# Table of contents

## About this document

5

## About Cyber Protect

6

Cyber Protect services ........................................... 6

Billing modes for Cyber Protect .................................. 7

Offering items and quota management .......................... 9

Services and offering items ...................................... 9

Cyber Protection service editions and sub-editions ........ 19

Mixing offering items from different sub-editions ......... 20

Changing editions for a partner tenant ....................... 21

Changing the edition for a customer tenant .................. 21

Switching between editions and billing modes ............... 22

## Using the management portal ................................ 25

Supported web browsers ........................................ 25

Activating the administrator account ......................... 25

Accessing the management portal .............................. 25

Navigation in the management portal ......................... 26

Limiting the access to the web interface ..................... 26

Accessing the services ........................................... 27

Overview tab ....................................................... 27

Clients tab ................................................................ 28

7-day history bar ................................................... 29

User accounts and tenants ........................................ 29

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

Configuring company contacts .................................. 37

Refreshing the usage data for a tenant ....................... 39

Disabling and enabling a tenant ............................... 39

Moving a tenant to another tenant ............................. 39

Converting a partner tenant to a folder tenant and vice versa ...................................................... 40

Limiting the access to your tenant ............................. 41

Deleting a tenant .................................................... 41

Managing users ...................................................... 42
About this document

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

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

THIS IS A BETA VERSION OF THE DOCUMENTATION. SOME FEATURE DESCRIPTIONS MIGHT BE MISSING OR INCOMPLETE.
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.

Legacy editions are still available, but not recommended to use because they provide less flexibility in billing. For information about legacy editions and sub-editions, see "Cyber Protection service editions and sub-editions" (p. 19).

The following services and feature sets are available in Cyber 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. 107).
  - 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. 22).

To switch from editions to billing modes for multiple customers, see Mass edition switch for multiple customers (67942).
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. 55).

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. 11).

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.

<table>
<thead>
<tr>
<th>Offering item</th>
<th>Disabling</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup storage</td>
<td>Can be disabled when the usage is equal to zero.</td>
<td>The cloud storage will become unavailable as a destination for backups within a customer tenant.</td>
</tr>
<tr>
<td>Local backup</td>
<td>Can be disabled when the usage is equal to zero.</td>
<td>The local storage will become unavailable as a destination for backups within a customer tenant.</td>
</tr>
<tr>
<td>Data sources (including Microsoft 365 and Google Workspace)</td>
<td>Can be disabled when the usage is equal to zero.</td>
<td>The backup and recovery of data sources (including Microsoft 365 and Google Workspace) will become unavailable within a customer tenant.</td>
</tr>
<tr>
<td>All Disaster Recovery offering items</td>
<td>Can be disabled when the usage is more than zero.</td>
<td>See the details in &quot;Soft and hard quotas&quot;.</td>
</tr>
<tr>
<td>All Notary offering</td>
<td>Can be disabled</td>
<td>The Notary service will be unavailable within a</td>
</tr>
</tbody>
</table>
items | when the usage is equal to zero. | 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.

**Levels on which quotas can be defined**

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

<table>
<thead>
<tr>
<th>Tenant/User</th>
<th>Soft quota (only quota)</th>
<th>Hard quota (quota and overage)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partner</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Folder</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Customer</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Unit</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>User</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>
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.

**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 the knowledge base article.

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

- Shared mailboxes
- Rooms and equipment
- External users with access to backed up SharePoint sites and/or Microsoft Teams
For more information about the licensing options with the per gigabyte billing mode, refer to Cyber Protect Cloud: Microsoft 365 per GB licensing.

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

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

- **Microsoft 365 SharePoint Online**
  This quota is applied by the service provider to the entire company. This quota enables or disables the ability to protect SharePoint Online sites and sets the maximum number of site collections and group sites that can be protected. Company administrators can view the quota in the management portal. They can also view the quota, together with the amount of storage occupied by the SharePoint Online backups, in the usage reports.

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

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

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

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

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

**Quotas for storage**

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

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

**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.

**Disaster Recovery quotas**

**Note**

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

These quotas are applied by the service provider to the entire company. Company administrators can view the quotas and the usage in the management portal, but cannot set quotas for a user.
• **Disaster recovery storage**
  This storage is used by primary and recovery servers. If the overage for this quota is reached, it is not possible to create primary and recovery servers, or add/extend disks of the existing primary servers. If the overage for this quota is exceeded, it is not possible to initiate a failover or just start a stopped server. Running servers continue to run.

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

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

• **Cloud servers**
  This quota limits the total number of primary and recovery servers. If the overage for this quota is reached, it is not possible to create primary or recovery servers.
  When the quota is disabled, the servers are visible in the service console, but the only available operation is **Delete**.

• **Internet access**
  This quota enables or disables the Internet access from the primary and recovery servers.
  When the quota is disabled, the primary and recovery servers will not be able to establish connections to the Internet.

**File Sync & Share quotas**
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.

<table>
<thead>
<tr>
<th>Enabled offering item</th>
<th>Server s</th>
<th>Workstations</th>
<th>Virtual machines</th>
<th>Microsoft 365 seats</th>
<th>Google Workspace seats</th>
<th>Mobile devices</th>
<th>Web hosting servers</th>
<th>Websites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent installer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workstations – Agent for Windows</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Workstations – Agent for Mac OS</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Servers – Agent for Windows</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Servers – Agent for Linux</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Agent for Hyper-V</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent for VMware</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent for Virtuozzo</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent for SQL</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent for Exchange</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent for Active Directory</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent for Microsoft</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
</tr>
</tbody>
</table>
The following editions are available:

- Cyber Protect
- Cyber Backup

### Cyber Protect edition

This edition is licensed per workload—that is, according to the number of protected machines, regardless of the size of backed-up data.

Within the Cyber Protect edition, the following sub-editions are available:

- Cyber Protect Essentials
- Cyber Protect Standard
Cyber Protect Advanced
Cyber Backup Standard

The Cyber Protect edition is flexible and allows partner administrators to mix features from different sub-editions in one customer tenant. For more information on how to create a tailored offering, refer to Mixing offering items from different sub-editions.

Cyber Backup edition

This edition is licensed per GB—that is, according to the size of backed-up data, regardless of the number of protected machines.

In the Cyber Backup edition, there are no sub-editions—only Cyber Backup Standard offering items are available.

Comparison of editions

The number and scope of the available features depend on the edition of Cyber Protection service. For a detailed comparison between the features in each edition and sub-edition, refer to Compare Cyber Protection Editions.

Disaster Recovery add-on

The Disaster Recovery add-on provides recovery functionality designed for companies that have high requirements for the Recovery Time Objective (RTO). This add-on is available only with the Cyber Protect edition.

Note
The Disaster recovery add-on cannot be used with the Cyber Protect Essentials sub-edition.

Mixing offering items from different sub-editions

Important
This topic contains information about a legacy licensing model. If you do not use editions as part of your legacy setup, please skip this information.

For a partner tenant, more than one edition can be available.

For a customer tenant, only one edition can be selected: either Cyber Protect or Cyber Backup.

However, the Cyber Protect edition allows mixing offering items from different sub-editions. Offering items from Cyber Backup Standard can also be added to the mix, but they will be billed per workload, like all other offering items in the Cyber Protect edition, including the Local storage.

Thus, in a customer tenant with the Cyber Protect edition, different workloads can be protected by features available in different sub-editions. For example, some machines in this tenant can be protected with the Workstations offering item from the Cyber Protect Essentials sub-edition, while
others can be protected with the **Servers** offering item from the Cyber Protect Advanced sub-edition.

You can also mix parallel offering items from different sub-editions, for example, **Workstations** from the Cyber Protect Essentials sub-edition and **Workstations** from the Cyber Protect Standard sub-edition.

The respective protection level is assigned automatically to a machine according to its type, the settings of its first protection plan, and this order of priority:

1. Cyber Protect Essentials
2. Cyber Backup Standard
3. Cyber Protect Standard
4. Cyber Protect Advanced

An administrator with access to the Cyber Protection service console can manually change the protection level of a specific machine, by selecting an appropriate service quota for it. For more information about how to do this, refer to Changing the service quota of machines.

### Changing editions for a partner tenant

**Important**

This topic contains information about a legacy licensing model. If you do not use editions as part of your legacy setup, please skip this information.

**To change the available editions for a partner tenant**

1. In the management portal, go to **Clients**.
2. Select the partner tenant whose editions you want to change, click the ellipsis icon ⋮, and then click **Configure**.
3. In the **Configure** tab, select the desired editions.
4. Enter your login to confirm your choice.

### Changing the edition for a customer tenant

**Important**

This topic contains information about a legacy licensing model. If you do not use editions as part of your legacy setup, please skip this information.

You can change the edition for a customer tenant by:

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

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

---

21
To switch the edition 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. In the Configure tab, select the new edition.

4. Enter your login to confirm your choice.

This change may take up to 10 minutes to complete.

Note

You can switch from the Cyber Protect edition with multiple parallel offering items—for example, Workstations from different sub-editions—to an edition with only one similar offering item, for example Cyber Backup. To do so, you need to move all of the usage in the source edition to one of the parallel offering items first.

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), between editions and billing modes, and between billing modes and editions.

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.

<table>
<thead>
<tr>
<th></th>
<th>Edition &gt; Billing modes</th>
<th>Billing modes &gt; edition (not recommended)</th>
<th>Billing mode &gt; Billing mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offering items</td>
<td>Enable offering items to fulfill the functionality that was available in the source edition.</td>
<td>Enable offering items to fulfill the functionality that was available in the source billing mode.</td>
<td>The identical set of the offering items will be enabled.</td>
</tr>
<tr>
<td>switch</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch direction</td>
<td>Edition &gt; Billing modes</td>
<td>Billing modes &gt; edition (not recommended)</td>
<td>Billing mode &gt; Billing mode</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------</td>
<td>-------------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td><strong>Quota switch</strong></td>
<td>Quota will be replicated from the source offering item to destination offering items. Source Standard → destination Standard product. Source Standard → destination packs. <strong>Note</strong> If you are switching from an edition with sub-editions (for example, &quot;Cyber Protect (per workload)&quot;), the quotas will be summarized.</td>
<td>The quota of Standard product offering item is used as a quota for destination offering item by default. <strong>Note</strong> Quotas of the source packs will be reset during the switch.</td>
<td>Quotas will be replicated from the source offering item to the destination offering item.</td>
</tr>
<tr>
<td><strong>Usage switch</strong></td>
<td>Offering items will be reassigned to the workloads according to the features requested in the protection plans assigned on these workloads.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Source offering items - usage/quota</th>
<th>Destination offering items - usage/quota</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Protect Advanced workstation 8/10</td>
<td>• Workstation - 8/10 \n• Advanced Security - 2/10 \n• Advanced Backup workstation - 1/10 \n• Advanced Management - 3/10</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Source offering items - usage/quota</th>
<th>Destination offering items - usage/quota</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Protect Essentials Workstation - 6/12</td>
<td>• Workstation - 14/42 \n• Advanced Backup workstation - 2/42 \n• Advanced Security - 13/42 \n• Advanced Management - 5/42</td>
</tr>
<tr>
<td>Cyber Protect Standard Workstation - 5/10</td>
<td></td>
</tr>
<tr>
<td>Cyber Protect Advanced Workstation - 2/10</td>
<td></td>
</tr>
<tr>
<td>Cyber Backup Standard Workstation - 1/10</td>
<td></td>
</tr>
</tbody>
</table>

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.
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:

- **An account activation link.** Click the link and set the password for the administrator account. Ensure that your password is at least eight characters long. Remember the login that is shown on the account activation page.
- **A link to the login page.** The login and password are the same as in the previous step.

Accessing the management portal

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 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.
Navigation in the management portal

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

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

All parts of the user interface display and affect only the 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 **Users** tab displays only 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.

<table>
<thead>
<tr>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>red</td>
<td>at least one of the backups during the one-hour period failed</td>
</tr>
<tr>
<td>orange</td>
<td>at least one of the backup during the one-hour period completed with a warning, but without any backup errors</td>
</tr>
<tr>
<td>green</td>
<td>there was at least one successful backup during the one-hour period, without any backup errors and warnings</td>
</tr>
<tr>
<td>grey</td>
<td>there were no completed backups during the one-hour period</td>
</tr>
</tbody>
</table>

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.
This is a beta version of the documentation. Some feature descriptions might be missing or incomplete.
The following table summarizes operations that can be performed by the administrators and users.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Users</th>
<th>Customer and unit administrators</th>
<th>Partner and folder administrators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create tenants</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Create accounts</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Download and install the software</td>
<td>Yes</td>
<td>Yes</td>
<td>No*</td>
</tr>
<tr>
<td>Manage services</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Create reports about the service usage</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Configure branding</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

*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 top-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.

The available types depend on the parent tenant type.

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.

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.


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 contact type.
   - **Billing** - a main contact for communication related to billing, payments, usage reports, and so on.
   - **Technical** - a main contact for communication related to new features and changes, technical questions, maintenance notifications, and so on.
   - **Business** - a main contact for business-related questions and business decisions.
   You can assign more than one contact type to a contact.

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.

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.

**Configuring company contacts**

As a partner, you can configure contact information for your company and for the tenants managed by you. We send important information about new features, technical updates, and billing to the contacts in this list.

You can add multiple contacts and assign contact types, 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 are not related to the system.

**To configure contacts for your company**

1. In the management console, go to Company Management > Partner 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 contact type.
       - **Billing** - a main contact for communication related to billing, payments, usage reports, and so on.
       - **Technical** - a main contact for communication related to new features and changes, technical questions, maintenance notifications, and so on.
       - **Business** - a main contact for business-related questions and business decisions.
         - You can assign more than one contact type to a contact.
   
   If you delete a contact that is associated with a user from the list of contacts in the Partner profile, the user will not be deleted. The system will unassign all contact types for the user, so they will no longer appear in the Contact types 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 Contact type.
    - **Billing** - a main contact for communication related to billing, payments, usage reports, and so on.
- **Technical** - a main contact for communication related to new features and changes, technical questions, maintenance notifications, and so on.
- **Business** - a main contact for business-related questions and business decisions.
  You can assign more than one contact type to a contact.

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 contact type.
    - **Billing** - a main contact for communication related to billing, payments, usage reports, and so on.
    - **Technical** - a main contact for communication related to new features and changes, technical questions, maintenance notifications, and so on.
    - **Business** - a main contact for business-related questions and business decisions.
      You can assign more than one contact type to a contact.

If you delete a contact that is associated with a user from the list of contacts in the Partner profile, the user will not be deleted. The system will unassign all contact types for the user, so they will no longer appear in the **Contact types** 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 **Contact type**.
    - **Billing** - a main contact for communication related to billing, payments, usage reports, and so on.
    - **Technical** - a main contact for communication related to new features and changes, technical questions, maintenance notifications, and so on.
- **Business** - a main contact for business-related questions and business decisions.
  You can assign more than one contact type to a contact.

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 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.
Restrictions

- A partner/folder tenant can be moved only to a partner/folder tenant.
- A customer tenant can be moved only to a partner/folder tenant.
- A unit tenant cannot be moved.
- A tenant can be moved only if the target parent tenant has the same or a larger set of services and offering items as the original parent tenant.
- Tenants can be moved only inside one partner account hierarchy. Moving customers between partner account hierarchies is not supported.
- 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.

How to move a tenant

1. Log in to the management portal.
2. On the **Clients** tab, select the target tenant to which you want to move a tenant.
3. On the tenant properties panel, click the vertical ellipse icon, and then click **Show ID**.
4. Copy the text string shown in the **Internal ID** field, and then click **Cancel**.
5. On the **Clients** tab, select the tenant which you want to move.
6. On the tenant properties panel, click the vertical ellipse icon, and then click **Move**.
7. Paste the internal identifier of the target tenant, and then click **Move**.

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 ellipse icon next to the tenant name.
   - Select the tenant, and then click the ellipse 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/unit administrator accounts — to delegate the service management to other people whose access permissions will be strictly limited to the corresponding customer/unit.
• User accounts within the customer or a unit tenant — to enable the users to access only a subset of the services.

Please 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.
3. In the top-right corner, click New > User.
4. Specify the following contact information for the account:
   • Login
     Important
     Each account must have a unique login.

       • Email
       • First name
       • Last name
       • Business phone
       • Job title
     • In Language, change the default language of notifications, reports, and the software that will be used for this account.
5. Specify the contact type.
   • Billing - a main contact for communication related to billing, payments, usage reports, and so on.
- **Technical** - a main contact for communication related to new features and changes, technical questions, maintenance notifications, and so on.
- **Business** - a main contact for business-related questions and business decisions.

You can assign more than one contact type to a contact.

You can view the assigned contact types for a user in the **Users** list, in column **Contact type**, and edit the user account to change the contact types 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.

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 **Users**.

2. Select the user whose password you want to reset, and then click the ellipsis icon > **Reset password**.

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

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

**User roles available for each service**

One user can have several roles but only one role per service.
For each service, you can define which role will be assigned to a user.

<table>
<thead>
<tr>
<th>Service</th>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>n/a</td>
<td>Company administrator</td>
<td>This role grants administrator rights for all services. This role grants access to the corporate whitelist. If the Disaster Recovery add-on of the Cyber Protection service is enabled for the company, this role also grants access to the disaster recovery functionality.</td>
</tr>
<tr>
<td>Management Portal</td>
<td>Administrator</td>
<td>This role grants access to the management portal where the administrator can manage users within the entire organization.</td>
</tr>
<tr>
<td></td>
<td>Read-only administrator</td>
<td>The role provides read-only access to all objects in the management portal. Such users can access data of other users of the organization in the read-only mode.</td>
</tr>
<tr>
<td>Cyber Protection</td>
<td>Administrator</td>
<td>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 whitelist.</td>
</tr>
<tr>
<td></td>
<td>Read-only administrator</td>
<td>The role provides read-only access to all objects of the Cyber Protection service. Such users can access data of other users of the organization in the read-only mode. The read-only administrator cannot configure and manage the Disaster Recovery functionality or the corporate whitelist.</td>
</tr>
<tr>
<td></td>
<td>Restore operator</td>
<td>The role provides access to backups of Microsoft 365 and Google Workspace organizations and allows their recovery, while restricting the access to sensitive content.</td>
</tr>
<tr>
<td>File Sync &amp; Share</td>
<td>Administrator</td>
<td>This role enables configuring and managing File Sync &amp; Share for your users.</td>
</tr>
</tbody>
</table>
Read-only administrator role

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

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

A read-only administrator cannot:

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

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

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

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

Restore operator role

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

A restore operator can do the following:

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

A restore operator cannot do the following:

- Delete alerts.
- Add or delete Microsoft 365 or Google Workspace organizations.
- Add, delete, or rename backup locations.
- Delete or rename backups.
- Create, delete, or rename folders when recovering a backup to a custom location.
- Apply a backup plan or run a backup.
- Access backed-up files or the content of backed-up emails.
- Download backed-up files or email attachments.
- Send backed-up cloud resources, such as emails or calendar items, as email.
- View or recover Microsoft 365 Teams conversations.

Changing the notification settings for a user

To change the notifications settings for a user, select the user on the Users tab, and then click the pencil icon in the Settings section. The following notifications settings are available if the Cyber Protection service is enabled for the tenant where the user is created:

- **Quota overuse notifications** (enabled by default)
  Notifications about exceeded quotas.
- **Scheduled usage reports** (enabled by default)
  Usage reports that are sent on the first day of each month.
- **Failure notifications, Warning notifications, and Success notifications** (disabled by default)
  Notifications about the execution results of protection plans and the results of disaster recovery operations for each device.
- **Daily recap about active alerts** (enabled by default)
  The daily recap is generated based on the list of active alerts that are present in the service console at the moment when the recap is generated. The recap is generated and sent once a day, between 10:00 and 23:59 UTC. The time when the report is generated and sent depends on the workload in the data center. If there are no active alerts at that time, the recap is not sent. The recap does not include information for past alerts that are no longer active. For example, if a user finds a failed backup and clears the alert, or the backup is retried and succeeds before the recap is generated, the alert will no longer be present and the recap will not include it.
- **Device control notifications** (disabled by default)
  Notifications about attempts to use peripheral devices and ports that are restricted by protection plans with the device control module enabled.
- **Recovery notifications** (disabled by default)
Notifications about recovery actions on the following resources: user email messages and entire mailbox, public folders, OneDrive / GoogleDrive: entire OneDrive and files or folders, SharePoint files, Teams: Channels, entire Team, email messages, and Team site.

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

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

- **Malware detection 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.

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

**Notifications received by user role**

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

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

* 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 \(\ldots\) > 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 \(\ldots\) > 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)
   - Microsoft Authenticator
     iOS app version (https://apps.apple.com/app/microsoft-authenticator/id983156458)

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

3. Your organization users must re-log in to the system.
4. After entering their login and password, they will be prompted to set up two-factor authentication for their user account.
5. They must scan the QR code by using their authentication application. If the QR code cannot be scanned, they can use the TOTP secret shown below the QR code and add it manually in the authentication application.

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

6. The one-time TOTP code will be generated in the authentication application. It is automatically regenerated every 30 seconds.

7. The users must enter the TOTP code on the “Set up two-factor authentication” screen after entering their password.

8. As a result, two-factor authentication for the users will be set up.

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

**Two-factor setup propagation across tenant levels**

Two-factor authentication is set up on the **organization** level. You can 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.
Units auto-inherit the two-factor authentication settings from their customer organization.

2FA setting propagation from a customer level

Enable 2FA

Customer admin

Customer

Unit 1

Unit admin

User

Unit 2

User

Unit 2.1

This is a beta version of the documentation. Some feature descriptions might be missing or incomplete.
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 the Users tab and check the 2FA status column. The 2FA status of users who have not yet configured two-factor authentication for their accounts is Setup Required.

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

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

As a result, two-factor authentication is disabled for your organization, all secrets are deleted, and all trusted browsers are forgotten. All users will log in to the system by using only their login and password. On the Users tab, the 2FA status column will be hidden.

Managing two-factor configuration for users

You can monitor two-factor authentication settings for all your users and reset the settings on the Users tab in the management portal.
Monitoring

In the management portal on the Users tab, you can see a list of all your organization users. The 2FA status reflects if the two-factor configuration is set up for a user.

To reset two-factor authentication for a user

1. In the management portal on the Users tab, find a user for whom you want to change the settings, and then click the ellipsis icon.
2. Click Reset two-factor authentication.
3. Enter the TOTP code generated in the authentication application on your second-factor device and click Reset.

As a result, the user will be able to set up two-factor authentication again.

To reset the trusted browsers for a user

1. In the management portal on the Users tab, find a user for whom you want to change the settings, and then click the ellipsis icon.
2. Click Reset all trusted browsers.
3. Enter the TOTP code generated in the authentication application on your second-factor device, and then click Reset.

The user for whom you have reset all trusted browsers will have to provide the TOTP code on the next login.

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

To disable two-factor authentication for a user

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

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

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

1. In the management portal on the Users tab, find a user for whom you want to change the settings, and then click the ellipsis icon.
2. Click Mark as service account. As a result, a user gets a special two-factor authentication status called Service account.
3. [If at least one user within a tenant has configured two-factor authentication] Enter the TOTP code generated in the authentication application on your second-factor device to confirm disabling.

To enable two-factor authentication for a user
You may need to enable two-factor authentication for a particular user for whom you have disabled it previously.

1. In the management portal on the Users tab, find a user for whom you want to change the settings, and then click the ellipsis icon.
2. Click Mark as regular account. As a result, a user will have to set up two-factor authentication or provide the TOTP code when entering the system.

Resetting two-factor authentication in case of lost second-factor device
To reset access to your account in case of lost second-factor device, follow one of the suggested approaches:

- Restore your TOTP secret (QR-code or alphanumeric code) from a backup.
  Use another second-factor device and add the saved TOTP secret in the authentication application installed on this device.
- Ask your administrator to reset the two-factor authentication settings for you.

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

The brute-force protection mechanism of the platform is based on device cookies.

The settings for brute-force protection that are used in the platform are pre-defined:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Entering the password</th>
<th>Entering the TOTP code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attempt limit</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>Attempt limit period (the limit is reset after timeout)</td>
<td>15 min (900 sec)</td>
<td>15 min (900 sec)</td>
</tr>
<tr>
<td>Lockout happens on</td>
<td>Attempt limit + 1 (11th attempt)</td>
<td>Attempt limit</td>
</tr>
<tr>
<td>Lockout period</td>
<td>5 min (300 sec)</td>
<td>5 min (300 sec)</td>
</tr>
</tbody>
</table>

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

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

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

### 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:

<table>
<thead>
<tr>
<th>Type of users in customer tenant</th>
<th>Action item</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator; buyer</td>
<td>The <strong>Buy now</strong> button is shown in the user interface.*</td>
</tr>
<tr>
<td>Administrator; not buyer</td>
<td>The message “Contact your partner to upgrade the edition” is shown in the user interface.</td>
</tr>
</tbody>
</table>
The message "Contact your partner to upgrade the edition" is shown in the user interface.

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 left pane, and then switch to 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

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.

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.

**To enable immutable storage for your tenant**

1. Log in to the management portal as an administrator, and then go to **Settings > Security**.
2. Enable the **Immutable storage** switch.
3. Set the desired retention period.
   - You can set the retention period within the range of 1 to 999 days. A longer retention period may result in increased storage usage.

**To disable immutable storage for your tenant**

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

---

**Warning!**

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

**To enable immutable storage for a child tenant**

1. Log in to the management portal as an administrator, and then go to **Clients**.
2. Click the name of the desired child tenant.
   - Now you configure the settings for this particular tenant.
3. In the navigation menu, go to **Settings > Security**.
4. Enable the **Immutable storage** switch.
5. Set the desired retention period.
   - You can set the retention period within the range of 1 to 999 days. A longer retention period may result in increased storage usage.

**To disable immutable storage for a child tenant**
1. Log in to the management portal as an administrator, and then go to **Clients**.
2. Click the name of the desired child tenant.
   Now you configure the settings for this particular tenant.
3. In the navigation menu, go to **Settings > Security**.
4. Disable the **Immutable storage** switch.

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

**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 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.

- **Logo.** The logo is displayed in the management portal and the services. Click the logo to upload an image file.

- **Color scheme.** The color scheme defines the combination of colors that is used for all user interface elements. Click the scheme, and then choose one of the predefined schemes that best fits your needs.
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.
- **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 top-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 top-right corner of the management portal user interface, and then clicks Help.

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 or on the Welcome screen after the first login.
- **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.
Important
If you do not want a document to appear on the Welcome screen, do not enter a URL for that document.

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.

Monitoring

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

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.
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.

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

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](image)

### Discovered machines

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

<table>
<thead>
<tr>
<th>Device name</th>
<th>IP address</th>
<th>OS</th>
<th>Organizational unit</th>
<th>Discovery type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2012 R2</td>
<td>10.248.90.221</td>
<td>Windows Server 2012 R2</td>
<td>-</td>
<td>Local Network</td>
</tr>
<tr>
<td>Windows 10 Enterprise 2016 LTSC</td>
<td>10.248.90.238</td>
<td>Windows 10 Enterprise 2016 LTSC</td>
<td>OU1</td>
<td>Active Directory, Local Network</td>
</tr>
<tr>
<td>device1</td>
<td>10.248.91.243</td>
<td>Windows 10 Enterprise 2016 LTSC</td>
<td>OU1</td>
<td>Active Directory, Manual, Loc...</td>
</tr>
<tr>
<td>device2</td>
<td>10.248.91.125</td>
<td>Windows 10 Enterprise 2016 LTSC</td>
<td>-</td>
<td>Active Directory, Local Network</td>
</tr>
<tr>
<td>device3</td>
<td>10.248.44.199</td>
<td>Windows 10 Enterprise 2016 LTSC</td>
<td>-</td>
<td>Active Directory, Manual</td>
</tr>
<tr>
<td>device4</td>
<td>10.250.41.189</td>
<td>-</td>
<td>-</td>
<td>Manual</td>
</tr>
<tr>
<td>device5</td>
<td>10.248.44.199</td>
<td>-</td>
<td>-</td>
<td>Manual</td>
</tr>
</tbody>
</table>

### #CyberFit Score by machine

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

• Antimalware
• Backup
• Firewall
• VPN
• Encryption
• NTLM traffic

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

For more details about the #CyberFit Score, refer to "#CyberFit Score for machines".

![#CyberFit Score by machine](image)

**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
• Security 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.
Security 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.

![Security incident burndown graph]

**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).

![Workload network status]

**Disk health monitoring**

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

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

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

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

How it works

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

1. The protection agent collects the SMART parameters of the disks and passes this data to the Disk Health Prediction Service:
   - SMART 5 – Reallocated sectors count.
   - SMART 9 – Power-on hours.
   - SMART 187 – Reported uncorrectable errors.
   - SMART 188 – Command timeout.
   - SMART 197 – Current pending sector count.
   - SMART 198 – Offline uncorrectable sector count.
   - SMART 200 – Write error rate.

2. The Disk Health Prediction Service processes the received SMART parameters, makes forecasts, and then provides the following disk health characteristics:
   - Disk health current state: OK, warning, critical.
   - Disk health forecast: negative, stable, positive.
   - Disk health forecast probability in percentage.
   The prediction period is one month.

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

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

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

Disk health overview

Resources

**HV12-long**
Total size: 2.27 TB
Warning: 1/3 disks
Disk level
Shows the current disk health status of all disks for the selected machine. Each disk block shows one of the following disk health forecasts and its probability in percentage:
- Will be degraded
- Will stay stable
- Will be improved

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

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

<table>
<thead>
<tr>
<th>Alert name</th>
<th>Severity</th>
<th>Disk health status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk failure is possible</td>
<td>Warning</td>
<td>(30 – 70)</td>
<td>The (&lt;\text{disk name})&gt; disk on this machine is likely to fail in the future. Run a full image backup of this disk as soon as possible, replace it, and then recover the image to the new disk.</td>
</tr>
<tr>
<td>Disk failure is imminent</td>
<td>Critical</td>
<td>(0 – 30)</td>
<td>The (&lt;\text{disk name})&gt; disk on this machine is in a critical state and will most likely fail very soon. An image backup of this disk is not recommended at this point as the added stress can cause the disk to fail. Back up the most important files on this disk immediately and replace it.</td>
</tr>
</tbody>
</table>

Data protection map

The data protection map feature allows you to 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.

• Machine level – shows information about the protection status of important files per machines of the selected customer.
To protect files that are not protected, hover over the block and click **Protect all files**. In the dialog window, you can find information about the number of unprotected files and their location. To protect them, click **Protect all files**.

You can also download a detailed report in CSV format.

**Vulnerability assessment widgets**

**Vulnerable machines**

This widget shows the vulnerable machines by the vulnerability severity.

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

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

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

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

### 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.

<table>
<thead>
<tr>
<th>Installation status</th>
<th>Total number of machines</th>
<th>Total number of updates</th>
<th>Microsoft updates</th>
<th>Application updates</th>
<th>Critical severity</th>
<th>High severity</th>
<th>Medium severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>8</td>
</tr>
</tbody>
</table>

Patch installation history

This widget shows the detailed information about patches on machines.

Missing updates by categories

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

- Security updates
- Critical updates
- Other
Backup scanning details

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

Recently affected

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

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

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

1. In the **Recently affected** widget, click **Download data**.
2. In the **Time period** field, enter the number of days for which you want to download data. The maximum number of days that you can enter is 200.
3. In the **Recipients** field, enter the email addresses of all the people who will receive an email with a link for downloading the CSV file.
4. Click **Download**.
   
   The system starts generating the CSV file with the data for the workloads that were affected in the time period that you specified. When the CSV file is complete, the system sends an email to the recipients. Each recipient can then download the CSV file.

**Blocked URLs**

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

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

<table>
<thead>
<tr>
<th>Folder</th>
<th>Name</th>
<th>Machine name</th>
<th>Package name</th>
<th>Software version</th>
<th>Vendor name</th>
<th>Status</th>
<th>Date installed</th>
<th>Last run</th>
<th>Scan time</th>
<th>Location</th>
<th>User</th>
<th>System</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>folder1</td>
<td>mark1</td>
<td>ACP-0429-1X01</td>
<td>Microsoft Visual C++ 6.0 SP2 (X64)</td>
<td>Microsoft Corporation</td>
<td>New</td>
<td>-</td>
<td>11/03/2023</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>folder2</td>
<td>mark2</td>
<td>ACP-0429-2X01</td>
<td>CyberGhost V 3.2.10</td>
<td>-</td>
<td>New</td>
<td>-</td>
<td>11/03/2023</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>folder3</td>
<td>mark3</td>
<td>ACP-0429-3X01</td>
<td>WonderCam</td>
<td>-</td>
<td>Malicious</td>
<td>-</td>
<td>11/03/2023</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

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).
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. 102).

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.
The default reports are listed below:

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

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.
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 top-right corner, and then click **Export**.

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

**Downloading a report**

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

- Excel and PDF
- Excel
- PDF

**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 top-right corner, and then click **Dump data**.
3. Specify the recipients' email addresses.
4. In **Time range**, specify the time range.
5. Click **Send**.

**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.

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cloud workloads protection status</strong></td>
<td>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):</td>
</tr>
<tr>
<td>Google Workspace Drive</td>
<td></td>
</tr>
<tr>
<td>Google Workspace Gmail</td>
<td></td>
</tr>
<tr>
<td>Google Workspace Shared Drive</td>
<td></td>
</tr>
<tr>
<td>Hosted Exchange mailboxes</td>
<td></td>
</tr>
<tr>
<td>Microsoft 365 mailboxes</td>
<td></td>
</tr>
<tr>
<td>Microsoft 365 OneDrive</td>
<td></td>
</tr>
<tr>
<td>Microsoft 365 SharePoint Online</td>
<td></td>
</tr>
<tr>
<td>Microsoft Teams</td>
<td></td>
</tr>
<tr>
<td>Websites</td>
<td></td>
</tr>
<tr>
<td>For some workload types, the following workload groups are used:</td>
<td></td>
</tr>
<tr>
<td>Microsoft 365: Users, Groups, Public Folders, Teams, and Site Collections</td>
<td></td>
</tr>
<tr>
<td>Widget</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
|                               | • 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

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Workstations</strong> - physical workstations.</td>
<td><strong>Virtual machines</strong> - both agent-based and agentless virtual machines.</td>
</tr>
<tr>
<td><strong>Web hosting servers</strong> - virtual or physical server with installed cPanel or Plesk.</td>
<td><strong>Mobile devices</strong> - physical mobile devices.</td>
</tr>
<tr>
<td>One workload can belong to more than one category. For example, a web hosting server is counted in two categories - <strong>Servers</strong>, and <strong>Web hosting servers</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

### 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.
<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
</table>
| Antimalware scan of files      | The widget shows the results of on-demand antimalware scanning of the devices for the specified date range.  
**Files** - the total number of scanned files  
**Clean** - the total number of clean files  
**Detected, quarantined** - the total number of infected files that were quarantined  
**Detected, not quarantined** - the total number of infected files that were not quarantined  
**Devices protected** - The total number of devices with applied antimalware protection policy  
**Total number of registered devices** - The total number of registered devices at the time of the report’s generation                                                                                                                                                                                                                                                                                                                                                   |
| 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.                                                                                                                                                                                                                                                                                       |
| Security 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.                                                                                                                                                                                                                   |
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).

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.

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Workloads backed up</strong></td>
<td>The widget shows the total number of registered workloads by backup status.</td>
</tr>
<tr>
<td><strong>Backed up</strong></td>
<td>- number of workloads that were backed up (at least one successful backup was performed) during the report date range.</td>
</tr>
<tr>
<td><strong>Not backed up</strong></td>
<td>- number of workloads which were not backed up (no successful backup was performed) during the report date range.</td>
</tr>
<tr>
<td><strong>Disk health status by physical device</strong></td>
<td>The widget shows the aggregated health status of physical devices based on the health statuses of their disks.</td>
</tr>
<tr>
<td><strong>OK</strong></td>
<td>- This disk health status relates to values [70-100]. The status of the device is OK when all its disks are in status OK.</td>
</tr>
<tr>
<td><strong>Warning</strong></td>
<td>- 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.</td>
</tr>
<tr>
<td><strong>Error</strong></td>
<td>- 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.</td>
</tr>
<tr>
<td><strong>Calculating disk data</strong></td>
<td>- The status of the device is Calculating disk data when the statuses of its disks are not calculated yet.</td>
</tr>
<tr>
<td><strong>Backup</strong></td>
<td>For the specified time range, the widget shows the total number and total</td>
</tr>
</tbody>
</table>
Vulnerability assessment and patch management widgets

The following table provides more information about the widgets in the **Vulnerability assessment and patch management** section.

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

Disaster Recovery widgets

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

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Disaster Recovery statistics</strong></td>
<td>The widget shows Disaster Recovery key performance metrics for the specified date range.</td>
</tr>
<tr>
<td><strong>Production failovers</strong></td>
<td>the number of production failover operations for the specified time range.</td>
</tr>
<tr>
<td><strong>Test failovers</strong></td>
<td>the total number of test failover operations that were</td>
</tr>
</tbody>
</table>
### Widget

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>performed during the specified time range.</td>
</tr>
</tbody>
</table>

**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 least 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.

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

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

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

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. 98).

To send an Executive summary report

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

Time zones in reports

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

<table>
<thead>
<tr>
<th>Report location and type</th>
<th>Time zone used in the report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management portal&gt; Overview &gt; Operations (widgets)</td>
<td>The time of report generation is in the time zone of the machine where the browser is running.</td>
</tr>
</tbody>
</table>
| Management portal> Overview > Operations (exported to PDF or xslx) | • The time stamp of the exported report is in the time zone of the machine that was used to export the report.  
• The time zone of the activities displayed in the report is UTC. |
| Management portal> Reports > Usage > Scheduled reports | • The report is generated at 23:59:59 UTC on the first day of the month.  
• The report is sent on the second day of the month. |
| Management portal> Reports > Usage > Custom reports | The time zone and date of the report is UTC. |
| Management portal> Reports > Operations (widgets) | • The time of report generation is in the time zone of the machine where the browser is running.  
• The time zone of the activities displayed in the report is UTC. |
| Management portal> Reports > Operations | • The time stamp of the exported report is in the time zone of the machine that was used to export the report. |
Reported data according to widget type

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

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

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

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

<table>
<thead>
<tr>
<th>Widget name</th>
<th>Data displayed in widget and reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>#CyberFit Score by machine</td>
<td>Actual</td>
</tr>
<tr>
<td>5 latest alerts</td>
<td>Actual</td>
</tr>
<tr>
<td>Active alerts details</td>
<td>Actual</td>
</tr>
<tr>
<td>Active alerts summary</td>
<td>Actual</td>
</tr>
<tr>
<td>Activities</td>
<td>Historical</td>
</tr>
<tr>
<td>Activity list</td>
<td>Historical</td>
</tr>
<tr>
<td>Alerts history</td>
<td>Historical</td>
</tr>
<tr>
<td>Antimalware scan of backups</td>
<td>Historical</td>
</tr>
<tr>
<td>Antimalware scan of files</td>
<td>Historical</td>
</tr>
<tr>
<td>Feature</td>
<td>Data Type</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Backup scanning details (threats)</td>
<td>Historical</td>
</tr>
<tr>
<td>Backup status</td>
<td>Historical - in columns <strong>Total runs</strong> and <strong>Number of successful runs</strong>&lt;br&gt;Actual - in all other columns</td>
</tr>
<tr>
<td>Backup storage usage</td>
<td>Historical</td>
</tr>
<tr>
<td>Blocked peripheral devices</td>
<td>Historical</td>
</tr>
<tr>
<td>Blocked URLs</td>
<td>Actual</td>
</tr>
<tr>
<td>Cloud applications</td>
<td>Actual</td>
</tr>
<tr>
<td>Cloud workloads protection status</td>
<td>Actual</td>
</tr>
<tr>
<td>Cyber protection</td>
<td>Actual</td>
</tr>
<tr>
<td>Cyber protection summary</td>
<td>Historical</td>
</tr>
<tr>
<td>Data protection map</td>
<td>Historical</td>
</tr>
<tr>
<td>Devices</td>
<td>Actual</td>
</tr>
<tr>
<td>Disaster recovery servers tested</td>
<td>Historical</td>
</tr>
<tr>
<td>Disaster recovery statistics</td>
<td>Historical</td>
</tr>
<tr>
<td>Discovered machines</td>
<td>Actual</td>
</tr>
<tr>
<td>Disk health overview</td>
<td>Actual</td>
</tr>
<tr>
<td>Disk health status</td>
<td>Actual</td>
</tr>
<tr>
<td>Disk health status by physical devices</td>
<td>Actual</td>
</tr>
<tr>
<td>eSigned documents across end users</td>
<td>Actual</td>
</tr>
<tr>
<td>Existing vulnerabilities</td>
<td>Historical</td>
</tr>
<tr>
<td>File Sync &amp; Share statistics</td>
<td>Actual</td>
</tr>
<tr>
<td>File Sync &amp; Share storage usage by end users</td>
<td>Actual</td>
</tr>
<tr>
<td>Hardware changes</td>
<td>Historical</td>
</tr>
<tr>
<td>Hardware details</td>
<td>Actual</td>
</tr>
<tr>
<td>Hardware inventory</td>
<td>Actual</td>
</tr>
<tr>
<td>Historical alerts summary</td>
<td>Historical</td>
</tr>
<tr>
<td>Locations summary</td>
<td>Actual</td>
</tr>
</tbody>
</table>
### Audit log

To view the audit log, click **Audit log**.

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

<table>
<thead>
<tr>
<th>Category</th>
<th>View Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missing updates by categories</td>
<td>Actual</td>
</tr>
<tr>
<td>Not protected</td>
<td>Actual</td>
</tr>
<tr>
<td>Notarized files across end users</td>
<td>Actual</td>
</tr>
<tr>
<td>Notary statistics</td>
<td>Actual</td>
</tr>
<tr>
<td>Patch installation history</td>
<td>Historical</td>
</tr>
<tr>
<td>Patch installation status</td>
<td>Historical</td>
</tr>
<tr>
<td>Patch installation summary</td>
<td>Historical</td>
</tr>
<tr>
<td>Patched vulnerabilities</td>
<td>Historical</td>
</tr>
<tr>
<td>Patches installed</td>
<td>Historical</td>
</tr>
<tr>
<td>Protection status</td>
<td>Actual</td>
</tr>
<tr>
<td>Recently affected</td>
<td>Historical</td>
</tr>
<tr>
<td>Security incident burndown</td>
<td>Historical</td>
</tr>
<tr>
<td>Security incident MTTR</td>
<td>Historical</td>
</tr>
<tr>
<td>Servers protected with disaster recovery</td>
<td>Actual</td>
</tr>
<tr>
<td>Software inventory</td>
<td>Actual</td>
</tr>
<tr>
<td>Software overview</td>
<td>Historical</td>
</tr>
<tr>
<td>Threat status</td>
<td>Actual</td>
</tr>
<tr>
<td>Threats detected by protection technology</td>
<td>Historical</td>
</tr>
<tr>
<td>Top incident distribution per workload</td>
<td>Actual</td>
</tr>
<tr>
<td>Vulnerable machines</td>
<td>Actual</td>
</tr>
<tr>
<td>Workload network status</td>
<td>Actual</td>
</tr>
<tr>
<td>Workloads backed up</td>
<td>Historical</td>
</tr>
<tr>
<td>Workloads protection status</td>
<td>Actual</td>
</tr>
</tbody>
</table>
• 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
• 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.

• **Severity**
  Can be one of the following:
  o **Error**
    Indicates an error.
  o **Warning**
    Indicates a potentially negative action. For example, Tenant was deleted, User was deleted, Quota was reached.
  o **Notice**
    Indicates an event that might need attention. For example, Tenant was updated, User was updated.
  o **Informational**
    Indicates a neutral informative change or action. For example, Tenant was created, User was created, Quota was updated.

• **Date**
  The date and time when the event occurred.

• **Object name**
  The object with which the operation was performed. For example, the object of the User was updated event is the user whose properties were changed. For events related to a quota, the quota is the object.

• **Tenant**
  The name of the 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 API.

• IP
  The IP address of the machine from which the event was initiated.

Filtering and search
You can filter the events by description, severity, or date. You can also search the events by object, unit, initiator, and initiator's unit.
Advanced 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 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

<table>
<thead>
<tr>
<th>Feature group</th>
<th>Included standard features</th>
<th>Advanced features</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security</strong></td>
<td>• #Cyber fit score</td>
<td>The Advanced Security pack includes:</td>
</tr>
<tr>
<td></td>
<td>• Vulnerability assessment</td>
<td>• Antivirus and antimalware protection with local signature-based detection (with real-time protection)</td>
</tr>
<tr>
<td></td>
<td>• Anti-ransomware protection: Active protection</td>
<td>• Exploit prevention</td>
</tr>
<tr>
<td></td>
<td>• Antivirus and Antimalware protection: Cloud signature-based file detection (no real-time protection, only scheduled scanning)*</td>
<td>• URL filtering</td>
</tr>
<tr>
<td></td>
<td>• Antivirus and Antimalware protection: Pre-execution AI-based file analyzer, behavior-based Cyber Engine</td>
<td>• Forensic backup, scan backups for malware, safe recovery, corporate allowlist</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Defender management</td>
<td>• Smart protection plans (integration with CPOC alerts)</td>
</tr>
<tr>
<td></td>
<td>*To detect zero day attacks, Cyber Protect uses heuristic scanning rules and algorithms to look for malicious commands.</td>
<td>• Centralized backup scanning for malware</td>
</tr>
<tr>
<td><strong>Data Loss Prevention</strong></td>
<td>• Device control</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Management</strong></td>
<td>• Group management of workloads</td>
<td>• Patch management</td>
</tr>
<tr>
<td></td>
<td>• Centralized management of protection plans</td>
<td>• HDD health</td>
</tr>
<tr>
<td></td>
<td>• Remote desktop</td>
<td>• Software inventory</td>
</tr>
<tr>
<td></td>
<td>• Remote assistance</td>
<td>• File safe inventory</td>
</tr>
<tr>
<td></td>
<td>• Hardware inventory</td>
<td></td>
</tr>
<tr>
<td><strong>Email security</strong></td>
<td>• Antispam Protection</td>
<td>Real-time protection for your Microsoft 365 and Gmail mailboxes:</td>
</tr>
<tr>
<td></td>
<td>• URL filtering</td>
<td>• Antimalware Antispam</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• URL scan in emails</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DMARC analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Anti-phishing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Impersonation protection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Attachments scan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Content disarm and reconstruction</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Graph of trust</td>
</tr>
</tbody>
</table>
Feature group | Included standard features | Advanced features
--- | --- | ---
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: 5.
  - 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

<table>
<thead>
<tr>
<th>Feature group</th>
<th>Pay-as-you-go features</th>
<th>Advanced features</th>
</tr>
</thead>
</table>
| Backup | • File backup  
  • Image backup  
  • Applications backup  
  • Network shares backup  
  • Backup to cloud storage  
  • Backup to local storage | • Microsoft SQL server and Microsoft Exchange clusters  
  • Oracle DB  
  • SAP HANA  
  • Data Protection Map  
  • Continuous Data Protection |
### Feature group

<table>
<thead>
<tr>
<th>Pay-as-you-go features</th>
<th>Advanced features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note Fees for cloud storage usage are applicable.</td>
<td>• Off-host data processing plans</td>
</tr>
</tbody>
</table>

**File Sync & Share**
- Store encrypted file-based content
- Synchronize files across designated devices
- Share folders and files with designated people and systems

**Advanced features**
- Notarization and e-signature
- Document templates*

*Backup of sync and share files

**Physical Data Shipping**
- Physical Data Shipping functionality

**Notary**
- File notarization
- File eSigning
- Document templates

**Advanced Data Loss Prevention**

**Important**
This is an Early Access version of the Advanced Data Loss Prevention documentation. Some of the features and descriptions may be incomplete.

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

Important
This is an Early Access version of the Advanced Data Loss Prevention documentation. Some of the features and descriptions may be incomplete.

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 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 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: 5.
• 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 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 extension for Cyber Cloud

1. Log in to the management portal.
2. Click *Settings > Integration*.
3. Click the name of the third-party system with which you want to enable the integration.
4. Follow the on-screen instructions.

More information about integration with third-party systems is available in the "Integration references" section at https://www.acronis.com/en-us/support/documentation/.

Managing API clients

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

What is an API client?

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

The client’s access is limited to a tenant, where an administrator creates the client, and its sub-tenants.
When being created, the client inherits the service roles of the administrator account and these roles cannot be changed later. Changing roles of the administrator account or disabling it does not affect the client.

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

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

**Typical integration procedure**

1. An administrator creates an API client in a tenant that a third-party system will manage.
2. The administrator enables the OAuth 2.0 client credentials flow in the third-party system.
   
   According to this flow, before accessing the tenant and its services via the API, the system should first send the credentials of the created client to the platform by using the authorization API. The platform generates and sends back a security token, the unique cryptic string assigned to this specific client. Then, the system must add this token to all API requests.

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


**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 with VMware Cloud Director**

A service provider can integrate VMware Cloud Director (formerly VMware vCloud Director) with Cyber 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 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 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 Cloud.

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

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.
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**.

![RabbitMQ Management Console](image)

### 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](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 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:

   a. URL of the Cyber 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. 57).
      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 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 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.

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.

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:
a. URL of the Cyber 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 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 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 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. 124).

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 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. 118).

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
   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 Cloud is a complex procedure. Please contact your support representative for help.
Index

# CyberFit Score by machine 67

7
7-day history bar 29

A
About Cyber Protect 6
About this document 5
Accessing the Cyber Protection web console 123
Accessing the management portal 25
Accessing the services 27
Actions in the Device list 56
Activating the administrator account 25
Adding a report 87
Adding new storages 58
Advanced Data Loss Prevention 110
Advanced Disaster Recovery 111
Advanced Email Security 112
Advanced Protection packs 107
Agent and installer branding 62
Agent installer dependency on offering items 18
Antimalware protection widgets 92
Appearance 61
Applying white labeling 64
Audit log 104
Audit log fields 105

Autodiscovery wizard 56

B
Backup 124
Backup quota transformation 14
Backup quotas 12
Backup scanning details 79
Backup widgets 94
Billing for Notary 8
Billing for Physical Data Shipping 8
Billing modes and editions 10
Billing modes for Cyber Protect 7
Billing modes for File Sync & Share 8
Billing modes for the Protection component 7
Blocked URLs 80
Branding items 61
Brute-force protection 54

C
Changing editions for a partner tenant 21
Changing the edition for a customer tenant 21
Changing the notification settings for a user 46
Changing the service quota of machines 16
Choosing locations and storages for partners and customers 57
Clients tab 28
Comparison of editions 20
Configuring branding 63
Configuring branding and white labeling 60
Configuring company contacts 37
Configuring custom usage reports 84
Configuring immutable storage 59
Configuring RabbitMQ message broker 117
Configuring scheduled usage reports 84
Configuring the offering items for a tenant 36
Configuring the settings of the Executive summary report 98
Configuring upsell scenarios for your customers 55
Converting a partner tenant to a folder tenant and vice versa 40
Creating a backup administrator 124
Creating a tenant 32
Creating a user account 42
Creating an API client 114
Creating an Executive summary report 99
Creating or editing a protection plan 56
Customizing the Executive summary report 99
Cyber Backup edition 20
Cyber Protect edition 19
Cyber Protect services 6
Cyber Protection service editions and sub-editions 19
Disabling and enabling a tenant 39
Disabling and enabling a user account 47
Disabling the branding 64
Disaster Recovery add-on 20
Disaster Recovery quotas 14
Disaster Recovery widgets 95
Discovered machines 67
Disk health monitoring 70
Disk health status alerts 74
Disk health widgets 72
Documentation and support 62
Downloading a report 89
Downloading data for recently affected workloads 80
Dumping the report data 89
Editing the report settings 87
Email server settings 63
Enabling a disabled API client 115
Enabling Advanced Data Loss Prevention 111
Enabling or disabling offering items 10
Endpoint Detection and Response (EDR) widgets 68
Enhanced security mode 34
Example
  Cyber Protect per workload edition to Per workload billing 24
  Switching Cyber Protect Advanced edition to Per workload billing 23
Exceeding the quota for backup storage 14
Executive summary 89

THIS IS A BETA VERSION OF THE DOCUMENTATION. SOME FEATURE DESCRIPTIONS MIGHT BE MISSING OR INCOMPLETE.
Executive summary widgets 90
Existing vulnerabilities 77
Exporting and importing the report structure 89

F
File Sync & Share quotas 15
File Sync & Share widgets 97
Filtering and search 106

H
Hardware inventory widgets 82
How it works 49, 71
How to move a tenant 40

I
Included and advanced features in the Protection service 108
Included features and advanced packs in Cyber Protect services 107
Installing a management agent 119
Installing backup agents 121
Installing the plug-in for VMware Cloud Director 118
Integration with third-party systems 113
Integration with VMware Cloud Director 116
Integrations 113

L
Legal documents settings 62
Levels on which quotas can be defined 11
Limitations 35, 71, 117, 124
Limiting the access to the web interface 26
Limiting the access to your tenant 41
Locations 57

M
Managing API clients 113
Managing locations and storage 57
Managing storage 58
Managing tenants 32
Managing two-factor configuration for users 52
Managing users 42
Metrics with zero usage 84
Missing updates by categories 78
Mixing offering items from different sub-editions 20
Mobile apps 63
Monitoring 53, 64
Moving a tenant to another tenant 39

N
Navigation in the management portal 26
Notary quotas 16
Notary widgets 98
Notifications received by user role 47

O
Offering items 9
Offering items and quota management 9
Operations 65
Operations reports 85
Operations with locations 57
Overview tab 27
P
Patch installation history 78
Patch installation status 77
Patch installation summary 78
Patch installation widgets 77
Pay as you go and advanced features in the Protection service 109
Physical Data Shipping quotas 16
Protection status 66

Q
Quotas for cloud data sources 12
Quotas for storage 13

R
Recently affected 79
Recovery 124
Refreshing the usage data for a tenant 39
Removing the integration with VMware Cloud Director 126
Report scope 84
Report type 83
 Reported data according to widget type 102
Reporting 83
Resetting the secret value of an API client 114
Resetting two-factor authentication in case of lost second-factor device 54
Restoring the default branding settings 63
Restrictions 40

S
Scheduling a report 88
Security incident burndown 69
Security incident MTTR 69
Selecting the services for a tenant 35
Sending Executive summary reports 101
Services 9
Services and offering items 9
Setting up an extension for Cyber Cloud 113
Setting up two-factor authentication 49
Setting up two-factor authentication for your tenant 52
Soft and hard quotas 11
Software inventory widgets 81
Software requirements 117
Supported VMware Cloud Director versions 117
Supported web browsers 25, 117
Switching between editions and billing modes 22
Switching from legacy editions to the current licensing model 8
System report, log files, and configuration files 125

T
Time zones in reports 101
To disable two-factor authentication for a user 53
To disable two-factor authentication for your tenant 52
To enable two-factor authentication for a user 54
To enable two-factor authentication for your tenant 52
To reset the trusted browsers for a user 53
To reset two-factor authentication for a user 53

Top incident distribution per workload 68

Transferring ownership of a user account 48

Two-factor setup propagation across tenant levels 50

Typical integration procedure 114

U

Updating the agents 122

Upsell 63

Upsell points shown to a customer 56

Usage 64, 83

User accounts and tenants 29

User roles available for each service 43

Using the billing modes with legacy editions 8

Using the management portal 25

V

Vulnerability assessment and patch management widgets 95

Vulnerability assessment widgets 76

Vulnerability list 56

Vulnerable machines 76

W

What is an API client? 113

White labeling 64

Workload network status 70

Workloads overview widgets 90