the user account whose ownership you want to transfer, and then click the pencil icon in the **General information** section.
3. Replace the existing email with the email of the future account owner, and then click **Done**.
4. Confirm your action by clicking **Yes**.

5. Let the future account owner verify their email address by following the instructions sent there.
6. Select the user account whose ownership you are transferring, and then click the ellipsis icon ••• > **Reset password**.
7. Confirm your action by clicking **Reset**.
8. Let the future account owner reset the password by following the instructions sent to their email address.

The new owner can now access this account.

Setting up two-factor authentication

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

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

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

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

How it works

1. You enable two-factor authentication on your organization level.
2. All of your organization users must install an authentication application on their second-factor devices (mobile phones, laptops, desktops, or tablets). This application will be used for generating one-time TOTP codes. The recommended authenticators:
   - Google Authenticator
     iOS app version (https://apps.apple.com/app/google-authenticator/id388497605)
     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 TOTP secret shown below the QR code and add it manually in the authentication application.

Important
It is highly recommended to save it (print the QR-code, write down the TOTP secret, use the application that supports backing up codes in a cloud). You will need the TOTP secret to reset two-factor authentication in case of lost second-factor device.

6. The one-time TOTP code will be generated in the authentication application. It is automatically regenerated every 30 seconds.
7. The users must enter the TOTP code on the "Set up two-factor authentication" screen after entering their password.
8. As a result, two-factor authentication for the users will be set up.

Now when users log in to the system, they will be asked to provide the login and password, and the one-time TOTP code generated in the authentication application. Users can mark the browser as trusted when they log in to the system, then the TOTP code will not be requested on subsequent logins via this browser.

Two-factor setup propagation across tenant levels

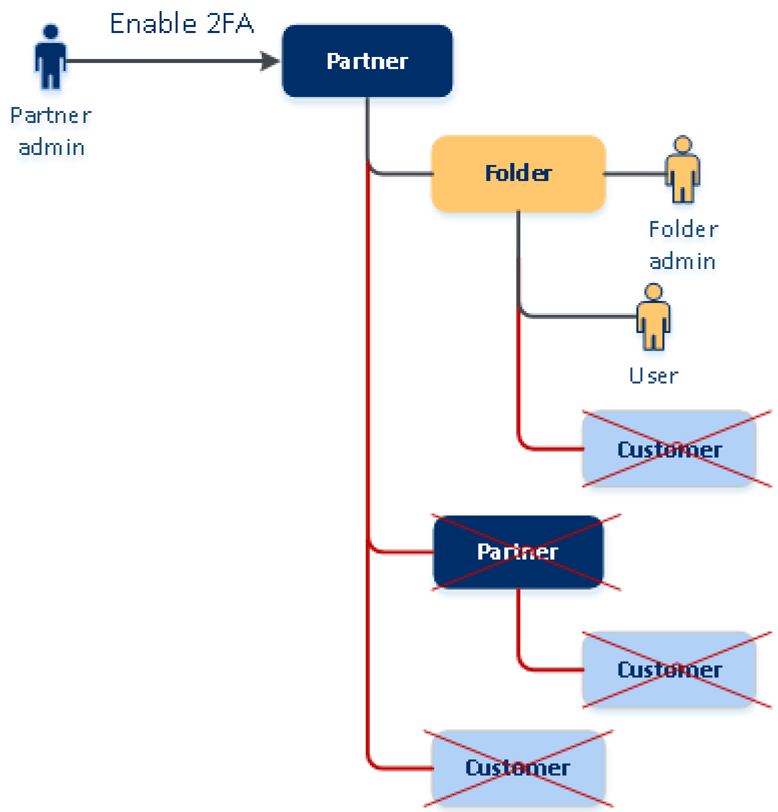
Two-factor authentication is set up on the **organization** level. You can enable or disable two-factor authentication:

- For your own organization.
- For your child tenant (only in case the **Support access** option is enabled within that child tenant).

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

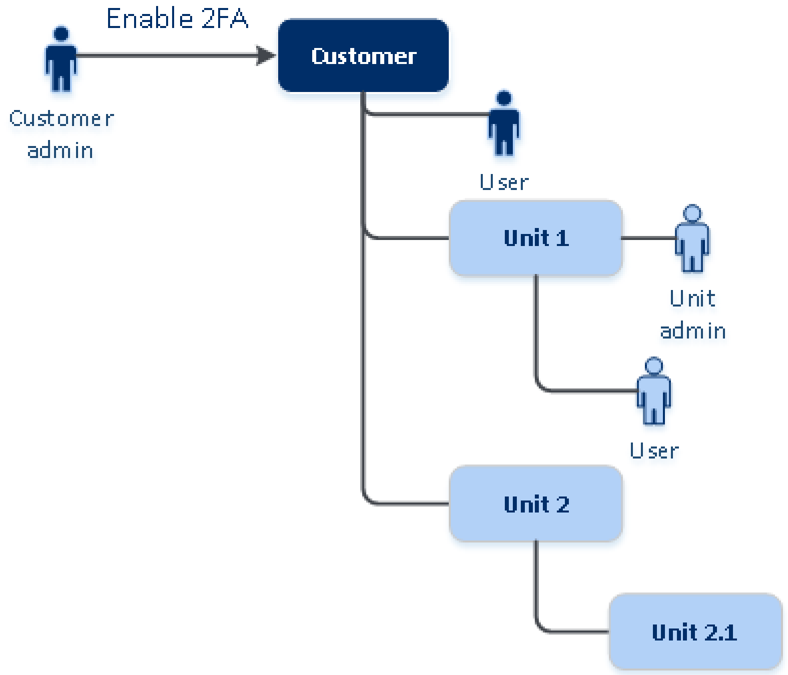
- Folders auto-inherit the two-factor authentication settings from their partner organization. On the scheme below, the red lines mean that the propagation of two-factor authentication settings is not possible.

2FA setting propagation from a partner level



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

2FA setting propagation from a customer level



Note

1. You can enable or disable two-factor authentication for your child organizations only in case the **Support access** option is enabled within that child organization.
2. You can manage the two-factor authentication settings for users of the child organizations only in case the **Support access** option is enabled within that child organization.
3. It is not possible to set up two-factor authentication on the folder or unit level.
4. You can configure the two-factor authentication setting even if your parent organization does not have this setting enabled.

Setting up two-factor authentication for your tenant

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

To enable two-factor authentication for your tenant

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

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

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

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

To disable two-factor authentication for your tenant

1. In the management portal, go to **Settings** > **Security**.
2. To disable two-factor authentication, turn off the toggle, and then click **Disable**.
3. [If at least one user configured two-factor authentication within the organization] Enter the TOTP code generated in your authentication application on the mobile device.

As a result, two-factor authentication is disabled for your organization, all secrets are deleted, and all trusted browsers are forgotten. All users will log in to the system by using only their login and password. On the **Company Management** > **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 **Company Management** > **Users** tab.

Monitoring

In the management portal, under **Company Management** > **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 **Company Management** > **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 **Company Management** > **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 **Company Management** > **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 **Company Management** > **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 upsell scenarios for your customers

Upselling is a technique to invite your customers to buy additional features.

Cyber Protection has several legacy editions, all of which differ in functionality and price. You may want to promote more expensive editions with more advanced capabilities for your existing customers who are using basic editions.

You can enable or disable the upsell capability per customer. By default, the upsell option is disabled. If you enable the upsell for a customer, they will then see additional functionality that is not available until the customer purchases the promoted edition. This additional functionality is marked with labels that show the name or icons of the promoted edition, all highlighted in orange. These upsell points will be shown to a customer, to motivate them to buy a more expensive edition. When clicking on these upsell points, a customer will see a dialog suggesting they purchase a more expensive edition, to enable the desired functionality.

The action item depends on the type of a customer user. The type of users (buyer or not buyer) can be configure by using the platform API, for details refer to the API documentation. For more information about action items, shown to your customers, refer to the table below:

Type of users in customer tenant	Action item
Administrator; buyer	The **Buy now** button is shown in the user interface.*
Administrator; not buyer	The message "Contact your partner to upgrade the edition" is shown in

	the user interface.
User; buyer	The message "Contact your partner to upgrade the edition" is shown in the user interface.
User; not buyer	The message "Contact your partner to upgrade the edition" is shown in the user interface.

* The link for the **Buy now** button, which will redirect a customer to a website to purchase a more advanced edition, can be configured in **Settings** > **Branding**. In the **Upsell** section, you can specify **Buy URL**. The branding settings will be applied to all direct and indirect child partners/folders and customers of the tenant where the branding is configured.

To enable or disable the upsell capability for a customer

1. In the management portal, go to **Clients**.
2. Select the customer, go to the right pane, and then click the **Configure** tab.
3. In the **Upsell** section, do the following:
   - Enable **Promote more advanced editions**, to turn on the upsell scenario for customers.
   - Disable **Promote more advanced editions**, to turn off the upsell scenario for customers.

Upsell points shown to a customer

Vulnerability list

In the service console, the vulnerability list can be found in **Software management** > **Vulnerabilities**. When a user clicks on the stitch icon, the edition promotion dialog will be opened to prompt the user to buy the more expensive edition.

Creating or editing a protection plan

In the service console, this can be found in **Plans** > **Protection**. Click **Create plan**. Cyber Backup editions have only the **Backup** and **Vulnerability** modules enabled; the rest of the modules are available only in the Cyber Protect editions. Your customer will be able to get all the modules enabled after buying one of the Cyber Protect editions.

Autodiscovery wizard

In the service console, this wizard can be found in **Devices** > **All devices**. Your customer should launch the autodiscovery wizard by clicking **Add**, and then going to the **Multiple devices** section, and then clicking **Windows only**. The automatic machine discovery methods will be available only in the Advanced editions.

Actions in the Device list

In the service console, this list can be found in **Devices** > **All devices**. Your customer should select the machine and then two additional options will be shown in the left pane:

- **Connect via HTML5 client**
- **Patch**

These options will be available only if a customer buys a more expensive edition than the existing one.

Managing locations and storage

The **Settings** > **Locations** section shows the cloud storages and disaster recovery infrastructures that you can use to provide the **Cyber Protection** and the **File Sync & Share** services to your partners and customers.

Storages configured for other services will be shown on the **Locations** section in the future releases.

Locations

A location is a container that enables you to conveniently group the cloud storages and disaster recovery infrastructures. It can represent anything of your choice, like a specific data center or a geographical location of your infrastructure components.

You can create any number of locations and populate them with backup storages, disaster recovery infrastructures, and **File Sync & Share** storages. A location can contain multiple cloud storages but only one disaster recovery infrastructure.

For information about operations with storages, refer to "Managing storage".

Choosing locations and storages for partners and customers

When creating a partner/folder tenant, you can select multiple locations and multiple storages per service within them that will be available in the new tenant.

When creating a customer tenant, you must select one location, and then select one storage per service within this location. The storages assigned to the customer can be changed later, but only if their usage is 0 GB – that is, either before the customer starts using the storage or after the customer removes all the backups from this storage.

The information about the storages that are assigned to a customer tenant is shown on the tenant details panel when the tenant is selected on the **Clients** tab. The information about the storage space usage is not updated in real time. Please allow up to 24 hours for the information to be updated.

Operations with locations

To create a new location, click **Add location**, and then specify the location name.

To move a storage or a disaster recovery infrastructure to another location, select the storage or the infrastructure, click the pencil icon in the **Location** field, and then select the target location.

To rename a location, click the ellipsis icon next to the location name, click **Rename**, and then specify the new location name.

To delete a location, click the ellipsis icon next to the location name, click **Delete**, and then confirm your decision. Only empty locations can be deleted.

Managing storage

Adding new storages

- **Cyber Protection** service:
  - By default, the backup storages are located in data centers.
  - If the **Partner-owned backup storage** offering item is enabled for a partner tenant by an upper-level administrator, the partner administrators can organize the storage in the partner's own data center, by using the Cyber Infrastructure software. Click **Add backup storage** on the **Locations** section to find information about organizing a backup storage in your own data center.
  - If the **Partner-owned disaster recovery infrastructure** offering item is enabled for a partner tenant by an upper-level administrator, the partner administrators can organize a disaster recovery infrastructure in the partner's own data center. For information about adding a disaster recovery infrastructure, contact the technical support.

  Note
  Backup validation is not possible with public cloud object storages, such as Amazon S3, Microsoft Azure, Google Cloud Storage, and Wasabi, used by the data centers.
  Backup validation is possible with public cloud object storages used by partners. However, enabling it is not recommended because the validation operations increase the egress traffic from these public object storages and may lead to significant expenses.

- For information about adding storages that will be used by other services, contact the technical support.

Deleting storages

You can delete storages that were added by you or your child tenants.

If the storage is assigned to any customer tenants, you must disable the service that uses the storage for all customer tenants, before deleting the storage.

To delete a storage

1. Log in to the management portal.
2. Navigate to the tenant in which the storage was added.
3. Click **Settings** > **Locations**.
4. Select the storage that you want to delete.

5. On the storage properties panel, click the ellipsis icon, and then click **Delete storage**.
6. Confirm your decision.

Configuring immutable storage

You can configure immutable storage on the partner level and on the customer level.

For partner tenants, there is no selection of immutable storage modes. An administrator can disable and re-enable immutable storage, and change its mode and retention period.

For customer tenants, immutable storage is available in the following modes:

- **Governance mode**
  In this mode, an administrator can disable and re-enable immutable storage, and change its mode and retention period.
- **Compliance mode**
  After this mode is selected, immutable storage cannot be disabled, and its mode or retention period cannot be changed anymore.

When no custom settings are applied to a child tenant, the child tenant inherits the settings of the parent tenant.

You can configure the immutable storage settings only if two-factor authentication is enabled for the tenant to which the administrator account belongs.

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

Note
Starting with the 21.12 release, immutable storage with a retention period of 14 days is enabled by default for new partner tenants. For existing tenants, you need to enable immutable storage manually.

To enable immutable storage for a partner tenant

1. Log in to the management portal as an administrator, and then go to **Settings** > **Security**.
2. Enable the **Immutable storage** switch.
3. Specify a retention period within the range of 14 to 999 days.
   The default retention period is 14 days. A longer retention period may result in increased storage usage.
4. Click **Save**.

To disable immutable storage for a partner tenant

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

Warning!
This change will be inherited by all child tenants that do not use custom settings for immutable storage. All deleted backups will be permanently erased. Deleting new backups will also be permanent.

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

To enable immutable storage for a customer tenant

1. Log in to the management portal as an administrator, and then go to **Clients**.
2. To edit the settings for a customer tenant, click its name.
3. In the navigation menu, go to **Settings** > **Security**.
4. Enable the **Immutable storage** switch.
5. Specify a retention period within the range of 14 to 999 days.

   The default retention period is 14 days. A longer retention period may result in increased storage usage.
6. Select the immutable storage mode.

Warning!
Selecting **Compliance mode** is irreversible. You cannot disable the immutable storage anymore, and you cannot change its mode or retention period.

7. Click **Save**.

To disable immutable storage for a customer tenant

1. Log in to the management portal as an administrator, and then go to **Clients**.
2. To edit the settings for a customer tenant, click its name.
3. In the navigation menu, go to **Settings** > **Security**.
4. Disable the **Immutable storage** switch.

Note
You can disable immutable storage only in Governance mode.

Warning!
If you disable immutable storage, all deleted backups will be permanently erased. Deleting new backups will also be permanent.

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

Limitations

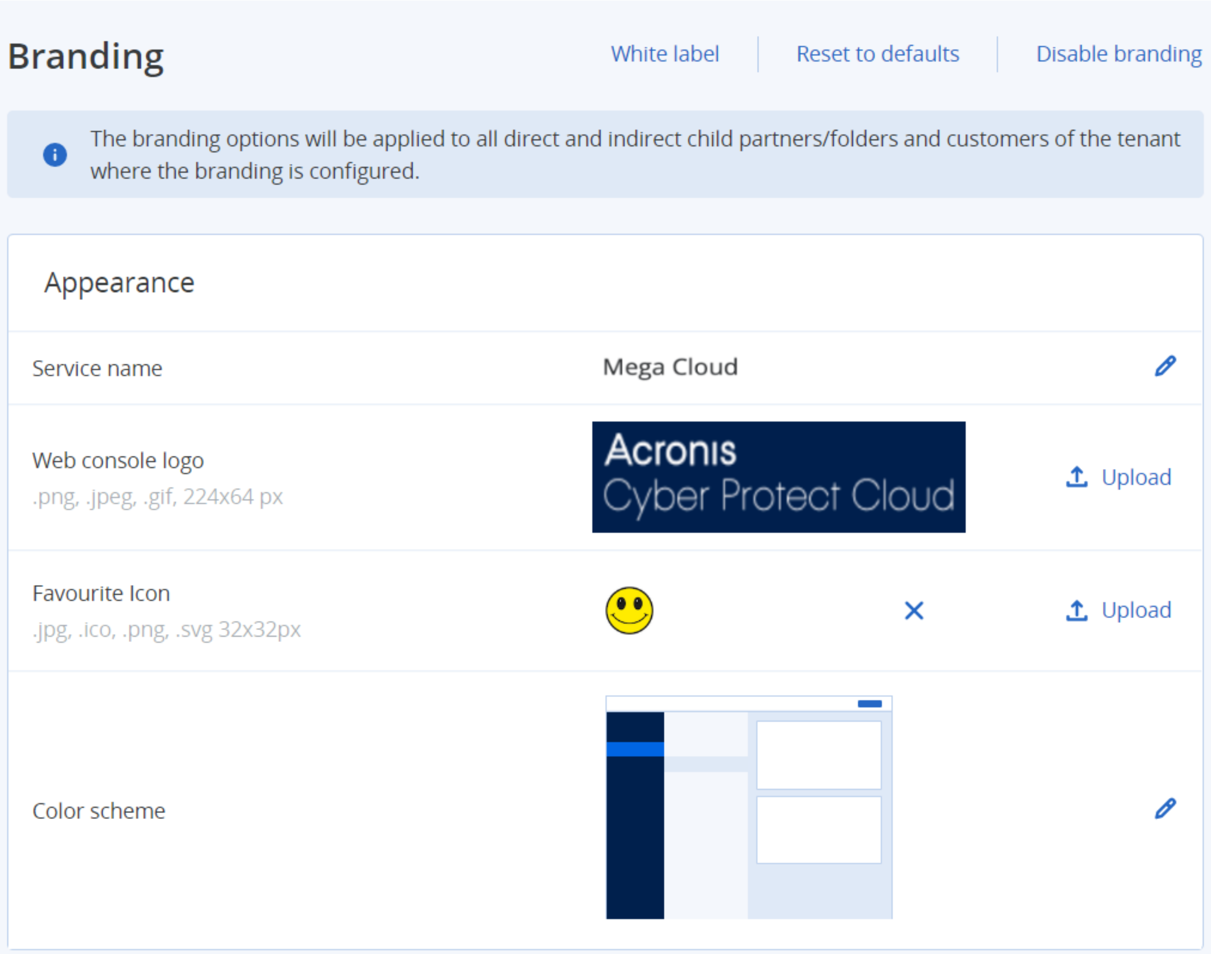
- Immutable storage is available for Acronis-hosted and partner-hosted storages that use Acronis Cyber Infrastructure version 4.7.1 or later.

Immutable storage requires that TCP port 40440 is open for the Backup Gateway service in Acronis 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, refer to the 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 branding and white labeling

The **Settings** > **Branding** section enables partner administrators to customize the user interface of the management portal and the **Cyber Protection** service to remove any association with the higher-level partners.



Branding

The branding options will be applied to all direct and indirect child partners/folders and customers of the tenant where the branding is configured.

Appearance

Service name	Mega Cloud	
Web console logo .png, .jpeg, .gif, 224x64 px	Acronis Cyber Protect Cloud	Upload
Favourite Icon .jpg, .ico, .png, .svg 32x32px		Upload
Color scheme		

Branding can be configured on the partner and the folder levels. The branding is applied to all direct and indirect child partners/folders and customers of the tenant where the branding is configured.

Other services provide separate branding capabilities in their service consoles. For more information, refer to the user guides of the corresponding services.

Branding items

Appearance

- **Service name**. This name is used in all email messages that are sent by the management portal and Cloud services (account activation messages, service notification email messages), on the **Welcome** screen after the first login, and as the management portal browser tab name.
- **Web console logo**. The logo is displayed in the management portal and the services. Click **Upload** to upload an image file.
- **Favourite Icon** [Available only if a custom URL is configured]. The favicon is displayed next to the page title in the browser tab. Click **Upload** to upload an image file.
- **Color scheme**. The color scheme defines the combination of colors that is used for all user interface elements.

Note
Click **Preview scheme in a new tab** to preview what the interface will look like to your child tenants. The branding will not be applied until you click **Done** on the **Choose color scheme** panel.

Agent and installer branding

You can customize the branding of agent installation files and tray monitor for Windows and macOS.

Note
To enable this branding functionality, you must update the Cyber Protection agents to version 15.0.28816 (Release 22.01) or later.

- **Agent installer filename**. The name of the installation file that is downloaded on protected workloads.
- **Agent installer logo**. The logo that is displayed in the Setup wizard during agent installation. Click **Upload** to upload an image file.
- **Agent name**. The name that is displayed in the Setup wizard during agent installation.
- **Tray monitor name**. The name that is displayed on top of the tray monitor window.

Documentation and support

- **Home URL**. This page is opened when a user clicks the company name on the **About** panel.
- **Support URL**. This page is opened when a user clicks the **Contact support** link on the **About** panel or in an email message that is sent by the management portal.
- **Support phone**. This phone number is shown on the **About** panel.
- **Knowledge base URL**. This page is opened when a user clicks the **Knowledge base** link in an error message.

- **Management Portal administrator's guide**. This page is opened when a user clicks the question mark icon in the upper-right corner of the management portal user interface, and then clicks **About** > **Administrator guide**.
- **Management Portal administrator's help**. This page is opened when a user clicks the question mark icon in the upper-right corner of the management portal user interface, and then clicks **Help**.

URL for Cyber Protect Cloud services

You can make Cyber Protect Cloud services available from your custom domain. Click **Configure** to set a custom URL for the first time, or click **Reconfigure** to change the existing one. To use the default URL (https://cloud.acronis.com), click **Reset to default**. For more information about custom URLs, refer to "Configuring custom web interface URLs".

Legal documents settings

- **End-user License agreement (EULA) URL**. This page is opened when a user clicks the **End-user license agreement** link on the **About** panel, on the **Welcome** screen after the first login, and on File Sync & Share Upload Request landing pages.
- **Platform terms URL**. This page is opened when a partner administrator clicks the **Platform terms** link on the **About** panel or the **Welcome** screen after the first login.
- **Privacy statement URL**. This page is opened when a user clicks the **Privacy statement** link on the **Welcome** screen after the first login, and on File Sync & Share Upload Request landing pages.

Important
If you do not want a document to appear on the Welcome screen, do not enter a URL for that document.

Note
For more information about File Sync & Share Upload Requests, see the Cyber Files Cloud User's Guide.

Upsell

- **Buy URL**. This page is opened when a user clicks **Buy now** to upgrade to a more advanced edition of the Cyber Protection service. For more information about upsell scenarios, refer to "Configuring upsell scenarios for your customers".

Mobile apps

- **App Store**. This page is opened when the user clicks **Add** > **iOS** in the **Cyber Protection** service.
- **Google Play**. This page is opened when the user clicks **Add** > **Android** in the **Cyber Protection** service.

Email server settings

You can specify a custom email server that will be used to send email notifications from the management portal and the services. To specify a custom email server, click **Customize**, and then specify the following settings:

- In **From**, enter the name that will be shown in the **From** field of the email notifications.
- In **SMTP**, enter the name of the outgoing mail server (SMTP).
- In **Port**, enter the port of the outgoing mail server. By default, the port is set to 25.
- In **Encryption**, select whether to use SSL or TLS encryption. Select **None** to disable encryption.
- In **User name** and **Password**, specify the credentials of an account that will be used to send messages.

Configuring branding

1. Log in to the management portal.
2. Navigate to the tenant in which you want to configure branding.
3. Click **Settings** > **Branding**.
4. [If branding has not been enabled yet] Click **Enable branding**.
5. Configure the branding items described above.

Restoring the default branding settings

You can reset all branding items to their default values.

1. Log in to the management portal.
2. Navigate to the tenant in which you want to reset the branding.
3. Click **Settings** > **Branding**.
4. In the upper right, click **Restore to defaults**.

Disabling the branding

You can disable the branding for your account and all child tenants.

1. Log in to the management portal.
2. Navigate to the tenant in which you want to disable the branding.
3. Click **Settings** > **Branding**.
4. In the upper right, click **Disable branding**.

White labeling

You can control if the Cyber Protection agent (for Windows, macOS, and Linux) and Cyber Protection Monitor (for Windows, macOS, and Linux) will be branded or white-labeled for all your child partners and customers. If you enable white labeling, the agent and tray monitor will be white-labeled. This setting will also affect the names and logos used in the installer and the Cyber Protection Monitor.

Applying white labeling

1. Log in to the management portal.
2. Navigate to the tenant in which you want to apply white labeling.
3. Click **Settings** > **Branding**.
4. In the upper end of the window, click **White label** to clear all branding items, except for **Service name**, **End-user License agreement (EULA) URL**, **Management portal administrator's guide**, **Management portal administrator's help**, and **Email server settings**.

Configuring custom web interface URLs

Note
A customized URL will point to a different IP address compared to the default URL. Keep it in mind when configuring firewall policies.

To configure the web interface URL for Cyber Protect Cloud services

1. In the management portal, click **Settings** > **Branding**.
2. In the **URL for Cyber Protect Cloud services** section:
   - Click **Configure** to set a custom URL for the first time.
   - Click **Reconfigure** to change the existing custom URL.
3. On the **Domain Settings** step, prepare your domain and CNAME record.

   To use a custom URL, you must have an active domain name and a CNAME record that is configured to point to the data center where your account is. The configuration of the CNAME record is done by your DNS registrar and might take up to 48 hours to propagate.

   To locate the domain name of your data center and request the configuration of your CNAME record, refer to article Branding Web Console URL (58275).
4. On the **Check Your URL** step, verify that your custom URL is accessible, and that your CNAME record is configured correctly. To do that, enter the main URL name and click **Check**. If you use a wildcard SSL certificate, you can add up to ten alternative domain names. If you use a "Let's Encrypt" certificate, alternative domain names will be ignored.
5. On the **SSL Certificate** step, you can do one of the following:
   - Create a "Let's Encrypt" certificate. To do this, click **Free SSL certificate with "Let's Encrypt"**. This option uses "Let's Encrypt" certificates issued by a third-party entity. The service provider is not liable for any issues resulting from the use of these free certificates. For more information about the "Let's Encrypt" terms, refer to https://letsencrypt.org/repository/.
   - Upload your wildcard certificate. To do this, click **Upload wildcard certificate**, and then provide a wildcard certificate and a private key.
6. Click **Submit** to apply the changes.

To reset the custom URL to default

1. In the management portal, click **Settings** > **Branding**.
2. In the **URL for Acronis Cyber Protect Cloud services** section, click **Reset to default** to use the default URL (https://cloud.acronis.com).

Updating agents automatically

Cyber Protect has three types of agent which can be installed on protected machines: Agent for Windows, Agent for Linux, and Agent for Mac.

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 management of multiple workloads, you can configure (and disable) automatic, unattended updates for all agents on all machines.

Important
Currently, only partners and customers with Protection enabled have access to agent update management functionality.

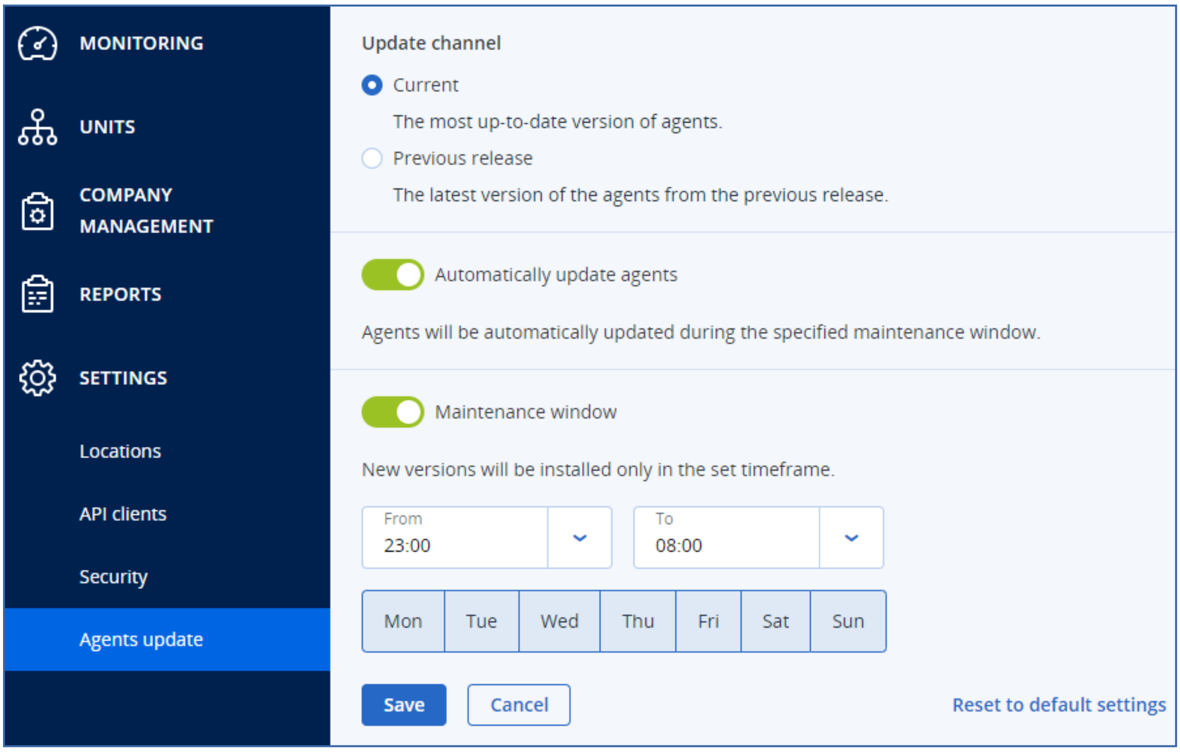
Note
To manage agents on individual machines, and customize auto-update settings, please refer to the Cyber Protect User Guide section on Updating Agents.

To update agents automatically

Note
Settings for automatically updating Agent for File Sync & Share are inherited by partners and customers who do not have Protection enabled.

To set an automatic, update of agents from the initial page of the Management Portal

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



Update channel

● Current

The most up-to-date version of agents.

○ Previous release

The latest version of the agents from the previous release.

Automatically update agents

Agents will be automatically updated during the specified maintenance window.

Maintenance window

New versions will be installed only in the set timeframe.

From 23:00

To 08:00

Mon | Tue | Wed | Thu | Fri | Sat | Sun

2. Select which version to detect for automatic updates: either **Current** or **Previous release**. (The default is **Current**.)
3. Switch **Automatically update agents** on. (The default is **on**.)
4. Set the maintenance timeframe. (The default is from 23:00 to 08:00.)

   Note
   Although agent update processes are designed to be fast and seamless, we recommend choosing a time frame which will cause minimum disruption for users, as users cannot prevent or postpone automatic updates.

5. [Optional] Select specific days for automatic updates to occur.
6. Select **Save.**

Note
Automatic updates are only available for:

- Cyber Protect agents version 15.0.26986 (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.

To monitor agent updates

Important
Agent updates can only be monitored by administrators of partners and customers who have the Protection module enabled.

To monitor agent updates, please refer to the Alerts and the Activities sections of the Cyber Protect User Guide.

Monitoring

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

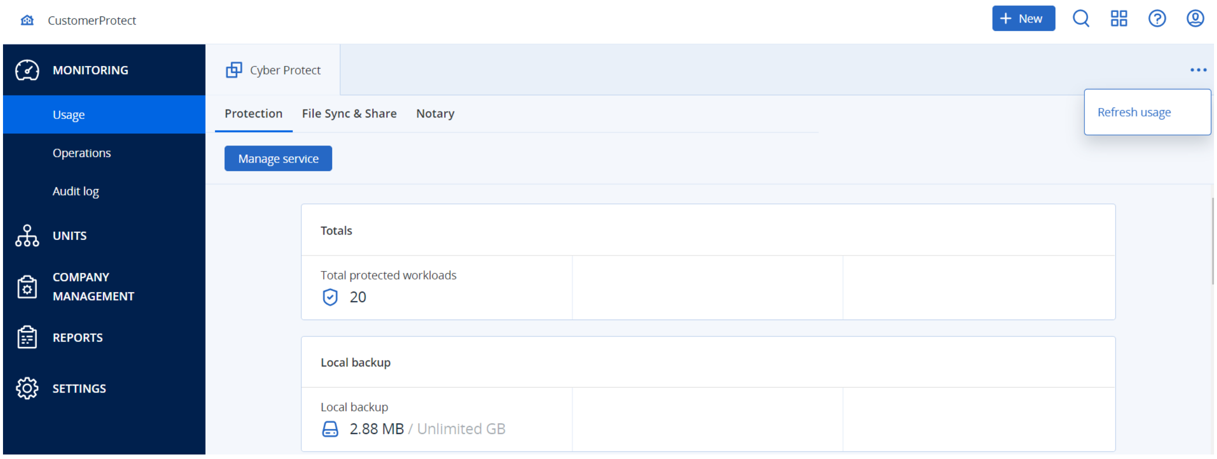
Usage

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.

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

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



Totals

Total protected workloads
20

Local backup

Local backup
2.88 MB / Unlimited GB

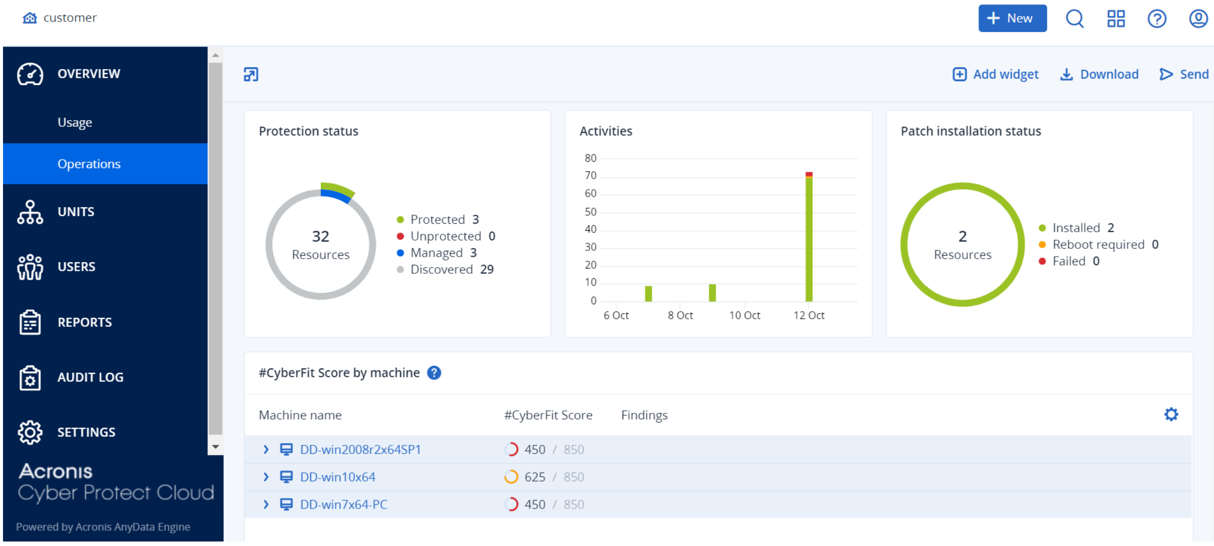
Operations

The **Operations** dashboard provides a number of customizable widgets that give an overview of operations related to the Cyber Protection service. Widgets for other services will be available in future releases.

By default, the data is displayed for the tenant in which you are operating. You can change the displayed tenant individually for each widget by editing it. Aggregated information about the direct child customer tenants of the selected tenant is also shown, including those that are located in folders. The dashboard does *not* display information about child partners and their child tenants; you must drill-down into the specific partner to see its dashboard. However, if you convert a child partner tenant to a folder tenant, the information about this tenant's child customers will appear on the parent tenant's dashboard.

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 in the .pdf or/and .xlsx format, or send it via email to any address, including external recipients.

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 for different tenants or with different filters.



Machine name	#CyberFit Score	Findings
DD-win2008r2x64SP1	450 / 850	
DD-win10x64	625 / 850	
DD-win7x64-PC	450 / 850	

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 period of time, select the tenant for which the data is displayed, and set filters.

To add a widget

Click **Add widget**, and then do one of the following:

- Click the widget that you want to add. The widget will be added with the default settings.
- To edit the widget before adding it, click the gear icon when the widget is selected. After editing the widget, click **Done**.

To remove a widget

Click the X sign next to the widget name.

Protection status

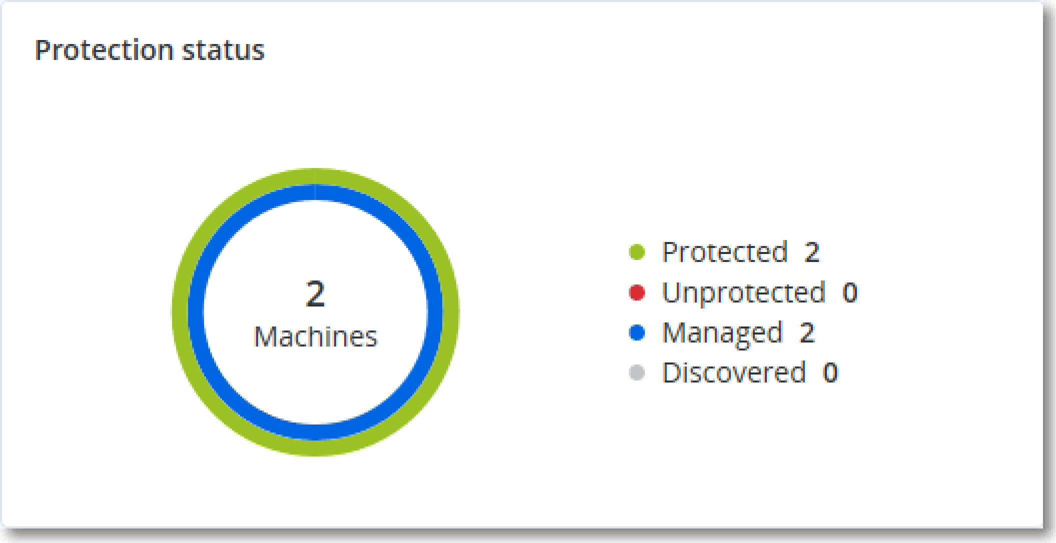
Protection status

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.

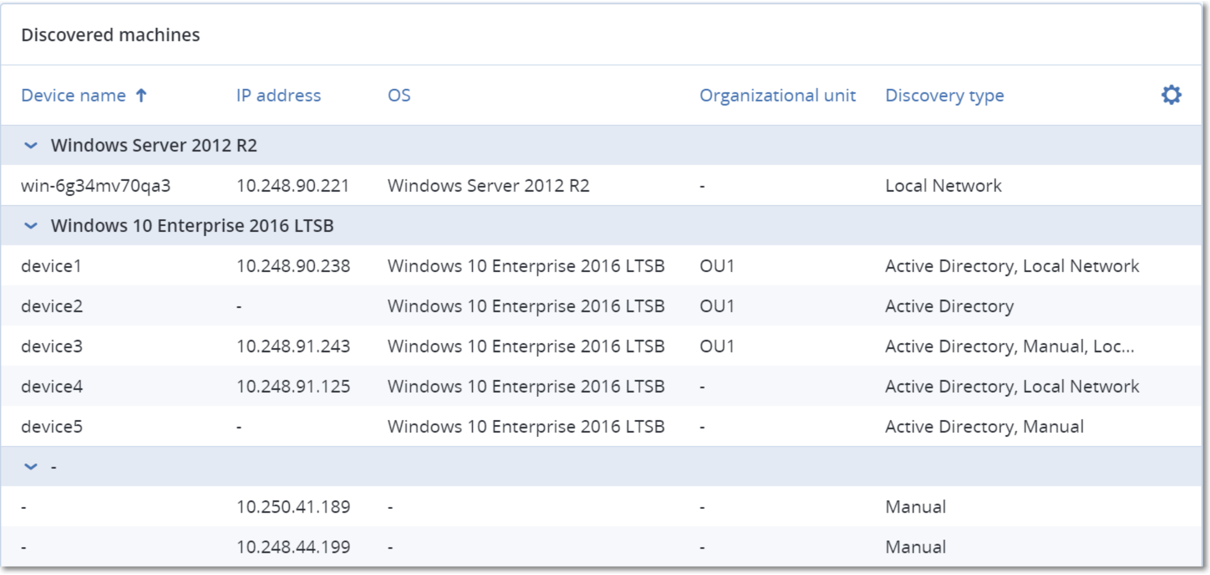
If you click on the machine status, you will be redirected to the list of machines with this status for more details.



Protection status

Discovered machines

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



Discovered machines

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

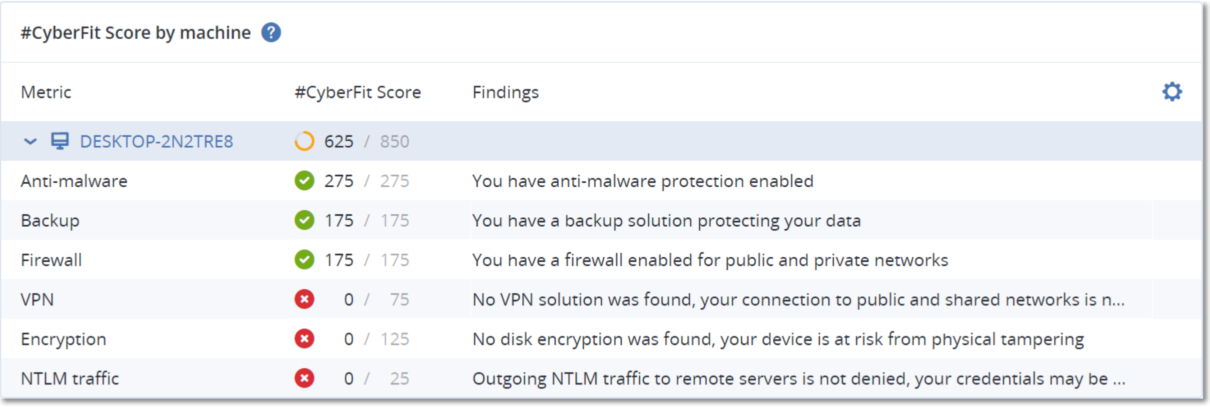
#CyberFit Score by machine

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

Important

This is an Early Access version of the EDR documentation. Some of the features and descriptions may be incomplete.

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

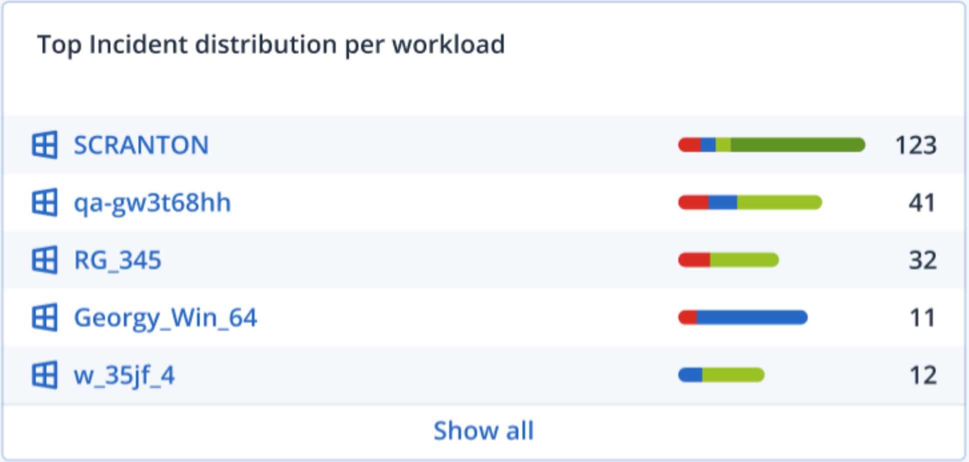
The widgets available are:

- 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

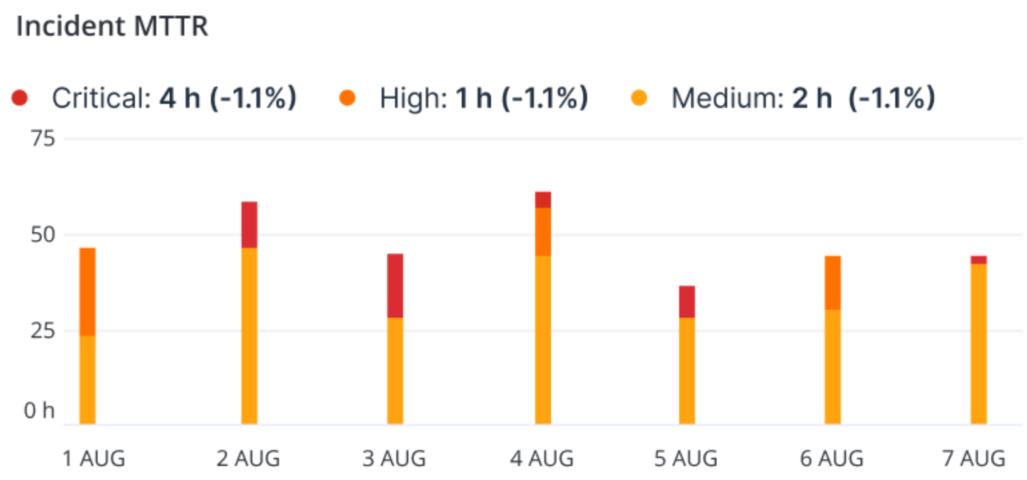
SCRANTON	123
qa-gw3t68hh	41
RG_345	32
Georgy_Win_64	11
w_35jf_4	12

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.

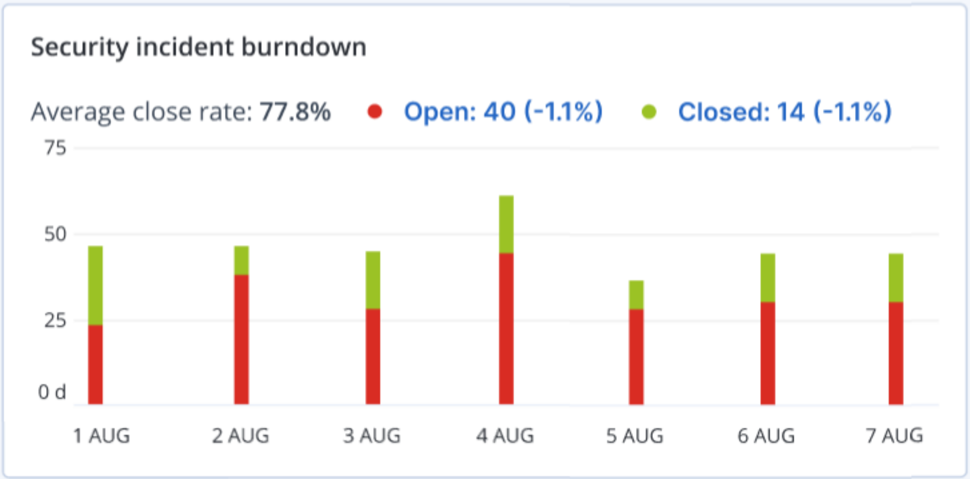


Security incident burndown

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).

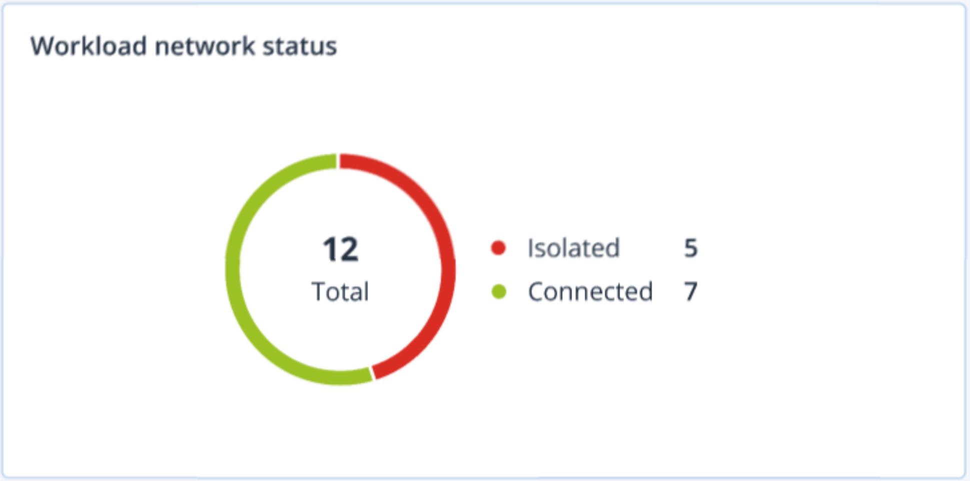
The % value shown in parentheses indicates the increase or decrease in comparison to the previous time period.



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.
- On NVMe drives, disk health monitoring is supported only for drives that communicate the SMART data via the Windows API. Disk health monitoring is not supported for NVMe drives that require reading the SMART data directly from the drive.

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

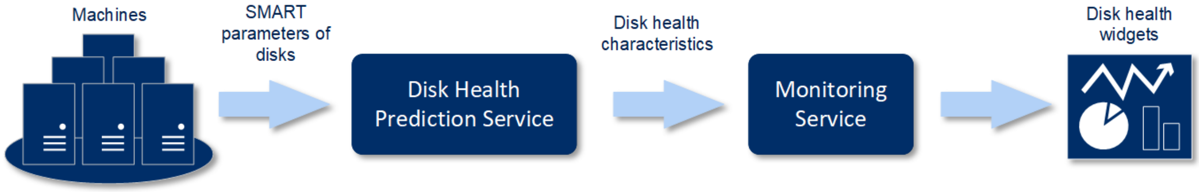
- **OK**
  Disk health is between 70% and 100%.
- **Warning**
  Disk health is between 30% and 70%.
- **Critical**
  Disk health is between 0% and 30%.
- **Calculating disk data**
  The current disk status and forecast are being calculated.

How it works

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

1. The protection agent collects the SMART parameters of the disks and passes this data to the Disk Health Prediction Service:
   - SMART 5 – Reallocated sectors count.
   - SMART 9 – Power-on hours.
   - SMART 187 – Reported uncorrectable errors.
   - SMART 188 – Command timeout.
   - SMART 197 – Current pending sector count.
   - SMART 198 – Offline uncorrectable sector count.
   - SMART 200 – Write error rate.
2. The Disk Health Prediction Service processes the received SMART parameters, makes forecasts, and then provides the following disk health characteristics:
   - Disk health current state: OK, warning, critical.
   - Disk health forecast: negative, stable, positive.
   - Disk health forecast probability in percentage.

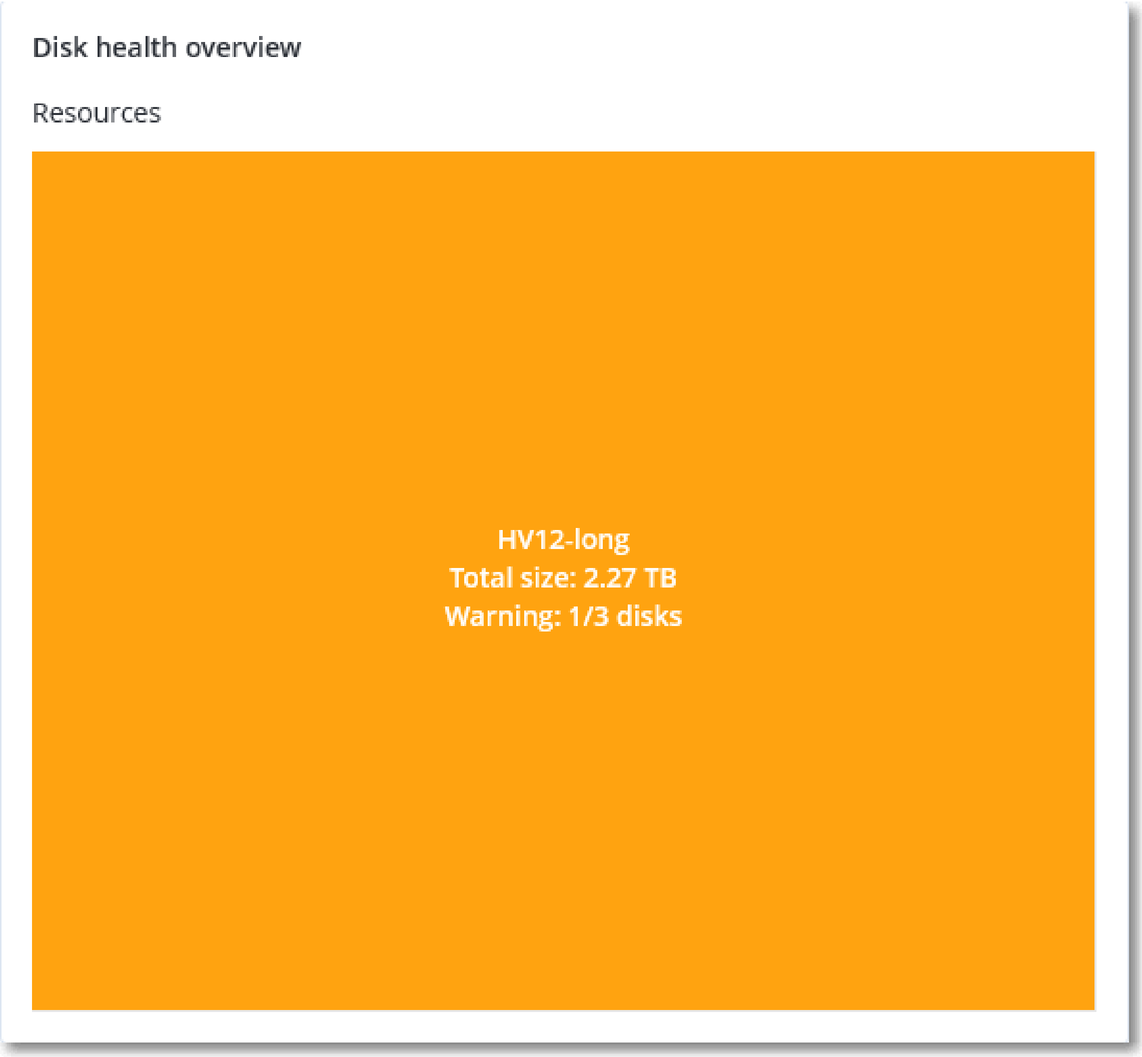
   The prediction period is one month.
3. The Monitoring Service receives these characteristics, and then shows the relevant information in the disk health widgets in the service console.


Machines
SMART parameters of disks
Disk Health Prediction Service
Disk health characteristics
Monitoring Service
Disk health widgets

Disk health widgets

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

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



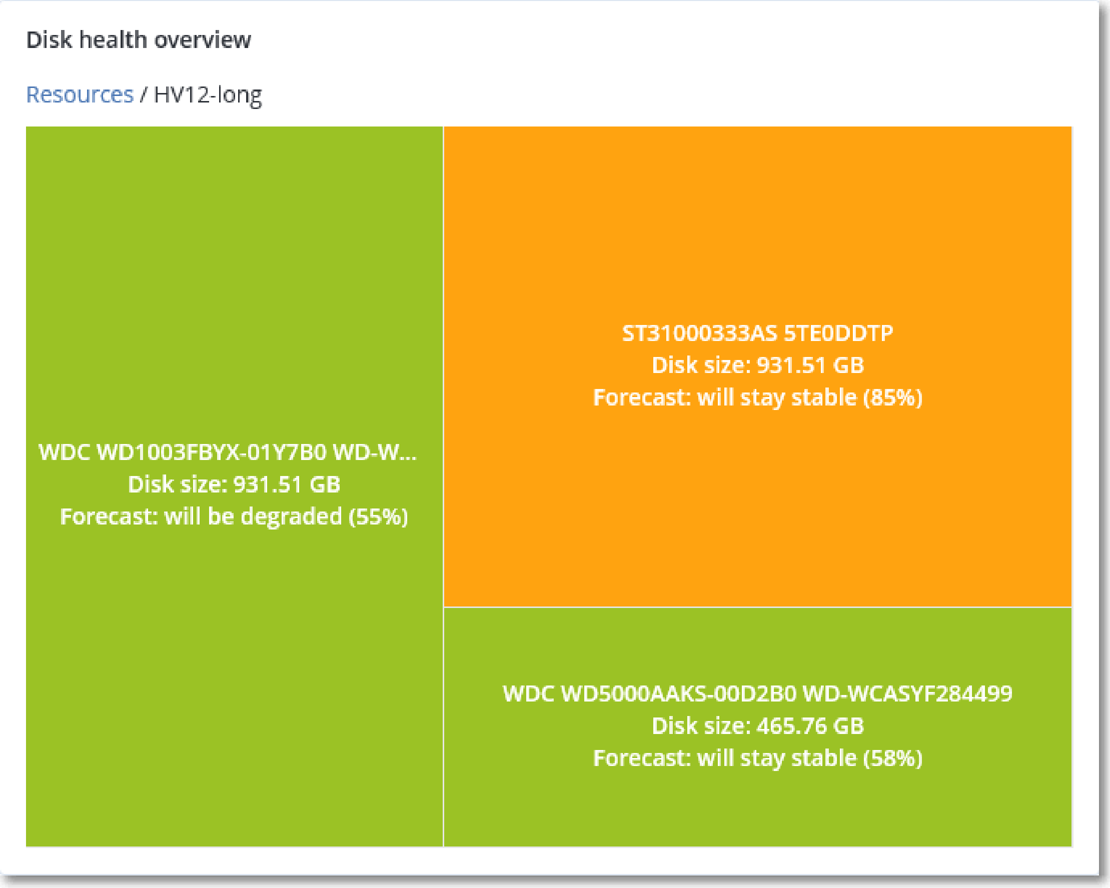
Disk health overview

Resources

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

- Disk level
  Shows the current disk health status of all disks for the selected machine. Each disk block shows one of the following disk health forecasts and its probability in percentage:
  - Will be degraded
  - Will stay stable

- Will be improved



Disk health overview

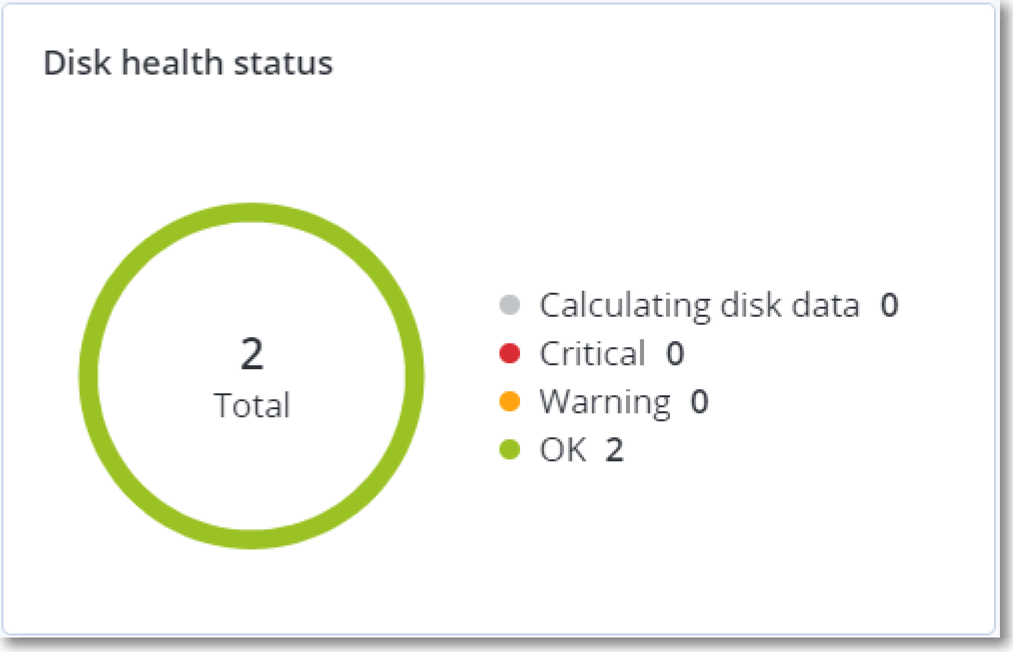
Resources / HV12-long

WDC WD1003FBYX-01Y7B0 WD-W...
Disk size: 931.51 GB
Forecast: will be degraded (55%)

ST31000333AS 5TE0DDTP
Disk size: 931.51 GB
Forecast: will stay stable (85%)

WDC WD5000AAKS-00D2B0 WD-WCASYF284499
Disk size: 465.76 GB
Forecast: will stay stable (58%)

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



Disk health 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. An image backup of this disk is not recommended at this point as the added stress can cause the disk to fail. Back up the most important files on this disk immediately and replace it.

Data protection map

The data protection map feature allows you to examine 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.

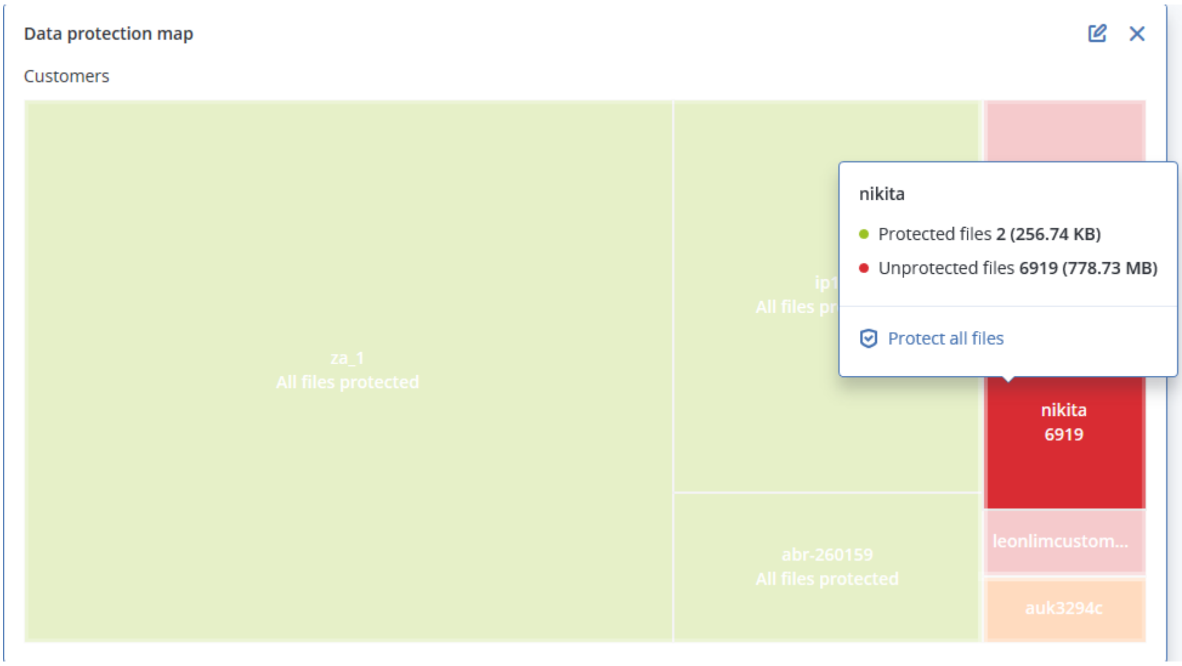
Each block size depends on the total number/size of all important files that belong to a customer/machine.

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 for the selected customer tenant/machine/location.
- **Low** – there are 21-50% of unprotected files with the extensions specified by you that are not being backed up for the selected customer tenant/machine/location.
- **Medium** – there are 1-20% of unprotected files with the extensions specified by you that are not being backed up for the selected customer tenant/machine/location.
- **High** – all files with the extensions specified by you are protected (backed up) for the selected customer tenant/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 has two levels of details that can be switched by drilling down:

- Customer tenant level – shows summarized information about the protection status of important files per customers that you have selected.


Data protection map

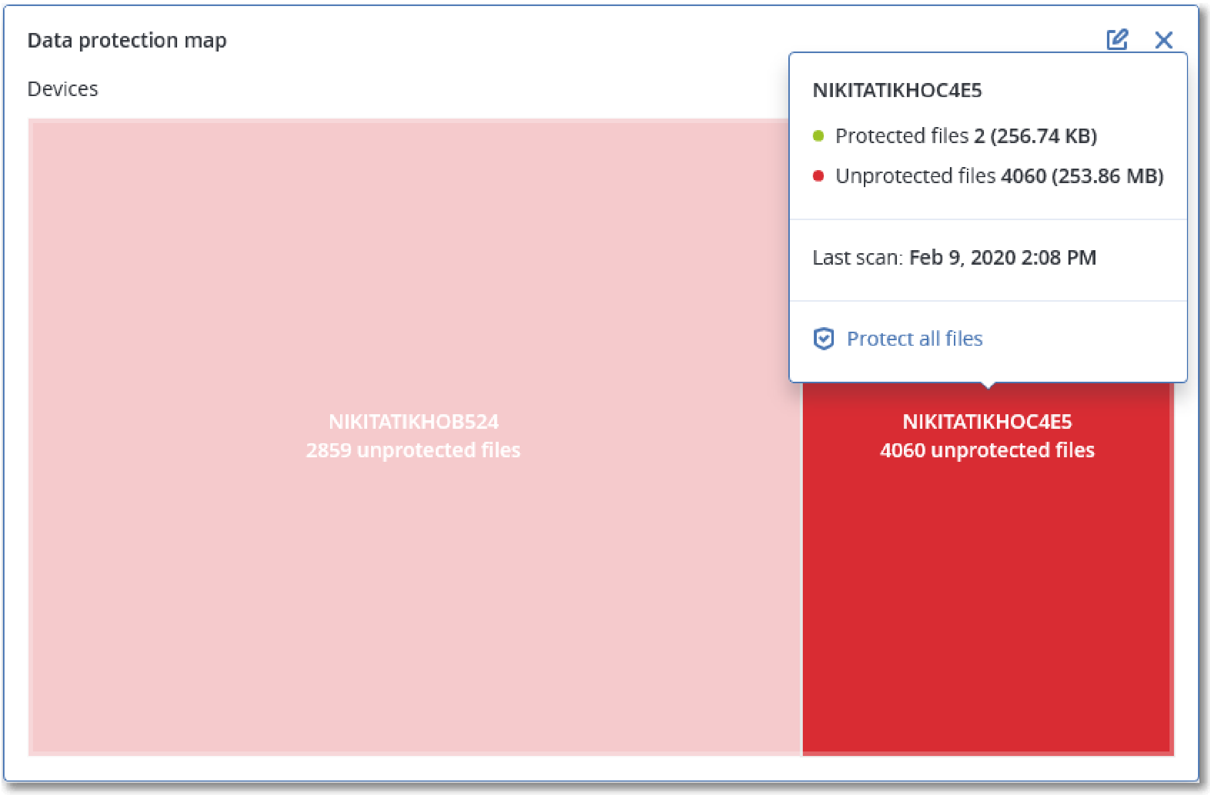
Customers

nikita

● Protected files **2 (256.74 KB)**

● Unprotected files **6919 (778.73 MB)**

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


Data protection map

Devices

NIKITATIKHOC4E5

● Protected files **2 (256.74 KB)**

● Unprotected files **4060 (253.86 MB)**

Last scan: **Feb 9, 2020 2:08 PM**

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.

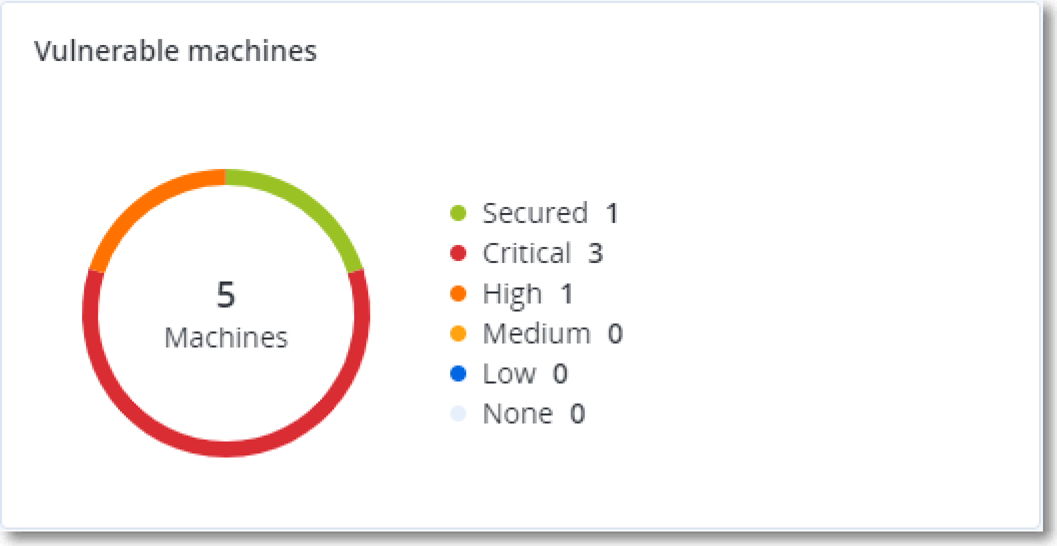
Vulnerability assessment widgets

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

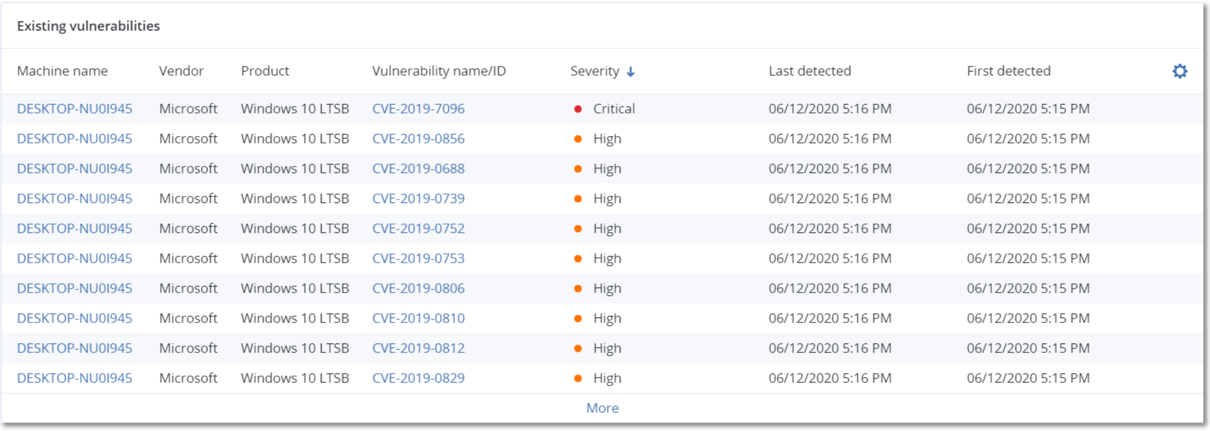


● Secured 1
● Critical 3
● High 1
● Medium 0
● Low 0
● None 0

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

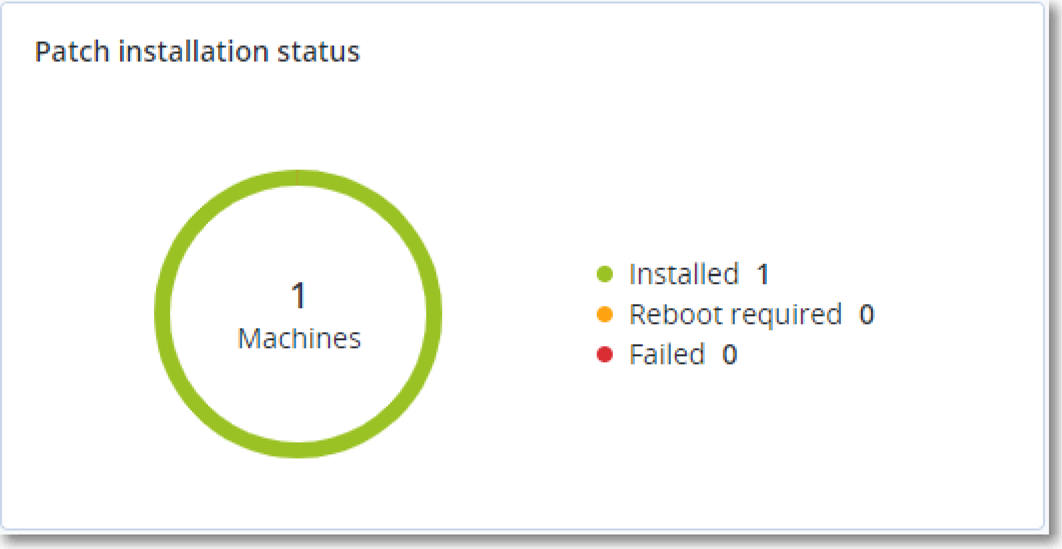
Patch installation widgets

There are four widgets related to the patch management functionality.

Patch installation status

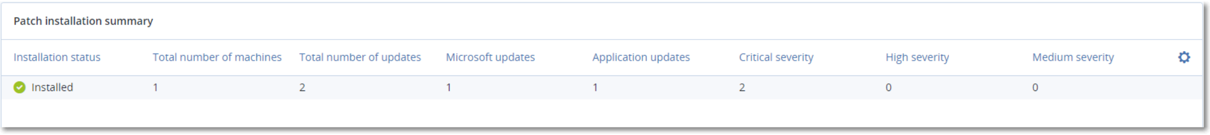
This widget shows the number of machines grouped by the patch installation status.

- **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.

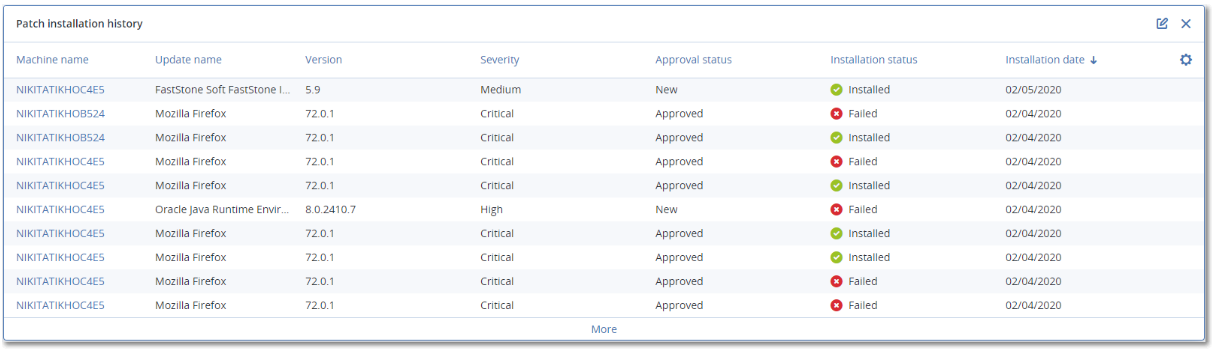


Patch installation summary

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.



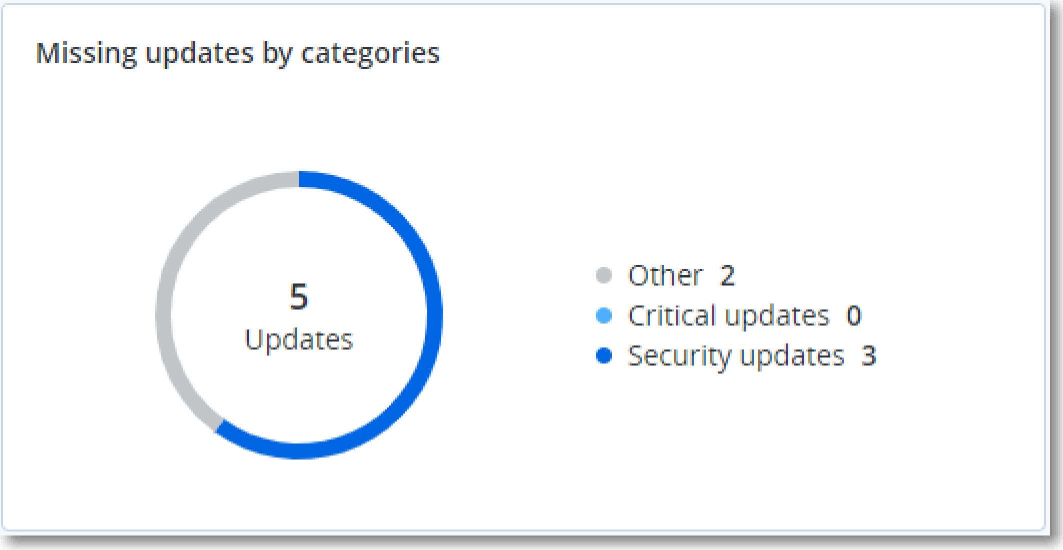
Patch installation history

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

Missing updates by categories

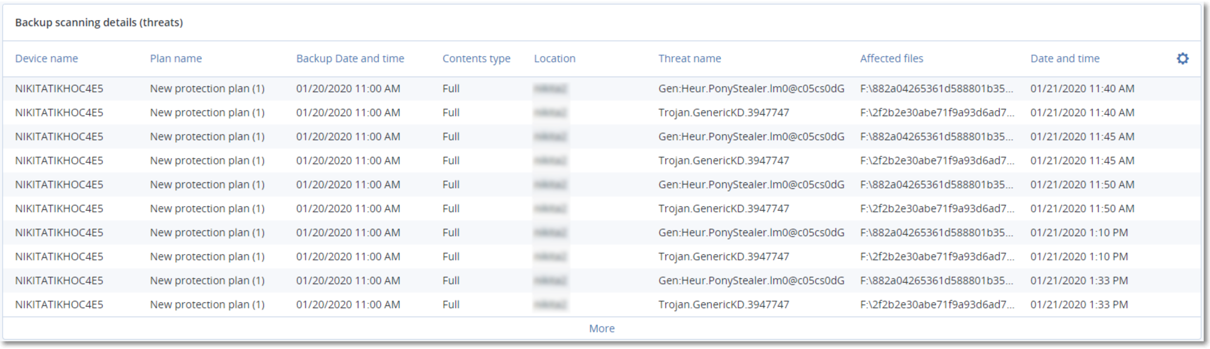
This widget shows the number of missing updates per category. The following categories are shown:

- Security updates
- Critical updates
- Other



Backup scanning details

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

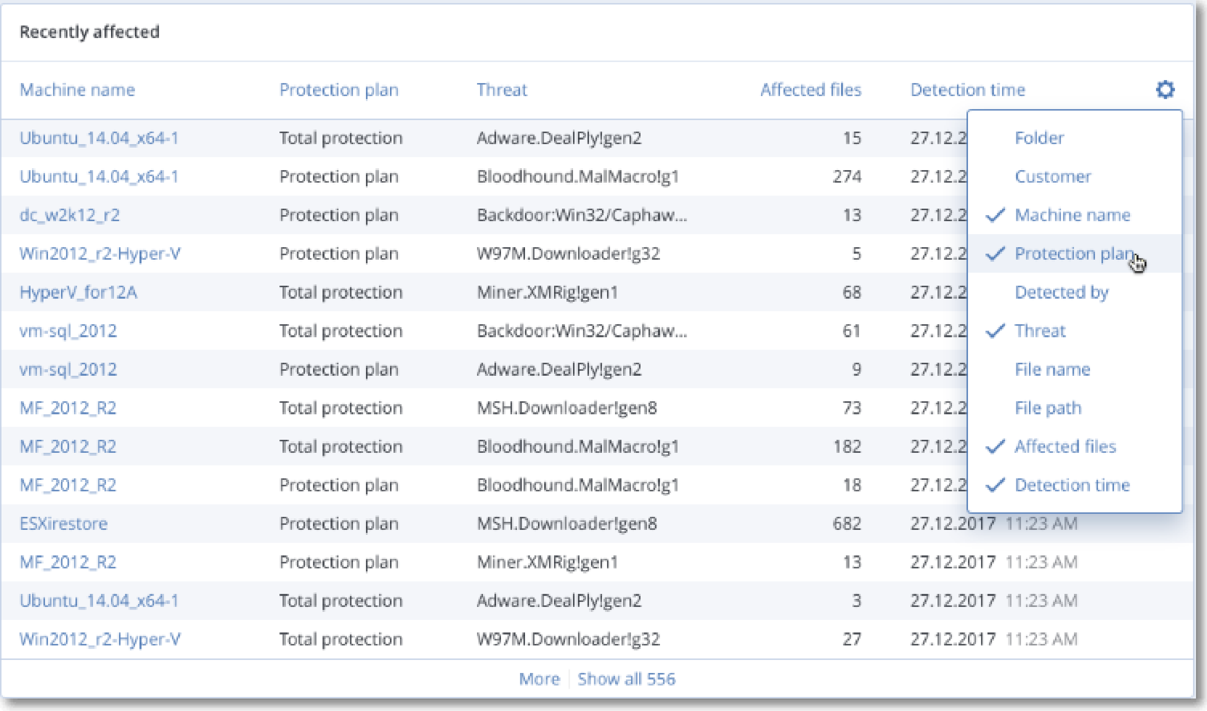


Backup scanning details (threats)

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	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:33 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:33 PM

Recently affected

This widget shows detailed information about workloads that were affected by threats, such as viruses, malware, and ramsomeware. 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.DealPly!gen2	15	27.12.2
Ubuntu_14.04_x64-1	Protection plan	Bloodhound.MalMacro!g1	274	27.12.2
dc_w2k12_r2	Protection plan	Backdoor:Win32/Caphaw...	13	27.12.2
Win2012_r2-Hyper-V	Protection plan	W97M.Downloader!g32	5	27.12.2
HyperV_for12A	Total protection	Miner.XMRig!gen1	68	27.12.2
vm-sql_2012	Total protection	Backdoor:Win32/Caphaw...	61	27.12.2
vm-sql_2012	Protection plan	Adware.DealPly!gen2	9	27.12.2
MF_2012_R2	Total protection	MSH.Downloader!gen8	73	27.12.2
MF_2012_R2	Total protection	Bloodhound.MalMacro!g1	182	27.12.2
MF_2012_R2	Protection plan	Bloodhound.MalMacro!g1	18	27.12.2
ESXirestore	Protection plan	MSH.Downloader!gen8	682	27.12.2017 11:23 AM
MF_2012_R2	Protection plan	Miner.XMRig!gen1	13	27.12.2017 11:23 AM
Ubuntu_14.04_x64-1	Total protection	Adware.DealPly!gen2	3	27.12.2017 11:23 AM
Win2012_r2-Hyper-V	Total protection	W97M.Downloader!g32	27	27.12.2017 11:23 AM

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

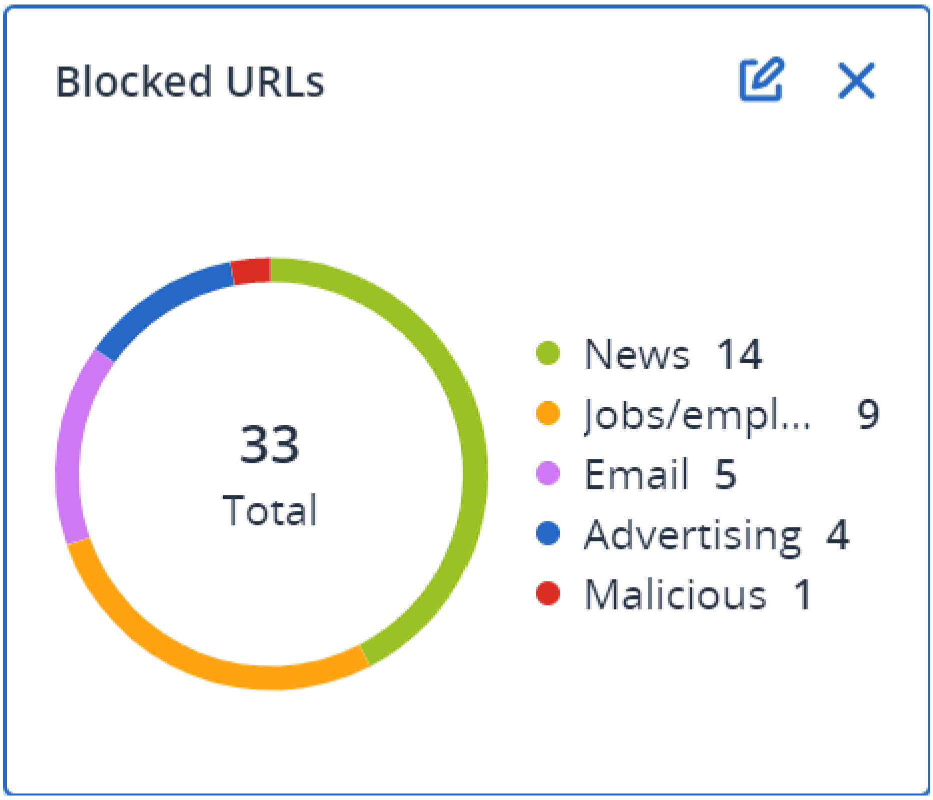
1. In the **Recently affected** widget, click **Download data**.
2. In the **Time period** field, enter the number of days for which you want to download data. The maximum number of days that you can enter is 200.
3. In the **Recipients** field, enter the email addresses of all the people who will receive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

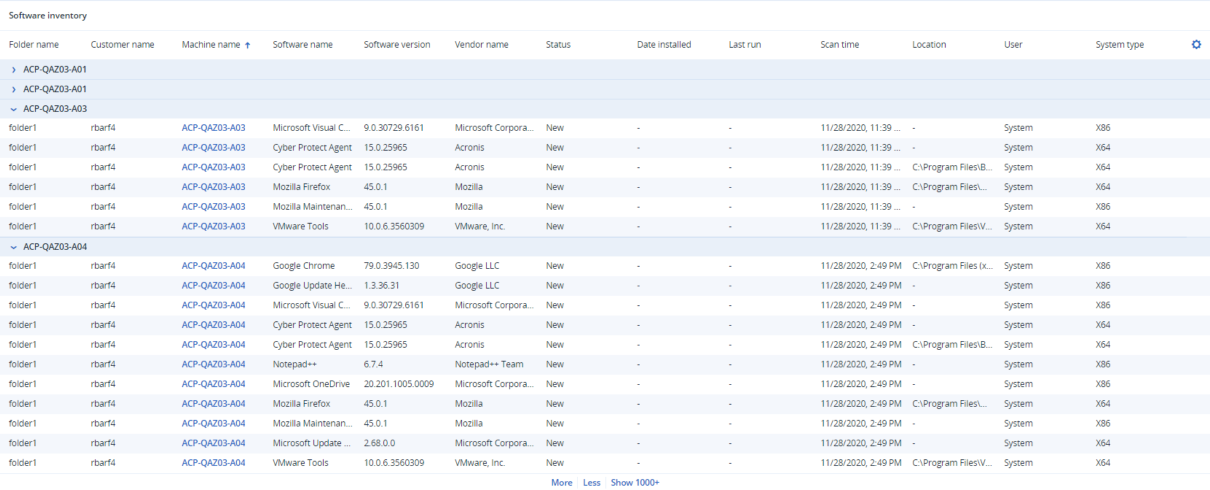
Blocked URLs

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

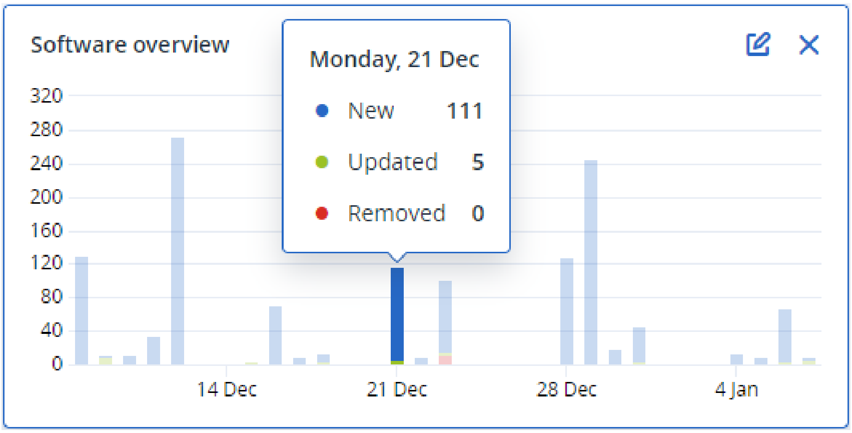
The **Software inventory** table widget shows detailed information about the all the software that is installed on Windows and macOS devices in your clients' organizations.



Software inventory

Folder name	Customer name	Machine name ↑	Software name	Software version	Vendor name	Status	Date installed	Last run	Scan time	Location	User	System type
› ACP-QAZ03-A01												
› ACP-QAZ03-A01												
⌄ ACP-QAZ03-A03												
folder1	rbarf4	ACP-QAZ03-A03	Microsoft Visual C...	9.0.30729.6161	Microsoft Corpora...	New	-	-	11/28/2020, 11:39 ...	-	System	X86
folder1	rbarf4	ACP-QAZ03-A03	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 11:39 ...	-	System	X64
folder1	rbarf4	ACP-QAZ03-A03	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 11:39 ...	C:\Program Files\B...	System	X64
folder1	rbarf4	ACP-QAZ03-A03	Mozilla Firefox	45.0.1	Mozilla	New	-	-	11/28/2020, 11:39 ...	C:\Program Files\...	System	X64
folder1	rbarf4	ACP-QAZ03-A03	Mozilla Maintenan...	45.0.1	Mozilla	New	-	-	11/28/2020, 11:39 ...	-	System	X86
folder1	rbarf4	ACP-QAZ03-A03	VMware Tools	10.0.6.3560309	VMware, Inc.	New	-	-	11/28/2020, 11:39 ...	C:\Program Files\V...	System	X64
⌄ ACP-QAZ03-A04												
folder1	rbarf4	ACP-QAZ03-A04	Google Chrome	79.0.3945.130	Google LLC	New	-	-	11/28/2020, 2:49 PM	C:\Program Files (x...	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Google Update He...	1.3.36.31	Google LLC	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Microsoft Visual C...	9.0.30729.6161	Microsoft Corpora...	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 2:49 PM	-	System	X64
folder1	rbarf4	ACP-QAZ03-A04	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 2:49 PM	C:\Program Files\B...	System	X64
folder1	rbarf4	ACP-QAZ03-A04	Notepad++	6.7.4	Notepad++ Team	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Microsoft OneDrive	20.201.1005.0009	Microsoft Corpora...	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Mozilla Firefox	45.0.1	Mozilla	New	-	-	11/28/2020, 2:49 PM	C:\Program Files\...	System	X64
folder1	rbarf4	ACP-QAZ03-A04	Mozilla Maintenan...	45.0.1	Mozilla	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Microsoft Update ...	2.68.0.0	Microsoft Corpora...	New	-	-	11/28/2020, 2:49 PM	-	System	X64
folder1	rbarf4	ACP-QAZ03-A04	VMware Tools	10.0.6.3560309	VMware, Inc.	New	-	-	11/28/2020, 2:49 PM	C:\Program Files\V...	System	X64

The **Software overview** widget shows the number of new, updated, and deleted applications on Windows and macOS devices in your clients' organizations 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.

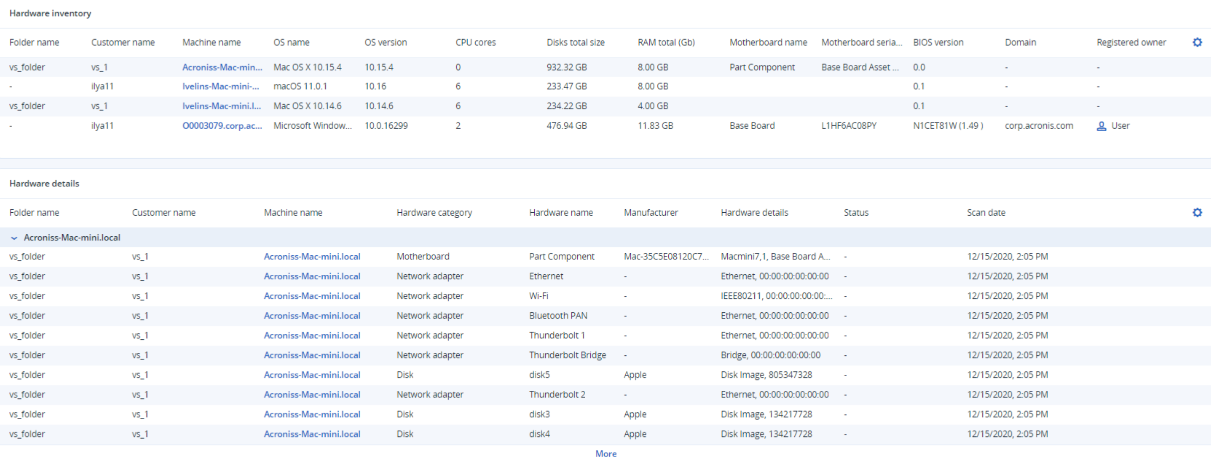
Updated - the number of updated applications.

Removed - the number of removed applications.

When you click the part of the bar that corresponds to a certain status, a pop-up window loads. It lists all the customers that have devices with applications in the selected status on the selected date. You can select a customer from the list, click **Go to customer**, and you will be redirected to the **Software Management** -> **Software Inventory** page in the customer's service console. The information in the page is filtered for the corresponding date and status.

Hardware inventory widgets

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



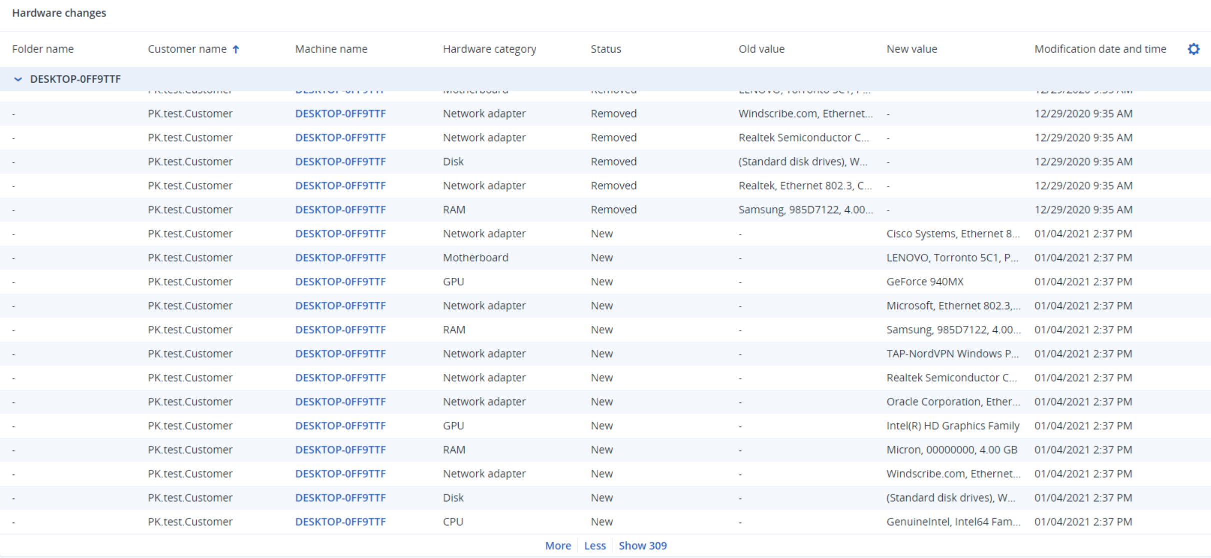
Hardware inventory

Folder name	Customer name	Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (Gb)	Motherboard name	Motherboard seria...	BIOS version	Domain	Registered owner
vs_folder	vs_1	Acroniss-Mac-min...	Mac OS X 10.15.4	10.15.4	0	932.32 GB	8.00 GB	Part Component	Base Board Asset ...	0.0	-	-
-	ilya11	Ivelins-Mac-mini-...	macOS 11.0.1	10.16	6	233.47 GB	8.00 GB			0.1	-	-
vs_folder	vs_1	Ivelins-Mac-mini.l...	Mac OS X 10.14.6	10.14.6	6	234.22 GB	4.00 GB			0.1	-	-
-	ilya11	O0003079.corp.ac...	Microsoft Window...	10.0.16299	2	476.94 GB	11.83 GB	Base Board	L1HF6AC08PY	N1CET81W (1.49)	corp.acronis.com	User

Hardware details

Folder name	Customer name	Machine name	Hardware category	Hardware name	Manufacturer	Hardware details	Status	Scan date
Acroniss-Mac-mini.local								
vs_folder	vs_1	Acroniss-Mac-mini.local	Motherboard	Part Component	Mac-35C5E08120C7...	Macmini7,1, Base Board A...	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Ethernet	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Wi-Fi	-	IEEE80211, 00:00:00:00:00:...	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Bluetooth PAN	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Thunderbolt 1	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Thunderbolt Bridge	-	Bridge, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Disk	disk5	Apple	Disk Image, 805347328	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Thunderbolt 2	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Disk	disk3	Apple	Disk Image, 134217728	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Disk	disk4	Apple	Disk Image, 134217728	-	12/15/2020, 2:05 PM

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

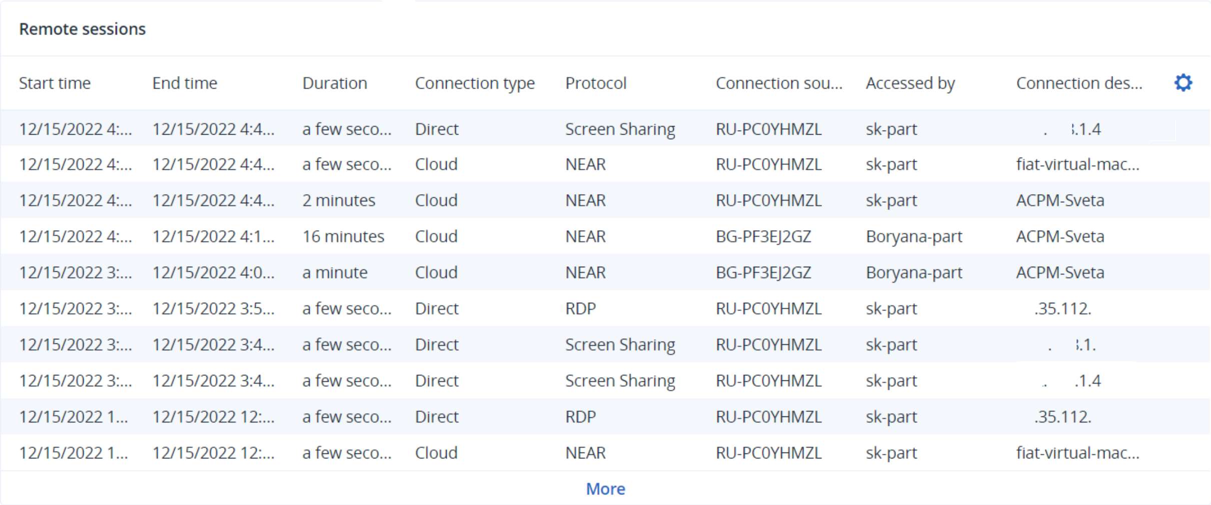


Hardware changes

Folder name	Customer name ↑	Machine name	Hardware category	Status	Old value	New value	Modification date and time
DESKTOP-0FF9TTF							
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	Removed	Windscribe.com, Ethernet...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	Removed	Realtek Semiconductor C...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Disk	Removed	(Standard disk drives), W...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	Removed	Realtek, Ethernet 802.3, C...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	RAM	Removed	Samsung, 985D7122, 4.00...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 8...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Torronto 5C1, P...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	GPU	New	-	GeForce 940MX	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Microsoft, Ethernet 802.3,...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows P...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor C...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ether...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Windscribe.com, Ethernet...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), W...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	CPU	New	-	GenuineIntel, Intel64 Fam...	01/04/2021 2:37 PM

Session history

The widget shows the detailed information about the remote desktop and file transfer sessions that were conducted in your clients' organizations 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	. 3.1.4
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	. 3.1.
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...

Reporting

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

Usage

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

Report type

You can select one of the following report types:

- **Current usage**

  The report contains the current service usage metrics.

  The usage metrics are calculated within each of the child tenants' billing periods. If the tenants included in the report have different billing periods, the parent tenant's usage may differ from the sum of the child tenants' usages.
- **Current usage distribution**

  This report is available only for partner tenants that are managed by an external provisioning system. This report is useful when the billing periods of child tenants do not match the billing period of the parent tenant. The report contains the service usage metrics for child tenants calculated within the current billing period of the parent tenant. The parent tenant's usage is guaranteed to be equal to the sum of the child tenants' usages.
- **Summary for period**

  The report contains the service usage metrics for the end of the specified period, and the difference between the metrics in the beginning and at the end of the specified period.
- **Day-by-day for period**

  The report contains the service usage metrics and their changes for each day of the specified period.

Report scope

You can select the scope of the report from the following values:

- **Direct customers and partners**

  The report will include the service usage metrics only for the immediate child tenants of the tenant in which you are operating.
- **All customers and partners**

  The report will include the service usage metrics for all child tenants of the tenant 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 tenant 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 top-most tenant 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

This type of report can be 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 tenant for which you want to create a report.

3. Click **Reports** > **Usage**.
4. Select the **Custom** tab.
5. In **Type**, select the report type as described above.
6. [Not available for the **Current usage** report type] In **Period**, select the reporting period:
   - **Current calendar month**
   - **Previous calendar month**
   - **Custom**
7. [Not available for the **Current usage** report type] If you want to specify a custom reporting period, select the start and the end dates. Otherwise, skip this step.
8. In **Level of detail**, select the report scope as described above.
9. [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**.

Operations reports

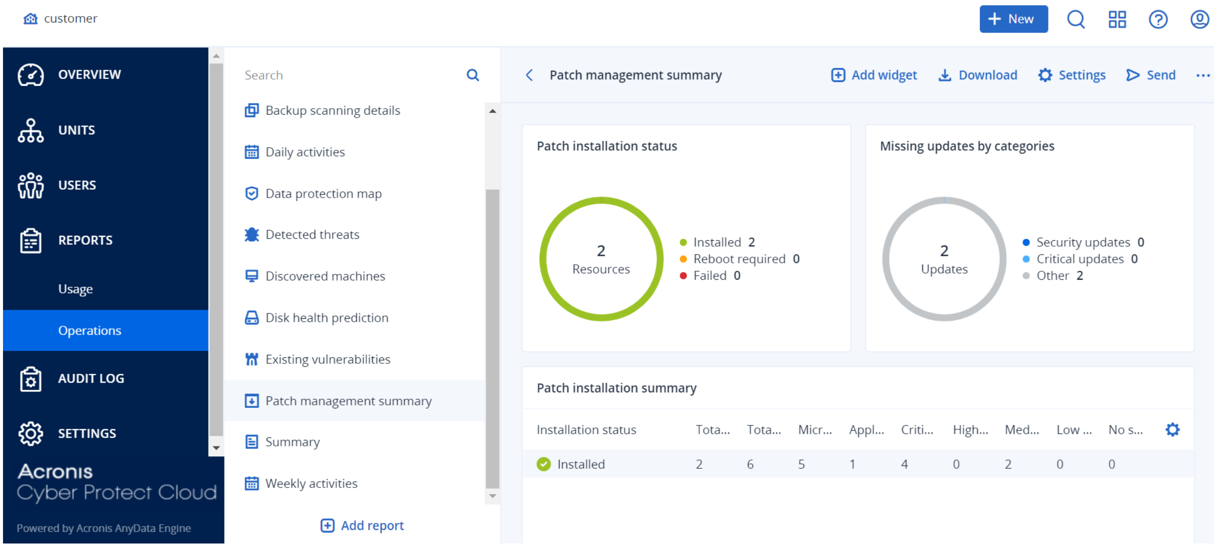
A report about operations can include any set of the **Operations** dashboard widgets. By default, all widgets show summary information for the tenant in which you are operating. You can change this individually for each widget by editing it, or for all widgets in the report settings.

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. 113).

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 about operations or send it via email in Excel (XLSX) or PDF format.



Patch installation summary

Installation status	Tota...	Tota...	Micr...	Appl...	Criti...	High...	Med...	Low ...	No s...
✓ Installed	2	6	5	1	4	0	2	0	0

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 machines	Shows all found machines in the organization network.
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 clients' organizations.
Hardware Inventory	Shows detailed information about the all the hardware that is available on physical and virtual Windows and macOS machines in your clients' organizations.
Remote sessions	Shows the detailed information about the remote desktop and file transfer sessions that were conducted in your clients' organizations during a specified time period.

To view a report, click its name.

To access operations with a report, click the vertical ellipsis icon on the report line. The same operations are available from within the report.

Adding a report

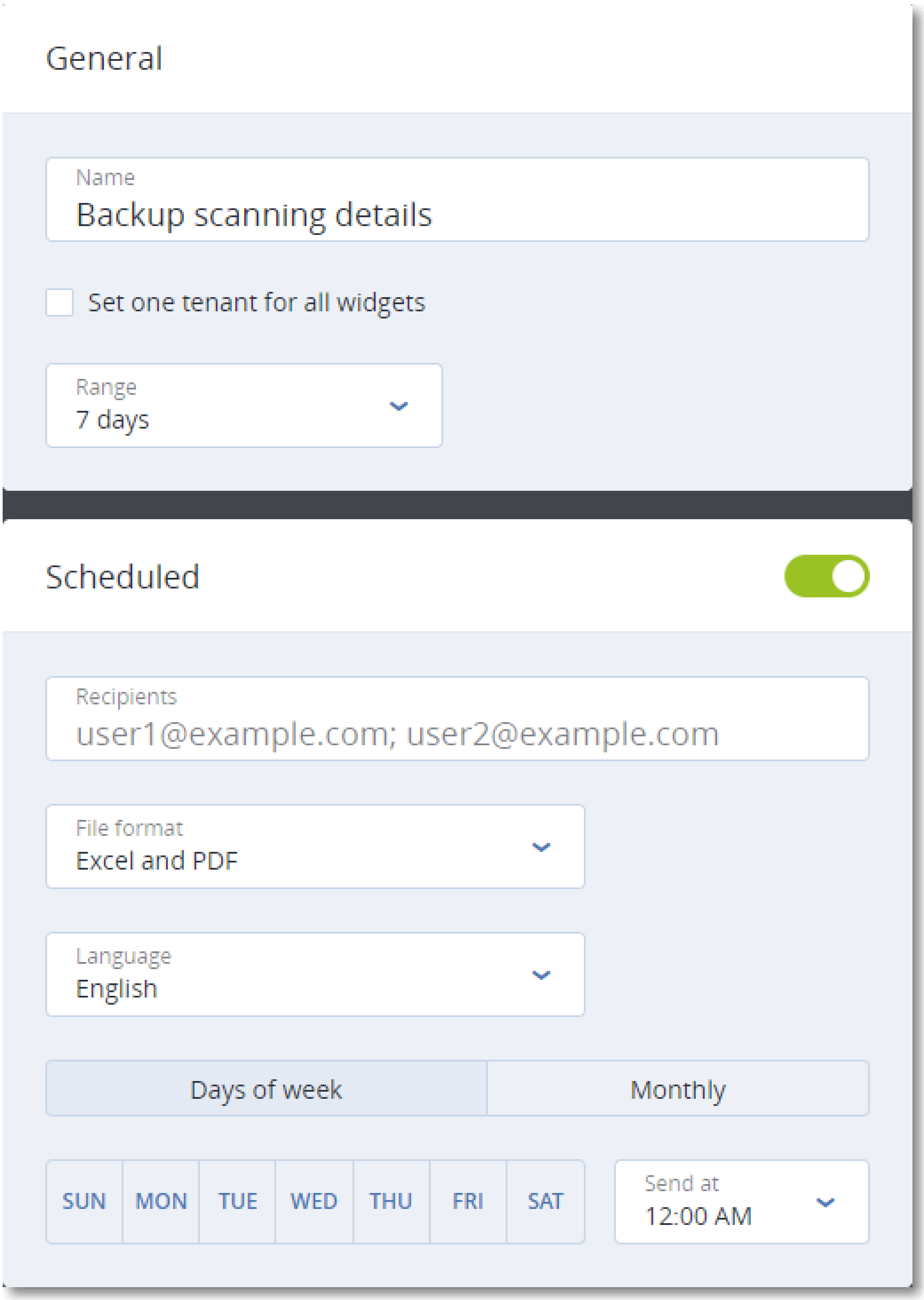
1. Click **Add report**.
2. Do one of the following:
   - To add a predefined report, click its name.
   - To add a custom report, click **Custom**, click the report name (the names assigned by default look like **Custom(1)**), and then add widgets to the report.
3. [Optional] Drag and drop the widgets to rearrange them.
4. [Optional] Edit the report as described below.

Editing the report settings

To edit a report, click its name, and then click **Settings**. When editing a report, you can:

- Rename the report
- Change the displayed tenant for all widgets included in the report

  If you have child tenants, then the **Set one tenant for all widgets** option is available for you. This option allows you to filter data in all widgets of the report by the selected tenant. If this option is not selected, then widgets will show data for all child tenants of your current tenant.
- Change the time range for all widgets included in the report
- Schedule sending the report via email in the PDF or/and Excel format.



General

Name
Backup scanning details

□ Set one tenant for all widgets

Range
7 days

Scheduled

Recipients
user1@example.com; user2@example.com

File format
Excel and PDF

Language
English

Days of week | Monthly

SUN MON TUE WED THU FRI SAT

Send at
12:00 AM

Scheduling a report

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

5. Select the days and the time when the report will be sent.
6. Click **Save** in the upper-right corner.

Exporting and importing the report structure

You can export and import the report structure (the set of widgets and the report settings) to a JSON file. This may be useful for copying the report structure from one tenant to another tenant.

To export the report structure, click the report name, click the vertical ellipsis icon in the upper-right corner, and then click **Export**.

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

Downloading a report

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

- Excel and PDF
- Excel
- PDF

Dumping the report data

You can send a dump of the report data in a CSV file via email. The dump includes all of the report data (without filtering) for a custom time range. The timestamps in CSV reports are in the UTC format whereas in Excel and PDF reports the timestamps are in the current system time zone.

The software generates the data dump on the fly. If you specify a long period of time, this action may take a long time.

To dump the report data

1. Click the report name.
2. Click the vertical ellipsis icon in the upper-right corner, and then click **Dump data**.
3. Specify the recipients' email addresses.
4. In **Time range**, specify the time range.
5. Click **Send**.

Executive summary

The Executive summary report provides an overview of the protection status of your customers' environments and their protected devices for a specified time range.

The Executive summary report includes sections with dynamic widgets which show key performance metrics related to the clients' use of the following cloud services: Backup, Antimalware protection, Vulnerability assessment, Patch management, Data Loss Prevention, Notary, Disaster Recovery, and Files Sync & Share.

There are several ways in which you can customize the report.

- 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 customers' organizations, so that they can easily see the technical and business value of the provided services.

Partner administrators can generate and send the Executive summary report to direct customers only. In case of a more complex tenant hierarchy that has sub partners, the sub partners will have to generate the report.

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	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): • Google Workspace Drive • Google Workspace Gmail • Google Workspace Shared Drive • Hosted Exchange mailboxes • Microsoft 365 mailboxes • Microsoft 365 OneDrive • Microsoft 365 SharePoint Online • Microsoft Teams • Websites For some workload types, the following workload groups are used: • Microsoft 365: Users, Groups, Public Folders, Teams, and Site Collections

Widget	Description
	• Google Workspace: Users, and Shared Drives • Hosted Exchange: Users If in one workload group there are more than 10 000 workloads, the widget does not display any data for the corresponding workloads. For example, if the customer has a Microsoft 365 account with 10 000 mailboxes and OneDrive service for 500 users, they all belong to the Users workload group. The sum of these workloads is 10 500, which exceeds the 10 000 limitation of a workload group. Therefore, the widget will hide the corresponding workload types: Microsoft 365 mailboxes, and Microsoft 365 OneDrive.
Cyber protection summary	The widget shows the key metrics of the Cyber protection performance for the specified time range. **Data backed up** - the total size of the archives that were created in the cloud and local storages. **Mitigated threats** - the total number of malware blocked across all devices. **Malicious URLs blocked** - the total number of URLs blocked on all devices. **Patched vulnerabilities** - the total number of vulnerabilities that were fixed through installation of software patches on all devices. **Installed patches** - the total number of installed patches on all devices. **Servers protected by DR** - the total number of servers protected by Disaster Recovery. **File Sync & Share users** - the total number of end and guest users who use Cyber Files. **Notarized files** - the total number of notarized files. **eSigned documents** - the total number of eSigned documents. **Blocked peripheral devices** - the total number of blocked peripheral devices.
Workload network status	This widget indicates how many workloads are isolated and how many are connected (the normal state of the workload). Select the relevant customer; 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 customer).
Workloads protection status	The widget shows the protected and unprotected workloads by type at the moment of the report's generation. Protected workloads are workloads on which at least one protection or backup plan is applied. Unprotected workloads are workloads on which no protection or backup plan is applied. The following workloads are counted: **Servers** - physical servers, and Domain Controller servers.

Widget	Description
	Workstations - physical workstations. **Virtual machines** - both agent-based and agentless virtual machines. **Web hosting servers** - virtual or physical server with installed cPanel or Plesk. **Mobile devices** - physical mobile devices. One workload can belong to more than one category. For example, a web hosting server is counted in two categories - **Servers**, and **Web hosting servers**.
Cloud workloads protection status	**Cloud workloads protection status** The widget shows the number of protected and unprotected cloud workloads by type at the moment of the report's generation. Protected cloud workloads are cloud workloads on which at least one backup plan is applied. Unprotected cloud workloads are cloud workloads on which no backup plan is applied. The following cloud workload types are shown in the chart (in alphabetical order from A to Z): • Google Workspace Drive • Google Workspace Gmail • Google Workspace Shared Drive • Hosted Exchange mailboxes • Microsoft 365 mailboxes • Microsoft 365 OneDrive • Microsoft 365 SharePoint Online • Microsoft Teams • Websites For some workload types, the following workload groups are used: • Microsoft 365: Users, Groups, Public Folders, Teams, and Site Collections • Google Workspace: Users, and Shared Drives • Hosted Exchange: Users If in one workload group there are more than 10 000 workloads, the widget does not display any data for the corresponding workloads. For example, if the customer has a Microsoft 365 account with 10 000 mailboxes and OneDrive service for 500 users, they all belong to the Users workload group. The sum of these workloads is 10 500, which exceeds the 10 000 limitation of a workload group. Therefore, the widget will hide the corresponding workload types: Microsoft 365 mailboxes, and Microsoft 365 OneDrive.

Antimalware protection widgets

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

Widget	Description
Antimalware scan of files	The widget shows the results of on-demand antimalware scanning of the devices for the specified date range. **Files** - the total number of scanned files **Clean** - the total number of clean files **Detected, quarantined** - the total number of infected files that were quarantined **Detected, not quarantined** - the total number of infected files that were not quarantined **Devices protected** - The total number of devices with applied antimalware protection policy **Total number of registered devices** - The total number of registered devices at the time of the report's generation
Antimalware scan of backups	The widget shows the results from the antimalware scanning of the backups for the specified date range, using the following metrics: • Total number of scanned recovery points • Number of clean recovery points • Number of clean recovery points with unsupported partitions • Number of infected recovery points. This metric includes the number of infected recovery points with unsupported partitions.
Blocked URLs	For the specified date range, the widget shows the number of blocked URLs grouped by website category. The widget lists the seven website categories that have the biggest number of blocked URLs, and combines the rest of the website categories into **Other**. For more information about the website categories, see the URL filtering topic in Cyber Protection.
Security incident burndown	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. 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	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

Widget	Description
	period.
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	For the specified date range, the widget shows the number of detected threats grouped by the following protection technologies: • Antimalware scanning • Behavior engine • Cryptomining protection • Exploit prevention • Ransomware active protection • 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	The widget shows the total number of registered workloads by backup status. **Backed up** - number of workloads that were backed up (at least one successful backup was performed) during the report date range. **Not backed up** - number of workloads which were not backed up (no successful backup was performed) during the report date range.
Disk health status by physical device	The widget shows the aggregated health status of physical devices based on the health statuses of their disks. **OK** - This disk health status relates to values [70-100]. The status of the device is **OK** when all its disks are in status **OK**. **Warning** - This disk health status relates to values [30-70]. The status of a device is **Warning** when the status of at least one of its disks is **Warning**, and when there are no disks in status **Error**. **Error** - This disk health status relates to values [0-30]. The status of the device is **Error** when the status of at least one of its disks is **Error**. **Calculating disk data** - The status of the device is **Calculating disk data** when the statuses of its disks are not calculated yet.
Backup	For the specified time range, the widget shows the total number and total

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

Disaster Recovery widgets

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

Widget	Description
Disaster Recovery statistics	The widget shows Disaster Recovery key performance metrics for the specified date range. **Production failovers** - the number of production failover operations for the specified time range. **Test failovers** - the total number of test failover operations that were

Widget	Description
	performed during the specified time range. **Primary servers** - the total number of primary servers at the moment of the report's generation. **Recovery servers** - the total number of recovery servers at the moment of the report's generation. **Public IPs** - the total number of public IP addresses (at the moment of the report's generation). **Total compute points consumed** - the total number of compute points consumed during the specified time range.
Disaster Recovery servers tested	The widget shows information about the servers that are protected by Disaster Recovery and tested with test failover. The widget shows the following metrics: **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. **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. **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. 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.
Servers protected with Disaster Recovery	The widget shows information about the servers protected with Disaster Recovery and the unprotected servers. The widget shows the following metrics: The total number of servers registered in customer tenant at the moment of the report's generation. **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. **Unprotected** - the total number of unprotected servers out of all registered servers at the moment of the report's generation.

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	The widget shows the following metrics: **Total cloud storage used** - The total storage usage of all users. **End users** - the total number of end users. **Average storage used per end user** - the average storage usage per end user. **Guest users** - the total number of guest users.
File Sync & Share storage usage by end users	The widget shows the total number of File Sync & Share end users who have a storage usage in the following ranges: • 0 - 1 GB • 1 - 5 GB • 5 - 10 GB • 10 - 50 GB

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

Configuring the settings of the Executive summary report

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

To update the settings of the executive summary report

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

Creating an Executive summary report

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

To create an Executive summary report

1. In the management console, go to **Reports**>**Executive summary**.
2. Click **Create executive summary report**.
3. In **Report name**, type the name of the report.
4. Select the Recipients of the report.
   - If you want to send the report to all direct customers, select **Send to all direct customers**.
   - If you want to send the report to specific customers
     a. Clear the **Send to all direct customers**.
     b. Click **Select contacts**.
     c. Select the specific customers. 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. 109).

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> Overview > Operations (widgets)	The time of report generation is in the time zone of the machine where the browser is running.
Management portal> Overview > Operations (exported to PDF or xslx)	• The time stamp of the exported report is in the time zone of the machine that was used to export the report. • The time zone of the activities displayed in the report is UTC.
Management portal> Reports > Usage > Scheduled reports	• The report is generated at 23:59:59 UTC on the first day of the month. • The report is sent on the second day of the month.
Management portal> Reports > Usage > Custom reports	The time zone and date of the report is UTC.
Management portal> Reports > Operations (widgets)	• The time of report generation is in the time zone of the machine where the browser is running. • The time zone of the activities displayed in the report is UTC.
Management portal> Reports > Operations	• The time stamp of the exported report is in the time zone of the machine that was used to export the report.

(exported to PDF or xslx)	• The time zone of the activities displayed in the report is UTC.
Management portal> Reports > Operations (scheduled delivery)	• The time zone of the report delivery is UTC. • The time zone of the activities displayed in the report is UTC.
Management portal> Users > Daily recap about active alerts	• This report is sent once a day between 10:00 and 23:59 UTC. The time when the report is sent depends on the workload in the datacenter. • The time zone of the activities displayed in the report is UTC.
Management portal> Users > Cyber Protection status notifications	• This report is sent when an activity is completed. **Note** Depending on the workload in the datacenter, some reports might be sent with delays. • The time zone of the activity in the report is UTC.

Reported data according to widget type

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

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

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

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

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 machines	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

Audit log

To view the audit log, click **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 Protection service console
- Cyber Scripting operations that are performed by users in the Cyber Protection service console
- System messages about reached quotas and quota usage

The log shows events in the tenant in which you are currently operating and its child tenants. 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 tenant that the object belongs to.
- **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 tenant 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.

Advanced Protection packs

Advanced protection packs can be enabled in addition to the Protection service and are subject to additional charge. Advanced protection packs provide unique functionality that does not overlap with the standard feature set and with other advanced packs. Clients can protect their workloads with one, several, or all advanced packs. The advanced protection packs are available for both billing modes of the Protection service - Per workload and Per gigabyte.

The Advanced File Sync & Share features can be enabled with the File Sync & Share service. It is available in both billing modes - Per user and Per gigabyte.

You can enable the following advanced protection packs:

- Advanced Backup
- Advanced Management
- Advanced Security
- Advanced Security + EDR
- Advanced Data Loss Prevention
- Advanced Disaster Recovery
- Advanced Email Security
- Advanced File Sync & Share

Note
Advanced packs can be used only when the feature that they extend is enabled. Users cannot use advanced features when the standard service feature is disabled. For example, users cannot use the features of the Advanced Backup pack if the Protection feature is disabled.

If an advanced protection pack is enabled, its features appear in the protection plan and are marked with the Advanced feature icon . When users try to enable the feature, they will be prompted that additional billing applies.

If an advanced protection pack is not enabled, but upsell is turned on, the advanced protection features appear in the protection plan, but are inaccessible for use. The following icon is displayed next to the feature name . A message will prompt users to contact their administrator to enable the required advanced feature set.

If an advanced protection pack is not enabled and upsell is turned off, customers will not see the advanced features in their protection plans.

Included features and advanced packs in Cyber Protect services

When you enable a service or feature set in Cyber Protect, you enable a number of features that are included and available by default. In addition, you can enable advanced protection packs.

The following sections contain high level overview of Cyber Protect service features and advanced packs. For a complete list of offerings, see the Cyber Protect Licensing Guide.

Included and advanced features in the Protection service

Included and advanced features in the Protection service

Feature group	Included standard features	Advanced features
Security	• #CyberFit score • Vulnerability assessment • Anti-ransomware protection: Active protection • Antivirus and Antimalware protection: Cloud signature-based file detection (no real-time protection, only scheduled scanning)* • Antivirus and Antimalware protection: Pre-execution AI-based file analyzer, behavior-based Cyber Engine • Microsoft Defender management *To detect zero day attacks, Cyber Protect uses heuristic scanning rules and algorithms to look for malicious commands.	There are two available advanced protection packs: **Advanced Security** and **Advanced Security + EDR**. The Advanced Security pack includes: • Antivirus and antimalware protection with local signature-based detection (with real-time protection) • Exploit prevention • URL filtering • Endpoint firewall management • Forensic backup, scan backups for malware, safe recovery, corporate allowlist • Smart protection plans (integration with CPOC alerts) • Centralized backup scanning for malware • Remote wipe The Advanced Security + EDR protection pack includes all of the above features, and the following Endpoint Detection and Response capabilities for identifying advanced threats or in-progress attacks: • Manage incidents in a centralized Incident page • Visualize the scope and impact of incidents • Recommendations and remediation steps • Check for publicly disclosed attacks on your workloads using Threat feeds • Store security events for 180 days For information on enabling Advanced Security + EDR, see "Enabling Advanced Security + EDR" (p. 123).

Feature group	Included standard features	Advanced features
Data Loss Prevention	• Device control	• Content-aware prevention of data loss from workloads via peripheral devices and network communication • Pre-built automatic detection of personally identifiable information (PII), protected health information (PHI), and Payment Card Industry Data Security Standard (PCI DSS) data, as well as documents in the “Marked as Confidential” category • Automatic data loss prevention policy creation with optional end user assistance • Adaptive data loss prevention enforcement with automatic learning-based policy adjustment • Cloud-based centralized audit logging, alerting, and end user notifications
Management	• Group management of workloads • Centralized management of protection plans • Hardware inventory • Remote control • Remote actions • Concurrent connections per technician • Remote connection protocol: RDP	• Patch management • Disk health • Software inventory • File safe patching • Cyber Scripting • Remote assistance • File transfer and sharing • Selecting a session to connect • Observing workloads in multi-view • Connection modes: control, observe, and curtain • Connection via the Quick Assist application • Remote connection protocols: NEAR and Screen Sharing • Session recording for NEAR connections • Screenshot transmission • Session history report
Email security	None	Real-time protection for your Microsoft 365 and Gmail mailboxes: • Antimalware Antispam • URL scan in emails

Feature group	Included standard features	Advanced features
		- DMARC analysis - Anti-phishing - Impersonation protection - Attachments scan - Content disarm and reconstruction - Graph of trust See the configuration guide.
Cyber Disaster Recovery Cloud	You can use the Disaster Recovery standard features to test Disaster Recovery scenarios for your workloads. Note the Disaster Recovery standard features that are available, and their limitations: - Test failover in an isolated network environment. Limited to 32 compute points per month, and up to 5 test failover operations at the same time. - Recovery server configurations: 1 CPU and 2 GB RAM, 1 CPU and 4 GB RAM, and 2 CPU and 8 GB RAM. - Number of recovery points available for failover: only the last recovery point that is available right after a backup. - Available connectivity modes: Cloud-only and Point-to-site. - Availability of the VPN gateway: The VPN gateway will be temporarily suspended if it is inactive for 4 hours after the last test failover completed, and will be deployed again when you start a test failover. - Number of cloud networks: 1. - Internet access - Operations with runbooks: create and edit.	You can enable the Advanced Disaster Recovery pack, and protect your workloads using the complete Disaster Recovery functionality. Note the Disaster Recovery advanced features that are available: - Production failover - Test failover in an isolated network environment. - Number of recovery points available for failover: all recovery points that are available after the creation of the recovery server. - Primary servers - Recovery/Primary server configurations: No limitations - Available connectivity modes: Cloud-only, Point-to-site, Site-to-site Open VPN, and Multi-site IPsec VPN. - Availability of the VPN gateway: always available. - Number of cloud networks: 23. - Public IP addresses - Internet access - Operations with runbooks: create, edit, and execute.

Pay as you go and advanced features in the Protection service

Pay-as-you-go and advanced features in the Protection service

Feature group	Pay-as-you-go features	Advanced features
Backup	• File backup • Image backup • Applications backup • Network shares backup • Backup to cloud storage • Backup to local storage **Note** Fees for cloud storage usage are applicable.	• Microsoft SQL server and Microsoft Exchange clusters • Oracle DB • SAP HANA • Data Protection Map • Continuous Data Protection • Off-host data processing plans • Notarization of backups • Microsoft 365 seats • Google Workspace seats
File Sync & Share	• Store encrypted file-based content • Synchronize files across designated devices • Share folders and files with designated people and systems	• Notarization and e-signature • Document templates* *Backup of sync and share files
Physical Data Shipping	Physical Data Shipping functionality	N/A
Notary	• File notarization • File eSigning • Document templates	N/A

Note

You cannot enable advanced protection packs without enabling the standard protection feature that they extend. If you disable a feature, its advanced packs are disabled automatically and the protection plans that use them will be automatically revoked. For example, if you disable the Protection feature, its advanced packs will be disabled automatically and all plans that use them will be revoked.

Users cannot use advanced protection packs without standard protection, but can use only included features of standard protection together with advanced packs on specific workloads. In this case, they will be charged only for the advanced packs that they use.

For information about billing, see "Billing modes for Cyber Protect" (p. 7).

Advanced Data Loss Prevention

The Advanced Data Loss Prevention module prevents the leakage of sensitive information from workstations, servers, and virtual machines by inspecting the content of data transferred through local and network channels and applying the organization-specific data flow policy rules.

Before you start using the Advanced Data Loss Prevention module, verify that you read and understand the basic concepts and logic of Advanced Data Loss Prevention management that are described in the Fundamentals guide.

You might also want to review the Technical Specifications document.

Enabling Advanced Data Loss Prevention

By default, Advanced Data Loss Prevention is enabled in the configuration for new tenants. If the functionality was disabled during the tenant creation process, Partner administrators can enable it later.

To enable Advanced Data Loss Prevention

1. In the Cyber Protect Cloud management console, navigate to **Clients**.
2. Select the tenant for editing.
3. In the **Select services** section, scroll to **Protection**, and under the billing mode that you apply, select **Advanced Data Loss Prevention**.
4. Under Configure services, scroll to the **Advanced Data Loss Prevention** and configure quotas. By default, the quota is set to unlimited.
5. Save your settings.

Advanced Security + EDR

Endpoint detection and response (EDR) detects suspicious activity on workloads, including attacks that have gone unnoticed, and generates incidents. These incidents provide a step-by-step overview of each attack, helping you understand how an attack happened and how to prevent it from happening again. With easy-to-understand interpretations of each stage in the attack, the time spent on investigating attacks can be reduced to a matter of minutes.

Enabling Advanced Security + EDR

As the partner administrator, you can enable the Advanced Security + EDR protection pack to provide Endpoint detection and response (EDR) functionality in client protection plans.

To enable the Advanced Security + EDR pack

1. Log in to the management portal.

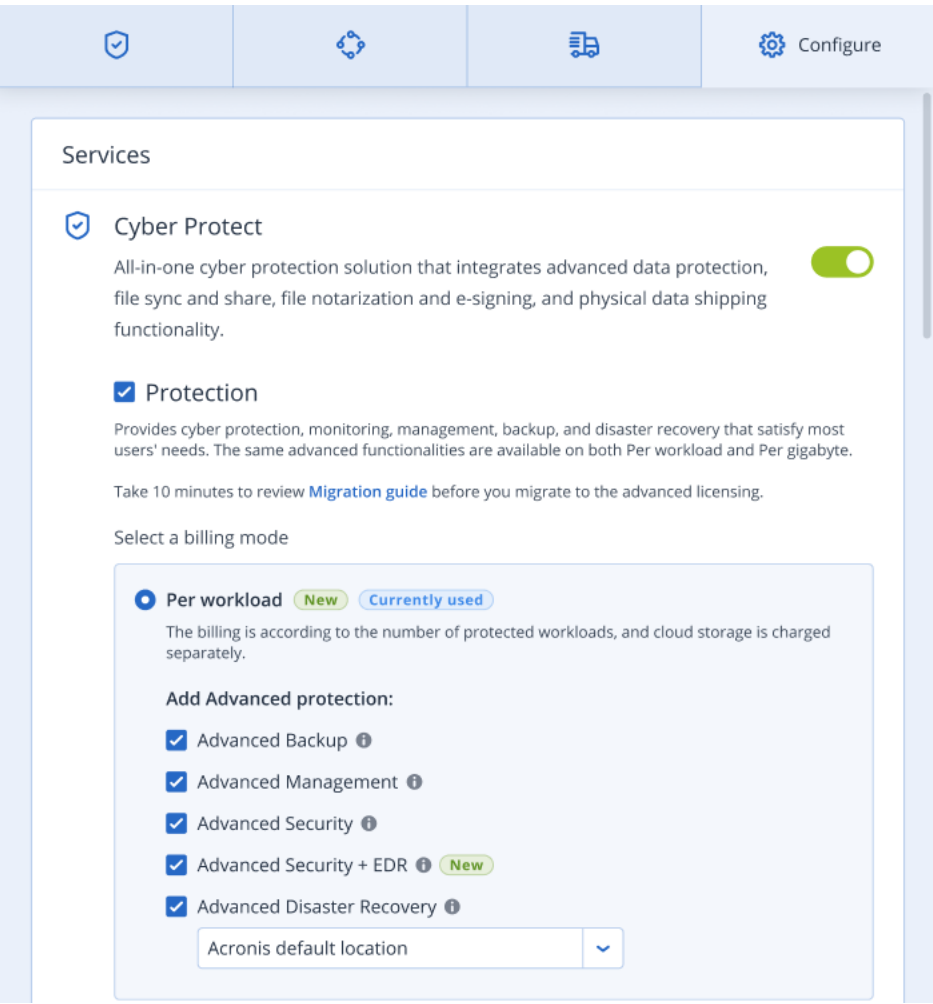
   Note
   If prompted, select the clients you want to apply the Advanced Security + EDR protection pack to, and click **Enable**.

2. In the left navigation pane, click **CLIENTS**.
3. Under Cyber Protect, click the **Protection** tab.

The list of existing clients subscribed to the Protection service is displayed.

4. Click the relevant client you want to add the Advanced Security + EDR pack to.

   In the **Configure** tab, under the Protection section, ensure the **Advanced Security + EDR** checkbox is selected.



Services

Cyber Protect

All-in-one cyber protection solution that integrates advanced data protection, file sync and share, file notarization and e-signing, and physical data shipping functionality.

☑ Protection

Provides cyber protection, monitoring, management, backup, and disaster recovery that satisfy most users' needs. The same advanced functionalities are available on both Per workload and Per gigabyte.

Take 10 minutes to review Migration guide before you migrate to the advanced licensing.

Select a billing mode

● Per workload New Currently used

The billing is according to the number of protected workloads, and cloud storage is charged separately.

Add Advanced protection:

☑ Advanced Backup

☑ Advanced Management

☑ Advanced Security

☑ Advanced Security + EDR New

☑ Advanced Disaster Recovery

Acronis default location

Advanced Disaster Recovery

You can enable the Advanced Disaster Recovery pack, and protect your workloads using the complete Disaster Recovery functionality.

The following advanced Disaster Recovery features are available:

- Production failover
- Test failover in an isolated network environment.
- Number of recovery points available for failover: all recovery points that are available after the creation of the recovery server.
- Primary servers
- Recovery/Primary server configurations: No limitations

- Available connectivity modes: Cloud-only, Point-to-site, Site-to-site Open VPN, and Multi-site IPsec VPN.
- Availability of the VPN gateway: always available.
- Number of cloud networks: 23.
- Public IP addresses
- Internet access
- Operations with runbooks: create, edit, and execute.

Advanced Email Security

The Advanced Email Security pack provides real-time protection for your Microsoft 365, Google Workspace, or Open-Xchange mailboxes:

- Antimalware and anti-spam
- URL scan in emails
- DMARC analysis
- Anti-phishing
- Impersonation protection
- Attachments scan
- Content disarm and reconstruction
- Graph of trust

Learn more about Advanced Email Security in the Advanced Email Security data sheet.

For configuration instructions, see Advanced Email Security with Perception Point.

Integrations

Integration with third-party systems

A service provider can integrate Cyber Protect Cloud with a third-party system as follows:

- By setting up a platform extension in this system.

  The **Integration** page of the management portal lists extensions available for the most popular Professional Services Automations (PSA) and Remote Monitoring and Management (RMM) systems.

  This is the recommended way of integrating the platform.
- By creating an API client for the system and thus enabling the system to access the application programming interfaces (APIs) of the platform and its services. API clients are part of the OAuth 2.0 authorization framework of the platform. For more information about OAuth 2.0, see https://tools.ietf.org/html/rfc6749.

  This is a low-level way of integrating the platform that requires programming skills. We recommend choosing it when there is no platform extension for the system or the system is to be customized for such cases of managing the platform and its services that are not covered by the available extension.

Setting up an integration for Cyber Protect Cloud

1. Log in to the management portal.
2. Go to **Integrations** in the main navigation menu.
3. Click the name of the third-party system with which you want to enable the integration.
4. Follow the on-screen instructions.

Find more information about available integrations with third-party systems, including step-by-step documentation at https://solutions.acronis.com.

Managing API clients

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

What is an API client?

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

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

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

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

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

Typical integration procedure

1. An administrator creates an API client in a tenant that a third-party system will manage.
2. The administrator enables the OAuth 2.0 client credentials flow in the third-party system.

   According to this flow, before accessing the tenant and its services via the API, the system should first send the credentials of the created client to the platform by using the authorization API. The platform generates and sends back a security token, the unique cryptic string assigned to this specific client. Then, the system must add this token to all API requests.

   A security token eliminates the need for passing the client credentials with API requests. For additional security, the token expires in two hours. After this time, all API requests with the expired token will fail and the system will need to request a new token from the platform.

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

Creating an API client

1. Log in to the management portal.
2. Click **Settings** > **API clients** > **Create API client**.
3. Enter a name for the API client.
4. Click **Next**.

   The API client is created with the **Active** status by default.
5. Copy and save the ID and secret value of the client and the data center URL. You will need them when enabling the OAuth 2.0 client credentials flow in a third-party system.

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

Resetting the secret value of an API client

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

4. Click ⋯, and then click **Reset secret**.
5. Confirm your decision by clicking **Next**.

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

   All security tokens assigned to this client will become immediately expired and API requests with these tokens will fail.
6. Copy and save the new secret value of the client.

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

7. Click **Done**.

Disabling an API client

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

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

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

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

Enabling a disabled API client

1. Log in to the management portal.
2. Click **Settings** > **API clients**.
3. Find the required client in the list.
4. Click ⋯, and then click **Enable**.

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

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

Deleting an API client

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

4. Click …, and then click **Delete**.
5. Confirm your decision.

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

   Important

   There is no way to recover a deleted client.

Integration references

The following table lists the implemented integrations with third parties and provides the links to the respective documentation.

INTEGRATION NAME	View online	Open PDF
Autotask PSA	https://www.acronis.com/support/documentation/AutotaskPSA/	https://dl.acronis.com/u/pdf/AutotaskPSA_Integration_quickstartguide_en-US.pdf
CloudBlue Commerce	https://www.acronis.com/support/documentation/CloudBlueCommerce/	https://dl.acronis.com/u/pdf/CloudBlue_Commerce_Integration_Guide_en-US.pdf
CloudBlue PSA	https://www.acronis.com/support/documentation/CloudBluePSA/	https://dl.acronis.com/u/pdf/CloudBluePSAIntegration_quickstartguide_en-US.pdf
ConnectWise Automate	https://www.acronis.com/support/documentation/ConnectWiseAutomate/	https://dl.acronis.com/u/pdf/AcronisConnectWiseAutomatePlugin_userguide_en-US.pdf
ConnectWise Command	https://www.acronis.com/support/documentation/ConnectWiseCommand/	https://dl.acronis.com/u/pdf/ConnectWiseCommandIntegration_quickstartguide_en-US.pdf
ConnectWise Control	https://www.acronis.com/support/documentation/ConnectWiseControl/	https://dl.acronis.com/u/pdf/ConnectWiseControl_integration_en-US.pdf
ConnectWise Manage	https://www.acronis.com/support/documentation/ConnectWiseManage/	https://dl.acronis.com/u/pdf/ConnectWiseManageIntegration_quickstartguide_en-US.pdf
Datto RMM	https://www.acronis.com/support/documentation/DattoRMM/	https://dl.acronis.com/u/pdf/DattoRMMIntegration_quickstartguide_en-US.pdf

INTEGRATION NAME	View online	Open PDF
Jamf Pro	https://www.acronis.com/support/documentation/JamfPro/	https://dl.acronis.com/u/pdf/JamfProIntegration_quickstartguide_en-US.pdf
Kaseya BMS	https://www.acronis.com/support/documentation/KaseyaBMS/	https://dl.acronis.com/u/pdf/AcronisKaseyaBMSPlugin_userguide_en-US.pdf
Kaseya VSA	https://www.acronis.com/support/documentation/KaseyaVSA/	https://download.acronis.com/pdf/AcronisKaseyaVSAPlugin_userguide_en-US.pdf
Matrix 42	https://www.acronis.com/support/documentation/Matrix42/	https://dl.acronis.com/u/pdf/Matrix42Integration_quickstartguide_en-US.pdf
Microsoft Intune	https://www.acronis.com/support/documentation/MicrosoftIntune/	https://dl.acronis.com/u/pdf/MicrosoftIntuneIntegration_quickstartguide_en-US.pdf
N-able N-central	https://www.acronis.com/support/documentation/NableNcentral/	https://dl.acronis.com/u/pdf/N-able_N-central_Integration_Guide_en-US.pdf
N-able N-sight RMM	https://www.acronis.com/en-us/support/documentation/NableNsightRMM/	https://dl.acronis.com/u/pdf/N-ableN-sightRMMIntegration_quickstartguide_en-US.pdf
Ninja One	https://www.acronis.com/support/documentation/NinjaOne/	https://dl.acronis.com/u/pdf/NinjaOneIntegration_quickstartguide_en-US.pdf
Omnivoice	https://www.acronis.com/support/documentation/Omnivoice/	https://dl.acronis.com/u/pdf/OmnivoiceIntegration_quickstartguide_en-US.pdf
Plesk	https://www.acronis.com/support/documentation/Plesk/	https://dl.acronis.com/u/pdf/Acronis_Backup_extension_for_Plesk_en-US.pdf
PRTG	https://www.acronis.com/support/documentation/PRTG/	https://dl.acronis.com/u/pdf/AcronisPRTGPlugin_userguide_en-US.pdf
ServiceNow	https://www.acronis.com/support/documentation/ServiceNow/	https://dl.acronis.com/u/pdf/ServiceNow_Integration_quickstartguide_en-US.pdf
Splashtop	https://www.acronis.com/support/documentation/Splashtop/	https://dl.acronis.com/u/pdf/Splashtop_Integration_quickstartguide_en-US.pdf
Tigerpaw One	https://www.acronis.com/en-us/support/documentation/TigerpawOne/	https://dl.acronis.com/u/pdf/TigerpawOneIntegration_quickstartguide_en-US.pdf
WHM & cPanel	https://www.acronis.com/en-us/support/documentation/WHMCPanel/	https://www.acronis.com/en-us/support/documentation/WHMCPanel/
WHMCS	https://www.acronis.com/en-us/support/documentation/WHMCS/	https://dl.acronis.com/u/pdf/WHMCS_Integration_Manual_en-US.pdf

Integration with VMware Cloud Director

A service provider can integrate VMware Cloud Director (formerly VMware vCloud Director) with Cyber Protect Cloud and provide its customers with out-of-the-box backup solution for their virtual machines.

The integration includes the following steps:

1. Configuring the RabbitMQ message broker for the VMware Cloud Director environment.

   RabbitMQ allows synchronizing the changes in the VMware Cloud Director environment to Cyber Protect Cloud.
2. Installing the plug-in for VMware Cloud Director.

   This plug-in adds Cyber Protection to the VMware Cloud Director user interface.
3. Deploying a management agent.

   The management agent automatically maps VMware Cloud Director Organizations to customer tenants in Cyber Protect Cloud, and Organization Administrators to customer tenant administrators. For more information about Organizations, see Creating an Organization in VMware Cloud Director in the VMware Knowledge Base.

   The customer tenants are created within the partner tenant for which the VMware Cloud Director integration is configured. These new customer tenants are in the **Locked** mode and cannot be managed by partner administrators within Cyber Protect Cloud.

   > **Note**
   > Only Organization Administrators with unique email addresses in VMware Cloud Director are mapped to Cyber Protect Cloud.

4. Deploying one or more backup agents.

   The backup agent provides backup and recovery functionality for the virtual machines in the VMware Cloud Director environment.

To disable the integration between VMware Cloud Director and Cyber Protect Cloud, contact the technical support.

Limitations

- Integration with VMware Cloud Director is possible only for partner tenants in the **Managed by service provider** management mode, whose parent tenant (if any) also uses the **Managed by service provider** management mode. For more information about the types of tenants and their management mode, see "Creating a tenant" (p. 32).

  All existing direct partners can configure integration with VMware Cloud Director. Partner administrators can enable this option also for sub-tenants by selecting the **Partner-owned VMware Cloud Director infrastructure** check box when creating a child partner tenant.

- Two-factor authentication must be disabled for the partner tenant in which the integration with VMware Cloud Director is configured.
- An administrator who has the Organization Administrator role in multiple VMware Cloud Director Organizations can manage the backup and recovery only for one customer tenant in Cyber Protection.
- Cyber Protection web console opens in a new tab.

Software requirements

Supported VMware Cloud Director versions

- VMware Cloud Director 10.0, 10.1, 10.2, 10.3, 10.4, 10.4.1

Supported web browsers

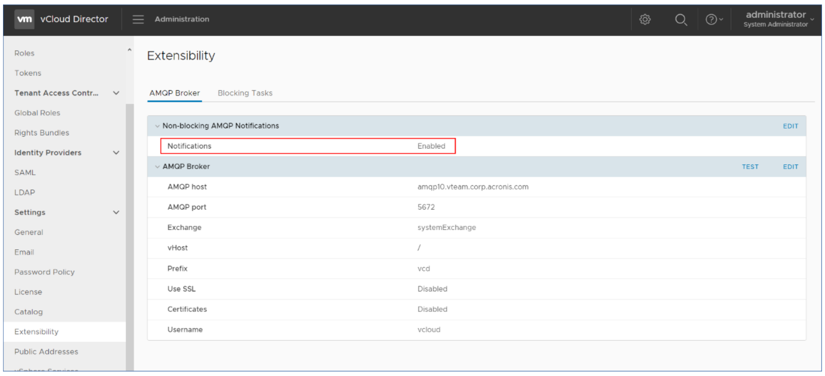
- Google Chrome 29 or later
- Mozilla Firefox 23 or later
- Opera 16 or later
- Microsoft Edge 25 or later
- Safari 8 or later running in the macOS and iOS operating systems

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.

Configuring RabbitMQ message broker

1. Install a RabbitMQ AMQP broker for your VMware Cloud Director environment.

   For more information on how to install RabbitMQ, see the VMware documentation: Install and Configure a RabbitMQ AMQP Broker.
2. Log in to the VMware Cloud Director provider portal as a System Administrator.
3. Go to **Administration** > **Extensibility**, and then verify that under **Non-blocking AMQP Notifications**, **Notifications** are enabled.



Extensibility

Non-blocking AMQP Notifications

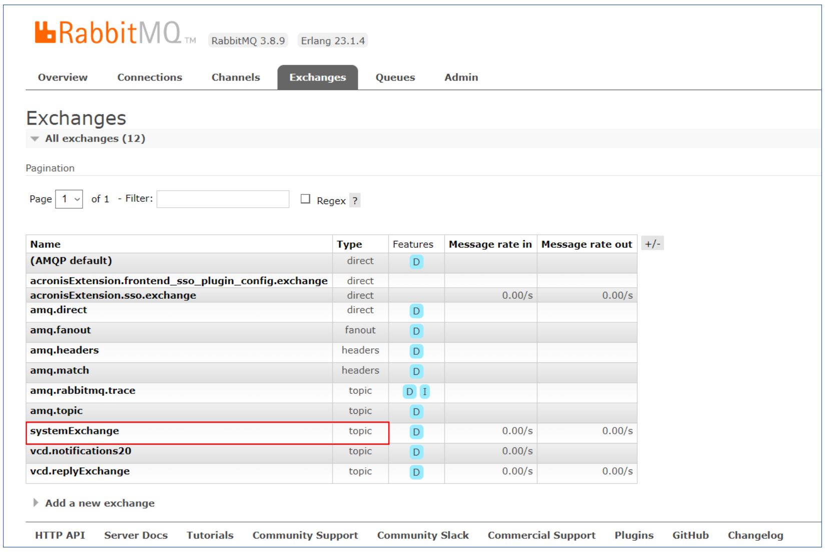
Notifications	Enabled

AMQP Broker

AMQP host	amqp10.vteam.corp.acronis.com
AMQP port	5672
Exchange	systemExchange
vHost	/
Prefix	vcd
Use SSL	Disabled
Certificates	Disabled
Username	vcloud

4. Log in to the RabbitMQ management console as an administrator.
5. On the **Exchanges** tab, verify that the exchange (by default, under the name **SystemExchange**)

is created, and its type is **topic**.



Name	Type	Features	Message rate in	Message rate out
(AMQP default)	direct	D		
acronisExtension.frontend_sso_plugin_config.exchange	direct			
acronisExtension.sso.exchange	direct		0.00/s	0.00/s
amq.direct	direct	D		
amq.fanout	fanout	D		
amq.headers	headers	D		
amq.match	headers	D		
amq.rabbitmq.trace	topic	D I		
amq.topic	topic	D		
systemExchange	topic	D	0.00/s	0.00/s
vcd.notifications20	topic	D	0.00/s	
vcd.replyExchange	topic	D	0.00/s	0.00/s

Installing the plug-in for VMware Cloud Director

1. Click the following link to download the **vCDPlugin.zip** file: https://dl.managed-protection.com/u/vCD/vCDPlugin.zip.
2. Log in to the VMware Cloud Director provider portal as a system administrator.
3. From the navigation menu, select **Customize Portal**.
4. On the **Manage Plugins** tab, click **Upload**.

   The **Upload Plugin** wizard opens.
5. Click **Select Plugin File**, and then select the **vCDPlugin.zip** file.
6. Click **Next**.
7. Configure the scope and publishing:
   a. In the **Scope to** section, select only the **Tenants** checkbox.
   b. In the **Publish to** section, select **All tenants** to enable the plug-in for all existing and future tenants, or select individual tenants for which you want to enable the plug-in.
8. Click **Next**.
9. Review your settings, and then click **Finish**.

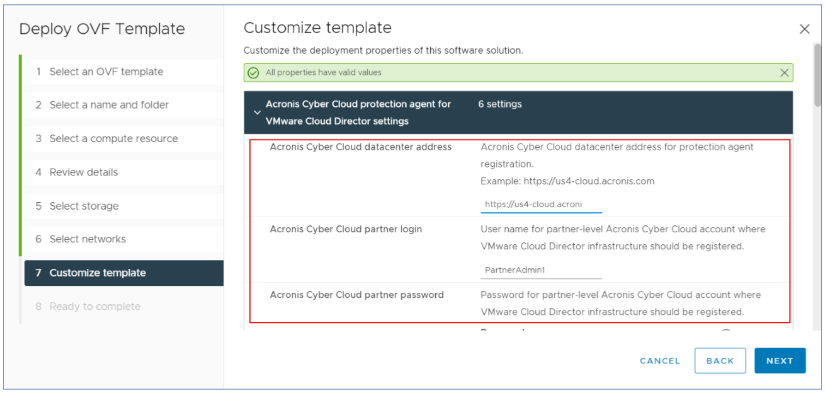
Installing a management agent

1. Log in to the Cyber Protect Cloud management portal as a partner administrator.
2. Go to **Settings** > **Location**, and then click **Add VMware Cloud Director**.
3. Click the **Management Agent** link and download the ZIP file.
4. Extract the management agent template file `vCDManagementAgent.ovf` and the virtual hard disk file `vCDManagementAgent-disk1.vmdk`.
5. In vSphere Client, deploy the management agent OVF template to an ESXi host under a vCenter instance that is managed by VMware Cloud Director.

Important

Install only one management agent per VMware Cloud Director environment.

6. In the **Deploy OVF Template** wizard, configure the management agent by setting the following:



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Select networks
7 Customize template
8 Ready to complete

Customize template

Customize the deployment properties of this software solution.

All properties have valid values

Acronis Cyber Cloud protection agent for VMware Cloud Director settings — 6 settings

Acronis Cyber Cloud datacenter address — Acronis Cyber Cloud datacenter address for protection agent registration. Example: https://us4-cloud.acronis.com — https://us4-cloud.acroni

Acronis Cyber Cloud partner login — User name for partner-level Acronis Cyber Cloud account where VMware Cloud Director infrastructure should be registered. — PartnerAdmin1

Acronis Cyber Cloud partner password — Password for partner-level Acronis Cyber Cloud account where VMware Cloud Director infrastructure should be registered.

   a. URL of the Cyber Protect Cloud data center. For example, `https://us5-cloud.example.com`.
   b. Partner administrator login and password.
   c. ID of the backup storage for virtual machines in the VMware Cloud Director environment.

      This backup storage can be partner-owned only. For more details on storages, refer to "Managing locations and storage" (p. 64).

      To check the ID, in the management portal, go to **Settings** > **Locations**, and then select the desired storage. You can see its ID after the **uuid=** part in the URL.
   d. Cyber Protect Cloud billing mode: **Per gigabyte** or **Per workload**.

      Note

      The selected billing mode applies to all new customer tenants that will be created.
   e. VMware Cloud Director parameters: infrastructure address, system administrator login, and password.
   f. RabbitMQ parameters: server address, port, virtual host name, administrator login, and password.
   g. Network parameters: IP address, subnet mask, default gateway, DNS, DNS suffix.

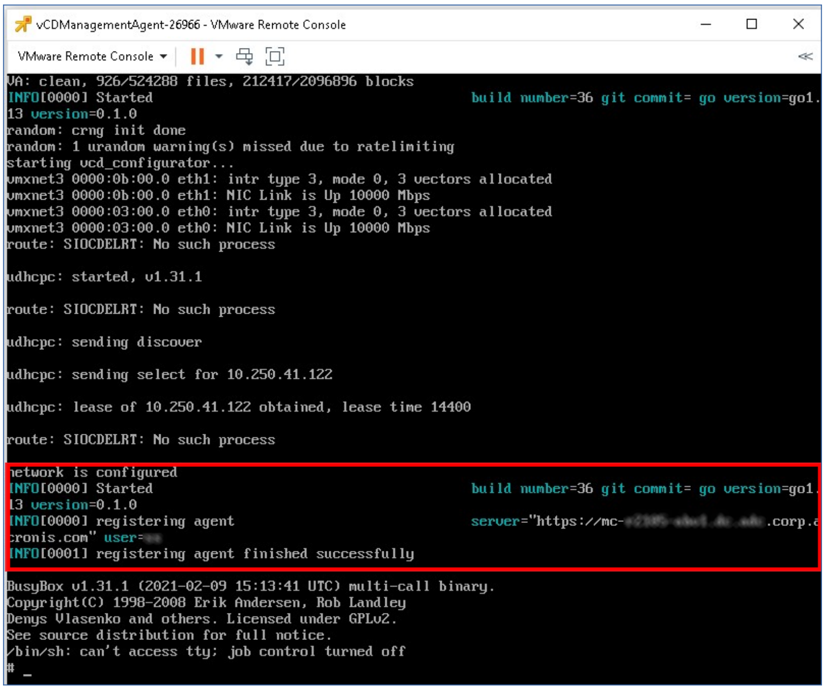
      By default, only one network interface is enabled. To enable a second network interface, select the checkbox next to **Enable eth1**.

      Note

      Ensure that your network settings allow the management agent to access both the VMware Cloud Director environment and your Cyber Protect Cloud data center.

You can also configure the management agent settings after the initial deployment. In vSphere Client, power off the virtual machine with the management agent, and then click **Configure** > **Settings** > **vApp Options**. Apply the desired settings, and then power on the virtual machine with the management agent.

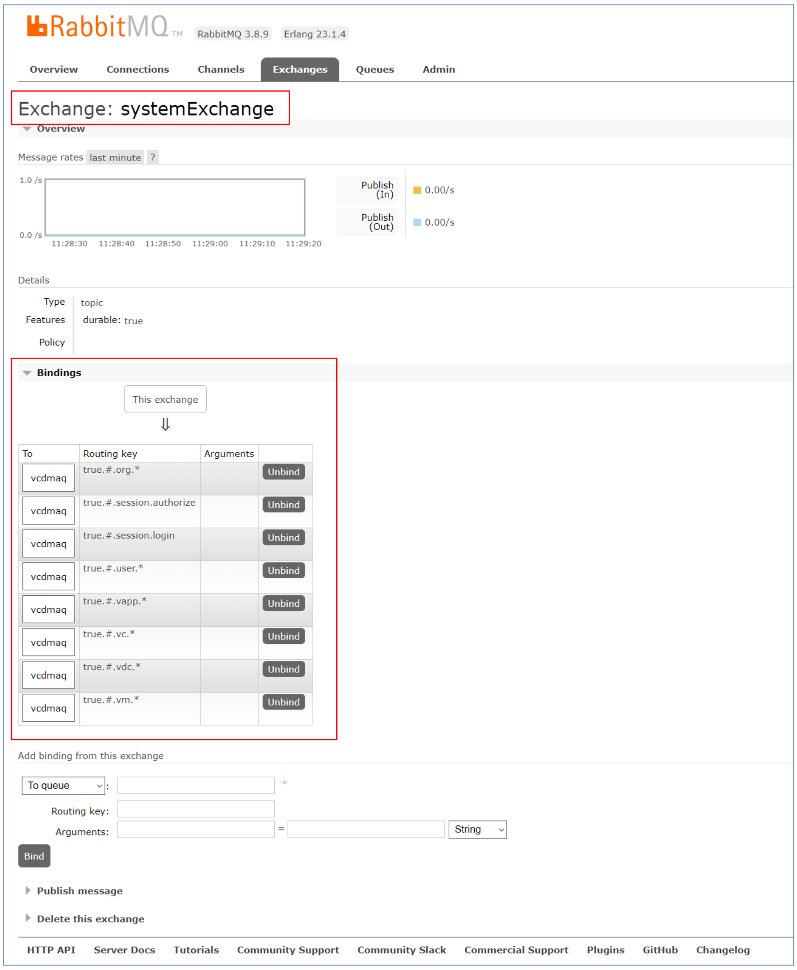
7. [Optional] In vSphere Client, open the console of the virtual machine with the management agent, and then verify your setup.



```
VA: clean, 926/524288 files, 212417/2096896 blocks
INFO[0000] Started                                       build number=36 git commit= go version=go1.
13 version=0.1.0
random: crng init done
random: 1 urandom warning(s) missed due to ratelimiting
starting vcd_configurator...
vmxnet3 0000:0b:00.0 eth1: intr type 3, mode 0, 3 vectors allocated
vmxnet3 0000:0b:00.0 eth1: NIC Link is Up 10000 Mbps
vmxnet3 0000:03:00.0 eth0: intr type 3, mode 0, 3 vectors allocated
vmxnet3 0000:03:00.0 eth0: NIC Link is Up 10000 Mbps
route: SIOCDELRT: No such process

udhcpc: started, v1.31.1

route: SIOCDELRT: No such process

udhcpc: sending discover

udhcpc: sending select for 10.250.41.122

udhcpc: lease of 10.250.41.122 obtained, lease time 14400

route: SIOCDELRT: No such process

network is configured
INFO[0000] Started                                       build number=36 git commit= go version=go1.
13 version=0.1.0
INFO[0000] registering agent                             server="https://mc-[redacted].corp.a
cronis.com" user=[redacted]
INFO[0001] registering agent finished successfully

BusyBox v1.31.1 (2021-02-09 15:13:41 UTC) multi-call binary.
Copyright(C) 1998-2008 Erik Andersen, Rob Landley
Denys Vlasenko and others. Licensed under GPLv2.
See source distribution for full notice.
/bin/sh: can't access tty; job control turned off
# _
```

8. Verify the RabbitMQ connection.
   a. Log in to the RabbitMQ management console as an administrator.
   b. In the **Exchanges** tab, select the exchange that you set during the RabbitMQ installation. By default, its name is **systemExchange**.

c. Verify the bindings to the **vcdmaq** queue.



Exchange: systemExchange

Message rates last minute ?

Publish (In) 0.00/s

Publish (Out) 0.00/s

Details

Type	topic
Features	durable: true
Policy	

Bindings

To	Routing key	Arguments	
vcdmaq	true.#.org.*		Unbind
vcdmaq	true.#.session.authorize		Unbind
vcdmaq	true.#.session.login		Unbind
vcdmaq	true.#.user.*		Unbind
vcdmaq	true.#.vapp.*		Unbind
vcdmaq	true.#.vc.*		Unbind
vcdmaq	true.#.vdc.*		Unbind
vcdmaq	true.#.vm.*		Unbind

Add binding from this exchange

To queue: *

Routing key:

Arguments: = String

Installing backup agents

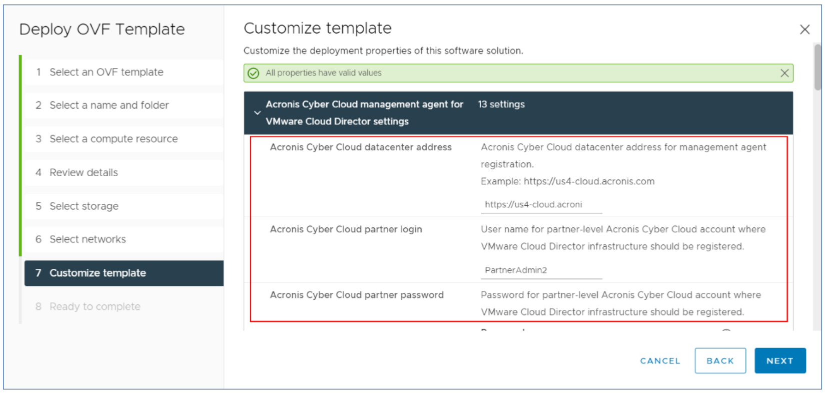
1. Log in to the management portal as a partner administrator.
2. Go to **Settings** > **Location**, and then click **Add VMware Cloud Director**.
3. Click the **Backup Agent** link and download the ZIP file.
4. Extract the backup agent template file `vCDCyberProtectAgent.ovf` and the virtual hard disk file `vCDCyberProtectAgent-disk1.vmdk`.
5. In vSphere Client, deploy the backup agent template to the desired ESXi host.

   You need at least one backup agent per host. By default, the backup agent is assigned 8 GB of RAM and 2 CPUs, and can process up to 10 backup or recovery tasks simultaneously. To process more tasks or to distribute the backup and recovery traffic, deploy additional agents to the same host.

   Note

   Backups of virtual machines on ESXi hosts where no backup agent is installed will fail with a "Task timeout expired" error.

6. In the **Deploy OVF Template** wizard, configure the backup agent by setting the following:



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Select networks
7 Customize template
8 Ready to complete

Customize template

Customize the deployment properties of this software solution.

All properties have valid values

Acronis Cyber Cloud management agent for VMware Cloud Director settings — 13 settings

Acronis Cyber Cloud datacenter address — Acronis Cyber Cloud datacenter address for management agent registration.
Example: https://us4-cloud.acronis.com
https://us4-cloud.acroni

Acronis Cyber Cloud partner login — User name for partner-level Acronis Cyber Cloud account where VMware Cloud Director infrastructure should be registered.
PartnerAdmin2

Acronis Cyber Cloud partner password — Password for partner-level Acronis Cyber Cloud account where VMware Cloud Director infrastructure should be registered.

a. URL of the Cyber Protect Cloud data center. For example, `https://us5-cloud.example.com`.
b. Partner administrator login and password.
c. VMware vCenter parameters: server address, login, and password.

   The agent will use these credentials to connect to the vCenter Server. We recommend that you use an account with the **Administrator** role assigned. Otherwise, provide an account with the necessary privileges on the vCenter Server.
d. Network parameters: IP address, subnet mask, default gateway, DNS, DNS suffix.

   By default, only one network interface is enabled. To enable a second network interface, select the checkbox next to **Enable eth1**.

   Note
   Ensure that your network settings will allow the backup agent to access both the vCenter Server and your Cyber Protect Cloud data center.
e. Download limit: the maximum download speed rate (in Kbps), which defines the backup archive read speed during recovery operation. The default value is 0 - unlimited.
f. Upload limit: the maximum upload speed rate (in Kbps), which defines the backup archive write speed during backup operation. The default value is 0 - unlimited.

You can also configure the backup agent setting parameters after the initial deployment. In vSphere Client, power off the virtual machine with the backup agent, and then click **Configure** > **Settings** > **vApp Options**. Apply the desired settings, and then power on the virtual machine with the backup agent.

7. In vSphere Client, ensure that **Host** and **Storage vMotion** are disabled for the virtual machine with the backup agent.

Updating the agents

To update a management agent

1. Log in to the Cyber Protect Cloud management portal as a partner administrator.
2. Go to **Settings** > **Location**, and then click **Add VMware Cloud Director**.
3. Click the **Management Agent** link, and then download the ZIP file with the latest agent.
4. Extract the management agent template file `vCDManagementAgent.ovf` and the virtual hard disk file `vCDManagementAgent-disk1.vmdk`.

5. In vSphere Client, power off the virtual machine with the current management agent.
6. Deploy a virtual machine with the new management agent by using the latest `vCDManagementAgent.ovf` and `vCDManagementAgent-disk1.vmdk` files.
7. Configure the management agent by using the same settings as in the old one.
8. [Optional] Delete the virtual machine with the old management agent.

Important
You must have only one active management agent per VMware Cloud Director environment.

To update a backup agent

1. Log in to the Cyber Protect Cloud management portal as a partner administrator.
2. Go to **Settings** > **Location**, and then click **Add VMware Cloud Director**.
3. Click the **Backup Agent** link and download the ZIP file with the latest agent.
4. Extract the management agent template file `vCDCyberProtectAgent.ovf` and the virtual hard disk file `vCDCyberProtectAgent-disk1.vmdk`.
5. In vSphere Client, power off the virtual machine with the current backup agent.

   All backup and recovery tasks that might be currently running will fail. To check whether any tasks are running, in vSphere Client, open the console of the virtual machine with the backup agent, and then run the command `ps | grep esx_worker`. Ensure that there are no active `esx_worker` processes.
6. Deploy a virtual machine with the new backup agent by using the latest `vCDCyberProtectAgent.ovf` and `vCDCyberProtectAgent-disk1.vmdk` files.
7. Configure the backup agent by using the same settings as in the old one.
8. [Optional] Delete the virtual machine with the old backup agent.

Accessing the Cyber Protection web console

The following administrators can manage the backup of virtual machines in VMware Cloud Director Organizations:

- Organization Administrators
- Specifically assigned backup administrators
  For more information on how to create such an administrator, refer to "Creating a backup administrator" (p. 139).

Administrators can access the custom Cyber Protection web console by clicking **Cyber Protection** in the navigation menu of the VMware Cloud Director tenant portal.

Note
The single sign-on is available only for Organization Administrators and is not supported for System Administrators who use the VMware Cloud Director tenant portal.

In the Cyber Protection web console, administrators can access only their own VMware Cloud Director Organization elements: virtual data centers, vApps, and individual virtual machines. They can manage the backup and recovery of the VMware Cloud Director Organization resources.

Partner administrators can access the Cyber Protection web consoles of their customer tenants and can manage backup and recovery on their behalf.

Limitations

The list of limitations is subject to change in the upcoming releases of Cyber Protect Cloud.

Backup

- Only backup of the entire machine is supported. File filters, or selecting disks or volumes, are not available.
- Only cloud storage is supported as a backup location. The storage is configured in the management agent settings and users cannot change it in the protection plan.
- Dynamic groups are not supported.
- The following backup schemes are supported: **Always incremental (single file)**, **Always full**, and **Weekly full, Daily incremental**.
- Cleanup only after backup is supported.

Recovery

- Recovery only to the original virtual machine is supported. The original virtual machine must exist in the VMware Cloud Director environment.
- File-level recovery is not supported.

Creating a backup administrator

Organization Administrators can delegate the backup management to specifically assigned backup administrators.

To create a backup administrator

1. In the VMware Cloud Director tenant portal, click **Administration** > **Roles** > **New**.
2. In the **Add Role** window, specify a name and description for the new role.
3. Scroll down the list of permissions, and then, under **Other**, select **Self-service VM backup operator**.

   Note
   The **Self-service VM backup operator** permission becomes available after you install the plug-in for VMware Cloud Director. For more information on how to do this, refer to "Installing the plug-in for VMware Cloud Director" (p. 133).

4. In the VMware Cloud Director tenant portal, click **Users**.

5. Select a user, and then click **Edit**.
6. Assign this user the new role that you created.

   As a result, the selected user will be able to manage the backups for the virtual machines in this Organization.

Note

System Administrators of the VMware Cloud Director environment can define a global role with the **Self-service VM backup operator** permission enabled, and then publish this role to the tenants. Thus, the Organization Administrators will only need to assign the role to a user.

System report, log files, and configuration files

For troubleshooting purposes, you might need to create a system report by using the `sysinfo` tool, or to check the log and configuration files on a virtual machine with an agent.

You can access the virtual machine either directly, by opening its console in vSphere Client, or remotely – via an SSH client. To access the virtual machine via an SSH client, first you have to enable the SSH connection to this machine.

To enable the SSH connection to a virtual machine

1. In vSphere Client, open the console of the virtual machine with the agent.
2. At the command prompt, run the following command: `/bin/sshd` to start the SSH daemon.

As a result, you can connect to this virtual machine by using an SSH client, such as WinSCP, for example.

To run the `sysinfo` tool

1. Access the virtual machine with the agent.
   - To access it directly, in vSphere Client, open the console of the virtual machine.
   - To access it remotely, connect to the virtual machine via an SSH client.

     Use the following default login:password combination: `root`:`root`.
2. Navigate to the `/bin` directory, and then run the `sysinfo` tool.

   ```
   # cd /bin/
   # ./sysinfo
   ```

   As a result, a system report file will be saved to the default directory: `/var/lib/Acronis/sysinfo`.

   You can specify another directory by running the `sysinfo` tool with the `--target_dir` option.

   ```
   ./sysinfo --target_dir path/to/report/dir
   ```
3. Download the generated system report by using an SSH client.

To access a log or configuration file

1. Connect to the virtual machine via an SSH client.

   Use the following default login:password combination: `root:root`.
2. Download the desired file.

   You can find the log files in the following locations:

   - Backup agent: `/opt/acronis/var/log/vmware-cloud-director-backup-service/log.log`
   - Management agent: `/opt/acronis/var/log/vmware-cloud-director-management-agent/log.log`

   You can find the configuration files in the following locations:

   - Backup agent: `/opt/acronis/etc/vmware-cloud-director-backup-service/config.yml`
   - Management agent: `/opt/acronis/etc/vmware-cloud-director-management-agent/config.yaml`

Removing the integration with VMware Cloud Director

Reverting the configuration and unregistering the VMware Cloud Director instance from Cyber Protect Cloud is a complex procedure. Please contact your support representative for help.

Privacy settings

Privacy settings help you indicate whether or not you give consent for the collection, use and disclosure of your personal information.

Depending on the country in which you are using Cyber Protect and the Cyber Protect Cloud data center that provides services to you, on the initial launch of Cyber Protect you may be asked to confirm whether you agree to use Google Analytics in Cyber Protect.

Google Analytics helps us better understand user behavior and improve user experience in Cyber Protect by collecting pseudonymized data.

If you do not see Google Analytics consent and menus in Cyber Protect interface, in means that Google Analytics is not used in your country.

If you enabled or refused to enable Google Analytics on the initial launch of Cyber Protect, you can change your decision at any time later.

To enable or disable Google Analytics

1. In the Cyber Protect console, click on the account icon in the upper-right corner.
2. Select **My privacy settings**.
3. In the **Google Analytics data collection** section click one of the following buttons:
   - **On** to enable Google Analytics
   - **Off** to disable Google Analytics

Index

#

#CyberFit Score by machine 78

7

7-day history bar 29

A

About Cyber Protect 6

About this document 5

Accessing the Cyber Protection web console 138

Accessing the Cyber Protection console from the management portal 26

Accessing the management portal 25

Accessing the services 28

Actions in the Device list 63

Activating the administrator account 24

Adding a report 98

Adding new storages 65

Advanced Data Loss Prevention 122

Advanced Disaster Recovery 124

Advanced Email Security 125

Advanced Protection packs 118

Advanced Security + EDR 123

Agent and installer branding 69

Agent installer dependency on offering items 21

Antimalware protection widgets 103

Appearance 69

Applying white labeling 72

Audit log 115

Audit log fields 116

Autodiscovery wizard 63

B

Backup 139

Backup quota transformation 17

Backup quotas 15

Backup scanning details 89

Backup widgets 105

Billing for Notary 8

Billing for Physical Data Shipping 8

Billing modes and editions 12

Billing modes for Cyber Protect 7

Billing modes for File Sync & Share 8

Billing modes for the Protection component 7

Blocked URLs 91

Branding items 69

Brute-force protection 61

C

Changing the billing mode for a customer tenant 11

Changing the billing mode for a partner tenant 10

Changing the notification settings for a user 53

Changing the service quota of machines 20

Choosing locations and storages for partners and customers 64

Clients tab 28

Configuring branding 71

Configuring branding and white labeling 68

Configuring company contacts 40

Configuring contacts in the Company profile wizard 25

Configuring custom usage reports 95

Configuring custom web interface URLs 72

Configuring immutable storage 66

Configuring RabbitMQ message broker 132

Configuring scheduled usage reports 95

Configuring self-managed customer profile 39

Configuring the offering items for a tenant 36

Configuring the settings of the Executive summary report 109

Configuring upsell scenarios for your customers 62

Converting a partner tenant to a folder tenant and vice versa 44

Creating a backup administrator 139

Creating a tenant 32

Creating a user account 46

Creating an API client 127

Creating an Executive summary report 110

Creating or editing a protection plan 63

Customizing the Executive summary report 110

Cyber Protect services 6

D

Data Loss Prevention widget 108

Data protection map 85

Deleting a tenant 45

Deleting a user account 55

Deleting an API client 128

Deleting storages 65

Disabling an API client 128

Disabling and enabling a tenant 42

Disabling and enabling a user account 54

Disabling the branding 71

Disaster Recovery quotas 18

Disaster Recovery widgets 106

Discovered machines 77

Disk health monitoring 81

Disk health status alerts 85

Disk health widgets 82

Documentation and support 69

Downloading a report 100

Downloading data for recently affected workloads 90

Dumping the report data 100

E

Editing the report settings 98

Email server settings 71

Enabling a disabled API client 128

Enabling Advanced Data Loss Prevention 123

Enabling Advanced Security + EDR 123

Enabling maintenance notifications 39

Enabling or disabling offering items 12

Enabling services for multiple existing tenants 37

Endpoint Detection and Response (EDR) widgets 79

Enhanced security mode 34

Example

Cyber Protect per workload edition to Per workload billing 10

Switching Cyber Protect Advanced edition to Per workload billing 9

Exceeding the quota for backup storage 17

Executive summary 100

Executive summary widgets 101

Existing vulnerabilities 87

Exporting and importing the report structure 100

F

File Sync & Share quotas 19

File Sync & Share widgets 108

Filtering and search 117

H

Hardware inventory widgets 92

How it works 56, 81

How to move a tenant 44

I

Incident MTTR 79

Included and advanced features in the Protection service 119

Included features and advanced packs in Cyber Protect services 118

Installing a management agent 133

Installing backup agents 136

Installing the plug-in for VMware Cloud Director 133

Integration references 129

Integration with third-party systems 126

Integration with VMware Cloud Director 131

Integrations 126

L

Legal documents settings 70

Levels on which quotas can be defined 14

Limitations 35, 81, 131, 139

Limiting the access to the web interface 27

Limiting the access to your tenant 45

Locations 64

M

Managing API clients 126

Managing locations and storage 64

Managing storage 65

Managing tenants 32

Managing two-factor authentication for users 59

Managing users 46

Metrics with zero usage 95

Missing updates by categories 89

Mobile apps 70

Monitoring 60, 75

Moving a tenant to another tenant 43

N

Navigation in the management portal 26

Notary quotas 20

Notary widgets 109

Notifications received by user role 54

O

Offering items 12

Offering items and quota management 11

Operations 75

Operations reports 96

Operations with locations 64

Overview tab 28

P

Password requirements 24

Patch installation history 89

Patch installation status 88

Patch installation summary 88

Patch installation widgets 88

Pay as you go and advanced features in the Protection service 122

Physical Data Shipping quotas 19

Preventing unlicensed Microsoft 365 users from signing in 18

Privacy settings 142

Protection status 77

Q

Quotas for cloud data sources 15

Quotas for storage 17

R

Recently affected 90

Recovery 139

Refreshing the usage data for a tenant 42

Removing the integration with VMware Cloud Director 141

Report scope 95

Report type 94

Reported data according to widget type 113

Reporting 94

Requirements and restrictions 43

Resetting the secret value of an API client 127

Resetting two-factor authentication in case of lost second-factor device 61

Restoring the default branding settings 71

S

Scheduling a report 99

Security incident burndown 80

Selecting the services for a tenant 35

Sending Executive summary reports 112

Services 11

Services and offering items 11

Session history 93

Setting up an integration for Cyber Protect Cloud 126

Setting up soft and hard quotas 14

Setting up two-factor authentication 56

Setting up two-factor authentication for your tenant 59

Soft and hard quotas 13

Software inventory widgets 91

Software requirements 132

Supported VMware Cloud Director versions 132

Supported web browsers 24, 132

Switching between editions and billing modes 9

Switching from legacy editions to the current licensing model 8

System report, log files, and configuration files 140

T

Time zones in reports 112

To disable two-factor authentication for a user 60

To disable two-factor authentication for your tenant 59

To enable two-factor authentication for a user 61

To enable two-factor authentication for your tenant 59

To monitor agent updates 75

To reset the trusted browsers for a user 60

To reset the two-factor authentication for a user 60

To update agents automatically 73

Top incident distribution per workload 79

Transferring ownership of a user account 55

Two-factor setup propagation across tenant levels 57

Type of tenants that can be moved 43

Typical integration procedure 127

U

Updating agents automatically 73

Updating the agents 137

Upsell 70

Upsell points shown to a customer 63

URL for Cyber Protect Cloud services 70

Usage 75, 94

User accounts and tenants 30

User roles and Cyber Scripting rights 51

User roles available for each service 48

Using the billing modes with legacy editions 8

Using the management portal 24

V

Vulnerability assessment and patch management widgets 106

Vulnerability assessment widgets 87

Vulnerability list 63

Vulnerable machines 87

W

What is an API client? 126

White labeling 71

Workload network status 80

Workloads overview widgets 101