Management Portal

25.06

Partner Administrator Guide

REVISION: TUESDAY, JUNE 24, 2025

Table of contents

About this document

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

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

About Cyber Protect

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

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

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

The management portal enables administrators to:

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

Cyber Protect services

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

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

- **Cyber Protect**
  - **Protection** - complete cyber protection with security and management functionality included in the base product, and disaster recovery, back up and recovery, automation, and email security available as pay as you go features. This functionality can be extended with advanced protection packs that are subject to additional charges.
    Advanced protection packs are sets of unique features that address more sophisticated scenarios in a specific functional area, for example, Advanced Backup, Advanced Security + XDR, 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. 161).
  - **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. 8).

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 licenses 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. 11).

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

Switching between editions and billing modes

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

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

The switching process includes the following steps.

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

The following table illustrates the process in both directions.

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

Example: Switching Cyber Protect Advanced edition to Per workload billing

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

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

Source offering items - usage/quota	Destination offering items - usage/quota
	• Advanced Security + XDR - 2/10 • Advanced Backup workstation - 1/10 • Advanced Management (RMM) - 3/10

The following steps were executed during the switch:

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

Example: Cyber Protect per workload edition to Per workload billing

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

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

The following steps were executed during the switch:

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

Changing the billing mode for a partner tenant

To change the billing mode for a partner tenant

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

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

Changing the billing mode for a customer tenant

You can change the billing for a customer tenant by:

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

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

To switch the billing mode for a customer tenant

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

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

Offering items and quota management

This section describes the following:

- What are services and offering items?
- How are offering items enabled or disabled?
- What are billing modes?
- What are Advanced protection packs?
- What are legacy editions and sub-editions?
- What are the soft and hard quotas?
- When can the hard quota be exceeded?
- What is backup quota transformation?
- How does the offering item availability affect the workload type availability in the Cyber Protect 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. 8).

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. 80).

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. 9).

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. 16).

Enabling or disabling offering items

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

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

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

Offering item	Disabling	Result
Backup storage	Can be disabled when the usage is equal to zero.	The cloud storage will become unavailable as a destination for backups within a customer tenant.
Local backup	Can be disabled when the usage is equal to zero.	The local storage will become unavailable as a destination for backups within a customer tenant. Disabling the Local backup quota will disable backups to local disks, network shares, and public clouds, such as S3 compatible, Azure, AWS, Wasabi, and Impossible Cloud.
Data sources (including Microsoft 365 and Google Workspace)*	Can be disabled when the usage is equal to zero.	The protection of the disabled data sources (including Microsoft 365 and Google Workspace) will become unavailable within a customer tenant, as follows:
All Disaster Recovery offering items	Can be disabled when the usage is more than zero.	See the details in "Soft and hard quotas".
All Notary offering items	Can be disabled when the usage is equal to zero.	The Notary service will be unavailable within a customer tenant.
All File Sync & Share offering items	Offering items cannot be enabled or disabled separately.	The File Sync & Share service will be unavailable within a customer tenant.
All Physical	Can be	The Physical Data Shipping service will be unavailable within a customer

Data Shipping offering items	disabled when the usage is equal to zero.	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.

* The offering items relate to the workloads that you can add in the Cyber Protect console. For more information, refer to "Workload dependency on offering items" (p. 27). The table below summarizes which workload types will not be available if an offering item, a combination of offering items, or an advanced pack is not enabled in the Management portal.

If you disable these offering items or advanced packs	You will not be able to add these types of workloads
The following combination: • Microsoft 365 seats • Microsoft 365 SharePoint online • Microsoft 365 Teams	Microsoft 365 Business
The following combination: • Google Workspace • Google Workspace Shared Drive	Google Workspace
The following combination: • Servers • Virtual machines	• Microsoft SQL Server • Microsoft Exchange Server • Microsoft Active Directory
The following offering item: • NAS	Synology
The following offering item: • Mobile	• iOS devices • Android devices
The following advanced pack: • Advanced Backup	Oracle Database
The following combination: • Email archiving seats • Archiving storage	Mail server

Soft and hard quotas

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

When a quota is exceeded, a notification is sent to the user's email address. If you do not set a quota overage, the quota is considered "**soft.**" This means that restrictions on using the Cyber Protection service are not applied.

When you specify the quota overage, then the quota is considered "**hard.**" An **overage** allows the user to exceed the quota by the specified value. When the overage is exceeded, restrictions on using the service are applied.

Example

Soft quota: You have set the quota for workstations equal to 20. When the number of the customer's protected workstations reaches 20, the customer will get a notification by email, but the Cyber Protection service will be still available.

Hard quota: If you have set the quota for workstations equal to 20 and the overage is 5, then your customer will get the notification by email when the number of protected workstations reaches 20, and the Cyber Protection service will be disabled when the number reaches 25.

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

Levels on which quotas can be defined

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

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

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

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

Setting up soft and hard quotas

To set up quotas for your clients

1. In the management portal, go to **Clients**.
2. Select the client for which you want to setup quotas.
3. Select the **Protection** tab, and then click **Edit**.

4. Select the type of quota that you want to set. For example, select **Workstations** or **Servers**.
5. Click the **Unlimited** link on the right to open the **Quota edit** window.
   - If you want to inform the client about the quota and do not want to limit the client's ability to use the service, set the quota value in the **Soft quota** field.

     The client will receive an email notification upon reaching the quota, but the Cyber Protection service will be still available.
   - If you want to limit the client's ability to use the service, select **Hard quota** and set the quota value in the field below **Hard quota**.

     The client will receive an email notification upon reaching the quota, and the Cyber Protection service will be disabled.
6. In the **Quota edit** window, click **Done**, and then click **Save**.

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

Backup quotas

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

Quotas for devices

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

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

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

Quotas for cloud data sources

- **Microsoft 365 seats**

  This quota is applied by the service provider to the entire company. Company administrators can view the quota and its usage in the management portal. When the hard quota is exceeded, backup plans cannot be applied to new seats.

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

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

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

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

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

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

- Mailbox to which a backup plan is applied
- OneDrive to which a backup plan is applied
- Access to a protected company-level resource, such as Microsoft 365 SharePoint Online site or Microsoft 365 Teams.

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

A seat becomes unprotected in the following cases:

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

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

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

Note

Blocked Microsoft 365 users that do not have a protected personal mailbox or OneDrive, and can only access shared resources (shared mailboxes, SharePoint sites, and Microsoft Teams), are not charged. Blocked users are those who do not have a valid login and cannot access the Microsoft 365 services. To learn how to block all unlicensed users in a Microsoft 365 organization, see "Preventing unlicensed Microsoft 365 users from signing in" (p. 23).

Important

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

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

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

- **Microsoft 365 SharePoint Online**

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

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

- **Microsoft 365 Teams**

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

- **Microsoft 365 email archiving seats**

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

- **Email archiving seats (obsolete)**

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

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

Important

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

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

Google Workspace seats

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

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

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

- **Google Workspace Shared drive**

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

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

Quotas for storage

Important

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

- **Cloud resources**
  - **Backup storage**
    - **Backup storage**

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

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

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

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

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

    - **Archiving storage**

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

  - **Advanced Disaster Recovery**

    This section contains disaster recovery-related quotas.

- **Local resources**
  - **Local backup**

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

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

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

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.

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

Backup 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 Cyber Protect console.

Example

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

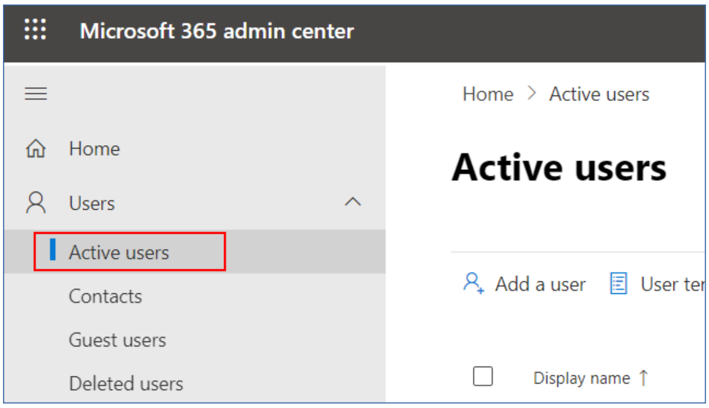
First, the system will check if there is an allocated **Virtual machines** quota. If it is not found, then the system automatically tries to acquire the **Workstations** quota. If that is also not found, the other quota will not be automatically acquired. If you have enough quota that is more expensive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

Preventing unlicensed Microsoft 365 users from signing in

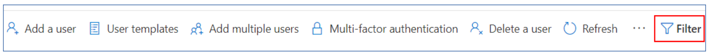
You can prevent all unlicensed users in your Microsoft 365 organization from signing in by editing their sign-in status.

To prevent unlicensed users from signing in

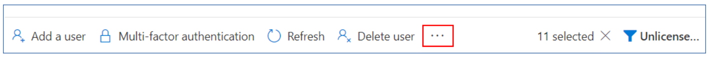
1. Log in to the Microsoft 365 admin center (https://admin.microsoft.com) as a global administrator.
2. In the navigation menu, go to **Users** > **Active Users**.



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



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



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

Disaster Recovery quotas

Note

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

These quotas are applied by the service provider to the entire company. Company administrators can view the quotas and the usage in the management portal, but cannot set quotas for a user.

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

- **DR and direct backup to Azure**

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

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

- **Disaster recovery storage**

  The Disaster recovery storage shows the backup storage size of the servers that are protected with disaster recovery. The usage of the Disaster recovery storage equals the usage of the backup storage of the workloads that are protected with disaster recovery servers. This storage is calculated starting from the time when a recovery server is created, regardless of whether the server is currently running. If the overage for this quota is reached, it will not be possible to create primary and recovery servers, or add/extend disks of the existing primary servers. If the overage for this quota is exceeded, it will not be possible to initiate a failover or start a stopped server. Running servers continue to run.
- **Compute points**

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

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

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

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

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

  When the quota is disabled, the servers are visible in the Cyber Protect console, but the only available operation is **Delete**.

- **Internet access**

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

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

File Sync & Share quotas

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

- **Users**

  This defines the limit to the number of File Sync & Share users.

  Note
  Only User and User + Administrator user roles count towards this quota.
  Administrator and Guest user roles are excluded from this quota.

- **Cloud storage**

  This defines the limit to the cloud storage allocated for the tenant.

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**

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

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

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

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

  Defines the maximum number of digital eSignatures.

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 Windows desktop 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 the protection agent of which 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 when 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 Protect 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 quota** window, select the service quota or **No quota**, and then click **Change**.

To change the service quota for a group of machines

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

Workload dependency on offering items

Depending on the enabled offering items, different workload types will be available in the **Add devices** pane in the Cyber Protect console. In the table below, you can see which workload types are available with different offering items.

Workload type (Agent installer)	**Enabled offering items**										
	Servers	**Workstations**	**Virtual machines**	**Microsoft 365 seats**	**Google Workspace seats**	**Mobile devices**	**Web hosting servers**	**Websites**	**NAS**	**Email archiving seats**	**Archiving storage**
Workstations – Agent for Windows		+	+					+			
Workstations – Agent for macOS		+	+					+			
Servers – Agent for Windows	+		+				+	+			
Servers – Agent for Linux	+		+				+	+			
Agent for Hyper-V			+								

Workload type (Agent installer)	Enabled offering items										
	Servers	Workstations	Virtual machines	Microsoft 365 seats	Google Workspace seats	Mobile devices	Web hosting servers	Websites	NAS	Email archiving seats	Archiving storage
Agent for VMware			+								
Agent for Virtuozzo			+								
Agent for SQL	+		+								
Agent for Exchange	+		+								
Agent for Active Directory	+		+								
Agent for Synology									+		
Microsoft 365 Business workloads				+							
Google Workspace workloads					+						
Mail server										+	+
Full installer for Windows	+	+	+				+	+			
Mobile (iOS and Android)						+					

Using the management portal

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

Supported web browsers

The web interface supports the following web browsers:

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

In other web browsers (including Safari browsers running in other operating systems), the user interface might be displayed incorrectly or some functions may be unavailable.

Activating the administrator account

After signing the partnership agreement, you will receive an email message containing the following information:

- **Your login.** This is the user name that you use to log in. Your login is also shown on the account activation page.
- **Activate account** button. Click the button and set the password for your account. Ensure that your password is at least nine characters long. For more information about the password, see "Password requirements" (p. 29).

Password requirements

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

- Weak
- Medium
- Strong

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

Note
Password requirements are subject to change.

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

Accessing the management portal

After you activate your administrator account, you can log in to Management Portal by using your login and the password that you set.

To access Management Portal for the first time

1. Go to the service login page.

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

   Note

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

   For more information about the onboarding survey, see "Onboarding survey" (p. 30).
5. Use the menu to the right to navigate the Management Portal.

The timeout period for Management Portal is 24 hours for active sessions and 1 hour for idle sessions.

Some services include the capability to switch to Management Portal from the service console.

Onboarding survey

The onboarding survey must be completed by the first partner administrator of the tenant upon their initial login to Management Portal. This survey adapts dynamically, based on the administrator’s responses regarding the priority area for protection, business model, and company size. By tailoring the onboarding experience to the business’s needs and interests, the process becomes more relevant and efficient.

The survey cannot be skipped or closed. All the questions are mandatory.

Configuring contacts in the Company profile wizard

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

You can configure contact information for your company in the wizard and modify them later, if needed. We will send updates on new features and other important changes in the platform to the contacts you provide.

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

Note
The following procedure is applicable only when you log in to Management Portal for the first time. To modify your company details or contacts later, go to **My Company** > **Company profile**.

To configure company contacts using the Company profile wizard

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

   You can use a contact for more than one purpose.

   Select an option to create the contact.
   - **Create from existing user**. Select a user from the drop-down list.
   - **Create a new contact**. Provide the following contact information:
     - **First name** — First name of the contact. This field is required.
     - **Last name** — Last name of the contact. This field is required.
     - **Business email** — Email address of the contact. This field is required.
     - **Business phone** — This field is optional.
     - **Job title** — This field is optional.
4. If you plan to use the Billing contact as a business or technical contact as well, select the corresponding flags in the **Billing contact** section:
   - **Use the same contact for Business contact**
   - **Use the same contact for Technical contact**
5. Click **Done**.

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

Accessing the Cyber Protect console from the management portal

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

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

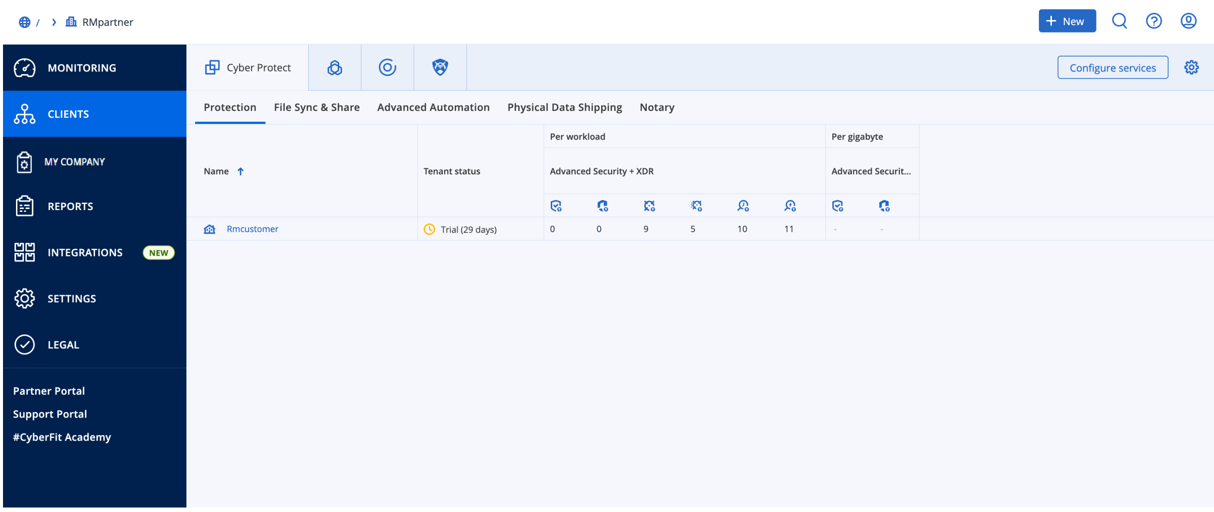
As a result, you are redirected to the Cyber Protect console.

Important
If the customer is in **Self-service** management mode, you cannot manage services for him. Only the customer administrators can change the customer mode to **Managed by service provider**, and then manage the services.

Navigation in the management portal

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

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



Name ↑	Tenant status	Per workload						Per gigabyte	
		Advanced Security + XDR						Advanced Securit...	
Rmcustomer	Trial (29 days)	0	0	9	5	10	11	-	-

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 child objects of the tenant in which you are currently operating.

- The **My Company** tab displays the company profile and the user accounts that exist in the tenant in which you are currently operating.
- The **Monitoring** tab displays information about the usage and operations of the direct child objects of the tenant in which you are currently operating.

> **Note**
> You may have additional options in this tab, depending on the services you are subscribed to.

- 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.

> **Note**
> You may have additional options in this menu, depending on the services you are subscribed to. For example, if you have activated Advanced Automation (PSA), you will also be able to create new tickets and time registrations

My Inbox

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

Overview

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

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

Checking your notifications

Checking your notification section

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

Searching My Inbox

To search for unread messages

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

To search for important information in your inbox

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

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

What's new in the Management portal

When new features of Cyber Protect Cloud are released, you see a pop-up window with a brief description of these features upon logging in to the Management portal.

You can also view the description of the new features by clicking the **What's new** link in the bottom-left corner of the main Management portal window.

Limiting access to the web interface

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

Important
Enabling login control prevents recovery from cloud storage by using unregistered bootable media. See this KB article.

Note

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

To limit access to the web interface

1. Log in to Management Portal.
2. Navigate to the 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

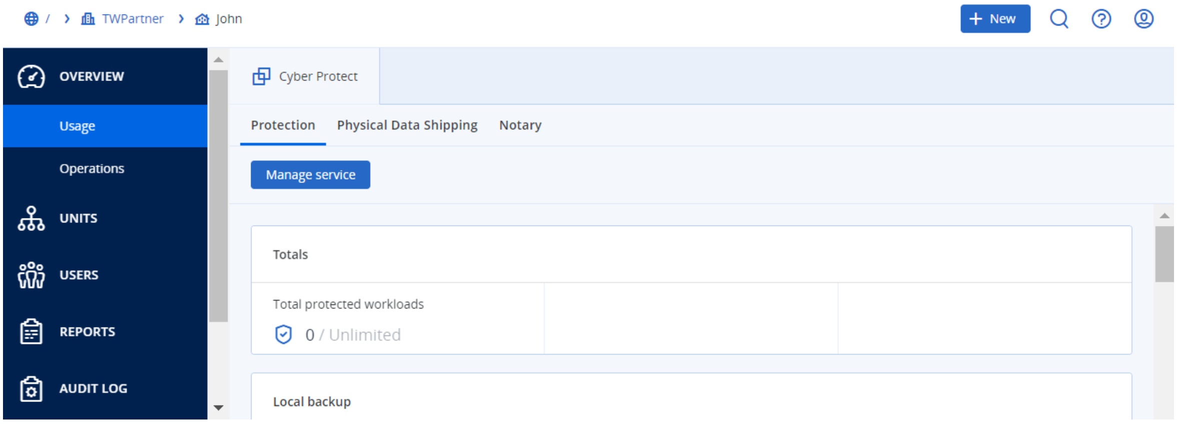
The **Overview** > **Usage** section provides an overview of the service usage and enables you to access the services within the tenant in which you are operating.

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.



Totals

Total protected workloads

0 / Unlimited

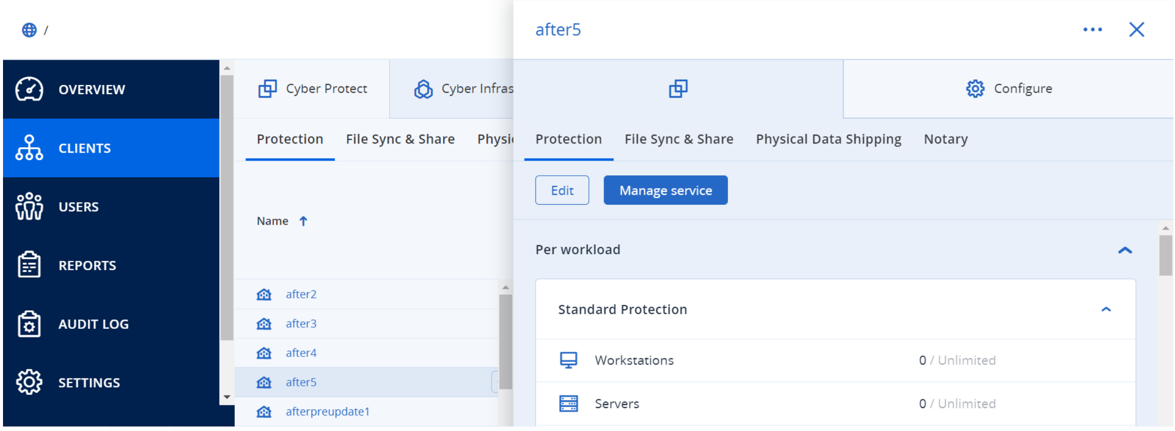
Local backup

Clients tab

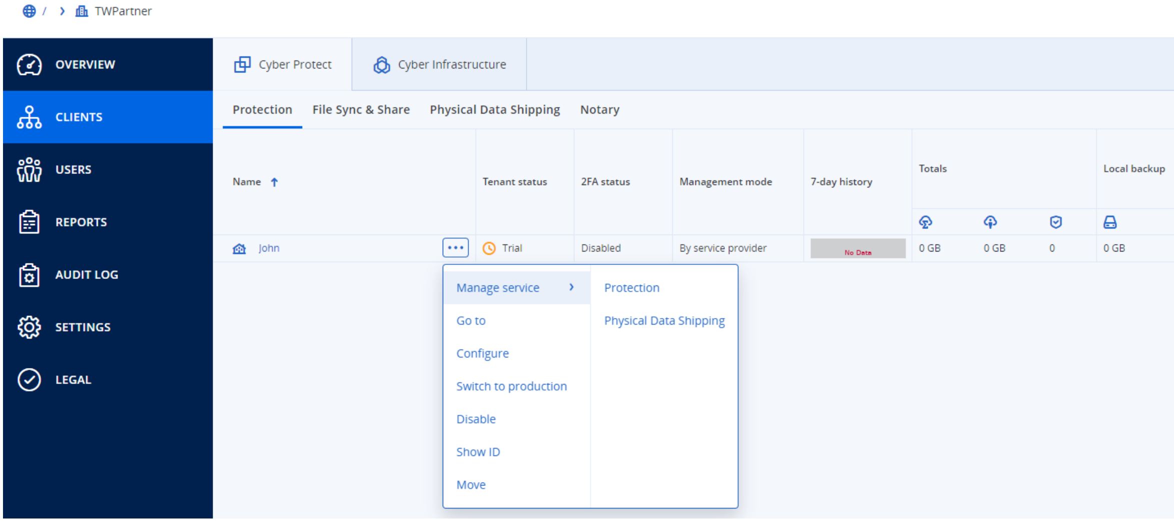
The **Clients** tab displays the child tenants of the tenant in which you are operating and enables you to access the services within them.

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

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



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



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

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

7-day history bar

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

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

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

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

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

User accounts and tenants

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

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

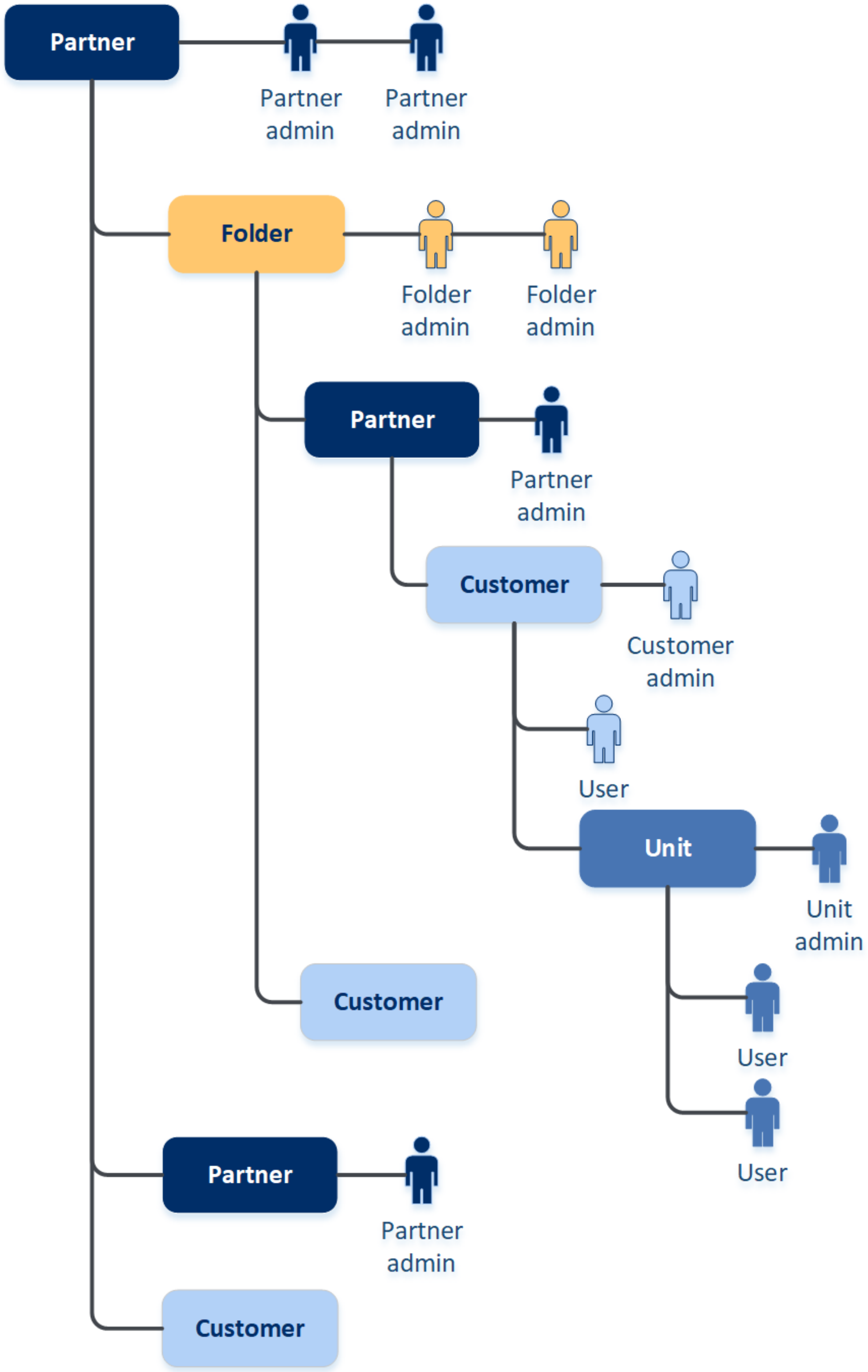
Each account belongs to a tenant. A tenant is a part of the management portal resources (such as user accounts and child tenants) and service offerings (enabled services and offering items within them) dedicated to partner or a customer. The tenant hierarchy is supposed to match the client/vendor relationships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

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

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

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

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


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

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

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

Note

- A user can be created from any type of tenant, and to have a shared email address as long as it is created from the most privileged to the least privileged. For example, a partner tenant can create a Folder, Customer and Unit tenant, while a Customer tenant cannot create a Folder tenant.
- Unit administrators cannot create, modify, or apply Disaster Recovery protection plans.

Managing tenants

The following tenants are available in Cyber Protect:

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

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

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

Creating a tenant

1. Log in to the management portal.
2. Navigate to the tenant in which you want to create a tenant.

3. In the upper-right corner, click **New**, and then click one of the following, depending on the type of the tenant that you want to create:
   - A **Partner** tenant is normally created for each partner that signs the partnership agreement.
   - A **Folder** tenant is normally created to group partners and customers to configure separate offerings and/or different branding.
   - A **Customer** tenant is normally created for each organization that signs up for a service.
   - A **Unit** tenant is created within a customer tenant to expand the service to a new organizational unit.

   The available types depend on the parent tenant type. Note that if the Advanced Automation (PSA) service is enabled, you can also select the relevant tenant type in the **Billing information** section (see "Defining billing information for a tenant" (p. 43)).
4. In **Name**, specify a name for the new tenant.
5. [Only when creating a partner tenant] Enter **Legal company name** (required) and **Tax ID or VAT number** (optional).
6. [Only when creating a customer tenant]
   a. Under **Operation mode**, select whether the tenant is using services in the Trial mode or in the Production mode. Monthly service usage reports include usage data for tenants in both modes.

   Important

   The Trial mode enables a 30-day evaluation period, providing full access to the product. Note that once a customer is switched to Production mode, their usage will be automatically included in the nearest billing cycle.

   You can switch to Production mode at any time. However, reverting from Production to Trial mode is not possible.

   If you decide to cancel the trial for a customer, you must delete the corresponding customer tenant as well. Otherwise, upon the expiration of the 30-day trial, the customer will be automatically switched to Production mode, and the corresponding usage will be included in the nearest billing cycle. For more information, see this knowledge base article.

   b. Under **Advanced settings**, select the management mode for the tenant.
   - **Managed by service provider** – this mode grants full access to the Customer for administrators of the parent tenant: modify properties, manage tenants, users, services; access backups and other resources. This mode is selected by default.
   - **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, units, services, backups, and other resources).

   Note

   If you select **Self-service**, only the administrator of the Customer tenant will be able to change the management mode. To do this, the Customer administrator must navigate to **Settings** > **Security**, and enable the **Support access** switch.

You can check the selected Management mode for your child tenants in the **Clients** tab.

7. [Only when creating a partner tenant] Under **Advanced settings**, select one of the following modes for managing access to the tenant:
   - **Full access** – this mode grants full access to the tenant for administrators in the parent tenant: manage partner's quotas, users and properties, access partner's customers, and get usage reports for the partner and their customers. This mode is selected by default.
   - **Limited access** – this mode limits the access to this partner tenant for administrators of the parent tenant: they can only modify the tenant properties and quotas, and get usage reports for the partner, but cannot access or manage anything inside (e.g. tenants, users, services, backups, and other resources under the partner), and will not get usage reports for partner's customers.

     Note
     If you select **Limited access**, only the administrator of the tenant will be able to change the management mode. To do this, the administrator must navigate to **Settings** > **Security**, and enable 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 (2FA) for the tenant.
   If 2FA is enabled, all users of this tenant will be required to configure two-factor authentication for their accounts for more secure access. Users must install the authentication application on their second-factor devices and use the one-time generated TOTP code along with the traditional login and password to log in to the console. For more details, refer to "Setting up two-factor authentication". To view the two-factor authentication status for your customers, go to **Clients**.
9. [Only when creating a customer tenant in the Compliance mode] In **Security**, select the **Compliance mode** check box.

   With this mode, only encrypted backups are allowed. The encryption password must be set on the protected device and without it, creating backups will fail. All operations that require providing the encryption password to a cloud service are not available. For more details, see "Compliance mode" (p. 42).

   Important
   You cannot disable the Compliance 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 an email for the administrator account. This email will also serve as a login.
    b. If you prefer to use a login that is different from the email, select the check box **Use login that is different from email**, and then enter 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.

c. Select a language.
   If you do not select a language, English will be used by default.

d. Specify the company contacts.
   - **Billing**—the contact that will get updates about important changes in usage reporting in the platform.
   - **Technical**—the contact that will get updates about important technical changes in the platform.
   - **Business**—the contact that will get updates about important business-related changes in the platform.

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

11. In **Language**, change the default language of notifications, reports, and the software that will be used within this tenant.
12. Do one of the following:
    - To finish the tenant creation, click **Save and close**. In this case, all services will be enabled for the tenant. The billing mode for the Protection service will be set to per workload.
    - To select services for the tenant, click **Next**. See "Selecting the services for a tenant" (p. 44).
13. [If Advanced Automation (PSA) is activated] Enter the billing information for your client. For more information, see "Defining billing information for a tenant" (p. 43).

Compliance mode

The Compliance mode is designed for clients with higher security demands. This mode requires mandatory encryption for all backups and allows only locally set encryption passwords.

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

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

Limitations

- The Compliance mode is compatible only with agents version 15.0.26390 or higher.
- The Compliance mode is not available for devices running Red Hat Enterprise Linux 4.x or 5.x, and their derivatives.
- Cloud services cannot access encryption passwords. Due to this limitation, some features are not available for tenants in Compliance mode.

Unsupported features

The following features are not available for tenants in Compliance mode:

- Recovery through the Cyber Protect console
- File-level browsing of backups through the Cyber Protect console
- Access to the Web Restore 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

Defining billing information for a tenant

When Advanced Automation (PSA) is activated for your tenant, you need to define billing information for the client being created. Billing information ensures the provided services and products are correctly billed for.

Note
If billing information is not defined at this stage, you will be prompted to enter the relevant information before using certain features of Advanced Automation (PSA), such as when approving time registrations, or creating contracts or sales items. For more information, see "Onboarding existing clients" (p. 195).

To define billing information

1. In the **Billing information** section of the create/edit tenant dialog, define the following fields:
   - **Business name**: The tenant's business name, pre-selected as the customer tenant name.
   - **Type**: The Advanced Automation (PSA) tenant type (select from **Partner**, **Customer**, **Prospect**).
   - **Email**: The tenant's email address, predefined with the administrator email address used in the **General information** section.
   - **Language**: Select the relevant language for the tenant.
   - **Country**: Select the relevant country for the tenant.
   - **Sales tax**: Select the relevant sales tax for the tenant. If no sales tax is selected, the default tax rate is applied. You can also select the **Tax exempt** checkbox if the tenant is tax exempt.

2. [Optional] Click **Advanced settings** to define additional billing information. Note that some of the fields in this section are optional, and some are pre-set by the system.
   - **External ID**: The customer code used in third party systems, such as accounting software.
   - **Website**: The tenant's website.
   - **Time registration roundup time (minutes)**: Set the time (in minutes) of your ticket roundup time. When ticket work is approved for billing, the total billable hours will be rounded up according to this value. For example, if you set the roundup time value to 15 minutes, 7 minutes of ticket work will be rounded up to 15 before invoicing. Likewise, 21 minutes will be rounded up to 30, and 36 minutes will be rounded to 45, and so on. The default value is **10**.
   - **Payment terms (days)**: Define the number of days in which a customer has to make payment.
   - **Send invoices by**: Select the method (**Email** or **Mail**) for sending invoices for this customer. This setting overrides the default billing setting. For more information, see "Defining your default billing settings" (p. 326).
   - **Payment method**: Select from **Manual payment** or **Direct debit** to define the default invoice payment option for the customer. This option can be adjusted in quotes, contracts, and sales items, as required. When **Direct debit** is selected:
     - Customers can pay invoices via wire transfer or using one of the payment integrations (PayPal, Stripe).
     - Customers can send invoices to their local bank for direct debit processing.
   - **Create subtotals on invoice**: Select the checkbox, if required.
   - **Bank account**: Enter the bank account number for the tenant.
   - **VAT / Sales tax number**: The relevant VAT or sales tax number.
   - **Main office**: Select the parent company from the list.
3. In the **Address** section, enter the relevant address fields.
4. To configure the services for the tenant, click **Next**. See "Selecting the services for a tenant" (p. 44).

Selecting the services for a tenant

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

You can also select and enable services for multiple existing tenants in one action. For more information, see "Enabling services for multiple existing tenants" (p. 46).

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. 45).

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

   For details about storages, refer to "Managing locations and storage".
3. To specify the quota for an item, click on the **Unlimited** link next to the offering item.
   These quotas are "soft". If any of these values are exceeded, an email notification is sent to the tenant administrators and the administrators of the parent tenant. Restrictions on using the services are not applied. For a partner tenant it is expected that the offering item usage can exceed the quota because the overage cannot be set when creating a partner tenant.

4. [Only when creating a customer tenant] Specify the quota overages.
   An overage allows a customer tenant to exceed the quota by the specified value. When the overage is exceeded, restrictions on using the corresponding service are applied.
5. Click **Save and close**.

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

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

Enabling services for multiple existing tenants

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

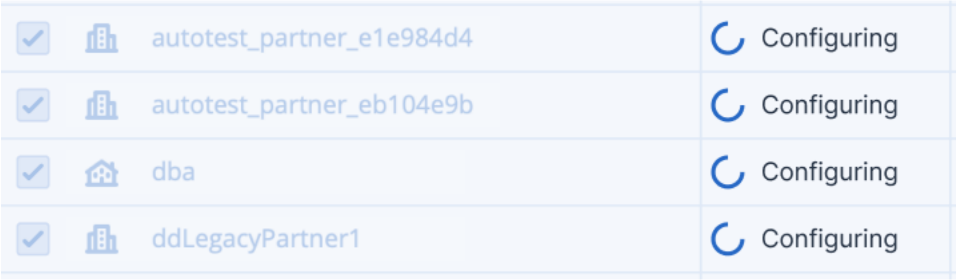
This procedure is applicable to sub-root, partner, folder, and customer tenants. Tenants of any of these different types can be selected simultaneously.

To enable services for multiple tenants

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

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

5. In the **Configure services** section, select the service features and offering items you want to enable for the selected tenants, and then click **Next**.
6. In the **Summary** section, review the changes that will be applied to the selected tenants.
   You can click **Expand all** to see all the tenants' selected services and offering items that will be applied. Alternatively, you can expand each tenant to view the selected services and offering items specific to that tenant.
7. Click **Apply changes**. While the services are configured for each tenant, the tenant is disabled, and the **Tenant status** column indicates the services and offering items are currently being configured, as shown below.



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

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

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

Viewing and updating a tenant's configuration

After a tenant has been created and configured, you can view and update their configured services and offerings as and when required.

To view and update a tenant's configuration

1. In the management portal, go to **Clients**.
2. Click the ellipsis icon for the tenant you want to view or update, and then select **Configure**.
3. In the right pane, you can:
   - Update the settings for available services by clicking on the relevant service tab. For example, click the **Protection** tab to update and manage the service.
   - Click the **Configure** tab to view and update sections in the tenant's configuration, including:
     - **Service**: Enable and disable services, as required.
     - **Company profile**: Update the company profile, add and remove company contacts, as required.
     - **General settings**: Update general information about the company, including the name, country, language and the status of the Compliance mode.
     - **Billing information**: Available only for the activated Advanced Automation (PSA) service, you can update the tenant's billing and address details. For more information, see "Defining billing information for a tenant" (p. 43).
     - **Finance**: (Read-only) Available only for the activated Advanced Automation (PSA) service, you can view a number of key metrics, including the current value of contracts and sales items to be invoiced, and the number of end users being served.
     - **Tickets**: (Read-only) Available only for the activated Advanced Automation (PSA) service, you can view key metrics, including open tickets, SLA breaches, and unassigned tickets. You can also view a list of current open tickets.
     - **Service desk**: Available only for the activated Advanced Automation (PSA) service, you can update the tenant's default settings.

Enabling maintenance notifications

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

Note

- The maintenance notification emails are branded by the data center. Custom branding is not supported for these notifications.
- Maintenance notifications are not supported for VMware Cloud Director users.

To enable the maintenance notifications for child partners or customers

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

Note

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

To enable the maintenance notifications for a user

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

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

Enabling notifications about discovered devices

You can enable notifications about newly discovered devices for Partner and Customer users accounts that are assigned one of the following roles:

- Administrator for the Management Portal.
- Administrator or Cyber administrator for the Protection console.

In that case, on Mondays and Thursdays, the system will send email notifications that include the following information:

- For Customer administrators: the number of devices, grouped by device type, that were newly discovered after the last check.
- For Partner administrators: the number of newly discovered devices per customer.

To enable the notifications for discovered devices

1. Log in to the Management Portal as a Partner user or a Company administrator.
2. Navigate to **Company Management** > **Users**, and then click the name of the user for whom you want to enable the notifications.
3. On the **Services** tab, in the **Settings** section, click the pencil icon.
4. Select **Notifications about newly discovered devices**, and then click **Done**.

The selected user will receive email notifications about the devices that were newly discovered in their corporate networks.

Configuring self-managed customer profile

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

To configure self-managed customer profile

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

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

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

Configuring company contacts

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

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

To configure contacts for your company

1. In the management console, go to **My Company** > **Company profile**.
2. In the **Contacts** section, click **+**.
3. Select an option to create the contact.
   - **Create from existing user**
     - Select a user from the drop-down list.
     - Select a company contact.
       - **Billing**—the contact that will get updates about important changes in usage reporting in the platform.
       - **Technical**—the contact that will get updates about important technical changes in the platform.
       - **Business**—the contact that will get updates about important business-related changes in the platform.

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

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

     If you want to change the email address of the contact that is associated with the user, the system will request verification of the newly defined address. An email will be sent to this address, and the user will need to confirm the change.
   - **Create a new contact**
     - Provide the contact information.
       - **First name**—First name of the contact. This field is required.
       - **Last name**—Last name of the contact. This field is required.
       - **Business email**—Email address of the contact. This field is required.
       - **Business phone**—This field is optional.
       - **Job title**—This field is optional.
     - Select the **Company contacts**.
       - **Billing**—the contact that will get updates about important changes in usage reporting in the platform.
       - **Technical**—the contact that will get updates about important technical changes in the platform.
       - **Business**—the contact that will get updates about important business-related changes in the platform.

         You can assign more than one company contact to a user.
4. Click **Add**.

To configure contacts for a tenant

Note

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

1. In the management portal, go to **Clients**.
2. Click the tenant, and click **Configure**.
3. In the **Contacts** section, click **+**.
4. Select an option to create the contact.
   - **Create from existing user**
     - Select a user from the drop-down list.
     - Select a company contact.
       - **Billing**—the contact that will get updates about important changes in usage reporting in the platform.
       - **Technical**—the contact that will get updates about important technical changes in the platform.
       - **Business**—the contact that will get updates about important business-related changes in the platform.

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

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

       If you want to change the email address of the contact that is associated with the user, the system will request verification of the newly defined address. An email will be sent to this address, and the user will need to confirm the change.
   - **Create a new contact**
     - Provide the contact information.
       - **First name**—First name of the contact. This field is required.
       - **Last name**—Last name of the contact. This field is required.
       - **Business email**—Email address of the contact. This field is required.
       - **Business phone**—This field is optional.
       - **Job title**—This field is optional.
     - Select the **Company contacts**.
       - **Billing**—the contact that will get updates about important changes in usage reporting in the platform.
       - **Technical**—the contact that will get updates about important technical changes in the platform.
       - **Business**—the contact that will get updates about important business-related changes in the platform.

         You can assign more than one company contact to a user.
5. Click **Add**.

Refreshing the usage data for a tenant

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

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

> **Note**
> Fetching the data may take up to 10 minutes.

4. Reload the page to view the updated data.

Disabling and enabling a tenant

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

To disable a tenant

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

As the result:

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

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

Moving a tenant to another tenant

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

Type of tenants that can be moved

Type of tenant	Can be moved	Target tenant
Partner	Yes	Partner or Folder
Folder	Yes	Partner or Folder

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

Requirements and restrictions

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

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

How to move a tenant

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

The operation starts immediately and takes up to 10 minutes.

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

Converting a partner tenant to a folder tenant and vice versa

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

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

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

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

To convert a tenant

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

Limiting the access to your tenant

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

If access to the tenant is not limited, the administrators of the parent tenants will have full access to your tenant. They will be able to perform the following operations:

- Modify the properties of your tenant
- Manage tenants, users, and services for your tenant
- Access backups and other resources in your tenant
- Get usage reports for your tenant, your child tenants, and all customers.

If access to the tenant is limited, the administrators of the parent tenants can perform the following operations:

- Modify the properties of your tenant
- Get usage reports for your tenant, your child tenants, and all customers.

To limit the access of higher-level administrators to your tenant

1. Log in to Management Portal.
2. Go to **Settings** > **Security**.

3. Disable the **Support access** switch.

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.

> **Note**
> While Cyber Protect offers an opportunity to recover tenants, please note that recovery is not supported for the File Sync&Share service.

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.
- You will see the **Tenant status** as **Deleted**. When you hover over the **Deleted** status, you will see the date when the tenant was deleted.

  > **Note**
  > You can still recover all relevant data and settings within 30 days of this deletion date.

Recovering a tenant

In the event a tenant is deleted accidentally, Cyber Protect allows 30 days to recover the tenant.

You might need to recover a tenant for example in the following cases:

- The Partner has accidentally deleted his tenants.
- The Partner development team have accidentally deleted a part of or even the whole tenants hierarchy while testing their integration.

- The Partner integration accidentally de-provisioned the application instead of switching to the new edition, and you need to restore the data.
- The Partner has accidentally disabled the application while switching to new licensing, and you need to restore the data in the disabled application.

To recover a tenant

1. In the management portal, go to **Clients**.
2. On the **Cyber Protect** tab, find the tenant that you want to recover. Its status is displayed as **Deleted**.
3. Hover over the tenant, and then click the ellipsis icon ⋯.
4. Click **Recover**.

   You will see a confirmation window saying that the tenant will be recovered in the same state it was before being deleted, and it will be disabled by default.
5. [Optional] If you need to enable the tenant, select the check box **I want to enable the tenant**. You can enable the tenant at any time later.
6. Click **Recover**.

As a result:

- The tenant and its sub-tenants will be recovered.
- All services that were enabled within the tenant and its sub-tenants will be restarted.

Note
Recovery is not supported for the File Sync&Share service.

- All users within the tenant and its sub-tenants will be recovered.
- All machines in the tenant and its sub-tenants will be re-registered.
- All service-related data, for example backups, in the tenant and its sub-tenants will be recovered.
- All API clients within the tenant and its sub-tenants will be recovered and all integrations using these clients will start working again.
- You will see the **Tenant status** as **Active**, if you have enabled the tenant, or as **Disabled**, if you have not enabled the tenant yet.

Managing users

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

Creating a user account

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

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

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

To create a user account

1. Log in to the management portal.
2. Navigate to the tenant in which you want to create a user account. See "Navigation in the management portal" (p. 32).
3. In the upper-right corner, click **New** > **User**.

   Alternatively, go to **My Company** > **Users**, and click **+ New**.
4. Specify the following contact information for the account:
   - **Email** — This email will also serve as a login.. If you prefer to use a login that is different from the email, select the check box **Use login that is different from email**, and then enter **Login** and **Email**.

     Important
     Each account must have a unique login.

   - **First name** — This field is required for creating user accounts and for creating users within a folder.
   - **Last name**— This field is required for creating user accounts and for creating users within a folder.
   - [Optional] **Business phone**

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

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

   - **Business**—the contact that will get updates about important business-related changes in the platform.

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

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

6. [Not available when creating an account in a partner / folder tenant] Select the services to which the user will have access and the roles in each service.

   Available services depend on the services that are enabled for the tenant in which the user account is created.

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

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

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

To reset a user's password

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

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

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

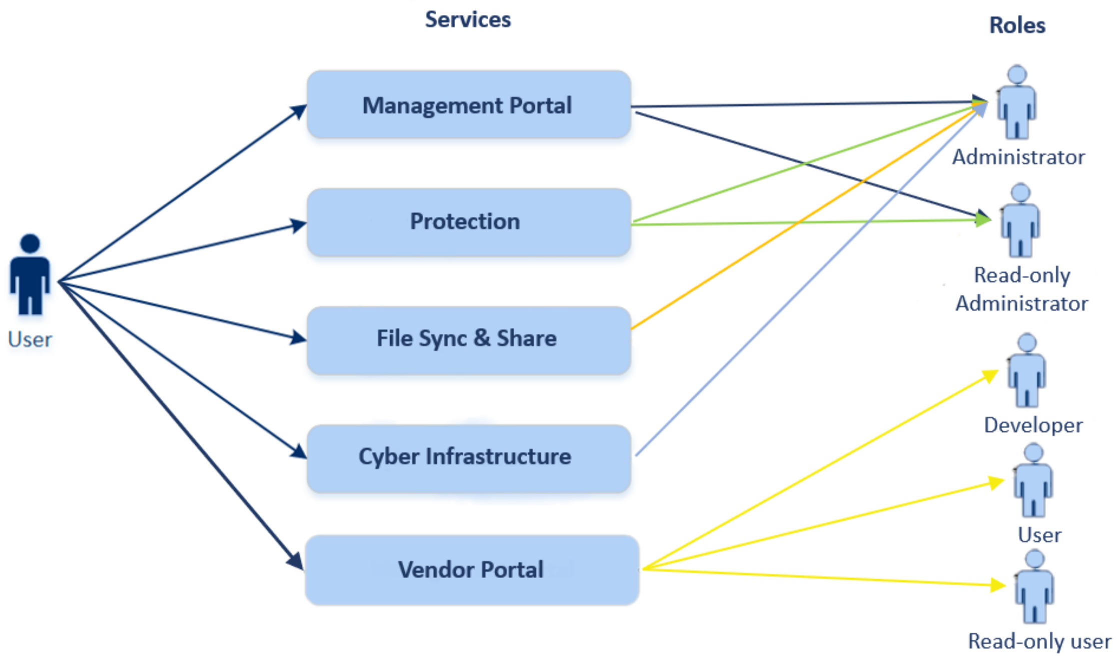
To convert a user account to a service account

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

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

User roles available for each service

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



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

Note

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

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

	Read-only administrator Partner level	This role provides read-only access to all objects in the partner's Management Portal and the Management Portal of all customers of this partner. See "Read-only administrator role" (p. 63).
	Read-only administrator Customer level	This role provides read-only access to all objects in the Management Portal of the entire company. See "Read-only administrator role" (p. 63).
	Read-only administrator Unit level	This role provides read-only access to all objects in the Management Portal of the company unit and sub-units. See "Read-only administrator role" (p. 63).
Vendor Portal	Developer	This role provides full access to Vendor Portal. Developers can create and manage CyberApps, CyberApp Descriptions, and CyberApp Versions. They can also submit deployment requests and monitor CyberApp metrics.
	User	This role allows the user to create, manage, and request approvals of CyberApp Descriptions.
	Read-only user	This role provides read-only access to Vendor Portal.

Protection	

	Administrator	This role enables configuring and managing the Protection service for your customers. This role is required for: • configuring and managing the Disaster Recovery functionality. • configuring and managing the corporate allowlist. • performing autodiscovery of devices. • performing all actions related to software deployment by using DeployPilot (working with software deployment plans, software repositories, software packages, and performing quick deploy actions).
	Cyber administrator	In addition to the rights of the Administrator role, this role enables configuring and managing the Protection service, and approving actions in Cyber Scripting. The Cyber administrator role is only available for tenants with enabled RMM pack.
	Read-only administrator	The role provides read-only access to all objects of the Protection service. See "Read-only administrator role" (p. 63).
	User	This role enables using the Protection service but without administrative privileges. Access is provided to functionality such as Endpoint Detection and Response, but users assigned this role cannot access the data of other users in the organization.
	Restore operator	Applicable to Microsoft 365 and Google Workspace organizations, the role provides access to backups and allows their recovery, while restricting the access to sensitive content inside the backups. See "Restore operator role" (p. 64).
	Security Analyst	The role can be assigned only in customer tenants for which the Advanced Security + EDR or Advanced Security + XDR pack is enabled. It provides access to the Cyber Protection console and enables the user to manage EDR incidents and perform response actions.
	DR support operator	This role provides read-only access to all

		objects of the Protection service in the organization and access to Disaster Recovery environment and allows to perform advanced troubleshooting.
File Sync & Share	Administrator	This role enables configuring and managing File Sync & Share for your users.
Cyber Infrastructure	Administrator	This role enables configuring and managing Cyber Infrastructure for your users.
Advanced Automation (PSA)	There are a number of roles that can be assigned to Advanced Automation (PSA) users. For more information, see "Advanced Automation (PSA) roles" (p. 201).	
Partner Portal	There are a number of roles that can be assigned to Partner portal users. For more information, see "Partner portal roles" (p. 387).	
Notary	Administrator	This role enables configuring and managing Notary for your users.
	User	This role enables using the Notary service but without administrative privileges. Such users cannot access data of other users of the organization.

Note

Vendor Portal is available to technology partners who registered on the Acronis Technology Ecosystem website after October 04, 2023.

If you are looking to build an integration and require access to Vendor Portal and a dedicated Sandbox, see the Integrations chapter.

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

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

Read-only administrator role

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

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

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

A read-only administrator cannot do the following:

- Start or stop any tasks.

  For example, a read-only administrator cannot start a recovery or stop a running backup.
- Configure and manage the Disaster Recovery functionality or the corporate allowlist, and has a read-only access to software deployment plans, software repositories, and software packages.
- Access the file system on source or target machines.

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

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

  For example, a read-only administrator cannot delete backups or delete, update, and rebuild search indexes for cloud-to-cloud backups.

  Note

  In the Management portal, read-only administrators can initiate the creation of new child tenants and configure all their properties for demonstration purposes, but cannot save them.
- Save any changes to scripting plans, monitoring plans, or agent plans.

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

Restore operator role

Note

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

A restore operator can do the following:

- View alerts and activities.
- View and refresh the list of backups.
- View the list of recovery points.

- Browse backups without accessing their content.

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

- Search backups (full text search is not supported).
- Recover cloud-to-cloud backups only to their original location within the original Microsoft 365 or Google Workspace organization.

A restore operator cannot do the following:

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

User roles and Cyber Scripting rights

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

Administrators can manage objects, such as plans or workloads, in their own tenants and in their child tenants, with the following limitations:

- Customer tenants can restrict access for partner administrators.
- Units can always be accessed by customer administrators and partner administrators who manage the parent customer tenant.

Administrators cannot see or access objects at a level above their own tenant.

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

The following roles provide rights with regard to Cyber Scripting:

- **Company administrator**

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

- **Cyber administrator**

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

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

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

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

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

Role	Object	Script status		
		Draft	Testing	Approved
Cyber administrator **Company administrator**	Scripting plan	Edit (Remove a draft script from a plan) Delete Revoke Disable Stop	Create Edit Apply Enable Run Delete Revoke Disable Stop	Create Edit Apply Enable Run Delete Revoke Disable Stop
	Script	Create Edit Change status Clone Delete Cancel running	Create Edit Change status Run Clone Delete Cancel running	Create Edit Change status Run Clone Delete Cancel running
Administrator	Scripting plan	View	View	Create

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

Changing the notification settings for a user

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

To configure the notifications for a user

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

Notifications	Description
Maintenance notifications	Notifications that inform partner users, child tenants (partners, and customers), and individual users about upcoming maintenance activities on the Cyber Protect data center. These notifications can be enabled by partner users for their child tenants, and by partner users or company administrators for individual users within their organization.
Quota overuse notifications	Notifications about exceeded quotas.
Scheduled	Usage reports that are sent on the first day of each month.

Notifications	Description
usage reports	
URL branding notifications	Notifications about the upcoming expiration of the certificate used for the custom URL for the Cyber Protect Cloud services. The notifications are sent to all administrators of the selected tenant - 30 days, 15 days, 7 days, 3 days, and 1 day prior the expiration of the certificate.
Countdown to production switch notifications	Notifications about the customer trial expiration that will be sent 10 days before the trial expires and 3 days before the trial expires.
Production mode activation notification	Notifications about the activation of production mode.
Failure notifications	Notifications about the execution results of protection plans and the results of disaster recovery operations for each device.
Warning notifications	Notifications about the execution results of protection plans and the results of disaster recovery operations for each device.
Success notifications	Notifications about the execution results of protection plans and the results of disaster recovery operations for each device.
Daily recap about active alerts	The daily recap is generated based on the list of active alerts that are present in the Cyber Protect console at the moment when the recap is generated. The recap is generated and sent once a day, between 10:00 and 23:59 UTC. The time when the report is generated and sent depends on the workload in the data center. If there are no active alerts at that time, the recap is not sent. The recap does not include information for past alerts that are no longer active. For example, if a user finds a failed backup and clears the alert, or the backup is retried and succeeds before the recap is generated, the alert will no longer be present and the recap will not include it.
Device control notifications	Notifications about attempts to use peripheral devices and ports that are restricted by protection plans with the device control module enabled.
Notifications about newly discovered devices	Notifications about newly discovered devices. These notifications are sent every Monday and Thursday.
Recovery notifications	Notifications about recovery actions on the following resources: user email messages and entire mailbox, public folders, OneDrive /

Notifications	Description
	GoogleDrive: entire OneDrive and files or folders, SharePoint files, Teams: Channels, entire Team, email messages, and Team site. In the context of these notifications, the following actions are considered recovery actions: send as email, download, or start a recovery operation.
Data loss prevention notifications	Notifications about data loss prevention alerts related to the activity of this user on the network.
Security incident notifications	Notifications about detected malware during on-access, on-execution, and on-demand scans, and about detections from the behavioral engine and the URL filtering engine. There are two options available: **Mitigated** and **Not mitigated.** These options are relevant for Endpoint Detection and Response (EDR) incident alerts, EDR alerts from threat feeds, and individual alerts (for workloads that do not have EDR enabled on them). When an EDR alert is created, an email is sent to the relevant user. If the threat status of the incident changes, a new email is sent. The emails include action buttons that enable the user to see details of the incident (if it was mitigated), or to investigate and remediate the incident (if it was not mitigated).
Infrastructure notifications	Notifications about issues with the Disaster Recovery infrastructure: when the Disaster Recovery infrastructure is unavailable, or the VPN tunnels are unavailable.

Note

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

Default notification settings enabled by notification type and user role

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

Notification type\User role	Partner, folder administrators	Customer, unit administrators (Self-service)	Customer, unit administrators (Managed by Service Provider)
Maintenance notifications	Yes (enabled by default for users of direct partners,	No	No

	disabled for non-direct partners)		
Quota overuse notifications	Yes	Yes	No
Scheduled usage reports notifications	Yes	Yes	No
URL branding notifications	No	No	No
Failure notifications	No	No	No
Warning notifications	No	No	No
Success notifications	No	No	No
Daily recap about active alerts	No	Yes	No
Device Control notifications	No	No	No
Recovery notifications	No	No	No
Data Loss Prevention notifications	No	No	No
Security incident notifications: Mitigated	No	No	No
Security incident notifications: Not mitigated	No	No	No
Infrastructure notifications	No	No	No

Notifications enabled by default per device type and user role

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

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

Disabling and enabling a user account

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

To disable a user account

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

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

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

To enable a disabled user account

1. In the management portal, go to **Users**.
2. Select the disabled user in the users list, and then click the ellipsis icon ••• > **Enable**.

Deleting a user account

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

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

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

To delete a user account

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

As a result:

- All notifications configured for this account will be disabled.
- All data that belongs to this user account will be deleted.
- The administrator will not be able to access the management portal.
- All backups of workloads associated with this user will be deleted.
- All machines associated with this user account will be unregistered.
- All protection plans will be revoked from all workloads associated with this user.
- All File Sync & Share data that belongs to this user (for example, files and folders) will be deleted.
- Notary data that belongs to this user (for example, notarized files, eSigned files) will be deleted.

- You will see the user **Status** as **Deleted**. When you hover over the **Deleted** status, you will see the date when the user was deleted and the note that you can still recover all relevant user data and settings within 30 days of this deletion date.

Recovering a user account

A user account can be deleted accidentally, so Cyber Protection offers an opportunity to recover user accounts.

You might need to recover a user account for example in the following case: the company administrator has deleted a user who has left the company, but you still need all the resources registered under that user.

To recover a user account

1. In the management portal, go to **My Company** > **Users**.
2. On the **Users** tab, find the user account that you want to recover. Its status is displayed as **Deleted**.
3. Hover over the user account, and then click the ellipsis icon ... .
4. Click **Recover**.

   You will see a confirmation window saying that the user account will be recovered in the same state it was before being deleted, and it will be disabled by default.
5. [Optional] If you need to enable the user account, select the check box **I want to enable the user**. You can enable the user account at any time later.
6. Click **Recover**.

As a result:

- This user account will be recovered.
- All data that belongs to this user account will be recovered.
- All machines associated with this user account will be re-registered.
- You will see the user status as **Active**, if you have enabled the user account, or as **Disabled**, if you have not enabled the user account yet.

Transferring ownership of a user account

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

Important
You cannot reassign the content of a deleted account.

To transfer the ownership of a user account:

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

The new owner can now access this account.

Setting up two-factor authentication

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

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

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

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

Note

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

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

Partner administrator accounts that are used by an integration must be converted to service accounts. Otherwise, the integrations will not be able to authenticate to Cyber Protect Cloud. For example, accounts used by an integration are the accounts for the management agent and the backup agent in the VMware Cloud Director integration. For more information about how to create a service account, see "To convert a user account to a service account" (p. 58).

How it works

1. You enable two-factor authentication on your organization level.
2. All of your organization users must install an authentication application on their second-factor devices (mobile phones, laptops, desktops, or tablets). This application will be used for generating one-time TOTP codes. The recommended authenticators:
   - Google Authenticator

     iOS app version (https://apps.apple.com/app/google-authenticator/id388497605)

     Android version (https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2)
   - Microsoft Authenticator

     iOS app version (https://apps.apple.com/app/microsoft-authenticator/id983156458)

     Android version (https://play.google.com/store/apps/details?id=com.azure.authenticator)

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

3. Your organization users must re-log in to the system.
4. After entering their login and password, they will be prompted to set up two-factor authentication for their user account.
5. They must scan the QR code by using their authentication application. If the QR code cannot be scanned, they can use the 32-digit code shown below the QR code and add it manually in the authentication application.

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

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

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

To restore two-factor authentication on a new device

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

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

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

3. If you missed saving the PDF file during the setup:

a. *Click **Reset 2FA** and enter the one-time password shown in the previously set-up mobile authenticator app.*
b. Follow the on-screen instructions.

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

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

Two-factor setup propagation across tenant levels

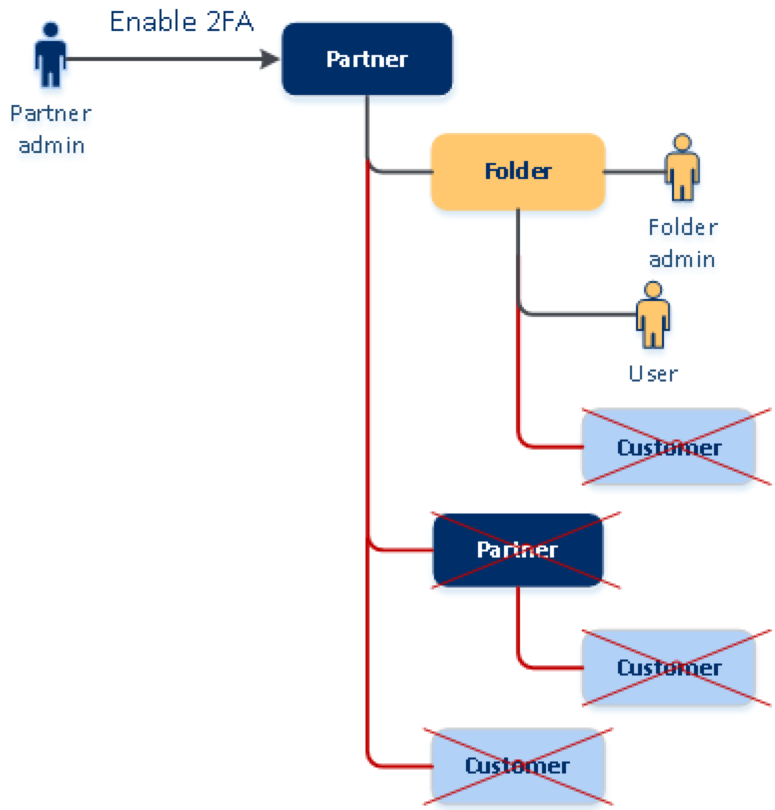
Two-factor authentication is set up on the **organization** level. You can enable or disable two-factor authentication:

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

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

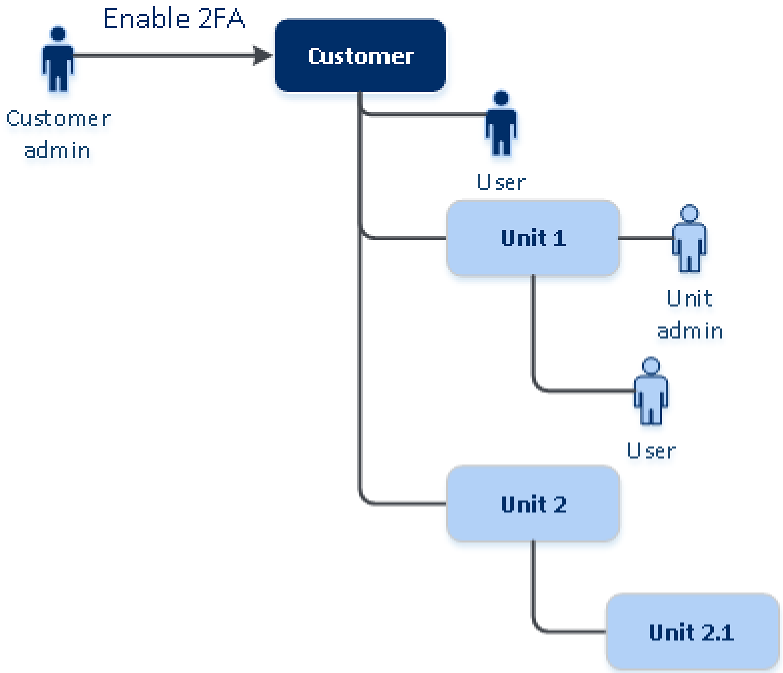
- Folders auto-inherit the two-factor authentication settings from their partner organization. On the scheme below, the red lines mean that the propagation of two-factor authentication settings is not possible.

2FA setting propagation from a partner level



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

2FA setting propagation from a customer level



Note

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

Setting up two-factor authentication for your tenants

Starting with the 24.09 release, Two-factor authentication (2FA) is enabled by default for all Partner tenants (direct and indirect) in production mode, and it cannot be disabled.

Trial partners will get 2FA auto-enabled only when their account is switched to production mode.

Support for service accounts (users with 2FA disabled) will continue. A Partner administrator can still temporarily disable 2FA for a user by converting it to a service account. Existing service accounts remain unaffected, which is important for custom integrations that use basic authentication, as it is not compatible with 2FA. The recommended solution for such integrations is to migrate them to API clients.

2FA is not enforced for Customer tenants, but we strongly recommend that they enable it for their organizations. As a Partner administrator, you can impersonate a Customer administrator and enable 2FA for customers that are managed by you.

To enable two-factor authentication

Required role: Partner administrator

1. Log in to the management portal.
2. Navigate to **Clients** and select the customer tenant for which you want to enable the two-factor authentication.
3. Go to **Settings** > **Security**.
4. Slide the **Two-factor authentication** toggle, and then click **Enable**.

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

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

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

To disable two-factor authentication

Required role: Partner administrator

1. Log in to the management portal.
2. Navigate to **Clients** and select the customer tenant for which you want to disable the two-factor authentication.
3. Go to **Settings** > **Security**.
4. To disable two-factor authentication, turn off the toggle, and then click **Disable**.
5. [If at least one user configured two-factor authentication within the organization] Enter the TOTP code generated in your authentication application on the mobile device.

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

Managing two-factor authentication for users

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

Monitoring

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

To reset the two-factor authentication for a user

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

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

To reset the trusted browsers for a user

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

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

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

To disable two-factor authentication for a user

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

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

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

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

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

To enable two-factor authentication for a user

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

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

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

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

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

Brute-force protection

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

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

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

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

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

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

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

Configuring upsell scenarios for your customers

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

You may want to promote more advanced capabilities for your existing customers who are using standard Cyber Protect functionality.

You can enable or disable the upsell capability per customer. By default, the upsell option is enabled. Your customers will see additional functionality that is not available until the customer purchases it. This additional functionality is marked with labels that show the name or icons of the promoted advanced pack, all highlighted in green. When a customer clicks on an upsell point, a dialog suggests them to enable the required advanced pack. If the customer clicks the **Enable required advanced pack** link, a confirmation dialog opens. If the customer clicks the **Enable** button and the purchasing URL is configured on the partner level, the customer is redirected to that URL.

To configure the purchasing link

You can configure the link for the **Enable** button, which will redirect your customers to your website to purchase advanced services.

1. In the navigation menu of the Management portal, select **Settings** > **Branding**.
2. In the **Upsell** section, edit the value for the **Buy URL** string.

Note
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.

To disable the upsell capability for a customer

1. In the management portal, go to **Clients**.
2. Select the customer, go to the right pane, click the **Configure** tab, and then click **General settings**.
3. In the **Upsell** section, disable the **Promote advanced protection options** to turn off the upsell scenario for the selected customer.

Upsell points shown to a customer

Whitelist

The **Whitelist** menu is added under **Protection** > **Anti-malware**.

When a company has corporate specific applications that can be recognized and detected as false positive by antivirus solutions, it might be time-consuming to manually add the trusted applications to the whitelist. Whitelist can automate the process of adding such applications to the allowlist. Backups are scanned by the Antivirus and Antimalware protection module and the scanned data are analyzed to allowlist such applications and prevent the false positive detections.

This upsell point promotes the Advanced Security pack.

Creating or editing a protection plan

Various advanced features of the following packs are presented to customers while they are creating or editing protection plans.

- Advanced Backup
- RMM
- Advanced Data Loss Prevention
- Antivirus & Antimalware Protection
- Advanced Security + XDR

Data Loss Prevention

The **Data Loss Prevention** upsell point is located in the Cyber Protection console, under the **Protection** menu item.

This upsell point promotes the Advanced Data Loss Prevention pack.

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, see "Managing storage" (p. 83).

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.

For information about geo-redundancy, see "Geo-redundant storage" (p. 89).

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. You can delete a storage when its usage is equal to zero.

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.

Immutable storage

Immutable storage is a type of data storage that prevents backups from being altered, modified, or deleted for a defined period. It ensures that the data remains secure and tamper-proof, providing an extra layer of protection against unauthorized or unintended modification or ransomware attacks. Immutable storage is available for all cloud backups stored in a supported cloud storage instance. See "Supported storages and agents" (p. 85).

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

The immutable storage contains the following backups:

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

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

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

Immutable storage modes

For Partner tenants, there is no selection of immutable storage modes. A Partner can disable or re-enable immutable storage for another Partner or Customer tenant, and set the retention period.

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

Immutable storage is available in the following modes:

- **Governance mode**

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

  Note
  Starting in September 2024, immutable storage Governance mode with a retention period of 14 days is enabled by default on all Acronis-hosted storages for all Partner and Customer tenants. See this KB article for details.

- **Compliance mode**

  Warning!
  Selecting Compliance mode is irreversible.

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

Supported storages and agents

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

Configuring immutable storage

After September 2024, immutable storage in Governance mode is enabled by default, with a retention period of 14 days, for all partner and customer tenants.

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

To configure immutable storage

In a partner tenant

1. Log in to Management Portal as an administrator, and then go to **Settings** > **Security**.
2. Verify that the **Immutable storage** switch is on.
3. Specify a retention period within the range of 14 to 3650 days.

   The default retention period is 14 days. A longer retention period will result in increased storage usage.
4. Click **Save**.

In a customer tenant

1. Log in to Management Portal as an administrator, and then go to **Clients**.
2. To edit the settings for a customer tenant, click the tenant name.
3. In the navigation menu, go to **Settings** > **Security**.
4. Verify that the **Immutable storage** switch is on.
5. Specify a retention period within the range of 14 to 3650 days.

   The default retention period is 14 days. A longer retention period will result in increased storage usage.
6. Select the immutable storage mode and, if prompted, confirm your choice.
   - **Governance mode**

     This mode ensures that ransomware or malicious actors cannot tamper with or erase backup data, because all deleted backups are kept in the immutable storage for the retention period that you specified. It also guarantees the integrity of backup data, which is critical for disaster recovery.

     In this mode, you can disable and re-enable the immutable storage, change the retention period, or switch to Compliance mode.
   - **Compliance mode**

     In addition to the benefits of the Governance mode, the Compliance mode helps organizations meet the regulatory requirements for data retention and security by preventing data tampering.

     Warning!
     Selecting Compliance mode is irreversible. After selecting this mode, you cannot disable the immutable storage, change the retention period, or switch back to Governance mode.
7. Click **Save**.
8. To add an existing archive to the immutable storage, create a new backup in that archive by running the corresponding protection plan manually or on a schedule.

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

To disable immutable storage

In a partner tenant

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

Important

This change will be inherited only by child tenants in which immutable storage is not enabled by default and the immutable storage settings were not changed on the customer level.

Starting from the 24.09 release, immutable storage is being enabled by default in customer tenants. To check the enablement status by datacenter, see this knowledge base article. Disabling immutable storage on the partner level will not affect these tenants. To disable immutable storage, go to the customer tenant.

Warning!

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

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

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

In a customer tenant

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

Note

You can disable immutable storage only in the Governance mode.

Warning!

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

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

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

Viewing immutable storage usage

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

Limitations

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

To view the immutable storage usage

In the Cyber Protect console

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

In the Current usage report

1. Log in to Management Portal as administrator.
2. Go to **Reports** > **Usage**.
3. Select **Ad hoc**.
4. Select **Current usage**, and then click **Generate and send**.

   A report in CSV and HTML format is sent to your email address.

   The HTML file is included in a ZIP archive.
5. In the report, check the **Metric name** column.

   You can see the immutable storage usage in the **Cloud storage - Immutable** row.

Billing example for immutable storage

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

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

Date	Backups	Storage usage	Billing
May, 31			Billed 10 GB for May

Geo-redundant storage

With Geo-redundant storage, your backed-up data is asynchronously copied to a replication location that is geographically distant to the primary backup location. Thus, the data remains durable and accessible even if the primary location becomes unavailable.

The replicated data uses the same amount of storage space as the original data.

Limitations

- Geo-redundant storage might not be available in all data centers.
- Geo-redundancy is supported only with the cloud storage. It is not supported with third-party storages, such as partner-hosted storages or public cloud storages.
- Location for the replicated data depends on your datacenter. For more information, see this knowledge base article.
- Additional limitations apply when you use Geo-redundant storage with Disaster Recovery. For more information, see the Cyber Protect Cloud documentation.

Provisioning Geo-redundant storage

Geo-redundant storage becomes available in a customer tenant after it is provisioned for this tenant in Management Portal.

To provision Geo-redundant storage

1. Log in to Management Portal as administrator.
2. In **Clients**, next to the tenant name, click ellipsis button (...) > **Configure**.
3. On the **Protection** tab, click **Edit**.
4. Under **Cloud resources**, find the storage for which you want to enable geo-redundancy.
5. Next to **Geo-redundancy**, click **Enable**.
6. Click **Save**.

As a result, Geo-redundant cloud storage becomes available in this customer tenant, but it is not automatically enabled. To use Geo-redundant storage, enable it in the Cyber Protect console. See "Enabling Geo-redundant storage" (p. 89).

For more information about provisioning Geo-redundant storage in multiple tenants, see "Enabling services for multiple existing tenants" (p. 46).

Enabling Geo-redundant storage

Prerequisites

- A storage that supports geo-redundancy is assigned to the customer tenant. See "Choosing locations and storages for partners and customers" (p. 82).
- Geo-redundant storage is provisioned for the customer tenant in Management Portal. See "Provisioning Geo-redundant storage" (p. 89).

  Geo-redundant storage cannot be provisioned if a non-compatible storage is assigned. For example, a partner-hosted storage.

You can enable Geo-redundant storage on the main screen of the Cyber Protect console or on the **Settings** tab. The result of both procedures is the same.

To enable Geo-redundant storage

On the Main screen

1. Log in to the Cyber Protect console as administrator.

   A warning message appears at the top of the Cyber Protect console.
2. In the warning message, click **Enable Geo-redundant cloud storage**.
3. To acknowledge your understanding of replication locations and fees, select the checkbox.
4. To confirm your choice, click **Enable**.

As a result, Geo-redundant storage is enabled and backed-up data will be copied to the replication location.

On the Settings tab

1. Log in to the Cyber Protect console as administrator.
2. Go to **Settings** > **System settings**.
3. Collapse the list of default backup options, and then click **Geo-redundant cloud storage**.
4. Enable the **Geo-redundant cloud storage** switch.
5. Click **Save**.
6. To acknowledge your understanding of replication locations and fees, select the checkbox.
7. To confirm your choice, click **Enable**.

As a result, Geo-redundant storage is enabled and backed-up data will be copied to the replication location.

Disabling Geo-redundant storage

You can disable Geo-redundant storage from the Cyber Protect console or you can deprovision it in Management Portal.

To disable Geo-redundant storage

1. Log in to the Cyber Protect console as administrator.
2. Go to **Settings** > **System settings**.
3. Collapse the list of default backup options, and then click **Geo-redundant cloud storage**.
4. Disable the **Geo-redundant cloud storage** switch.

5. Click **Save**.
6. To confirm your choice, type **Disable**, and then click **Disable**.

   As a result, Geo-redundant storage is disabled. Replicated data will be deleted within one day.

To deprovision Geo-redundant storage

1. Log in to Management Portal as administrator.
2. In **Clients**, next to the name of the customer tenant, click the ellipsis button (...) > **Configure**.
3. On the **Protection** tab, click **Edit**.
4. Under **Cloud resources**, clear the **Geo-redundancy** checkbox under the storage name.
5. Click **Save**.

As a result, Geo-redundant storage is disabled for the customer tenant and cannot be enabled in the Cyber Protect console. Replicated data will be deleted within one day.

Viewing the geo-replication status

Geo-replication status shows if the data from the primary backup location is copied to the replication location.

The following statuses are possible:

- **In sync** – Data was copied to the replication location.
- **Syncing** – Data is being copied to the replication location. The duration of this operation depends on the size of the data.
- **On hold** – Data replication is temporarily suspended.
- **Disabled** – Data replication is disabled.

To check the replication status

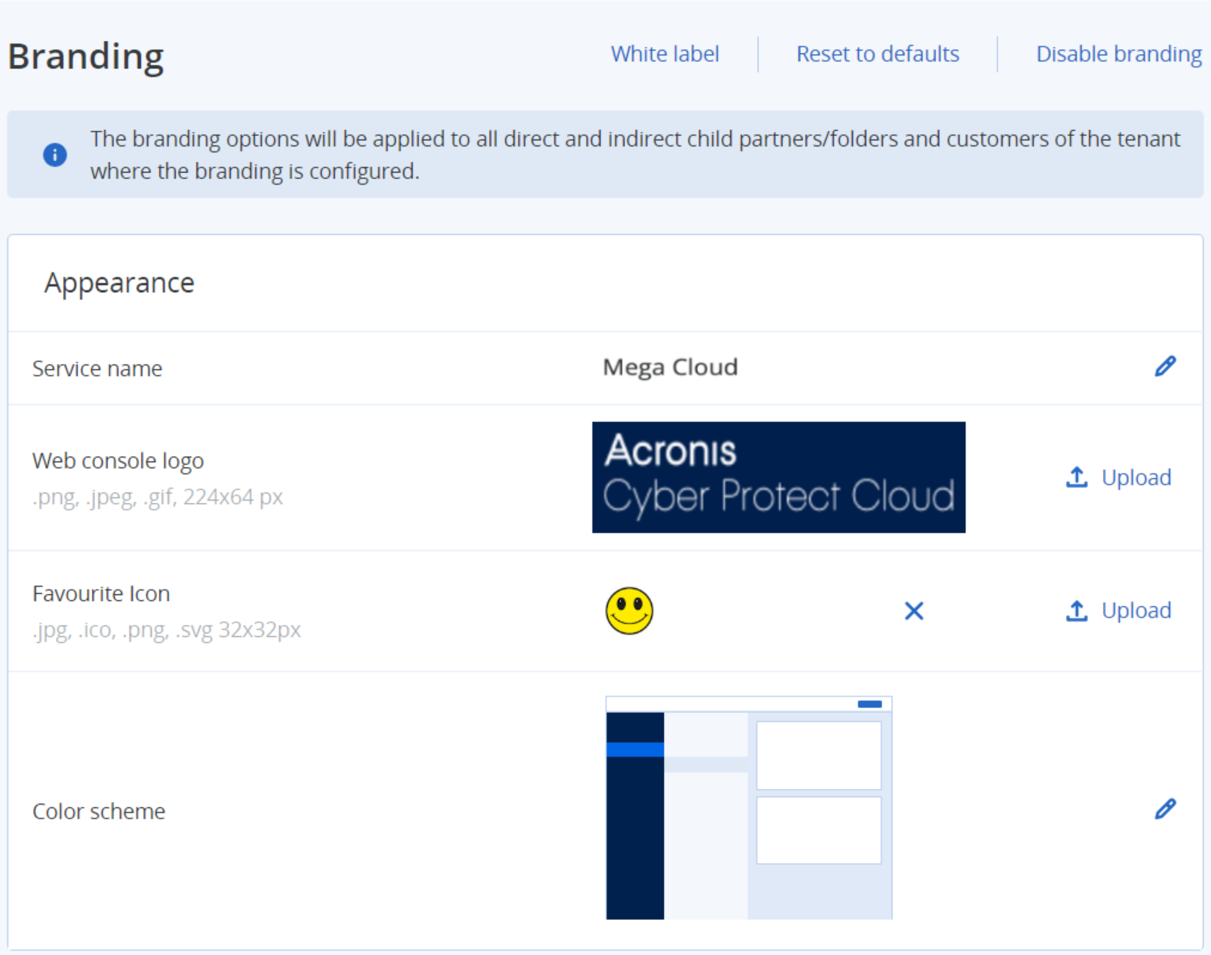
1. Log in to the Cyber Protect console.
2. On the **Backup storage** tab, select the backup location, and then select the backup archive.
3. Click **Details**, and then check the status in the **Geo-replication status** section.

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 for their child tenants to remove any association with the higher-level partners.

Note

Branding settings are applied to all your child tenants, direct and indirect. The branding setting for your own tenant are configured by your service provider.



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

Service name: Mega Cloud

Web console logo .png, .jpeg, .gif, 224x64 px

Favourite Icon .jpg, .ico, .png, .svg 32x32px

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

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

Branding items

Appearance

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

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

Agent and installer branding

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

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

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

Documentation and support

- **Home URL**. This page is opened when a user clicks the company name on the **About** panel.
- **Support URL**. This page is opened when a user clicks the **Contact support** link on the **About** panel or in an email message that is sent by the management portal.
- **Support phone**. This phone number is shown on the **About** panel.
- **Knowledge base URL**. This page is opened when a user clicks the **Knowledge base** link in an error message.
- **Management Portal administrator's guide**. This page is opened when a user clicks the question mark icon in the upper-right corner of the management portal user interface, and then clicks **About** > **Administrator guide**.
- **Management Portal administrator's help**. This page is opened when a user clicks the question mark icon in the upper-right corner of the management portal user interface, and then clicks **Help**.

URL for Cyber Protect Cloud services

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

Legal documents settings

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

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

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

Upsell

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

Mobile apps

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

Email server settings

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

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

Configuring branding

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

Restoring the default branding settings

You can reset all branding items to their default values.

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

Disabling the branding

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

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

White labeling

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

Applying white labeling

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

Configuring custom web interface URLs

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

To configure the web interface URL for Cyber Protect Cloud services

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

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

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

     Note
     A certificate validation error might occur with the error message: "Failed to verify the certificate: x509: certificate signed by unknown authority". Usually it means that some intermediate certificates are missing. Use a certificate chain resolver to fix the structure of your certificate and upload the full certificate chain.
6. Click **Submit** to apply the changes.

To reset the custom URL to default

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

Configuring the updates of the Cyber Protection agent

Important

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

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

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

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

Note

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

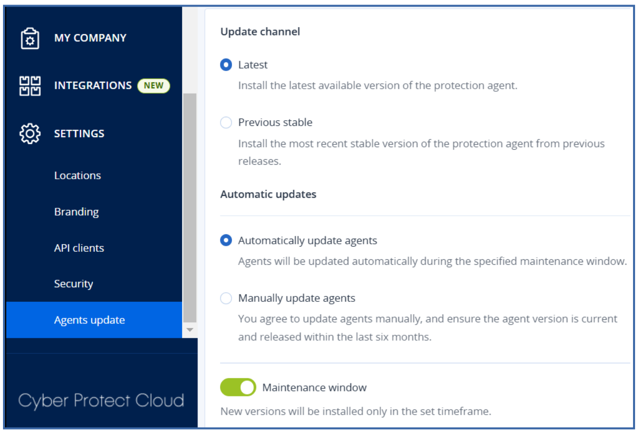
Automatic updates

Note

Partners and customers who do not have the Protection service enabled inherit the settings for automatic updates of the Agent for File Sync & Share from their service provider.

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

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



Update channel

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

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

Automatic updates

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

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

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

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

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

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

   Note
   Automatic updates are only available for the following agents:
   - Cyber Protect agent versions 26986 (released in May 2021) or later.
   - Desktop Agent for File Sync & Share, version 15.0.30370 or later.

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

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

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

5. Click **Save**.

Manual updates

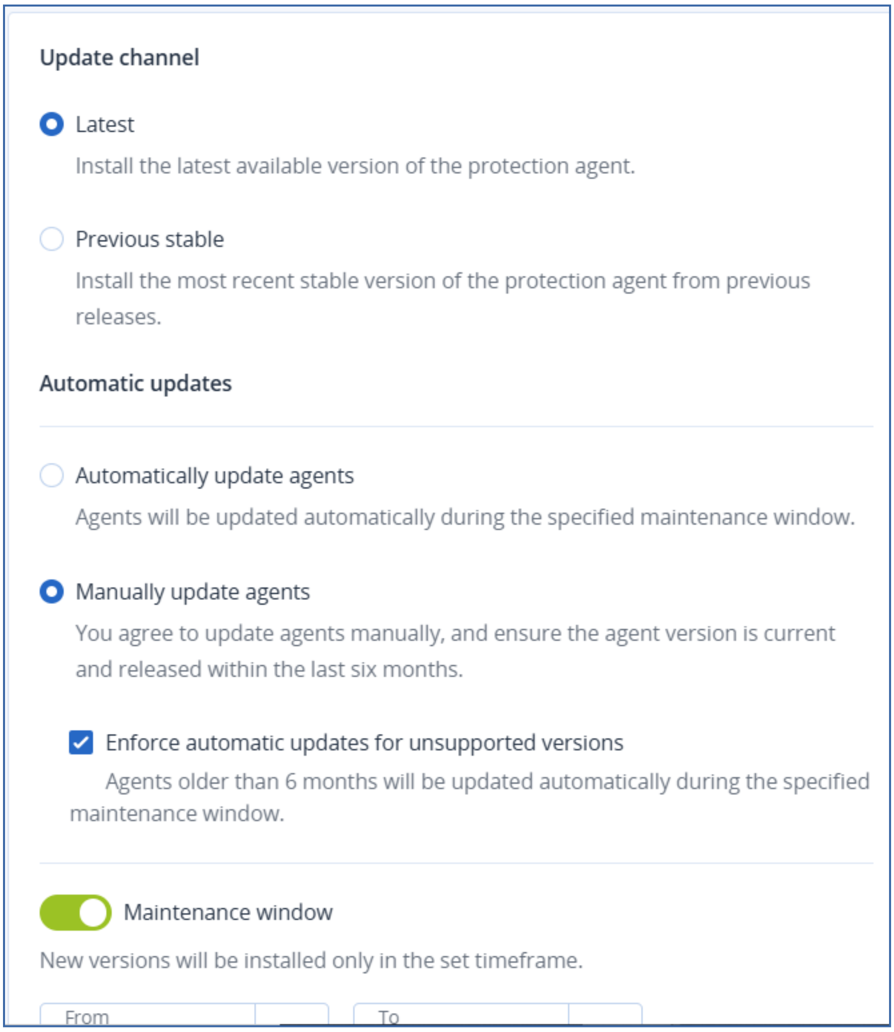
Important
We strongly recommend that you enable automatic updates for your agents. Regular updates ensure your agents stay up to date, offering improved performance, bug fixes, and enhanced protection and security features.

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

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

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

3. Select **Manually update agents.**



Update channel

● Latest

Install the latest available version of the protection agent.

○ Previous stable

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

Automatic updates

○ Automatically update agents

Agents will be updated automatically during the specified maintenance window.

● Manually update agents

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

☑ Enforce automatic updates for unsupported versions

Agents older than 6 months will be updated automatically during the specified maintenance window.

Maintenance window

New versions will be installed only in the set timeframe.

From To

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

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

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

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

5. Click **Save.**

Monitoring the agent updates

Important

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

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

Monitoring

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

Usage

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

The usage data includes both standard features and advanced features.

Important

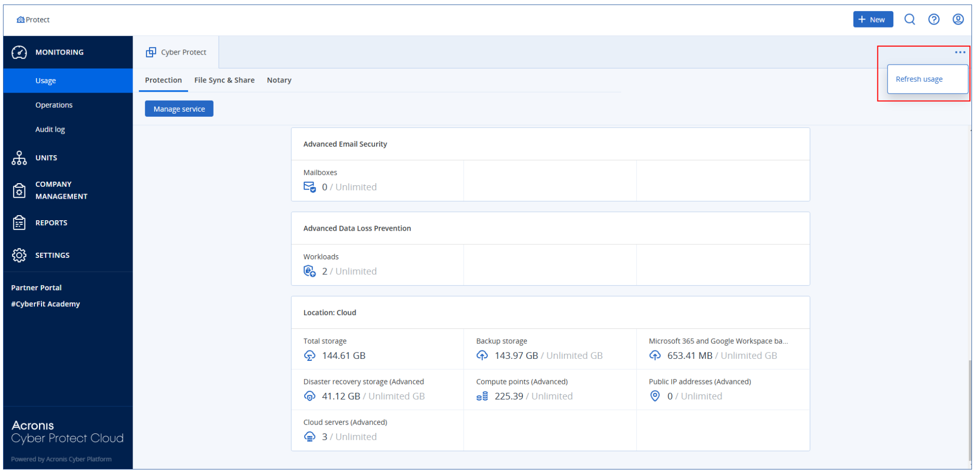
The values of storage usage displayed in the product UI are in binary byte units – mebibytes (MiB), gibibytes (GiB), and tebibytes (TiB) – even though the labels show MB, GB, and TB respectively. For example, if the actual usage is 3105886629888 bytes, the value displayed in the UI is correctly shown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

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

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

Note

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



Advanced Email Security

Mailboxes
0 / Unlimited

Advanced Data Loss Prevention

Workloads
2 / Unlimited

Location: Cloud

Total storage 144.61 GB	Backup storage 143.97 GB / Unlimited GB	Microsoft 365 and Google Workspace ba... 653.41 MB / Unlimited GB
Disaster recovery storage (Advanced 41.12 GB / Unlimited GB	Compute points (Advanced) 225.39 / Unlimited	Public IP addresses (Advanced) 0 / Unlimited
Cloud servers (Advanced) 3 / Unlimited		

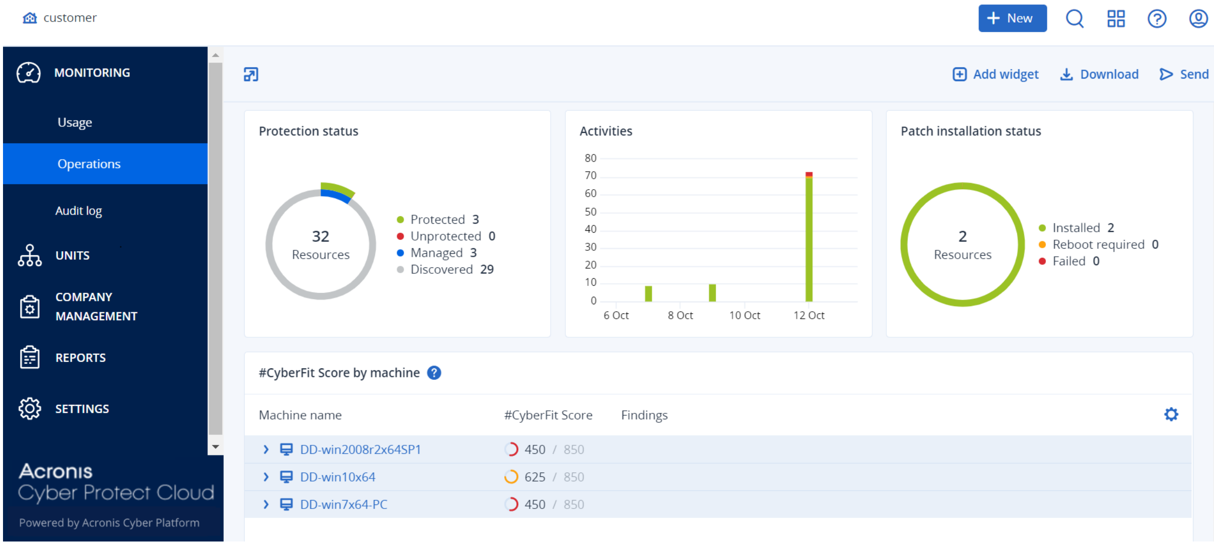
Operations

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.



#CyberFit Score by machine

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

To rearrange the widgets on the dashboard

Drag and drop the widgets by clicking on their names.

To edit a widget

Click the pencil icon next to the widget name. Editing a widget enables you to rename it, change the period of time, select the tenant for which the data is displayed, and set filters.

To add a widget

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

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

To remove a widget

Click the X sign next to the widget name.

Protection status

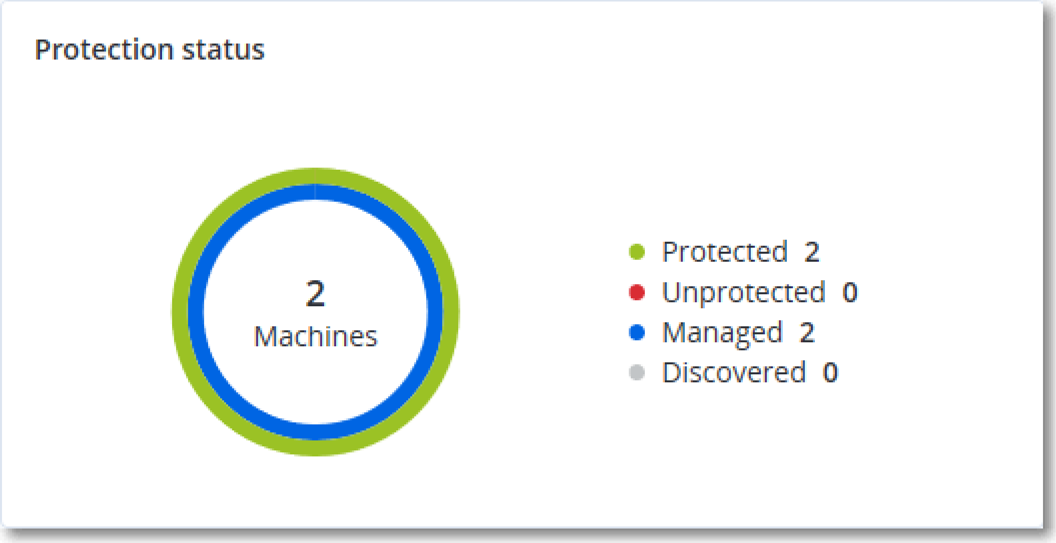
Protection status

This widget shows the current protection status for all machines.

A machine can be in one of the following statuses:

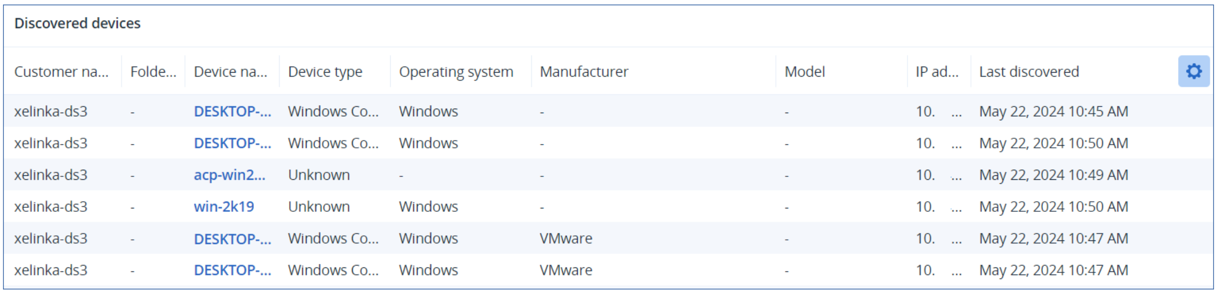
- **Protected** – machines with applied protection plan.
- **Unprotected** – machines without applied protection plan. These include both discovered machines and managed machines with no protection plan applied.
- **Managed** – machines with installed protection agent.
- **Discovered** – machines without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

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



Discovered devices

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



Discovered devices

Customer na...	Folde...	Device na...	Device type	Operating system	Manufacturer	Model	IP ad...	Last discovered
xelinka-ds3	-	DESKTOP-...	Windows Co...	Windows	-	-	10. ...	May 22, 2024 10:45 AM
xelinka-ds3	-	DESKTOP-...	Windows Co...	Windows	-	-	10. ...	May 22, 2024 10:50 AM
xelinka-ds3	-	acp-win2...	Unknown	-	-	-	10. ...	May 22, 2024 10:49 AM
xelinka-ds3	-	win-2k19	Unknown	Windows	-	-	10. ...	May 22, 2024 10:50 AM
xelinka-ds3	-	DESKTOP-...	Windows Co...	Windows	VMware	-	10. ...	May 22, 2024 10:47 AM
xelinka-ds3	-	DESKTOP-...	Windows Co...	Windows	VMware	-	10. ...	May 22, 2024 10:47 AM

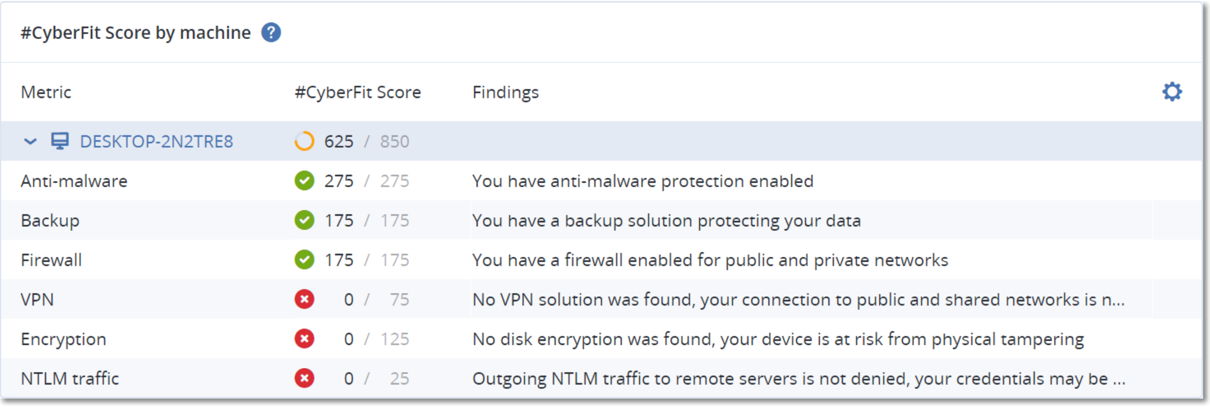
#CyberFit Score by machine

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

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

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

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



#CyberFit Score by machine

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

Endpoint Detection and Response (EDR) widgets

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

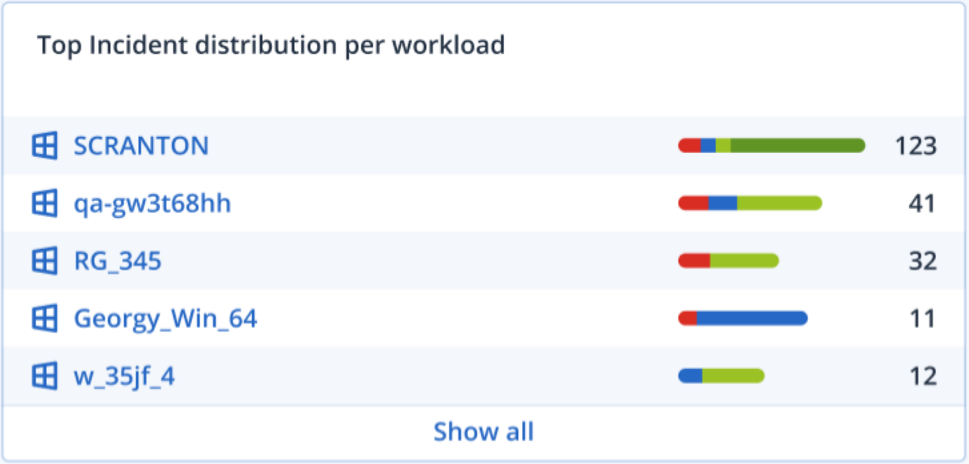
The widgets available are:

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

Top incident distribution per workload

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

Hover over a workload row to view a breakdown of the current investigation state for the incidents; the investigation states are **Not started**, **Investigating**, **Closed**, and **False positive**. Then click on the workload you want to analyze further, and select the relevant customer in the displayed popup; the incident list is refreshed according to the widget settings.



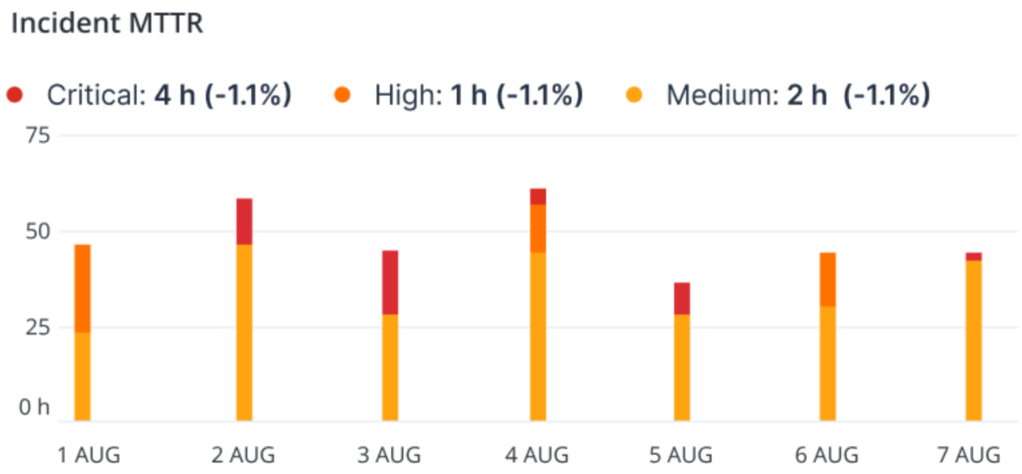
Top Incident distribution per workload

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

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.

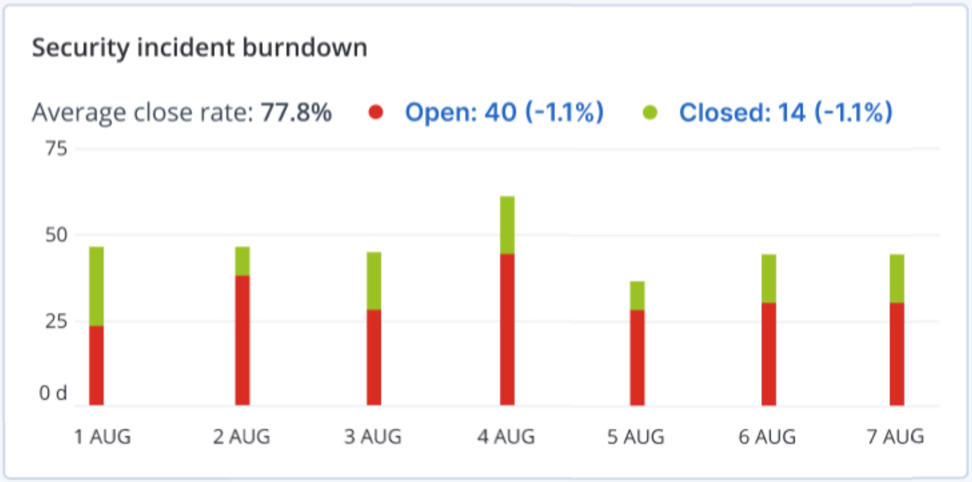


Security incident burndown

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.

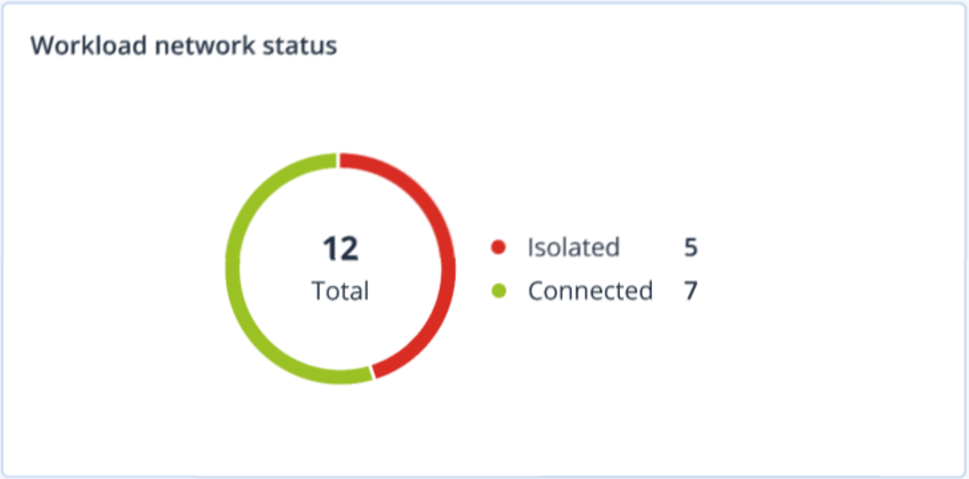

Security incident burndown

Average close rate: 77.8% ● Open: 40 (-1.1%) ● Closed: 14 (-1.1%)

Workload network status

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

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



Disk health monitoring

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

Limitations

- Disk health forecast is supported only for machines running Windows.
- Only disks of physical machines are monitored. Disks of virtual machines cannot be monitored and are not shown in the disk health widgets.
- RAID configurations are not supported. The disk health widgets do not include any information about machines with RAID implementation.
- NVMe SSDs are not supported.
- External storage devices are not supported.

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

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

How it works

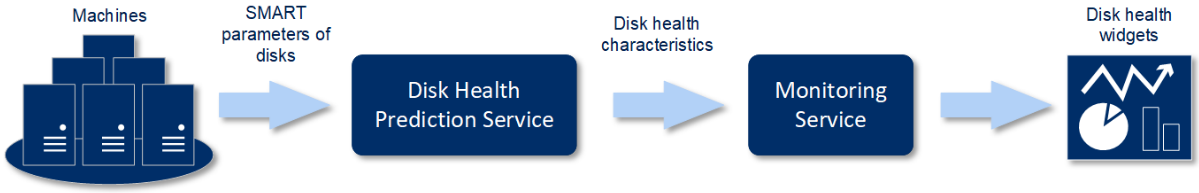
The Disk Health Prediction Service uses an AI-based prediction model.

1. The protection agent collects the SMART parameters of the disks and passes this data to the Disk Health Prediction Service:

- SMART 5 – Reallocated sectors count.
- SMART 9 – Power-on hours.
- SMART 187 – Reported uncorrectable errors.
- SMART 188 – Command timeout.
- SMART 197 – Current pending sector count.
- SMART 198 – Offline uncorrectable sector count.
- SMART 200 – Write error rate.

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

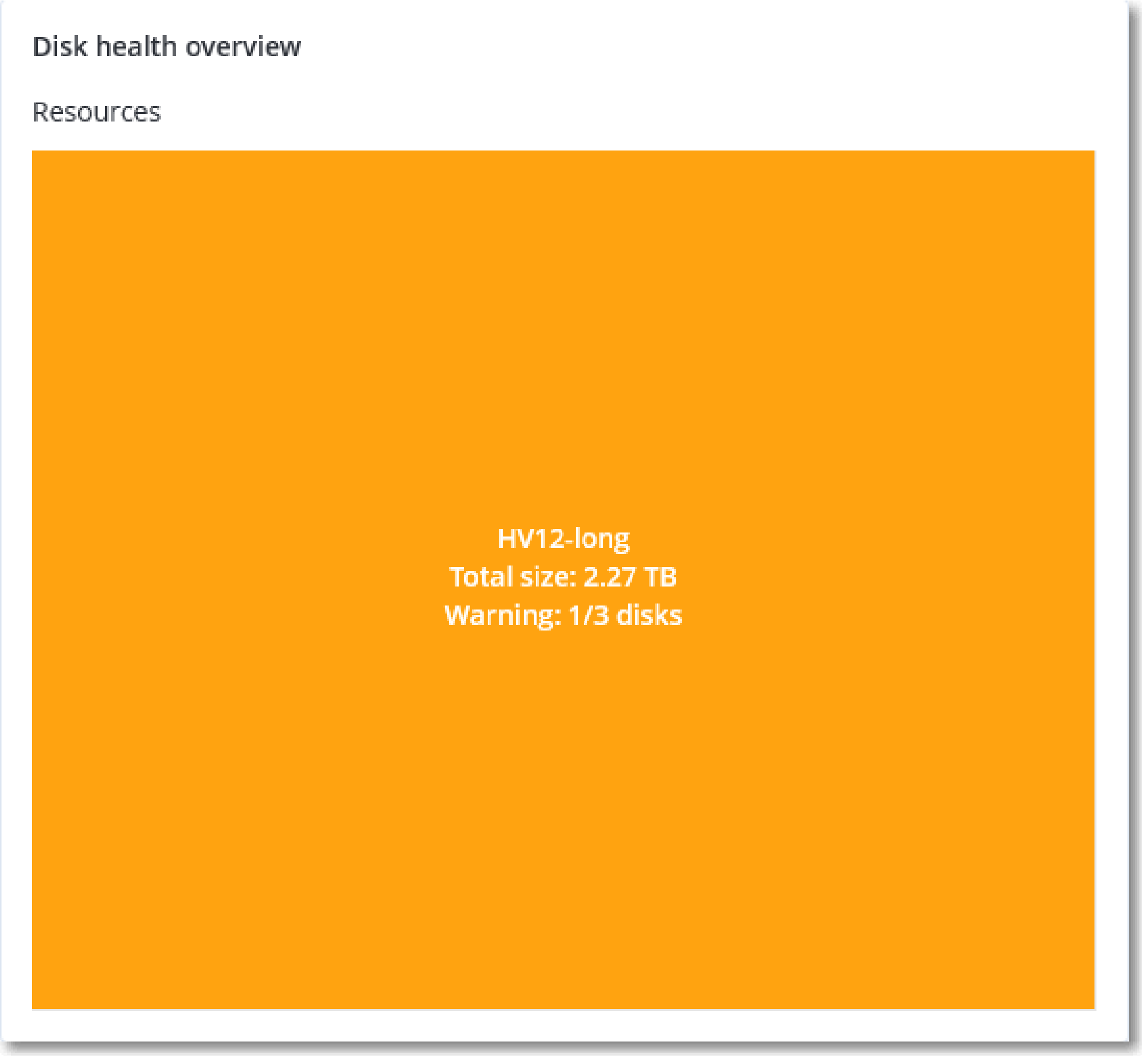
   The prediction period is one month.
3. The Monitoring Service receives these characteristics, and then shows the relevant information in the disk health widgets in the Cyber Protect console.


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

Disk health widgets

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

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



Disk health overview

Resources

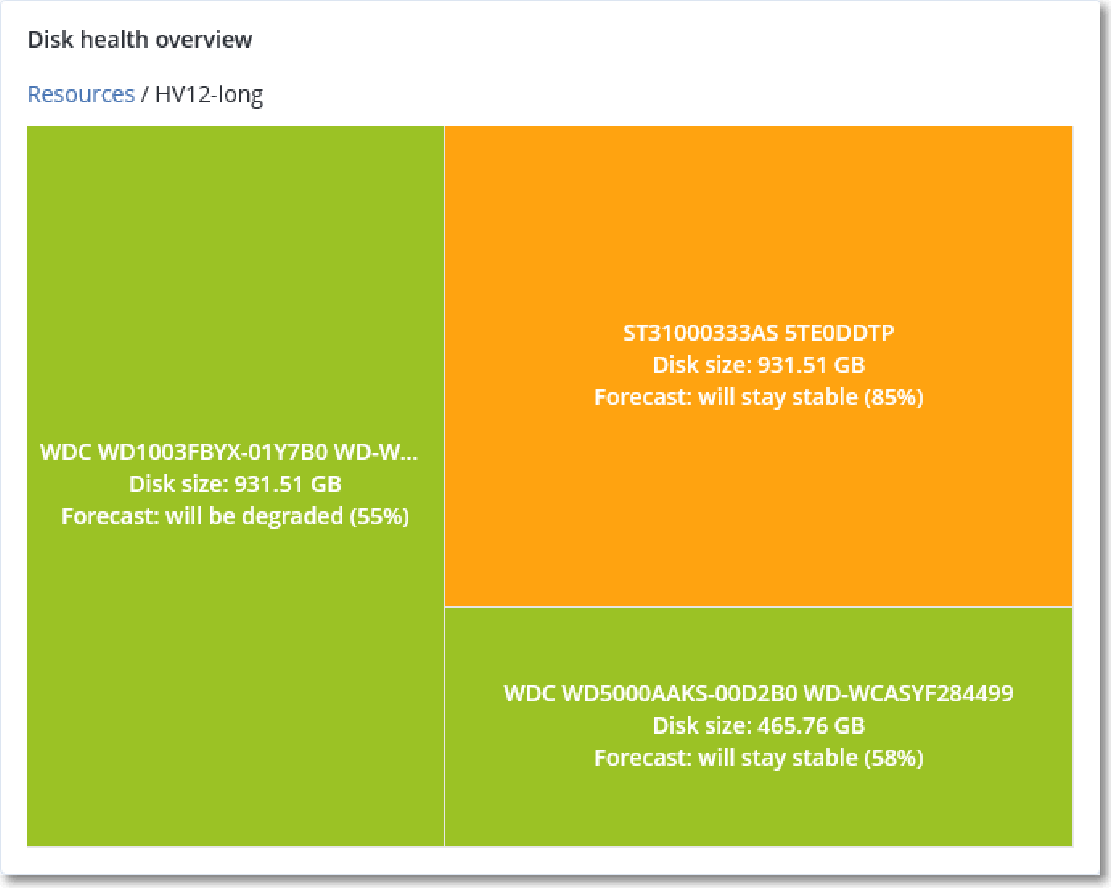
HV12-long
Total size: 2.27 TB
Warning: 1/3 disks

- Disk level

  Shows the current disk health status of all disks for the selected machine. Each disk block shows one of the following disk health forecasts and its probability in percentage:

  - Will be degraded
  - Will stay stable

- Will be improved



Disk health overview

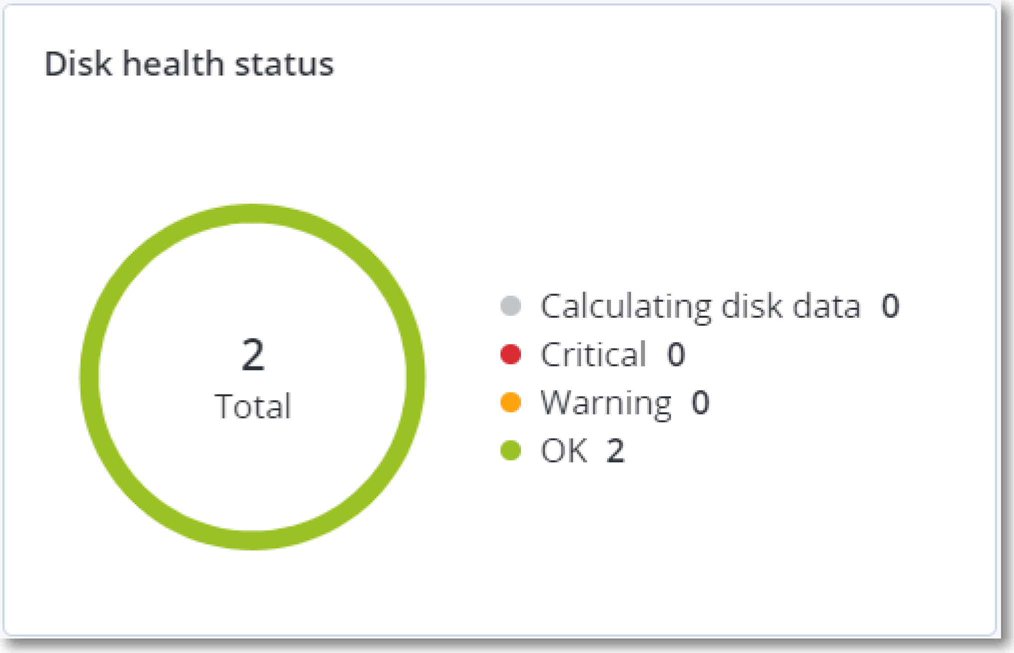
Resources / HV12-long

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

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

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

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



Disk health status

2
Total

●	Calculating disk data	0
●	Critical	0
●	Warning	0
●	OK	2

Disk health status alerts

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

Alert name	Severity	Disk health status	Description
Disk failure is possible	Warning	(30 – 70)	The <disk name> disk on this machine is likely to fail in the future. Run a full image backup of this disk as soon as possible, replace it, and then recover the image to the new disk.
Disk failure is imminent	Critical	(0 – 30)	The <disk name> disk on this machine is in a critical state, and will most likely fail very soon. We do not recommend an image backup of this disk at this point, as the added stress can cause the disk to fail. Back up the most important files on this disk immediately and replace it.

Data protection map

The data protection map feature allows you to 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.

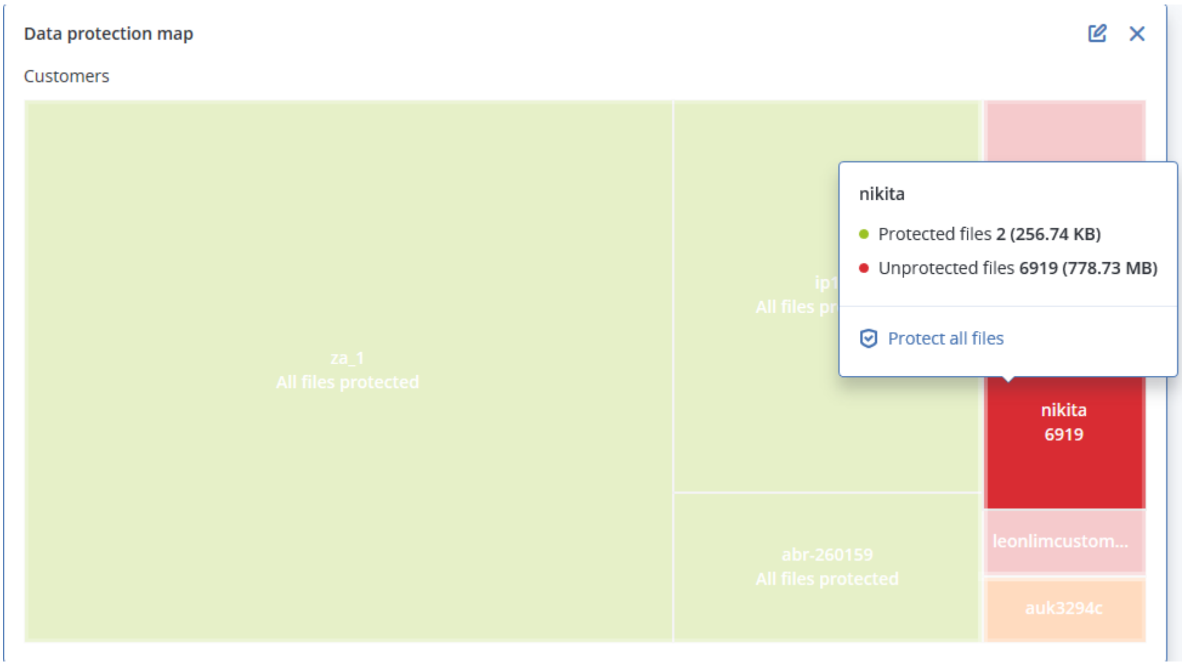
Each block size depends on the total number/size of all important files that belong to a customer/machine.

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.

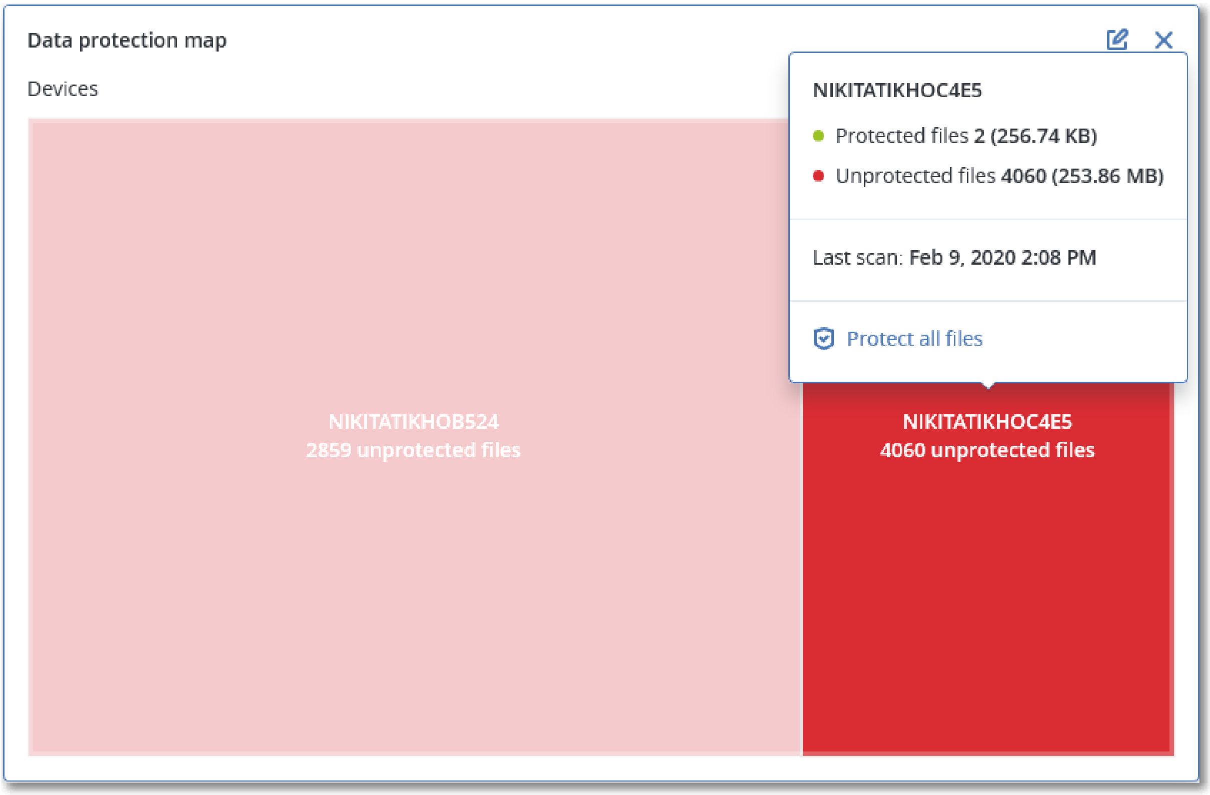


nikita

● Protected files 2 (256.74 KB)

● Unprotected files 6919 (778.73 MB)

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



NIKITATIKHOC4E5

● Protected files 2 (256.74 KB)

● Unprotected files 4060 (253.86 MB)

Last scan: Feb 9, 2020 2:08 PM

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

You can also download a detailed report in CSV format.

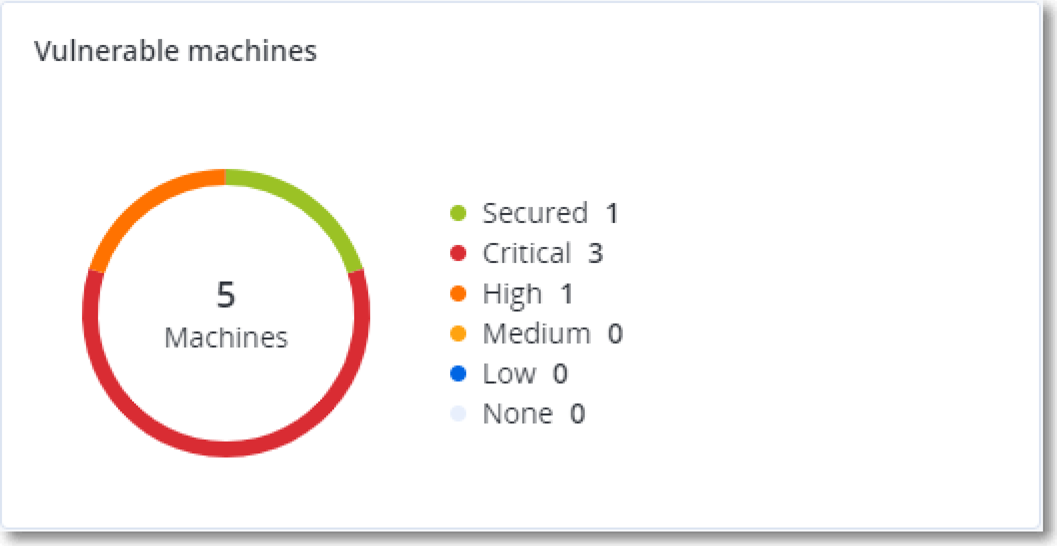
Vulnerability assessment widgets

Vulnerable machines

This widget shows the vulnerable machines by the vulnerability severity.

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

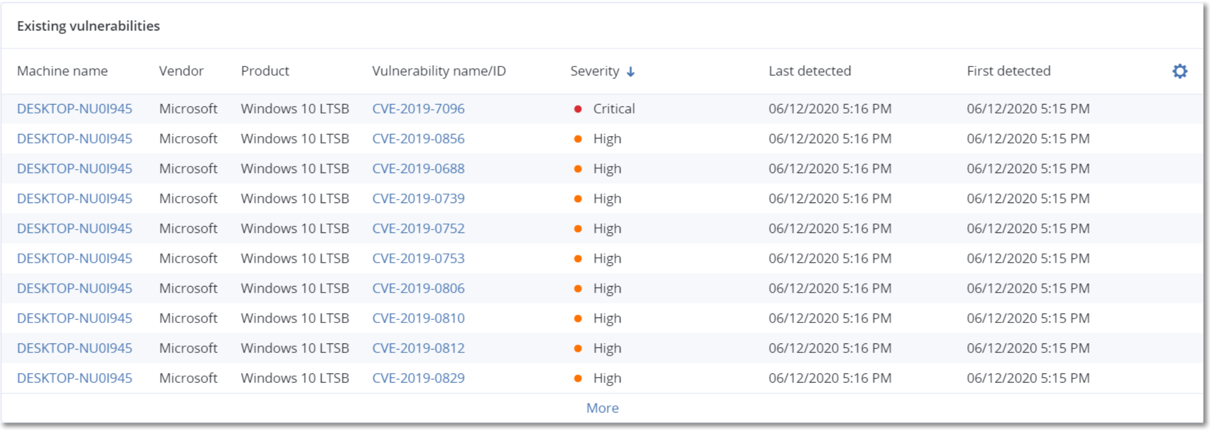
- Secured: no vulnerabilities are found
- Critical: 9.0 - 10.0 CVSS
- High: 7.0 - 8.9 CVSS
- Medium: 4.0 - 6.9 CVSS
- Low: 0.1 - 3.9 CVSS
- None: 0.0 CVSS



Existing vulnerabilities

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

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



Existing vulnerabilities

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

More

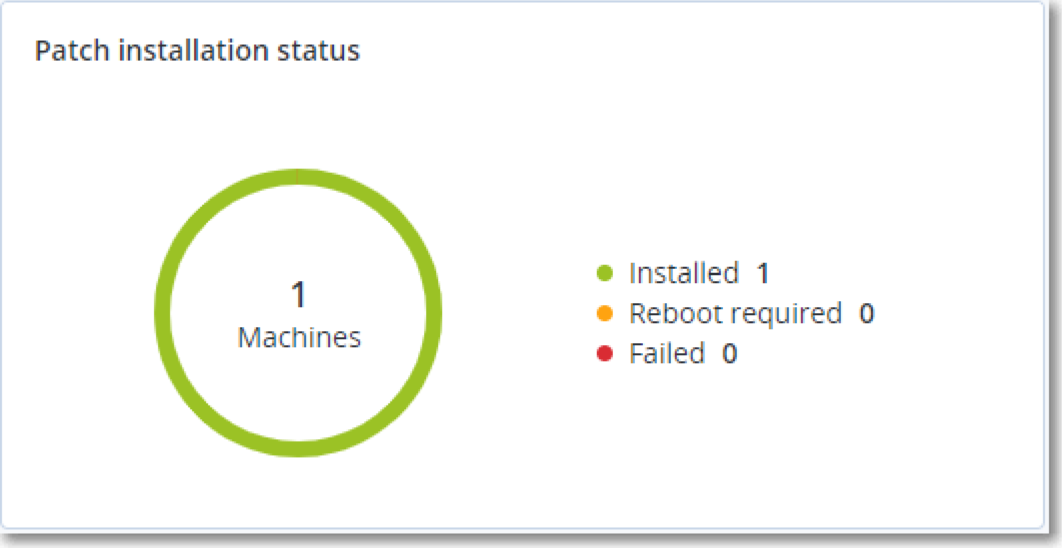
Patch installation widgets

There are four widgets related to the patch management functionality.

Patch installation status

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

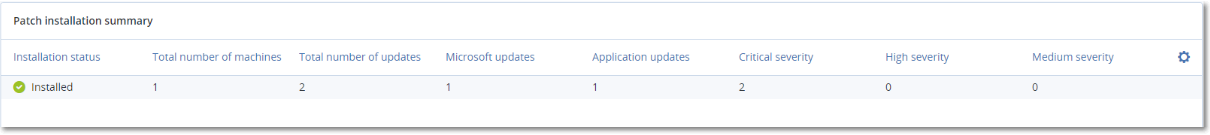
- **Installed** – all available patches are installed on a machine
- **Reboot required** – after patch installation reboot is required for a machine
- **Failed** – patch installation failed on a machine



Patch installation status

Patch installation summary

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

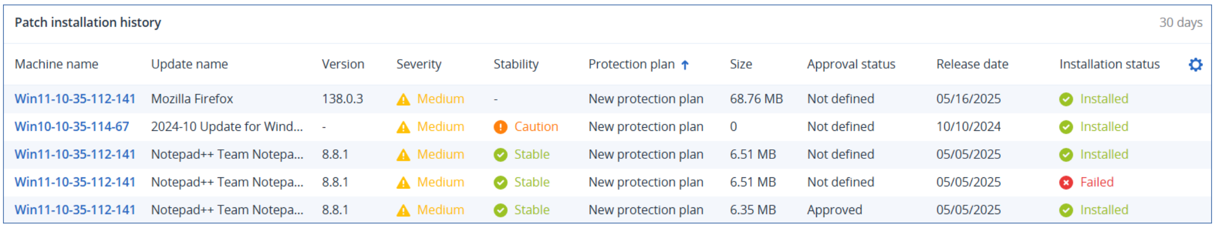


Patch installation summary

Installation status	Total number of machines	Total number of updates	Microsoft updates	Application updates	Critical severity	High severity	Medium severity
✓ Installed	1	2	1	1	2	0	0

Patch installation history

This widget shows the detailed information about patches on machines.



Patch installation history

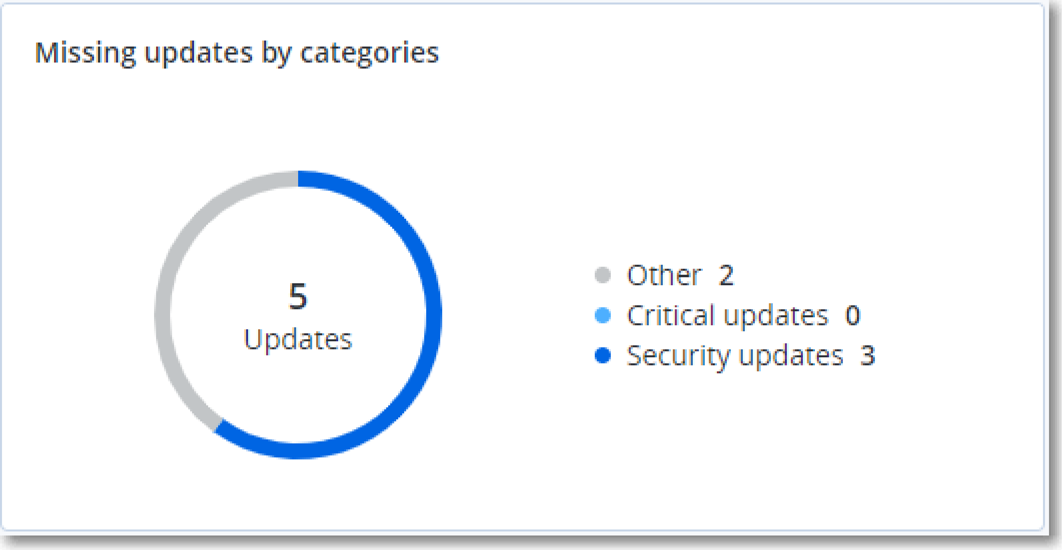
30 days

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

Missing updates by categories

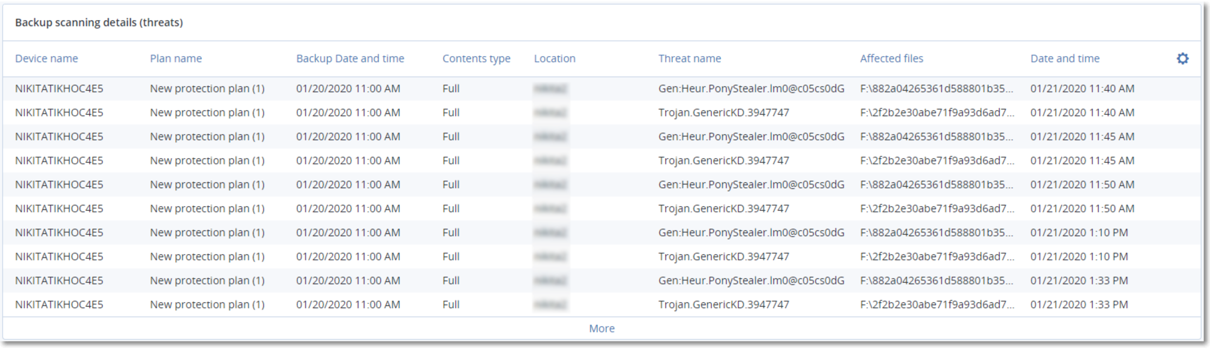
This widget shows the number of missing updates per category. The following categories are shown:

- Security updates
- Critical updates
- Other



Backup scanning details

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



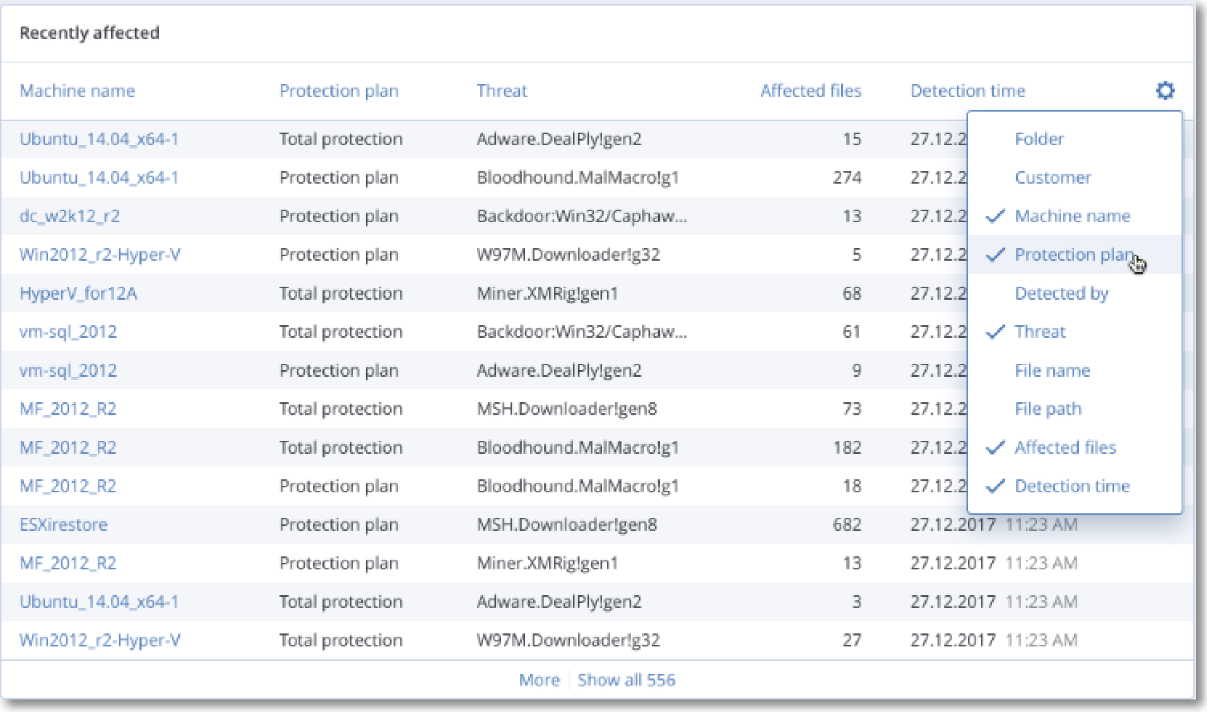
Backup scanning details (threats)

Device name	Plan name	Backup Date and time	Contents type	Location	Threat name	Affected files	Date and time
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:33 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:33 PM

More

Recently affected

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



Recently affected

Machine name	Protection plan	Threat	Affected files	Detection time
Ubuntu_14.04_x64-1	Total protection	Adware.DealPly!gen2	15	27.12.2
Ubuntu_14.04_x64-1	Protection plan	Bloodhound.MalMacro!g1	274	27.12.2
dc_w2k12_r2	Protection plan	Backdoor:Win32/Caphaw...	13	27.12.2
Win2012_r2-Hyper-V	Protection plan	W97M.Downloader!g32	5	27.12.2
HyperV_for12A	Total protection	Miner.XMRig!gen1	68	27.12.2
vm-sql_2012	Total protection	Backdoor:Win32/Caphaw...	61	27.12.2
vm-sql_2012	Protection plan	Adware.DealPly!gen2	9	27.12.2
MF_2012_R2	Total protection	MSH.Downloader!gen8	73	27.12.2
MF_2012_R2	Total protection	Bloodhound.MalMacro!g1	182	27.12.2
MF_2012_R2	Protection plan	Bloodhound.MalMacro!g1	18	27.12.2
ESXirestore	Protection plan	MSH.Downloader!gen8	682	27.12.2017 11:23 AM
MF_2012_R2	Protection plan	Miner.XMRig!gen1	13	27.12.2017 11:23 AM
Ubuntu_14.04_x64-1	Total protection	Adware.DealPly!gen2	3	27.12.2017 11:23 AM
Win2012_r2-Hyper-V	Total protection	W97M.Downloader!g32	27	27.12.2017 11:23 AM

- Folder
- Customer
- ✓ Machine name
- ✓ Protection plan
- Detected by
- ✓ Threat
- File name
- File path
- ✓ Affected files
- ✓ Detection time

Downloading data for recently affected workloads

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

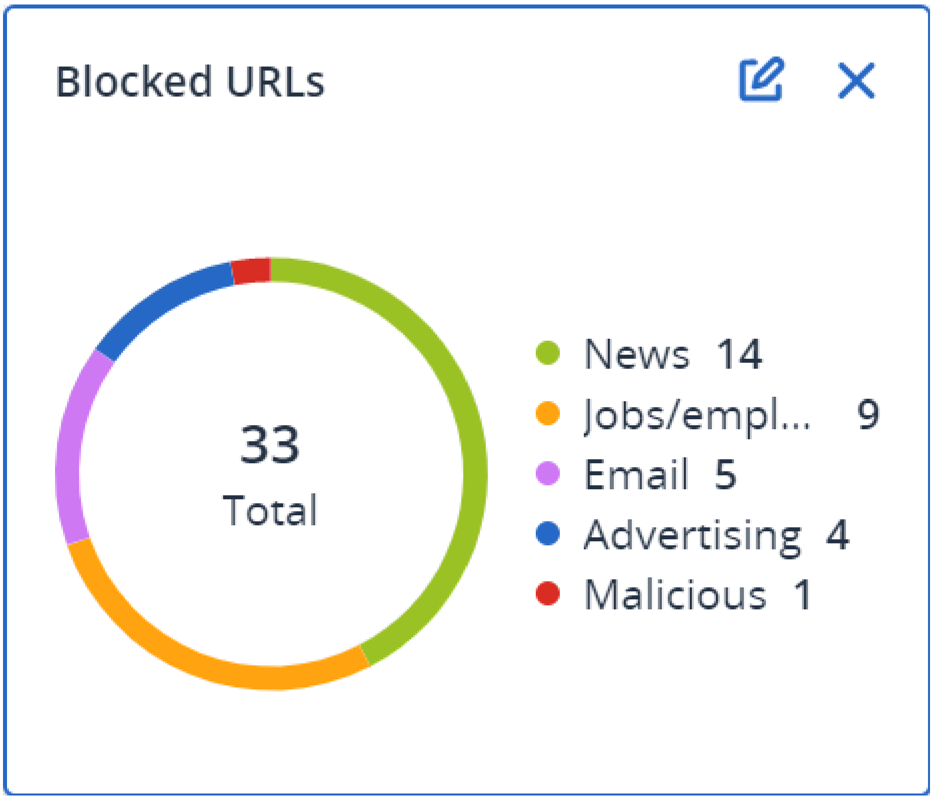
To download the data for the recently affected workloads

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

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

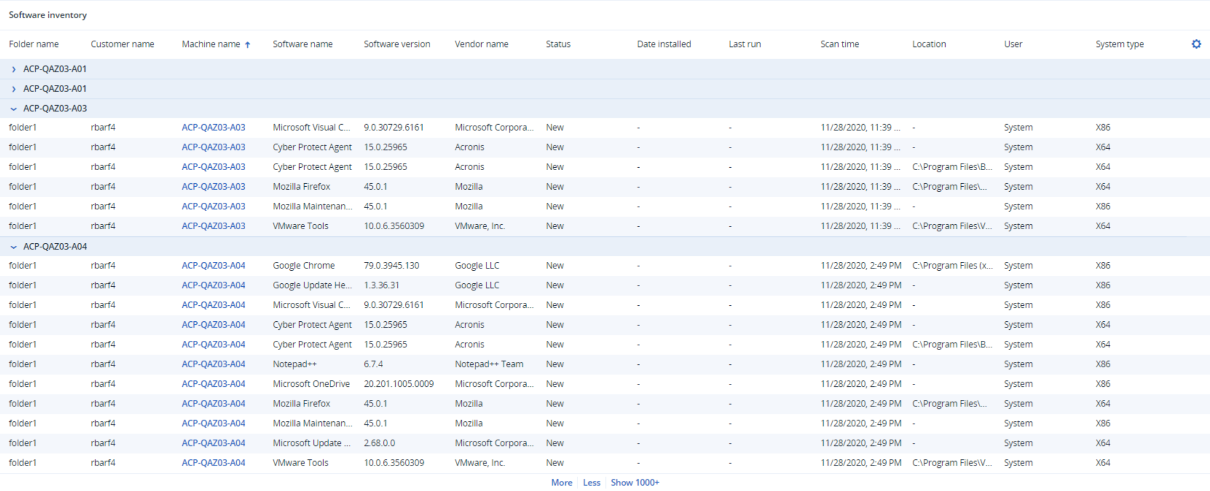
Blocked URLs

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



Software inventory widgets

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

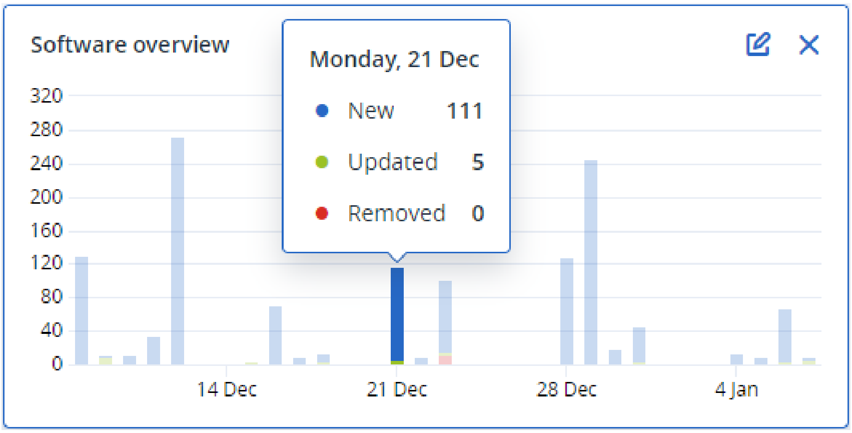


Software inventory

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

More | Less | Show 1000+

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.

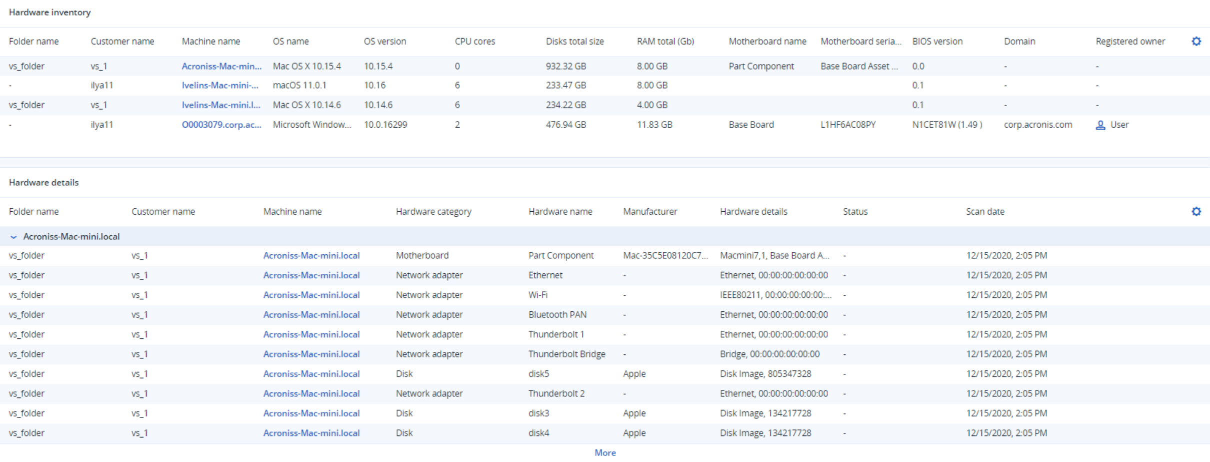
Updated - the number of updated applications.

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 Cyber Protect console. The information in the page is filtered for the corresponding date and status.

Hardware inventory widgets

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



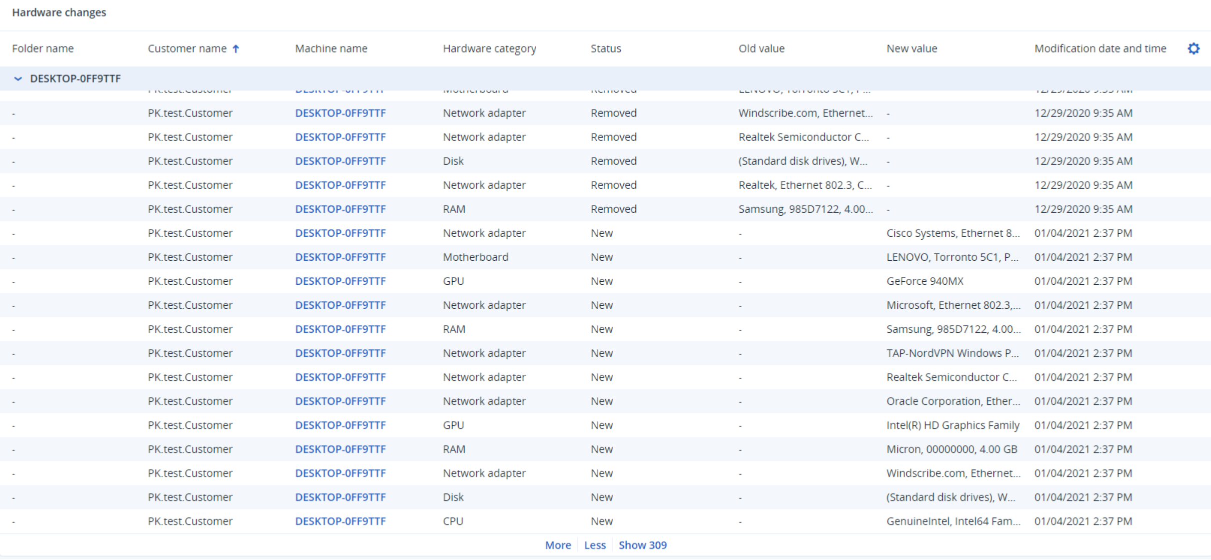
Hardware inventory

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

Hardware details

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

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

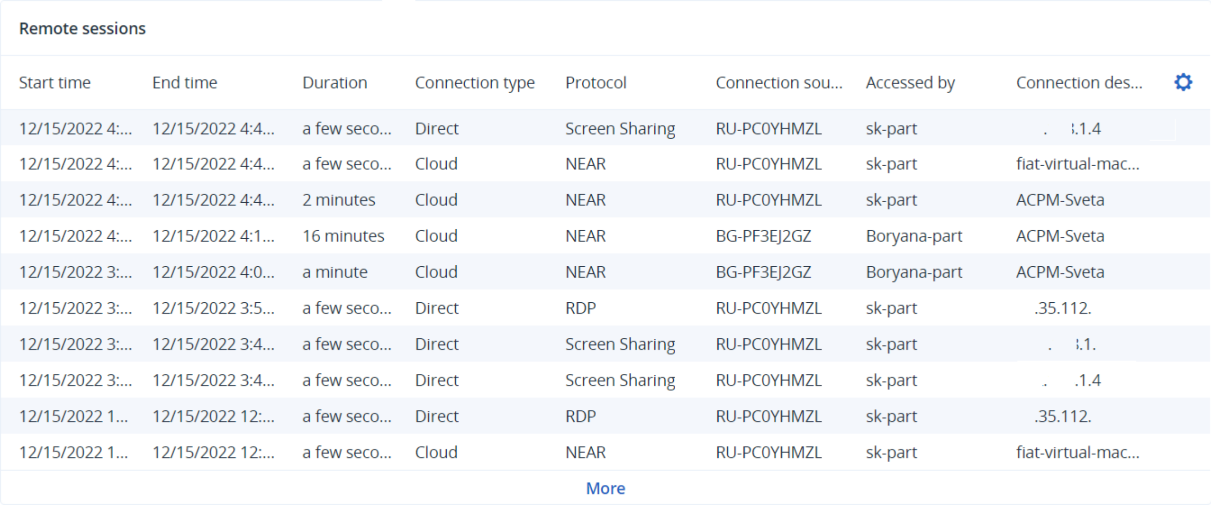


Hardware changes

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

Session history

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

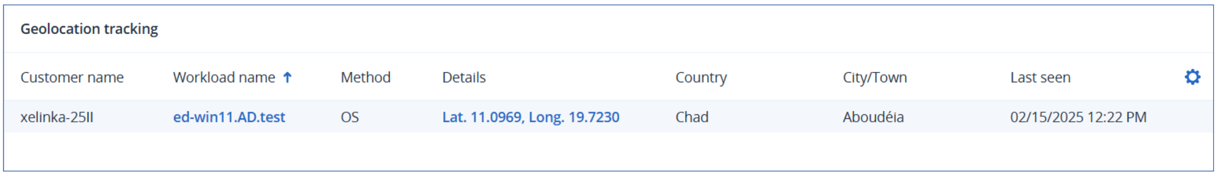


Remote sessions

Start time	End time	Duration	Connection type	Protocol	Connection sou...	Accessed by	Connection des...
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Direct	Screen Sharing	RU-PCOYHMZL	sk-part	. 3.1.4
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Cloud	NEAR	RU-PCOYHMZL	sk-part	fiat-virtual-mac...
12/15/2022 4:...	12/15/2022 4:4...	2 minutes	Cloud	NEAR	RU-PCOYHMZL	sk-part	ACPM-Sveta
12/15/2022 4:...	12/15/2022 4:1...	16 minutes	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 4:0...	a minute	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 3:5...	a few seco...	Direct	RDP	RU-PCOYHMZL	sk-part	.35.112.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PCOYHMZL	sk-part	. 3.1.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PCOYHMZL	sk-part	. .1.4
12/15/2022 1...	12/15/2022 12:...	a few seco...	Direct	RDP	RU-PCOYHMZL	sk-part	.35.112.
12/15/2022 1...	12/15/2022 12:...	a few seco...	Cloud	NEAR	RU-PCOYHMZL	sk-part	fiat-virtual-mac...

Geolocation tracking widget

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

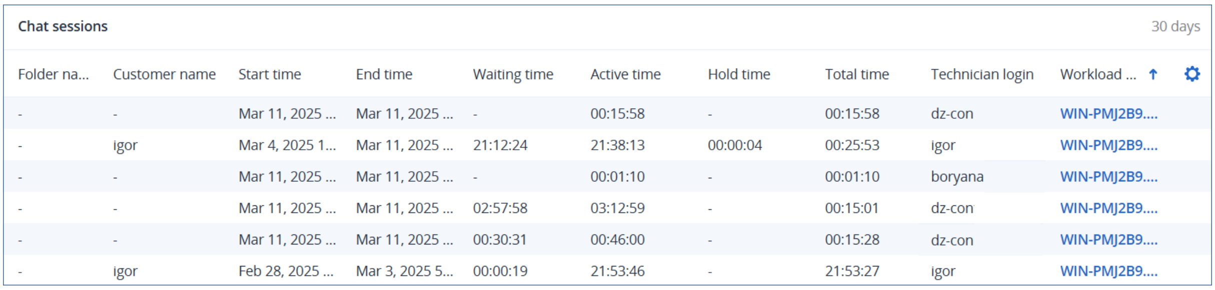


Geolocation tracking

Customer name	Workload name ↑	Method	Details	Country	City/Town	Last seen
xelinka-25II	ed-win11.AD.test	OS	Lat. 11.0969, Long. 19.7230	Chad	Aboudéia	02/15/2025 12:22 PM

Chat sessions widget

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



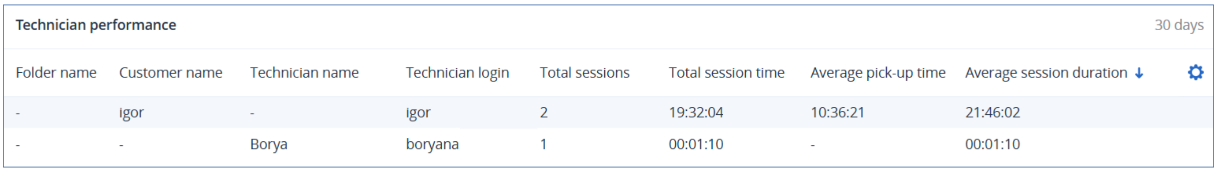
Chat sessions

30 days

Folder na...	Customer name	Start time	End time	Waiting time	Active time	Hold time	Total time	Technician login	Workload ... ↑
-	-	Mar 11, 2025 ...	Mar 11, 2025 ...	-	00:15:58	-	00:15:58	dz-con	WIN-PMJ2B9....
-	igor	Mar 4, 2025 1...	Mar 11, 2025 ...	21:12:24	21:38:13	00:00:04	00:25:53	igor	WIN-PMJ2B9....
-	-	Mar 11, 2025 ...	Mar 11, 2025 ...	-	00:01:10	-	00:01:10	boryana	WIN-PMJ2B9....
-	-	Mar 11, 2025 ...	Mar 11, 2025 ...	02:57:58	03:12:59	-	00:15:01	dz-con	WIN-PMJ2B9....
-	-	Mar 11, 2025 ...	Mar 11, 2025 ...	00:30:31	00:46:00	-	00:15:28	dz-con	WIN-PMJ2B9....
-	igor	Feb 28, 2025 ...	Mar 3, 2025 5...	00:00:19	21:53:46	-	21:53:27	igor	WIN-PMJ2B9....

Technician performance widget

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



Technician performance

30 days

Folder name	Customer name	Technician name	Technician login	Total sessions	Total session time	Average pick-up time	Average session duration ↓
-	igor	-	igor	2	19:32:04	10:36:21	21:46:02
-	-	Borya	boryana	1	00:01:10	-	00:01:10

Sales and billing

The **Sales and billing** dashboard provides a number of customizable widgets that give an overview of operations related to Advanced Automation (PSA).

By default, the data is displayed for the tenant in which you are operating, provided they have the Advanced Automation (PSA) service enabled.

The widgets have clickable elements that enable you to investigate and troubleshoot issues. You can also download the current state of the dashboard in the .pdf format, or send it via email to any address, including external recipients.

To rearrange the widgets on the dashboard

Drag and drop a widget by clicking on its name.

To edit a widget

Click the pencil icon in the top right corner of the widget. Editing a widget enables you to rename it.

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 **Customize** when the widget is selected. After editing the widget, click **Done**.

To remove a widget

Click the X sign next to the widget name.

Sales and billing widgets

This dashboard shows key metrics related to your current sales and billing, and includes:

- **Contracts to be invoiced**: This section displays the total amount of all current contract items that have not been billed for.
- **Sales items to be invoiced**: This section displays the total amount of all current sales Items that have not been billed for, including sales items in **Draft** status. You can switch to the Invoices screen and start a new billing run for these items by clicking **Start billing run**.
- **Number of end users being served**: This section displays the total number of end customer's users and contacts being served (including all active and inactive users and contacts).
- **Monthly services revenue per user**: This section displays the revenue value amount as a ratio of the *Contracts to be invoiced* divided by the *Number of end users being served*. You can switch to the Clients screen by clicking **Go to Clients**.
- **Net new MRR**: This graph displays three key metrics - MRR churn, MRR expansion, and net new MRR. The three metrics are displayed together by default but can be shown separately by clicking on the relevant metric name.
- **All sales items revenue**: This graph shows two key metrics - all sales items revenue that has been billed for, and all new sales items revenue. The two metrics are displayed together by default but can be shown separately by clicking on the relevant metric name.
- **Workloads**: This section displays the number of workloads under management, and the number of workloads that are included as part of a contract.

Service desk

The **Service desk** dashboard provides a number of customizable widgets that give an overview of service desk operations related to Advanced Automation (PSA).

By default, the data is displayed for the tenant in which you are operating, provided they have the Advanced Automation (PSA) service enabled.

The widgets have clickable elements that enable you to investigate and troubleshoot issues. You can also download the current state of the dashboard in the .pdf format, or send it via email to any address, including external recipients.

To rearrange the widgets on the dashboard

Drag and drop a widget by clicking on its name.

To edit a widget

Click the pencil icon in the top right corner of the widget. Editing a widget enables you to rename it.

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 **Customize** when the widget is selected. After editing the widget, click **Done**.

To remove a widget

Click the X sign next to the widget name.

Service desk widgets

The Service desk dashboard shows key metrics related to your current ticketing operations in a number of widgets. The dashboard displays metrics for service desk and quote tickets, but not for project tickets.

The dashboard includes:

- **Service desk**: This widget is displayed at the top of the page, and includes a number of key metrics:
  - **Open tickets**: Displays the total number of current tickets that are not in the **Closed** or **Solved** status.
  - **SLA breaches**: Displays the total number of tickets that are not **Closed** or **Solved**, and that breach an SLA. Click **View all SLA breaches** to view the relevant tickets.
  - **Unassigned tickets**: Displays the total number of current tickets that are not assigned to a technician.
  - **Tickets due today**: Displays the total number of current tickets due today. Click **Go to Tickets due today** to view the relevant tickets.
  - **Upcoming on-site visits**: Displays the total number of planned on-site visits. Click **Go to Upcoming on-site visits** to view the relevant tickets.
- **Closed tickets**: Displays the total number of closed tickets, which is then broken down to tickets for today, this month, and this year. The metrics are shown in two widgets, one for the current user, and one for the groups that the user is also a member of.
- **Net promoter score**: Displays the NPS score for the current month. The metrics are shown in two widgets, one for the current user, and one for the groups that the user is also a member of.
- **Ticket types**: Displays a pie chart and a breakdown in percentage values for all currently opened tickets per ticket type. The metrics are shown in two widgets, one for the current user, and one for the groups that the user is also a member of.
- **Ticket statistics**: Displays the total number of all closed tickets vs tickets with SLA breaches over the last seven days. The metrics are shown in two widgets, one for the current user, and one for the groups that the user is also a member of.

- **Occupancy rate**: Displays your organization's average technician occupancy rate over the last seven days. The metrics are shown in two widgets, one for the current user, and one for the groups that the user is also a member of.

Audit log

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

- Operations that are performed by users in the management portal
- Operations with cloud-to-cloud resources that are performed by users in the Cyber Protect console
- Cyber Scripting operations that are performed by users in the Cyber Protect console
- Operations related to email archiving
- System messages about reached quotas and quota usage

The log shows events in the tenant in which you are currently operating and its child tenants. You can click an event to view more information about it.

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

The log is cleaned up on a daily basis. The events are removed after 180 days.

Audit log fields

For each event, the log shows:

- **Event**

  Short description of the event. For example, **Tenant was created**, **Tenant was deleted**, **User was created**, **User was deleted**, **Quota was reached**, **Backup content was browsed**, **Script was changed**.
- **Severity**

  Can be one of the following:
  - **Error**

    Indicates an error.
  - **Warning**

    Indicates a potentially negative action. For example, **Tenant was deleted**, **User was deleted**, **Quota was reached**.
  - **Notice**

    Indicates an event that might need attention. For example, **Tenant was updated**, **User was updated**.
  - **Informational**

    Indicates a neutral informative change or action. For example, **Tenant was created**, **User was created**, **Quota was updated**, **Scripting plan was deleted**.
- **Date**

The date and time when the event occurred.

- **Object name**

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

  The name of the tenant that the object belongs to.
- **Initiator**

  The login of the user who initiated the event. For system messages and events initiated by upper-level administrators, the initiator is shown as **System**.
- **Initiator's tenant**

  The name of the tenant that the initiator belongs to. For system messages and events initiated by upper-level administrators, this field is empty.
- **Method**

  Shows whether the event was initiated via the web interface or via the API.
- **IP**

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

Filtering and search

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

Collecting performance data for Cyber Protection agents

For the protected Windows machines in your environment, you can collect performance logs manually or enable the automatic collection of diagnostic data if the system performance drops below the factory-defined thresholds. See "Performance thresholds for ETL data collection" (p. 125).

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

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

As a Partner administrator, you can enable the automatic collection of logs for randomly selected agents in your child tenants or for specific agents in an organization that you manage.

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

Note

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

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

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

Automated collection for multiple agents

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

Required role: Partner administrator, Customer administrator

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

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

Note

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

Automated collection for a single agent

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

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

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

Manual collection

To collect performance data manually

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

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

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

To collect the performance logs

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

The ETL traces are also included in the `sysinfo` package.

Performance thresholds for ETL data collection

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

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

Default thresholds for ETL data collection

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

Parameter	Description	Default value
"process-memory-consumption"	Threshold for memory overuse	
"allocated-memory-percent"		15
"minimum-allocated-memory-duration-seconds"		10
"allocated-memory-free-limit-seconds"		300
"process-disk-io"	Threshold for high disk I/O usage	

Parameter	Description	Default value
"maximum-operations-number"		10000
"maximum-transferred-bytes"		100000000
"estimation-period-seconds"		5
"process-file-io"	Threshold for high file I/O usage	
"maximum-operations-number"		30000
"maximum-transferred-bytes"		100000000
"estimation-period-seconds"		5
"process-cpu-usage"	Threshold for high CPU consumption	
"cpu-percent"		15
"estimation-period-seconds"		10
"acronis-component-thresholds"	Performance of protection agent components	
"behavioral-engine"	Threshold for the Behavior engine	
"average-system-utilization-percent"		50
"be-stats-event-number"		10
"avc-scan"	Threshold for the Antivirus and Antimalware protection component	
"average-scan-duration-seconds"	Maximum average scan duration	3
"estimation-period-seconds"		10
"maximum-scan-duration-seconds"	Maximum scan duration for a single scan	5

Reporting

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

Usage reports

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

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

Report type

You can select one of the following report types:

- **Current usage**

  The report contains the current service usage metrics.

  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.

  Note
  Local storage usage data is reported only at the unit and customer tenant levels. Users do not receive information about the local storage usage in the Summary reports.
- **Day-by-day for period**

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

Report scope

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

- **Direct customers and partners**

  The report will include the service usage metrics only for the immediate child 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.

Note

The filtration by date is done by the timestamp when the event was submitted to the cloud, not by the time of activity start or completion. Therefore, if the connection to the server was interrupted, a daily report might contain data for more than one day.

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**.

Sales and billing

The Sales and billing component of Advanced Automation (PSA) includes a number of reports which can be accessed from the **Reports** > **Sales and billing** menu.

Note
Sales and billing reports are available to users with the following roles: Administrator, Director, Group manager, Finance manager, HR.

Each Sales and billing report includes data within a specified time range, which can be changed as required.

The Sales and billing reports also separate the amount of a service "sold" (shown in the **Sold quantity** column, where relevant) according to the billing configuration and the amount of a service actually "used" (shown in the **Used quantity** column, where relevant). This ensures expenses are correctly calculated, as well as the profitability for sales and expenses. For example, when using contracts with minimum commitments, and you sell a customer 1 TB of storage (configured via the contract's minimum billable product quantity) but the customer only used 600 GB of storage this month, the report will show:

- **Sold quantity** = 1 TB
- **Used quantity** = 600 GB

As the actual usage was only 600 GB and not 1 TB, the report will show the correct profit for the month.

The Sales and billing reports available are:

- Customer revenue
- Expenses
- "Predictive profitability" (p. 131)
- Gross profit by customer
- Gross profit summary

Creating a new report

You can create a new report based on one of the available reports.

1. Click **Create new report**.
2. Select the relevant report.
   A new report is automatically created with the same name (suffixed with (1)).
3. [Optional] To update the report name, click **Settings**, and enter the new name. Then click **Save**.
   You can also clone and delete the report, as required.

Downloading a report

You can download any report by clicking the ellipsis icon (...) next to the time range selection, and selecting the required format:

- **PDF**
- **Excel and PDF** (only available for the Expenses report)
- **Excel** (only available for the Expenses report)

Customer revenue

The Customer revenue report enables you to track key sales metrics for each customer, including information for:

- All customers, selected one at a time.
- A specified time range.

To generate the Customer revenue report, go to **Reports** > **Sales and billing**, and then select **Customer revenue**. Then select the customer and relevant time period; for more information about customizing, downloading, and sending the report by email, see "Sales and billing" (p. 129).

The generated report includes the following widgets:

- Client spend, including:
  - Total amount recurring
  - Total amount non-recurring
  - Total amount VAR
  - Total amount
- Client average hourly rate, which shows the average hourly rate for tickets and projects for the selected period.

- Client time spent, including:
  - Time spent on fixed price basis.
  - Time spent on subsequent calculation basis.
  - Time spent on projects.
  - Time spent on other, non billable.
- Endpoints part of a contract, which shows the total number of endpoints that are part of contracts with the customer.
- Total endpoints under management, which shows the total number of the customer's endpoints under management.
- Number of end users being served, which shows the total number of customer's users being served.
- Contracts to be invoiced, which shows the total amount of all current contract items.
- Monthly services revenue per user, which shows the total amount as the contracts to be invoiced divided by the number of end users being served.
- Contract items, which displays a list of contract items including their full year value.

Expenses

The Expenses report shows information about the cost of products and services provided to customers, and includes:

- Sales and contract line items within the defined report period.
- Billed or not yet billed items (including sales items in **Pending** and **Draft** status).
- Specific customer information or a report for all customers.
- Specific product information or a report for all products.

To generate the Expenses report, go to **Reports > Sales and billing**, and then select **Expenses**. Then select the customer, product, expense type, and relevant time period; for more information about customizing, downloading, and sending the report by email, see "Sales and billing" (p. 129).

The generated report includes:

- A general summary section.
- A customer section, which is a line by line review of product names or services provided to a customer.

Predictive profitability

The Predictive profitability report shows information about future profitability, based on the following information:

- Current contracts and active contract periods.
- Current active contract line items and the periods defined for these line items.
- History of ticket-based activities.

- History of sales items.
- Current prices and costs of products and services.

To generate the Predictive profitability report, go to **Reports > Sales and billing**, and then select **Predictive profitability**. Then select the customer, product, and relevant time period; for more information about customizing, downloading, and sending the report by email, see "Sales and billing" (p. 129).

The generated report includes:

- A general summary section.
- A summary per month section, including the % month on month and year on year growth rates.
- A summary of the last six months.
- A customer section, which is a line by line review of product names or services provided to a customer.

Note
Sales items in the **Pending** or **Draft** status are included in the summary per month and customer sections. They are also calculated as part of the **Total cost**, **Total revenue**, and **Total profit** widgets.

Gross profit by customer

The Gross profit by customer report enables you to track the profits and costs for specific customers, including information for:

- All customers, selected one at a time.
- A specified time range.

To generate the Gross profit by customer report, go to **Reports > Sales and billing**, and then select **Gross profit by customer**. Then select the customer and relevant time period; for more information about customizing, downloading, and sending the report by email, see "Sales and billing" (p. 129).

The generated report includes:

- A summary section.
- A breakdown of each contract for the selected customer.
- An overview of the profitability of the customer's contracts, sales items, projects, and labor costs.

Gross profit summary

The Gross profit summary report provides you with an analysis of your profits and costs, including information for:

- All customers, including one line summaries for each customer.
- A specified time range.
- A specified aggregation period (month / quarter / year).

To generate the Gross profit summary report, go to **Reports > Sales and billing**, and then select **Gross profit summary**. Then select the relevant dates in the **Period** field; for more information about customizing, downloading, and sending the report by email, see "Sales and billing" (p. 129).

The report includes a main summary section of all the selected customers and time period, where the total profit for a customer is calculated as the difference between profits and costs.

Service desk

The Service desk component of Advanced Automation (PSA) includes a number of reports which can be accessed from the **Reports** > **Service desk** menu.

Note
Service desk reports are available to users with the following roles: Administrator, Director, Group manager, Finance manager, HR

Each Service desk report includes data within a specified time range, which can be changed as required.

The Service desk reports available are:

- "Customer tickets summary" (p. 134)
- Duration of finished tickets
- "NPS tracking" (p. 134)
- Number of updates in ticket
- SLA summary
- "Technician capacity planning" (p. 136)
- Technician performance metrics
- Tickets statistics
- Tickets with specific status
- "Timesheets" (p. 137)

Creating a new report

You can create a new report based on one of the available reports.

1. Click **Create new report**.
2. Select the relevant report.
   A new report is automatically created with the same name (suffixed with (1)).
3. [Optional] To update the report name, click **Settings**, and enter the new name. Then click **Save**.
   You can also clone and delete the report, as required.

Downloading a report

You can download any report by clicking the ellipsis icon (...) next to the time range selection, and selecting the required format:

- **PDF**
- **Excel and PDF** (only available for the Customer tickets summary report)
- **Excel** (only available for the Customer tickets summary report)

Customer tickets summary

The Customer tickets summary report provides a list of a specific customer's tickets and statistics for a defined period, including:

- Tickets created during the period. All service desk tickets are included in the report. Quote, project, and purchase order tickets are excluded from the report.

  The report preview initially displays up to 100 tickets in the ticket details. Click **More** to see more tickets.
- General statistics for the period, including the number of opened, closed, and SLA breached tickets, as well as ticket types and categories.
- Ticket details, including the number, title, category, priority, end-user, agent, SLA, and time spent on the ticket (billable, non-billable, or billed time).

To generate the Customer tickets summary report, go to **Reports** > **Service desk**, and select **Customer tickets summary**. Then select the relevant customer and time range in the **Customer** and **Period** fields.

You can also use the **Filter** tool to filter and customize the displayed list according to your requirements. For example, you can show or hide columns shown in the report, such as the time actually spent on a ticket, or SLA breaches.

For more information about customizing, downloading, and sending the report by email, see "Service desk" (p. 133).

Duration of finished tickets

The Duration of finished tickets report provides information about the duration of ticket resolutions, particularly the number of days between ticket creation and closure. This information enables you to pinpoint any excesses and manage them more efficiently.

To generate the Duration of finished tickets report, go to **Reports > Service desk**, and then select **Duration of finished tickets**. Then select the relevant dates in the **Period** field.

For more information about customizing, downloading, and sending the report by email, see "Service desk" (p. 133).

NPS tracking

The NPS (Net promoter score) tracking report displays ticket ratings based on end-user feedback. Once a ticket is closed, an email is automatically sent to users so that they can rate the service.

The report enables you to track a number of key client metrics, including:

- The percentage ratio of all promoters to all respondents.
- The number of promoter respondents (end-users) with set ticket ratings of 9 and 10.
- The percentage ratio of all neutrals to all respondents.
- The number of neutral respondents (end-users) with set ticket ratings of 7 and 8.
- The percentage ratio of all detractors to all respondents.
- The number of detractor respondents (end-users) with set ticket ratings from 0 to 6.
- The NPS value, which is calculated as an average rating for all respondents.

To generate the NPS tracking report, go to **Reports** > **Service desk**, and then select **NPS tracking**. Then select the relevant dates in the **Period** field; you can also select a specific client and client end-user, and a support agent and support group to fine-tune the report further.

For more information about customizing, downloading, and sending the report by email, see "Service desk" (p. 133).

Number of updates in ticket

The Number of updates in ticket report provides information on how many updates were made on tickets over a specific period of time, enabling you to locate tickets that are causing issues and not getting resolved quickly. For example, many updates may indicate a lack of knowledge from the engineer, with updates from both the engineer and end-user as they try to resolve the issue.

To generate the Number of updates in ticket report, go to **Reports > Service desk**, and then select **Number of updates in ticket report**. Then select the relevant dates in the **Period** field.

For more information about customizing, downloading, and sending the report by email, see "Service desk" (p. 133).

SLA summary

The SLA summary report enables you to review key SLA metrics per company, group and technician.

The following three key SLA metrics can be tracked in this report:

- First response SLA
- Next response time
- Resolution time

To generate the SLA summary report, go to **Reports > Service desk**, and then select **SLA summary**. Then select the relevant dates in the **Period** field; you can also select a specific user group and user to fine-tune the report further.

For more information about customizing, downloading, and sending the report by email, see "Service desk" (p. 133).

Technician performance metrics

The Technician performance metrics report enables you to track key technicians' performance metrics, including:

- Hours coverage, including available working hours and actual work time registered.
- Accountability, including the cost of employment (calculated by multiplying the number of hours worked by the cost of those hours).
- Work coverage for tickets, including tickets assigned and worked on by the selected technician, in addition to the top three tickets with the highest lead time.
- Work coverage for projects, including current projects worked on and closed projects completed / not completed within the budgeted time.
- NPS (net promoter score) for the technician, including the best / worst rated tickets.

To generate the Technician performance metrics report, go to **Reports > Service desk**, and then select **Technician performance metrics**. Then select the relevant dates in the **Period** field; you can also select a specific user to fine-tune the report further.

For more information about customizing, downloading, and sending the report by email, see "Service desk" (p. 133).

Technician capacity planning

The Technician capacity planning report enables you to track your engineers' workloads and their projected capacity over future periods. For each engineer included in the report, you can:

- View the total number of all available working hours (all available time minus weekends, approved PTOs, sick leave and public holidays) for the selected period.
- View the total number of all scheduled activities (including service desk and project activities) in days.
- View the total number of non-working days (including approved PTOs, sick leaves and public holidays) for the selected period.
- View the total time available for the selected period (calculated as working days minus all scheduled activities).

To generate the Technician capacity planning report, go to **Reports** > **Service desk**, and then select **Technician capacity planning**. Then, select the relevant dates in the **Period** field and the relevant group type in the **Reports group by** field; you can also select a specific engineer to fine-tune the report further.

For more information about customizing, downloading, and sending the report by email, see "Service desk" (p. 133).

Tickets statistics

The Ticket statistics report displays a graph of the total number of closed tickets and tickets that had an SLA breach. It displays the statistics for the current day, for the current month and the overall yearly statistics. The report enables you to quickly see the performance of your team and quickly identifies closed tickets versus breached tickets and if there was any improvement over the last months.

To generate the Tickets statistics report, go to **Reports > Service desk**, and then select **Tickets statistics**. Then select the relevant dates in the **Period** field; you can also select a specific client to fine-tune the report further.

For more information about customizing, downloading, and sending the report by email, see "Service desk" (p. 133).

Tickets with specific status

The Tickets with specific status report enables you to locate tickets in a specific status, belonging to a specific category, or of a certain priority.

To generate the Tickets with specific status report, go to **Reports > Service desk**, and then select **Tickets with specific status**. Then select the relevant dates in the **Period** field; you can also select a status, category, and/or priority to fine-tune the report further.

For more information about customizing, downloading, and sending the report by email, see "Service desk" (p. 133).

Timesheets

The Time management component of Advanced Automation (PSA) includes a Timesheet report which you can access from the **Reports** > **Service desk** menu. This report enables you to view the average work time that users have logged and provides a quick overview of how much time was spent on tickets and other things (such as manual time entries).

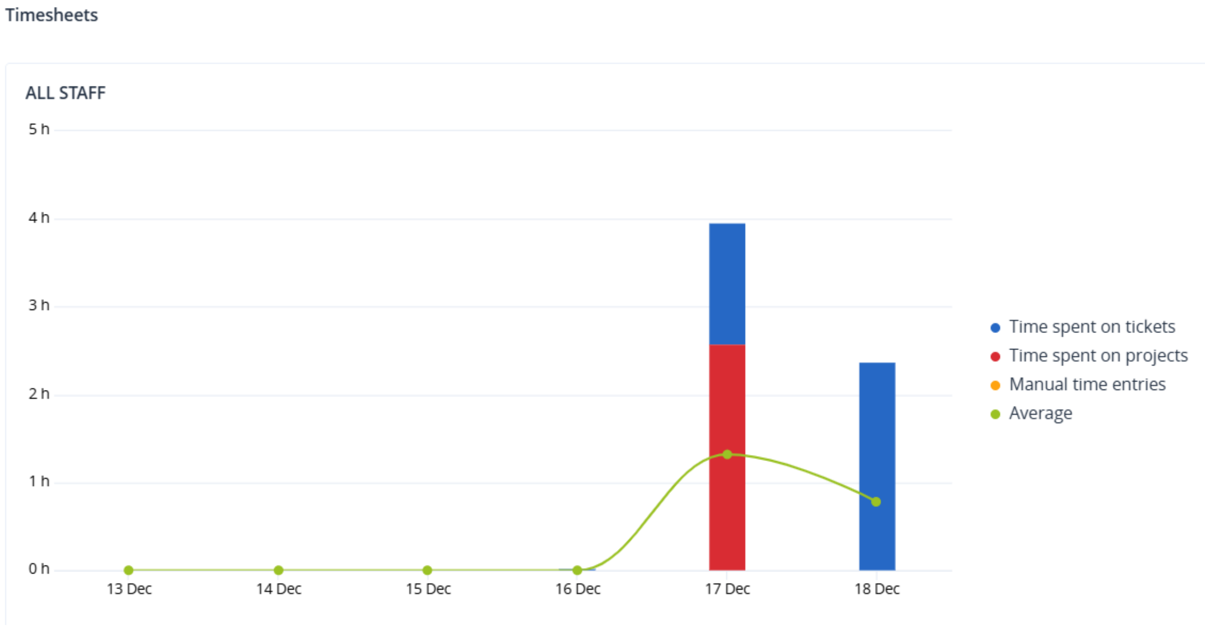
Note
The Timesheet report is available to users with the following roles: Administrator, Director, Group manager, Finance manager, HR

The Timesheet report includes data within a specified time range, which can be changed as required. The report consists of two main widget types:

- The **All Staff** widget, which includes a summary of all active users.
- Individual widgets for each user.

Each widget includes details on the average time logged during the selected period, the time spent on tickets, the time spent on projects, and the time allocated to manual time entries.

You can also add existing reports and widgets to the report to customize it according to your requirements, and download each report or send it via email in Excel (XLSX) or PDF format. See the relevant sections in "Service desk" (p. 133) for more information.



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. 154).

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

You can use default reports or create a custom report.

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

The default reports are listed below:

Report name	Description
#CyberFit Score by machine	Shows the #CyberFit Score, based on the evaluation of security metrics and configurations for each machine, and recommendations for improvements.
Alerts	Shows alerts that occurred during a specified time period.
Backup scanning details	Shows the detailed information about detected threats in the backups.
Daily activities	Shows the summary information about activities performed during a specified time period.
Data protection map	Shows the detailed information about the number, size, location,

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

Actions with reports

Add

To add a new report

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

View

To view a report

- To view a report, click its name.

Edit

To edit a report

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

Delete

To delete a report

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

Schedule

To schedule a report

1. In the Cyber Protect console, go to **Reports**.
2. In the list of reports, select the report that you want to schedule.
3. In the upper-right corner of the screen, click **Settings**.
4. Next to **Scheduled**, enable the switch.
   - Specify the email addresses of the recipients.
   - Select the format of the report.
   - **Note**
     You can export up to 1,000 items in a PDF file, and up to 10,000 items in a XLSX file. The timestamps in the PDF and XLSX files use the local time of your machine.
   - Select the language of the report.
   - Configure the schedule.
5. Click **Save**.

Download

To download a report

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

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

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

Send

To send a report

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

Export structure

To export the report structure

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

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

Dump data

To dump the report data

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

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

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

   Note
   Preparing CSV files for longer periods takes more time.

6. Click **Send**.

Executive summary

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

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

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

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

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

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

Executive summary widgets

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

Workloads overview widgets

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

Widget	Description
Cloud workloads protection status	This widget shows the number of protected and unprotected cloud workloads by type at the moment of the report's generation. Protected cloud workloads are cloud workloads on which at least one backup plan is applied. Unprotected cloud workloads are cloud workloads on which no backup plan is applied. The following cloud workload types are shown in the chart (in alphabetical order from A to Z): • Google Workspace Drive • Google Workspace Gmail • Google Workspace Shared Drive • Hosted Exchange mailboxes • Microsoft 365 mailboxes • Microsoft 365 OneDrive

Widget	Description
	• 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.
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).

Widget	Description
Workloads protection status	The widget shows the protected and unprotected workloads by type at the moment of the report's generation. Protected workloads are workloads on which at least one protection or backup plan is applied. Unprotected workloads are workloads on which no protection or backup plan is applied. The following workloads are counted: **Servers** - physical servers, and Domain Controller servers. **Workstations** - physical workstations. **Virtual machines** - both agent-based and agentless virtual machines. **Web hosting servers** - virtual or physical servers with installed cPanel or Plesk. **Mobile devices** - physical mobile devices. One workload can belong to more than one category. For example, a web hosting server is counted in two categories - **Servers**, and **Web hosting servers**.
Discovered devices	The widget shows the following information about the devices that were discovered in your customers' networks in a specified period: **Customer name** **Folder name** **Device name** **Device type** **Operating system** **Manufacturer** **Model** **IP address** You can edit the widget and filter the displayed information by tenant, organizational unit, device type, discovery type, first discovered date, last discovered date, IP address, MAC address, and discovery type.

Antimalware protection widgets

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

Widget	Description
Antimalware scan of files	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

Widget	Description
	Detected, quarantined - the total number of infected files that were quarantined **Detected, not quarantined** - the total number of infected files that were not quarantined **Devices protected** - The total number of devices with applied antimalware protection policy **Total number of registered devices** - The total number of registered devices at the time of the report's generation
Antimalware scan of backups	The widget shows the results from the antimalware scanning of the backups for the specified date range, using the following metrics: • Total number of scanned recovery points • Number of clean recovery points • Number of clean recovery points with unsupported partitions • Number of infected recovery points. This metric includes the number of infected recovery points with unsupported partitions.
Blocked URLs	For the specified date range, the widget shows the number of blocked URLs grouped by website category. The widget lists the seven website categories that have the biggest number of blocked URLs, and combines the rest of the website categories into **Other**. For more information about the website categories, see the URL filtering topic in Cyber Protection.
Security incident burndown	This widget shows the efficiency rate in closing incidents for the selected company; the number of open incidents are measured against the number of closed incidents over a period of time. Hover over a column to view a breakdown of the closed and open incidents for the selected day. The % value shown in parentheses indicates the increase or decrease in comparison to the previous time period.
Incident MTTR	This widget displays the average resolution time for security incidents. It indicates how quickly incidents are being investigated and resolved. Click on a column to view a breakdown of the incidents according to severity (**Critical**, **High**, and **Medium**), and an indication of how long it took to resolve the different severity levels. The % value shown in parentheses indicates the increase or decrease in comparison to the previous time period.
Threat status	This widget displays the current threat status for a company's workloads (regardless of the number of workloads), highlighting the current number of incidents that are not mitigated and that need investigating. The widget also

Widget	Description
	indicates the number of incidents that were mitigated (manually and/or automatically by the system).
Threats detected by protection technology	For the specified date range, the widget shows the number of detected threats grouped by the following protection technologies: • Antimalware scanning • Behavior engine • Cryptomining protection • Exploit prevention • Ransomware active protection • Real-time protection • URL filtering

Backup widgets

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

Widget	Description
Workloads backed up	The widget shows the total number of registered workloads by backup status. **Backed up** - number of workloads that were backed up (at least one successful backup was performed) during the report date range. **Not backed up** - number of workloads which were not backed up (no successful backup was performed) during the report date range.
Disk health status by physical device	The widget shows the aggregated health status of physical devices based on the health statuses of their disks. **OK** - This disk health status relates to values [70-100]. The status of the device is **OK** when all its disks are in status **OK**. **Warning** - This disk health status relates to values [30-70]. The status of a device is **Warning** when the status of at least one of its disks is **Warning**, and when there are no disks in status **Error**. **Error** - This disk health status relates to values [0-30]. The status of the device is **Error** when the status of at least one of its disks is **Error**. **Calculating disk data** - The status of the device is **Calculating disk data** when the statuses of its disks are not calculated yet.
Backup storage usage	For the specified time range, the widget shows the total number and total size of the backups in the cloud and local storage.

Vulnerability assessment and patch management widgets

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

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

Software widgets

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

Widget	Description
Installation status	This widget shows the total number of installation activities on your customers' managed devices, grouped by status. Clicking a segment of the donut chart redirects you to the **Activities** page, where only activities with the corresponding status are shown, ordered chronologically.
Uninstallation status	The widget shows the total number of uninstallation activities from your customers' managed devices, grouped by status. Clicking a segment of the donut chart redirects you to the **Activities** page, where only activities with the corresponding status are shown, ordered chronologically.

Widget	Description
Software installation history	This widget provides detailed status information about remote software installations on your customers' managed devices. Clicking a status in the **Installation status** column redirects you to the **Activities** page, where activities with the corresponding status are displayed in chronological order.
Software uninstallation history	The widget provides detailed status information about remote software uninstallations from your customers' managed devices. Clicking a status in the **Uninstallation status** column redirects you to the **Activities** page, where activities with the corresponding status are displayed in chronological order.

Disaster Recovery widgets

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

Widget	Description
Disaster Recovery statistics	The widget shows Disaster Recovery key performance metrics for the specified date range. **Production failovers** - the number of production failover operations for the specified time range. **Test failovers** - the total number of test failover operations that were performed during the specified time range. **Primary servers** - the total number of primary servers at the moment of the report's generation. **Recovery servers** - the total number of recovery servers at the moment of the report's generation. **Public IPs** - the total number of public IP addresses (at the moment of the report's generation). **Total compute points consumed** - the total number of compute points consumed during the specified time range.
Disaster Recovery servers tested	The widget shows information about the servers that are protected by Disaster Recovery and tested with test failover. The widget shows the following metrics: **Server protected** - the number of servers protected by Disaster Recovery (servers which have at last one recovery server) at the moment of the report's generation. **Tested** - the number of servers protected by Disaster Recovery which were tested using test failover during the selected time range, out of all servers protected by Disaster Recovery.

Widget	Description
	Not tested - the number of servers protected by Disaster Recovery which were not tested using test failover during the selected time range, out of all servers protected by Disaster Recovery. The widget also shows the size of the Disaster Recovery storage (in GB) at the moment of the report's generation. It is the sum of the backup sizes of the cloud servers.
Servers protected with Disaster Recovery	The widget shows information about the servers protected with Disaster Recovery and the unprotected servers. The widget shows the following metrics: The total number of servers registered in customer tenant at the moment of the report's generation. **Protected** - the number of servers protected by Disaster Recovery (have at least one recovery server and an entire server backup) out of all registered servers at the moment of the report's generation. **Unprotected** - the total number of unprotected servers out of all registered servers at the moment of the report's generation.

Data Loss Prevention widget

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

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

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

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

File Sync & Share widgets

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

Widget	Description
File Sync & Share statistics	The widget shows the following metrics: **Total cloud storage used** - The total storage usage of all users. **End users** - the total number of end users. **Average storage used per end user** - the average storage usage per end user. **Guest users** - the total number of guest users.
File Sync & Share storage usage by end users	The widget shows the total number of File Sync & Share end users who have a storage usage in the following ranges: • 0 - 1 GB • 1 - 5 GB • 5 - 10 GB • 10 - 50 GB • 50 - 100 GB • 100 - 500 GB • 500 - 1 TB • 1+ TB

Notary widgets

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

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

Widget	Description
	• 1000+ files
eSigned documents across end users	The widget shows the total number of eSigned documents and eSigned files for all end users. The users are grouped based on the number of eSigned documents and files that they have. • Up to 10 files • 11 - 100 files • 101 - 500 files • 501 - 1000 files • 1000+ files

Configuring the settings of the Executive summary report

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

To update the settings of the executive summary report

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

Creating an Executive summary report

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

To create an Executive summary report

1. In the management console, go to **Reports**>**Executive summary**.
2. Click **Create executive summary report**.
3. In **Report name**, type the name of the report.
4. Select the Recipients of the report.
   - If you want to send the report to all direct customers, select **Send to all direct customers**.
   - If you want to send the report to specific customers
     a. Clear the **Send to all direct customers**.
     b. Click **Select contacts**.
     c. Select the specific customers. You can use the Search to easily find a specific contact.
     d. Click **Select**.
5. Select Range: **30 days** or **This month**

6. Select file format: **PDF**, **Excel**, or **Excel and PDF**.
7. Configure the scheduling settings.
   - If you want to send the report to the recipients at specific date and time:
     a. Enable the **Scheduled** option.
     b. Click the **Day of the month** field, clear the Last day field, and click the date that you want to set.
     c. In the **Time** field, enter the hour that you want to set.
     d. Click **Apply**.
   - If you want to create the report without sending it to the recipients, disable the **Scheduled** option.
8. Click **Save**.

Customizing the Executive summary report

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

To add a section

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

To rename a section

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

To delete a section

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

To add a widget with default settings to a section

1. In the section where you want to add the widget, click **Add widget**.
2. In the **Add widget** window, click the widget that you want to add.

To add a customized widget to a section

1. In the section where you want to add the widget, click **Add widget**.
2. In the **Add widget** window, find the widget that you want to add, and click **Customize**.

3. Configure the fields as necessary.
4. Click **Add widget**.

To add a widget with default settings to the report

1. Click **Add item** > **Add widget**.
2. In the **Add widget** window, click the widget that you want to add.

To add a customized widget to the report

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

To reset the default settings of a widget

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

To customize a widget

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

Sending Executive summary reports

You can send an Executive summary report on demand. In this case, the **Scheduled** setting is disregarded, and the report is sent immediately. When sending the report, the system uses the Recipients, Range, and File format values that are configured in **Settings**. You can manually change these settings before sending the report. For more information, see "Configuring the settings of the Executive summary report" (p. 151).

To send an Executive summary report

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

   The system sends the Executive summary report to the selected recipients.

Time zones in reports

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

Report location and type	Time zone used in the report

Management portal > Monitoring > Operations (widgets)	The time of report generation is in the time zone of the machine where the browser is running.
Management portal > Monitoring > Operations (exported to PDF or xslx)	• The time stamp of the exported report is in the time zone of the machine that was used to export the report. • The time zone of the activities displayed in the report is UTC.
Management portal > Reports > Usage > Scheduled reports	• The report is generated at 23:59:59 UTC on the first day of the month. • The report is sent on the second day of the month.
Management portal > Reports > Usage > Custom reports	The time zone and date of the report is UTC.
Management portal > Reports > Operations (widgets)	• The time of report generation is in the time zone of the machine where the browser is running. • The time zone of the activities displayed in the report is UTC.
Management portal > Reports > Operations (exported to PDF or xslx)	• The time stamp of the exported report is in the time zone of the machine that was used to export the report. • The time zone of the activities displayed in the report is UTC.
Management portal > Reports > Operations (scheduled delivery)	• The time zone of the report delivery is UTC. • The time zone of the activities displayed in the report is UTC.
Management portal > Users > Daily recap about active alerts	• This report is sent once a day between 10:00 and 23:59 UTC. The time when the report is sent depends on the workload in the datacenter. • The time zone of the activities displayed in the report is UTC.
Management portal > Users > Cyber Protection status notifications	• This report is sent when an activity is completed. **Note** Depending on the workload in the datacenter, some reports might be sent with delays. • The time zone of the activity in the report is UTC.

Reported data according to widget type

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

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

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

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

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

Disk health overview	Actual
Disk health status	Actual
Disk health status by physical devices	Actual
eSigned documents across end users	Actual
Existing vulnerabilities	Historical
File Sync & Share statistics	Actual
File Sync & Share storage usage by end users	Actual
Hardware changes	Historical
Hardware details	Actual
Hardware inventory	Actual
Historical alerts summary	Historical
Locations summary	Actual
Missing updates by categories	Actual
Not protected	Actual
Notarized files across end users	Actual
Notary statistics	Actual
Patch installation history	Historical
Patch installation status	Historical
Patch installation summary	Historical
Patched vulnerabilities	Historical
Patches installed	Historical
Protection status	Actual
Recently affected	Historical
Remote sessions	Historical
Security incident burndown	Historical
Security incident MTTR	Historical
Servers protected with disaster recovery	Actual
Software inventory	Actual

Software overview	Historical
Threat status	Actual
Threats detected by protection technology	Historical
Top incident distribution per workload	Actual
Vulnerable machines	Actual
Workload network status	Actual
Workloads backed up	Historical
Workloads protection status	Actual

Estimating Cyber Protect Cloud costs with the calculator

If you are using a trial version of Cyber Protect Cloud, you can estimate your costs using the calculator.

Note

The Cyber Protect Cloud calculator is accessible from the management portal only for trial partners and not accessible for their customers or non-trial partners.

To estimate your Cyber Protect Cloud costs using the calculator

1. Click **Calculate Monthly Costs** in the bottom-left corner of the management portal.
2. Specify the following details for your planned load:
   - The number of your workloads by workload type. For example, specify the number of virtual machines, workstations, hosting servers, Google Workplace seats, mobile devices, and Microsoft 365 seats.
   - The details of your data storage, such as the location of your data center and storage amount.
3. [Optional] Specify advanced backup, security, or management options you plan to use, along with the number of workloads for each.
4. Select a licensing model: per-workload or per-GB.

You will see an estimated monthly cost on the right.

You can become a partner by clicking the corresponding button, engaging in a chat with a specialist, or requesting a Cloud Advisor to reach out to you directly—all from the calculator page.

You can also initiate communication with the sales department by clicking **Contact Sales** in the bottom-left corner of the management portal.

Copilot

Copilot is the in-product AI chat assistant. Copilot uses the official Cyber Protect Cloud documentation and licensing guide as a source and generates answers that assist you and guide you through the following tasks:

- Understanding how the product works.
- Understanding licensing topics.
- Understanding how to configure tenants.
- Understanding how to configure services.
- Start using the product with minimum effort.
- Getting fast answers of your questions about how to use the features.

If Copilot cannot answer your question, it can transfer the chat to a live specialist or submit a ticket, if a specialist is currently unavailable.

You can chat with live specialists not only in English, but in your native language too. Copilot will automatically translate all non-English messages, so that you can communicate with a specialist in any language.

You can unpin the chat window and move it anywhere inside the application window. Thus, you can adjust the location of the chat to the most convenient place for you.

Working with Copilot

Copilot can give you information about the product and licensing models and assist you in common configuration tasks. When you need more specialized assistance, Copilot can connect you to a live specialist. If currently there are no live specialists available, Copilot can create a ticket for you. A specialist will contact you regarding this ticket as soon as possible.

You can rate your chat with Copilot and leave feedback.

Start chat

To start a chat with Copilot

1. Click **Copilot**.
2. In the chat window that opens, do one of the following:
   - To get information regarding one of the predefined common topics or question, click it.
   - To get information about another topic or an answer to another question, type it in the message field, and then press Enter or click the arrow icon.
3. Repeat step 2 until you get the necessary information.
4. [Optional] To copy a Copilot's reply, click the copy icon under the reply.

   The text is copied to your machine's clipboard.

Chat with a live specialist

To start a chat with a live specialist

1. Click **Copilot**.
2. Open a new or existing chat.
3. Ask Copilot to connect you to a live specialist.
4. Chat with the specialist.

> **Note**
> If the specialist closes the chat, a feedback form will be displayed in the chat window.

Rate response

You can rate Copilot's responses in the chat.

To rate a response

1. Click **Copilot**.
2. In the chat window that opens, do one of the following:
   - To get information regarding one of the predefined common topics or question, click it.
   - To get information about another topic or an answer to another question, type it in the message field, and then press Enter or click the arrow icon.
3. To rate Copilot's response, do one of the following:
   - If the response was helpful, click the like icon under it.
   - If the response was not helpful, click the dislike icon under it.

Rate chat

You can rate a chat which contains responses from Copilot when you exit it.

To rate the chat

1. In an active chat window, click the **X** icon.

   The feedback form opens.
2. Rate your chat experience (ranging from 1-poor to 5-great).
3. In the text field, enter your feedback.

   > **Note**
   > This step is mandatory for scores 1-4, but you can skip it for score 5.

4. Click **Send feedback**.

   The chat window closes.

Exit chat

When you exit a chat with Copilot, the chat history is not deleted. You will be asked to rate your experience.

To exit a chat

1. In an active chat window, click the **X** icon.

   The feedback window opens. You can send feedback or skip it.

2. [Optional] If you do not want to send feedback, click **Skip**.

   The chat window closes. Until you delete the chat, you will be able to access it from the chat list. If you have not sent feedback, the form will also be displayed every time you close the chat.

Manage chat

You can view the list of chat sessions that you had with Copilot and delete the ones that you do not need anymore.

To view the chats list and delete a chat

1. Click **Copilot**.
2. Click the hamburger icon to see the list of chats.
3. Hover over the chat that you want to delete, and then click the trash bin icon.

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

  The Advanced Backup pack includes a number of separate licenses and quotas for workstations, servers, virtual machines, web hosting servers, Google Workspace seats, and Microsoft 365 seats.
- RMM
- Advanced Security + XDR (Extended detection and response)
- Advanced Data Loss Prevention
- Advanced Disaster Recovery
- Advanced Email Security
- Advanced File Sync & Share
- Advanced Security Awareness Training

  Enables teaching individuals about the risks and threats of information security, training them with simulated phishing emails, and providing them with the knowledge and skills necessary to protect themselves and their organization from cyber attacks.

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. A message will prompt users to contact their administrator to enable the required advanced feature set.

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

Included features and advanced packs in Cyber Protect services

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

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

Included and advanced features in the Protection service

Included and advanced features in the Protection service

Feature group	Included standard features	Advanced features
Security + XDR	• #CyberFit score • Vulnerability assessment • Antivirus and Antimalware protection: Cloud signature-based file detection (no real-time protection, only scheduled scanning)* • Antivirus and Antimalware protection: Pre-execution AI-based file analyzer, behavior-based Cyber Engine • Microsoft Defender management *To detect zero day attacks, Cyber Protect uses heuristic scanning rules and algorithms to look for malicious commands.	The Advanced Security + XDR pack includes XDR, Endpoint Detection and Response (EDR), and Managed Detection and Response (MDR): • Integrate with third party solutions, including Advanced Email Security, Microsoft 365 collaboration applications, and Microsoft Entra ID • Manage incidents in a centralized Incident page • Visualize the scope and impact of incidents • Recommendations and remediation steps • Check for publicly disclosed attacks on your workloads using Threat feeds • Store security events for 180 days • Managed Detection and Response (MDR) • Anti-ransomware protection: Active protection • Antivirus and antimalware protection with local signature-based detection (with real-time protection) • Exploit prevention • URL filtering • Endpoint firewall management • Forensic backup, scan backups for malware, safe recovery, corporate

Feature group	Included standard features	Advanced features
		allowlist • Smart protection plans (integration with CPOC alerts) • Centralized backup scanning for malware • Remote wipe • Microsoft Defender Antivirus • Microsoft Security Essentials • Backup scanning for malware of Microsoft 365 mailboxes For information on how to enable Advanced Security + XDR, see "Enabling Advanced Security + XDR" (p. 168).
Data Loss Prevention	• Device control	• Content-aware prevention of data loss from workloads via peripheral devices and network communication • Pre-built automatic detection of personally identifiable information (PII), protected health information (PHI), and Payment Card Industry Data Security Standard (PCI DSS) data, as well as documents in the “Marked as Confidential” category • Automatic data loss prevention policy creation with optional end user assistance • Adaptive data loss prevention enforcement with automatic learning-based policy adjustment • Cloud-based centralized audit logging, alerting, and end user notifications
RMM	For endpoints: • Group management • Centralized management of protection plans • Hardware inventory • Remote control • Remote actions • Concurrent connections per technician • Remote connection protocol: RDP	RMM pack includes the following features: For endpoints: • Patch management • Disk health • Software inventory • Vulnerability assessment of third-party products for Windows operating systems • Fail-safe patching

Feature group	Included standard features	Advanced features
	• Four monitors • Threshold-based monitoring • Show last logged-in user • Vulnerability assessment for Windows and macOS For Microsoft 365 seats: • Auditing of Microsoft 365 security posture with best practice baselines, user management, and user onboarding	• Cyber Scripting • Remote assistance • File transfer and sharing • Selecting a session to connect • Observing workloads in multi-view • Connection modes: control, view-only, and curtain • Connection via the Quick Assist application • Remote connection protocols: NEAR and Apple Screen Sharing • Session recording for NEAR connections • Screenshot transmission • Session history report • 24 monitors • Threshold-based monitoring • Anomaly-based monitoring • Remote software deployment by using DeployPilot • Vulnerability assessment for third-party Windows applications • Geolocation tracking • Helpdesk chat For Microsoft 365 seats: • Automatic and manual remediation of baseline deviations, and user offboarding
Email security	None	Real-time protection for your Microsoft 365 and Gmail mailboxes: • Antimalware Antispam • URL scan in emails • DMARC analysis • Anti-phishing • Impersonation protection • Attachments scan • Content disarm and reconstruction • Graph of trust See the configuration guide.

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

Pay as you go and advanced features in the Protection service

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

Feature group	Pay-as-you-go features	Advanced features
Backup	• File backup • Image backup • Applications backup	• One-click recovery • Continuous data protection • Backup support for Microsoft SQL

Feature group	Pay-as-you-go features	Advanced features
	• Network shares backup • Backup to cloud storage • Backup to local storage **Note** Fees for cloud storage usage are applicable.	Server clusters and Microsoft Exchange clusters – Always On Availability Groups (AAG) and Database Availability Groups (DAG) • Backup support for MariaDB, MySQL, Oracle DB, and SAP HANA • Data protection map and compliance reporting • Off-host data processing • Backup frequency for Microsoft 365 and Google Workspace workloads • Remote operations with bootable media • Direct backup to Microsoft Azure, Amazon S3, and Wasabi public cloud storage
File Sync & Share	• Store encrypted file-based content • Synchronize files across designated devices • Share folders and files with designated people and systems	• Notarization and e-signature • Document templates* *Backup of sync and share files
Physical Data Shipping	Physical Data Shipping functionality	N/A
Notary	• File notarization • File eSigning • Document templates	N/A

Note

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

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

For information about billing, see "Billing modes for Cyber Protect" (p. 9).

Advanced Data Loss Prevention

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

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

You might also want to review the Technical Specifications document.

Enabling Advanced Data Loss Prevention

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

To enable Advanced Data Loss Prevention

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

Advanced Security + XDR

The Advanced Security + XDR (Extended Detection and Response) pack provides a complete, natively integrated, highly efficient solution, purpose-built for MSPs.

Use Advanced Security + XDR to:

- Extend protection for client environments across vulnerable attack surfaces, with extensive visibility covering endpoints, email, Microsoft Entra ID, and Microsoft 365 applications (SharePoint, OneDrive, Teams), ensuring protection against sophisticated threat landscapes.
- Natively integrate across cybersecurity, data protection, and endpoint management. XDR is designed to protect vulnerable attack surfaces for unmatched business continuity.
- Improve efficiency, with the ability to easily launch, manage, scale, and deliver security services. In addition, XDR includes AI-based incident analysis and single-click response for easy investigation, a single agent and console for all services, and a customizable platform to integrate additional tools into your technology stack.

Note that the Advanced Security + XDR pack is comprised of Extended Detection and Response (XDR), Endpoint Detection and Response (EDR), and "Managed Detection and Response (MDR)" (p. 176), and protects your workloads continuously from all malware threats.

Enabling Advanced Security + XDR

As the partner administrator, you can enable the Advanced Security + XDR protection pack to provide Extended Detection and Response (XDR) functionality in client protection plans.

Note
Endpoint Detection and Response (EDR) also needs to be enabled in the protection plan for all workloads that you want to protect. For more information, see Enabling EDR.

To enable the Advanced Security + XDR pack

1. Log in to the management portal.

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

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

   The list of existing clients subscribed to the Protection service is displayed.
4. Click the relevant client you want to add the Advanced Security + XDR pack to.

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

Integrating Advanced Security + XDR with third party platforms

Advanced Security + XDR supports the following integrations:

- Perception Point
- Microsoft Entra ID
- Microsoft 365 services

To access your integrations, in the management portal go to **Integrations**.

Note
This functionality is only available for users assigned the Administrator role.

Integrating with Perception Point

This topic describes how to integrate Perception Point with Advanced Security + XDR.

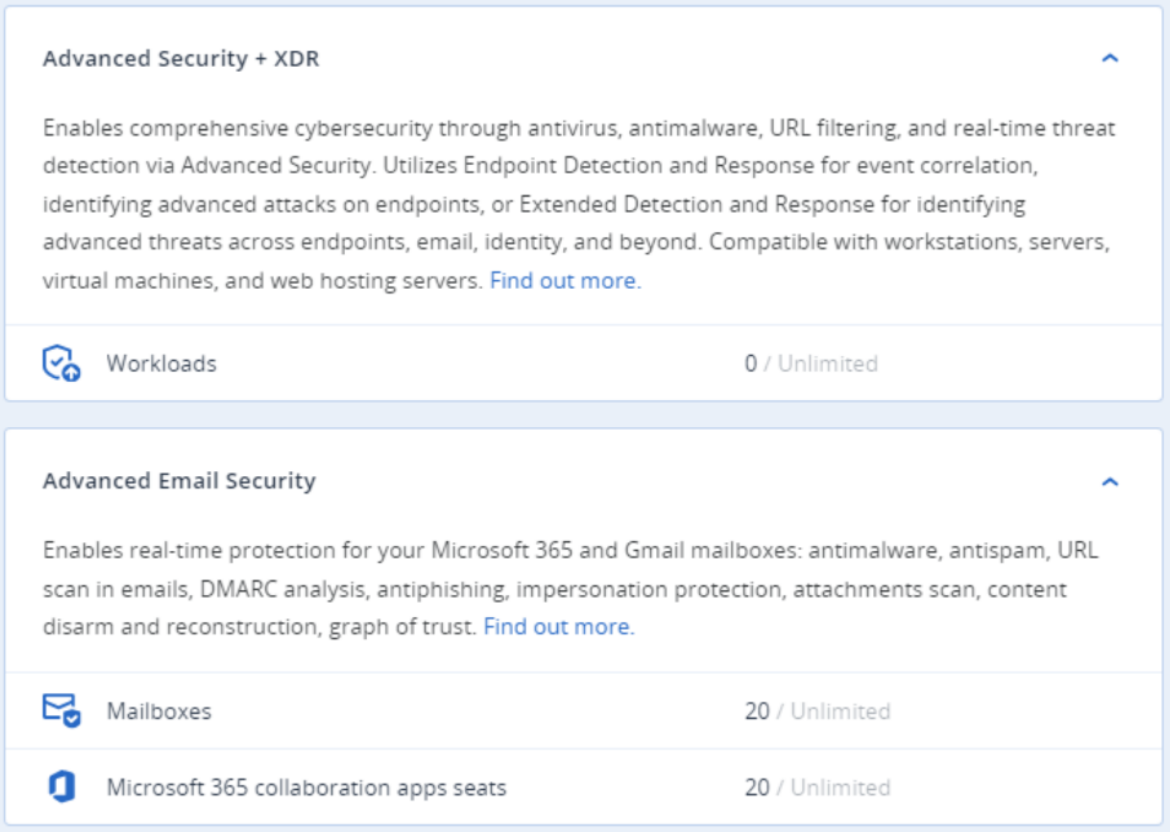
This integration enables you to offer an Extended Detection and Response (XDR) solution to customers who use Microsoft 365 for their email security and collaboration apps. The XDR integration enriches the functionality of the existing Endpoint Detection and Response (EDR) solution with Perception Point.

There are three main steps to integrate Perception Point with Advanced Security + XDR:

1. Enable the required advanced protection packs.
2. In Perception Point, configure email security and/or collaboration app channels and extract an API key.
3. Enable Perception Point XDR integration for customers.

To enable the required advanced protection packs

1. In the management portal, access the relevant customer that you want to activate the integration for.
2. Enable the Advanced Security + XDR pack and the Advanced Email Security pack. For more information, see "Advanced Protection packs" (p. 161).



Advanced Security + XDR

Enables comprehensive cybersecurity through antivirus, antimalware, URL filtering, and real-time threat detection via Advanced Security. Utilizes Endpoint Detection and Response for event correlation, identifying advanced attacks on endpoints, or Extended Detection and Response for identifying advanced threats across endpoints, email, identity, and beyond. Compatible with workstations, servers, virtual machines, and web hosting servers. Find out more.

Workloads 0 / Unlimited

Advanced Email Security

Enables real-time protection for your Microsoft 365 and Gmail mailboxes: antimalware, antispam, URL scan in emails, DMARC analysis, antiphishing, impersonation protection, attachments scan, content disarm and reconstruction, graph of trust. Find out more.

Mailboxes 20 / Unlimited

Microsoft 365 collaboration apps seats 20 / Unlimited

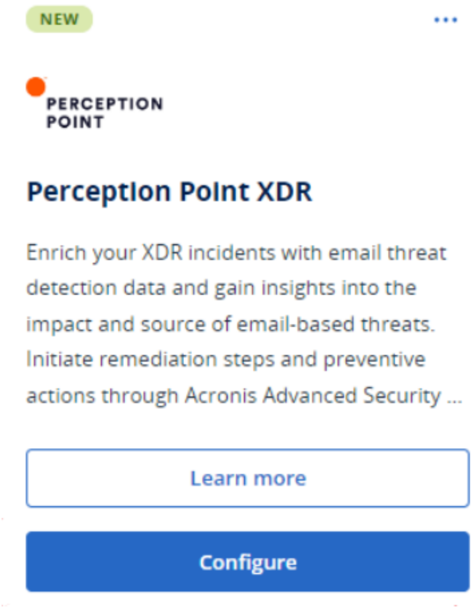
To configure email security and/or collaboration app channels and extract an API key in Perception Point

1. In the management portal, access the relevant customer that you want to activate the integration for, and then click **Manage service** to open the Cyber Protect console.
2. Go to **Email security**, and then click **Go to the email security console** to open Perception Point.
3. Create the relevant email security and/or collaboration app channels in Perception Point. For more information, see the Perception Point documentation.

4. In the left navigation menu, click **Profile**.
5. In the **Security** section, click the copy icon next to the API key. This key is used to enable the XDR integration, as described in the following procedure.

To enable Perception Point XDR integration for customers

1. In the management portal, go to **Integrations**.
2. Search for the **Perception Point XDR** integration and, in the displayed tile, click **Configure**.



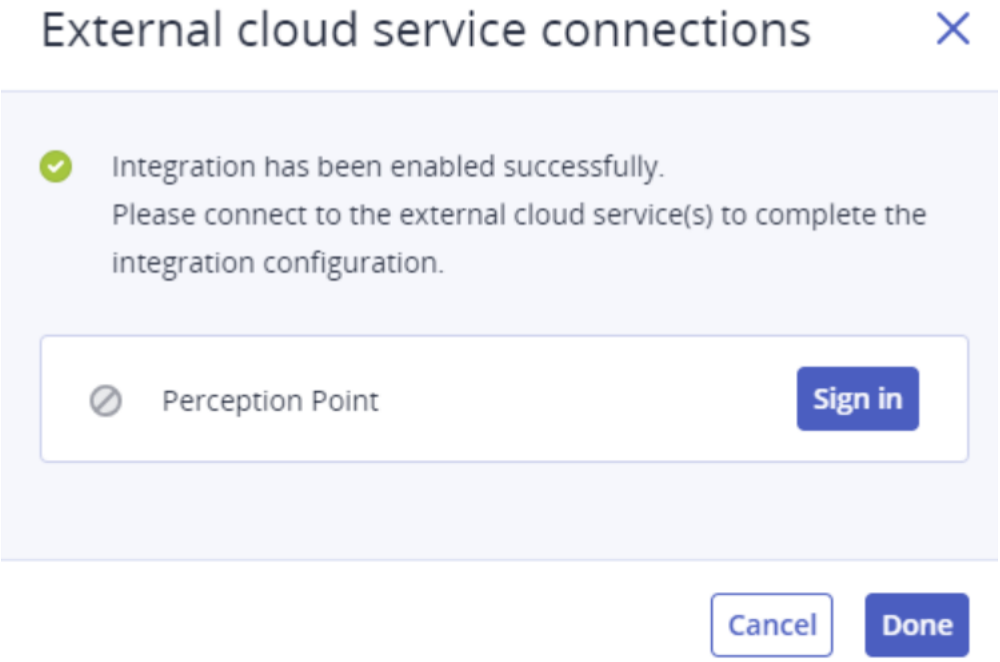
NEW

PERCEPTION POINT

Perception Point XDR

Enrich your XDR incidents with email threat detection data and gain insights into the impact and source of email-based threats. Initiate remediation steps and preventive actions through Acronis Advanced Security ...

3. Click the **Customer Management** tab, select a customer you want to enable the XDR integration for, and click **Enable**.
4. In the displayed dialog, click **Sign in**.



External cloud service connections

Integration has been enabled successfully.
Please connect to the external cloud service(s) to complete the integration configuration.

Perception Point

5. Enter the Perception Point API key you copied in the previous procedure, and then click **Done**.
6. To ensure the integration is up and running, verify that the **Enablement state** column shows **Enabled** and the **Service connection(s)** column shows **1 of 1** (a connection is running).

Integrating with Microsoft 365 services

This topic describes how to integrate Microsoft 365 services with Advanced Security + XDR.

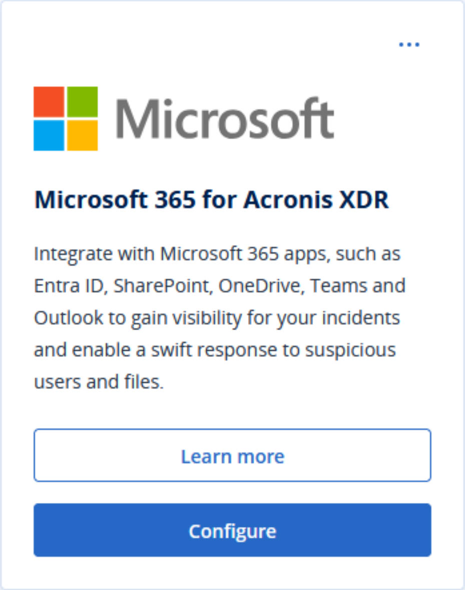
This integration provides enriched metadata to Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) incidents to those end customers using Microsoft 365 for their collaboration applications. The integration also provides details on the authenticated user affected by the incident. You can also perform response actions, such as blocking or limiting access for the user account.

Important
You must have one of the following licenses in order for the integration to work correctly:

- Microsoft 365 Business Standard
- Microsoft 365 Business Premium
- Office 365 E1
- Office 365 E3
- Microsoft 365 E3
- Microsoft 365 E5

To integrate with Microsoft 365 services

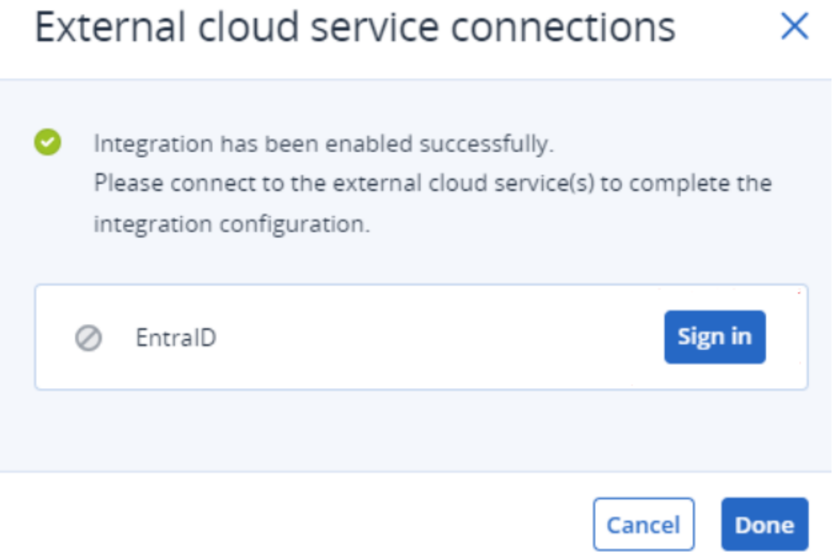
1. Go to the Microsoft Azure portal and login as the customer tenant.
2. Follow the onscreen instructions to create a new application, and assign the necessary roles for the new application. For more information about configuring Microsoft 365 API access, see this knowledge base article.
3. In the management portal, verify that the relevant customer tenant has the **Workpack** option under the Advanced Security + XDR pack enabled.
4. Go to **Integrations**, and search for the **Microsoft 365 XDR** integration.
5. On the **Microsoft 365 for XDR** catalog tile, click **Configure**, and then click **Enable**.



Microsoft 365 for Acronis XDR

Integrate with Microsoft 365 apps, such as Entra ID, SharePoint, OneDrive, Teams and Outlook to gain visibility for your incidents and enable a swift response to suspicious users and files.

6. Click the **Customer management** tab, select the customer tenant(s) you want to enable the integration for, and then click **Enable**.
7. Define the following:
   - **Custom domain**: If the customer is using a custom domain in Microsoft 365, enter it here. If no custom domain is in use, leave this field empty.
   - **Region**: Select the relevant region for Microsoft 365 tenants from the dropdown list.
8. Click **Enable**. In the displayed dialog, click **Sign in**.



External cloud service connections

Integration has been enabled successfully.
Please connect to the external cloud service(s) to complete the integration configuration.

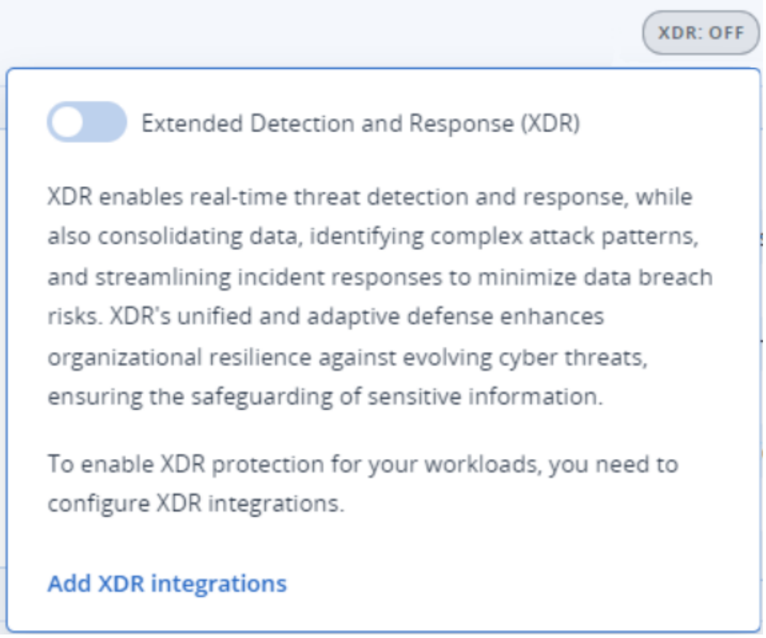
9. Enter the following:
   - **ID**: The object ID of the application you created in step 2.

     Note
     In Microsoft 365, make sure that you copy the object ID from the **App registrations** > **Overview** page by clicking the app name link in the **Managed application in local directory** field, and then selecting the object ID on the displayed page. Do not copy the object ID displayed on the main **App registrations** > **Overview** page.

   - **Secret**: The API client secret created for the application.
   - **Tenant ID**: The Microsoft 365 tenant.
10. Click **Sign in**, and then click **Done**.

    To ensure the connection is successful, verify that the **Service connection(s)** column shows **1 of 1** (a connection is running).
11. Go to **Clients**, select the relevant customer you want to enable XDR for, and click **Manage service**.

    The Cyber Protect console is displayed.
12. Go to **Protection**, and then click **XDR: Off**.
13. In the displayed popup, click the toggle switch to enable XDR.



Extended Detection and Response (XDR)

XDR enables real-time threat detection and response, while also consolidating data, identifying complex attack patterns, and streamlining incident responses to minimize data breach risks. XDR's unified and adaptive defense enhances organizational resilience against evolving cyber threats, ensuring the safeguarding of sensitive information.

To enable XDR protection for your workloads, you need to configure XDR integrations.

Incidents that include a workload registered in Microsoft 365 will now include enriched XDR information and response actions for this user.

Integrating with Fortinet

This topic describes how to integrate Fortinet with Advanced Security + XDR.

This integration provides enriched metadata to Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) incidents by ingesting and correlating events from Fortinet security software and appliances.

Important
Customers must have a FortiGate Cloud Service license for the relevant network for the integration to work correctly.

There are three main steps to integrate Fortinet with Advanced Security + XDR:

- Enable the Advanced Security + XDR pack.
- Configure Fortinet to work with Acronis.
- Enable the integration in the Management Portal.

To enable the Advanced Security + XDR pack

1. In the Management Portal, access the relevant customer that you want to activate the integration for.
2. Ensure the Advanced Security + XDR pack is enabled. For more information, see "Advanced Protection packs" (p. 161).

To configure Fortinet to work with Acronis

1. Log in to your FortiGate or FortiGate Cloud Service account.
2. For response actions to block a URL or IP address:
   - Go to **Security Profiles** > **Web Filter**, and define a filter with the name **Acronis Web Filter**. Then under the **Static URL Filter** section, click the **URL Filter** switch to enable it.
   - Go to **Policy & Objects** > **Firewall Policy**, and ensure the **Acronis Web Filter** is added to the relevant policy (in the **Security Profiles** section).

   When the response action is initiated, the reputation is received from Fortinet, even if the Web Filter and the Firewall Policy are not defined. Adding the Web Filter ensures the URL or IP address can be blocked.

   Note
   If the **Acronis Web Filter** is not defined or located, the block response action is not shown in the XDR graph.

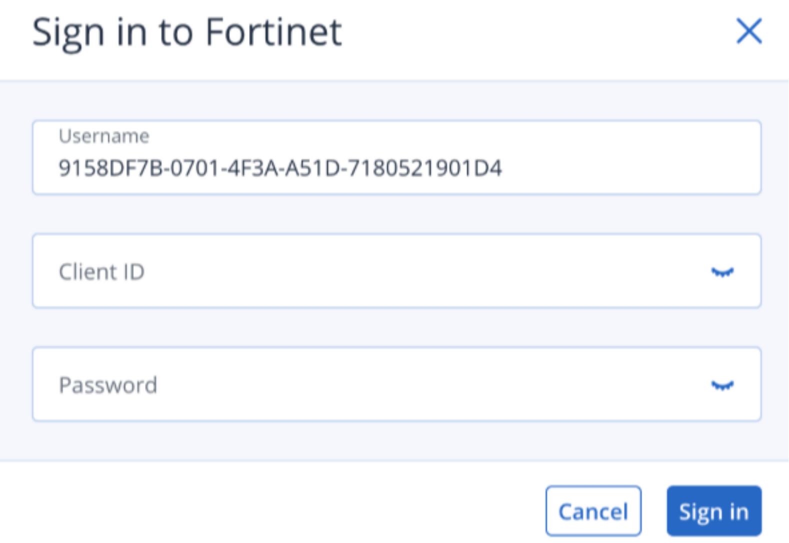
3. To isolate an endpoint:
   - Go to **Policy & Objects** > **Firewall Policy**, and define two policies for blocking and accepting outgoing connections (for Acronis domains and IP addresses).
   - Go to **Policy & Objects** > **Addresses**, and in the **Address Groups** tab, define the following:
     - The **Acronis Isolated Group**, where blocked addresses are automatically stored. The **Acronis Isolated Group** is a **Group** type, and should be linked to the blocking policy.
     - The **Acronis Allowed Hosts** group is where allowed addresses and domains are stored. The **Acronis Allowed Hosts** is a **Group** type, and should be linked to the policy that accepts outgoing connections. For example, the **Acronis Isolated Group** should be added

to the **Source** field in the policy, and the **Acronis Allowed Hosts** group should be added to the **Destination** field.

> **Note**
> The Acronis datacenter addresses and ports required for the Acronis agent to work, are listed here.

To enable Fortinet XDR integration for customers

1. In the Management Portal, go to **Integrations**.
2. Search for the **Fortinet XDR** integration and, in the displayed tile, click **Configure**.
3. Click the **Customer management** tab, select a customer you want to enable the XDR integration for, and click **Enable**.
4. In the dialog, enter the relevant Fortinet username, client ID, and password.

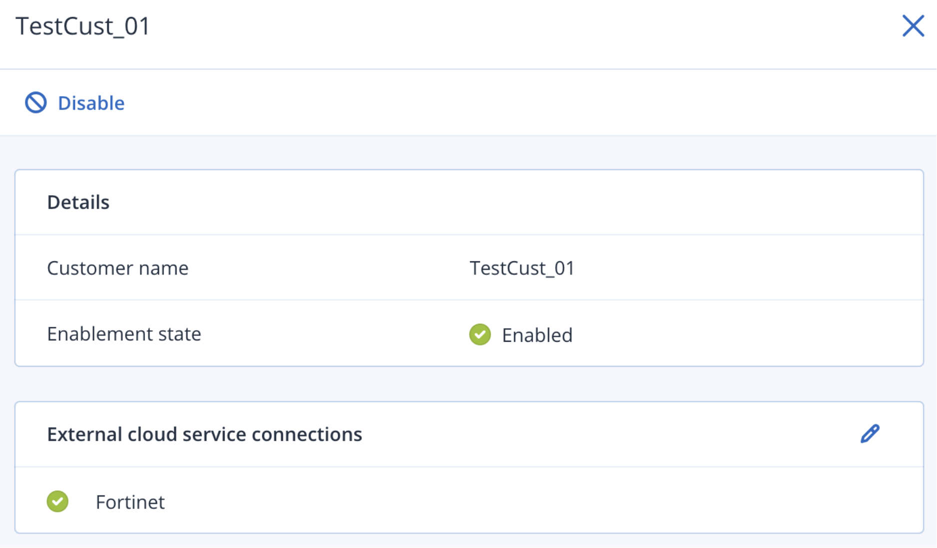


Sign in to Fortinet

Username
9158DF7B-0701-4F3A-A51D-7180521901D4

> **Note**
> The Fortinet credentials are generated when you create the IAM API user and set administrator permissions for FortiGate Cloud. For more information, see the FortiGate Cloud documentation. Alternatively, if you are a Fortinet client and have access to their development network pages, see this documentation.

5. Click **Sign in**.
6. To ensure the integration is up and running, click the relevant customer row, and verify that the **Enablement state** field shows **Enabled**.



TestCust_01

Details

Customer name	TestCust_01
Enablement state	✓ Enabled

External cloud service connections

✓ Fortinet

7. [Optional] To update the Fortinet username, client ID, and password, click the pencil icon in the **External cloud service connections** section.

To disable the Fortinet XDR integration

1. In the Management Portal, go to **Integrations**.
2. Search for the **Fortinet XDR** integration and, in the displayed tile, click **Configure**.
3. Click the **Customer management** tab, select a customer you want to disable the XDR integration for, and click **Disable**.

Managed Detection and Response (MDR)

MDR provides a 24/7 service for MSPs who have no in-house security expertise or need additional assistance to investigate and respond to security incidents detected by Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR).

The MDR functionality is enabled in the management portal under the Advanced Security + XDR pack, and the MDR service is provided by an external MDR vendor. When MDR is enabled for a specific customer, the MDR vendor receives incident data from Acronis for workloads where EDR or XDR is enabled in protection plans belonging to that customer. The MDR vendor then performs different levels of service to triage the incidents using the available response actions. For more information, see "What is Managed Detection and Response (MDR)?" (p. 176)

For more information about working with XDR, see Extended Detection and Response (XDR).

For more information about working with EDR, see Endpoint Detection and Response (EDR).

What is Managed Detection and Response (MDR)?

MDR is a service provided by third party vendors that uses a combination of skilled analysts, integrated tools, threat intelligence and technologies from both the vendor and Acronis to monitor for and respond to potential security threats and breaches.

When MDR is enabled for customers in the management portal, Acronis forwards incident telemetry to the MDR vendor to conduct investigation and response activities on these incidents. Note that only incidents that are not automatically mitigated are forwarded to the MDR vendor.

Key components of MDR

MDR is composed of three main components:

- Monitoring
- Isolation
- Response and remediation

Monitoring

MDR vendors monitor the detected security alerts and notifications from the customer's endpoint. The vendor then correlates and prioritizes these alerts with common threats, threat intelligence and third-party threat intelligence using analytics, security orchestration and responses. As a result, the vendor determines whether the alerts or notifications are a breach or compromise.

Any security events that the MDR vendor believes may pose a potential security threat are escalated into a customer-facing security incident and made available in the Cyber Protect console. The vendor provides context on the severity of the threat and the recommended remediation (including any action which has already been taken).

Isolation

MDR vendor analysts leverage pre-defined playbooks to initiate responses for endpoint isolation. Any response actions by the MDR vendor are reflected in the relevant security incident. The decision to isolate an endpoint is reached by drawing on data from the endpoint, with further input from threat intelligence and threat research.

Response and remediation

Response and remediation activities occur after the initial monitoring and isolation activities are completed. After a security incident is detected, the MDR vendor initiates responses according to the security incident. Responses and remediation activities include:

- Guidance on how to mitigate, stop or prevent a security incident based on the data, intelligence and advisories provided.
- Analysis and investigation of security events to determine the root cause and extent of the compromise.
- The performing of approved workflows (as defined in the MDR vendor's response playbooks) to isolate workloads, quarantine threats, or fully remediate the threat.
- Providing the service provider with a more detailed security escalation, citing the customer-facing security incident, threat intelligence and advisories.
- Escalating incidents through various channels, including the creation of a security incident, email notifications and phone calls, all via the contact details provided by the customer.

- Maintaining a line of communication with the customer until the threat has been remediated, providing timely updates as new information arises.
- Where response actions are outside the scope of the MDR service, the MDR vendor provides recommendations on areas to focus. This may include recommendations for additional services, such as incident response.

Enabling Managed Detection and Response (MDR)

You enable MDR for selected customers by performing the following two steps:

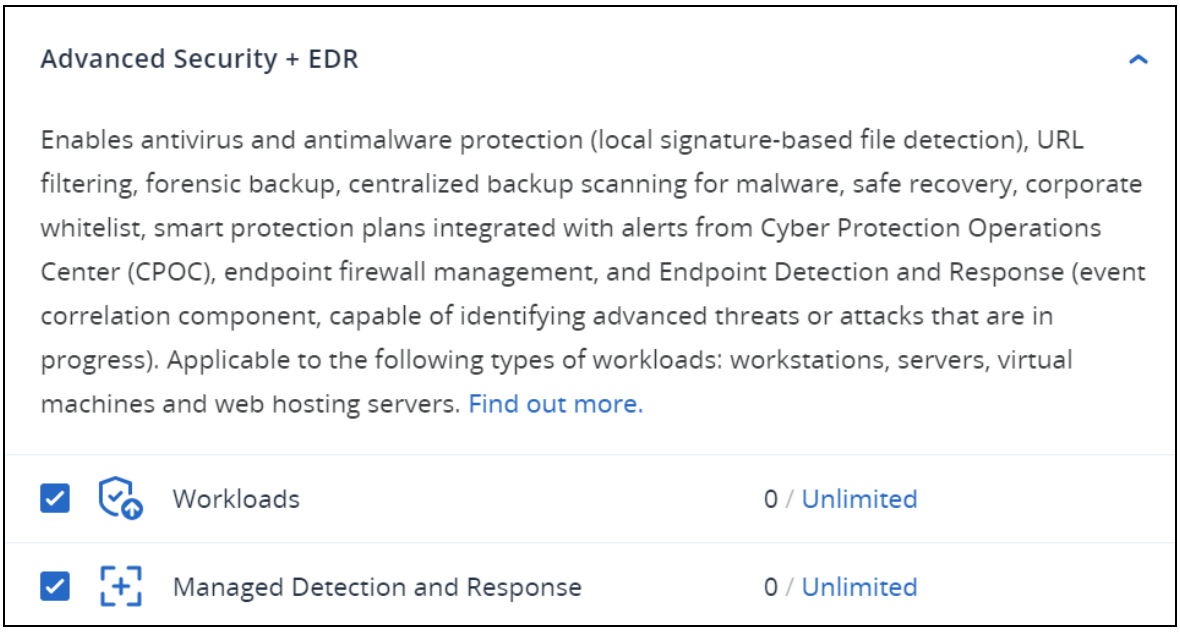
- Step 1: Enable the MDR offering item for customers.
- Step 2: Configure the integration with the MDR vendor's app.

Note
Self-managed customers cannot enable MDR. For more information about configuring self-managed customers, see "Configuring self-managed customer profile" (p. 49).

In addition, only one MDR vendor per customer can be selected, but you can change the selected MDR vendor, as and when required. You can also use different MDR vendors for different customers.

To enable MDR for selected customers

1. In the management portal, go to **Clients**.
2. Click the ellipsis icon (...) next to the relevant customer, and select **Configure**.
3. In the **Protection** tab, click **Edit**.
4. In the **Advanced Security + EDR** section, ensure that the **Workloads** and **Managed Detection and Response** checkboxes are selected. Then click **Save** to apply any changes.



Advanced Security + EDR

Enables antivirus and antimalware protection (local signature-based file detection), URL filtering, forensic backup, centralized backup scanning for malware, safe recovery, corporate whitelist, smart protection plans integrated with alerts from Cyber Protection Operations Center (CPOC), endpoint firewall management, and Endpoint Detection and Response (event correlation component, capable of identifying advanced threats or attacks that are in progress). Applicable to the following types of workloads: workstations, servers, virtual machines and web hosting servers. Find out more.

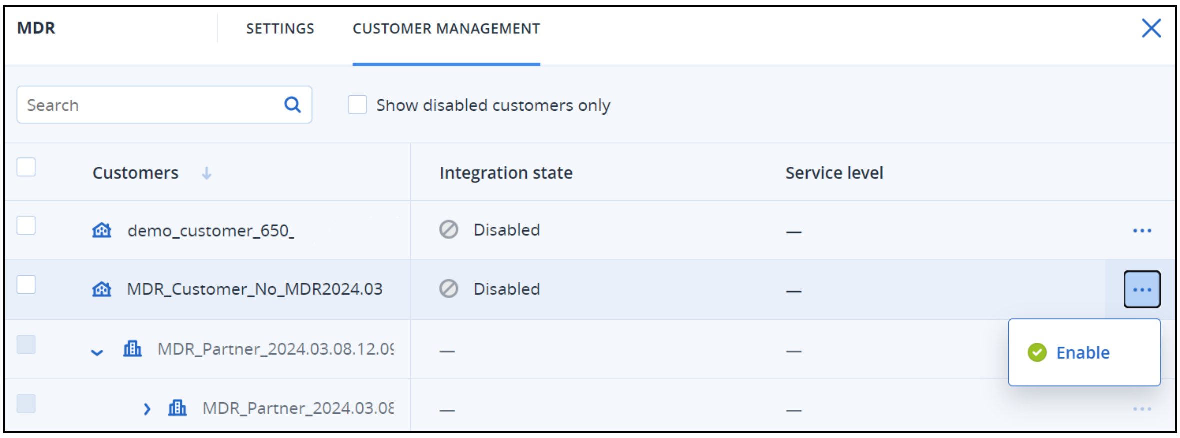
☑ Workloads 0 / Unlimited

☑ Managed Detection and Response 0 / Unlimited

To configure the integration with the MDR vendor's app

1. In Management Portal, go to **Integrations**.
2. Use the search bar to locate the MDR vendor's app.
3. In the displayed MDR catalog card, click **Configure**.
4. In the **Settings** tab, click the pencil icon and enter the contact details of at least one partner contact. This contact will be contacted by the MDR vendor when a security event is detected. Note that you can add the details of up to three contacts. When done, click **Enable**.

   When a security event is detected, the vendor calls each contact six times before moving on to the next contact. Following a call, or in the event no contact is made, the vendor sends an email to all contacts, providing an overview of the escalation and the incident.
5. In the **Customer management** tab, click the ellipsis icon (...) in the far right column for the relevant customer, and then click **Enable**.



MDR | SETTINGS | CUSTOMER MANAGEMENT

Search

□ Show disabled customers only

□	Customers	Integration state	Service level	
□	demo_customer_650_	Disabled	—	...
□	MDR_Customer_No_MDR2024.03	Disabled	—	...
□	MDR_Partner_2024.03.08.12.0	—	—	Enable
□	MDR_Partner_2024.03.0	—	—	...

   To enable multiple customers, select the checkbox next to the relevant customers, and then click **Enable** in the top left of the **Customer management** tab.
6. From the **Service level** drop-down list in the displayed dialog, select the level of MDR service you want to apply to the selected customer(s):
   - **Standard**: Includes 24/7/365 monitoring of customer endpoints to catch attacks, AI-powered event triage and prioritization, threat containment and isolation of affected endpoints, and real-time in-console visibility over a prioritized list of incidents.
   - **Advanced**: In addition to the features included in **Standard**, this level also enables complete remediation, including attack rollback, recovery and the closing of security gaps.
7. Click **Enable** to complete the MDR integration.

   If the IP allowlist feature is enabled (see "Limiting access to the web interface" (p. 34)), you are prompted to add the MDR vendor's IPs to the allowlist. This ensures that the vendor can monitor the relevant workloads. Click **Enable** to confirm.

   MDR is now enabled and security incidents will be forwarded to the MDR vendor to conduct investigation and response activities. For further information about the MDR service, see "What is Managed Detection and Response (MDR)?" (p. 176)

Disabling Managed Detection and Response (MDR)

You can disable MDR at the offering item level. You can also disable MDR for individual customers in the MDR vendor's integration app.

To disable the MDR offering item

1. In the management portal, go to **Clients**.
2. Click the ellipsis icon (...) next to the relevant customer, and select **Configure**.
3. In the **Protection** tab, click **Edit**.
4. In the **Advanced Security + EDR** section, ensure that the **Workloads** and **Managed Detection and Response** checkboxes are not selected. Then click **Save** to apply your changes.

   Alternatively, you can disable the **Advanced Security + EDR** service in the **Configure** tab, which automatically disables MDR.

To disable MDR for individual customers in the MDR vendor's integration app

1. In the management portal, go to **Integrations**.
2. Search for the relevant MDR vendor app.
3. In the displayed MDR catalog card, click **Configure**.
4. In the **Customer management** tab, click the ellipsis icon (...) in the far right column for the relevant customer, and select **Disable**.

   To disable multiple customers, select the checkbox to the left of each customer, and then click **Disable** in the top left of the **Customer management** tab.

Response actions available in Managed Detection and Response (MDR)

MDR includes a number of response actions that can be applied at the incident level.

Response actions are performed by MDR security analysts, who apply the relevant actions by accessing the Cyber Protect console or by running API calls. These analysts login to the Cyber Protect console with the **Security analyst** role.

All response actions are logged in the **Activities** list. Customers can view a list of the response action activities performed and the status of these activities (In progress/Success/Failed). In the **Initiated by** column, the user who initiated the action is displayed, whether it is a partner user, a customer user, or the MDR security analyst.

Note
The response actions listed in the table below include references to the relevant sections in the Endpoint Detection and Response (EDR) documentation.

Response action	Additional information
Change investigation state	The state can be set to any of the following: • **Investigating** • **Closed** • **False positive** For more information about changing the investigation state, see How to investigate incidents in the cyber kill chain.

Response action	Additional information
Network isolation	MDR security analysts can: • Isolate the workload • De-isolate the workload • Check the isolation state For more information about isolating the workload, see Manage the network isolation of a workload.
Add comments	MDR security analysts can add comments to the incident, by clicking **Post comment** in the cyber kill chain for the incident. These comments are shown in the **Activities** tab for the specific incident. For more information, see Understand the actions taken to mitigate an incident.
Stop process / process tree	This action can be applied to the entire incident. The response action can be triggered even if the processes were already stopped for the incident. An asynchronous response is sent after the response action was processed. The response can be one of the following: • Success: All processes were stopped successfully. • Success with warning: Some processes were stopped successfully or there are no processes to stop (or were stopped outside of MDR). • Error: No processes were stopped. For more information about stopping a process or process tree, see Define response actions for a suspicious process.
Quarantine	This action can be applied to the entire incident. The response action can be triggered even if the files or processes were already quarantined. An asynchronous response is sent after the response action was processed. The response can be one of the following: • Success: All files and processes were quarantined successfully.

Response action	Additional information
	• Success with warning: Some files and processes were quarantined successfully or there are no files or processes to quarantine (or were quarantined outside of MDR). • Error: No files or processes were quarantined. For more information about quarantining a process, see Define response actions for a suspicious process. For more information about quarantining files, see Define response actions for a suspicious file.
Delete files	This action can be applied to the entire incident. The response action can be triggered even if the files were already deleted. An asynchronous response is sent after the response action was processed. The response can be one of the following: • Success: All files were deleted successfully. • Success with warning: Some files were deleted successfully or there are no files to delete (or were deleted outside of MDR). • Error: No files were deleted. For more information about deleting files, see Define response actions for a suspicious file.
Restart workload	Enables the setting of a time interval before restarting the workload or to restart immediately. For more information about restarting workloads, see Restart a workload.
Add URL, file or process to allowlist / blocklist	Adds the URLs, files or processes to the allowlist / blocklist on the default plan (the plan currently assigned to the workload). An asynchronous response is sent after the response action was processed. The response can be one of the following:

Response action	Additional information
	• Success: All URLs, files, and processes were added successfully. • Success with warning: Some URLs, files, and processes were added successfully and some were not (for example, they may already be included in the allowlist). • Error: The action failed. For more information about adding URLs, files, or processes to the allowlist and blocklist, see Add a process, file or network to the protection plan blocklist or allowlist.

Advanced Disaster Recovery

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

The following advanced Disaster Recovery features are available:

- Production failover
- Automated test failover with AI screenshot validation
- Automated incremental failback to virtual and physical machines with near-zero downtime
- Point-in-time recovery; 100 recovery points are available
- Failover to a malware-free point to avoid reinfection
- Runbooks automation
- Real-time DR dashboard with RPO-compliance tracking
- Multiple network connectivity options: Cloud-only, Point-to-site, Site-to-site Open VPN, and Multi-site IPsec VPN (Disaster Recovery to Cyber Protect Cloud)
- Maximum number of cloud networks in Cyber Protect Cloud: 23
- Multiple network connectivity options: Azure IPsec VPN, Azure ExpressRoute (Disaster Recovery to Microsoft Azure):
- Maximum number of cloud networks in Microsoft Azure: limited by Microsoft Azure subscription policies.
- Customers retain full control over Azure networking and connectivity, with the flexibility to leverage native Azure platform capabilities or bring their own custom solution (Microsoft Azure)

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
- Self-service release of quarantined spam by mailbox owner

You can also enable Microsoft 365 collaboration app seats, which allows the protection of Microsoft 365 cloud collaboration applications from content-borne security threats. These applications include OneDrive, SharePoint, and Teams.

Advanced Email Security can be enabled per workload or per gigabyte and will impact your licensing model.

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

For configuration instructions, see the Advanced Email Security documentation.

Advanced Backup

You can enable the Advanced Backup pack and protect your workloads with advanced backup and recovery features.

The following features are available:

- One-click recovery
- Continuous data protection
- Backup support for Microsoft SQL Server clusters and Microsoft Exchange clusters – Always On Availability Groups (AAG) and Database Availability Groups (DAG)
- Backup support for MariaDB, MySQL, Oracle DB, and SAP HANA
- Data protection map and compliance reporting
- Off-host data processing
- Backup frequency for Microsoft 365 and Google Workspace workloads
- Remote operations with bootable media
- Direct backup to Microsoft Azure, Amazon S3, and Wasabi public cloud storage

Advanced Security Awareness Training

Partners can enable the Advanced Security Awareness Training service for their Customer tenants so that the users in their organization can access security awareness training materials from the Protection console.

The direct access to the security awareness training from the Cyber Protection cloud console promotes the adoption and coverage of more users in the organization, which helps customers to meet the requirements of compliance (PCI, HIPPA, FedRamd, Soc 2), vendor risk management, cyber insurance, and others. In addition, the training helps customers improve their cyber security by reducing the risk of human errors.

The service is delivered by a third-party learning management system, Wizer, that supports the following functionality:

- Multitenancy: In the Wizer Admin Panel, a Partner administrator can view all their customers and direct users that are enrolled for Security Awareness Training. The platform does not support multi-level view, i.e. partners cannot view child partners and their child tenants. Customer administrators can view only users in their organization.
- Auto-provisioning of tenants and administrator users: When the service is enabled in the Cyber Protect Cloud console for the first time, the integration creates automatically a new tenant in Wizer for the administrator who enabled the integration. The administrator then accesses the Wizer Admin Panel to add users manually or to configure SSO. See How to add users.
- Appealing content that makes the training fun
- Ease of use
- Monthly subscription

Learn more about Wizer at https://www.wizer-training.com/.

Enabling the Advanced Security Awareness Training service

The Security Awareness Training is provided by a third-party vendor, Wizer, as an integration in the Cyber Protect Cloud console. Partners have to enable the integration for their own tenant before they can enable the service for their customers.

The enabling of the service consists of the following high-level steps.

1. In the Cloud management console, a Partner administrator enables the Security Awareness Training service for a Customer (once for each customer).
2. In the Cyber Protect Cloud console, an administrator enables the integration with Wizer in their organization (one time per organization).
3. The administrator user navigates to Wizer admin console to add users to the training platform.

Note
The service is not accessible for Unit administrators and Folder administrators.

To enable the Advanced Security Awareness Training service for a Customer tenant

Required role: Partner administrator

1. In the Cloud management console, click **Clients** and locate the customer for which you want to enable the service.
2. In the context menu, click **Configure**.

3. In the list of services, under **Per workload**, select the **Advanced Security Awareness Training** check box.

To enable the integration with Wizer for an Organization

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

Note
This initial configuration is performed only once.

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

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

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

RMM

RMM provides an advanced level of monitoring and management for endpoints and Microsoft 365 seats. Learn more, try, or request a demo here.

- For endpoints, RMM provides the following:
  - **Software inventory** - See the complete list of software used by clients, and save time and effort when preparing, planning, or tracking updates.
  - **Software deployment by using DeployPilot** - Remotely deploy software on your managed workloads. Use software deployment plans to automate the software deployment process, and to ensure that software distribution across workloads is uniform.
  - **Automated patch management** - Remediate vulnerabilities before they are exploited.
  - **Fail-safe patching** - Recover workloads from faulty patches quickly and easily by performing automatic system backups before patching.
  - **Monitoring and smart alerting based on machine learning** - Mitigate operational risks and optimize the monitoring effort with predictive monitoring and alerts.
  - **Out-of-the-box Cyber Scripting** - Automate and streamline routine tasks.
  - **Drive health monitoring** - Use predictive monitoring and alerts, and proactively mitigate downtime caused by drive failures.
  - **Remote desktop and remote assistance** - Access remote workloads and resolve technical issues quickly. Save time and provide reliable support with excellent performance, even with limited bandwidth. The feature includes better platform coverage (Windows, macOS, and Linux), and extended capabilities for session recordings, remote actions, file transfers, monitoring, reporting, and observing workloads in multi view.
  - **Vulnerability assessment for third-party Windows applications** - Enhance the security posture for Windows third-party applications by detecting and managing vulnerabilities across 314 critical applications, supported by an internally maintained database.

    Vulnerability assessment for third-party Windows applications was moved to the RMM pack and might incur additional costs. If you want to stop the protection of these applications and disable the feature or to enable it in multiple existing plans, see "Mass disabling and enabling of vulnerability assessment for Windows third-party applications" (p. 188).
  - **Geolocation tracking** - View the real-time physical location of your managed workloads.
  - **Helpdesk chat** - Use the real-time communication tool between technicians and remote users of managed Windows and macOS workloads to provide faster issue resolution and better customer service.
- For Microsoft 365 seats, RMM provides a continuous audit of the Microsoft 365 security posture, with best practice baselines, and remediation of baseline deviations. Two product modes are available when you enable the Microsoft 365 management service:
  - **Free**: Enables the auditing of the Microsoft 365 security posture with best practice baselines, and user onboarding. The Free mode is available in the standard protection feature set.
  - **Advanced**: Includes all the Free mode features, and also enables the automatic remediation of security posture baseline deviations, and user offboarding.

Mass disabling and enabling of vulnerability assessment for Windows third-party applications

Disabling or enabling the vulnerability assessment for Windows third-party applications on multiple customer tenants with multiple managed workloads can be time-consuming, tedious task. Therefore, we have built utilities for mass disablement and enablement of the feature. See these knowledge base articles for details:

- If you configured vulnerability assessment for third-party Windows applications in your protection plans but the customer does not have the RMM pack enabled on their tenant, use this utility to disable vulnerability assessment for third-party Windows applications in all affected plans while retaining all other vulnerability assessment components: https://care.acronis.com/s/article/Acronis-Cyber-Protect-Disabling-Vulnerability-Assessment-of-Third-Party-Windows-Applications-when-Advanced-Management-pack-is-not-enabled-for-the-tenant.
- If you need to enable vulnerability assessment for third-party Windows applications to ensure their protection across all protection plans where the general vulnerability assessment policy is already active and the RMM pack is enabled for the corresponding tenants, use this utility to mass-enable the sub-policy: https://care.acronis.com/s/article/Acronis-Cyber-Protect-Enabling-Vulnerability-Assessment-for-Windows-Third-Party-Applications-when-Vulnerability-Assessment-module-is-enabled-in-Protection-plans.

Advanced Automation (PSA)

The Advanced Automation (PSA) service makes it easy and intuitive for clients to take advantage of business management platforms and software. Comprised of a number of paid tools, Advanced Automation (PSA) enables MSPs to fully manage and automate various daily tasks, including:

- Customer billing and invoicing.
- Customer support and service desk ticketing.
- Sales and project management.

Advanced Automation (PSA) can also be enabled to work in tandem with other Management Portal services, and is subject to additional charge. Your account will be charged based on the number of users (or technicians) that are granted access to the Advanced Automation (PSA) service.

What is Advanced Automation (PSA)?

Advanced Automation (PSA) is a Business Management Tool for Managed Service Providers (MSPs), designed to make it easy and intuitive for MSPs to manage and automate various daily tasks.

Advanced Automation (PSA) ensures your clients get the service they need while, at the same time, you remain in full control of your operations. The components that make up Advanced Automation (PSA) include ticketing, RMM integration, project management, automatic time registration, and consumption-based billing, while also providing quick and easy access to your client’s billing and ticketing data. You can also use the dedicated mobile application for your day-to-day service desk operations, including the monitoring and processing of tickets, and the tracking and registering of work time. The Acronis Advanced Automation (PSA) app can be downloaded from the App Store and Google Play Store.

After the Advanced Automation (PSA) service is activated, your account is charged for each user granted access to the service.

Key features of Advanced Automation (PSA) include:

- **Manage service desk tickets**: Support tickets are automatically converted from incoming emails and alerts from third-party integrated platforms, if enabled. For more information, see "Service desk" (p. 206).
- **Manage billing**: Invoices are automatically generated based on the time spent with your client or according to the billing arrangement you have with them. For more information, see "Managing sales and billing functionality" (p. 252).
- **Manage projects**: Create customer-oriented project plans with defined timelines and budgets, and assign project steps to be completed by project team members. Then monitor and track the progress of projects, and bill clients for the relevant project work. For more information, see "Projects" (p. 221).
- **Manage time registrations and activities**: Approve ticket time for billing, request time off, and approve holidays as an admin user or manager. For more information, see "Time entries" (p. 244).

- **Native integration with Acronis services**: This includes usage-based customer billing and device control with Advanced Management.

Enabling Advanced Automation (PSA) for clients

As described during the tenant creation process (see "Selecting the services for a tenant" (p. 44)), you can add services as required for tenants.

The Advanced Automation (PSA) service is available for the following tenant types:

- Partner
- Customer

Note
Partners cannot view the Advanced Automation (PSA) data of their clients (whether they are sub-partners or customers), because, unlike other products, Advanced Automation (PSA) data is private business data specific to a sub-partner (or customer) account. However, partners can still view specific account data by logging in to the management portal as the relevant client (sub-partner or customer).

To enable Advanced Automation (PSA)

1. In the management portal, go to **Clients**.
2. Select the tenant for editing.
3. In the **Configure** tab, under the **Service** section, scroll down and select **Advanced Automation (PSA)**.

   Advanced Automation (PSA) is now available for the selected client.

Setting up Advanced Automation (PSA)

This section describes the various steps you need to complete to get up and running with Advanced Automation (PSA).

Activating Advanced Automation (PSA)

If the Advanced Automation (PSA) service is enabled for your account, you can activate the service by navigating to **Settings**. If the Advanced Automation (PSA) service is not enabled, contact your administrator.

To activate Advanced Automation (PSA)

1. In the management portal, click **Settings > Advanced Automation (PSA)**.

   Note
   After you have activated Advanced Automation (PSA), as described in the following steps, this menu option is not available.

2. In the displayed screen, click **Activate Advanced Automation (PSA)**.
3. In the Activate Advanced Automation (PSA) screen, provide the company business information in the **Company information** tab. Then click **Next**.
4. In the **User roles** tab, define the Advanced Automation (PSA) role for each user, and then click **Next**. The available roles are:
   - Engineer
   - HR
   - Finance
   - Sales
   - Group manager
   - Finance manager
   - Director
   - Administrator

     To understand more about each of the Advanced Automation (PSA) roles and their access privileges, see "Advanced Automation (PSA) roles" (p. 201).

     Note
     You can also add new users after activating Advanced Automation (PSA). First create the user account(s), and then apply the relevant services the user will have access to. For more information, see "Creating a user account" (p. 56).
5. In the **Confirmation** tab, review the activation information, and click **Activate**. The Advanced Automation (PSA) service is configured, which may take a few seconds.
6. In the displayed onboarding wizard screen, select from the following Advanced Automation (PSA) options:
   - **Accounting platforms integration**: Click **Configure** to redirect to the Accounting integrations page. For more information, see "Integrating with accounting platforms" (p. 333).
   - **RMM platforms integration**: Click **Configure** to redirect to the Advanced Automation (PSA) RMM integrations page. For more information, see "Integrating with RMM platforms" (p. 339).
   - **Service desk configuration**: Click **Configure** to redirect to **Settings > Service desk**. For more information, see "Service desk settings" (p. 289).
   - **Email server configuration**: Click **Configure** to redirect to the Configure email server screen. For more information, see "Configuring your email settings" (p. 202).

If you no longer want to use the functionality included in Advanced Automation (PSA), you can deactivate the Advanced Automation (PSA) service. For more information, see "Deactivating the Advanced Automation (PSA) service" (p. 356).

Quick start to setting up Advanced Automation (PSA)

This quick start guide describes the basic steps required to get up and running with Advanced Automation (PSA).

Follow the steps in the table below to ensure:

- New and existing customers are set up in Advanced Automation (PSA).
- Your products and services are set up and available, with automatic billing also in place.
- Your service desk is set up and ready to support customers, monitor SLAs and track time spent on tickets and other activities.
- Your RMM and/or accounting platform is integrated and synchronized with Advanced Automation (PSA).
- Incoming emails are converted into tickets, and automated responses configured.

Note
You can also use the dedicated but more limited mobile application ("Acronis Advanced Automation (PSA)", which can be downloaded from the App Store and Google Play Store), to work with service desk tickets and time entries.

The table below describes the general steps required to start working with Advanced Automation (PSA).

Step	Description
STEP 1: Login and launch the Advanced Automation (PSA) onboarding wizard	Login to your account and access the management portal. When Advanced Automation (PSA) is available in your account, two new menu options are displayed, **Task management** and **Sales and billing**. Select one of these options to access the Advanced Automation (PSA) onboarding wizard; click **Activate** to activate the service, as described in STEP 2. For more information, see "Activating Advanced Automation (PSA)" (p. 190).
STEP 2: Activate the Advanced Automation (PSA) service	To activate the Advanced Automation (PSA) service for your account, you will need to complete the following two steps: a. Provide company business information, including bank account details, in the **Provide company info** tab. The company information is used in invoices to end customers. Then click **Next**. b. Assign existing users to the following roles within Advanced Automation (PSA): • Engineer • HR • Finance • Sales • Group manager • Finance manager • Director • Administrator Note that there are two additional roles for your customer's users: • Client • Client manager For more information about the roles in Advanced Automation (PSA), see "Advanced

Step	Description
	Automation (PSA) roles" (p. 201). If required, you can add additional users at a later time; see also "Managing users" (p. 56). When done, you are now ready to start defining your Advanced Automation (PSA) settings, as described in the following steps.
STEP 3: Define Service desk settings	Service desk settings determine essential sections of your service desk ticket flow, including categories, default values, default country and language settings, and Service Level Agreements (SLAs). To access Service desk settings, in the management portal go to **Settings > Service desk**. These settings enable you to: • Configure canned responses • Set priorities • Manage SLAs • Define categories and subcategories • Set default values • Define default country and language settings • Activate and deactivate statuses • Define default RMM ticket integration settings • Manage email templates • Define activities for time tracking • Set the default project billing entity
STEP 4: Define Billing and quoting settings	Billing and quoting settings enable you to fully customize your billing, including the layout of invoices, the default export format (if you then need to import into another system), the setting up of taxes, and much more. Note that billing information for end users should be specified in each customer's settings or during the creation of sales items, contracts, and quotes. To access billing and quoting settings, in the management portal go to **Settings > Billing and quoting**. These settings enable you to: • Define and customize your billing • Define and customize the look and feel of your quotes • Define the taxes to be used
STEP 5: Add your customers	In the management portal you can add and manage your customers, as and when required. Note that in Acronis you can define different account types for customers, including partners, customers, and prospects. These different types are referred to as *tenants*. For more information about the different types of tenant, see "User accounts and tenants" (p. 37). To add partners, customers, and prospects in the management portal, go to **Clients**. Then click **+ New** and select the relevant tenant type.

Step	Description
	For more information, see "Managing tenants" (p. 39).
STEP 6: Define your products	You can create a catalog of both non-recurring products or services and recurring (managed) services that you deliver to your customers, such as antivirus subscriptions or ad hoc support. You can also make certain products available for sale directly in a support ticket, for example, when a customer logs a ticket to add an Office 365 subscription or needs additional memory. This helps save time on additional administrative processes. To access products, go to **Sales and billing > Sales**, and click the **Products** tab. Users with the Administrator, Director, Finance, or Finance manager role can create products. These products can then be used in contracts, tickets, quotes, sales items, etc. For more information, see "Products" (p. 272).
STEP 7: Define contracts	Set up and define your contracts for customers carefully to ensure that Advanced Automation (PSA) can: • Automatically provide periodic billing items and retainers, and enable user or device based billing where required. • Make the connection between configuration items, customers, and the applicable SLA. • Automatically link a service, customer, and configuration item to the applicable SLA in the service desk. • Automatically allocate new configuration items to the right customer, contract, and SLA. To access contracts, go to **Sales and billing > Sales**, and click the **Contracts** tab. For more information, see "Working with contracts" (p. 261).
STEP 8: Set up integrations with third party platforms	Set up your integrations with third party platforms. Advanced Automation (PSA) currently supports: • **RMM**: NinjaOne, Datto RMM, Kaseya VSA, N-able N-Central, and N-able RMM • **Accounting**: FreshBooks, QuickBooks, Sage, Xero, and SnelStart • **VAR**: Microsoft CSP • **Payment**: PayPal and Stripe To access integrations, in the management portal go to **Integrations**. For more information, see "Integrating Advanced Automation (PSA) with third party platforms" (p. 333).
STEP 9: Configure your email settings	This is the last step in setting up Advanced Automation (PSA). Before configuring your email settings, make sure you have first set up your email responses. Once you have configured your inbound email settings, Advanced Automation (PSA) fetches all messages in your defined inbox and creates a ticket for each message (if

Step	Description
	relevant). When an email is processed, it is then moved to the 'archive' folder for future reference. If there is no 'archive' folder it is created for you. There are three email configurations to set up: • **Incoming email**: This is usually configured to have a help desk or support email account directly linked to the Advanced Automation (PSA) service desk. Incoming emails are converted into tickets, and customizable responses sent to the end-user to keep them informed. • **Outgoing email**: The email server and account used to send or reply to messages. • **Invoice email**: The email server and account used to send invoices to customers. To access the email configuration settings, go to **Settings > Service desk > Mail server configuration**. For more information, see "Configuring your email settings" (p. 202).

Onboarding existing clients

When Advanced Automation (PSA) is activated for your account (see "Activating Advanced Automation (PSA)" (p. 190)), you need to onboard your existing clients in order to bill and process their service requests.

Important
Advanced Automation (PSA) currently supports direct Partner and Customer tenants, and Partner and Customer tenants located under Folder tenants. Tenants under a Folder are managed the same way as direct Partner and Customer tenants, and all are available for selection in all Advanced Automation (PSA) features. For more information, see "Managing tenants" (p. 39).

To ensure you have Advanced Automation (PSA) configured correctly for your existing clients, do the following:

- Provide billing information for existing clients.
- Create contracts in order to start billing existing clients for your services and products.
- Ensure you can receive and process service desk tickets for existing clients.
- Ensure you can create sales items for existing clients.
- Ensure you can run the billing process and issue invoices for existing clients.

Note

If your clients are Partner tenants, you cannot view the clients or client billing data managed under these Partner tenant accounts. However, you can convert Partner tenants to Folder tenants to enable Advanced Automation (PSA) with the transparency required to bill a Partner's tenants. For more information, see "Converting a partner tenant to a folder tenant and vice versa" (p. 54).

Similarly, for any defined Folder tenants, you can view the billing data for each Customer or Partner tenant under a Folder tenant. However, in Advanced Automation (PSA) reports, you cannot view the aggregated billing data or service desk report data when selecting a Folder tenant, as these tenants are not displayed in the Advanced Automation (PSA) customer list (for example, when selecting a customer for a report preview).

Provide billing information

If Advanced Automation (PSA) is activated, when you access the **Clients** section you will be prompted to submit billing information for your existing clients. Billing information ensures you can use Advanced Automation (PSA) to bill and process service requests for your clients.

Note

If billing information is not provided for a client, you cannot approve client tickets and time registrations, and you will be prompted when processing these tickets and requests to enter the information for the specified clients. Similarly, when creating a sales item, you will be prompted to complete billing information for the selected client if they do not have the information defined in Advanced Automation (PSA). See the relevant sections below for more information.

To add billing information for existing clients

1. In the management portal, go to **Organization** > **Clients**.
2. Click the ellipsis icon (...) next to the relevant client name. In the displayed menu, select **Add billing information**.

   Or

   Click on a client row from the displayed list. In the displayed sidebar, click the **Configure** tab. Then click on the **Billing** and **Address** sections to add the relevant billing information.
3. Complete the fields shown in the displayed form. For more information about these fields, see "Defining billing information for a tenant" (p. 43).
4. Click **Add** to complete the billing information setup.

   Note

   If you want to manage and have access to user phone numbers in the service desk, in the same **Configure** tab, click the **General settings** section and enable the **Enable self-managed customer profile** switch. When enabled, this option displays to both administrators and client users the relevant contact related fields, including phone numbers (and company contact and job title). For more information, see "Configuring self-managed customer profile" (p. 49).

Create contracts to start billing existing clients for services and products

Contracts ensure you can use Advanced Automation (PSA) to bill your clients on a regular basis.

If Advanced Automation (PSA) is activated, when you access the **Sales and billing** module you are prompted to create contracts for your existing clients. This prompt is displayed only if one or more clients have Acronis services or products assigned.

To create contracts for existing clients

1. In the management portal, go to **Sales and billing** > **Sales**.
2. If the displayed banner informs you that a specified number of clients do not have contracts assigned, click **Create**.

   Alternatively, if you previously closed this banner, click the **Create contracts for existing customers** link, located in the top right of the screen.
3. In the Create new contract wizard, do the following:
   a. Select the relevant client, and click **Next**.
   b. Add contract information, including payment details and the contract period. For more information, see "Working with contracts" (p. 261). When done, click **Next**.
   c. Add billing information, and click **Next**. Note that if you have already defined billing information, as described in "Provide billing information" (p. 196), this step is not displayed.
   d. Add contract parts, as required. For more information, see "Creating a new contract" (p. 261). By default contract parts based on Acronis services already assigned to the client are added to the contract template. These contract parts can be edited or deleted, as required. Ensure you set the correct prices for the contract parts.
4. Click **Done**. The contract is added to the list of existing contracts in the **Contracts** tab.

Ensure you can receive and process service desk tickets for existing clients

If Advanced Automation (PSA) is activated, you can receive and process tickets for an existing client even if billing information is not defined for that client. This ensures you can create, respond to, resolve and close tickets as required. For more information about working with the service desk features, see "Service desk" (p. 206).

However, you cannot approve a client's reported ticket time if billing information is not provided for that client. When you attempt to approve ticket time registrations, you are prompted to add billing information for the relevant clients; for more information, see Provide billing information.

Ensure you can create sales items for existing clients

When Advanced Automation (PSA) is activated, you can create sales items for an existing client even if billing information is not defined for that client. If no billing information is provided, sales items in **Draft** status are automatically generated for clients (see "How billing automation works in Advanced Automation (PSA)" (p. 198)).

However, when creating a sales item (see "Managing sales items" (p. 258)), if you select a client without billing information specified, you are prompted to provide the billing information before proceeding with the creation of the sales item.

In addition, when editing an existing sales item, you cannot change the existing client assigned to the sales item to a client without billing information specified. You are prompted to provide the billing information before proceeding with the editing of the sales item.

Ensure you can run the billing process and issue invoices for existing clients

On the first billing run you are prompted to verify the default invoice numbering settings before generating invoices; created invoices must have numbers aligned with your accounting software. This step ensures that you have correctly setup your billing and invoicing information. For more information, see "Invoices" (p. 267).

How billing automation works in Advanced Automation (PSA)

Advanced Automation (PSA) provides fully automated monthly billing for services out of the box.

By default, on every first day of a new month, the system automatically generates sales items for all customers with products in use in the just completed month. This monthly billing process relies on the Cyber Protect Cloud platform's Usage report and fully covers the PAYG (pay-as-you-go) billing model for providers. In addition, contracts can be configured for customers, which enables providers to configure specific billing rules and terms.

When Advanced Automation (PSA) is activated, the system automatically performs monthly billing for the last completed month, enabling providers to immediately test the billing and invoicing functionality. This initial billing is shown in the form of sales items within 15-20 minutes (depending on the customer base) after Advanced Automation (PSA) is activated. These sales items are based on usage from the previous month.

Subsequently, on the first day of a new month, the system automatically runs contract billing that includes invoicing data preparation for customers, and sales items for items above the minimum commitment defined in the contract. The billing run also includes sales items defined for usage outside of contracts.

Limitations

- For customers without billing information, sales items are generated in **Draft** status. These items cannot be billed for until billing information is provided for the customer.
- Sales items are not generated for trial customers, regardless if you are performing the initial or subsequent monthly billing run.

Working with custom fields

By defining custom fields, you can store additional (optional) information for customers, products, sales items, contracts and contract parts, and tickets. Custom fields are listed under a new

Additional information section in the relevant entity.

For example, you can add custom fields that are applicable to customers. When creating or editing a customer, you can complete these pre-defined custom fields in the **Additional information** section, which are then added to the customer's details.

This section describes how to add a new custom field, and how to edit or remove an existing custom field.

Note
This feature is only available for users assigned the Administrator role.

Creating a custom field

To create a custom field

1. In the management portal, go to **Settings** > **Billing and quoting**, and then select **Custom fields**.
2. Click **+ New custom field**.
3. Define the following:
   - In the **Name** field, enter a name for the custom field.
   - In the **Type** field, select the relevant type of field from one of the following:
     - String
     - Integer
     - Boolean
     - Text
     - Date
   - In the **Required** column, click the option switch to **Yes** if you want the field to be mandatory.
   - In the **Apply to** field, select the relevant entity the custom field will be applied to:
     - Customer
     - Product
     - Project
     - Project step
     - Contract
     - Contract part
     - Sales item
     - Ticket

       Note
       When applying the custom field to tickets, all ticket types (including service desk tickets, quotes, and others) are affected.
     - Inventory item
   - In the **Status** column, select from **Active** or **Inactive**.

   - In the **Sort number** column, enter a numeric value that defines the display preference for the custom field. This is relevant when you have a number of custom fields in a displayed form; the lower the number, the higher the custom field is displayed.

4. Click **Create custom field** to add the new custom field.

Editing a custom field

This section describes how to edit or remove an existing custom field.

To edit a custom field

1. In the management portal, go to **Settings** > **Billing and quoting**, and then select **Custom fields**.
2. Click the row of the custom field you want to edit.
3. Edit as required. For more information about the editable fields, see "Creating a custom field" (p. 199).
4. When done, click ✓.

To remove a custom field

In the **Custom fields** screen, click the ellipsis icon (...) in the row of the custom field you want to remove, and then click **Remove**.

The custom field is removed from the **Custom fields** screen, and is no longer shown in the **Additional information** section in the relevant entity.

Managing your users

After you have activated Advanced Automation (PSA) (see "Activating Advanced Automation (PSA)" (p. 190)), your existing users are automatically assigned roles to have immediate access to Advanced Automation (PSA) features. Note that, by default, company administrators are granted the Administrator role; all other users are assigned the Engineer role, but this can be updated as required.

You can also add users and user groups, as required. Note that when you assign a user with an Advanced Automation (PSA) role, they are automatically assigned to the default user group. User group settings can be updated in the Settings section (see "Service desk settings" (p. 289)).

For more information about creating your Advanced Automation (PSA) users in the management portal, see "Creating a user account" (p. 56).

Managing user groups

Users assigned with the Administrator or Director role can manage user groups within their organization.

To add a new user group to your organization

1. In Management Portal, go to **Settings** > **Service desk**, and then select **User groups**.

   The displayed list shows your active and inactive groups, and how many users are in each group. These groups can be edited or activated/deactivated, as described below.
2. Click **+ New**.
3. Enter a **User group name**.
4. Select the **Group manager**.
5. Select the **Active** check box to activate the group.
6. Select the relevant users from the **Users** list (on the right). Then click the left arrow icon to add the users to the **Group members** list.
7. Click **Create new group**.

To update a user group

1. In the **User groups** screen, click on the group you want to update.
2. In the right sidebar, click the pencil icon to edit the user group. In addition to updating the group name and manager, you can also edit group members and activate/deactivate the group by selecting/clearing the **Active** check box.
3. When done, click ✓.

To delete a user group

1. In the **User groups** screen, click on the group you want to delete.
2. In the right sidebar, click the trash can icon.

   The user group is deleted.

Note

You can only delete a user group if it is currently **Inactive**, and if all users are assigned to another **Active** group. In addition, the group must not be used in any Advanced Automation (PSA) settings, such as the service desk default settings or quote settings.

Advanced Automation (PSA) roles

Advanced Automation (PSA) includes a number of roles, which can be assigned to your users as required.

When you activate Advanced Automation (PSA) (as described in "Activating Advanced Automation (PSA)" (p. 190)), all your existing users are automatically granted access to the functionality in Advanced Automation (PSA). During the account creation process, you can assign the relevant role to each user. Note that, by default, management portal administrators are granted the Administrator role, and read-only administrators are granted the Engineer role.

To update the role at a later date, go to **My Company** > **Users**, select the relevant user, and in the **Services** tab, update the role. In the same tab, you can also disable the Advanced Automation (PSA) functionality for that specific user.

The table below describes each of the available roles, and the rights assigned to each role within Advanced Automation (PSA):

Role	Description
Engineer	The default role applied to all users. Includes access to the Service desk and Project management modules plus time tracking functionality. This role also includes limited access to customer details and their end users.
HR	Includes limited access to the Service desk, Project management, Reports and Time management modules.
Finance	Includes access to the CRM, Sales and billing, Service desk, Project management, plus time tracking functionality. This role also includes limited access to client's financial statistics and no access to company reports.
Sales	Includes access to the CRM, Sales, Service desk, and Project management modules, plus time tracking functionality. This role also includes limited access to invoices data and no access to company reports.
Group manager	Includes access to the CRM, Service desk, and Project management. This role also includes full access to client's financial statistics, company reports, and Time management functionality, as well as limited access to the Sales module.
Finance manager	Includes access to the CRM, Sales and billing, Service desk, and Project management modules. This role also includes full access to client's financial statistics and company reports, and Time management functionality.
Director	Includes access to all modules but without the capability to manage global company settings.
Administrator	Full access rights and the capability to manage global company settings for the Service desk, Billing and Invoicing.
*The following roles are available for your customer's users (select the relevant customer, and then go to **Company management > Users**). When users are first added, their status is Inactive and an invitation email is sent to the user. You can activate or deactivate their access to Advanced Automation (PSA) at any time.*	
Client	Includes access to the Service desk module (limited to within a customer's organization).
Client manager	Includes access to the Service desk, Invoices, and Reports modules (limited to within a customer's organization).

Configuring your email settings

Advanced Automation (PSA) has a built-in email parser to convert incoming email to tickets. To use this feature, ensure you use a dedicated email account or test email account. In addition, note the following:

- Do not use a personal email account with the same address as an Management Portal user account.
- All *unread* messages that the system finds in the inbox will be converted into tickets.
- Tickets cannot be assigned to users that are not present in Management Portal as there can be no association with an email address.
- Once an email message is processed, Advanced Automation (PSA) moves it to an archive folder (it is not deleted):
  - If there is no archive folder, it is created.
  - If you are using a mail server other than Office365 or Gmail, ensure it supports RFC 6851.

To access the mail server settings, go to **Settings > Service desk > Mail server configuration**.

Note
The configuration of the mail server for outgoing invoices and incoming tickets is only available when the Advanced Automation (PSA) service is activated. This functionality is also accessed when first onboarding with Advanced Automation (PSA), as described in "Activating Advanced Automation (PSA)" (p. 190).

Defining outgoing email settings

Note
Contact your email administrator for your server setup details.

1. Go to **Settings** > **Service desk** > **Mail server configuration**.
2. In the **Outgoing email settings** row, click the pencil icon.
3. Click the **Active** option switch to enable outgoing email.
4. Select the relevant mail server protocol type from one of the following:
   - SMTP (default)
   - Exchange
   - Office365
5. To enable SSL, select the **Enable SSL** check box. Secure Sockets Layer (SSL) encrypts your email messages during transport and is only supported in these scenarios:
   - Secure (TLS) - StartTLS - Port 587
   - Secure (SSL) - SSL - Port 465
6. Enter the host name and its port.
7. Enter the account username and password.
8. In the **From** field, enter the account username. If you selected the Office365 protocol type, note that it supports alias email addresses in a single mailbox. When you want to use any of these addresses as the sender address, use this field. Only email addresses that are associated with the Office365 account are used. The system does not spoof any addresses.

9. Enter the **Timeout** value in milliseconds. This value specifies how long the system waits for a successful connection to your email server before it times out. Note that if you are using SMTP as protocol type, select the **Requires Authentication** check box.
10. Click **Test Connection** to verify your outgoing email settings. Once the system validates all your settings, a confirmation message is displayed.
11. Click ✓ to apply your settings.

    You can also define settings for the invoice emails you send to customers (see "Defining outgoing invoice email settings" (p. 204)) and incoming email settings (see "Defining incoming email settings" (p. 205)).

Defining outgoing invoice email settings

Note
Contact your email administrator for your mail server setup details.

The invoice email settings enable you to configure your mail server to send invoices to your customers.

To define your invoice email settings

1. Go to **Settings > Service desk > Mail server configuration**.
2. In the **Invoice email settings** row, click the pencil icon.
3. Click the **Active** option switch to enable outgoing invoice emails.
4. Select the relevant mail server protocol type from one of the following:
   - SMTP (default)
   - Exchange
   - Office365
5. To enable SSL, select the **Enable SSL** check box. Secure Sockets Layer (SSL) encrypts your email messages during transport. SSL is only supported in these scenarios:
   - Secure (TLS) - StartTLS - Port 587
   - Secure (SSL) - SSL - Port 465
6. Enter the host name and its port.
7. Enter the account username and password.
8. In the **From** field, enter the account username. If you selected the Office365 protocol type, note that it supports alias email addresses in a single mailbox. When you want to use any of these addresses as the sender address, use this field. Only email addresses that are associated with the Office365 account are used. The system does not spoof any addresses.
9. Enter the **Timeout** value in milliseconds. This value specifies how long the system waits for a successful connection to your email server before it times out. Note that if you are using SMTP as protocol type, select the **Requires Authentication** check box.
10. Click **Test Connection** to verify your outgoing email settings. Once the system validates all your settings, a confirmation message is displayed.
11. Click ✓ to apply your settings.

You can also define settings for outgoing emails (see "Defining outgoing email settings" (p. 203)) and incoming email (see "Defining incoming email settings" (p. 205)).

Defining incoming email settings

Note
Contact your email administrator for your mail server setup details.

The incoming email settings enable you to configure your mail server to receive emails from your customers. Advanced Automation (PSA) automatically converts these emails into tickets and assigns them to the relevant user or company.

Important
When email integration is activated, Advanced Automation (PSA) manages the inbox for the specified account. Any unread messages are automatically processed and moved to the Archive folder.

To define your incoming email settings

1. Go to **Settings > Service desk > Mail server configuration**.
2. In the **Incoming email settings** row, click the pencil icon.
3. Click the **Active** option switch to enable incoming emails.
4. Select the relevant mail server protocol type from one of the following:
   - IMAP (default)
   - Exchange
   - Office365
5. To enable SSL, select the **Enable SSL** check box. Secure Sockets Layer (SSL) encrypts your email messages during transport. SSL is only supported in these scenarios:
   - Secure (TLS) - StartTLS - Port 587
   - Secure (SSL) - SSL - Port 465
6. Enter the host name and its port.
7. Enter the account username and password.
8. Enter the **Timeout** value in milliseconds. This value specifies how long the system waits for a successful connection to your email server before it times out.
9. Select the **Process messages from unknown users** check box to ensure messages from unknown users will be converted, but the tickets will not be automatically assigned to a user or company. If not selected, when an email comes in from an address that is not in the customer database, the message is not converted into a ticket.
10. Select the **Do not process messages received before the specified date** check box to ensure that tickets are created for emails received after a specified date only. This option prevents tickets from being automatically created for all existing emails, including those received prior to defining your incoming email settings. When the check box is selected, additional date and time fields are displayed.

11. Click **Test Connection** to verify your incoming email settings. Once the system validates all your settings, a confirmation message is displayed.
12. Click ✓ to apply your settings.

    You can also define settings for the invoice emails you send to customers (see "Defining outgoing invoice email settings" (p. 204)) and other outgoing email settings (see "Defining outgoing email settings" (p. 203)).

Managing your service desk, projects, and time entries

The **Task management** module of Advanced Automation (PSA) is where you manage your service desk, projects, and time entries.

- **Service desk**: Manage customer service requests, and plan and track service activities.
- **Projects**: Manage projects and the phases and steps that make up a project, and bill clients for project activities.
- **Time entries**: Manage your time registrations, approve ticket time for billing, request a day off, and approve holidays as an admin user or manager.

Note
You can also use the dedicated but more limited mobile application ("Acronis Advanced Automation (PSA)", which can be downloaded from the App Store and Google Play Store), to work with service desk tickets, and time entries. Projects are not available in the mobile application.

Service desk

The **Service desk** module enables you to create, update, and schedule your tickets.

To access the Service desk functionality, in the management portal go to **Task management > Service desk**. From the two displayed tabs (**Tickets** and **Scheduler**), you can view the entire organization's tickets and their statuses, including customer ratings. You can also:

- Create new tickets
- Review and update current tickets
- Merge tickets
- Create and modify custom ticket filters
- Schedule tickets
- Export ticket data

Note
Users assigned with the Client manager or Client roles have limited access to the above service desk functionality. They can review, create and modify tickets (with some limitations, as described in the Customer Administrator's guide). They can also export ticket data as required, but cannot schedule or merge tickets.

How tickets are created and updated

Advanced Automation (PSA) creates and updates service desk tickets via multiple sources. In addition to users (or requestors) creating and updating tickets manually in the management portal, users (or requestors) can create tickets via a public ticket portal, and via integrated RMM alerts.

How are tickets created?

There are four options for creating tickets in Advanced Automation (PSA):

- Tickets are created manually by customers, or by MSPs, using the management portal. For more information, see "Creating a new ticket" (p. 208).
- Tickets are created via incoming email when:
    - A new unread email from a new thread is identified.
    - A new unread email from an existing email thread is identified, but an associated ticket is already closed.
    - A requestor is identified by their email address.
    - A requestor is not identified by their email address, but incoming email settings (see "Defining incoming email settings" (p. 205)) allow tickets to be submitted by unknown users.
- Tickets are created via the public ticket portal, when configured accordingly (see "Setting default values" (p. 294)). The ticket portal can be accessed without registering or signing in to the system (see Submitting service desk tickets via the ticket portal).
    - If the email address is recognized by the system, or the provider has selected not to restrict requests from unregistered users, the ticket is created.
    - If the email address is not recognized, and the provider has selected to not process requests from unregistered users, the ticket is not created.
- Tickets are created from integrated RMM alerts:
    - Tickets are created automatically if a bi-directional alerts-to-tickets synchronization is enabled for the RMM integration.
    - Tickets are created manually from Cyber Protect Cloud alerts via the Cyber Protectconsole.

  When tickets are created from RMM alerts, incoming email, or via the public ticket portal, the following default values are applied:

    - If the requestor is not identified, service desk default values are used (see "Setting default values" (p. 294)).
    - If a ticket is created by an RMM alert, three default values (the **Default SLA**, **Category** and **Priority**) are taken from the default RMM settings (see "Defining default RMM ticket integration settings" (p. 298)).
    - If the requestor is identified, a new ticket is associated with the company service desk settings, default SLA, default priority, default category, default support user, and any devices linked with this specific user.

How are tickets updated?

There are three options for updating tickets in Advanced Automation (PSA):

- Tickets can be manually updated (see "Updating tickets" (p. 211)).
- Via incoming email, when an unread email from an existing email thread is identified and the corresponding ticket is not closed.
- Tickets can be updated automatically by linked alerts from integrated RMM or Cyber Protect Cloud alerts.

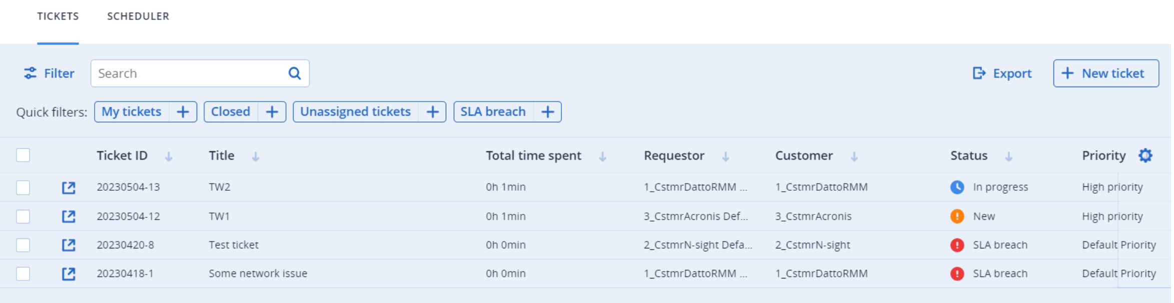
Creating a new ticket

In addition to the automatic creation of tickets by Advanced Automation (PSA) (see "How tickets are created and updated" (p. 207)), you can also manually create a ticket, as described below.

Note
When creating a ticket, many values are pre-filled with the default Service desk settings. These settings can be updated as required, as described in "Service desk settings" (p. 289).

To create a new ticket

1. Go to **Task management > Service desk**. The **Tickets** tab, which lists all the organization's current tickets, is displayed by default.

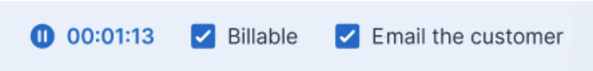


□		Ticket ID	Title	Total time spent	Requestor	Customer	Status	Priority
□		20230504-13	TW2	0h 1min	1_CstmrDattoRMM ...	1_CstmrDattoRMM	In progress	High priority
□		20230504-12	TW1	0h 1min	3_CstmrAcronis Def...	3_CstmrAcronis	New	High priority
□		20230420-8	Test ticket	0h 0min	2_CstmrN-sight Defa...	2_CstmrN-sight	SLA breach	Default Priority
□		20230418-1	Some network issue	0h 0min	1_CstmrDattoRMM ...	1_CstmrDattoRMM	SLA breach	Default Priority

2. Click **+ New ticket**. The Create new ticket dialog is displayed.

   Note
   When Advanced Automation (PSA) is activated for your account, you can also click **New > Client ticket** from the management portal toolbar at the top of the screen, even when you are not in the Service desk module. This option automatically opens the Create new ticket dialog via which you can create a ticket, as described in the following steps.

3. In the header row, the ticket timer is displayed. This timer can be paused and started as required by users working on the ticket. Note that you can also set the ticket timer to automatically pause if the user navigates away from the ticket screen (see "Setting default values" (p. 294)).



   In addition to the ticket timer, you can also select the following check boxes, as required:

   - **Billable**: Selected by default, this option defines if the ticket is billable. Depending on the SLA applied to the ticket (see the steps below), the check box can also be selected or cleared; for example, if the SLA is of the **Subsequent calculation** type, the check box will be selected (to ensure the work reported on the ticket is billable). If the SLA is of the **Fixed price** type, the check box is cleared (to ensure any work on the ticket is not billable).

- **Email the customer**: Selected by default, this option defines if ticket updates are emailed to the end user.

4. Define the following:
   - In the **Ticket title** field, add the title for the ticket.
   - In the **Customer information** section, add the customer details, including the relevant end user who requested the ticket and their manager. Click the **End user** field to select the user from the displayed list; the other fields are auto-populated where relevant.
   - In the **Configuration item or service** section, select one of **Managed service** or **ICT service**:
     - **Managed service**: This option is selected and pre-filled with the relevant details if the Managed service product type is available in the contract. When selected, find the contract part to which the device is assigned, and then verify the SLA on that contract part and apply it to the ticket. Note that if there are no Managed service product types in the contract, this option is disabled.
     - **ICT service**: This option is selected and pre-filled with the relevant details if the ICT (information and communication technology) service product type is available in the contract. When selected, the SLA from the ICT service contract part is applied to the ticket. Note that if there are no ICT service product types in the contract, this option is disabled.
     - The **Configuration item** field shows devices that are linked to the selected Managed or ICT service (**Unknown CI** is shown if there are no integrations or the device is unknown); selecting a device after selecting a service is optional (when you select a device in this scenario, the SLA does not change but remains the SLA that belongs to the service).

       If the configuration item has been linked to a specific user (see "Viewing configuration items" (p. 325)), the relevant device is automatically associated with the ticket when the ticket is created.

       > **Note**
       > The listed devices include those with Acronis products and services (for example, Disaster Recovery, and Cyber Protection), and RMM integrations. If the Acronis product or RMM integration provides a remote control option for a listed device, you can connect remotely from the ticket using the RDP protocol or HTML5 client.

     - In the **Priority** and **SLA** fields, select the relevant ticket priority and SLA.
   - In the **Support agent** section, select the relevant user to be assigned to the ticket (the current user or technician is set by default). You can also select a **Category** for the ticket and **Support group** if relevant.

     You can set the ticket as "unassigned" by selecting **Support group** > **Ticket pool**. This means that until the ticket is assigned to someone, it is considered as unassigned and displayed as such in the **Tickets** tab, dashboards, and reports.

- In the **Ticket description** section, you can:
    - Select the relevant **Status** for the ticket (**New** is displayed by default).
    - Add the relevant recipients in the **To**, **Cc**, and **Bcc** fields. A maximum of 20 recipients can be added to each field.

      If the **End user** field was defined (see above), the selected recipient cannot be removed from the **To** field.

      Note

      The Acronis Advanced Automation (PSA) mobile application does not show the **To**, **Cc**, and **Bcc** fields. However, when the ticket is updated, notifications to the **To**, **Cc**, and **Bcc** recipients are supported. These notifications are sent if the **Email the customer** checkbox is selected.

    - Add rich text descriptions and comments (including images and other media files, up to a maximum of 25 MB) in the displayed text box. Any of the following formats and types can be added or dragged and dropped into the text box:
        - Media: .avi, .mp4, .mp3
        - Emails: .eml, .msg
        - Images: .png, .gif, .jpeg, .jpg, .heic, .bmp, .tiff, .svg
        - Document and log files: .doc, .docx, .xls, .xlsx, .ppt, .pptx, .txt, .log, .pdf
        - Archives: .zip, .rar
    - In the **Canned response** field, click to select a predefined canned response. Note that if you select a canned response, it replaces the rich text description and comments (see the previous bullet). For more information about defining canned responses, see "Creating a canned response" (p. 290).
    - In the **Billing activity type** field, click to select the relevant product name. Note that only products with the attribute **Product for activity-based ticket billing** assigned to them are available.

  Note that the **Ticket description** section can be set to mandatory in the Service desk settings (see "Service desk settings" (p. 289)).
- In the **Schedule** section, enable the **Schedule ticket** option to schedule the ticket with the relevant starting time and date, and duration. See also "Scheduling tickets" (p. 213).

  When **Schedule ticket** is enabled, you can also enable **Recurring tickets** to define a recurring schedule for this ticket. For more information, see "Defining recurring tickets" (p. 214).
- In the **Attachments** section, click to add any relevant attachments.
- In the **Billable items** section, click to add the relevant ticket products that should be linked to the ticket.
- In the **Internal notes** section, click to add notes and actions.

5. Click **Create**. When the ticket is generated, it is added to the **Tickets** tab.

Note
Once you have created tickets, you can export your ticket data at any time by clicking **Export** in the **Tickets** tab. An Excel file is automatically downloaded to your workload.

Updating tickets

To update a ticket

1. Go to **Task management > Service desk**. The **Tickets** tab is displayed by default.
2. (Optional) If you have a large number of tickets, use the filter to locate the relevant ticket(s).

   Click **Filter** (or **Saved filters** if you have previously defined a filter), and select the relevant values from the displayed fields. Note that you can click the **Add to Saved filters** option switch to save the defined filter for future use. Advanced Automation (PSA) also comes with a number of predefined filters, which can be selected as required.

   Alternatively, use the **Search** bar to locate the relevant ticket(s).
3. Click the Ticket row link in the **Tickets** tab.

   To bulk edit a number of tickets, select the relevant tickets in the **Tickets** tab and then click **Bulk edit**. The changes you make are applied to all the selected tickets.

   To open a specific ticket in a new browser tab, click ↗.
4. Modify the ticket as required in any of the displayed tabs:
   - **Activities**: Displays recent activity on the ticket, including the current status, and comments made on the ticket. You can also merge the ticket (see "Merging tickets" (p. 219)) and schedule the ticket (see "Scheduling tickets" (p. 213)) in this tab.

     Note that in this tab you can change the status of the ticket. For example, change it to **In progress** when you start working on it, or move it to **Closed** when it can be closed. When the status is changed to **Closed**, a ticket rating request email is sent to customers. For more information, see "Receiving customer feedback on tickets" (p. 219).

     You can also modify any previous updates to the ticket, which are listed at the bottom of the **Activities** tab. Click the arrow icon next to the relevant ticket update, and in the expanded section, click the pencil icon to modify the duration and/or existing comments.

     Note
     If you change the status of a ticket that was created by an alert in the Cyber Protect console to **Closed**, the alert in the Cyber Protect console is also closed.
   - **Overview**: Displays general ticket settings and customer details and contacts that can be modified as required. For more information, see "Creating a new ticket" (p. 208).

     In the **Support agent** section, you can set a ticket to "unassigned" by selecting **Support group** > **Ticket pool**. However, if you update a ticket assigned to the **Ticket pool** but do not reassign the ticket to another user, the ticket is automatically assigned to you.

You can change devices linked to a ticket; for example, if a ticket is created that does not include the correct device, you can click on the **Configuration item** drop-down list to select the relevant device.

Alternatively, you can click **Open remote desktop** to remotely connect to the selected device or **Go to device** to view additional options available for the currently linked device. These options include access to the integrated RMM platform where applicable:

- **Active issues view**: This opens an external list of issues in the RMM platform.
- **Device Page - Status Tab**: This opens an external RMM page with the device's general information.
- **Device Page - Properties Tab**: This opens an external RMM page with the device's properties.

Note

Only Datto RMM, N-able N-Central, and N-able RMM integrations currently support the option to remotely connect to the selected device. For devices managed by the Acronis platform (for example, with an Acronis agent), you can navigate directly to the linked device's details from a ticket and review its details, initiate a remote connection (if applicable and allowed for the device), manage the device, and so on.

- **Billable items**: Displays any billable items applied to the ticket, which can be updated as required. Products can be added to the ticket and once the ticket is closed and its time is processed, a sales item is automatically created for these products.

  This functionality enables you to bill customers for extra activities and services as part of the ticket. For example, advisory services charged per hour, network cables, or software licenses. Sales items can be billed in the standard way.

  Note the following:

  - Only products defined as **Ticket products** (in the product's settings) can be added to tickets as additional billable items.
  - You need to select the product, its price, and its quantity.
  - Engineers cannot change the standard product price if the **Price adjustable by engineer** check box is not selected in the product's settings.
- **Internal info**: Displays any internal notes or actions that have been applied to the ticket. You can add notes or actions, as required.
- **Last tickets**: (Read only) Displays the last three tickets from the specific user, and the last three tickets from the customer.

Note

The **Billable items**, **Internal info**, and **Last tickets** tabs are not displayed to users assigned the Client manager or Client roles.

For more information about the various fields available when editing a ticket, see "Creating a new ticket" (p. 208).

5. Click **Save changes**.

Scheduling tickets

The **Scheduler** tab displays all tickets that are scheduled for you, and, if you are assigned the Group manager role, for your team. Using this tab, you can easily identify tickets allocated per day and change the view to a monthly, weekly or daily format. You can also schedule tickets for yourself or, if you are a Group manager, schedule tickets for your group.

You can also schedule a ticket from within the ticket itself, as described below.

The **Scheduler** tab also enables you to add new time registrations, approve or decline time off requests, and to sync the **Scheduler** tab with your Microsoft Outlook calendar. When your Outlook calendar is linked, you can also view Outlook events in the **Scheduler** tab. For more details, see "Adding a new time registration" (p. 245) and "Syncing your calendar with Microsoft Outlook" (p. 218).

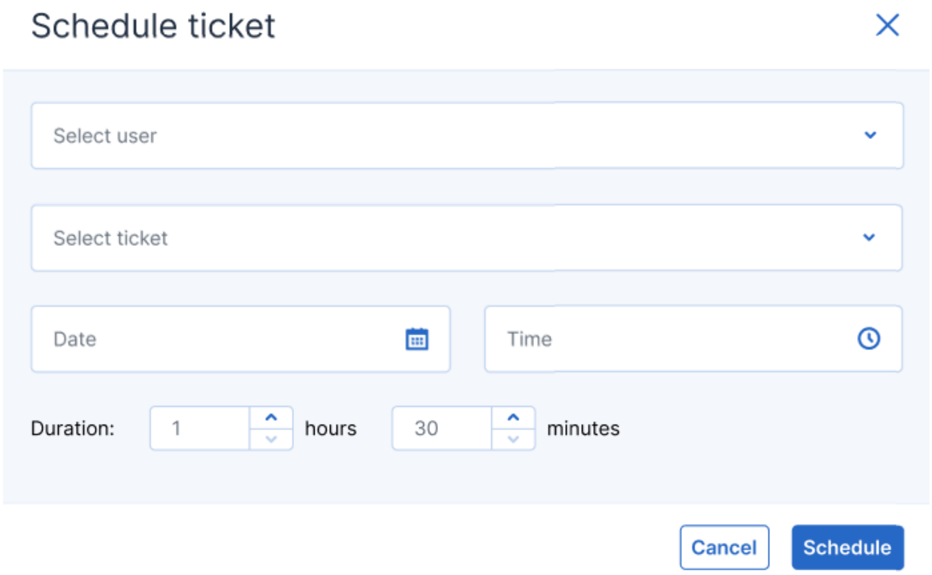
Note
Advanced Automation (PSA) has a built-in predictive ticket handling system. It keeps a six month record of the time spent per ticket category, which aggregates into an average handling time per ticket category. For instance, the system can track how much time your technicians spend on a ticket with category *workstation* and subcategory *install printer driver*. This information is shown on current tickets to calculate the time your team will need to process them. This is also done for individual users, with the calculated values also shown in the **Scheduler** tab.

To schedule a ticket in the Scheduler tab

1. Go to **Task management > Service desk**, and then click the **Scheduler** tab.

   The displayed tab shows several types of events:

   - Time registrations made from tickets
   - Time registrations manually defined in this tab
   - Scheduled tickets
   - Days off and sick leave notices
   - Third party calendar events
2. Select the relevant user from the **Support group** and **Support agent** drop-down lists. Note that these lists are only available to Group managers, and list the relevant users with shared calendars.
3. Click the required day and click **Schedule ticket**. The Schedule ticket dialog is displayed.



4. Select the relevant user (the ticket owner).
5. Select the ticket that you want to schedule. Note that you can also select a ticket that has already been scheduled to reschedule it.
6. Set the date, time, and estimated duration of the ticket.
7. Click **Schedule**. You can now view the scheduled item that you just created.

   Note that you can update scheduled tickets and manual time registrations only.

To schedule a ticket from within the ticket

1. Go to **Task management > Service desk**, and create a new ticket (see "Creating a new ticket" (p. 208)) or locate the relevant ticket in the **Tickets** tab.
2. When creating a ticket, select the **Schedule ticket** checkbox. Then set the start hour and estimated duration of the ticket, and, after completing the rest of the required fields in the dialog, click **Done**.

   Or

   When scheduling an existing ticket, click the **Activities** tab of the relevant ticket, and then select the **Schedule ticket** checkbox. Then click **Save changes**.

   When **Schedule ticket** is enabled, you can also define a recurring schedule for the selected ticket. For more information, see "Defining recurring tickets" (p. 214).

Defining recurring tickets

By defining a recurring ticket, you can automate the creation of service desk tickets for repetitive tasks.

For example, you can:

- Schedule a weekly task to review incident reports and provide status updates.
- Schedule a monthly task to install server updates and send a report.

- Schedule annual tasks to process a domain and SSL certificate renewal.
- Schedule annual IT training sessions for customers.

> **Note**
> Recurring tickets are only available for service desk tickets. Project and quote tickets cannot be set with a recurring schedule.
>
> In addition, recurring tickets - both the original ticket and its recurring instances - are included in dashboards and reports as part of service desk tickets.

To define a recurring ticket

1. Create or update a service desk ticket.
2. [When creating a ticket] Click the **Schedule** section to expand it, and then click the **Schedule ticket** option switch to enable it.

   [When updating a ticket] In the ticket's **Activities** tab, select the **Schedule ticket** checkbox to expand the scheduling section.

   > **Note**
   > If you disable the **Schedule ticket** option in the original ticket, recurring ticket settings are also disabled.
   >
   > If you disable the **Recurring ticket** option, tickets that were previously scheduled to be created will not be created. Any non-modified recurring ticket instances are also deleted and removed from the system. Any modified ticket instances (for example, the ticket was reassigned to a different user) are saved as not scheduled. These saved tickets can only be updated or closed manually.

3. Define the schedule for the ticket. For more information, see "Scheduling tickets" (p. 213).
4. Click the **Recurring ticket** option switch to enable it.
5. Define your recurring settings:
   - Select a start date.

     > **Note**
     > It is possible to select a start date in the past. However, recurring ticket instances are only scheduled for the future. As a result, any recurring instances scheduled in the past (between the start date and today) will not be created.

   - Select the **End by** option to select an end date, or select the **End after** option to end the recurring schedule after a set number of occurrences.
   - Select how new recurring tickets are created from one of the following:
     - Select **When the previous scheduled ticket is closed** to ensure the next scheduled ticket is only created when the previous ticket is closed. Note that the first ticket is created when clicking **Create** (the original ticket is not the first ticket).

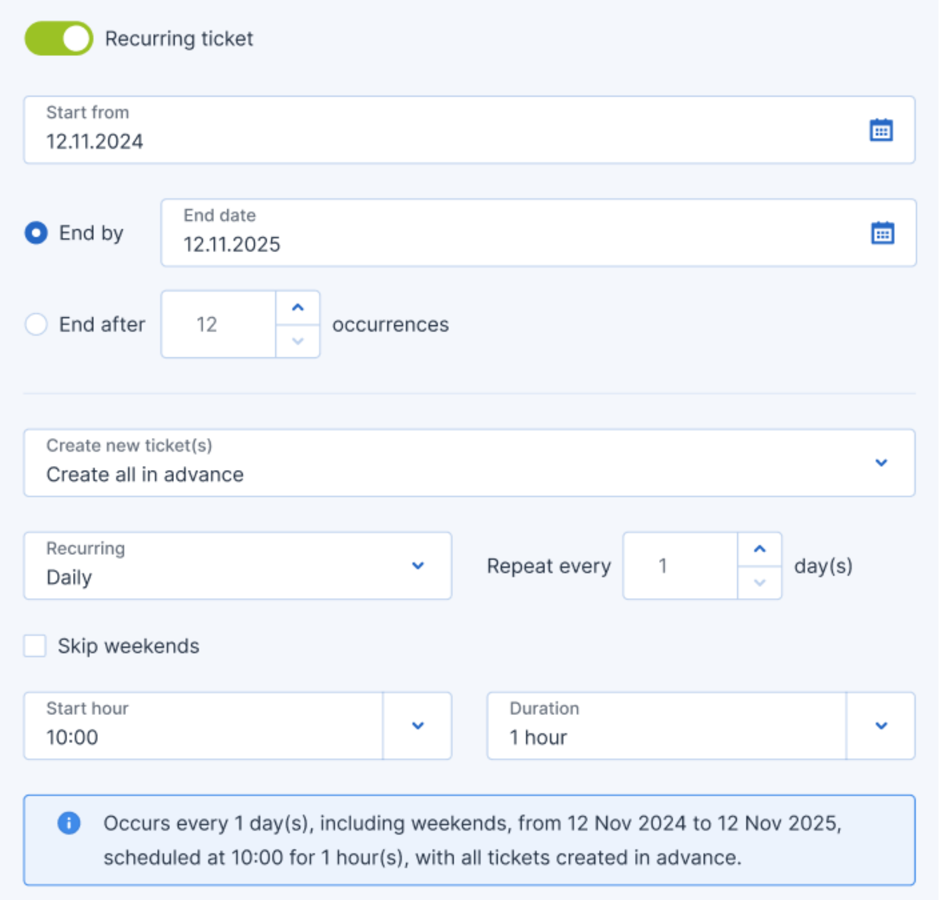
  - Select **A set number of days before the scheduled date** to ensure the ticket is created a set number of days before the scheduled date. Select the relevant number of days, as required.
  - Select **Create all in advance** to create all tickets in advance (up to a maximum of 100). All tickets will be available in your calendar upon clicking **Create**.
- From the **Recurring** dropdown, select from one of **Daily**, **Weekly**, **Monthly**, or **Yearly**. Then define the frequency in the **Repeat every** field. For example, if you want to create a ticket every fortnight, select **Weekly**, and then **2** in the **Repeat every** field.

  When selecting **Daily**, select the **Skip weekends** checkbox to ensure a recurring ticket is not created on the weekend (Saturday and Sunday).

  When selecting **Weekly**, select the relevant day(s) of the week you want the ticket created. For example, if you require a ticket created three times a week, select the relevant days.

  When selecting **Monthly**, select one of the following:

  - A specific day in the month. For example, the 21st of every month. If a ticket is scheduled for the 31st, the ticket is created on the last day of the month for months with less than 31 days.
  - The [first/second/third/fourth] [day of the week] in the month. For example, the second Wednesday of the month.
  - The last [day of the week] in the month. For example, the last Wednesday of the month.
  - The first day of the month.
  - The last day of the month.
- In the **Start hour** and **Duration** fields, define the time and duration in which the recurring ticket should be scheduled.



Recurring ticket

Start from
12.11.2024

● End by — End date
12.11.2025

○ End after 12 occurrences

Create new ticket(s)
Create all in advance

Recurring
Daily

Repeat every 1 day(s)

□ Skip weekends

Start hour
10:00

Duration
1 hour

Occurs every 1 day(s), including weekends, from 12 Nov 2024 to 12 Nov 2025, scheduled at 10:00 for 1 hour(s), with all tickets created in advance.

6. [When creating a ticket] Click **Create**.

   [When updating a ticket] Click **Save changes**.

   The initial recurring ticket is scheduled and can be viewed in the **Scheduler** tab. Any recurring instances of the ticket that are created are also shown in the **Scheduler** tab.

   The recurring instances of the ticket are set with the status of **Activities scheduled**, and include details about the next contact date (the ticket instance date), the date, hour, and duration of the scheduled ticket instance, as well as other details set in the initial ticket.

   For information about updating a recurring ticket schedule and its ticket instances, see "Updating recurring tickets" (p. 217).

Note

Recurring ticket instances are scheduled for a future date. Any ticket instances scheduled in the past (prior to the current date/today) are not created.

Updating recurring tickets

The recurring schedule can only be updated or disabled from the initial ticket in which the schedule was defined. Individual recurring ticket instances cannot be unscheduled or removed, but their date, start time, and duration can be updated.

In addition, note the following:

- When updating the recurring schedule and you need to add or remove tickets:
  - New ticket instances are created according to the new schedule.
  - Any created ticket instances that were updated (for example, with logged time, reassigned users, or the status was updated) are kept as is. New ticket instances will be created if there are no tickets scheduled on the relevant dates in the updated schedule.
  - Any created ticket instances not yet updated are removed from the system.
- If only the **Start hour** and **Duration** fields are modified:
  - Any created ticket instances that were not yet updated will be automatically updated.
  - Any created ticket instances that were updated are kept as is.
- Any other updates made to the original ticket are applied to any new ticket instances that are created.

Syncing your calendar with Microsoft Outlook

You can synchronize tickets in the **Scheduler** tab with Microsoft Outlook, and share your calendar with co-workers.

To sync tickets with Microsoft Outlook

1. Go to **Task management > Service desk**, and then click the **Scheduler** tab.
2. Click **Calendar sync**.
3. Log in to your Outlook account and enable your calendar to synchronize with Advanced Automation (PSA).
4. Select the **Share the Calendar's synced content with everyone** option to share your calendar content with other Advanced Automation (PSA) users.

Approving and declining time off requests

You can approve or decline pending PTO or sick leave requests in the **Scheduler** tab.

Approved and pending PTO or sick days are displayed in the **Scheduler** tab in all view modes (**Day**, **Week**, or **Month**). Approved and pending days are not synced with the user's calendar, if calendar integration is enabled.

Note
Time off requests are displayed according to the Advanced Automation (PSA) role. For example, administrators and managers can see their employees requests, while employees can only view their own schedule.

To approve or decline time off requests

1. Go to **Task management > Service desk**, and then click the **Scheduler** tab.
2. Select the relevant user from the **Support group** and **Support agent** dropdown lists. Note that these lists are only available to Group managers, and list the relevant users with shared calendars.

3. In the displayed calendar, click the relevant pending time off request or sick notice, and then click **View**.
4. [Optional] In the right pane, add a response in the **Comment** field, and then click **Save**.

   In the **Time balance information** section, you can also view the user's remaining balance to confirm they have the relevant days available. You can also view any approved, rejected, or unreviewed time off requests.
5. Click **Approve** or **Decline**.

   The calendar is immediately updated.

   If a request was approved, the user's remaining days off balance is updated.

Merging tickets

When updating a ticket you can also choose to merge it with another existing ticket (which can be in any status but must be linked to the same customer and end user).

Note
Tickets set with a recurring schedule cannot be merged if they are the original ticket in which the schedule is defined. However, recurring instances set by this original ticket can be merged with other service desk tickets, as described below.

To merge a ticket

1. Go to **Task management > Service desk**.
2. In the displayed **Tickets** tab, select the relevant ticket to merge.
3. In the **Activities** tab, select the **Merge ticket** check box.
4. Select the relevant ticket from the list of available tickets, and click **Merge**.
5. In the displayed confirmation message, click **Merge**.

   Note
   The original ticket is no longer available, and will not be included in any active or closed ticket searches. However, any updates or time registrations included in the original ticket are added to the merged ticket.

   In addition, any recipients selected in the **To**, **Cc**, and **Bcc** fields of the original ticket are added to the merged ticket.

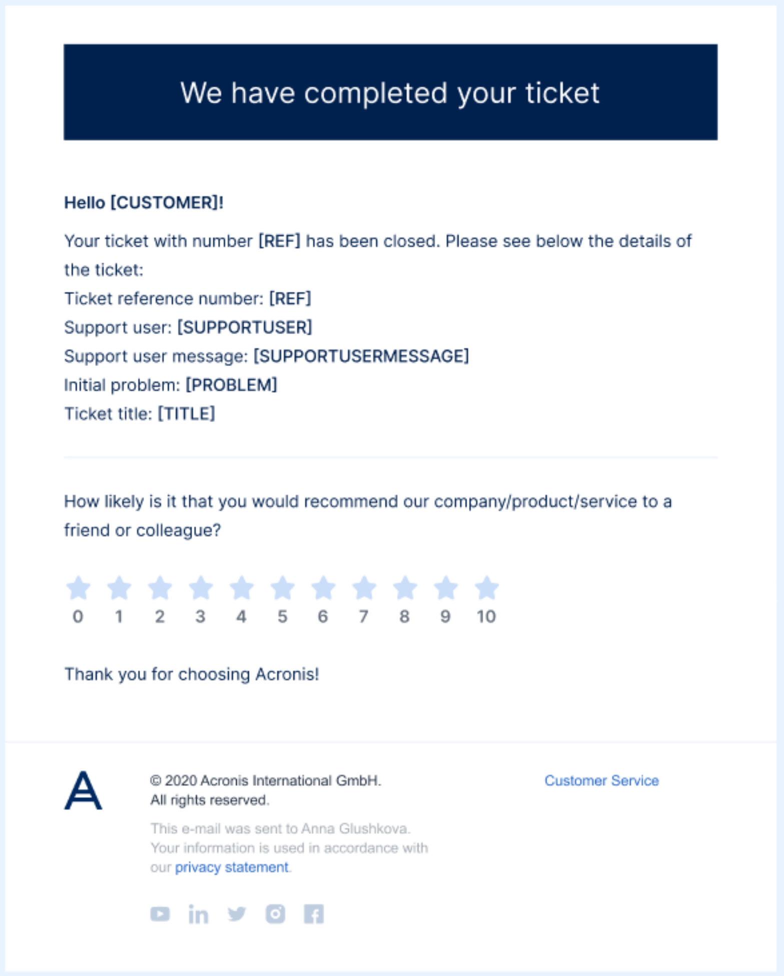
Receiving customer feedback on tickets

When a ticket's status is updated to **Closed**, Advanced Automation (PSA) automatically sends a Ticket rating request email to the customer. This email is included by default in Advanced Automation (PSA), and can be customized as required (see "Managing email templates" (p. 299)). The email is sent only once.

When the customer receives the Ticket rating request email, as shown below, they can rate the ticket as required by clicking on the relevant star rating. Once clicked, they can also add comments. A confirmation message is then displayed to the customer, thanking them for their rating feedback.

To see customer feedback, go to **Task management > Service desk**, and locate and select the relevant ticket. In the displayed right sidebar, click the **Overview** tab to view the feedback.

Note
Customers can submit their ticket rating regardless of their access to the management or Cyber Protect portals. In addition, they do not need access to the Advanced Automation (PSA) service or have a specific Advanced Automation (PSA) role.



We have completed your ticket

Hello [CUSTOMER]!

Your ticket with number **[REF]** has been closed. Please see below the details of the ticket:
Ticket reference number: **[REF]**
Support user: **[SUPPORTUSER]**
Support user message: **[SUPPORTUSERMESSAGE]**
Initial problem: **[PROBLEM]**
Ticket title: **[TITLE]**

How likely is it that you would recommend our company/product/service to a friend or colleague?

☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆
0 1 2 3 4 5 6 7 8 9 10

Thank you for choosing Acronis!

© 2020 Acronis International GmbH.
All rights reserved.

This e-mail was sent to Anna Glushkova.
Your information is used in accordance with our privacy statement.

Customer Service

Embedding the ticket submission form on your website

You can add the public ticket submission form for your end customers by embedding the iframe code included in the following procedure on your website.

To embed the ticket form on a customer website

1. In the Management Portal, go to **Settings** > **Service desk**, and then click the **Default values** tab.
2. Enable the **Public ticket portal** setting, and then click **Save**.

3. Copy the portal URL.
4. Modify your website with the following code.

   Note
   Replace the `src` URL with the portal URL you copied in step 2.

   ```
   <html>
   <body>
   <h1>MSP ticket portal</h1>
   <iframe title="MSP ticket portal" width="800" height="1000" src="https://portal-url">
   </iframe>
   </body>
   </html>
   ```
5. To verify the form works, submit a ticket via the form.

Projects

In the Projects module, you can create, plan, and manage projects.

Use the module's precise budget planning and tracking tools to enhance the profitability of each project. These tools enable you to accurately track your project expenses, monitor the project status, and quickly identify potential or existing delays and budget issues. You can also invoice the relevant customers using flexible billing options with different billing models.

After first defining your project details (see "Creating a project" (p. 223)), you then plan your project phases and steps, the two main elements within every project:

- **Phases**: Phases consist of all the steps required to complete the project phase. Example phases include: planning, designing, project initiation, and final testing.
- **Steps**: You can create multiple steps within a phase. For each step, a ticket is created and assigned to the selected team member.

To access the Projects module, in the Management Portal go to **Task management** > **Projects**.

Note
Project tickets are included in the **Service desk** tab with service desk and quote tickets, but are different from these ticket types in that they are created automatically when you create a project step. For more information, see "Working with project tickets" (p. 235).

Viewing projects

To view all your projects, in the Management Portal, go to **Task management** > **Projects**. In the **Projects** screen, you can view all the tenant's projects in Advanced Automation (PSA).

Information about each project is displayed, including:

- The project name
- The project's current status (**New**, **Pending start**, **In progress**, **Delayed**, **On hold**, or **Completed**)

> **Note**
> The project status is calculated according to the status of the project phases and steps. Each phase and step status is weighted, and the overall project status is calculated based on the following order: **On hold** > **Delayed** > **In progress** > **Pending start** > **New** > **Completed**.
>
> For example, if a project has three phases in the **Pending start**, **Delayed**, and **On hold** status, the project status is shown as **On hold**.
>
> By default, projects with the status of **Completed** are not shown.

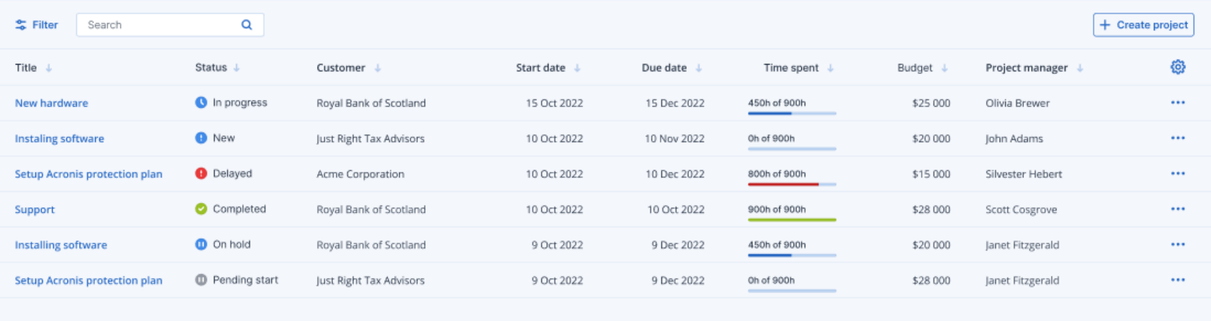
- The customer for whom the project is created
- The project start and due dates
- The time spent on the project by all project team members
- The total project budget

> **Note**
> This is the expected revenue for the project, calculated according to the hours planned multiplied by the product price.

- The assigned project manager

In the far right column of each project row, click the ellipsis icon (...) to open, copy (see "Copying a project" (p. 224)), or delete (see "Updating a project" (p. 226)) the project.

You can also filter and sort the displayed list to locate a specific project. For more advanced filtering, use the **Filter** tool to define which projects should be displayed.



Title	Status	Customer	Start date	Due date	Time spent	Budget	Project manager	⚙
New hardware	In progress	Royal Bank of Scotland	15 Oct 2022	15 Dec 2022	450h of 900h	$25 000	Olivia Brewer	...
Instaling software	New	Just Right Tax Advisors	10 Oct 2022	10 Nov 2022	0h of 900h	$20 000	John Adams	...
Setup Acronis protection plan	Delayed	Acme Corporation	10 Oct 2022	10 Dec 2022	800h of 900h	$15 000	Silvester Hebert	...
Support	Completed	Royal Bank of Scotland	10 Oct 2022	10 Oct 2022	900h of 900h	$28 000	Scott Cosgrove	...
Installing software	On hold	Royal Bank of Scotland	9 Oct 2022	9 Dec 2022	450h of 900h	$20 000	Janet Fitzgerald	...
Setup Acronis protection plan	Pending start	Just Right Tax Advisors	9 Oct 2022	9 Dec 2022	0h of 900h	$28 000	Janet Fitzgerald	...

To view a summary of a specific project, click the project row. In the right pane, you can view a summary of the current finances and progress of the project. You can also view if the project is at risk (usually due to a budget or scheduling issue, as indicated by the **Project health** field). To access and edit the project, click the **Open project** link.

Creating a project

When you create a new project, a wizard guides you through three main steps. In these steps, you can:

- Add basic project information
- Define the project budget
- Define the project team

When you complete the wizard, the project is automatically added to the list of existing projects displayed in the Projects screen. Any existing project can be then be viewed, copied, and updated, as required.

To create a project

1. In the management portal, go to **Task management** > **Projects**.
2. In the Projects screen, click **+ Project**.

   If there are no existing projects, click **Create project**.

   The **Create new project** wizard is displayed.
3. In the **Project information** tab, define the following:
   - **Project title**: The project name.
   - **Customer name**: Select the relevant customer from the drop-down list.

     Note
     If the selected customer does not have billing information defined, an additional **Billing information** tab is added to the project wizard. When you click **Next**, you should complete the relevant billing information fields, including the payment terms and address. This information is then saved and used when selecting the customer in other Advanced Automation (PSA) modules. For more information about the billing information fields, see "Defining billing information for a tenant" (p. 43).

   - **Start date**: The project start date.
   - **Due date**: The date the project is scheduled to end.
   - **Project manager**: Select the relevant user from the drop-down list.
   - **Project sponsor**: Select the relevant customer contact or user from the drop-down list.
   - **Billing model**: Select from one of **Bill per closed step**, **Bill total upfront**, or **Bill based on milestone**. For more information, see "Project billing" (p. 242).
   - [Optional] **Project notes**: Add brief summaries of important project information to the rich text editor.
4. Click **Next**.
5. In the **Project budget** tab, select the relevant products from the displayed list. These project products can be selected during project creation, or at a later stage when the project is already in progress.

You can only change the price of a product if the **Price adjustable per project** field in the product's properties is set to **Yes**. For more information about setting product properties, see "Adding a product" (p. 273).

Note
To include a product in a project, it must be defined as a project product. For more information about adding products, see "Adding a product" (p. 273).

6. Click **Next**.
7. In the **Project team** tab, select the relevant project team members. Team members can be selected now or at a later stage, but must be added to the project before defining project steps.
8. If you defined any custom fields to be applied to projects, the **Additional information** tab is displayed. In this tab, define the custom fields as required. For more information, see "Working with custom fields" (p. 198).

Note
If you defined custom fields to be applied to project steps, they are displayed when creating a project step. For more information, see "Adding project phases" (p. 230).

9. Click **Create**.

   The project is added to the Projects screen, where you can then define additional project details, such as adding the project's phases and steps. For more information, see "Managing projects" (p. 227).

Copying a project

Copy a project to create a new project that is similar to an existing project, without having to manually create all the phases, steps, team members, and budget.

Note
When copying a project, all project steps are set with the status of **New**. In addition, if the project name is not updated, a new project with the same name is displayed in the Projects screen. We recommend you change the name of the new project to avoid confusion.

To copy a project

1. In the management portal, go to **Task management** > **Projects**.
2. In the far right column of the project you want to copy, click the ellipsis icon (...), and then select **Copy**.
3. In the **Project information** tab, define the relevant date in the **Start date** field.

   When the start date is set, the **Due date** field is automatically set based on the original project's settings.

   All other fields are populated according to the project you are copying.

> **Note**
>
> If the original project manager is no longer available due to the new start date, you are prompted to select a new manager from the **Project manager** drop-down list.

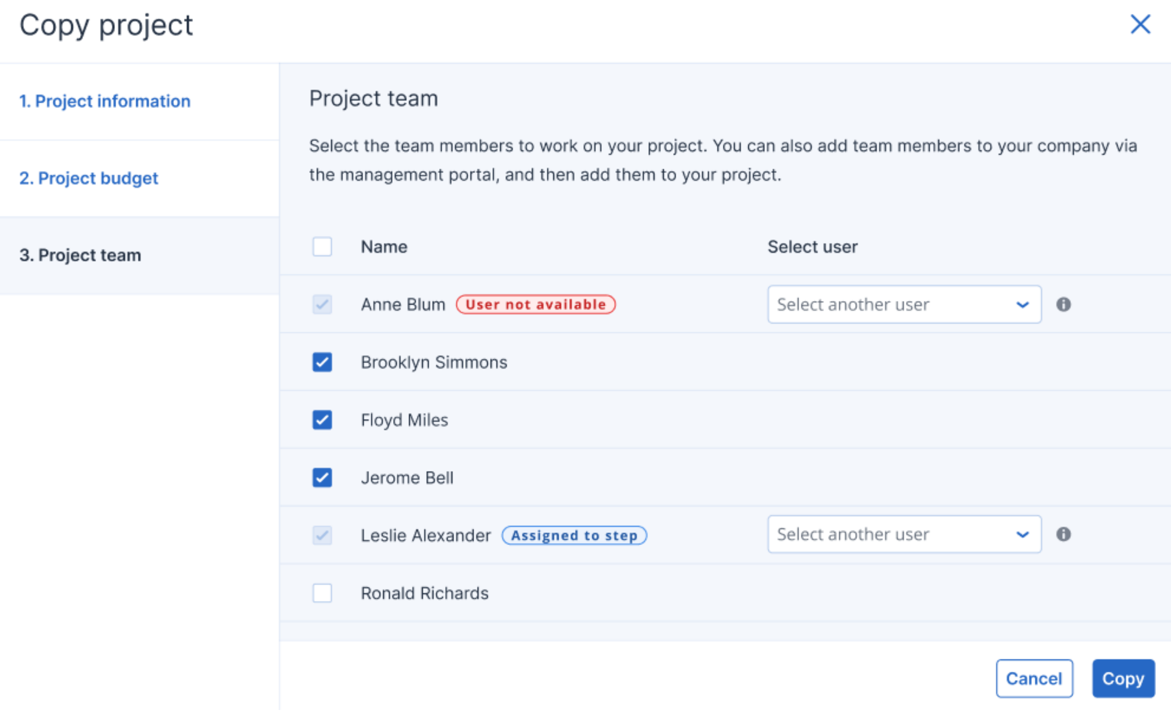
4. Click **Next**.
5. In the **Project budget** tab, define the products for the project.

   Note the following:

   - Prices are set according to the current product price or custom product price for the customer.
   - You cannot remove a product that is assigned to one or more project steps.
   - You can only edit a listed product if the **Price adjustable per project** field in the product's properties is set to **Yes**. For more information about setting product properties, see "Adding a product" (p. 273).
   - The budget cannot be set to less than the time required for the project steps to complete.
   - You can add additional products after the project is copied. For more information, see "Managing projects" (p. 227).
6. Click **Next**.
7. In the **Project team** tab, select the project team members.

   Note the following:

   - If any of the original team are not available, you are prompted to select another user to replace them.
   - You can replace a team member who was assigned tasks in the copied project. These tasks will be assigned to the user replacing the copied team member.
   - You can add or remove team members after the project is copied. For more information, see "Managing projects" (p. 227).



Copy project

1. Project information

2. Project budget

3. Project team

Project team

Select the team members to work on your project. You can also add team members to your company via the management portal, and then add them to your project.

□	Name	Select user
☑	Anne Blum User not available	Select another user
☑	Brooklyn Simmons	
☑	Floyd Miles	
☑	Jerome Bell	
☑	Leslie Alexander Assigned to step	Select another user
□	Ronald Richards	

8. If you defined any custom fields to be applied to projects, click **Next** to display the **Additional information** tab. In this screen, define the custom fields as required. For more information, see "Working with custom fields" (p. 198).
9. When done, click **Copy**.

   The copied project is added to the Projects screen, where you can open it and add or update the relevant phases, steps, budget, and team members. For more information, see "Managing projects" (p. 227).

Updating a project

You can update and delete projects, as required.

You can also update a project even if it is set as **Completed**. You can add new steps to the project, and you can add to or edit the hours logged in a step even after it is set as **Completed**. For additional updates, such as adding or updating products, and updating the schedule, you must create a new step. For more information, see "Adding project steps" (p. 231).

Important
When you delete a project, all of the project's associated items, such as tickets, sales items, and scheduled items, are also deleted. Only sales items that have been billed for are not deleted.

To update a project

1. In the Management Portal, go to **Task management** > **Projects**.
2. In the far right column of the project you want to update, click the ellipsis icon (...), and then click **Open**.

3. In the **Project details** tab, update the project as required. For more information about the available fields and settings, see "Creating a project" (p. 223).

   When updating a project, some fields cannot be modified, such as the **Customer name**, **Start date**, and **Billing model** fields. The **Due date** field cannot be set to a date earlier than any of the existing steps.

   Any products in the budget that are assigned to a step also cannot be modified. In addition, if the product's **Price adjustable per project** setting is set to **No**, the price is disabled.

To delete a project

1. In the Management Portal, go to **Task management** > **Projects**.
2. In the far right column of the project you want to delete, click the ellipsis icon (...), and then click **Delete**.
3. In the confirmation dialog, click **Delete**.

   The project and all of the project's associated items, such as tickets, sales items, and scheduled items, are deleted.

   Note
   Sales items that have been billed for are not deleted.

Managing projects

After you have defined the core details of your project (see "Creating a project" (p. 223)), you can then define and manage additional project elements, including:

- Project phases and steps
- Project team members and their available capacity
- Project tickets

Working with project plans

The project plan is where you define your project phases and steps.

After you have created the project's phases and steps, the project plan provides a quick glance overview of the current status of the project, including its progress. You can also tailor the view according to a table view (the default view) or a Gantt chart format.

Viewing and understanding a project plan

You manage a project in a project plan, where you can define and monitor project phases and steps.

To access the project plan, navigate to the **Project plan** tab. In this tab, you can:

- View the project plan in two different views: the default table view, or a Gantt chart view. For more information, see Project plan views.
- Add project phases and steps. For more information, see "Adding project phases" (p. 230) and "Adding project steps" (p. 231).

- Update and delete project phases and steps. For more information, see "Updating and deleting project phases" (p. 232) and "Updating and deleting project steps" (p. 233).
- View the current status of a phase or step (**Completed**, **New**, **Pending start**, **In progress**, **Delayed**, or **On hold**).
- View the team member assigned to a step, and any capacity issues for the team member that might put the project at risk.
- View the start and due dates of a phase or step.
- View the hours planned for a phase or step, and the hours remaining to complete the phase or step.
- Monitor the current % progress of a phase or step.

> **Note**
> Progress is based on the percentage of work completed, not the time spent.

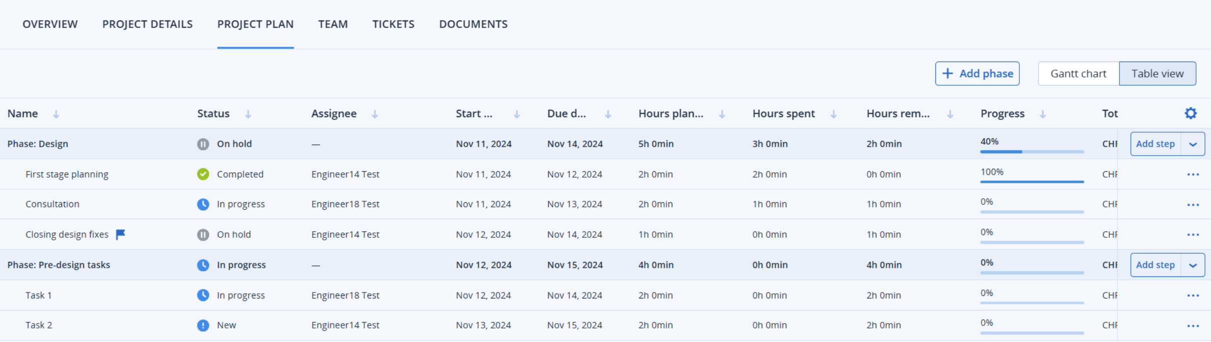
- View the total current monetary value of a phase or step, based on the selected project products, and hours planned.
- Click a link to view the project step ticket.

Project plan views

The project plan can be viewed in two different views, the table view (displayed by default) or the Gantt chart view. In the **Project plan** tab, click **Table view** or **Gantt chart** to display the relevant view.

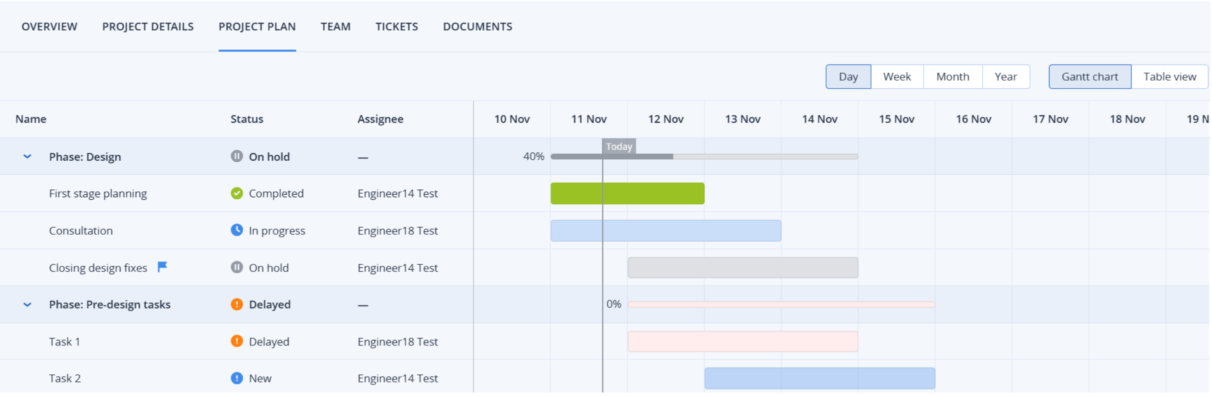
> **Note**
> You can view and edit phases and steps in both views. You can only add new phases and steps in the table view.

The table view displays all the available columns, as well as buttons to add, view, and delete project phases and steps.



Name	Status	Assignee	Start ...	Due d...	Hours plan...	Hours spent	Hours rem...	Progress	Tot	
Phase: Design	On hold	—	Nov 11, 2024	Nov 14, 2024	5h 0min	3h 0min	2h 0min	40%	CHI	Add step
First stage planning	Completed	Engineer14 Test	Nov 11, 2024	Nov 12, 2024	2h 0min	2h 0min	0h 0min	100%	CHF	···
Consultation	In progress	Engineer18 Test	Nov 11, 2024	Nov 13, 2024	2h 0min	1h 0min	1h 0min	0%	CHF	···
Closing design fixes	On hold	Engineer14 Test	Nov 12, 2024	Nov 14, 2024	1h 0min	0h 0min	1h 0min	0%	CHF	···
Phase: Pre-design tasks	In progress	—	Nov 12, 2024	Nov 15, 2024	4h 0min	0h 0min	4h 0min	0%	CHI	Add step
Task 1	In progress	Engineer18 Test	Nov 12, 2024	Nov 14, 2024	2h 0min	0h 0min	2h 0min	0%	CHF	···
Task 2	New	Engineer14 Test	Nov 13, 2024	Nov 15, 2024	2h 0min	0h 0min	2h 0min	0%	CHF	···

The Gantt chart view, as shown below, provides a more visual display of the project's progress, enabling you to track the status of phases and steps, and quickly identify potential or existing delays. You can view the chart in four different time periods: **Day**, **Week**, **Month**, or **Year**.



Name	Status	Assignee
Phase: Design	On hold	—
First stage planning	Completed	Engineer14 Test
Consultation	In progress	Engineer18 Test
Closing design fixes	On hold	Engineer14 Test
Phase: Pre-design tasks	Delayed	—
Task 1	Delayed	Engineer18 Test
Task 2	New	Engineer14 Test

Note

Only phases that include steps are displayed in the Gantt chart view.

In addition, only phases show an indication of the phase progress (as a %). The progress of individual steps is not shown in the Gantt chart view.

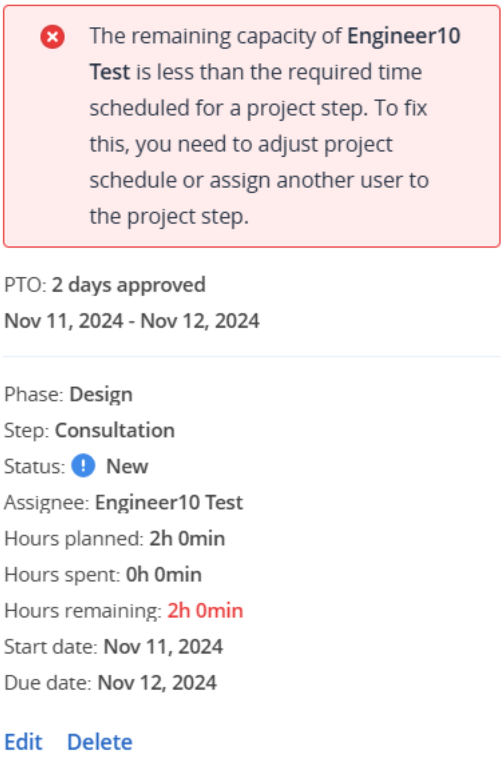
The Gantt chart provides a more visual understanding of any issues or delays. The above example shows a **Delayed** step (Task 1) and the visual impact it has on the project. The phase is also set as **Delayed**, and both the phase and step are highlighted on the Gantt chart.

Project steps can also be highlighted as **Overdue** if the due date of the step has passed, or if the step's completed date is after the due date. Similarly, if any team members assigned to project steps have capacity issues, these are also highlighted in the chart with **User capacity issue**.

Note

The visual highlights of a step issue on the Gantt chart, for example if it is **Overdue** or has a **User capacity issue**, provide an indication only that there is an issue, and do not automatically update the phase status. The status of a phase is calculated automatically based on the status of the steps, which can only be updated manually.

Click on the step to view more details, and then adjust the step details accordingly. For example, the team member assigned to the step might not have enough available hours to work on the step. You are prompted to adjust the project schedule or assign another user to the step. For more information, see "Reassigning team members to project steps" (p. 239).



⊗ The remaining capacity of **Engineer10 Test** is less than the required time scheduled for a project step. To fix this, you need to adjust project schedule or assign another user to the project step.

PTO: **2 days approved**
Nov 11, 2024 - Nov 12, 2024

Phase: **Design**
Step: **Consultation**
Status: ❗ **New**
Assignee: **Engineer10 Test**
Hours planned: **2h 0min**
Hours spent: **0h 0min**
Hours remaining: **2h 0min**
Start date: **Nov 11, 2024**
Due date: **Nov 12, 2024**

Adding project phases

You can add phases to any project, regardless of the project status.

To add a project phase

1. In the management portal, go to **Task management** > **Projects**.
2. In the far right column of the project you want to add phases to, click the ellipsis icon (...), and then select **Open**.
3. Click the **Project plan** tab.
4. If you are adding the first phase to the project, click **Create phase**.

   If you are adding additional phases to the project, click **Add phase**.
5. Enter a name for the phase, and click **Create**.

   The phase is added to the relevant project, and you can now add steps to the phase. For more information, see "Adding project steps" (p. 231).

   Note
   The phase status is calculated according to the status of the project steps. Each step status is weighted, and the phase status is calculated based on the following order: **On hold** > **Delayed** > **In progress** > **Pending start** > **New** > **Completed**.

   For example, if a phase has three steps in the **Pending start**, **Delayed**, and **On hold** status, the phase status is shown as **On hold**.

Adding project steps

You can add steps to any project, regardless of the project status.

To add a project step

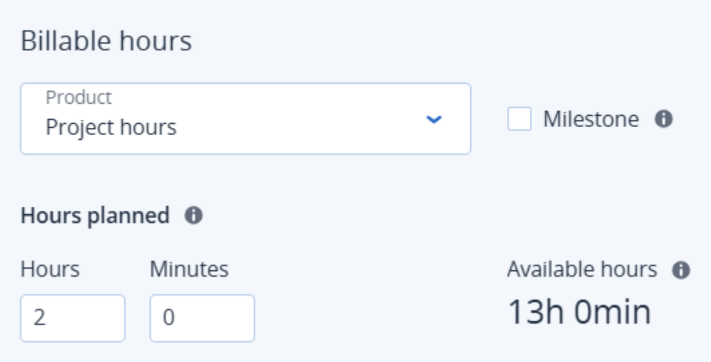
1. In the Management Portal, go to **Task management** > **Projects**.
2. In the far right column of the project you want to add steps to, click the ellipsis icon (...), and then select **Open**.
3. In the **Project plan** tab, click **Add step** in the relevant project phase row.
4. In the **Step information** section, define the following:
   - **Title**: The step name.
   - **Notes**: An optional text description of the step.
   - **Assignee**: Select the relevant team member from the dropdown.
   - **Status**: Select one of **New** (set by default), **In progress**, **Delayed**, **Pending start**, or **On hold** from the drop-down list.
   - **Start date**: Define a start date for the step. The date you select will start from 00:00:00.

     Note
     When you create the first step in a project, the project start date is automatically set as the default start date for the step.

   - **Due date**: Define a due date for the step. The date you select will end at 23:59:59.

     Note
     The step due date must be within the project start and due dates.

5. In the **Billable hours** section, do the following:
   - Select the relevant product to assign to the step. Only products that were added to the project budget are available for selection.
   - In the **Hours planned** sub-section, define the number of hours and minutes the step should take. The number of hours should not exceed the displayed **Available hours**.
   - If you want the step to be a milestone, select the **Milestone** checkbox. This ensures the step will be automatically billed for when your billing model requires payment for each completed milestone. For more information, see "Project billing" (p. 242).



Billable hours

Product: Project hours

□ Milestone

Hours planned

Hours: 2

Minutes: 0

Available hours: 13h 0min

6. If you defined any custom fields to be applied to project steps, an **Additional information** section is displayed. In this section, define the custom fields as required. For more information, see "Working with custom fields" (p. 198).
7. Click **Save**.

   Alternatively, click **Save this step and add a new step** to save the step and add another step. Repeat the procedure above, as required.

   The saved step is added to the relevant project phase.

   A project ticket is also created, in which time spent on the step should be logged. The ticket can be viewed in the **Tickets** tab. For more information, see "Working with project tickets" (p. 235).

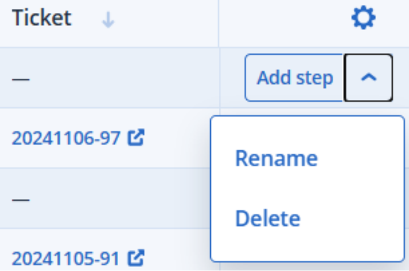
Updating and deleting project phases

You can update a project phase by renaming it, regardless of the status of the phase. You can rename and delete the phase in both the table or Gantt chart views.

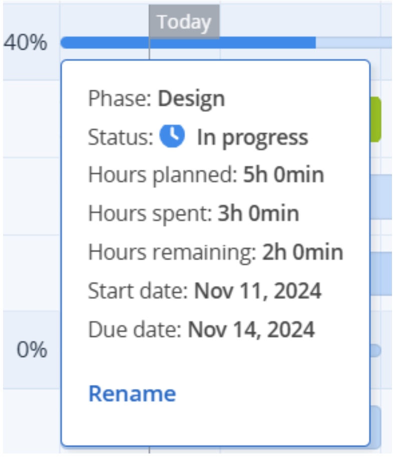
Note
You can only delete a phase if its status is set as **New**. Any project step tickets and logged time are also deleted.

To rename a phase

1. In the Management Portal, go to **Task management** > **Projects**.
2. In the far right column of the project you want to update, click the ellipsis icon (...), and then select **Open**.
3. [In the table view] In the **Project plan** tab, click the arrow icon next to the **Add step** menu in the relevant project phase row, and then select **Rename**.



   [In the Gantt chart view] In the **Project plan** tab, click **Gantt chart**. Click the relevant phase node, and in the displayed popup, click **Rename**.



Phase: Design
Status: In progress
Hours planned: 5h 0min
Hours spent: 3h 0min
Hours remaining: 2h 0min
Start date: Nov 11, 2024
Due date: Nov 14, 2024

4. In the **Rename phase** dialog, enter a new name for the phase, and click **Rename**.

To delete a phase

1. [In the table view] In the **Project plan** tab, click the arrow icon next to the **Add step** menu in the relevant project phase row, and then select **Delete**.

   [In the Gantt chart view] In the **Project plan** tab, click **Gantt chart**. Click the relevant phase node, and in the displayed popup, click **Delete**.

   Note
   If the project phase status is set to anything other than **New**, it cannot be deleted.

2. In the confirmation dialog, click **Delete**.

   All steps (including any step tickets and logged time) under the phase are deleted. In addition, the project status and progress-related metrics are re-calculated to take into account the deleted phase and steps.

Updating and deleting project steps

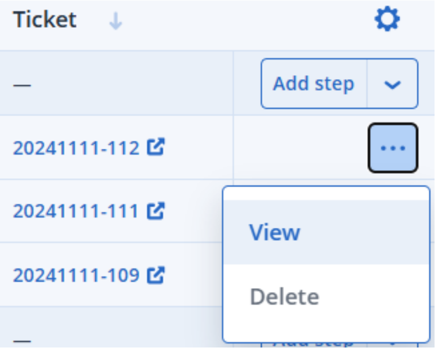
You can update the details of a project step (including its status, the assigned team member, and start and due dates) and billable hours for any step that is not set as **Completed**. You can also delete any step that is set as **New**.

You can update and delete project steps in both the table or Gantt chart views.

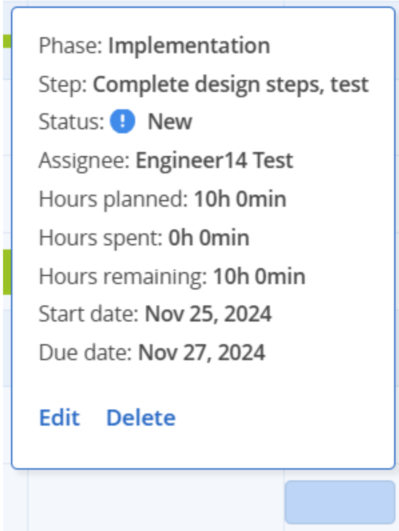
Note
If the project step is already in progress, or set to any status other than **New**, it cannot be deleted.

To update a project step

1. In the Management Portal, go to **Task management** > **Projects**.
2. In the far right column of the project you want to update, click the ellipsis icon (...), and then select **Open**.
3. [In the table view] In the **Project plan** tab, click the ellipsis icon (...) in the relevant project step row, and then select **View**.



[In the Gantt chart view] In the **Project plan** tab, click **Gantt chart**. Click the relevant phase step, and in the displayed popup, click **Edit**.



Phase: Implementation
Step: Complete design steps, test
Status: ! New
Assignee: Engineer14 Test
Hours planned: 10h 0min
Hours spent: 0h 0min
Hours remaining: 10h 0min
Start date: Nov 25, 2024
Due date: Nov 27, 2024

4. In the right pane, click the pencil icon to update the relevant fields in the **Step information** and **Billable hours** sections.

   For more information about the available fields and settings, see "Adding project steps" (p. 231).
5. Click ✓ to confirm your changes.

   The changes are applied to the step's existing ticket. In addition, the project status and progress-related metrics are re-calculated to take into account the updated step.

To delete a project step

1. [In the table view] In the **Project plan** tab, click the ellipsis icon (...) in the relevant project step row, and then select **Delete**.

   [In the Gantt chart view] In the **Project plan** tab, click **Gantt chart**. Click the relevant step, and in the displayed popup, click **Delete**.

   Note

   A project step can only be deleted if its status is set as **New**.

2. In the confirmation dialog, click **Delete**.

The project status and progress-related metrics are re-calculated to take into account the deleted step. For example, hours planned for the step are released, and can be used in other project steps. The ticket for the deleted project step is also deleted.

Working with project tickets

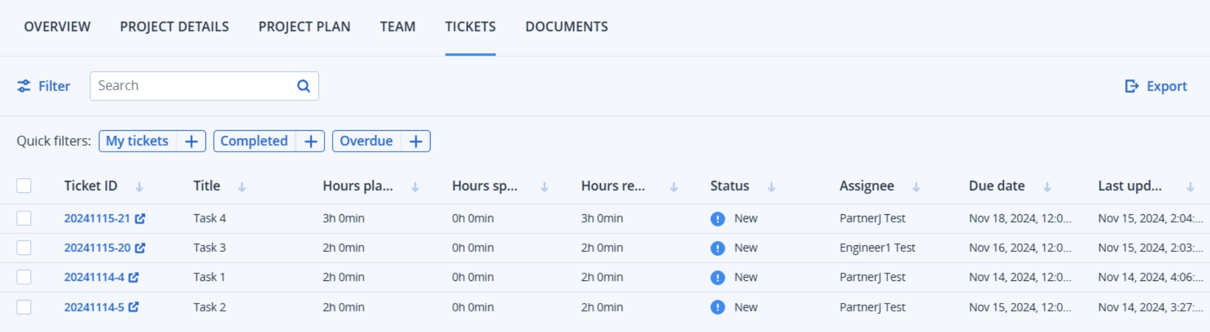
Project tickets enable you to track time spent on project steps. Any time spent working on a project step must be logged under the relevant project ticket.

Advanced Automation (PSA) creates project tickets automatically when a project step is created. When a change is made to the project step, the relevant information is updated in the project ticket. When the status of a project ticket is updated, the project step status is also updated.

Note
Project steps can only be completed by setting the project ticket status to **Completed**.

All project tickets are displayed in the **Tickets** tab of the relevant project. In this tab, you can see the status of each ticket (which is also the status of the project step), the hours already spent on the ticket, the team member assigned to the ticket, and when the ticket was last updated. For more information about tracking time and work in the ticket itself, see "Viewing and editing a project ticket" (p. 235).

You can also export the contents of the **Tickets** tab by clicking **Export**. A file in XLS format is automatically created and downloaded.



□	Ticket ID	Title	Hours pla...	Hours sp...	Hours re...	Status	Assignee	Due date	Last upd...
□	20241115-21	Task 4	3h 0min	0h 0min	3h 0min	New	PartnerJ Test	Nov 18, 2024, 12:0...	Nov 15, 2024, 2:04:...
□	20241115-20	Task 3	2h 0min	0h 0min	2h 0min	New	Engineer1 Test	Nov 16, 2024, 12:0...	Nov 15, 2024, 2:03:...
□	20241114-4	Task 1	2h 0min	0h 0min	2h 0min	New	PartnerJ Test	Nov 14, 2024, 12:0...	Nov 14, 2024, 4:06:...
□	20241114-5	Task 2	2h 0min	0h 0min	2h 0min	New	PartnerJ Test	Nov 15, 2024, 12:0...	Nov 14, 2024, 3:27:...

Note
Project tickets can also be viewed in the **Service desk** module, but are not displayed by default. Go to **Task management** > **Service desk**, and use the **Filter** tool to select and display **Project** ticket types.

Viewing and editing a project ticket

You can view, edit, and track the time and progress of any project ticket.

Important
Time spent on the project step must be recorded in the project ticket. Time spent on a project cannot be logged anywhere else within Advanced Automation (PSA).

In each ticket, you can:

- Log time spent on the project step.
- Complete the project step (project steps can only be completed by setting the project ticket status to **Completed**).
- Add a comment, or canned response.
- Email updates to the customer (who is defined as the project sponsor when creating the project).
- Change the project step status (only if the ticket has not been set as **Completed**).
- Attach files.
- Schedule the ticket (which does not change the step start or due date). This enables you to adjust the ticket schedule more precisely if, for example, you set the scheduled time to less than the project step time frame.

To update a project ticket

1. In the Management Portal, go to **Task management** > **Projects**.
2. In the far right column of the project you want to update a ticket for, click the ellipsis icon (...), and then select **Open**.
3. Click the **Tickets** tab.
4. In the list of project step tickets, click the ticket you want to update.

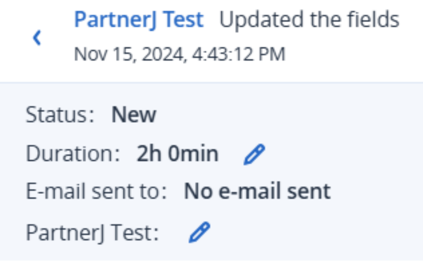
> **Note**
> You can also access the project step ticket from the **Project ticket** section in the relevant project step in the project plan.

5. Using the timer at the top of the project step pane, define the relevant time spent on the project step.

00:30:27

6. Select the **Email the customer** checkbox if you want to send ticket updates to the customer.
7. In the ticket's **Activities** tab:
   - Click the **Status** dropdown list to update the ticket status to one of **Completed**, **New**, **Pending start**, **In progress**, **Delayed**, or **On hold**.
     Note that when a ticket is set to **Completed**, the associated project step is automatically set as **Completed**. The ticket cannot be reopened, or its status updated. However, you can log additional time to the ticket, if required.
   - In the text box, add rich text descriptions and comments, including images and other media files, up to a maximum of 25 MB (the supported formats and types are listed below under the **Attach files** link).
   - Click **Attach files** to upload files. Attachments can include any of the following formats and types (up to a maximum of 25 MB):
     - Media: .avi, .mp4, .mp3
     - Emails: .eml, .msg
     - Images: .png, .gif, .jpeg, .jpg, .heic, .bmp, .tiff, .svg

  - Document and log files: .doc, .docx, .xls, .xlsx, .ppt, .pptx, .txt, .log, .pdf
  - Archives: .zip, .rar
- In the **Canned response** dropdown list, select the relevant canned response. The response is added to the text box.
- Select the **Schedule ticket** checkbox if you want to schedule the ticket for a specific time and date. The time frame you set for the schedule does not affect the hours planned for the step, and is used to block some time on your calendar. You can view scheduled tickets in the **Scheduler** tab, which is accessed from the **Service desk** module.
- In the lower section of the tab, you can view recent actions performed on the ticket. Click the arrow icon alongside each action to edit some of the fields, such as the time spent on the ticket, or add additional comments.



PartnerJ Test Updated the fields
Nov 15, 2024, 4:43:12 PM

Status: New
Duration: 2h 0min
E-mail sent to: No e-mail sent
PartnerJ Test:

Note
If the **Duration** field is updated, the **Hours spent** field is also recalculated.

8. In the ticket's **Overview** tab:
   - If you want to update the ticket details, click **Edit project step**. You can also access links to the project and the project step in the **Project information** section.
   - In the **Attachments** section, upload any files you want to add to the ticket.
9. Click **Save changes**.

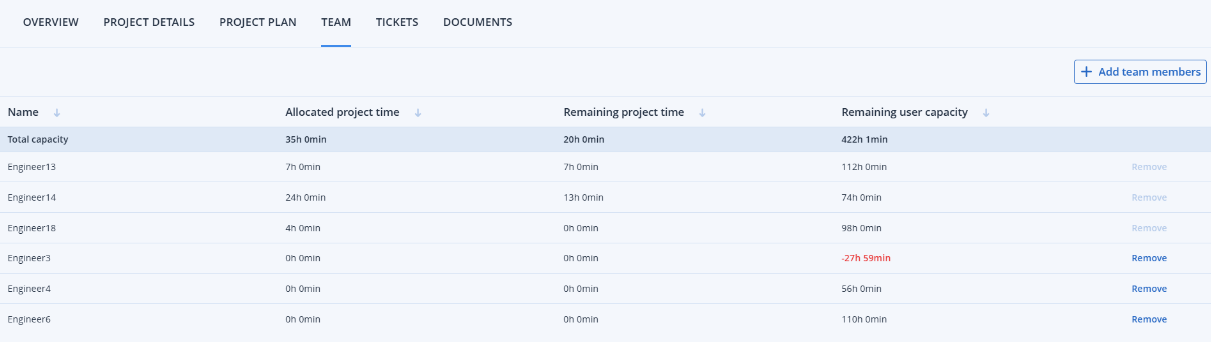
   Any updates to the ticket, such as additional logged time, is added to the project. The progress-related metrics are re-calculated to take into account the updated ticket.

   Time logged on the ticket is also shown in the **Time registration** tab, accessed from the **Service desk** module. For more information, see "Time entries" (p. 244).

Managing the project team

In the selected project's **Team** tab, you can add additional team members to your project (see "Adding team members to a project" (p. 238)), check planned and remaining work, and review the user capacity for each of your team members (see "Reviewing team member capacity" (p. 240)).

The initial project team is defined when creating the project (see "Creating a project" (p. 223)). As the project progresses, you might want to reassign steps to other team members, due to capacity issues. This is done through the project plan, where you manage the project's phases and steps, or in the **Team** tab. For more information, see "Reassigning team members to project steps" (p. 239).



Name	Allocated project time	Remaining project time	Remaining user capacity	
Total capacity	35h 0min	20h 0min	422h 1min	
Engineer13	7h 0min	7h 0min	112h 0min	Remove
Engineer14	24h 0min	13h 0min	74h 0min	Remove
Engineer18	4h 0min	0h 0min	98h 0min	Remove
Engineer3	0h 0min	0h 0min	-27h 59min	Remove
Engineer4	0h 0min	0h 0min	56h 0min	Remove
Engineer6	0h 0min	0h 0min	110h 0min	Remove

Adding team members to a project

You can add and remove team members to and from a project, as required.

Note
You cannot remove a team member from a project if they are currently assigned to a project step.

To add team members

1. In the management portal, go to **Task management** > **Projects**.
2. In the far right column of the project you want to add team members to, click the ellipsis icon (...), and then select **Open**.
3. Click the **Team** tab, and then click **Add team members**.
4. In the Add team members dialog, select the relevant team members from the displayed list.

   Note
   Team members can be selected from users assigned an Advanced Automation (PSA) role. You can add additional users for selection by navigating to **Company management > Users** and then defining the relevant users.

5. Click **Add**.

   The selected team members are added to the project, and can be assigned to the relevant project steps.

To remove team members

1. In the **Team** tab of the selected project, click **Remove** in the relevant team member row.

   Note
   The **Remove** option is disabled if a team member is assigned to a project step. To remove the team member from the project, you first need to remove them from the relevant project step(s), and reassign the step(s) to another team member. For more information, see "Reassigning team members to project steps" (p. 239).

2. In the confirmation dialog, click **Remove**.

Reassigning team members to project steps

You can reassign team members to and from project steps when:

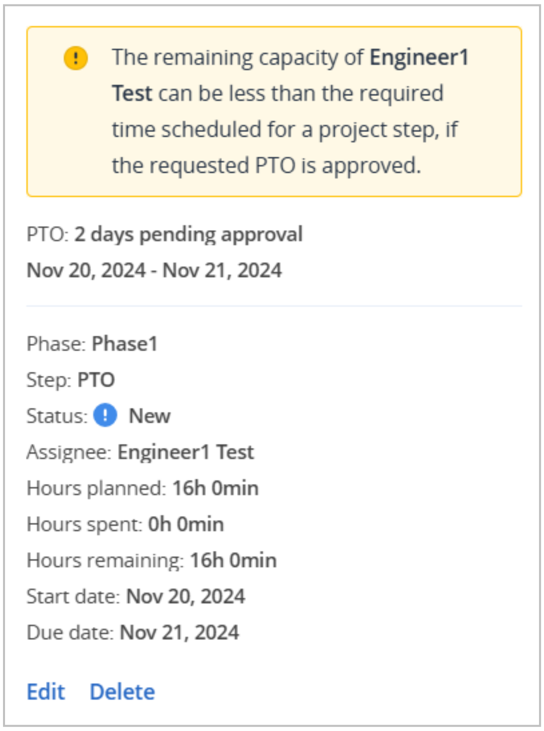
- You need to reassign team members if, for example, a different team member is a better fit for the step.
- There is a team capacity issue. For example, pending PTO or sick leave for an existing team member will put the project at risk of delay. For more information about understanding team capacity, see "Reviewing team member capacity" (p. 240).

Team members should be reassigned through the project plan, as described below. For more information about working in the project plan, see "Project plan views" (p. 228).

To reassign team members to project steps

1. In the Management Portal, go to **Task management** > **Projects**.
2. In the far right column of the project of which you want to reassign team members, click the ellipsis icon (...), and then select **Open**.
3. Click the **Project plan** tab.
4. Click the step that is highlighted with a user capacity issue (highlighted in red) or warning (highlighted in yellow).

   The example below indicates that if the pending PTO is approved, the team member's capacity might be impacted.

   ! The remaining capacity of **Engineer1 Test** can be less than the required time scheduled for a project step, if the requested PTO is approved.

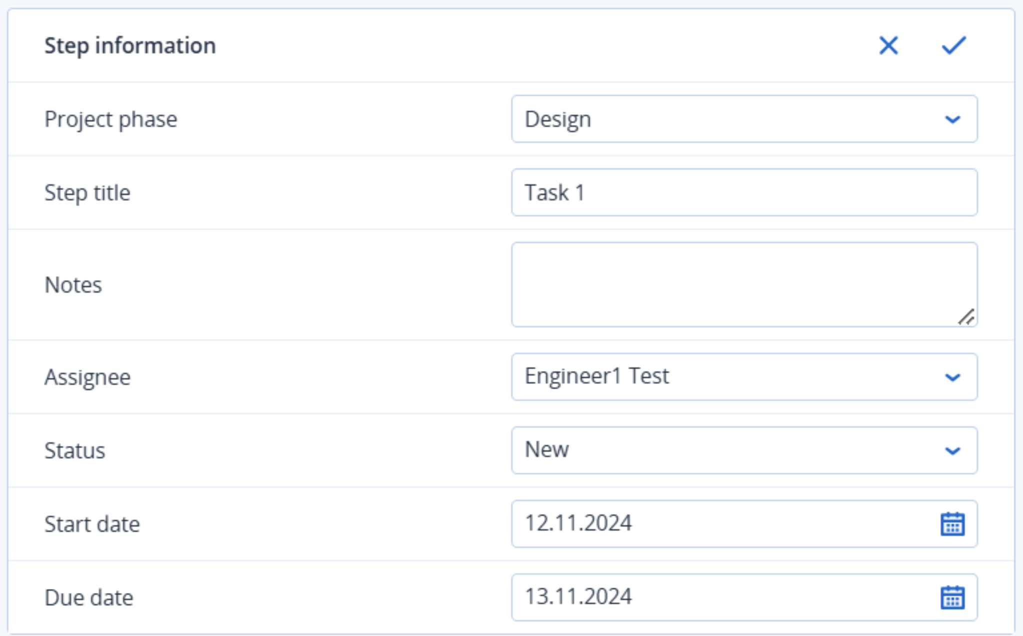
   PTO: **2 days pending approval**
   Nov 20, 2024 - Nov 21, 2024

   Phase: **Phase1**
   Step: **PTO**
   Status: ! **New**
   Assignee: **Engineer1 Test**
   Hours planned: **16h 0min**
   Hours spent: **0h 0min**
   Hours remaining: **16h 0min**
   Start date: **Nov 20, 2024**
   Due date: **Nov 21, 2024**

5. Click **Edit**.

   The right pane shows information about the step, including details about the currently assigned team member.
6. In the **Step information** section, click the pencil icon.

7. In the **Assignee** dropdown, select the relevant team member to replace the current team member assigned to the step.



Step information

Project phase	Design
Step title	Task 1
Notes	
Assignee	Engineer1 Test
Status	New
Start date	12.11.2024
Due date	13.11.2024

8. Click ✓.

   The project status and progress-related metrics are re-calculated to take into account the reassigned team member.

Reviewing team member capacity

Team member capacity refers to a team member's available working time for a project (in hours and minutes).

The team member capacity is calculated according to all the team member's available working hours in the project period (from the current day onwards), minus any approved PTO or sick leave, any assigned time to other Advanced Automation (PSA) tickets (other than project tickets), and any remaining time in other project steps from other projects. Capacity issues occur when the team member's available working hours is less than hours required to complete a project step.

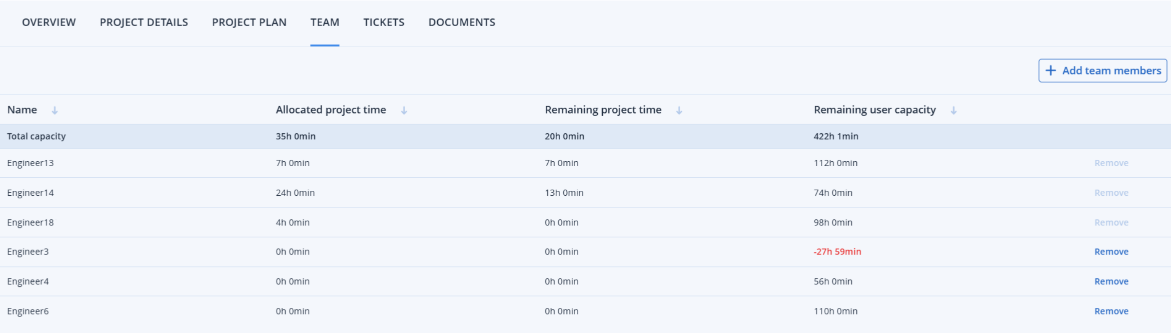
Any issues that occur with team member capacity are displayed:

- At the project step level, in the **Project plan** widget of the **Overview** tab, as described below.
- In individual project steps in the **Project plan** tab. For more information, see "Project plan views" (p. 228).

You can also view the current availability, or capacity, of project team members in the **Teams** tab of the selected project, as described below.

To review team member capacity in the Team tab

1. After accessing the relevant project, click the **Team** tab.
   The current list of project team members is displayed. The **Remaining user capacity** column shows each team member's current capacity.

Name	Allocated project time	Remaining project time	Remaining user capacity	
Total capacity	35h 0min	20h 0min	422h 1min	
Engineer13	7h 0min	7h 0min	112h 0min	Remove
Engineer14	24h 0min	13h 0min	74h 0min	Remove
Engineer18	4h 0min	0h 0min	98h 0min	Remove
Engineer3	0h 0min	0h 0min	-27h 59min	Remove
Engineer4	0h 0min	0h 0min	56h 0min	Remove
Engineer6	0h 0min	0h 0min	110h 0min	Remove

2. Click a team member row to view the following details:
   - **Allocated project time**: Shows the total planned hours for the steps assigned to the team member.
   - **Remaining project time**: Shows the team member's remaining project time (in hours and minutes) in their assigned steps.

     Note
     The **Remaining project time** value is equal to the hours planned less the reported hours spent. The value shown includes time logged by other team members who worked on the step.

     For example, a project step assigned to team member A is allocated ten hours. Team member A has not yet reported any time for the step, but team member B has reported three hours for the step. In this scenario, the remaining project time for the step assigned to team member A is seven hours.

   - **Remaining user capacity**: Shows the team member's available working time for a project (in hours and minutes).
     If there is an issue with the team member's capacity, the **Remaining user capacity** field is highlighted in red and an alert message is displayed at the top of the pane. Capacity issues occur when the **Remaining user capacity** value is less than the **Remaining project time** value.
   - **Days off**: Shows details of approved (and pending approval) PTO and sick leave during the project period.

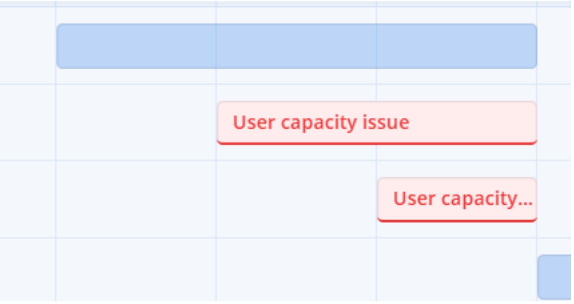
   To resolve capacity issues, you need to adjust the project schedule, or assign another user to the relevant project step(s). For more information, see "Reassigning team members to project steps" (p. 239).

To review team member capacity at the project step level

1. In the Management Portal, go to **Task management** > **Projects**.
2. In the rightmost column of the relevant project, click the ellipsis icon (...), and then select **Open**.

3. In the **Overview** tab, scroll down to the **Project plan** widget.

   Any team member capacity issues are displayed in the widget, as shown below.

4. Click the issue to view more details, and then adjust the step details accordingly. For example, the team member assigned to the step might not have enough available hours to work on the step. You are prompted to adjust the project schedule or assign another user to the step. For more information, see "Reassigning team members to project steps" (p. 239).

   The team member capacity is recalculated when a team member is added to or removed from the project, or when the project is updated and the update impacts the allocated project time, remaining project time or remaining capacity.

Project billing

Project activities are billed as sales items that are created automatically according to the project's billing model, which is defined when creating the project.

The created project sales items can be updated, deleted (if they have not yet been billed for), and billed for using regular billing runs within Advanced Automation (PSA). For more information about working with sales items, see "Managing sales items" (p. 258).

There are three billing models available in the **Projects** module:

- **Bill per closed step**: A new sales item is created automatically when a ticket linked to a project step is completed. For more information, see Billing per closed step.
- **Bill total upfront**: A new sales item is created automatically when a project is created with at least one project product selected. For more information, see Billing the total upfront.
- **Bill based on milestone**: A new sales item is created automatically when a step that is marked as a **Milestone** step is completed. For more information, see Billing based on milestones.

Billing per closed step

When the **Bill per closed step** billing model is enabled, a sales item is generated when a team member completes a project step.

When the associated project ticket is set to **Completed**, you can still log or edit time, and add comments and attachments, but you cannot change dates, planned hours, or the status. A sales item is generated according to the planned hours for the project step, and the customer is billed according to the existing billing flow in Advanced Automation (PSA).

Billing the total upfront

When the **Bill total upfront** billing model is enabled, there are three possible ways in which a sales item is created:

- **When a project with a budget is created**: If a project is created (by creating a new project from scratch, or by copying an existing project) with a budget (meaning at least one project product is selected), a sales item is automatically generated. You can bill the customer according to the existing billing flow.
- **When a project without a budget is created**: If a project is created (by creating a new project from scratch, or by copying an existing project) without a budget (meaning no project products are selected), no sales item is generated. Before creating the sales item, you first need to set the project budget by adding project products and allocating the relevant hours. You should then create a sales item manually, to match the project budget. You can then bill the customer according to the existing billing flow.
- **When updating a project**: If you are working on a project and need to increase the budget, but the customer has already been billed for the budgeted hours, you need to create a sales item manually. The sales item should match the increase in the project budget. You can then bill the customer according to the existing billing flow. If the customer was not billed, you can update the project budget and the existing sales item.

Billing based on milestones

When the **Bill based on milestone** billing model is enabled, a sales item is generated when a team member completes a project step which is set as a **Milestone** step.

The sales item includes line items for each completed step (including the latest milestone step) since the last milestone step was completed, or after the project started:

- On completion of the first milestone, all steps completed since the project was started are billed for.
- On completion of the next milestone, all steps completed since the last completed milestone are billed for. From that point on, if any other project steps are worked on and set as **Completed**, they are included in the bill when the next milestone project step is completed.

Setting the default project billing entity

Advanced Automation (PSA) enables you to create multiple billing entities. This means that you can bill from multiple businesses, and each billing entity will have its own invoice settings, background, and so on. In the **Project management** screen of the service desk settings, you can set the default billling entity for sales items created for project billing.

To set the default project billing entity

1. Go to **Settings > Service desk**, and then select **Project management**.
2. Click **Edit**, and then select the relevant billing entity.
3. Click **Save**.

Time entries

The **Time entries** module enables you to manage users' time records and track their day-to-day activities.

To access the Time entries functionality, in Management Portal go to **Task management** > **Time entries**. In the displayed **Time registration** tab, you can view all current time entries that are registered in Advanced Automation (PSA). In this tab and the additional Time entries tabs, you can:

- Add new time registrations
- View and modify existing time registrations
- Review and approve time registrations
- Request days off
- Add and review sick notices
- Review and approve PTO requests
- Export time registration data

What are time entries / time registrations?

Time can be registered in Advanced Automation (PSA) in two ways:

- **Automatically**: Automatic time registrations are created as a result of someone working on a service desk ticket. The time worked on the ticket is captured automatically by a built-in ticket timer; it can also be modified by a ticket engineer.
- **Manually**: Manual time registrations are submitted by engineers manually. For more information, see "Adding a new time registration" (p. 245).

Proper and regular time registration enables you to increase your billable time. It also provides a good overview of your business metrics with Advanced Automation (PSA) built-in reports, including time spent on a specific client, your engineers' occupancy rates, and others.

Viewing existing time registrations

To view existing time registrations, in Management Portal go to **Task management** > **Time entries**. In the displayed **Time registration** tab, you can view all current time registrations that are registered in Advanced Automation (PSA).

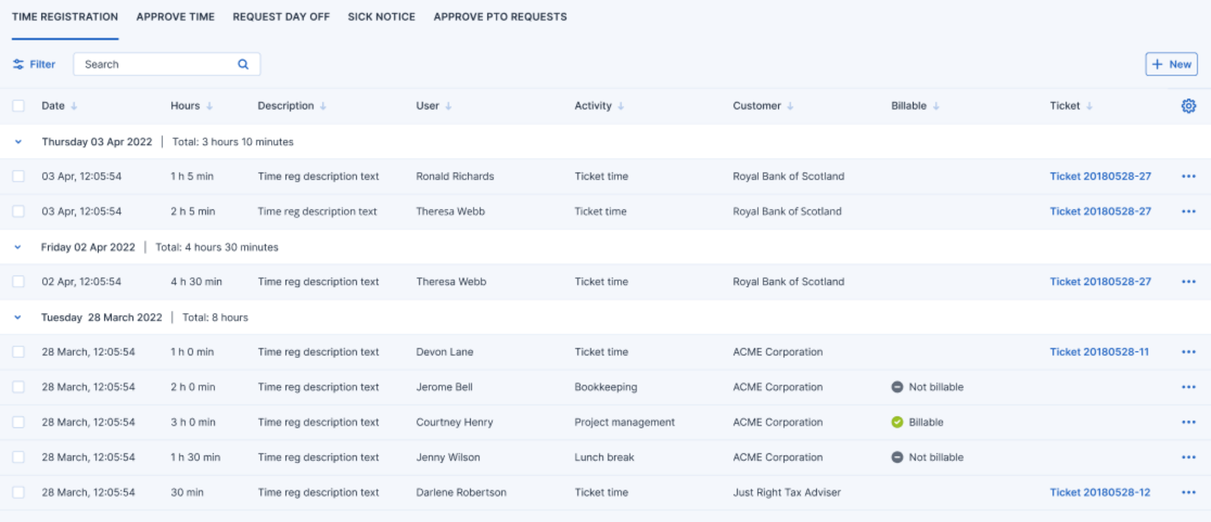
Information about each entry is displayed, including:

- The hours registered
- The specific user who performed the task
- The type of activity
- The customer
- If the time registration is billable or not
- A link to the relevant ticket (if relevant)

Time registrations are grouped by date, and the total hours for each day is displayed.

To export time registration data, select the relevant time registrations and then click **Export to XLS**. An XLS file called **Time registrations** is downloaded to your workload.

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



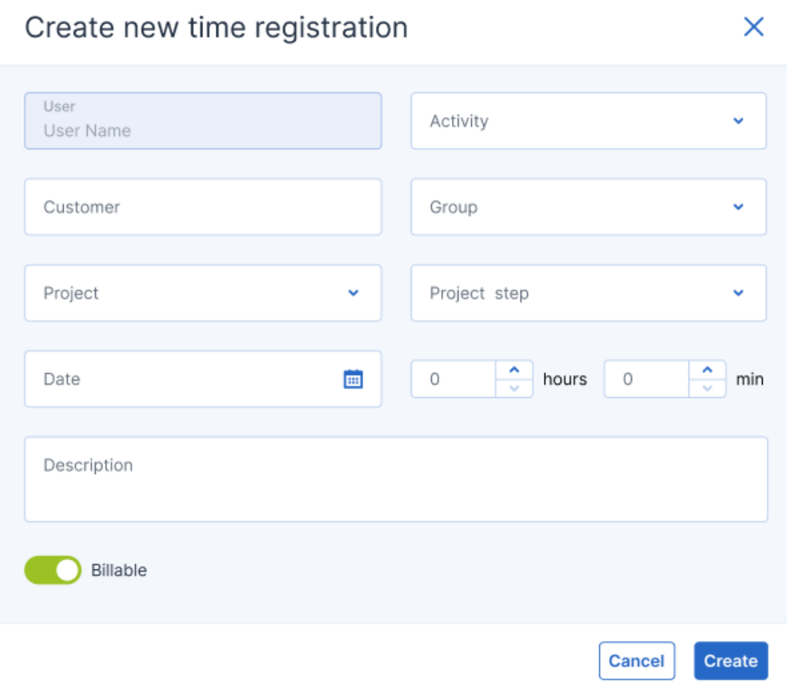
□	Date	Hours	Description	User	Activity	Customer	Billable	Ticket	⚙
	Thursday 03 Apr 2022 | Total: 3 hours 10 minutes								
□	03 Apr, 12:05:54	1 h 5 min	Time reg description text	Ronald Richards	Ticket time	Royal Bank of Scotland		Ticket 20180528-27	•••
□	03 Apr, 12:05:54	2 h 5 min	Time reg description text	Theresa Webb	Ticket time	Royal Bank of Scotland		Ticket 20180528-27	•••
	Friday 02 Apr 2022 | Total: 4 hours 30 minutes								
□	02 Apr, 12:05:54	4 h 30 min	Time reg description text	Theresa Webb	Ticket time	Royal Bank of Scotland		Ticket 20180528-27	•••
	Tuesday 28 March 2022 | Total: 8 hours								
□	28 March, 12:05:54	1 h 0 min	Time reg description text	Devon Lane	Ticket time	ACME Corporation		Ticket 20180528-11	•••
□	28 March, 12:05:54	2 h 0 min	Time reg description text	Jerome Bell	Bookkeeping	ACME Corporation	⊖ Not billable		•••
□	28 March, 12:05:54	3 h 0 min	Time reg description text	Courtney Henry	Project management	ACME Corporation	✓ Billable		•••
□	28 March, 12:05:54	1 h 30 min	Time reg description text	Jenny Wilson	Lunch break	ACME Corporation	⊖ Not billable		•••
□	28 March, 12:05:54	30 min	Time reg description text	Darlene Robertson	Ticket time	Just Right Tax Adviser		Ticket 20180528-12	•••

Adding a new time registration

By manually adding a new time registration you can log the time spent working on tickets. This enables you to see what engineers are spending their time on, and, combined with other Advanced Automation (PSA) metrics and reports, determine the relevant resources required for specific projects.

To add a new time registration

1. Go to **Task management > Time entries**. The **Time registration** tab is displayed by default.
2. Click **+ New**. The following dialog is displayed.



Note

When Advanced Automation (PSA) is activated for your account, you can also click **New > Time registration** from the management portal toolbar at the top of the screen, even when you are not in the Time entries module. This option automatically opens the Create new time registration dialog via which you can create a time registration, as described in the following steps.

3. Define the following:
    - **Activity**: Select the relevant activity from the **Activity** drop-down list. For more information about activities, see "Defining activities for time tracking" (p. 323).
    - **Customer**: Select the relevant customer from the **Customer** drop-down list. You can select your own organization, which will make this entry not billable. To register work for a specific client, enter the client name.
    - **Group**: Select the relevant group (the department you are making the registration for) from the **Group** drop-down list. Only groups in which you are included are displayed.
    - **Project**: Select the relevant project from the **Project** drop-down list. This option is only available if you are assigned to a project team.
    - **Project step**: Select the relevant project step from the **Project step** drop-down list. This option is only available if you are assigned to a project team and steps in the project are not closed.
    - **Date**: Define the relevant date.
    - **Time period**: Define the length of the time registration (in hours and minutes).
    - **Description**: Enter a description for the activity.
    - **Billable**: Click the **Billable** option switch to register this activity as billable. This option is only available if you have selected a customer.

Note

When creating a new time registration, the **User** field is automatically filled with your name.

4. Click **Create**.

Editing a time registration

Note

You can only edit a time registration if it has not been processed. For more information about the processing of time registrations, see "Approving time registrations for billing" (p. 248).

To edit a time registration

1. Go to **Task management > Time entries**. The **Time registration** tab is displayed by default.
2. Click on the time registration that you want to edit.
3. In the right sidebar, click the pencil icon to edit the time registration. For more information about the available fields, see "Adding a new time registration" (p. 245).
4. When done, click ✓.

Billable time registrations

Advanced Automation (PSA) includes two main billable time entry scenarios:

- Automatic time registration when working on generic tickets and alert tickets.
- Manual time entries.

Note

Regardless of the time entry scenario, the MSP administrator ultimately determines if time is billed or not. This means that any of the selections in the sections below can be overruled, as required.

For more information about working with sales items, see "Managing sales items" (p. 258).

Automatic time registration when working on generic tickets and alert tickets

Note the following:

- This time can be non-billable when the applicable SLA has the **Fixed price** option enabled (in an "all-in" SLA); this time can be billable when the applicable SLA has the **Subsequent calculation** option enabled.
- The billing rate can be based on several scenarios:
  - Default billing rate for office hours work.
  - Default billing rate for outside office hours work if the timestamp of the ticket update is outside the SLA coverage timeframe.
  - Specific billing rate for the customer (custom pricing).

  - Specific billing rate based on the work types in the ticket. For example, Update 1 in the ticket is for 1 hour of standard support work, and Update 2 in the ticket is for 1 hour and the 'Network engineering' activity type is selected in the ticket. The end result is that the customer is billed for two different rates; note however, that billing rates can be overruled by custom pricing settings.

Manual time entries

This time can be marked as billable time. A specific billing rate can be configured for each manual time registration activity type. Note that this rate can be overruled by custom pricing settings (for more information, see "Working with custom prices" (p. 266)).

Approving time registrations for billing

You can approve the following time registrations recorded in Advanced Automation (PSA) and listed in the **Approve time** tab:

- Time registrations not yet approved, meaning reported ticket time from tickets that are in the **Closed** state only, or for manual time registrations.
- Time entries that meet the threshold of the minimal time spent on a ticket (which is defined in the billing settings, see "Billing settings" (p. 326)). For example, if the threshold is set to **5**, time entries with less than five minutes are not listed.

Note
Time registrations can only be approved by users with the following roles: Administrator, Director, Group manager, Finance manager

Each listed time registration includes the full details of each activity and also enables you to process and bill the associated customers. You can approve single or multiple time registrations as billable to customers; alternatively, you can define time registrations as pending, or non-billable.

Important
You cannot approve a customer's reported ticket time if billing information is not provided for that customer. When you attempt to approve ticket time registrations, you are prompted to add billing information for the relevant customers. For more information, see Provide billing information.

To approve a time registration

1. Go to **Task management > Time entries**. Then click the **Approve time** tab.

   The list of time registrations awaiting approval is displayed. Information displayed includes the customer, the date and title of the time registration, and its duration.

Note

If ◔ is displayed next to the Duration column, this indicates some of the registered time was recorded beyond the time frame of the relevant SLA. For more details about learning what time was billed, follow the steps below.

2. (Optional) To verify the details of a specific time registration, select the relevant row. The details for the selected time registration are displayed in the right sidebar:
   - You can click **Process** to create a sales item for this time registration and **View ticket** to see the actual ticket. See Step 4 for details of how Advanced Automation (PSA) handles the time registration when clicking **Process**.
   - In the **Overview** section, you can view general details for the time registration. You can also edit the information, and enable the **Block hours** option switch (if block hours are enabled on the contract level, such as an agreement for "all-in" support work for 20 hours per month). If there is an available balance of block hours (such as unused support hours), the time registration is deducted from this balance without creating an extra sales item. You can redefine this default rule as required, and still bill for the recorded time if needed.
   - In the **SLA billable time** section, you can see the actual customer's round-up time value (in minutes) that will be used to round up the total billable time. You can view and edit the total rounded time per billing rate. For example, you can select the relevant billing rate and manually adjust the final billable time.
   - In the lower section of the sidebar, you can review details of the ticket's time registrations, if required. For each time registration the following details are available:
     - The user that made the time registration.
     - The user's support group name.
     - The date and time of the time registration.
     - The user's hourly rate.
     - A description of the time registration.
3. After verifying or editing the time registration, click in the relevant row and select from one of the following options in the **Approve time** tab:
   - **Billable**: Select this option to bill the relevant customer and to generate an invoice.

     Note

     Advanced Automation (PSA) automatically pre-selects whether a ticket is to be billed based on the SLA (you can override this by selecting the relevant option). When a manual time entry is marked as **Billable** during its creation (see "Creating a new ticket" (p. 208)), Advanced Automation (PSA) marks it as **Billable** in the **Approve time** tab. If required, you can change the billing option to **Pending**.

   - **Not billable**: Select this option if you do not want to bill the selected time registration.
   - **Pending**: Select this option to keep the time registration in the list after processing any billable items.

You can also select multiple time registrations, as required. When selected, the relevant action buttons are enabled above the list of time registrations. Select from **Mark as billable**, **Mark as not billable**, **Mark as pending**, or **Process** (see the following step).

4. Click the **Process** action button to process the selected time registrations.

   If a time registration was set as **Billable**, a sales item is created with the relevant company details for the customer. In addition, if there are multiple time registrations selected, multiple rows are added to the sales item. The generated invoice includes the ticket title, ticket number, and billable time based on the applicable rate.

   If a time registration was set as **Not billable**, it is removed from the **Approve time** tab.

   If a time registration was set as **Pending**, it remains in the **Approve time** tab.

Requesting days off

You can view and update your day off requests in the **Request day off** tab. This tab displays all the day off requests you have created and their details, including if they have been approved or not. You can also request additional days off, as required.

Note
Day off requests are based on the **Days off per year** and **Remaining days off policy** fields in the service desk default settings. For more information, see "Setting default values" (p. 294).

To request days off

1. Go to **Task management > Time entries**, and then click the **Request day off** tab.
2. Click **+ New**.
3. In the displayed dialog, select one of the following:
   - **Request one day**: Select the relevant day, and time (by default, eight hours is selected).
   - **Request multiple days**: Select the relevant start and end dates.
4. Enter a description for the request, and click **Create**.

   If you requested multiple days off, one request is registered for each day.

   Note
   You can also edit day off requests that are awaiting approval (click on the relevant row in the list of requests and then edit as required). When the request has been approved or declined, it cannot be edited.

Creating a sick notice

You can view and update all sick notices waiting approval in the **Sick notice** tab. You can also create a new sick notice for any user in your account.

Note
Sick notices can only be created by users with the following roles: Administrator, Director, Group manager, Finance manager, HR

To create a new sick notice

1. Go to **Task management > Time entries**, and then click the **Sick notice** tab.
2. Click **+ New**.
3. In the displayed dialog, define the following:
   - **User**: Select the user that you want to create the sick notice for.
   - **Request one day**: Select the relevant day, and time (by default, eight hours is selected).

     Or

     Request multiple days: Select the relevant start and end dates.
4. Enter the sick notice description and click **Create**.

   If you requested multiple sick days, one request is registered for each day.

   Note
   You can also edit sick notice requests that are awaiting approval (click on the relevant row in the list of sick notices and then edit as required). When the sick notice has been approved or declined, it cannot be edited.

Approving PTO and sick leave requests

You can view and update PTO and sick leave requests from all users in the **Approve PTO request** tab. You can approve or decline a PTO or sick leave request, as required.

Note
PTO requests can only be approved by users with the following roles: Administrator, Director, Group manager, Finance manager

To approve PTO requests

1. Go to **Task management > Time entries**, and then click the **Approve PTO request** tab.
2. In the list of requests, select the relevant request, and then click **Approve** or **Decline**.

   You can also select multiple requests, as required.

   If a request was approved, it is removed from the displayed list in the **Approve PTO request** tab, and the user's remaining days off value is updated. If a request was declined, it is also removed from the **Approve PTO request** tab.

   The **Type** column indicates the type of request, **PTO** or **Sick leave**.
3. (Optional) Click a request row to view the details of the request. You can also add a comment, if required.

   Note that the **Remaining time balance** field in the **Time balance information** section shows the remaining value in days, hours and minutes. This value is calculated as the difference between the permitted number of days off over the year (which is set as part of your service desk's default values; see "Setting default values" (p. 294)) and the total amount of all already approved PTO requests during the current year.

Managing sales and billing functionality

The Sales and billing module (in the management portal, go to **Sales and billing**) is where you can manage the following functionality:

- Quotes
- Sales items
- Contracts
- Invoices
- Ledgers
- Products
- Custom prices

Note
Before proceeding with this section, ensure that you have fully set up your account in the **Settings** section, including the creation of products.

Sales

The **Sales** module enables you to manage the following:

- Quoting
- Sales items
- Contracts
- Custom prices

To access the **Sales** module, in the management portal go to **Sales and billing** > **Sales**.

Managing quotes

Use Advanced Automation (PSA) quote functionality to provide customers with quotes for your products and services. When a quote is approved, it is then automatically converted to a number of tasks to help you track and deliver the quote delivery status:

- A generic quote ticket is created for the approved quote as a task to track its progress, keep notes and log time spent on the task.
- A purchase order ticket is created for quote items that need to be purchased in order to fulfill the quote. The ticket can be also used by your team members to track its progress, keep important notes such as purchase details, and log time spent on the task.
- Quote items for contract products are automatically converted to new contracts and contract parts, or are added to existing client contracts, depending on the quote's original setup for such quote items.

To access the quotes functionality, go to **Sales and billing** > **Sales**, and then click the **Quotes** tab. The **Quotes** tab shows all the quotes you have created for customers.

Note
This feature is only available for users assigned the following roles: Administrator, Director, Engineer, Group manager, Finance manager, Finance, Sales

Creating a quote

When you create a new quote, an onscreen wizard guides you through the main steps. In these steps, you will:

- Add basic quote information.
- Add products and/or quote templates to the quote.
- Review and send the quote (or save to edit and send at a later date).

To create a quote

1. In the management portal, go to **Sales and billing > Sales**.
2. Click the **Quotes** tab, and then click **+ New**. Note that if you haven't yet created a quote, you are prompted to click **Create new**.

   Note
   When Advanced Automation (PSA) is activated for your account, you can also click **New** > **Quote** from the management portal toolbar at the top of the screen, even when you are not in the Sales module. This option automatically opens the new quote wizard via which you can create a quote, as described in the following steps.

3. In Step 1 of the displayed new quote wizard, define the following:
   - **Description**: Enter a description for the quote.
   - **End-user**: Select the relevant end user. The selected user will receive the quote when it is sent for approval.

     Note
     If the selected end user does not have billing information defined, an additional **Billing information** step is added to the quote wizard. When you click **Next**, you should complete the relevant billing information fields, including the payment terms and address. This information is then saved and used when selecting the end user in other Advanced Automation (PSA) modules. For more information about the billing information fields, see "Defining billing information for a tenant" (p. 43).

   - **Company name**: This field is automatically filled with the relevant company when the **End-user** field is defined.
   - (Optional) In the free text editor box, define a quote preface. This text can include a brief introduction and description of the quote. For example: *Thank you for requesting a quote for new laptops. We have included a list of our very latest models.* You can also add formatting and images to the text, as required.
4. Click **Next**. The next step of the new quote wizard is displayed.

5. Click **Add template** or **Add product** to select the relevant template or product.
   - If you click **Add template**: You are prompted to select a quote template; click **Add** to add the relevant template to the quote. You can select additional quote templates and/or products, as required.
   - If you click **Add product**: Select the relevant category in the **Product category** field. Then select a product from the available list in the **Products** field.

     If the product you selected is a non-contract product (such as a standard sales item, like a piece of hardware), define the **Inventory item**, **Quantity**, and **Discount** fields, as applicable. Note that the **Price** and **Description** fields are automatically filled with the selected inventory item's details.

     If the product you selected is a contract product (such as repeated billing for managed services) the following additional fields are displayed:
     - **Invoice interval**: Select from **Every month**, **Quarterly**, **Semi-annually**, or **Every year**.
     - **When to bill**: Select from **Upfront** or **Afterwards**.
     - **Payment method**: Select from **Manual payment** or **Direct debit**. The **Direct debit** option enables customers to pay invoices via wire transfer or by using one of the payment integrations (PayPal, Stripe) - they can also send the invoice to their local bank for direct debit processing.
     - **Contract period (months)**: Select the relevant number of months (regardless of the option you selected in the **Invoice interval** field).
6. Click **Add** to add the product to the quote.

   If you want to add additional products, in the displayed summary screen click **Add template** or **Add product**.

   Note

   If any of the products you selected include mandatory fields that were not completed, you are prompted to complete these fields for the relevant products before proceeding.
7. Click **Next**. The last step of the new quote wizard is displayed.
8. Review the quote, and select one of the following:
   - Click **Save** to save the quote. It is not sent to customers, but can be edited as required and sent at a later date.
   - Click **Save and send** to save and send the quote to the selected user.

When the quote is accepted or rejected by the customer by email or phone, you can mark the quote in the **Quotes** tab accordingly. Otherwise, if the quote is accepted or rejected in the quote portal, it is automatically reflected in the **Quotes** tab. For more information, see "Marking a quote as accepted or rejected" (p. 256).

For more information about how Advanced Automation (PSA) handles the rejection or acceptance of a quote, see "How Advanced Automation (PSA) processes accepted or rejected quotes" (p. 255).

How Advanced Automation (PSA) processes accepted or rejected quotes

When a customer accepts or rejects a quote, you can locate the relevant quote in the **Quotes** tab and mark it as accepted or rejected (for more information, see "Marking a quote as accepted or rejected" (p. 256)). This, in turn, launches a series of events in Advanced Automation (PSA), depending on the option selected.

When a quote is marked as accepted

When you mark the quote as accepted by the customer, or the customer accepts the quote themselves, the following events occur:

- A "Thank you" message is displayed to the customer.
- The quote's status in the **Quotes** tab is updated to **Accepted**. As a result, the quote can no longer be edited, but it can be copied.
- Notification is sent to the relevant MSP user (the user who created the quote) to inform them a quote was accepted.
- A generic quote ticket is created which contains all the quote's details. The ticket is assigned to the same user selected in the quote and is accessed via the **Service desk** module.
- A purchase order (PO) ticket is created and assigned to the manager of the support group set for purchase order tickets in the quote settings. This ticket includes only the details of products that are non-contract products and that are not in stock.
- For non contract products, sales items are created and can be viewed in the **Sales items** tab.
- For contract products that are selected:
  - A new contract is created for the customer and line items are added for all contract products in a quote. Note that if a specific contract was not selected when defining a quote product, a new contract with this contract part is created. If a specific contract was selected, then it will have this contract part added to it.
  - The contract's start date is set according to the quote acceptance date. The contract's end date is set according to the quote acceptance date plus the quote's duration, which is defined in the **Contract period (months)** field in the quote.

When a quote is marked as rejected

When you mark the quote as rejected by the customer, the following events occur:

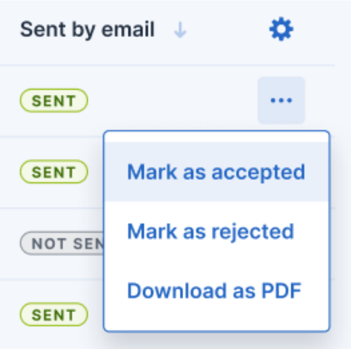
- A "Thank you" message is displayed to the customer, informing them the quote has been marked as rejected.
- The quote's status in the **Quotes** tab is updated to **Rejected**. As a result, the quote can no longer be edited, but it can be copied.
- Notification is sent to the relevant MSP user (the user who created the quote) to inform them a quote was rejected.
- Inventory items are updated to 'in stock' and are available for other quotes or sales items.

Marking a quote as accepted or rejected

When a customer accepts or rejects a quote, it can be marked accordingly in the **Quotes** tab. In turn, this triggers a series of events within Advanced Automation (PSA). For more information, see "How Advanced Automation (PSA) processes accepted or rejected quotes" (p. 255).

To mark a quote as accepted or rejected

1. In the management portal, go to **Sales and billing > Sales**.
2. In the **Quotes** tab, locate the relevant quote.
3. In the far right column, click the ellipsis icon and select one of the following:
   - **Mark as accepted**
   - **Mark as rejected**

   The quote's status is automatically updated.

Updating a quote

You can modify quotes as required. You cannot delete a quote.

Note
You can only modify a quote if its status is **Pending**. If the quote has been accepted or rejected, it cannot be updated (it can, however, be copied; see "Copying a quote" (p. 257)).

To update a quote

1. Go to **Sales and billing > Sales**, and click the **Quotes** tab.
2. Click the quote you want to update. The quote's details are displayed in the right sidebar.
3. Update the relevant sections, as required:
   - In the toolbar at the top of the sidebar, select from any of the following:
     - **Mark as rejected**: Marks the quote as Rejected in the **Quotes** tab. For more information about what happens to the quote when rejected, see "How Advanced Automation (PSA) processes accepted or rejected quotes" (p. 255).
     - **Download PDF**: Downloads a copy of the quote PDF.
     - **Go to quote portal**: Displays an online version of the quote.
     - **Resend email**: Resends the quote email to the selected user.

- In the **Quote information** section, click the pencil icon and update the relevant fields. When done, click ✓.
- In the **Products** section, click + to add a new product or update an existing product associated with the quote. When done, click ✓.

4. When you have finished updating the quote, close the right sidebar.

Copying a quote

You can copy a quote in any status.

To copy a quote

1. Go to **Sales and billing > Sales**, and click the **Quotes** tab.
2. In the row of the quote you want to copy, click the ellipsis icon (...) and then select **Copy**.
3. Update the quote, as required. For more information, see "Creating a quote" (p. 253).

Managing quote templates

Quote templates enable you to register standard offers and use them in quotes for customers, so when creating a new quote you don't need to add them manually and configure each one. For example, you can create a quote template called "Managed services" with an included set of products covering solutions for backups, security, recovery, managed services, support and monitoring.

Advanced Automation (PSA) enables you to add and modify or delete quote templates as required (see "Updating or deleting a quote template" (p. 257)).

Note
Quote templates do not currently support inventory items.

Adding a new quote template

1. Go to **Sales and billing > Sales**.
2. In the displayed screen, click the **Quote templates** tab.
3. If there are no existing templates, click **Add new template**. Otherwise, click **+ New**.
4. In the **Template name** field, enter a name for the template.
5. In the **Select products** field, click to select the relevant product. Then click **Add**.
6. To add additional products to the template, click **Add product**, and select the relevant product. Repeat as required.
7. Click **Done**. The new template is shown in the **Quote templates** tab, and is set to **Active** by default.

Updating or deleting a quote template

1. Go to **Sales and billing > Sales > Quote templates**. The displayed tab lists the existing quote templates.

2. To update a template, click on the relevant template, and in the right pane, click the pencil icon. Then update the template as required. When done, click ✓.
3. To delete a template, click on ellipsis icon (...) for the relevant template, and then click **Delete**.

Managing sales items

Sales items are services or goods provided to a customer that are subject to billing and invoicing.

Note
This feature is only available for users assigned the following roles: Administrator, Director, Group manager, Finance manager, Finance, Sales

Sales items are managed in the **Sales items** tab (go to **Sales and billing > Sales**), where you can view all your current sales items. Information about each sales item is also available, including the customer, the total amount of the sales items (excluding discounts), the invoice date, and if the sales item has been billed for or not. You can also filter and sort the displayed list to locate a specific or set of sales items; for more advanced filtering, use the **Filter** tool to define which sales items should be displayed.

Note
For customers using Acronis services and products, the system automatically creates sales items as part of the monthly billing run, and on the initial activation of Advanced Automation (PSA) for each partner.

Draft sales items are created to help automate the billing of customers, but customers cannot be billed until billing information is submitted. You can provide billing information for the customer in multiple ways, including when creating a contract or by clicking the relevant sales item in the **Sales items** tab, and then clicking **Add billing information** in the banner message. For more information, see "Onboarding existing clients" (p. 195).

After providing billing information for the customer, **Draft** sales items are automatically changed to **Pending**, and are available for billing.

Advanced Automation (PSA) enables you to manage sales items that are:

- Automatically registered based on contract parts.
- Automatically registered as a result of ticket-based activities.
- Automatically registered for customers using Acronis services and products, but without contract parts.
- Registered manually.

Creating a new sales item

The **Sales items** tab displays all sales items that have been created and billed. You can also add new sales items.

To create a sales item

1. Go to **Sales and billing** > **Sales**, and click the **Sales items** tab.

   > **Note**
   > When Advanced Automation (PSA) is activated for your account, you can also click **New** > **Sales item** from the management portal toolbar at the top of the screen, even when you are not in the Sales module. This option automatically opens the Create new sales item wizard via which you can create a sales item, as described in the following steps.

2. In the **Customer information** section, do the following:
   - Select the relevant customer. When selected, some of the following fields are automatically filled with the relevant customer information:
     - **Billing entities** (Manually select the relevant entity. The entity will be included on the invoice.)
     - **Payment method** (**Manual payment** or **Direct debit**. The **Direct debit** option enables customers to pay invoices via wire transfer or by using one of the payment integrations (PayPal, Stripe) - they can also send the invoice to their local bank for direct debit processing).
     - **Send invoice by** (**Mail** or **Email**).
     - **Email address contact**.
   - Define the invoice date.
3. In the **Customer address** section, the relevant details for the selected customer are displayed. You can manually update the address for this specific sales item, if required.

   > **Note**
   > If the selected customer does not have billing information defined, an additional **Billing information** step is added. When you click **Next**, you should complete the relevant billing information fields, including the payment terms and address. This information is then saved and used when selecting the customer in other Advanced Automation (PSA) modules. For more information about the billing information fields, see "Defining billing information for a tenant" (p. 43).

4. Click **Next**. The **Products** tab is displayed, where you can add any products to the sales item.

   > **Note**
   > Products are a service or item that you sell to customers. For example, antivirus subscriptions or ad hoc support.

5. Click **Add product** to select the relevant pre-defined products in Advanced Automation (PSA) (including Acronis products).

> **Note**
> Ensure that you have created one or more products that have the **Use in contracts** option disabled. This ensures the relevant product types are available when creating a sales item (if a product is set with **Use in contracts**, it can only be used in contracts).

6. In the **Product** field, select the relevant product.
7. Add a **Quantity** and **Price** in the relevant fields.
8. (Optional) Select the **Apply discount** check box (when selected, you can apply the discount amount and add a reason for the discount) and a **Description** for the product.
9. Click **Add** to add the product to your sales item. To add additional products, click **Add product** and repeat the steps above.
10. Click **Next**. The **Line item note** tab is displayed.
11. Click **Add line item note**, enter the relevant description, and then click **Add**. Repeat as required for additional line item notes.
12. Click **Done**. The sales item is added to the **Sales items** tab.

Modifying sales items

You can modify and delete sales items as required.

> **Note**
> You can only modify or delete a sales item if it has not yet been billed for. After it has been included in a billing, a sales item can be viewed only, it cannot be edited or deleted.

To modify a sales item

1. Go to **Sales and billing > Sales**, and click the **Sales items** tab.
2. Click the sales item you want to modify. The sales item's details are displayed in the right sidebar.
3. Modify the relevant sections, as required:
   - In the **Customer information** section, click the pencil icon and edit the relevant fields. Then click **Save**.
   - In the **Products** and **Line item notes** sections, click ⊞ to add new products or line item notes. Alternatively, click the pencil or trash can icons to edit or delete existing items. For each product or line item note that you add or modify, click **Save** when done.

Note

If a sales item is in **Draft** status, you can modify product parts and line items, but you cannot edit the **Customer information** section. You can also submit billing information for the customer by clicking **Add billing information** in the displayed banner message. In turn, this changes the status of the sales item to **Pending**, meaning it can now be billed for.

For further information about the editable fields in a sales item, see "Creating a new sales item" (p. 258).

To delete a sales item

1. Go to **Sales and billing > Sales**, and click the **Sales items** tab.
2. In the far right column of the sales item you want to delete, click the ellipsis icon and then select **Delete**.

   [Optional] To select multiple sales items to delete, first select the checkboxes in the left column of the relevant sales item rows. Then click **Delete** (located above the list of sales items). Note that the bulk deletion option is not enabled if you select both billed and non-billed sales items.
3. In the displayed confirmation message, click **Delete**.

Working with contracts

The **Contracts** tab shows all the contracts you have created for customers.

Each contract defines a set of services that you provide to a customer, including the price, terms and conditions. Invoices are then issued according to the payment terms defined in the contract.

When creating a contract, complete the onscreen wizard by adding the relevant contract information, billing information, and contract parts.

To access the contracts functionality, go to **Sales and billing > Sales**, and then click the **Contracts** tab.

Creating a new contract

When you create a new contract, a wizard guides you through three main steps. In these steps, you will:

- Add basic contract information
- Add billing information
- Add contract parts

Note

If you activated Advanced Automation (PSA) (see "Activating Advanced Automation (PSA)" (p. 190)) and defined a new customer with billing information, when you create a new contract for this customer they will have only two steps in the contract wizard (basic contract information and contract parts).

When you complete the wizard, the contract is automatically added to the list of existing contracts displayed in the **Contracts** tab. They can be then be viewed and updated, as required; see "Modifying a contract" (p. 265).

To create a new contract

1. In the management portal, go to **Sales and billing > Sales**.
2. Click the **Contracts** tab, and then click **+ New contract**.

   Note
   If you have existing customers that have no contracts assigned, you will be prompted to create contracts for them. When clicking **Create** or **Create contracts for existing customers**, you can select the relevant customer, and click **Next**. You must then define contract information, as described in the next step.

3. In the displayed wizard, define the following contract information:
   - **Reference number**: (Optional) The reference number that is frequently used in paper contracts.
   - **Contract name**: The contract name.
   - **Organization**: Select the relevant organization from the dropdown list.
   - **Contact email**: (Optional) Email contact for this contract.
   - **Billing entity**: Select the relevant billing entity.
   - In the **Payment details** section, select an interval period (**Every month**, **Quarterly**, **Semi-annually**, **Every year**), when to bill (**Upfront** or **Afterwards**), and select the payment method (**Manual payment** or **Direct debit**. The **Direct debit** option enables customers to pay invoices via wire transfer or by using one of the payment integrations (PayPal, Stripe) - they can also send the invoice to their local bank for direct debit processing.)
   - In the **Contract period** section, define the contract period (if the contract has no defined end, select the **Forever** check box), and select whether to send the invoice by email or mail.
   - In the **Customer address** section, define the relevant address details.
   - If you want to include block hours in your services, enable the **Block hours** option switch. Then define the number of block hours and the renewal threshold percentage. Select the **Retainer** check box if this contract is a retainer agreement (and the block hours are billed every month, quarter, or half year). Once enabled, you can:

     Discard remaining hours (to discard the remaining hours not consumed during the retainer billing period).

     Keep remaining hours (to keep the remaining hours not consumed during the retainer billing period).

     Time spent on tickets is either invoiced separately, marked as non-billable if the work is part of a fixed price agreement, or booked against the current block hour credit.

> **Note**
> Block hours enable you to reserve a block of support hours for customers, and are billed based on the default block hour product rate as set in the invoice settings. The renewal threshold is used to notify you when the current block has a specific number of hours remaining. The notification allows you to create a sales item for a new block by clicking **Renew block hours**. Once the new block is billed, it is shown in the available block hours balance.

- Select the **Pro-rated** check box if changes made to the contract will be billed prorated or at their full price.

4. Click **Next** to move to Step 2 of the contract wizard, billing information. For more information about the available billing fields, see "Defining billing information for a tenant" (p. 43). Note that if you have already defined billing information for this customer, you proceed to Step 3 of the contract wizard, adding contract parts (see below).
5. Click **Next** to move to Step 3 of the contract wizard, the adding of contract parts.
6. Click **Add contract part**.

> **Note**
> If the selected customer has defined Acronis products or services, you are prompted to edit or delete these, as required. You can then add additional contract parts, as described below.

7. Define the following fields:
   - **Contract part type**: Select the relevant contract part type from one of the following:
     - **Default type**: Used for general contracts that do not use an integration.
     - **ICT service**: This type enables you to sell an ICT (information and communication technology) service, such as *File storage*. When offering this service, multiple ICT assets can be added, including data centers, storage servers, network switches, etc. However, you can also use these assets in other contract parts. For example, when you create the *File storage* ICT service, you can add the data center, storage server and switch; when adding another ICT service that also uses the data center, you can still add the data center in this other contract part. When you create a ticket for the customer, the system lets you first select an ICT service and then the associated asset(s).
     - **Managed service**: This type is generally used for managed services such as *Workstation management*. Add the relevant machines to the contract part. Once done, these assets are removed from the list of available machines so they cannot be connected to another contract part.
   - In the **Product or services** section, select the relevant products or services you want to add, including the quantity and price of the product or service.

     The **Actual quantity** field defines the amount of service you currently provide to your customer within the scope of the contract. This value can be set:
     - **Manually**: Your customer is invoiced for a fixed amount of service every billing period. For example, five managed workstations monthly.

    - **Automatically**: Your customer is invoiced for the amount of service reported by one of the enabled integrations. For example, five servers are reported by Acronis Cyber Cloud integration in one month, and six servers reported the following month.

  The **Minimum quantity** field enables you to set a minimum service quantity to bill customers. If the value defined in the **Actual quantity** field is higher than the value defined in the **Minimum quantity** field, the actual quantity is used for billing. If the value defined in the **Minimum quantity** field is higher than the value defined in the **Actual quantity** field, the minimum quantity is used. These fields are also used for calculating usage and profitability in reports.

  The minimum billable quantity enhances the option to sell services as packs. For example, if you create a contract for a customer to backup at least two devices and using at least 500 GB of storage, the created invoice includes two line items for the devices and for the storage, without creating a sales item for the storage. The customer can be also billed for any usage above the minimal quantity specified in the contract (a separate sales item is created for the consumed storage above the defined 500 GB).

- In the **Contract period** section, define the relevant period. If there is no end date, select the **Forever** check box. By default, these dates are copied from the contract information settings (see above). Note that the date range should be shorter than the main contract date range. To apply a longer period, you must first adjust the main contract period.
- Click the **Trial** option switch if you want the contract part to be part of a trial period. To define the trial period, select the relevant number of months. Trial contract parts are included in invoices during a billing run with zero prices for information. When the trial period ends, the contract part shows the regular price in generated invoices.

Note

The trial option can only be applied one-time per contract part. In addition, if the selected contract part has previously been billed for, you cannot enable the trial option.

- **Integrations**: Select the relevant integration. When an integration is selected, an additional **Show machines in invoice** field is displayed. This field defines if machine details are included in the invoice; **Yes** is selected by default.

  Integrations enable you to tie the quantity of a contract part to real usage provided by the selected integration (such as the number of active workloads for a specific customer, or the number of virtual machines or amount of gigabytes used by a customer in   hosted storage).

  The available workloads include those with Acronis products and services (for example, Disaster Recovery, and Cyber Protection), and RMM integrations.

  To find the relevant integrated workloads, you can filter by client (meaning those workloads related to the selected client), workload type (workloads of a specific workload type), and individual workloads (search for and select the relevant workloads from the workloads list).

  In this section, you can also select an RMM integration and link the different agents associated with it (for the RMM alert-to-email functionality to work correctly, you must have the correct machines added to valid contracts). Advanced Automation (PSA) uses these to connect the

RMM site or group with the right customer. Using this information, it can apply the SLA to the ticket, based on the contract to which the machine is connected.

> **Note**
> An additional **Automatic updates** check box is also displayed, and enables the automatic workload number calculation for invoices. When selected, it disables the **Actual quantity** field in the **Product or services** section.

- **Service Level Agreement**: Select the relevant SLA.

8. Click **Add** to add the contract part to the contract.
9. (Optional) Click **Add contract parts** to add additional contract parts.
10. Click **Done**. The contract is added to the list of existing contracts in the **Contracts** tab.

Modifying a contract

You can modify a contract at any time, including the products or services attached to a contract.

> **Note**
> You cannot delete a contract or contract part. Instead, set the contract period to "end" to stop it (for example, at the end of the current month). This should be applied to the relevant contract parts first, and then the contract itself. The contract will then be inactive, but will still be available when searched for.

To modify a contract

1. In the management portal, go to **Sales and billing** > **Sales**.
2. In the **Contracts** tab, click the contract you want to edit.
3. In the right pane, modify the relevant contract details. Click the pencil icon in each relevant section; when done, click ✓.

   For more information about the editable fields, see "Creating a new contract" (p. 261).

   > **Note**
   > If block hours were enabled for a contract, you can renew the block hours manually by clicking **Renew block hours**. A new sale Item for block hours is automatically created and a confirmation message displayed.

4. When done, click **Save**.

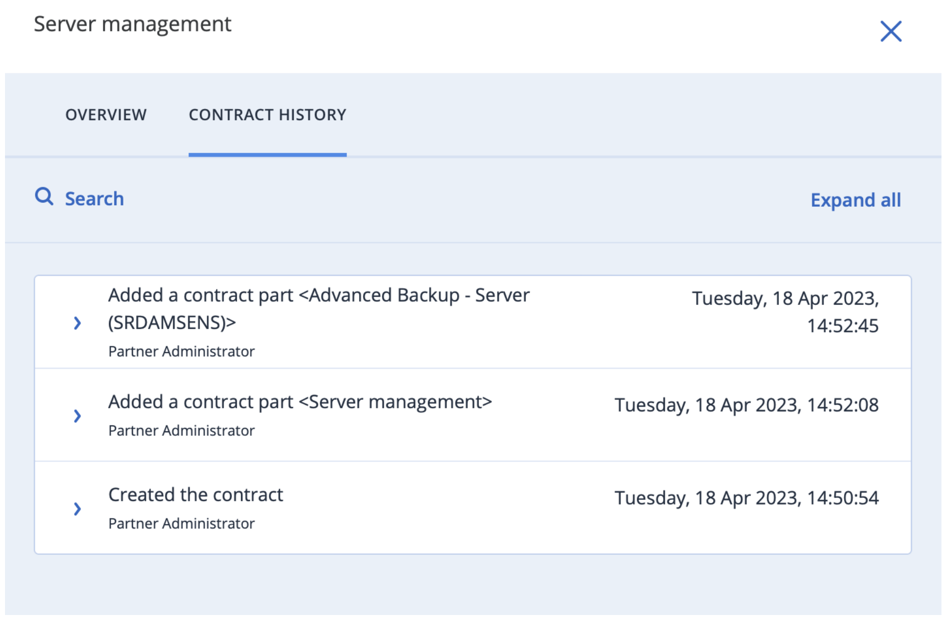
Reviewing the change history of a contract

You can review any changes made to a contract throughout the life of the contract. The log that stores this change history includes the initial creation of the contract and any subsequent updates.

To review the change history of a contract

1. In the management portal, go to **Sales and billing** > **Sales**.
2. Click the **Contracts** tab, and in the displayed list of contracts, click on the relevant contract.

3. In the displayed right pane, click the **Contract history** tab.



Added a contract part <Advanced Backup - Server (SRDAMSENS)>
Partner Administrator
Tuesday, 18 Apr 2023, 14:52:45

Added a contract part <Server management>
Partner Administrator
Tuesday, 18 Apr 2023, 14:52:08

Created the contract
Partner Administrator
Tuesday, 18 Apr 2023, 14:50:54

4. [Optional] Use the **Search** tools to navigate to the relevant update. You can also use the **Expand all** / **Collapse all** options to view/hide the details of all updates.
5. To review a specific change made to the contract, click on the relevant row. Depending on the change made, different information is shown:
   - When the contract is created: Most of the information defined when creating the contract is shown, including billing information.
   - When the contract is updated: Only the updated contract attributes and their previous/new values are shown.
   - When a contract part is added: Most of the information defined when adding the contract part is shown, including any enabled integrations.
   - When a contract part is updated: Only the updated contract part and its previous/new values are shown.
   - When a contract part is removed: The last state of the contract part, including any enabled integrations, is shown.

Working with custom prices

Custom pricing enables you to customize the price of a product. This can help you to automate the application of specific pricing agreements with clients.

For example, if you have a standard rate for project work of $100 per hour, but with another client you have agreed a rate of $130 per hour, you can create a custom price for the '*project work hourly rate*' for that client, with a price of $130. Each time you create a sales item or tickets for this kind of work for this client, the custom price is applied.

Note

You can only customize a price if the product is not a contract product.

To access custom prices, go to **Sales and billing > Sales**, and then click the **Custom prices** tab.

Adding a custom price

To add a custom price

1. In the management portal, go to **Sales and billing > Sales**, and then click the **Custom prices** tab.
2. Click **+ New custom price**.
3. Select the customer you want to apply the custom price to, and then click **Add product custom price**. Note that the list of customers shows only customers without custom prices yet specified.
4. In the **Product category** field, select the relevant category from the drop-down list.
5. In the **Product** field, select the relevant product from the drop-down list. This list only shows products with standard prices; products already defined with a custom price are not shown.
6. Enable the **Active** toggle switch if you want this custom price to be available.
7. Enter the product custom price and click **OK**.

   For more precise billing, the prices for products used in contracts, quotes, and sales items can use up to four digits after the decimal separator. For example: $0.0750. These prices will be rounded up in invoices, reports, billing items in tickets, and hourly rates.
8. To add another custom price, click **Add product custom price**, otherwise click **Create**.

Editing a custom price

To edit a custom price

1. In the management portal, go to **Sales and billing > Sales**, and then click the **Custom prices** tab.
2. Click on the customer whose custom prices you want to edit.
3. In the right pane, click the pencil icon and make your changes.

   For example, you can add a new custom price (see "Adding a custom price" (p. 267)), or edit the details of an existing custom price.
4. When done, click ✓.

Invoices

The **Invoices** module enables you to manage and track invoices you create for your customers. Using this module, you can:

- Generate new invoices for customers.
- Confirm payment of an invoice.
- Resend an invoice.
- Track the history of previously issued invoices.
- Download and/or export an invoice or invoice batch.

To access the **Invoices** module, in the management portal go to **Sales and billing > Invoices**.

Note
Only users with the Administrator, Director, Finance, Finance manager or Sales roles can generate invoices. Users assigned the Client manager or Client roles can only view and download invoices.

Viewing current invoices

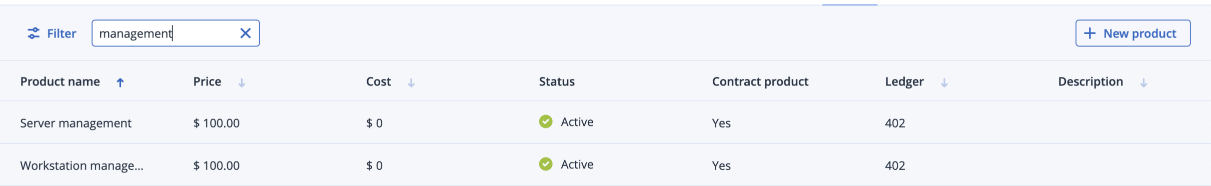
To view your current invoices, in Management Portal go to **Sales and billing** > **Invoices**. In the displayed **Invoices** screen, you can view all invoices in Advanced Automation (PSA).

Information about each invoice is displayed, including:

- The date the invoice was created.
- The payment status (**Confirmed** or **Not confirmed**), and, if paid, the date payment was made.
- If an email was sent to the customer.
- The amount of the invoice.
- If the invoice was synced with your accounting software (if activated).

Click on an invoice to view additional details about the invoice in the right pane. This information includes a general overview of the invoice, and details on each of the invoice items. In this pane you can also download and export the invoice as required.

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



Product name	Price	Cost	Status	Contract product	Ledger	Description
Server management	$ 100.00	$ 0	✓ Active	Yes	402	
Workstation manage...	$ 100.00	$ 0	✓ Active	Yes	402	

Generating a new invoice

When you generate a new invoice or invoice batch, you are actually creating the invoice data using an invoice template (as defined in "Billing settings" (p. 326)). This data can then be sent as an invoice via Advanced Automation (PSA) (if defined accordingly in your billing and contract settings), or sent by an alternative way. For example, your accounting software might be configured to send invoices to your customer, or invoices are sent as hard copies.

You can also resend an invoice, if required; see "Resending an invoice" (p. 270).

To generate a new invoice

1. In Management Portal, go to **Sales and billing** > **Invoices**.
2. If you have not yet created an invoice, click **Create new**. Otherwise, click **+ New**.

   The Create new invoice wizard is displayed.
3. Select the invoice date and the relevant billing entity. Then click **Next**.

4. Select the direct debits, manual payment contracts, and sales items you want to add to the invoice:
   - In the **Manual payment contracts** tab, select the contracts that were defined with **Manual payment**.
   - In the **Direct debit contracts** tab, select the relevant direct debits from the displayed list.

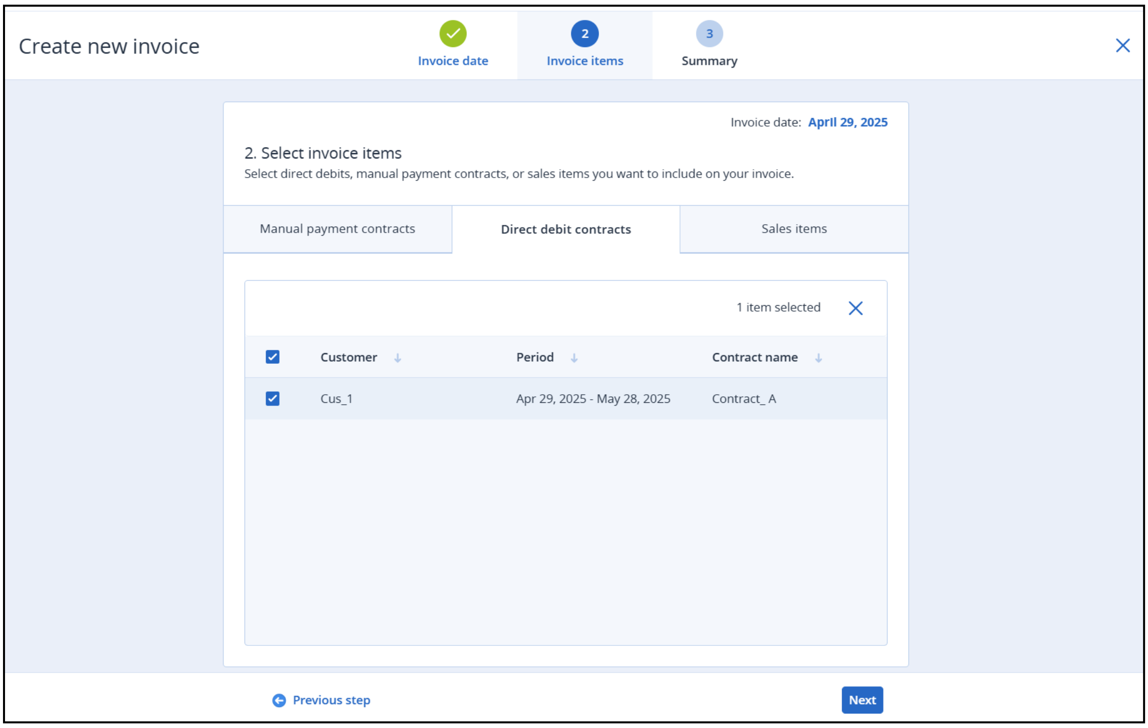
     Note

     If a contract was defined with **Direct debit** as the payment method, it is categorized as a direct debit contract. This enables customers to pay invoices via wire transfer or by using one of the payment integrations. They can also send the invoice to their local bank for direct debit processing.

   - In the **Sales items** tab, select the relevant sales items.

     Note

     You cannot select sales items that are in the **Draft** status. However, you can hover over the item and then click **Add billing information**. After you have defined billing information for the customer, the sales item is available for invoicing.

   Invoice date: AprIl 29, 2025

   2. Select invoice items

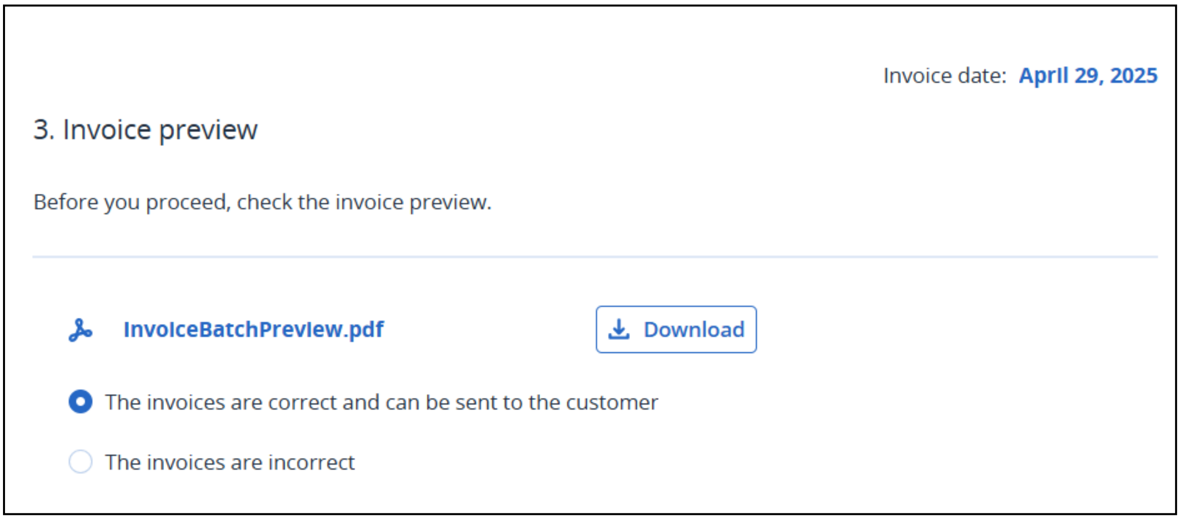
   Select direct debits, manual payment contracts, or sales items you want to include on your invoice.

   1 item selected

☑	Customer	Period	Contract name
☑	Cus_1	Apr 29, 2025 - May 28, 2025	Contract_ A

   When you finish selecting invoice items, click **Next**.

5. In the Summary screen, click **Download** to see a preview of the invoice batch in PDF format.



Invoice date: April 29, 2025

3. Invoice preview

Before you proceed, check the invoice preview.

InvoiceBatchPreview.pdf

● The invoices are correct and can be sent to the customer

○ The invoices are incorrect

If the invoice preview is correct, select the **The invoices are correct and can be sent to the customer** option button.

If the invoice preview is not correct, select **The invoices are incorrect**. This redirects you to the main Invoices screen and stops the invoice process. It also enables you to reevaluate your contract and invoice items. You can reprocess the invoice once it is corrected.

6. Click **Done**.

   You are redirected to the Invoices list, where you can view the invoice batch you just generated; the invoice batch also shows the individual invoices inside the batch. Invoices are then sent by email or not depending on the customer settings.

Note

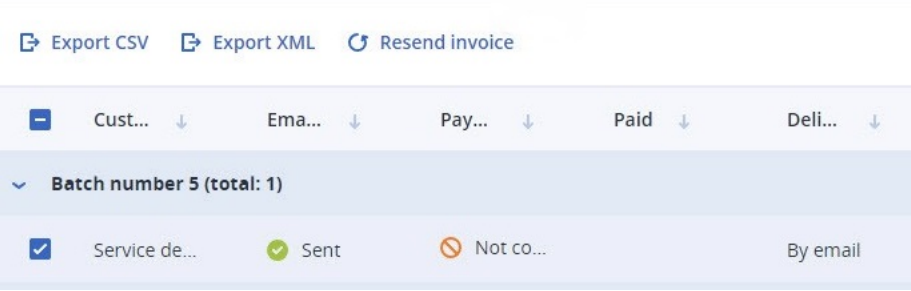
You cannot update an invoice, but you can update individual sales items, time entries, and contract parts that will be included in a corrected future invoice. When you have made those updates, you can then generate the correct invoice.

Resending an invoice

You can resend any invoice that has not yet been confirmed as paid, and that was set to be sent by email. Any invoice that was paid or set to be sent by post, cannot be resent.

To resend an invoice

1. In the management portal, go to **Sales and billing** > **Invoices**.
2. Select the invoice(s) you want to resend. The **Resend invoice** button is displayed, as shown below.



▬	Cust...	Ema...	Pay...	Paid	Deli...
Batch number 5 (total: 1)					
☑	Service de...	✓ Sent	Not co...		By email

Note
If you select multiple invoices but one or more of the invoices was confirmed as paid or was set to be sent by post, the **Resend invoice** button is displayed, but disabled.

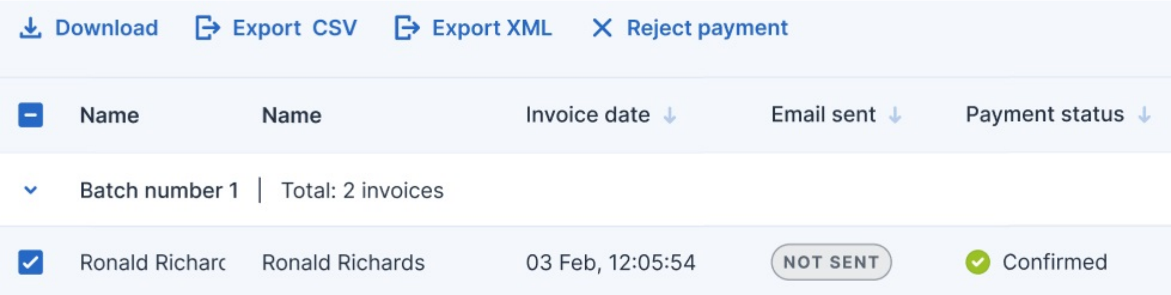
3. Click **Resend invoice**. The invoice is resent to the customer, and a confirmation message displayed.

Confirming or rejecting an invoice payment

You can manually confirm or reject payment for an invoice, as required.

To confirm or reject payment

1. In the management portal, go to **Sales and billing** > **Invoices**.
2. Select the invoice(s) you want to confirm or reject.
3. If the payment was already confirmed, and you need to reject it for some reason, click **Reject payment** in the top bar located above the list of invoices.



▬	Name	Name	Invoice date	Email sent	Payment status
Batch number 1 | Total: 2 invoices					
☑	Ronald Richarc	Ronald Richards	03 Feb, 12:05:54	NOT SENT	✓ Confirmed

If the payment is not confirmed, click **Confirm payment**.

Alternatively, click the ellipsis icon (...) in the far right column. In the displayed menu, click **Reject payment** or **Confirm payment**.

The displayed list of invoices is updated.

Downloading an invoice as a PDF file

Note
Before performing the steps below, ensure that you have a PDF reader installed on your device.

To download an invoice as a PDF

1. In the management portal, go to **Sales and billing** > **Invoices**.
2. Select the invoice(s) you want to download.
3. In the top menu bar located above the list of invoices, click **Download**.

   Alternatively, click the ellipsis icon (...) in the far right column. In the displayed menu, click **Download**.

   The invoice is downloaded to your device in PDF format.

Exporting an invoice as a CSV or XML file

You can export an invoice as a CSV or XML file. These files can then be used in a third party system, such as your accounting platform, which is not integrated with Advanced Automation (PSA).

To export an invoice as a CSV or XML file

1. In the management portal, go to **Sales and billing** > **Invoices**.
2. Select the invoice(s) you want to export.
3. In the top menu bar located above the list of invoices, click **Export CSV** or **Export XML**.

   Alternatively, click the ellipsis icon (...) in the far right column. In the displayed menu, click **Export CSV** or **Export XML**.

   The file is downloaded to your device in the chosen format.

Products

The **Products** module enables you to define and manage your products, which are typically a service or item you sell to your customers. For example, antivirus subscriptions, ad hoc support, hardware deliveries, and so on.

Products can be used when creating contracts or sales items. The values that you enter for the product item are reused when you create a sales item or contract and can be changed to reflect what has been agreed with your customer.

Note that only users with the Administrator, Director, Finance, or Finance manager roles can create products. Once created, products can then be used in contracts, tickets, projects, quotes, etc, by other Advanced Automation (PSA) users.

To access the **Products** module, go to **Sales and billing > Products**.

Viewing existing products

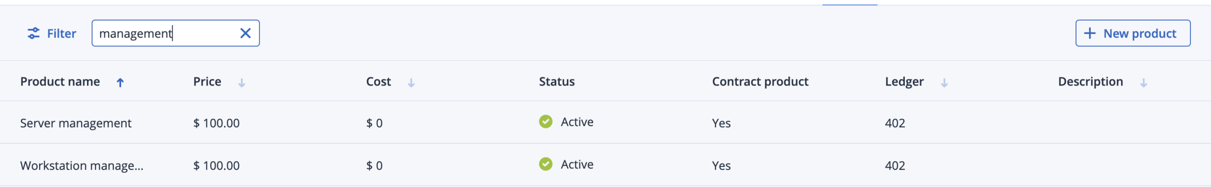
To view existing products, in Management Portal go to **Sales and billing** > **Products**. In the displayed **Products** tab, you can view all current products in Advanced Automation (PSA). These products include pre-configured Acronis products and services, as well as your own products.

Information about each product is displayed, including:

- The price of the product
- The cost of the product
- The product's current status (**Active** or **Inactive**)

- The type of product (contract, ticket, or project (available in future versions))
- The ledger the product belongs to
- A short description of the product

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



Product name	Price	Cost	Status	Contract product	Ledger	Description
Server management	$ 100.00	$ 0	✓ Active	Yes	402	
Workstation manage...	$ 100.00	$ 0	✓ Active	Yes	402	

Adding a product

In addition to the Acronis products and services available in Advanced Automation (PSA), you can create any number of your own products and offerings.

To add a product

1. In the management portal, go to **Sales and billing** > **Products**. The **Products** tab is displayed by default.
2. Click **+ New product**. The Create new product screen is displayed.
3. Define the following:
    - **Name**: Enter the name of the product.
    - **Description**: (Optional) Enter a description of the product.
    - **External ID**: (Optional) Enter a unique identifier for the product. This ID should be used outside the current line of products in Advanced Automation (PSA).
    - **Price**: Enter a price for your product. Select the **Taxable** check box if the product is taxable (this will depend on your local tax laws).

      For more precise billing, the prices for products used in contracts, quotes, and sales items can use up to four digits after the decimal separator. For example: $0.0750. These prices will be rounded up in invoices, reports, billing items in tickets, and hourly rates.
    - **Cost**: Enter the cost of the product, or the price paid to a vendor or distributor for the product.

      For more precise reporting, the cost for products can use up to four digits after the decimal separator. For example: $0.0750.

      Note

      In order to provide more details about the profitability of a product and its related statistics, we recommend you configure not only prices for products, but also their cost.
    - In the **Product properties** section, select any or all of the following:
        - **Contract product**: Select the check box if you want the product to be available in contracts.

    - **Ticket product**: Select the check box if you want the product to be available in tickets. When selected, you can also select the additional **Price adjustable by engineer** check box; this enables engineers to adjust the default price when using this product in a ticket.
    - **Project product**: Select the check box if you want the product to be available in projects. When selected, select the additional **Price adjustable per project** check box to enable the default price to be adjusted when using this product in a specific project. For more information, see "Projects" (p. 221).
    - In addition, select the **Product for activity-based billing** check box if you want the product to be listed in tickets for engineers. This field is not available if **Contract product** is selected.

      Note
      This option ensures additional time required for experts (for example, when a technician needs assistance from an architect or security expert) can be assigned to a ticket. In turn, these hours can be billed under their special rate instead of a default ticket rate.

  - **Ledger**: (Optional) Select the relevant ledger from the drop-down list.
  - **Active**: (Optional) Select the check box to make the product available.

    Note that the **Active** check box is disabled when the product is:
    - Set as the default product in billing settings (see "Defining your default billing settings" (p. 326)).
    - Part of a bundle.
    - Added to a contract.
  - **VAR product**: (Optional) Select the check box if you are reselling the product - meaning that you first purchase the product from somewhere else. When this check box is selected, revenue for this product is aggregated separately as 'VAR' revenue.

4. After reviewing your new product's details, click **Done**.

Editing a product

To edit a product

1. In the management portal, go to **Sales and billing** > **Products**. The **Products** tab is displayed by default.
2. Click on a product you want to edit.
3. In the right pane, click the pencil icon and edit the product. For more information about the editable fields for a product, see "Adding a product" (p. 273).

   Note
   If a contract product is included in a product bundle, you cannot update it. You are prompted to first remove it from the relevant product bundle before updating it here.

4. When done, click ✓.

Defining the costs and prices of Acronis products

In the **Products** tab, you can define the cost and prices of Acronis products used in Advanced Automation (PSA). The defined *cost* determines how much you spend on Acronis products, while *prices* define how much you will get paid by customers.

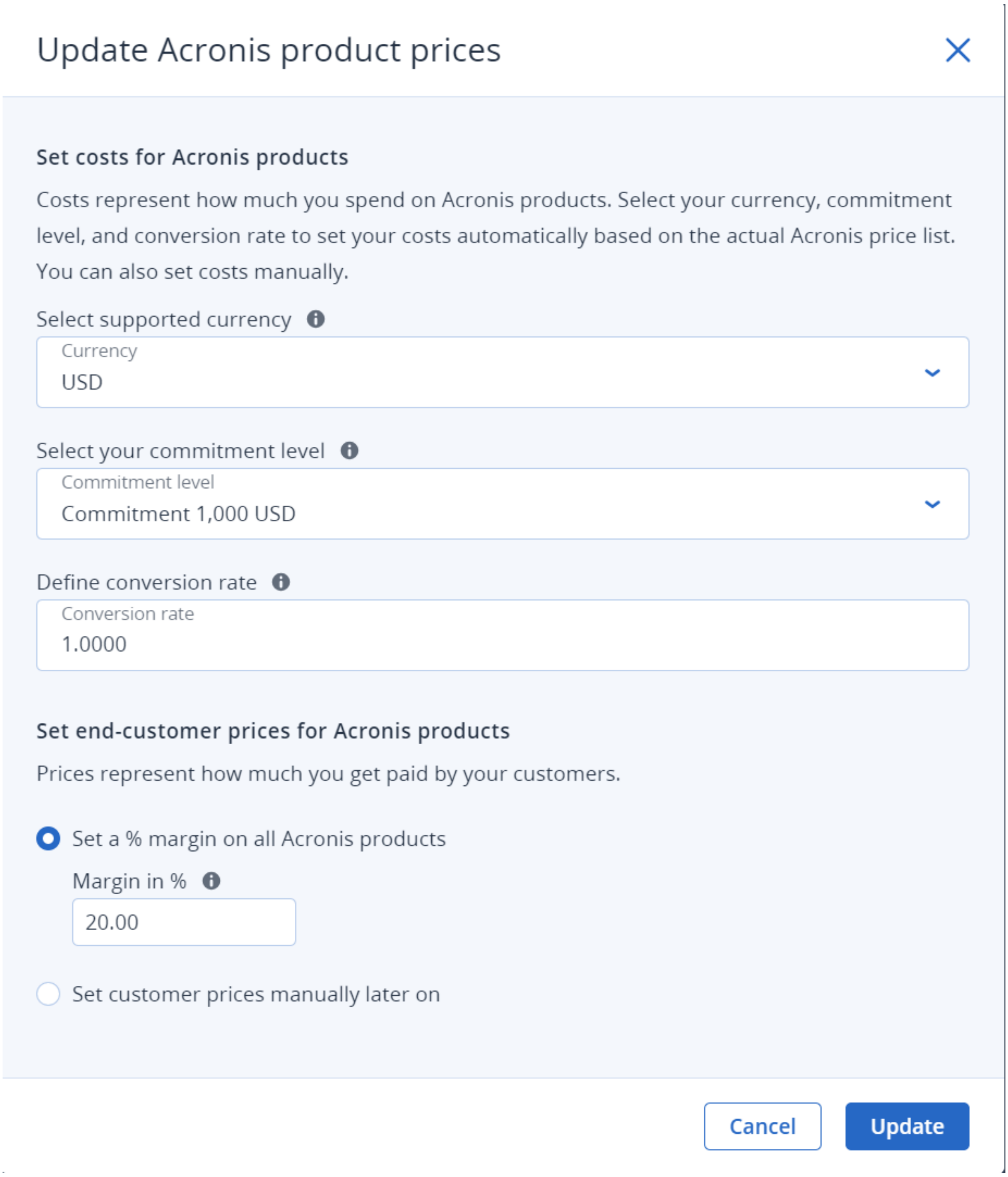
This feature enables you to:

- Define Acronis product costs based on the actual Acronis price list, the relevant partner's currency (and exchange rate, if the price list is not provided by Acronis), and the partner's tier (commitment level).
- Define Acronis product prices for customers based on costs and a specified margin percentage.

To define costs and prices of Acronis products

1. Go to **Sales and billing** > **Products**.
2. In the **Products** tab, click **Update Acronis product prices**.

   The following dialog is displayed.



Update Acronis product prices

Set costs for Acronis products

Costs represent how much you spend on Acronis products. Select your currency, commitment level, and conversion rate to set your costs automatically based on the actual Acronis price list. You can also set costs manually.

Select supported currency

Currency: USD

Select your commitment level

Commitment level: Commitment 1,000 USD

Define conversion rate

Conversion rate: 1.0000

Set end-customer prices for Acronis products

Prices represent how much you get paid by your customers.

● Set a % margin on all Acronis products

Margin in %: 20.00

○ Set customer prices manually later on

3. In the **Set costs for Acronis products** section, define the following:
   - In the **Select supported currency** dropdown list, select the currency to be applied to Acronis products.

     Note
     Your default currency set in Advanced Automation (PSA) is automatically applied here. This field is also read-only if your default currency is one of the supported currencies (USD, EUR, GBP, AUD, JPY, CAD, BRL, INR), as shown in the example above.

   - In the **Select your commitment level** dropdown list, select the relevant commitment level.

- In the **Define conversion rate** field, set the conversion rate for Acronis products. The default value is 1.0000.

  Note
  This field is mandatory if your default currency is not one of the supported currencies (see above).

4. In the **Set end-customer prices for Acronis products** section, select one of the following:
   - **Set a % margin on all Acronis products**. Select this option if you want to set the relevant profit margin to all Acronis products. Prices are set according to the following formula:

     Price = Cost * 100 / (100 - Margin value)

     For example, a 20% margin on a $100 product will set the price at $125, with the $25 margin being 20% of $125.
   - **Set customer prices manually later on**. Select this option if you do not want to automatically update Acronis product prices but want to set them manually at a later time.
5. Click **Update**.

   Advanced Automation (PSA) automatically applies the defined costs and prices to the Acronis products you sell to your customers.

Managing inventory

The Inventory module enables you to add records for, manage, sell, and analyze your stock inventory (meaning items such as servers, computers, networking equipment, and peripherals that you want to have available for one-time sales to clients). Inventory items can be offered in quotes or sold as sales items by selecting a non-contract product, such as 'Hardware sale'.

Unlike subscription-based products, inventory items are limited in quantity and not recurring. For example, when adding an item to quotes or sales items, the quantity is 'consumed', meaning it cannot be added to other quotes or sales items. If the quote is then rejected, or the quantity (or item) removed from the quote or sales item, the item is again made available in the Inventory module. The item can then be added to other sales items or quotes. For more information about working efficiently with your inventory, see "Creating an inventory item with a serial number" (p. 281).

To access and manage your inventory, go to **Sales and billing > Products**, and then click the **Inventory** tab. From this tab, you can track and manage inventory items across multiple locations, identify items that require replenishment, and monitor your inventory utilization. You can manage quantities, prices, serial numbers, warranty details, and supplier and purchase data, as well as define and use custom fields tailored to your needs.

By using the Inventory module, you can streamline inventory management and sales processes, enhance client services, and gain actionable financial and inventory insights.

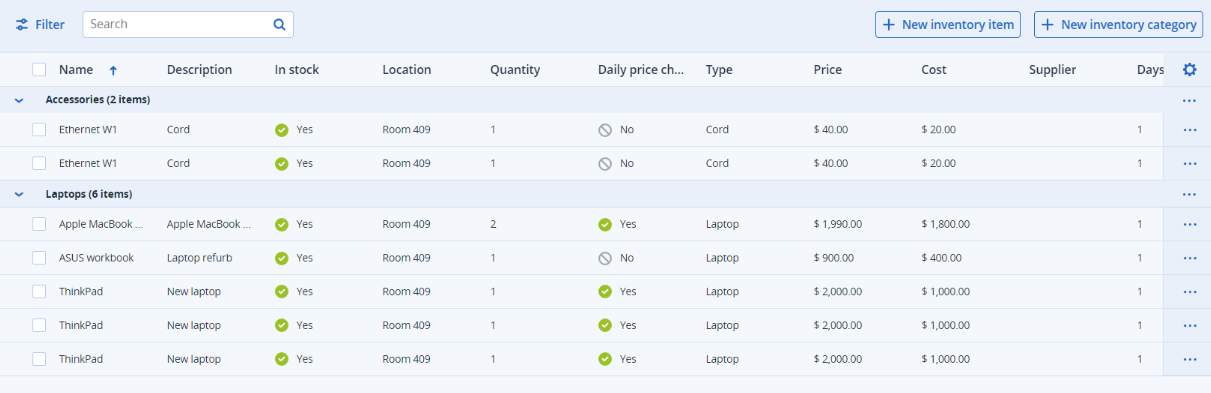
Viewing existing inventory

To view existing inventory, in the management portal go to **Sales and billing > Products**.

Click the **Inventory** tab to view all inventory items (including already sold items) in Advanced Automation (PSA). You can view information about each inventory item, including:

- The name of the item.
- A short description of the item.
- Indication if the item is currently in stock (**Yes** or **No**) and how long it has been in stock.
- The item's location.
- The current quantity of the item available for selling.
- The cost (purchase price) and price (selling price) of the item.
- The item type, and category.
- The item's serial number.

The inventory items are grouped by category. You can filter and sort the displayed list to locate a specific item; for more advanced filtering, use the **Filter** tool to define which items should be displayed.



□	Name ↑	Description	In stock	Location	Quantity	Daily price ch...	Type	Price	Cost	Supplier	Days
	Accessories (2 items)										
□	Ethernet W1	Cord	✓ Yes	Room 409	1	⃠ No	Cord	$ 40.00	$ 20.00		1
□	Ethernet W1	Cord	✓ Yes	Room 409	1	⃠ No	Cord	$ 40.00	$ 20.00		1
	Laptops (6 items)										
□	Apple MacBook ...	Apple MacBook ...	✓ Yes	Room 409	2	✓ Yes	Laptop	$ 1,990.00	$ 1,800.00		1
□	ASUS workbook	Laptop refurb	✓ Yes	Room 409	1	⃠ No	Laptop	$ 900.00	$ 400.00		1
□	ThinkPad	New laptop	✓ Yes	Room 409	1	✓ Yes	Laptop	$ 2,000.00	$ 1,000.00		1
□	ThinkPad	New laptop	✓ Yes	Room 409	1	✓ Yes	Laptop	$ 2,000.00	$ 1,000.00		1
□	ThinkPad	New laptop	✓ Yes	Room 409	1	✓ Yes	Laptop	$ 2,000.00	$ 1,000.00		1

Adding an inventory item

When you add an inventory item with a quantity larger than 0, the inventory item can then be offered as part of a quote, or sold via a sales item.

To add an inventory item

1. In the management portal, go to **Sales and billing** > **Products**, and then click the **Inventory** tab.
2. If you are adding your first inventory item, click **Create new**. If you have existing inventory items, click **+ New inventory item**.

   The **Create new inventory item** wizard is displayed.
3. In the **General information** tab, define the following:
   - **Name**: Enter the name of the inventory item.
   - **Description**: Enter a description of the item.
   - **Category**: Select a category from the list of current active categories. Note that you can also add a new category by clicking **+ New inventory category** in the drop-down list.
   - **Location**: (Optional) Select a location from the current list of locations. Note that you can also add a new location by clicking **+ New location** in the drop-down list.

> **Note**
> If a default inventory location was defined, the default location is shown here, but it can be changed. For more information, see "Adding an inventory location" (p. 284).

- **Type**: (Optional) Select a type from the current list of types. Note that you can also add a new type by clicking **+ New type** in the drop-down list.

4. Click **Next**.
5. In the **Item details** tab, define the following:
   - **Cost**: By default, cost is set as 0.
   - **Price**: By default, price is set as 0.
   - **Quantity**: By default, quantity is set as 0. However, if any serial numbers are entered (see below), this field automatically displays the number of serial numbers added. Note that when added to a sales item or a quote, the available quantity is "reserved", so you cannot add the same quantity twice.
   - In the **Serial numbers** text box, enter a unique serial number for each inventory item, with a maximum of 60 characters. You can add up to 1000 serial numbers, delimited by a new line or space.
6. Click **Next**.
7. In the **Purchase details** tab, define the following:
   - **Supplier**: (Optional) Select a supplier from the current list of suppliers.
   - **Supplier purchase order**: (Optional) Enter the supplier purchase order number.
   - **Internal purchase order**: (Optional) Enter the internal purchase order number.
   - **Supplier invoice number**: (Optional): Enter the supplier invoice number.
   - Select the **Daily price check** checkbox to indicate if the inventory item's price should be manually verified by employees before they purchase it from a supplier or sell it to customers. When selected, the **Daily price check** column in the main inventory screen shows **Yes** in the relevant inventory item row.
8. In the **Additional information** tab, you can view any custom fields for the inventory item. Note that this tab is only displayed when custom fields are configured and there is at least one active custom field for your inventory.

   For example, if a **Warranty valid until** custom field was defined and applied to inventory items, it is shown for all inventory items when creating or updating the item. All inventory items will have different values applicable for this field, or can even be left empty. For more information about defining custom fields, see "Working with custom fields" (p. 198).
9. Click **Create**.

For more information about working efficiently with your inventory, see "Creating an inventory item with a serial number" (p. 281).

Editing an inventory item

You can edit or remove an inventory item as required.

To edit an inventory item

1. In the management portal, go to **Sales and billing** > **Products** and then click the **Inventory** tab.
2. Click on the inventory item you want to edit.
3. In the right pane, click the pencil icon in the relevant sections (**General information**, **Item details**, and **Purchase details**) and edit as required. For more information about the editable fields for an inventory item, see "Adding an inventory item" (p. 278).

   Note the following:

   - You cannot edit the **Quantity** field if serial numbers were added to the inventory item. The read-only value shown is **1** (if the item is not included as part of a sales item or quote) or **0** (if the item was added to a sales item or quote). Serial numbers can be edited only if the inventory item was not added to a pending quote (the quote was not accepted or rejected) or a sales item (that was billed for or not billed for). To edit the serial number, the inventory item needs to be removed, the serial number changed, and the item then added back.
   - You can update the locations of a number of items in bulk by selecting the relevant items and clicking **Update item(s) location**. In the displayed dialog, select the new location and click **Update**. The new location is applied to all the selected items.
   - If you update the inventory item price, name or description, you need to manually update these fields for any associated sales items and quotes.
   - Setting an **Inactive** item to **Active** will also set the inventory location to **Active**.
4. When done, click **Save**.

To remove an inventory item

1. In the relevant inventory item row, click the ellipsis icon (...), and then select **Remove**.
2. In the displayed confirmation dialog, click **Remove**.

   The inventory item is set as **Inactive**. Note that existing sales, billing, and procurement operations where this item is used are not affected.

   You can still view **Inactive** inventory items in the main inventory screen by using the **Filter** option and selecting **Status** > **Inactive**.

How to work with your inventory

After you have added your inventory (see "Adding an inventory item" (p. 278)), Advanced Automation (PSA) enables you to work with your inventory by updating, tracking, and selling inventory items via the relevant quotes and sales items.

The following sections include some tips and tricks to help you manage your inventory, including:

- Working with inventory with serial numbers
- Selling inventory via sales items and quotes
- Updating quotes, sales items, and inventory

Creating an inventory item with a serial number

You can create an inventory item with a serial number (see "Adding an inventory item" (p. 278)). When a serial number is applied during an inventory item's creation, the item's quantity is automatically set as 1, and cannot be changed manually.

You can also create inventory items by bulk (up to 1000 items) with serial numbers. This is done through the same inventory item dialog used to create a single inventory item by adding multiple serial numbers. The item's quantity in the creation wizard is automatically based on the number of provided serial numbers, and cannot be changed manually. On completing the creation wizard, a single inventory item (with a quantity of 1) is added for each serial number.

Note
By applying a serial number to an inventory item, you can easily keep track of warranty details, serial numbers, and any other information added through the use of custom fields. This enables you to manage your inventory more efficiently.

You can also reuse an inventory item without a serial number if you do not need to track these details. In this way, you can increase the inventory item quantity and sell as required.

Updating an inventory item with a serial number

The quantity of an inventory item with a serial number cannot be updated: the quantity is either 1 (if not yet sold or offered in a quote) or 0 (if offered in a pending quote or pending sales item, or if sold). Note that the item's quantity automatically decreases to 0 if it is offered in a quote, or sold as a sales item.

You can set a serial number to an existing inventory item that does not have a serial number assigned to it. However, if a serial number is applied to an inventory item, the item's quantity is reset to 1, which may result in a discrepancy between the real number of items and the items cataloged in Advanced Automation (PSA). As a result, we recommend you:

- Create a new inventory item with the relevant serial number.
- Manually decrease the inventory item's quantity.

After-sales

When sold, the inventory item is stored for book-keeping purposes only, which also enables you to track the item's serial number and warranty, and any other information that might be added through the use of custom fields.

You can also track your inventory in the Sales and billing reports. For more information, see "Sales and billing" (p. 129).

Selling inventory via sales items and quotes

There are two ways to sell inventory items - through direct sales via sales items, and by offering inventory items in a quote. Note that inventory items are added to sales items and quotes by specifying a non-contract product (meaning that the **Use in contracts** option is disabled), then selecting the relevant in-stock inventory items.

- To sell inventory items via sales items:
  a. Create the relevant sales items for customers, and add the inventory items. For more information, see "Creating a new sales item" (p. 258).
  b. Create an invoice for the customer using the relevant sales items. For more information, see "Generating a new invoice" (p. 268).

  Note
  The ledger included in the invoice line is the ledger configured for the product (ledgers are defined at the product level, not the inventory level). For more information, see "Managing ledgers" (p. 288).

  Similarly, the tax applied in the invoice is the tax defined for the product (when imported via an accounting integration) or the default system tax. For more information, see "Tax settings" (p. 332).

- To offer inventory items in a quote:
  a. Create a quote with the relevant inventory items. For more information, see "Creating a quote" (p. 253).
  When the customer accepts the quote, a sales item and quote ticket are created. You can track the sales process and log time via the quote ticket. For more information, see "How Advanced Automation (PSA) processes accepted or rejected quotes" (p. 255).
  b. Invoice the customer, by creating an invoice from the sales item. For more information, see "Generating a new invoice" (p. 268).

Important
Only in-stock inventory items that have a quantity greater than 0 can be sold as sales items or in quotes. Only the available quantity can be sold.

Note that the quantity for each inventory item is automatically updated when:

- Added to a quote or sales item. The inventory item is automatically reserved from existing stock, and cannot be offered in another quote or sales item.
- Sales items are deleted or quotes rejected. The reserved quantity of inventory items is returned to stock and is then available for use in other quotes and sales items.

Updating quotes, sales items, and inventory

Be aware of the following when updating quotes, sales items, and inventory items:

- When you update the inventory item name and description, it does not automatically update the description of the same items included in quotes or sales items. These descriptions must be manually updated.
- Adjusting the inventory item's price will automatically adjust the price set in the quote or sales item. However, if you adjust the inventory item's price in the quote or sales item, you need to manually update the price for the inventory item.
- If you need to update the serial number assigned to an inventory item which is included in a quote or sales item, do the following:
  a. Remove the inventory item from the quote or sales item.
  b. Update the serial number for the inventory item.
  c. Add the updated inventory item back to the quote or sales item.
- Quote templates do not currently support inventory items.

Managing inventory categories

Inventory categories enable you to quickly locate and monitor the status of specific inventory items.

You can add inventory categories as required. You can also edit and remove inventory categories.

To add an inventory category

1. In the management portal, go to **Sales and billing** > **Products**, and then click the **Inventory** tab.
2. Click **+ Add inventory category**.
3. Enter the name of the inventory category, and then click **Add**.

   The inventory category is now available for selection when creating or editing an inventory item.

To edit an inventory category

1. In the **Inventory** tab, click the ellipsis icon (...) in the relevant inventory category row, and then select **Edit**.
2. Edit as required. You can:
   - Rename the inventory category.
   - Switch the inventory category's status to **Active** or **Inactive**.

   Note
   You cannot set an **Active** inventory category to **Inactive** if **Active** inventory items are assigned to it. You should move the inventory items to another category or set them as **Inactive**, and then try again.

3. Click **Save**.

To remove an inventory category

1. In the **Inventory** tab, click the ellipsis icon (...) in the relevant inventory category row, and then select **Remove**.
2. If the inventory category is empty or has no **Active** inventory items, it is removed.

Note

You cannot remove an inventory category if **Active** inventory items are assigned to it. You should move the inventory items to another category or set them as **Inactive**, and then try again.

Managing inventory locations

Advanced Automation (PSA) enables you to define and manage locations for your stock inventory. This can help employees easily find the location of existing inventory items that should be sent to customers, and also the location where purchased inventory needs to be delivered.

To view and manage your inventory locations, go to **Sales and billing > Products**, and then click the **Inventory locations** tab.

Note

For further information about viewing, creating, and editing inventory items, see "Managing inventory" (p. 277).

Adding an inventory location

To add an inventory location

1. In the management portal, go to **Sales and Billing > Sales**, and click the **Inventory location** tab.
2. If you are adding your first location, click **Create new**. If you have existing locations, click **Add location** in the top right corner.
3. In the displayed dialog:
   a. Enter the location's name.
   b. Enter a description of the location.
   c. (Optional) Select the **Default location** checkbox. This option ensures that this location is selected by default when adding a new inventory item. For more information, see "Adding an inventory item" (p. 278).
   d. Click **Add** to add the location.

   The location is added to the list of existing locations, and by default is set to **Active**.

   For more information about updating the location and its status, see "Editing an inventory location" (p. 284).

Editing an inventory location

You can edit and delete inventory locations as required.

To edit an inventory location

1. In the management portal, go to **Sales and Billing > Sales**.
2. Click the **Inventory location** tab to view any existing locations.

   If no locations are displayed, you can click **Create new** to add a location. For more information, see "Adding an inventory location" (p. 284).

3. In the relevant inventory location row, click the ellipsis icon (...), and then select **Edit**.
4. Edit the displayed fields as required. For example, if you want the location to be inactive, clear the **Active status** checkbox.
5. When done, click **Save**.

To delete an inventory location

1. In the relevant inventory location row, click the ellipsis icon (...), and then select **Delete**.
2. In the displayed confirmation dialog, click **Delete**. The location is deleted.

Note
If the inventory location is currently in use, you are prompted to first assign the associated inventory to another inventory location. Alternatively, you can clear the **Active status** checkbox to make the location inactive, and then try again.

Product categories

Advanced Automation (PSA) enables you to add new categories as required.

When you apply categories to your tickets, you get a good overview of the most common issues affecting each customer. For example, when a customer has 50% of their tickets categorized as *Workstation/virus*, you might want to replace security measures and upgrade training for the relevant personnel.

Categorizing your products also enables you to organize multiple products into a single group. If you have hundreds of products listed, creating a category will help you find them easily.

Adding product categories

You can add new product categories as required.

Once created, you can enable or disable a category, as described below, and edit according to your requirements (see "Editing product categories" (p. 286)).

Note
This option is only available to users assigned the following roles: Administrator, Director, Finance manager, Finance

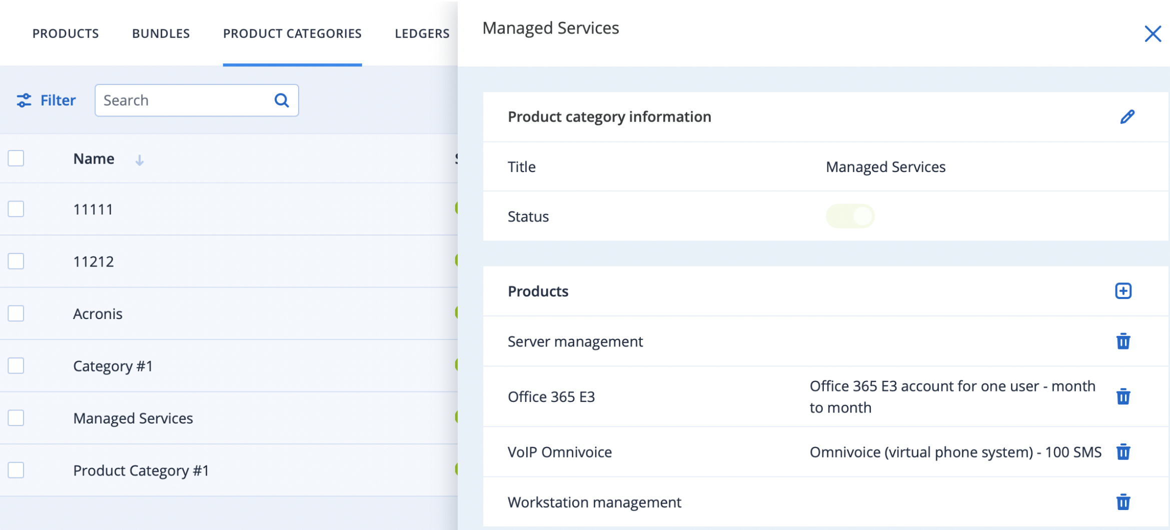
Adding a new product category

1. Go to **Sales and billing > Products**.
2. In the displayed screen, click the **Product categories** tab.
3. If there are no existing categories, click **Create new**. Otherwise, click **+ New**.
4. In the **Product category name** field, enter a name for the category.
5. In the **Select products** field, click to select the relevant product. Then click **Add**.
6. To add additional products to the category, click **Add product**, and select the relevant product. Repeat as required.

7. Click **Done**. The new category is shown in the **Product categories** tab, and is set to **Active** by default.

Enabling or disabling a product category

1. Go to **Sales and billing > Products**. The displayed **Products** tab lists the existing categories.
2. To activate a category, click on the relevant Inactive category, and in the right pane, click the pencil icon. Then enable the **Status** toggle switch. When done, click ✓.



Name
11111
11212
Acronis
Category #1
Managed Services
Product Category #1

Managed Services

Product category information

Title	Managed Services
Status	

Products

Server management	
Office 365 E3	Office 365 E3 account for one user - month to month
VoIP Omnivoice	Omnivoice (virtual phone system) - 100 SMS
Workstation management	

3. To disable a category, click on the relevant Inactive category, and in the right pane, click the pencil icon. Then disable the **Status** toggle switch. When done, click ✓.

Note
You can also enable or disable the category status when editing the category. See "Editing product categories" (p. 286) for more information.

Editing product categories

To edit a product category

1. Go to **Sales and billing > Products**. The displayed **Products** tab lists the existing categories.
2. To edit a category, click on the relevant category, and in the right pane, click the pencil icon.
3. Make the required changes. For example, remove and add products, or change the category status to **Active**/**Inactive**.
4. When done, click ✓.

Managing product bundles

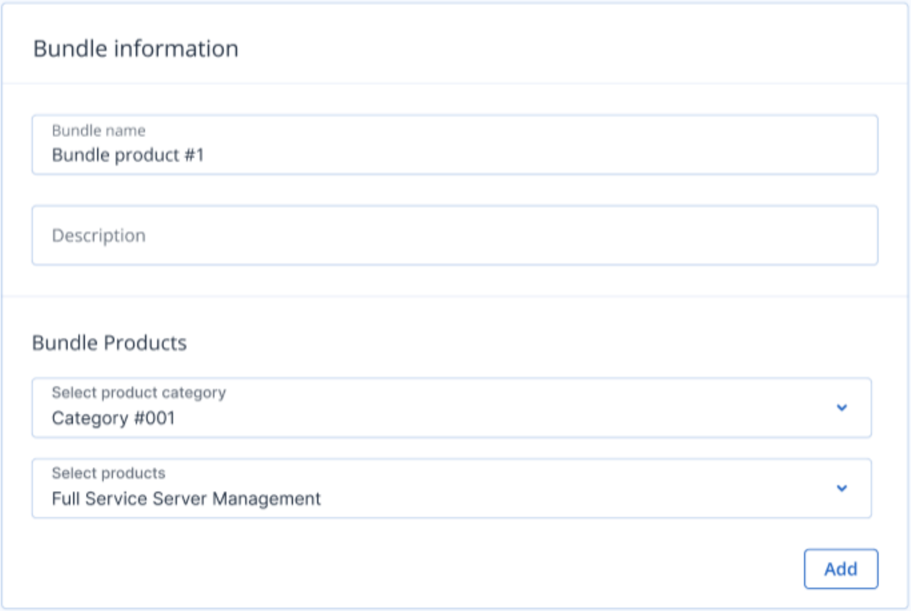
Product bundles enable you to combine multiple products and services into a single package.

Note that product bundles currently only support products that are marked as contract products.

Creating a product bundle

To create a product bundle

1. In the management portal, go to **Sales and Billing** > **Sales**, and click the **Bundles** tab.
2. If you are creating your first product bundle, click **Create new**. If you have existing bundles, click **New** in the top right corner.
3. In the displayed dialog, do the following:
   a. Enter the bundle's name.
   b. Enter a description of the bundle.
   c. Select a product category.
   d. Select a product. Note that only contract products are available for selection in bundles.
   e. Click **Add** to add the product to the bundle.



Bundle information

Bundle name: Bundle product #1

Description

Bundle Products

Select product category: Category #001

Select products: Full Service Server Management

   f. To add an additional product to the bundle, click **Add product**. Then select the relevant product category and product, and click **Add**. Repeat as required.
4. When you have added all the relevant products to the bundle, click **Done**.

   The bundle is now available for use when adding or updating a contract. For more information, see "Working with contracts" (p. 261).

Editing product bundles

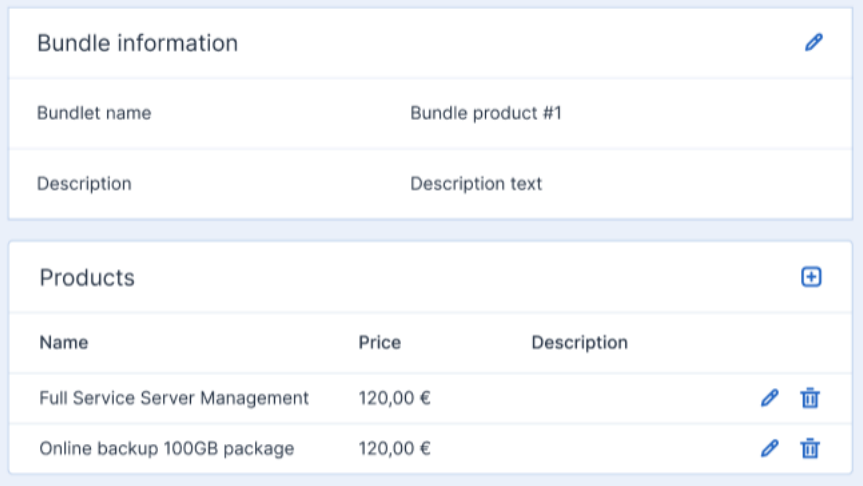
You can edit and delete product bundles as required.

To edit product bundles

1. In the management portal, go to **Sales and Billing** > **Sales**.
2. Click the **Bundles** tab to view any existing product bundles.

   If no bundles are displayed, you can click **Create new** to create a bundle. See "Creating a product bundle" (p. 286) for more information.

3. Click the relevant bundle row, and in the right pane, click the pencil icon.



Bundle information

Bundlet name	Bundle product #1
Description	Description text

Products

Name	Price	Description
Full Service Server Management	120,00 €	
Online backup 100GB package	120,00 €	

4. In the **Bundle information** section, modify the bundle name and description as required.
5. In the **Products** section:
   - Click ⊞ to add a new product. Then select the relevant product category and product, and click **Add**. Repeat as required.
   - Click the pencil icon to edit the product. For example, you might want to replace an existing product with a different product from the same category. When done, click **Save**.
   - Click the trash can icon to delete a product from the bundle.
6. When done, click ✓.

To delete a product bundle

1. Click the relevant bundle row, and in the far right column, click the ellipsis icon (...).
2. Select **Delete**. The bundle is deleted.

Note
Even if a product bundle was assigned to a current, ongoing contract, it can be deleted. This is because the bundle is basically just wrapping a number of individual products to a contract; a contract part is then added to the contract, one contract part for each product. After the contract is created, the bundle can be deleted.

Managing ledgers

The Ledgers section enables you to manage the ledger numbers that you currently use in your accounting system. These ledgers can then be connected to products you sell to your customers.

For example, when you create a CSV or XML export of your billing run, the export will contain all transactions including the correct ledger number. This allows for fast and easy imports.

To access ledgers, go to **Sales and billing** > **Products** and then click the **Ledgers** tab.

Creating a ledger

To create a ledger

1. In the management portal, go to **Sales and billing** > **Products**, and then click the **Ledgers** tab.
2. Click **+ New**.
3. In the Ledger information screen, define the following:
   - Define the ledger number.
   - (Optional) Enter the ledger's External ID.
   - (Optional) Enter a description for the ledger.
   - To use the ledger immediately, select the **Active** check box.
4. Click **Done**.

Editing a ledger

Note
Ledgers can be edited as required, but cannot be deleted.

To edit a ledger

1. In the management portal, go to **Sales and billing** > **Products**, and then click the **Ledgers** tab.
2. Click on the ledger row you want to edit.
3. In the displayed right pane, click the pencil icon and edit as required.
4. To deactivate an active ledger, disable the **Status** toggle switch.
5. When done, click ✓.

Configuring Advanced Automation (PSA) settings

In the **Settings** module you can configure various settings for your Advanced Automation (PSA) account.

These settings should be defined before working with the service, as they include a number of key settings required for getting started with your billing and service desk. This section includes settings for:

- Service desk
- Billing and quoting

Service desk settings

Service desk settings enable you to set up all essential sections of your service desk.

It is important for this to be done correctly for your tickets to function properly.

To access the service desk settings, go to **Settings** > **Service desk**.

Note
Under the service desk settings, you can also define user groups for your Advanced Automation (PSA) users. This is described in "Managing user groups" (p. 200), in the Managing your users section.

Configuring canned responses

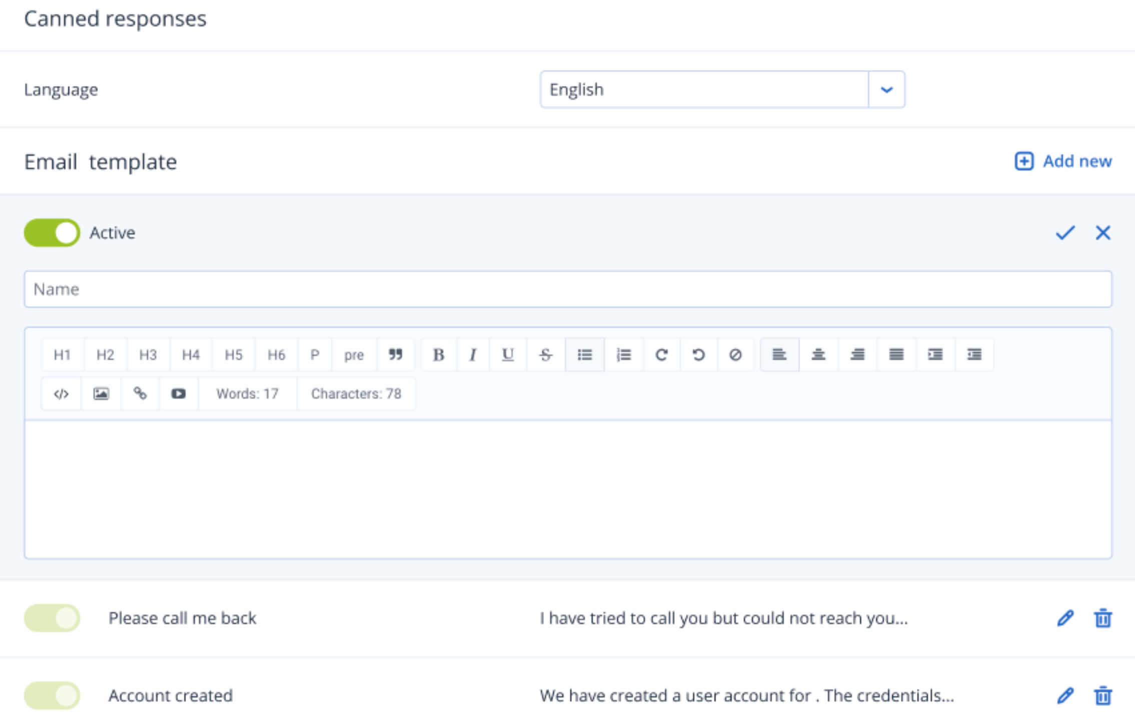
Canned responses enable you to add comment templates as part of your standard comments when creating a new ticket. These comments are included in the ticket's description.

Creating a canned response

You can add any number of canned responses to your service desk.

To create a new canned response

1. Go to **Settings** > **Service desk**, and then select **Canned responses**.
2. Click **Add new**.
3. Define a name for the canned response, and then add the relevant content.



Canned responses

Language: English

Email template

Please call me back — I have tried to call you but could not reach you...

Account created — We have created a user account for . The credentials...

You can use the following variables:

[SUPERIOR] - The name of the user's manager

[ENDUSER] - The name of the user

[SUPPORTUSER] - The name of the person that updates the ticket

[STATUS] - The status of the ticket

[TITLE] - The ticket title

4. By default, the canned response is **Active**. To deactivate the canned response, click the **Active** option switch.
5. Click ✓ to save the canned response. Once saved, the canned response can be used as content in the **Comments** field.

Editing or deleting a canned response

You can edit and delete canned responses as required.

To edit a canned response

1. Go to **Settings** > **Service desk**, and then select **Canned responses**.
2. Click the pencil icon for the canned response you want to edit, and then edit as required. For more information about the available options, see "Creating a canned response" (p. 290).
3. Click ✓ to save your changes.

To delete a canned response

1. In the **Canned responses** screen, click the trash can icon for the canned response you want to delete.
2. In the displayed confirmation message, click **Yes**.

Setting up priorities

You can define the priorities for your tickets. These priorities are used during the processing of a ticket, which will depend on the priority you set for each individual ticket. For example, an *urgent* priority is generally processed before a ticket that has a normal priority.

Adding a priority

To add a new priority

1. Go to **Settings** > **Service desk**, and then click **Priorities**.
2. Click **Add new**.
3. Enter the priority name and click ✓ . Note that the name does not reflect the level of priority but should be self-descriptive.

   By default, the priority is set as active.

   After you have successfully added the new priority, it can be used in the **Priority** field of your tickets (see "Creating a new ticket" (p. 208)). If required, you can set default priorities for tickets and default priorities for tickets coming from specific customers.

Editing or deleting a priority

You can edit and delete priorities as required.

To edit a priority

1. Go to **Settings** > **Service desk**, and then select **Priorities**.
2. Click the pencil icon for the priority you want to edit, and edit as required.
3. Click ✓ to save your changes.

   Note that you can also deactivate a priority by disabling the option switch next to the relevant active priority.

To delete a priority

1. In the **Priorities** screen, click the trash can icon for the priority that you want to delete.
2. In the displayed confirmation message, click **Yes**.

> **Note**
> The priority can only be deleted if it is currently deactivated and if it was not used in any tickets.

Managing your SLA policies

A service level agreement (SLA) policy is an official commitment between you and the customer. The SLA covers the quality of service you are offering to a customer and your committed availability to them.

Advanced Automation (PSA) enables you to manage SLAs, which, in turn, helps you organize the flow of support tickets and automate billable time calculations. In addition to the customer facing aspect, it helps you ensure that engineers stay on top of tickets and prevents tickets from existing for months without being handled.

You can configure and define SLAs to use for customer contracts, ticket activities and compliance tracking.

Creating a new SLA

To create a new SLA

1. Go to **Settings** > **Service desk**, and then select **SLA**.
2. Click **Add new**.
3. In the displayed screen, enter the name of your new SLA.
4. Define the applicable time range of your SLA by entering the initial response time (in hours) and feedback interval (in hours), and then entering the start and end time.
5. Select the **Apply SLA during** > **Weekends** checkbox to activate or deactivate this SLA during weekends.
6. Select the **Apply SLA during** > **Holidays** checkbox to activate or deactivate this SLA during holidays.
7. Set how your SLA is charged, by selecting **Fixed Price** or **Subsequent Calculation**.
8. Select a default product for billing, and a special rate activity for billing in the relevant drop-down lists.
   - **Default product for billing**: This optional parameter indicates a billable ticket-type product for ticket updates made within the SLA hours. For example, when a ticket engineer works on a ticket and an SLA is set, **Default product for billing** is pre-selected as a billable product for ticketed work. The product is automatically included in the ticket's time approval process, so a customer can be automatically billed for the relevant hours.
   - **Special rate activity for billing**: This optional parameter is the same as for **Default product for billing**, but for ticket updates outside the SLA hours.
9. If you want to set this SLA as the default, select the **Assign as default Service Level Agreement** check box.

10. Click ✓ to save the SLA.

    By default, the SLA is set as **Active**; to deactivate it, click the **Active** option switch.

    After you have successfully created the new SLA, it can be used in the **SLA** field of your tickets. For more details, see "Creating a new ticket" (p. 208).

Editing an SLA

To edit an SLA

1. Go to **Settings** > **Service desk**, and then select **SLA**.
2. Click the pencil icon for the relevant SLA.
3. Make the changes you want to the SLA. For more details, see "Creating a new SLA" (p. 292).
4. Click ✓ to save your changes.

Note

If the SLA was previously used for by customers (in tickets), you cannot deactivate the SLA.

Defining categories and subcategories

You can define any number of ticket categories to use in the Advanced Automation (PSA) service desk.

Advanced Automation (PSA) comes pre-filled with a set of categories and subcategories; when applied to your tickets, categories and subcategories provide a good overview of the most issues that are taking the most time and respond accordingly. You can also see these insights on a per customer basis.

In turn, this can help you improve your services. For example, when a client has 50% of their tickets categorized as *Workstation/virus*, you might want to upgrade security measures and staff training.

Creating a category or subcategory

To define a new category or subcategory

1. Go to **Settings** > **Service desk**, and then click **Categories and subcategories**.
2. Click **Add new**, and then enter the name for the category. If you want to make the category a subcategory, select the relevant parent category. The category or subcategory is created, and can be activated or deactivated as required, as described below.

To activate / deactivate a category or subcategory

In the **Categories and subcategories** screen, click the active switch to activate or deactivate the relevant category or subcategory.

Editing or deleting a category or subcategory

To edit a category or subcategory

1. In the **Categories and subcategories** screen, click the pencil icon for the relevant category or subcategory.
2. Edit as required.

To delete a category or subcategory

1. In the **Categories and subcategories** screen, click the trash can icon for the relevant category or subcategory.
2. In the displayed confirmation message, click **Yes**.

Note
The category or subcategory can only be deleted if it is currently deactivated and if it was not used in any tickets.

Setting default values

You can define default values for many Advanced Automation (PSA) features.

Important
Initial system default settings are applied on the activation of all existing customers. When new customers are subsequently created, the current default settings (listed below) are applied to the customer's service desk settings. When you later update the default settings, the customer's service desk values are not automatically updated, and must be updated manually.

Note
You can override the general default settings with customer-specific values in each customer's settings. To access these customer-specific settings, go to **Clients**, click the ellipsis icon for the relevant tenant, and then select **Configure**. Then click the **Configure** tab, and under the **Service desk** section, click the pencil icon to update the relevant default settings for the selected customer.

The values that can be updated include: **Default SLA**, **Default category**, **Default priority**, **Default group**, **Default support user**, **Default primary contact**, and **Customer documentation**.

The **Days off per year** setting can be updated in the **User settings** section. To access these settings, go to **My Company** > **Users**, select the relevant user, and then click **User settings**.

To define default values

1. Go to **Settings > Service desk**.
2. Select **Default values**.

   The list of default values is displayed:

   - **Default SLA**: The default SLA applied to tickets. By default, **Default SLA** is selected.
   - **Category**: The default ticket category. By default, **Hardware issue** is selected.
   - **Default priority**: The default priority for tickets. By default, **Normal** is selected.
   - **Default group**: The default group for tickets. By default, **Support group** is selected.

- **Default support user**: The default support user for tickets. By default, the user who activated the Advanced Automation (PSA) service is selected. Alternatively, you can select **Ticket pool**, to ensure that new tickets are automatically assigned to the Ticket pool, rather than a specific user.
- **Days off per year**: The default days off per year for users. By default, **15**.
- **Remaining days off policy**: The organizational policy for any remaining days off for users. Note that when a new year begins (1 January, 00:00), Advanced Automation (PSA) automatically recalculates the PTO balances for all users with an Advanced Automation (PSA) role according to the policy specified. Select from one of the following:
  - **Discard remaining days off** (selected by default)
  - **Move all remaining days off to the next year**
  - **Move some days off to the next year**

    When **Move some days off to the next year** is selected, the additional **Maximum number of days to move** field is displayed, in which you define the number required.
- **Customer documentation**: A link to customer-related documentation. By default, this field is empty.

  When a link is defined, a **Customer documentation** link is displayed in the **Create new ticket** screen when you create a new ticket (see "Creating a new ticket" (p. 208)), and the **Overview** tab when editing a ticket (see "Updating tickets" (p. 211)).
- **Occupancy rate notification threshold**: The notification threshold is where the amount of worked time recorded by you or a group of which you are a member or manager of is below the set hours for that day; a reminder is sent to complete the hour registration. By default, **85** is selected.
- **Auto pause ticket timer on screen leave**: You can auto-pause the ticket timer whenever users switch their active screen to a different one. By default, **No** is selected.
- **Ticket update mandatory**: Define if the **Ticket description** field in the ticket settings is mandatory. This enables you to more closely track changes to a ticket during the processing of the ticket. By default, **No** is selected.
- **Public ticket portal**: The page users can access to submit tickets directly, without registering or signing in to the system. When enabled, **Ticket portal URL** (a system-generated link) is displayed.

  For more information about how to submit a ticket, see Submitting service desk tickets via the ticket portal.

  Note

  The public ticket portal has the same branding as defined for your tenant, as described in "Configuring branding and white labeling" (p. 91).

  You can also embed the ticket form on third party websites. For more information, see "Embedding the ticket submission form on your website" (p. 220).

    - **Process requests from unknown users**: Define if the public ticket portal will process requests from users that are not registered in the system. This option is only displayed if the **Public ticket portal** option is enabled. By default, **Off** is selected.

3. Apply the default values you want, and click **Save**.

Defining country and language settings

The **Country settings** screen enables you to define global company settings when working with Advanced Automation (PSA), including your default country and time zone. These global settings impact the currency and hours displayed, and are especially important for hours that are part of a Service Level Agreement (SLA).

To define country and language settings

1. Go to **Settings** > **Service desk**, and then select **Country settings**.
2. In the **Country settings** section, click the pencil icon to edit any of the following settings:
    - **Default country**: Select the relevant country. The selected country defines the default currency used for all prices and costs in Advanced Automation (PSA).
    - **Time zone**: Select the relevant time zone. The time zone impacts SLA hours by determining whether tickets are received within SLA hours or outside of SLA hours. It can also impact the price for ticketed work.
    - **Daylight savings**: Click the toggle switch to enable Daylight Saving Time.
3. Click ✓ to save your changes.
4. In the **Languages** section, click the pencil icon to define the default system language used in Advanced Automation (PSA).
5. Click the toggle switch to enable the relevant language.
6. Click ✓ to save your changes.

Activating and deactivating statuses

The **Statuses** screen shows the various statuses available for service desk, quote and project tickets. You can activate or deactivate the statuses for tickets.

Note
You cannot add or delete a status or delete or change the name of the status. For some integrations, statuses are linked to ticket statuses.

To activate or deactivate statuses

1. Go to **Settings** > **Service desk**, and then select **Statuses**.
2. Click **Edit**.
3. In the displayed list of statuses, click the activate/deactivate switch for the relevant statuses.

    If a status is non-editable, it indicates that the status is predefined in Advanced Automation (PSA) and cannot be changed. In addition, if a status is currently in use, it cannot be deactivated.

Note

The following statuses cannot be deactivated because they are used in the default ticket flow and integrations:

- New
- In Progress
- SLA breach
- Waiting for response
- Completed
- Reopened
- Solved
- Closed

For more information about the ticket status types available for the service desk, quotes, and projects, see "Ticket status types" (p. 297).

4. Click **Save**.

Ticket status types

The full list of mandatory and optional ticket status types is shown in the **Statuses** screen.

Mandatory ticket statuses are system predefined and cannot be deactivated. Optional ticket statuses can be activated and deactivated, as required. For more information, see "Activating and deactivating statuses" (p. 296).

Mandatory ticket statuses

Status	Included in service desk (service desk and quote tickets)	Included in projects (project step tickets)
New	Yes	Yes
In progress	Yes	Yes
Completed	No	Yes
Closed	Yes	No
Solved	Yes	No
Waiting for response	Yes	No
SLA breach	Yes	No
Reopened	Yes	No

Optional ticket statuses

Status	Included in service desk (service desk and quote tickets)	Included in projects (project step tickets)
On-site work scheduled	Yes	No
Incident	Yes	No
Outstanding quote	Yes	No
Activities scheduled	Yes	No
Waiting for approval	Yes	No
Change	Yes	No
Update by employee	Yes	No
Client update received	Yes	No
Scheduled activities	Yes	No
Schedule on-site activities	Yes	No
Update added by supplier	Yes	No
Pending vendor/supplier	Yes	No
On hold	Yes	Yes
Pending start	No	Yes
Delayed	No	Yes

Defining default RMM ticket integration settings

When integrating with Remote Monitoring and Management (RMM) systems, you can set the **Default SLA**, **Category** and **Priority** fields for tickets generated by your RMM. If a ticket is RMM-integrated, default values are automatically applied, depending on the values you define in the following procedure.

To define default RMM ticket integration settings

1. Go to **Settings** > **Service desk**, and then select **RMM ticket integration**.
2. Click **Edit**.
3. Set your **Default SLA**, **Category**, and **Priority** values and click **Save**.

Managing email templates

In the **Email templates** screen you can view all the predefined email templates in Advanced Automation (PSA). These templates are used for external communication with end users. You can customize the templates by using either the rich text editor or pasting your custom HTML code into the editor.

You cannot add to or delete any of the email templates.

Note
The default email templates are designed to be displayed correctly in most email clients on desktops and mobiles. When making changes, try to ensure the correct display is maintained.

Editing an email template

To edit an email template

1. Go to **Settings** > **Service desk**, and then select **Email templates**.
2. Click the pencil icon for the template you want to edit.
3. Update the template as required.

   You can use the following variables for the different message types:

Add ticket from email		Update ticket from email		Add ticket from application		Update ticket from application	
Subject	**Body**	**Subject**	**Body**	**Subject**	**Body**	**Subject**	**Body**
[REF]	[REF]	[REF]	[REF]	[REF]	[REF]	[REF]	[REF]
[TITLE]	[STATUS]	[TITLE]	[STATUS]	[TITLE]	[STATUS]	[TITLE]	[STATUS]
	[TITLE]		[TITLE]	[SUPPORTUSER]	[TITLE]		[TITLE]
	[UPDATE]		[UPDATE]		[UPDATE]		[UPDATE]
	[ENDUSER]		[ENDUSER]		[ENDUSER]		[ENDUSER]
					[SUPPORTUSER]		[SUPPORTUSER]

4. To customize the email background color, add a style code snippet to the HTML code of your template. Otherwise, the default style will be added when the email message is created.

   Example paragraph style code for a white background:

   <p style="background-color: #ffffff;"> [YOUR EMAIL TEMPLATE CONTENT] </p>
5. Click ✓ to save your changes.

Note

If you make a number of changes to an email template and then want to reset the template to its default layout and text, you will need to reapply the HTML code for that template. For more information, see "Email template defaults" (p. 300)

Email template defaults

Advanced Automation (PSA) includes a set of customizable default email templates. If you need to restore a template to its default, you can use the HTML codes of the default templates, provided below.

- Closed solved ticket
- Quote created
- New ticket from email
- Ticket update
- Ticket rating request
- Ticket rating received
- Quote processed
- New ticket
- New invoice
- Merged ticket

Closed solved ticket

Subject: Closed solved ticket

Code:

```
<table class="body-wrap" style="font-size: 14px;width: 100%;background-color: #f6f6f6;" bgcolor="#f6f6f6">

 <tbody>

  <tr style="font-size: 14px;">

   <td style="font-size: 14px;vertical-align: top;">

   </td>

   <td class="container" width="600" style="font-size: 14px;vertical-align: top;">

   <div class="content" style="font-size: 14px;">

   <table class="main" width="100%" cellpadding="0" cellspacing="0" style="font-size: 14px;background-color: #fff;" bgcolor="#fff">

    <tbody>
```

```
     <tr style="font-size: 14px;">
      <td class="alert alert-warning" style="font-size: 16px;vertical-align:
top;color: #fff;text-align: center;background-color: #0065E3;text-align: center;"
bgcolor="#0065E3">
      Solved ticket has been closed</td>
      </tr>
      <tr style="font-size: 14px;">
       <td class="content-wrap" style="font-size: 14px;vertical-align: top;">
        <table width="100%" cellpadding="0" cellspacing="0" style="font-size:
14px;">
        <tbody>
         <tr style="font-size: 14px;">
          <td class="content-block" style="font-size: 14px;vertical-align: top;">
          </td>
          </tr>
          <tr style="font-size: 14px;">
          <td class="content-block" style="font-size: 14px;vertical-align:
top;">Hello [ENDUSER]!</td>
          </tr>
          <tr style="font-size: 14px;">
          <td class="content-block" style="font-size: 14px;vertical-align:
top;">Your ticket with reference number [REF] has been closed automatically because
it has been in the 'Solved' status for more than [WAITINGDAYS] days.</td>
          </tr>
          <tr style="font-size: 14px;">
          <td class="content-block" style="font-size: 14px;vertical-align: top;">
          <br>
          </td>
          </tr>
         </tbody>
         </table>
        </td>
       </tr>
      </tbody>
     </table>
    <div class="footer" style="font-size: 14px;width: 100%;color: #999;"></div>
    </div>
   </td>
   <td style="font-size: 14px;vertical-align: top;"></td>
   </tr>
 </tbody>
</table>
```

Quote created

Subject: A new quote with description: [TITLE] has been created for you

Code:

```
<table class="body-wrap" style="font-size: 14px;width: 100%;background-color:
#f6f6f6;" bgcolor="#f6f6f6">
 <tbody>
  <tr style="font-size: 14px;">
   <td style="font-size: 14px;vertical-align: top;"></td>
   </tr>
   <tr>
    <td class="container" width="600" style="font-size: 14px;vertical-align: top;">
     <div class="content" style="font-size: 14px;">
      <table class="main" width="100%" cellpadding="0" cellspacing="0" style="font-
size: 14px;background-color: #fff;" bgcolor="#fff">
        <tbody>
         <tr style="font-size: 14px;">
           <td class="alert alert-warning" style="font-size: 16px;vertical-align:
top;color: #fff;text-align: center;background-color: #0065E3;text-align: center;"
bgcolor="#0065E3">A new quote was created for you</td>
         </tr>
         <tr style="font-size: 14px;">
           <td class="content-wrap" style="font-size: 14px;vertical-align: top;">
           <table width="100%" cellpadding="0" cellspacing="0" style="font-size:
```

```
14px;">
           <tbody>
            <tr style="font-size: 14px;">
             <td class="content-block" style="font-size: 14px;vertical-align:
top;"></td>
            </tr>
            <tr style="font-size: 14px;">
             <td class="content-block" style="font-size: 14px;vertical-align:
top;">Hello [CLIENT]!</td>
            </tr>
            <tr style="font-size: 14px;">
             <td class="content-block" style="font-size: 14px;vertical-align:
top;">Please find attached your new quote with description [TITLE] and number
[number].</td>
            </tr>
            <tr style="font-size: 14px;">
             <td class="content-block" style="font-size: 14px;vertical-align:
top;">Please use the following link to review the quote.</td>
            </tr>
            <tr style="font-size: 14px;">
             <td class="content-block" style="font-size: 14px;vertical-align: top;">
             <a href="[QUOTE_LINK]">New Quote</a>
             </td>
            </tr>
            <tr style="font-size: 14px;">
             <td class="content-block" style="font-size: 14px;vertical-align: top;">
             <br>
             </td>
            </tr>
           </tbody>
          </table>
         </td>
        </tr>
       </tbody>
```

```
      </table>
      <div class="footer" style="font-size: 14px;width: 100%;color: #999;"></div>
     </div>
    </td>
    <td style="font-size: 14px;vertical-align: top;"></td>
   </tr>
  </tbody>
</table>
```

New ticket from email

Subject: New ticket with reference number: [REF]

Code:

```
<table class="body-wrap" style="font-size: 14px;width: 100%;background-color: #f6f6f6;" bgcolor="#f6f6f6">
 <tbody>
  <tr style="font-size: 14px;">
   <td style="font-size: 14px;vertical-align: top;"></td>
   <td class="container" width="600" style="font-size: 14px;vertical-align: top;">
    <div class="content" style="font-size: 14px;">
     <table class="main" width="100%" cellpadding="0" cellspacing="0" style="font-size: 14px;background-color: #fff;" bgcolor="#fff">
      <tbody>
       <tr style="font-size: 14px;">
        <td class="alert alert-warning" style="font-size: 16px;vertical-align: top;color: #fff;text-align: center;background-color: #0065E3;text-align: center;" bgcolor="#0065E3">New ticket created from email</td>
       </tr>
       <tr style="font-size: 14px;">
        <td class="content-wrap" style="font-size: 14px;vertical-align: top;">
         <table width="100%" cellpadding="0" cellspacing="0" style="font-size: 14px;">
          <tbody>
```

```
           <tr style="font-size: 14px;">

            <td class="content-block" style="font-size: 14px;vertical-align:
top;"></td>

           </tr>

           <tr style="font-size: 14px;">

            <td class="content-block" style="font-size: 14px;vertical-align: top;">A
new ticket has been created from email with the following reference number:
[REF]</td>

           </tr>

           <tr style="font-size: 14px;">

            <td class="content-block" style="font-size: 14px;vertical-align:
top;">Ticket Status: [STATUS]</td>

           </tr>

           <tr style="font-size: 14px;">

            <td class="content-block" style="font-size: 14px;vertical-align:
top;">Ticket title: [TITLE]</td>

           </tr>

           <tr style="font-size: 14px;">

            <td class="content-block" style="font-size: 14px;vertical-align:
top;">Request: [UPDATE]</td>

           </tr>

           <tr style="font-size: 14px;">

            <td class="content-block" style="font-size: 14px;vertical-align: top;">A
support engineer will handle your request as soon as possible.</td>

           </tr>

           <tr style="font-size: 14px;">

            <td class="content-block" style="font-size: 14px;vertical-align: top;">

            <br>

            </td>

           </tr>

          </tbody>

         </table>

        </td>

       </tr>
```

```
      </tbody>
     </table>
     <div class="footer" style="font-size: 14px;width: 100%;color: #999;"></div>
    </div>
   </td>
   <td style="font-size: 14px;vertical-align: top;"></td>
  </tr>
 </tbody>
</table>
```

Ticket update

Subject: New update for your ticket [TITLE] - ref number - [REF]

Code:

```
<table class="body-wrap" style="font-size: 14px;width: 100%;background-color:
#f6f6f6;" bgcolor="#f6f6f6">
 <tbody>
  <tr style="font-size: 14px;">
   <td style="font-size: 14px;vertical-align: top;"></td>
   <td class="container" width="600" style="font-size: 14px;vertical-align: top;">
    <div class="content" style="font-size: 14px;">
     <table class="main" width="100%" cellpadding="0" cellspacing="0" style="font-
size: 14px;background-color: #fff;" bgcolor="#fff">
      <tbody>
       <tr style="font-size: 14px;">
        <td class="alert alert-warning" style="font-size: 16px;vertical-align:
top;color: #fff;text-align: center;background-color: #0065E3;text-align: center;"
bgcolor="#0065E3">Ticket update</td>
       </tr>
       <tr style="font-size: 14px;">
        <td class="content-wrap" style="font-size: 14px;vertical-align: top;">
         <table width="100%" cellpadding="0" cellspacing="0" style="font-size:
14px;">
```

```
          <tbody>
           <tr style="font-size: 14px;">
            <td class="content-block" style="font-size: 14px;vertical-align:
top;"></td>
           </tr>
           <tr style="font-size: 14px;">
            <td class="content-block" style="font-size: 14px;vertical-align: top;">
A new update has been made for your ticket with reference number : [REF]</td>
           </tr>
           <tr style="font-size: 14px;">
            <td class="content-block" style="font-size: 14px;vertical-align:
top;">Ticket Status : [STATUS]</td>
           </tr>
           <tr style="font-size: 14px;">
            <td class="content-block" style="font-size: 14px;vertical-align:
top;">Support engineer message: [UPDATE]</td>
           </tr>
           <tr style="font-size: 14px;">
            <td class="content-block" style="font-size: 14px;vertical-align: top;">
            <br>
            </td>
           </tr>
          </tbody>
         </table>
        </td>
       </tr>
      </tbody>
     </table>
     <div class="footer" style="font-size: 14px;width: 100%;color: #999;"></div>
    </div>
   </td>
   <td style="font-size: 14px;vertical-align: top;"></td>
  </tr>
```

```
 </tbody>

</table>
```

Ticket rating request

Subject: Ticket rating request

Code:

```
<table class="body-wrap" style="font-size: 14px;width: 100%;background-color: #f6f6f6;" bgcolor="#f6f6f6">

 <tbody>

  <tr style="font-size: 14px;">

   <td style="font-size: 14px;vertical-align: top;"></td>

  </tr>

  <tr>

   <td class="container" width="600" style="font-size: 14px;vertical-align: top;">

    <div class="content" style="font-size: 14px;">

     <table class="main" width="100%" cellpadding="0" cellspacing="0" style="font-size: 14px;background-color: #fff;" bgcolor="#fff">

      <tbody>

       <tr style="font-size: 14px;">

        <td class="alert alert-warning" style="font-size: 16px;vertical-align: top;color: #fff;text-align: center;background-color: #0065E3;text-align: center;" bgcolor="#0065E3">We have closed your ticket - Please let us know how we did</td>

       </tr>

       <tr style="font-size: 14px;">

        <td class="content-wrap" style="font-size: 14px;vertical-align: top;">

         <table width="100%" cellpadding="0" cellspacing="0" style="font-size: 14px;">

          <tbody>

           <tr style="font-size: 14px;">

            <td style="font-size: 14px;vertical-align: top;"></td>

           </tr>

           <tr style="font-size: 14px;">
```

```
            <td style="font-size: 14px;vertical-align: top;">Hello [CUSTOMER]!</td>
           </tr>
           <tr style="font-size: 14px;">
            <td style="font-size: 14px;vertical-align: top;">
            Your ticket with number [REF] has been closed. Please find the details
of the ticket here:<br>
            <br>
            </td>
           </tr>
           <tr style="font-size: 14px;">
            <td style="font-size: 14px;vertical-align: top;">
            <div style="float: left;">Ticket reference number:</div>
            <div style="float: left;">[REF]</div>
            </td>
           </tr>
           <tr style="font-size: 14px;">
            <td style="font-size: 14px;vertical-align: top;">
            <div style="float: left;">Support engineer:</div>
            <div style="float: left;">[SUPPORTUSER]</div>
            </td>
           </tr>
           <tr style="font-size: 14px;">
            <td style="font-size: 14px;vertical-align: top;">
            <div style="float: left;">Support engineer message:</div>
            <div style="float: left;">[SUPPORTUSERMESSAGE]</div>
            </td>
           </tr>
           <tr style="font-size: 14px;">
            <td style="font-size: 14px;vertical-align: top;">
            <div style="float: left;">Initial problem:</div>
            <div style="float: left;">[PROBLEM]</div>
            </td>
           </tr>

           <tr style="font-size: 14px;">

            <td style="font-size: 14px;vertical-align: top;">

            <div style="float: left;">Ticket title:</div>

            <div style="float: left;">

            [TITLE]<br>

            <br>

            </div>

            </td>

           </tr>

           <tr style="font-size: 14px;">

            <td style="font-size: 14px;vertical-align: top;">How likely is it that
you would recommend our company/product/service to a friend or colleague?</td>

           </tr>

           <tr style="font-size: 14px;">

            <td style="font-size: 14px;vertical-align: top;">

             <table cellspacing="0">

              <tbody>

               <tr>

                <td style="width: 50px;height: 50px;text-align: center;vertical-
align: middle;">

                 <a href="[URL]/?key=[KEY]&amp;rateValue=0" class="fa fa-star"
id="rating0">

                 <div style="font-size: 14px;vertical-align:
bottom;color:#666f7b">0</div>

                 </a>

                </td>

                <td style="width: 50px;height: 50px;text-align: center;vertical-
align: middle;">

                 <a href="[URL]/?key=[KEY]&amp;rateValue=1" class="fa fa-star"
id="rating1">

                 <div style="font-size: 14px;vertical-align:
bottom;color:#666f7b">1</div>

                 </a>
                </td>
                <td style="width: 50px;height: 50px;text-align: center;vertical-
align: middle;">
                 <a href="[URL]/?key=[KEY]&amp;rateValue=2" class="fa fa-star"
id="rating2">
                 <div style="font-size: 14px;vertical-align:
bottom;color:#666f7b">2</div>
                 </a>
                </td>
                <td style="width: 50px;height: 50px;text-align: center;vertical-
align: middle;">
                 <a href="[URL]/?key=[KEY]&amp;rateValue=3" class="fa fa-star"
id="rating3">
                 <div style="font-size: 14px;vertical-align:
bottom;color:#666f7b">3</div>
                 </a>
                </td>
                <td style="width: 50px;height: 50px;text-align: center;vertical-
align: middle;">
                 <a href="[URL]/?key=[KEY]&amp;rateValue=4" class="fa fa-star"
id="rating4">
                 <div style="font-size: 14px;vertical-align:
bottom;color:#666f7b">4</div>
                 </a>
                </td>
                <td style="width: 50px;height: 50px;text-align: center;vertical-
align: middle;">
                 <a href="[URL]/?key=[KEY]&amp;rateValue=5" class="fa fa-star"
id="rating5">
                 <div style="font-size: 14px;vertical-align:
bottom;color:#666f7b">5</div>
                 </a>
                </td>
                <td style="width: 50px;height: 50px;text-align: center;vertical-
align: middle;">
                 <a href="[URL]/?key=[KEY]&amp;rateValue=6" class="fa fa-star"
id="rating6">
                 <div style="font-size: 14px;vertical-align:
```

```
bottom;color:#666f7b">6</div>

                 </a>

                </td>

                <td style="width: 50px;height: 50px;text-align: center;vertical-
align: middle;">

                 <a href="[URL]/?key=[KEY]&amp;rateValue=7" class="fa fa-star"
id="rating7">

                 <div style="font-size: 14px;vertical-align:
bottom;color:#666f7b">7</div>

                 </a>

                </td>

                <td style="width: 50px;height: 50px;text-align: center;vertical-
align: middle;">

                 <a href="[URL]/?key=[KEY]&amp;rateValue=8" class="fa fa-star"
id="rating8">

                 <div style="font-size: 14px;vertical-align:
bottom;color:#666f7b">8</div>

                 </a>

                </td>

                <td style="width: 50px;height: 50px;text-align: center;vertical-
align: middle;">

                 <a href="[URL]/?key=[KEY]&amp;rateValue=9" class="fa fa-star"
id="rating9">

                 <div style="font-size: 14px;vertical-align:
bottom;color:#666f7b">9</div>

                 </a>

                </td>

                <td style="width: 50px;height: 50px;text-align: center;vertical-
align: middle;">

                 <a href="[URL]/?key=[KEY]&amp;rateValue=10" class="fa fa-star"
id="rating10">

                 <div style="font-size: 14px;vertical-align:
bottom;color:#666f7b">10</div>

                 </a>

                </td>

               </tr>

              </tbody>
```

```
             </table>
            </td>
           </tr>
           <tr style="font-size: 14px;">
            <td style="font-size: 14px;vertical-align: top;">
            <br>
            </td>
           </tr>
          </tbody>
         </table>
        </td>
       </tr>
      </tbody>
     </table>
     <div class="footer" style="font-size: 14px;width: 100%;color: #999;"></div>
     </div>
    </td>
    <td style="font-size: 14px;vertical-align: top;"></td>
  </tr>
 </tbody>
</table>
```

Ticket rating received

Subject: Customer [Customer] rated ticket [REF]

Code:

```
<table class="body-wrap" style="font-size: 14px;width: 100%;background-color: #f6f6f6;" bgcolor="#f6f6f6">
 <tbody>
  <tr style="font-size: 14px;">
   <td style="font-size: 14px;vertical-align: top;"></td>
   <td class="container" width="600" style="font-size: 14px;vertical-align: top;">
    <div class="content" style="font-size: 14px;">
     <table class="main" width="100%" cellpadding="0" cellspacing="0" style="font-size: 14px;background-color: #fff;" bgcolor="#fff">
      <tbody>
       <tr style="font-size: 14px;">
        <td class="alert alert-warning" style="font-size: 16px;vertical-align: top;color: #fff;text-align: center;background-color: #0065E3;text-align: center;" bgcolor="#0065E3">Your ticket has been rated</td>
       </tr>
       <tr style="font-size: 14px;">
        <td class="content-wrap" style="font-size: 14px;vertical-align: top;">
         <table width="100%" cellpadding="0" cellspacing="0" style="font-size: 14px;">
          <tbody>
           <tr style="font-size: 14px;">
            <td class="content-block" style="font-size: 14px;vertical-align: top;"></td>
           </tr>
           <tr style="font-size: 14px;">
            <td class="content-block" style="font-size: 14px;vertical-align: top;">Hello [SUPPORTUSER]!</td>
           </tr>
           <tr style="font-size: 14px;">
            <td class="content-block" style="font-size: 14px;vertical-align: top;">Your ticket with number [REF] has been rated: </td>
           </tr>
           <tr style="font-size: 14px;">
            <td class="content-block" style="font-size: 14px;vertical-align: top;">Ticket reference number: [REF]</td>
           </tr>
           <tr style="font-size: 14px;">
            <td class="content-block" style="font-size: 14px;vertical-align: top;">Grade: [GRADE]</td>
           </tr>
           <tr style="font-size: 14px;">
            <td class="content-block" style="font-size: 14px;vertical-align: top;">
End user: [CLIENT]</td>
           </tr>
           <tr style="font-size: 14px;">
            <td class="content-block" style="font-size: 14px;vertical-align: top;">
Customer: [CUSTOMER]</td>
           </tr>
           <tr style="font-size: 14px;">
            <td class="content-block" style="font-size: 14px;vertical-align: top;">
            <br>
            </td>
           </tr>
          </tbody>
         </table>
        </td>
       </tr>
      </tbody>
     </table>
     <div class="footer" style="font-size: 14px;width: 100%;color: #999;"></div>
    </div>
   </td>
   <td style="font-size: 14px;vertical-align: top;"></td>
  </tr>
 </tbody>
</table>
```

Quote processed

Subject: Quote [DESCRIPTION] - [NUMBER] was [ACCEPTED]

Code:

```
<table class="body-wrap" style="font-size: 14px;width: 100%;background-color:
```

```
#f6f6f6;" bgcolor="#f6f6f6">
 <tbody>
  <tr style="font-size: 14px;">
   <td style="font-size: 14px;vertical-align: top;"></td>
  </tr>
  <tr>
   <td class="container" width="600" style="font-size: 14px;vertical-align: top;">
    <div class="content" style="font-size: 14px;">
     <table class="main" width="100%" cellpadding="0" cellspacing="0" style="font-size: 14px;background-color: #fff;" bgcolor="#fff">
      <tbody>
       <tr style="font-size: 14px;">
        <td class="alert alert-warning" style="font-size: 16px;vertical-align: top;color: #fff;text-align: center;background-color: #0065E3;text-align: center;" bgcolor="#0065E3">A quote was processed</td>
       </tr>
       <tr style="font-size: 14px;">
        <td class="content-wrap" style="font-size: 14px;vertical-align: top;">
         <table width="100%" cellpadding="0" cellspacing="0" style="font-size: 14px;">
          <tbody>
           <tr style="font-size: 14px;">
            <td class="content-block" style="font-size: 14px;vertical-align: top;"></td>
           </tr>
           <tr style="font-size: 14px;">
            <td class="content-block" style="font-size: 14px;vertical-align: top;">Hello [CLIENT]!</td>
           </tr>
           <tr style="font-size: 14px;">
            <td class="content-block" style="font-size: 14px;vertical-align: top;">Please be informed that quote [DESCRIPTION] - [NUMBER] was [ACCEPTED] by [USER].</td>
           </tr>
           <tr style="font-size: 14px;">
```

```
            <td class="content-block" style="font-size: 14px;vertical-align: top;">
            <br>
            </td>
           </tr>
          </tbody>
         </table>
        </td>
       </tr>
      </tbody>
     </table>
     <div class="footer" style="font-size: 14px;width: 100%;color: #999;"></div>
    </div>
   </td>
   <td style="font-size: 14px;vertical-align: top;"></td>
  </tr>
 </tbody>
</table>
```

New ticket

Subject: New ticket created: [TITLE] - reference number [REF] - Support engineer/Business unit [SUPPORTUSER]

Code:

```
<table class="body-wrap" style="font-size: 14px;width: 100%;background-color:
#f6f6f6;" bgcolor="#f6f6f6">
 <tbody>
  <tr style="font-size: 14px;">
   <td style="font-size: 14px;vertical-align: top;"></td>
   <td class="container" width="600" style="font-size: 14px;vertical-align: top;">
    <div class="content" style="font-size: 14px;">
     <table class="main" width="100%" cellpadding="0" cellspacing="0" style="font-
size: 14px;background-color: #fff;" bgcolor="#fff">
```

```
      <tbody>

       <tr style="font-size: 14px;">

        <td class="alert alert-warning" style="font-size: 16px;vertical-align:
top;color: #fff;text-align: center;background-color: #0065E3;text-align: center;"
bgcolor="#0065E3">New ticket has been created</td>

       </tr>

       <tr style="font-size: 14px;">

        <td class="content-wrap" style="font-size: 14px;vertical-align: top;">

         <table width="100%" cellpadding="0" cellspacing="0" style="font-size:
14px;">

          <tbody>

           <tr style="font-size: 14px;">

            <td class="content-block" style="font-size: 14px;vertical-align:
top;"></td>

           </tr>

           <tr style="font-size: 14px;">

            <td class="content-block" style="font-size: 14px;vertical-align: top;">A
new ticket has been created for you with the following reference number: [REF]</td>

           </tr>

           <tr style="font-size: 14px;">

            <td class="content-block" style="font-size: 14px;vertical-align:
top;">Ticket Status: [STATUS]</td>

           </tr>

           <tr style="font-size: 14px;">

            <td class="content-block" style="font-size: 14px;vertical-align:
top;">Ticket title: [TITLE]</td>

           </tr>

           <tr style="font-size: 14px;">

            <td class="content-block" style="font-size: 14px;vertical-align:
top;">Request: [UPDATE]</td>

           </tr>

           <tr style="font-size: 14px;">

            <td class="content-block" style="font-size: 14px;vertical-align:
top;">Support engineer/Business unit: [SUPPORTUSER]</td>

           </tr>
           <tr style="font-size: 14px;">
            <td class="content-block" style="font-size: 14px;vertical-align: top;">
            <br>
            </td>
           </tr>
          </tbody>
         </table>
        </td>
       </tr>
      </tbody>
     </table>
     <div class="footer" style="font-size: 14px;width: 100%;color: #999;"></div>
    </div>
   </td>
   <td style="font-size: 14px;vertical-align: top;"></td>
  </tr>
 </tbody>
</table>
```

New invoice

Subject: Invoice number [number] has been issued

Code:

```
<table class="body-wrap" style="font-size: 14px;width: 100%;background-color: #f6f6f6;" bgcolor="#f6f6f6">
 <tbody>
  <tr style="font-size: 14px;">
   <td style="font-size: 14px;vertical-align: top;"></td>
  </tr>
  <tr>
   <td class="container" width="600" style="font-size: 14px;vertical-align: top;">
```

```
    <div class="content" style="font-size: 14px;">
     <table class="main" width="100%" cellpadding="0" cellspacing="0" style="font-size: 14px;background-color: #fff;" bgcolor="#fff">
      <tbody>
       <tr style="font-size: 14px;">
        <td class="alert alert-warning" style="font-size: 16px;vertical-align: top;color: #fff;text-align: center;background-color: #0065E3;text-align: center;" bgcolor="#0065E3">We have issued a new invoice</td>
       </tr>
       <tr style="font-size: 14px;">
        <td class="content-wrap" style="font-size: 14px;vertical-align: top;">
         <table width="100%" cellpadding="0" cellspacing="0" style="font-size: 14px;">
          <tbody>
           <tr style="font-size: 14px;">
            <td class="content-block" style="font-size: 14px;vertical-align: top;"></td>
           </tr>
           <tr style="font-size: 14px;">
            <td class="content-block" style="font-size: 14px;vertical-align: top;">Hello [CUSTOMER]!</td>
           </tr>
           <tr style="font-size: 14px;">
            <td class="content-block" style="font-size: 14px;vertical-align: top;">Please find attached the invoice with number [number].</td>
           </tr>
           <tr style="font-size: 14px;">
            <td class="content-block" style="font-size: 14px;vertical-align: top;">Please use one of these links to complete your payment: </td>
           </tr>
           <tr style="font-size: 14px;">
            <td class="content-block" style="font-size: 14px;vertical-align: top;">
            <a href="[PAYPAL_LINK]">Pay with PayPal</a>
            </td>
           </tr>
           <tr style="font-size: 14px;">
            <td class="content-block" style="font-size: 14px;vertical-align: top;">
            <a href="[STRIPE_LINK]">Pay with Stripe</a>
            </td>
           </tr>
           <tr style="font-size: 14px;">
            <td class="content-block" style="font-size: 14px;vertical-align: top;">
            <br>
            </td>
           </tr>
          </tbody>
         </table>
        </td>
       </tr>
      </tbody>
     </table>
     <div class="footer" style="font-size: 14px;width: 100%;color: #999;"></div>
    </div>
   </td>
   <td style="font-size: 14px;vertical-align: top;"></td>
  </tr>
 </tbody>
</table>
```

Merged ticket

Subject: Your ticket [TITLE] - ref number - [REF] has been merged into another ticket

Code:

```
<table class="body-wrap" style="font-size: 14px;width: 100%;background-color:
#f6f6f6;" bgcolor="#f6f6f6">
 <tbody>
```

```
  <tr style="font-size: 14px;">

   <td style="font-size: 14px;vertical-align: top;"></td>

   <td class="container" width="600" style="font-size: 14px;vertical-align: top;">

    <div class="content" style="font-size: 14px;">

     <table class="main" width="100%" cellpadding="0" cellspacing="0" style="font-size: 14px;background-color: #fff;" bgcolor="#fff">

      <tbody>

       <tr style="font-size: 14px;">

        <td class="alert alert-warning" style="font-size: 16px;vertical-align: top;color: #fff;text-align: center;background-color: #0065E3;text-align: center;" bgcolor="#0065E3">Ticket merged</td>

       </tr>

       <tr style="font-size: 14px;">

        <td class="content-wrap" style="font-size: 14px;vertical-align: top;">

         <table width="100%" cellpadding="0" cellspacing="0" style="font-size: 14px;">

          <tbody>

           <tr style="font-size: 14px;">

            <td class="content-block" style="font-size: 14px;vertical-align: top;">Your ticket with reference number: [REF]</td>

           </tr>

           <tr style="font-size: 14px;">

            <td class="content-block" style="font-size: 14px;vertical-align: top;">Has been merged into ticket number: [MERGETARGETTICKETNUMBER]</td>

           </tr>

          </tbody>

         </table>

        </td>

       </tr>

      </tbody>

     </table>

     <div class="footer" style="font-size: 14px;width: 100%;color: #999;"></div>

   </div>

  </td>
  <td style="font-size: 14px;vertical-align: top;"></td>
  </tr>
 </tbody>
</table>
```

Defining activities for time tracking

Activities are used for time registrations, which, in turn, help you to understand your timesheets. For example, you can see how much time employees spend on client-related vs non client-related activities, and how much time they spend on billable vs non-billable work.

In more specific cases, for client-related billable activities you can apply specific rates, so that they are automatically applied during a time registration. For example, a unique, more expensive rate can be automatically applied to a time registration for a customer on-site visit.

The **Activities** screen displays a list of current activities. You can add to and edit the listed activities, and activate or deactivate an activity (by clicking the **Status** toggle switch), as required. Deactivating an activity removes it from the list in the **Activities** screen and from the time registration it was added to.

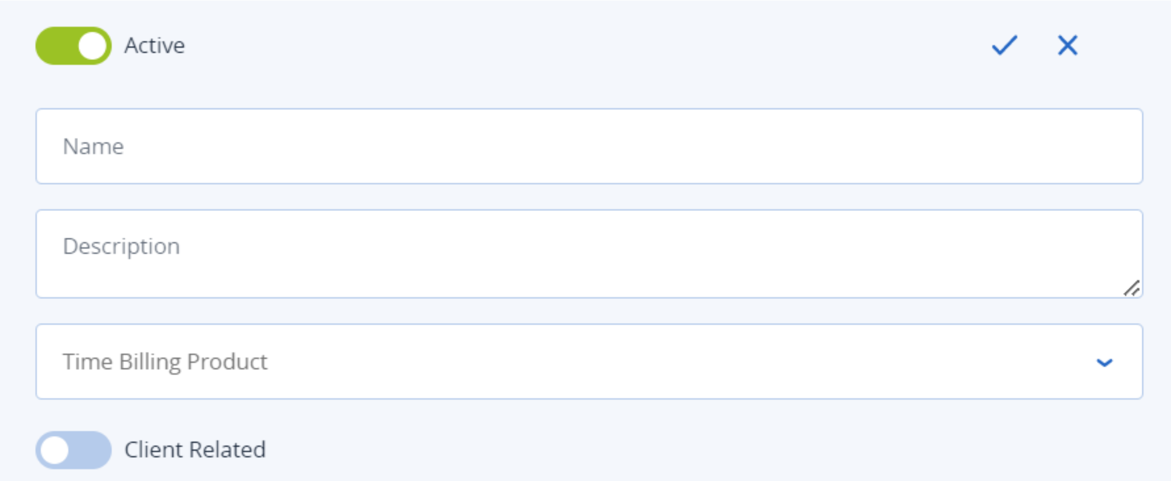
Note that Advanced Automation (PSA) comes with the following predefined activities by default:

- Bookkeeping
- Contract management
- Lunch break
- Project engineering
- Project management

Creating an activity

To create an activity

1. Go to **Settings** > **Service desk**, and then select **Activities**.
2. Click **Add new**.
   A new section is shown at the top of the Activities list.



3. Do the following:
   - Click the **Active** toggle switch to enable the activity (selected by default).
   - Enter a name for the activity, up to a maximum of 50 characters.
   - Enter a description for the activity. This is displayed in the main list of activities shown in the **Activities** screen.
   - Select the relevant product from the **Time Billing Product** drop-down list. When the selected product is used in a contract or sales item, the invoicing process uses its billing rate when the time registration (which includes the relevant activity) is invoiced.
   - Click the **Client related** toggle switch to enable it. When enabled, this activity's time will be shown as client-related in the Timesheet report. When disabled, this activity's time will be shown as internal in the Timesheet report.
4. Click ✓ to save the activity.

   The activity is now available for use in tracking timed activities. For example, when you define a new time registration you can select the relevant activity to assign to the time registration from the **Activity** field, such as *Project management* or *Lunch break*.

Editing an activity

All activities, including the predefined activities that come with Advanced Automation (PSA), are editable. You can also deactivate an activity, but you cannot delete an activity.

To edit an activity

1. Go to **Settings** > **Service desk**, and then select **Activities**.
2. Click the pencil icon for the relevant activity.
3. Make the changes you want to the activity. For more details, see "Creating an activity" (p. 323).

   You can deactivate the activity by clicking the **Active** toggle switch. This will remove it from the list of activities in the **Activities** screen, and from any time registrations that it was added to.
4. Click ✓ to save your changes.

Viewing configuration items

Configuration Items are assets (customer devices) managed by an external RMM platform that are automatically imported into Advanced Automation (PSA). You can view the details of these configuration items, and also link them to specific users, in the **Service desk** settings.

Note
Synchronization between customer sites and devices and the RMM software may take up to 15 minutes. For example, a new device set up in the RMM platform will become visible in Advanced Automation (PSA) within 15 minutes. All changes are updated in the Advanced Automation (PSA) database.

To view configuration items

1. Go to **Settings** > **Service desk**, and then select **Configuration items**.
2. Click on the relevant configuration item row. The following read-only details about the configuration item are displayed in the right pane:
   - Device name
   - RMM integration
   - Customer's site name
   - Description
   - Location
3. To link the configuration item to a specific user, click **Link to user** in the relevant row. Then select the relevant user from the drop-down list, and click **Link**. The configuration item is now linked to the selected user, meaning that any new service desk tickets created by or assigned to the user are automatically linked to the configuration item.

   To unlink a user from a configuration item, click **Link to user** in the relevant row, and in the displayed right pane, click **Unlink**.

Setting the default project billing entity

Advanced Automation (PSA) enables you to create multiple billing entities. This means that you can bill from multiple businesses, and each billing entity will have its own invoice settings, background, and so on. In the **Project management** screen of the service desk settings, you can set the default billling entity for sales items created for project billing.

To set the default project billing entity

1. Go to **Settings > Service desk**, and then select **Project management**.
2. Click **Edit**, and then select the relevant billing entity.
3. Click **Save**.

Billing and quoting settings

Advanced Automation (PSA) enables you to fully customize your billing. You can set the layout, the default export format (if you then need to import into another system), and much more. You can customize the look and feel, set up an address, text margins, and add a background image of your choice.

In this section, you can also set up the taxes to use in Advanced Automation (PSA), and define your integration with your preferred accounting software (see "Integrating with accounting platforms" (p. 333)).

To access billing and quoting settings, go to **Settings > Billing and quoting**.

Billing settings

This section describes how to configure default billing and invoicing settings, including customizing the look and feel of your invoices.

Defining your default billing settings

This section describes how to setup your billing and define default settings, including time registration roundup times, and the default tax to use in invoices. These settings are used as the defaults in sales items, invoices, and contracts.

Note that you cannot deactivate a product that is set as the default product in billing settings. When set as the default product, the **Active** checkbox is disabled in the product's settings. For more information, see "Adding a product" (p. 273).

To configure your billing settings

1. In the management portal, go to **Settings > Billing and quoting**. The **Billing settings** screen is displayed by default.
2. Click the pencil icon, and modify any of the following default settings:
   - **Time registration roundup**: Set the time (in minutes) of your ticket roundup time. When ticket work is approved for billing, the total billable hours will be rounded up according to this value. For example, if you set the roundup time value to 15 minutes, 7 minutes of ticket work will be rounded up to 15 before invoicing. Likewise, 21 minutes will be rounded up to 30, and 36 minutes will be rounded to 45, and so on. The default value is **10**.
   - **Roundup time for outside business hours**. Set the roundup time of tickets outside, for example, 08:00 to 17:00, which are common business hours. The default value is **20**.
   - **Discard tickets for approval with a time equal to or less than the threshold set below**: Enable the toggle switch if you want to discard tickets that do meet your minimum threshold. Define the relevant threshold value in the **Threshold value (in minutes)** field.
   - **Number of days until the ticket is automatically closed**: Set how many days the system waits before it closes a completed ticket. By default, this is set to **1**.

Note

Engineers can only set completed tickets to a status of **Completed**. After the set number of days have elapsed, the tickets close automatically. This ensures that when you complete a ticket and an email is sent to the customer, you often get a 'thank you' reply from them. However, this reply would reopen the ticket and impact your 'reopened tickets' statistics, forcing you to re-close the ticket. This auto-close functionality helps manage this issue. To disable this function, set the value to **0**.

- **Default bookkeeping software**: Select the relevant software from the list of available integrated accounting platforms (see "Integrating with accounting platforms" (p. 333)).
- **Default product ledger for export invoice**: Select the default product ledger number to be used for export invoices (the default is **400**). The product ledgers displayed in the list are the current ledger numbers available (see "Managing ledgers" (p. 288)).

Note

When invoices are exported to your accounting software, they are typically exported as a piece of general information (company, customer, totals) with information about invoice lines (product, description, ledger, quantity, price, total, tax, and so on). This field defines what ledger number will be used by default for a product if it does not have a ledger assigned in its product settings.

- **Default product for ticket time billing**: Select the default product to be used for ticket time billing. By default, this is set to **Support per hour**.
- **Default product for outside business hours**: Select the default product to be used for all billings set for outside business hours. By default, this is set to **Support outside of business hours**.
- **Default billing product for block hours**: If you offer block hours to customers, select the default product to be used for block hours. By default, this is set to **Block hours**.
- **Default sales tax**: Select the default sales tax you want to use from the list of available taxes (see "Tax settings" (p. 332)). By default, this is set to **Default tax**.
- **Send invoices by**: Select the default method for sending invoices. By default, this is set to **Mail**. This field is automatically applied:
  - When creating a customer.
  - In the **Billing information** tab, when defining billing information for customers with no billing information defined (for example, if the customer already existed before Advanced Automation (PSA) was activated).
  - In the **Billing information** tab, when creating a quote, contract, sales item or project for customers with no billing information defined (for example, if the customer already existed before Advanced Automation (PSA) was activated).
  - When manually creating a new contract or sales item (the **Send invoices by** field's selected value is taken from the customer's defined billing information - if no billing information is defined, the default **Mail** value is applied).

  The **Send invoices by** field is also set in your default quote settings, and is applied when creating a contract or sales item by accepting a quote. This is the only time the **Send invoices by** field is applied other than from the default billing settings, or from the customer's billing settings. For more information, see "Defining default quote settings" (p. 330).

  - **Default billing entity**: The default billing entity used for invoices. By default, **Default billing entity** is selected.

3. Click ✓ to apply your changes.

Adding a new billing entity

Billing entities enable you to send invoices from different legal entities that are part of your business. A default billing entity was created when your account was created. You can also update the details of this billing entity, if this is the only entity you need.

Note
Only users with the Administrator or Director roles can create or update billing entities.

To add a new billing entity

1. In the management portal, go to **Settings** > **Billing and quoting**, and then select **Billing entities**.

   The current billing entity is listed.
2. Click **+ New billing entities**.
3. Define the following:
   - **Company name**: Enter the company name.
   - **Bank account number**: Enter the relevant bank account number for this entity.
   - **Invoice start number**: Enter the starting number of the invoices once you start sending invoices to customers.
   - **Invoice serial number**: This option allows you to keep the same invoice number range if you switch to Advanced Automation (PSA) in the middle of a fiscal year.
4. (Optional) Enable the **Reset invoice numbering** toggle switch. This will reset your invoice numbers to the number you set in the **Invoice start number** field.
5. Enable the **Active** toggle switch to activate the new billing entity.
6. Click **Create**. The billing entity is added to the **Billing entities** screen, and can be selected when generating invoices (see "Generating a new invoice" (p. 268)), and creating sales items (see "Creating a new sales item" (p. 258)) and contracts (see "Creating a new contract" (p. 261)).

   You can update a billing entity as required. Click on the relevant billing entity in the **Billing entities** screen and edit as required. Note that you cannot delete a billing entity.

Customizing the look and feel of invoices

You can fully customize the layout of your invoices and quotes that you send to customers. You can upload your own background image, set your invoice footer text, and set margins for the texts that Advanced Automation (PSA) adds.

You can use a background image to include details such as your company logo, address, website and email addresses on your invoices.

Note

If you want to start your invoice customization from scratch, you can download an empty template image here. If you already have an invoice layout in PDF, you can convert it to JPG in high-resolution using third party online tools.

To customize your invoice

1. In the management portal, go to **Settings** > **Billing and quoting**, and then select **Invoice settings**.
2. Click the pencil icon to modify any of the following settings:
   - **Invoice background image**: Drag an image file into the displayed box or click **Browse** to upload your image. The image file should be an A4 size JPEG with a maximum size of 1MB.
   - **Invoice footer text for direct debit**: Change the footer text for direct debit as required. For example, using the variables available in Advanced Automation (PSA) (see below), your footer text for invoices set with a direct debit could read as follows:

     "Direct debit with bank account: [BANK_ACCOUNT_NUMBER], customer name > [CUSTOMER_NAME] and VAT number = [VAT_NUMBER]"

     This enables customers to pay invoices via wire transfer or by using one of the payment integrations (PayPal, Stripe). They can also send the invoice to their local bank for direct debit processing.

     The variables available for direct debit invoices are:
     - [BANK_ACCOUNT_NUMBER]
     - [CUSTOMER_NAME]
     - [VAT_NUMBER]
     - [INVOICE_NUMBER]
     - [INVOICE_DUE_DAYS]
   - **Invoice footer text for manual payment**: Edit the invoice footer text of your manual payment. For example, the invoice footer text of a manual payment can be as follows (assuming the invoice due days is set to 15 and invoice number is 2022020107): "15-2022020107"
   - **Invoice due days**: Enter the relevant number of days.
   - **Hide invoice number prefix**: Enable the toggle switch if you want to hide the invoice number prefix.
   - **Contract period billable in advance (days)**: Enter the relevant number of days.
   - **Invoice address position**: Select **Left** or **Right**.

     Note

     Before changing the position of your invoice address, make sure your company logo does not overlap.

- **Margin top**: Enter a value for the space between your company address and the top of the invoice document.

  Note
  All margin values are in centimeters.

- **Margin top for page 2 onwards**: Enter a value for the space between your company address and the top of the invoice document, from page 2 onwards.
- **Margin side**: Enter a value for the space from the left of the invoice document.
- **Address bottom margin**: Enter a value for the space between your company address and the date and invoice number details of the invoice document.
- **Page bottom margin**: Enter a value for the space between the page number and the bottom of the invoice document.
- **Page number position**: Select **Top** or **Bottom**.
- **Page number visibility**: Select from **Display on all pages**, **Hide for first page**, or **Hide it completely**.

3. Click **Download preview** to see a preview of the invoice in PDF format.
4. When done, click ✓.

   When an invoice is generated, the invoice footer is applied automatically, depending on the defined payment method option:

   - When direct debit is selected, the **Invoice footer text for direct debit** option is used.
   - If direct debit is not selected, the **Invoice footer text for manual payment** option is used.

Quoting settings

This section describes how to configure default quoting settings, including customizing the look and feel of the quote PDF which is sent to customers.

Defining default quote settings

When a quote is approved, Advanced Automation (PSA) automatically creates the following:

- A purchase order ticket for items that first need to be purchased (for example, via a distributor). Note that if an item is already in stock no purchase order ticket will be created.
- A quote ticket to deliver and bill quote items for the customer.

The default quote settings define which support groups each of the above ticket types should be automatically assigned to when they are created. You can also define other quote settings, such as the default category and default payment method for sales items.

To define default quote settings

1. In Management Portal, go to **Settings** > **Billing and quoting**, and then select **Quote settings**.
2. Click the pencil icon, and modify any of the following default settings:
   - **Group for purchase order tickets**: Select the relevant support group from the dropdown list.

- **Group for quote tickets**: Select the relevant support group from the dropdown list.
- **SLA for quote tickets**: Select the relevant SLA from the dropdown list.
- **Priority for quote tickets**: Select the relevant priority from the dropdown list.
- **Category for quote tickets**: Select the relevant category from the dropdown list.
- **Billing entity**: Select the relevant billing entity from the dropdown list.
- **Send invoices by**: Select from **Mail** or **Email**. By default, this is set to **Mail**.

  The **Send invoices by** field is applied when creating a contract or sales item by accepting a quote. This is the only time the **Send invoices by** field is applied other than from the default billing settings, or from the customer's billing settings.
- **Sales items payment method**: Select from **Manual payment** or **Direct debit**.
- **General conditions**: Add your own general conditions to all quotes. For example, any specific legal terms you want to include.

3. Click ✓ to apply your changes.

Customizing the look and feel of quote PDFs

This section describes how you can customize the default look and feel of the quote PDFs that are sent to customers. You can upload your own background image, set your quote footer text, and set the margins for the text that Advanced Automation (PSA) adds automatically. Optionally, you can use a background image to include these items on your quotes:

- Company logo
- Address details
- Bank account number
- Website and email address
- VAT number

Note

If you want to start your quote customization from scratch, you can download an empty template image here. If you already have a quote layout in PDF, you can convert it to JPG in high-resolution using third party online tools.

To customize quote PDFs

1. In Management Portal, go to **Settings** > **Billing and quoting**, and then select **Quote PDF settings**.
2. Click the pencil icon, and modify any of the following default settings:
   - **Quote PDF background image**: Drag an image file into the displayed box or click **Drop or select file to upload** to upload your image. The image file should be an A4 size JPEG with a maximum size of 1MB.
   - **Margin top**: Enter a value for the space between your company address and the top of the quote document.

Note

All margin values are in centimeters.

- **Margin top for page 2 and further**: Enter a value for the space between your company address and the top of the quote document, from page 2 onwards.
- **Margin side**: Enter a value for the space from the left of the quote document.
- **Address bottom margin**: Enter a value for the space between your company address and the date and quote number details of the quote document.
- **Page bottom margin**: Enter a value for the space between the page number and the bottom of the quote document.
- **Page number position**: Select **Top** or **Bottom**.
- **Page number visibility**: Select from **Display on all pages**, **Hide for first page**, or **Hide it completely**.

3. Click **Download preview** to see a preview of the quote PDF.
4. When done, click ✓ .

Tax settings

This section describes how to configure default tax settings for use in your invoices for customers. Taxes are applied to an invoice depending on your location and products sold.

Adding a tax

To add a tax

1. In the management portal, go to **Settings** > **Billing and quoting**, and then select **Taxes**.
2. Click **+ Add new**.
3. Enter the tax code, tax name, and set its value. By default, the tax is set as active.
4. Click ✓ to save the new tax.

   The new tax is added to the **Taxes** screen.

Editing a tax

You can edit a tax at any time, and activate/deactivate a tax as required. You can also delete a tax.

To edit a tax

1. In Management Portal, go to **Settings** > **Billing and quoting**, and then select **Taxes**.
2. Click the pencil icon of the tax you want to edit, and then modify as required.

   You can click the toggle switch to activate or deactivate the tax.

> **Note**
> To delete a tax, click on the trash can icon. Note that you cannot delete a tax if it is already assigned in the system (for example, as a sales tax).

3. Click ✓ to apply your changes.

Integrating Advanced Automation (PSA) with third party platforms

Advanced Automation (PSA) can integrate with some of the most popular accounting platforms, RMM tools, VAR, and payment platforms.

The following integrations are currently supported:

- **Accounting integrations**: FreshBooks, QuickBooks, Sage, Xero, and SnelStart
- **RMM integrations**: NinjaOne, Datto RMM, Kaseya VSA, N-able N-central, and N-able RMM
- **VAR integrations**: Microsoft CSP
- **Payment integrations**: PayPal and Stripe

To access your integrations, in the management portal go to **Integrations**.

> **Note**
> This functionality is only available for users assigned the Administrator role.

Integrating with accounting platforms

Advanced Automation (PSA) enables you to integrate with some of the most popular accounting platforms. These integrations automate the following functionality:

- Initial data import

  This functionality enables you to avoid initial routine data transfers from your accounting platform to the Acronis Cyber Protect Cloud platform and import key business data for further client billing with Advanced Automation (PSA). This key data includes customers, products, taxes, and ledgers.

- Invoice data export

  Every new invoice generated in Advanced Automation (PSA) is exported to your accounting platform automatically with no manual actions required.

Note that if the current supported integrations are incompatible with your platform, Advanced Automation (PSA) enables you to deliver invoices to your accounting software via CSV or XML files.

To access the accounting integrations, go to **Integrations**. In the displayed left menu, select **Automation** > **Accounting and Finance**.

Integrating with FreshBooks

This topic describes how to integrate FreshBooks with Advanced Automation (PSA).

For information about additional accounting platforms that integrate with Advanced Automation (PSA), see "Integrating with accounting platforms" (p. 333).

Note
When accessing the management portal using a custom web interface URL, integration with FreshBooks should only be enabled when you are signed-in via the default management portal URL (https://cloud.acronis.com). For more information about branding and custom web interface URLs, see "Configuring custom web interface URLs" (p. 96).

To integrate FreshBooks with Advanced Automation (PSA)

1. Go to **Integrations**, and then select **Automation** > **Accounting and Finance**.
2. On the FreshBooks tile, click **Configure**, and then click **Activate**. You are then prompted to activate the authentication process, where you are redirected to the FreshBooks login page.
3. Enter your FreshBooks account credentials to enable the integration.
4. Select the data you want to import from FreshBooks (Customers, Ledgers, Products, and Taxes), and click **Import**.

   Note that once the initial integration is complete, every time you click **Import** only new Customers, Ledgers, Products, and Taxes will be imported.
5. Click **Save** to save your integration settings.

   Note
   When the integration is enabled, Advanced Automation (PSA) automatically checks for new invoices every few minutes, and synchronizes them with FreshBooks. The synchronization status can be viewed in the **Invoice sync status** column in the **Invoices** screen (go to **Sales and billing > Invoices**).

To modify your FreshBooks integration settings

1. Go to **Integrations**, and then click the **Integrations in use** tab.
2. On the FreshBooks tile, click **Manage**.
3. Modify the settings as required (see above).

To deactivate your FreshBooks integration

1. Go to **Integrations**, and then click the **Integrations in use** tab.
2. On the FreshBooks tile, click **Deactivate**.
3. In the displayed confirmation message, click **Delete**.

Integrating with QuickBooks

This topic describes how to integrate QuickBooks Online with Advanced Automation (PSA).

For information about additional accounting platforms that integrate with Advanced Automation (PSA), see "Integrating with accounting platforms" (p. 333).

Note

When accessing the management portal using a custom web interface URL, integration with QuickBooks should only be enabled when you are signed-in via the default management portal URL (https://cloud.acronis.com). For more information about branding and custom web interface URLs, see "Configuring custom web interface URLs" (p. 96).

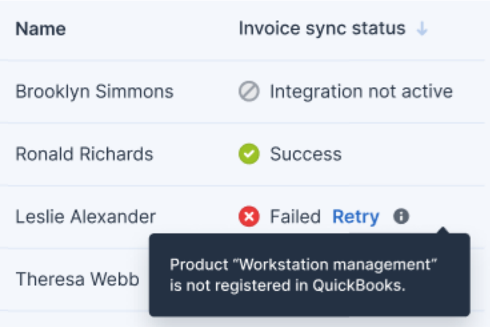
To integrate QuickBooks with Advanced Automation (PSA)

1. Go to **Integrations**, and then select **Automation** > **Accounting and Finance**.
2. On the QuickBooks tile, click **Configure**, and then click **Activate**. You are then prompted to activate the authentication process, where you are redirected to the QuickBooks login page.
3. Enter your QuickBooks account credentials to enable the integration.
4. Select the data you want to import from QuickBooks (Customers, Ledgers, Products, and Taxes), and click **Import**.

   Note that once the initial integration is complete, every time you click **Import** only new Customers, Ledgers, Products, and Taxes will be imported.
5. Click **Save** to save your integration settings.

   Note

   When the integration is active, Advanced Automation (PSA) automatically checks for new invoices every few minutes, and synchronizes them with QuickBooks. The synchronization status can be viewed in the **Invoice sync status** column in the **Invoices** screen (go to **Sales and billing > Invoices**).



Name	Invoice sync status ↓
Brooklyn Simmons	⊘ Integration not active
Ronald Richards	✓ Success
Leslie Alexander	☒ Failed Retry ⓘ
Theresa Webb	

Product "Workstation management" is not registered in QuickBooks.

To modify your QuickBooks integration settings

1. Go to **Integrations**, and then click the **Integrations in use** tab.
2. On the QuickBooks tile, click **Manage**.
3. Modify the settings as required (see above).

To deactivate your QuickBooks integration

1. Go to **Integrations**, and then click the **Integrations in use** tab.
2. On the QuickBooks tile, click **Deactivate**.

3. In the displayed confirmation message, click **Delete**.

Integrating with Sage Business Cloud

This topic describes how to integrate Sage Business Cloud with Advanced Automation (PSA).

Note that Advanced Automation (PSA) currently supports Sage Accounting only.

For information about additional accounting platforms that integrate with Advanced Automation (PSA), see "Integrating with accounting platforms" (p. 333).

Note
When accessing the management portal using a custom web interface URL, integration with Sage Business Cloud should only be enabled when you are signed-in via the default management portal URL (https://cloud.acronis.com). For more information about branding and custom web interface URLs, see "Configuring custom web interface URLs" (p. 96).

To integrate Sage Business Cloud with Advanced Automation (PSA)

1. Go to **Integrations**, and then click **Automation** > **Accounting and Finance**.
2. On the Sage Business Cloud tile, click **Configure**, and then click **Activate**.
   You are then prompted to activate the authentication process, where you are redirected to the Sage Business Cloud login page.
3. Enter your Sage Business Cloud account credentials to enable the integration.

   Note
   When the integration is enabled, Advanced Automation (PSA) automatically checks for new invoices every few minutes, and synchronizes them with Sage Business Cloud. The synchronization status can be viewed in the **Invoice sync status** column in the **Invoices** screen (go to **Sales and billing > Invoices**).

   In addition, unit prices in Sage Business Cloud invoice line items can only have up to two digits after the decimal separator. Other accounting platforms typically support four digits after the decimal separator. Prices are automatically rounded up in Advanced Automation (PSA) to two digits after the decimal separator and then synced with Sage Business Cloud. No configuration is required by the user.

4. Select the data you want to import from Sage Business Cloud (Customers, Ledgers, Products, and Taxes), and click **Import**.
   Note that once the initial integration is complete, every time you click **Import** only new Customers, Ledgers, Products, and Taxes will be imported.
5. Click **Save** to save your integration settings.

To modify your Sage Business Cloud integration settings

1. Go to **Integrations**, and then click the **Integrations in use** tab.
2. On the Sage Business Cloud tile, click **Manage**.

3. Modify the settings as required (see above).

To deactivate your Sage Business Cloud integration

1. Go to **Integrations**, and then click the **Integrations in use** tab.
2. On the Sage Business Cloud tile, click **Deactivate**.
3. In the displayed confirmation message, click **Delete**.

Integrating with Xero

This topic describes how to integrate Xero with Advanced Automation (PSA).

For information about additional accounting platforms that integrate with Advanced Automation (PSA), see "Integrating with accounting platforms" (p. 333).

Note
When accessing the management portal using a custom web interface URL, integration with Xero should only be enabled when you are signed-in via the default management portal URL (https://cloud.acronis.com). For more information about branding and custom web interface URLs, see "Configuring custom web interface URLs" (p. 96).

To integrate Xero with Advanced Automation (PSA)

1. Go to **Integrations**, and then select **Automation** > **Accounting and Finance**.
2. On the Xero tile, click **Configure**, and then click **Activate**. You are then prompted to activate the authentication process, where you are redirected to the Xero login page.
3. Enter your Xero account credentials to enable the integration.
4. Select the data you want to import from Xero (Customers, Ledgers, Products, and Taxes), and click **Import**.

   Note that once the initial integration is complete, every time you click **Import** only new Customers, Ledgers, Products, and Taxes will be imported.
5. Click **Save** to save your integration settings.

   Note
   When the integration is enabled, Advanced Automation (PSA) automatically checks for new invoices every few minutes, and synchronizes them with Xero. The synchronization status can be viewed in the **Invoice sync status** column in the **Invoices** screen (go to **Sales and billing > Invoices**).

To modify your Xero integration settings

1. Go to **Integrations**, and then click the **Integrations in use** tab.
2. On the Xero tile, click **Manage**.
3. Modify the settings as required (see above).

To deactivate your Xero integration

1. Go to **Integrations**, and then click the **Integrations in use** tab.
2. On the Xero tile, click **Deactivate**.
3. In the displayed confirmation message, click **Delete**.

Integrating with SnelStart

This topic describes how to integrate SnelStart with Advanced Automation (PSA).

For information about additional accounting platforms that integrate with Advanced Automation (PSA), see "Integrating with accounting platforms" (p. 333).

Note
When accessing the management portal using a custom web interface URL, integration with SnelStart should only be enabled when you are signed-in via the default management portal URL (https://cloud.acronis.com). For more information about branding and custom web interface URLs, see "Configuring custom web interface URLs" (p. 96).

To integrate SnelStart with Advanced Automation (PSA)

1. Go to **Integrations**, and then select **Automation** > **Accounting and Finance**.
2. On the SnelStart tile, click **Configure**, and then click **Activate**.
   You are then prompted to activate the authentication process, where you are redirected to the SnelStart login page.
3. Enter your SnelStart account credentials to enable the integration.
4. Select the data you want to import from SnelStart (Customers, Ledgers, Products, and Taxes), and click **Import**.

   Note that once the initial integration is complete, every time you click **Import** only new Customers, Ledgers, Products, and Taxes will be imported.
5. Click **Save** to save your integration settings.

   Note
   When the integration is enabled, Advanced Automation (PSA) automatically checks for new invoices every few minutes, and synchronizes them with SnelStart. The synchronization status can be viewed in the **Invoice sync status** column in the **Invoices** screen (go to **Sales and billing > Invoices**).

To modify your SnelStart integration settings

1. Go to **Integrations**, and then click the **Integrations in use** tab.
2. On the SnelStart tile, click **Manage**.
3. Modify the settings as required (see above).

To deactivate your SnelStart integration

1. Go to **Integrations**, and then click the **Integrations in use** tab.
2. On the SnelStart tile, click **Deactivate**.

3. In the displayed confirmation message, click **Delete**.

Note
When deactivated, Advanced Automation (PSA) still keeps all the Customers, Ledgers, Products and Taxes, so you can still continue to use them. However, new invoices in Advanced Automation (PSA) will no longer be synchronized with the accounting platform.

Resolving issues with your accounting platform integration

When Advanced Automation (PSA) sends an invoice to an accounting platform, the accounting platform typically expects to receive the following mandatory mapping codes to match data between the two systems (Cyber Protect Cloud and the accounting platform):

- A customer's "External ID", which should match with a customer tenant, and confirms the link between a new invoice and the correct customer.
- A product's "External ID", which should match with a product from an invoice line, and confirms the link between the invoice line and the correct product.

When importing customers and products from accounting platforms, these mapping codes are set automatically in Cyber Protect Cloud. They can be viewed in the management portal and updated manually, if required.

Mismatches in the mapping codes between the two systems is typically a result of manual changes, and can result in the failure to deliver an invoice to the accounting platform.

Invoice troubleshooting

The status of failed invoice exports can be viewed by navigating to **Sales and billing > Invoices**, and then viewing the **Invoice sync status** value in the relevant invoice line. A message is displayed from the accounting platform indicating the exact reason for the failure.

If the error message is related to a failure in recognizing a customer or product, the problem is typically due to empty or incorrect mapping codes for a customer or product in Cyber Protect Cloud.

For more information about Advanced Automation (PSA) and synchronization with third party accounting platforms, see this knowledge base article.

Integrating with RMM platforms

Advanced Automation (PSA) enables you to integrate with RMM (Remote Monitoring and Management) platforms. This enables you to automate ticket creation and management and align customer billing with managed customer assets.

To access the RMM integrations, go to **Integrations**. In the displayed left menu, select **Management** > **Remote Monitoring and Management**.

Note that when setting up your integration, ensure your RMM software remains open as you will need its URL and keys to complete the integration.

Integrating with NinjaOne

By integrating Advanced Automation (PSA) with NinjaOne, you can:

- Automatically import customer sites and devices from NinjaOne.
- Map customers to sites from NinjaOne.
- Create tickets from NinjaOne alerts.
- Access the NinjaOne device page from a ticket.
- Bill customers for the actual number of devices from NinjaOne.

NinjaOne supports OAuth 2.0 authentication, which is applicable for all new integrations. If you have an integration that was set up with an Access Key ID and Secret Access Key, it needs to be updated manually.

Note
In order to successfully integrate NinjaOne with Advanced Automation (PSA), the Advanced Automation (PSA) service must be enabled. You must also have a fully configured NinjaOne account.

Setting up the NinjaOne integration

There are two main steps in setting up your NinjaOne integration with Advanced Automation (PSA), as described in the procedures below:

1. Defining the integration settings to connect with the NinjaOne instance.
2. Mapping NinjaOne customers to Advanced Automation (PSA).

To define integration settings

1. In Management Portal, go to **Integrations**, and then select **Management** > **Remote Monitoring and Management**.
2. On the **NinjaOne** tile, click **Configure**.
3. Enter the relevant NinjaOne credentials to access the NinjaOne instance. For more information, see here.

   Note
   NinjaOne supports OAuth 2.0 authentication, which is applicable for all new integrations. If you have an integration that was set up with an Access Key ID and Secret Access Key, it needs to be updated manually.

4. After the credentials have been defined, the next step in setting up your integration is to map the NinjaOne customers with existing or new Advanced Automation (PSA) customers, as described below.

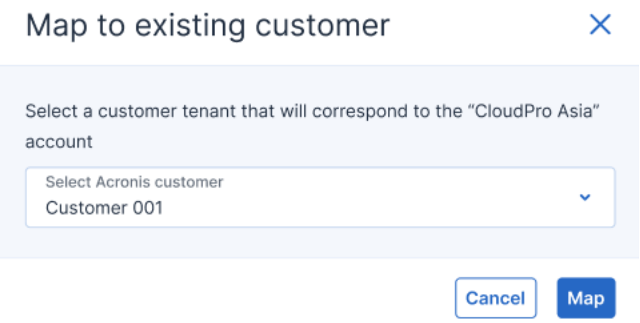
To map NinjaOne customers

1. In the management portal, go to **Integrations**, and then select **Management** > **Remote Monitoring and Management**.

2. On the **NinjaOne** tile, click **Configure**.
3. In the **Customer mapping** tab, click **Create Acronis customers from NinjaOne sites**. The mapping process is started for all the listed NinjaOne sites.

   All customers (customer sites) from NinjaOne are registered as new customers in Management Portal, complete with all available services granted.

   You can also select individual NinjaOne sites and map them to existing Management Portal customers; select the relevant site(s), and then click **Map to existing customer tenant**. You are then prompted to select an existing customer. Once selected, click **Map** to complete the mapping process.

   Map to existing customer

   Select a customer tenant that will correspond to the “CloudPro Asia” account

   Select Acronis customer: Customer 001

4. When complete, the **Mapping** column displays **Mapped**, and the **Acronis customer** column displays the relevant customer name.

> **Note**
> To remove a mapping, select the relevant row that is currently mapped, and then click **Remove mapping**. In the displayed confirmation popup, click **Remove**.

Reviewing and editing NinjaOne integration settings

You can review and edit your NinjaOne integration settings, as required. You can also deactivate the NinjaOne integration.

To review and edit NinjaOne integration settings

1. In Management Portal, go to **Integrations**, and then click the **Integrations in use** tab.

   On the **NinjaOne** tile, you can view the current status of the integration.
2. Click **Manage** to view and edit integration settings.

   For example, you can view and edit credentials and alert settings in the **Integration settings** tab, and NinjaOne customers mapped to Advanced Automation (PSA) in the **Customer mapping** tab.
3. Click the pencil icon to edit the relevant section. For more information about the editable fields, see "Setting up the NinjaOne integration" (p. 340).
4. When done, click ✓.

To deactivate the NinjaOne integration

1. Go to **Integrations**, and then click the **Integrations in use** tab.
2. On the **NinjaOne** tile, click **Deactivate**.
3. In the displayed confirmation message, click **Delete**.

Creating tickets from NinjaOne open alerts

When integration with NinjaOne is configured (see "Setting up the NinjaOne integration" (p. 340)), Advanced Automation (PSA) automatically creates new tickets from NinjaOne open alerts. Tickets are kept in sync with NinjaOne, ensuring that open alerts already linked with tickets in Advanced Automation (PSA) are ignored.

Note the following:

- Tickets are only created for customers that are mapped to NinjaOne customer sites.
- Ticket parameters are defined with the default settings for the relevant customer (as described in "Setting default values" (p. 294)).
- The ticket summary and description is taken from the alert's summary and description.
- The ticket includes links to the Management Portal customer, the customer user (via the user's email address, if provided by NinjaOne), and devices linked to the user (if relevant; devices can be viewed by users in the Cyber Protect console).
- If a ticket is linked to a user's device, a link is included to the Device Information section in NinjaOne.

For more information about creating a ticket, see "Creating a new ticket" (p. 208).

Adding external NinjaOne devices to contracts

When integration with NinjaOne is configured (see "Setting up the NinjaOne integration" (p. 340)), you can add external devices to contracts for customers in Advanced Automation (PSA).

- You can link a specific contract part to the NinjaOne integration. This is done in the contract parts section of a contract; select the relevant integration, group/site, and workload type, and then select the relevant configuration items.
- In the contract parts section of a contract you can select **Automatic update** to update the device quantity for the contract part.
- You can also select **Show workloads on invoice** to add information about specific devices to customer invoices.

For more information about defining contracts and adding devices to contracts, see "Working with contracts" (p. 261).

Integrating with Datto RMM

By integrating Advanced Automation (PSA) with Datto RMM, you can:

- Automatically import customer sites and devices from Datto RMM.
- Map customers to sites from Datto RMM.
- Create tickets from Datto RMM alerts.

- Access the Datto RMM device page from a ticket.
- Connect remotely to a Datto RMM device from a ticket.
- Bill customers for the actual number of devices using Datto RMM.

Note
In order to successfully integrate Datto RMM with Advanced Automation (PSA), the Advanced Automation (PSA) service must be enabled. You must also have a fully configured Datto RMM account.

Setting up the Datto RMM integration

There are two main steps in setting up your Datto RMM integration with Advanced Automation (PSA), as described in the procedures below:

1. Defining the integration settings to connect with the Datto RMM instance.
2. Mapping Datto RMM customers to Advanced Automation (PSA).

To define integration settings

1. In Management Portal, go to **Integrations**, and then select **Management** > **Remote Monitoring and Management**.
2. On the **Datto RMM** tile, click **Configure**.
3. Enter the following Datto RMM credentials to access the Datto RMM instance:
   - **Datto RMM Server**: Enter the URL of the Datto RMM server.
   - **API Key**: Enter the unique API Key for your Datto RMM account.
   - **API Secret**: Enter the unique API Secret for your Datto RMM account.

     All of the above credentials are created in your Datto RMM account. To generate them, first login to your Datto RMM account. Go to **Setup > Account Settings > Access Control**, and set **Enable API Access** to **ON**. Then click the **Users** tab, and click on the user you want to enable API access for. The copy the displayed URL, API Key, and API Secret.
4. (Optional) Click **Test connection** to test the entered credentials.
5. Click **Next**.
6. If you want Datto RMM alerts to be synchronized to tickets in Advanced Automation (PSA) automatically, ensure the **Create tickets from Datto RMM alerts** check box is selected (it is selected by default).
7. Select the **Ignore muted alerts** check box if you don't want to synchronize Datto RMM alerts that are of the "muted" type. The check box is selected by default.
8. Click **Save**. The next step in setting up your integration is to map the Datto RMM customers with existing or new Advanced Automation (PSA) customers, as described below.

To map Datto RMM customers

1. In Management Portal, go to **Integrations**, and then select **Management** > **Remote Monitoring and Management**.
2. On the **Datto RMM** tile, click **Manage**.

3. In the **Customer mapping** tab, click **Create Acronis customers from Datto RMM sites**. The mapping process is started for all the listed Datto RMM sites.

   All customers (customer sites) from Datto RMM are registered as new customers in Management Portal, complete with all available services granted.

   You can also select individual Datto RMM sites and map them to existing Management Portal customers; select the relevant site(s), and then click **Map to existing customer tenant**. You are then prompted to select an existing customer. Once selected, click **Map** to complete the mapping process.
4. When complete, the **Mapping** column displays **Mapped**, and the **Acronis customer** column displays the relevant customer name.

Note

To remove a mapping, select the relevant row that is currently mapped, and then click **Remove mapping**. In the displayed confirmation popup, click **Remove**.

Reviewing and editing Datto RMM integration settings

You can review and edit your Datto RMM integration settings, as required. You can also deactivate the Datto RMM integration.

To review and edit Datto RMM integration settings

1. In Management Portal, go to **Integrations**, and then click the **Integrations in use** tab.

   On the **Datto RMM** tile, you can view the current status of the integration, and the number of linked accounts.
2. Click **Open integration** to view and edit integration settings.

   For example, you can view and edit credentials and alert settings in the **Integration settings** tab, and Datto RMM customers mapped to Advanced Automation (PSA) in the **Customer mapping** tab.
3. Click the pencil icon to edit the relevant section. For more information about the editable fields, see "Setting up the Datto RMM integration" (p. 343).
4. When done, click ✓.

To deactivate the Datto RMM integration

1. Go to **Integrations**, and then click the **Integrations in use** tab.
2. On the **Datto RMM** tile, click **Deactivate**.
3. In the displayed confirmation message, click **Delete**.

Creating tickets from Datto RMM alerts

When integration with Datto RMM is configured (see "Setting up the Datto RMM integration" (p. 343)), Advanced Automation (PSA) automatically creates new tickets from Datto RMM alerts. Tickets are kept in sync with Datto RMM, ensuring that open alerts already linked with tickets in Advanced Automation (PSA) are ignored.

Note the following:

- Tickets are only created for customers that are mapped to Datto RMM customer sites.
- Ticket parameters are defined with the default settings for the relevant customer (as described in "Setting default values" (p. 294)).
- The ticket summary and description is taken from the alert's summary and description.
- The ticket includes links to the Management Portal customer, the customer user (via the user's email address, if provided by Datto RMM), and devices linked to the user (if relevant; devices can be viewed by users in the Cyber Protect console).
- If a ticket is linked to a user's device, a link is included to the Device Information section in Datto RMM. Additionally, if provided by Datto RMM, a link to initiate a remote connection is included.

For more information about creating a ticket, see "Creating a new ticket" (p. 208).

Adding external Datto RMM devices to contracts

When integration with Datto RMM is configured (see "Setting up the Datto RMM integration" (p. 343)), you can add external devices to contracts for customers in Advanced Automation (PSA).

- You can link a specific contract part to the Datto RMM integration. This is done in the contract parts section of a contract; select the relevant integration, group/site, and workload type, and then select the relevant configuration items.
- In the contract parts section of a contract you can select **Automatic update** to update the device quantity for the contract part.
- You can also select **Show workloads on invoice** to add information about specific devices to customer invoices.

For more information about defining contracts and adding devices to contracts, see "Working with contracts" (p. 261).

Integrating with Kaseya VSA

By integrating Advanced Automation (PSA) with Kaseya VSA using the existing Cyber Protect plug-in, you can:

- Automatically import customer sites and devices from Kaseya VSA.
- Map customers to sites from Kaseya VSA.
- Create tickets from Kaseya VSA alerts.
- Access the Kaseya VSA device page from a ticket.
- Connect remotely to a Kaseya VSA device from a ticket.
- Bill customers for the actual number of devices using Kaseya VSA.

Note
In order to successfully integrate Kaseya VSA with Advanced Automation (PSA), the Advanced Automation (PSA) service must be enabled. For more information about using the existing Cyber Protect plug-in for Kaseya VSA, see this guide.

Integrating with N-able N-central

By integrating Advanced Automation (PSA) with N-able N-central, you can:

- Automatically import customer sites and devices from N-able N-central.
- Map customers to sites from N-able N-central.
- Create tickets from N-able N-central alerts.
- Sync tickets between Advanced Automation (PSA) and N-able N-central.
- Access the N-able N-central device page from a ticket.
- Bill customers for the actual number of devices from N-able N-central.

Note
In order to successfully integrate N-able N-central with Advanced Automation (PSA), the Advanced Automation (PSA) service must be enabled. You must also have a fully configured N-able N-central account.

Setting up the N-able N-central integration

There are two main steps in setting up your N-able N-central integration with Advanced Automation (PSA), as described in the procedures below:

1. Defining the integration settings to connect with the N-able N-central instance.
2. Mapping N-able N-central customers to Advanced Automation (PSA).

To define integration settings

1. In the management portal, go to **Integrations**, and then select **Management** > **Remote Monitoring and Management**.
2. On the **N-able N-central** tile, click **Configure**.
3. Enter the following N-able N-central credentials to access the N-able N-central instance:
   - URL
   - Username
   - Password
4. (Optional) Click **Test connection** to test the entered credentials.
5. Click **Next**.
6. If you want N-able N-central alerts to be synchronized to tickets in Advanced Automation (PSA) automatically, ensure the **Ticket integration** check box is selected (it is selected by default).
7. Click **Save**. The next step in setting up your integration is to map the N-able N-central customers with existing or new Advanced Automation (PSA) customers, as described below.

To map N-able N-central customers

1. In the management portal, go to **Integrations**, and then select **Management** > **Remote Monitoring and Management**.
2. On the **N-able N-central** tile, click **Manage**.

3. In the **Customer mapping** tab, click **Create Acronis customers from N-able N-central sites**.

   The mapping process is started for all the listed N-able N-central sites.

   All customers (customer sites) from N-able N-central are registered as new customers in Management Portal, complete with all available services granted.

   You can also select individual N-able N-central sites and map them to existing Management Portal customers; select the relevant site(s), and then click **Map to existing customer tenant**. You are then prompted to select an existing customer. Once selected, click **Map** to complete the mapping process.
4. When complete, the **Mapping** column displays **Mapped**, and the **Acronis customer** column displays the relevant customer name.

Note

To remove a mapping, select the relevant row that is currently mapped, and then click **Remove mapping**. In the displayed confirmation popup, click **Remove**.

Reviewing and editing N-able N-central integration settings

You can review and edit your N-able N-central integration settings, as required. You can also deactivate the N-able N-central integration.

To review and edit N-able N-central integration settings

1. In Management Portal, go to **Integrations**, and then click the **Integrations in use** tab.

   On the **N-able N-central** tile, you can view the current status of the integration, and the number of linked accounts.
2. Click **Manage** to view and edit integration settings.

   For example, you can view and edit credentials and alert settings in the **Integration settings** tab, and N-able N-central customers mapped to Advanced Automation (PSA) in the **Customer mapping** tab.
3. Click the pencil icon to edit the relevant section. For more information about the editable fields, see "Setting up the N-able N-central integration" (p. 346).
4. When done, click ✓.

To deactivate the N-able N-central integration

1. Go to **Integrations**, and then click the **Integrations in use** tab.
2. On the **N-able N-central** tile, click **Deactivate**.
3. In the displayed confirmation message, click **Delete**.

Creating tickets from N-able N-central alerts

When integration with N-able N-central is configured (see "Setting up the N-able N-central integration" (p. 346)), Advanced Automation (PSA) automatically creates new tickets from N-able N-central alerts. Tickets are kept in sync with N-able N-central, ensuring that open alerts already linked with tickets in Advanced Automation (PSA) are ignored.

Note the following:

- Tickets are only created for customers that are mapped to N-able N-central customer sites.
- Ticket parameters are defined with the default settings for the relevant customer (as described in "Setting default values" (p. 294)).
- The ticket summary and description is taken from the alert's summary and description.
- The ticket includes links to the Management Portal customer, the customer user (via the user's email address, if provided by N-able N-central), and devices linked to the user (if relevant; devices can be viewed by users in the Cyber Protect console).
- If a ticket is linked to a user's device, a link is included to the device information section in N-able N-central.

For more information about creating a ticket, see "Creating a new ticket" (p. 208).

Adding external N-able N-central devices to contracts

When integration with N-able N-central is configured (see "Setting up the N-able N-central integration" (p. 346)), you can add external devices to contracts for customers in Advanced Automation (PSA).

- You can link a specific contract part to the N-able N-central integration. This is done in the contract parts section of a contract; select the relevant integration, group/site, and workload type, and then select the relevant configuration items.
- In the contract parts section of a contract you can select **Automatic update** to update the device quantity for the contract part.
- You can also select **Show workloads on invoice** to add information about specific devices to customer invoices.

For more information about defining contracts and adding devices to contracts, see "Working with contracts" (p. 261).

Integrating with N-able RMM

By integrating Advanced Automation (PSA) with N-able RMM, you can:

- Automatically import customer sites and devices from N-able RMM.
- Map customers to sites from N-able RMM.
- Create tickets from N-able RMM alerts.
- Bill customers for the actual number of devices from N-able RMM.

Note
In order to successfully integrate N-able RMM with Advanced Automation (PSA), the Advanced Automation (PSA) service must be enabled. You must also have a fully configured N-able RMM account.

Setting up the N-able RMM integration

There are two main steps in setting up your N-able RMM integration with Advanced Automation (PSA), as described in the procedures below:

1. Defining the integration settings to connect with the N-able RMM instance.
2. Mapping N-able RMM customers to Advanced Automation (PSA).

To define integration settings

1. In Management Portal, go to **Integrations**, and then select **Management** > **Remote Monitoring and Management**.
2. On the **N-able RMM** tile, click **Configure**.
3. Enter the following N-able RMM credentials to access the N-able RMM instance:
   - URL
   - API key
4. (Optional) Click **Test connection** to test the entered credentials.
5. Click **Next**.
6. If you want N-able RMM alerts to be synchronized to tickets in Advanced Automation (PSA) automatically, ensure the **Ticket integration** check box is selected (it is selected by default).
7. Click **Save**. The next step in setting up your integration is to map the N-able RMM customers with existing or new Advanced Automation (PSA) customers, as described below.

To map N-able RMM customers

1. In Management Portal, go to **Integrations**, and then select **Management** > **Remote Monitoring and Management**.
2. On the **N-able RMM** tile, click **Manage**.
3. In the **Customer mapping** tab, click **Create Acronis customers from N-able RMM sites**. The mapping process is started for all the listed N-able RMM sites.

   All customers (customer sites) from N-able RMM are registered as new customers in Management Portal, complete with all available services granted.

   You can also select individual N-able RMM sites and map them to existing Management Portal customers; select the relevant site(s), and then click **Map to existing customer tenant**. You are then prompted to select an existing customer. Once selected, click **Map** to complete the mapping process.
4. When complete, the **Mapping** column displays **Mapped**, and the **Acronis customer** column displays the relevant customer name.

   Note
   To remove a mapping, select the relevant row that is currently mapped, and then click **Remove mapping**. In the displayed confirmation popup, click **Remove**.

Reviewing and editing N-able RMM integration settings

You can review and edit your N-able RMM integration settings, as required. You can also deactivate the N-able RMM integration.

To review and edit N-able RMM integration settings

1. In Management Portal, go to **Integrations**, and then click the **Integrations in use** tab.

   On the **N-able RMM** tile, you can view the current status of the integration, and the number of linked accounts.
2. Click **Manage** to view and edit integration settings.

   For example, you can view and edit credentials and alert settings in the **Integration settings** tab, and N-able RMM customers mapped to Advanced Automation (PSA) in the **Customer mapping** tab.
3. Click the pencil icon to edit the relevant section. For more information about the editable fields, see "Setting up the N-able RMM integration" (p. 348).
4. When done, click ✓.

To deactivate the N-able RMM integration

1. Go to **Integrations**, and then click the **Integrations in use** tab.
2. On the **N-able RMM** tile, click **Deactivate**.
3. In the displayed confirmation message, click **Delete**.

Creating tickets from N-able RMM alerts

When integration with N-able RMM is configured (see "Setting up the N-able RMM integration" (p. 348)), Advanced Automation (PSA) automatically creates new tickets from N-able RMM alerts. Tickets are kept in sync with N-able RMM, ensuring that open alerts already linked with tickets in Advanced Automation (PSA) are ignored.

Note the following:

- Tickets are only created for customers that are mapped to N-able RMM customer sites.
- Ticket parameters are defined with the default settings for the relevant customer (as described in "Setting default values" (p. 294)).
- The ticket summary and description is taken from the alert's summary and description.
- The ticket includes links to the Management Portal customer, the customer user (via the user's email address, if provided by N-able RMM), and devices linked to the user (if relevant; devices can be viewed by users in the Cyber Protect console).
- If a ticket is linked to a user's device, a link is included to the device information section in N-able RMM.

For more information about creating a ticket, see "Creating a new ticket" (p. 208).

Adding external N-able RMM devices to contracts

When integration with N-able RMM is configured (see "Setting up the N-able RMM integration" (p. 348)), you can add external devices to contracts for customers in Advanced Automation (PSA).

- You can link a specific contract part to the N-able RMM integration. This is done in the contract parts section of a contract; select the relevant integration, group/site, and workload type, and then select the relevant configuration items.

- In the contract parts section of a contract you can select **Automatic update** to update the device quantity for the contract part.
- You can also select **Show workloads on invoice** to add information about specific devices to customer invoices.

For more information about defining contracts and adding devices to contracts, see "Working with contracts" (p. 261).

Integrating with VAR platforms

Note
This feature is only available for users assigned the Administrator role.

Advanced Automation (PSA) enables you to integrate with VAR (value-added reseller) platforms (currently only Microsoft CSP is supported). This enables you to access your customers' subscription usage data from third party vendors and, in turn, track, bill and invoice your customers in Advanced Automation (PSA), as required.

To access the VAR integrations, go to **Integrations**. In the displayed left menu, select **Automation** > **Cloud Commerce and Marketplaces**.

Integrating with Microsoft CSP

By integrating Advanced Automation (PSA) with Microsoft CSP, you can:

- Automatically import customers from the Microsoft CSP partner portal.
- Automatically import subscriptions and their usage data from the Microsoft CSP partner portal.
- Bill customers for actual Microsoft CSP subscriptions usage.

In order to successfully integrate Microsoft CSP with Advanced Automation (PSA), the Advanced Automation (PSA) service must be enabled. You must also have a fully configured Microsoft CSP account.

Note that Microsoft has two basic partner levels that allow service providers to resell Microsoft CSP services and licenses to end customers: Tier-1 and Tier-2.

- Tier-1 refers to partners that buy directly from Microsoft. For example, all distributors that sell Microsoft CSP program subscriptions are Tier-1 partners.
- Tier-2 refers to partners that buy Microsoft CSP program subscriptions from a distributor (Tier-1 partner).

Partners manage their Microsoft CSP services and licenses in one central console, the Microsoft partner portal, regardless of where they purchased the services and licenses.

Note
Advanced Automation (PSA) currently supports Tier-1 partners only.

To define integration settings

1. In Management Portal, go to **Integrations**, and then select **Automation** > **Cloud Commerce and Marketplaces**.
2. On the **Microsoft CSP** tile, click **Configure**, and then click **Activate**.
3. Enter the following Microsoft CSP credentials to access the Microsoft CSP account:
   - **App ID**: Enter the unique App ID for your Microsoft CSP account.
   - **Secret Key**: Enter the unique Secret Key for your Microsoft CSP account. The Secret Key is generated together with the App ID (see above).
   - **Domain**: Enter the relevant domain.
4. (Optional) Click **Test connection** to test the entered credentials.
5. Click **Save**.

   After defining the integration, you can then define a contract part (see "Creating a new contract" (p. 261)) and select a customer from Microsoft CSP to get the correct usage data from the relevant customer.

Reviewing and editing Microsoft CSP integration settings

You can review and edit your Microsoft CSP integration settings, as required. You can also deactivate the Microsoft CSP integration.

To review and edit Microsoft CSP integration settings

1. In Management Portal, go to **Integrations**, and then click the **Integrations in use** tab.

   On the **Microsoft CSP** tile, you can view the current status of the integration.
2. Click **Manage** to view and edit integration settings.
3. Click the pencil icon to edit the relevant field. For more information about the editable fields, see "Integrating with Microsoft CSP" (p. 351).
4. When done, click ✓.

To deactivate the Microsoft CSP integration

1. Go to **Integrations**, and then click the **Integrations in use** tab.
2. On the **Microsoft CSP** tile, click **Deactivate**.
3. In the displayed confirmation message, click **Delete**.

Using Microsoft CSP usage data in contracts

When integration with Microsoft CSP is configured (see "Integrating with Microsoft CSP" (p. 351)), you can add Microsoft CSP usage data to contracts for customers in Advanced Automation (PSA).

Note the following:

- You can link a specific contract part to the Microsoft CSP integration.
- You can filter license types from Microsoft CSP by:
  - **VAR Group**: Select the relevant customer from the list of customers on the Microsoft CSP partner portal in order to filter licenses related only to a specific customer.
  - **License Type**: Select from the available license types from the Microsoft CSP partner portal.

- The **Automatic update** check box in the **Contract parts** section of the creating a contract wizard is enabled by default and hidden: it automatically disables the **Quantity** field. When configured, Advanced Automation (PSA) synchronizes the actual usage data to this field, so you can bill for the actual license usage.

For more information about defining contracts, see "Working with contracts" (p. 261).

Note
When you generate an invoice for a customer with Microsoft CSP license usage, it automatically includes the relevant lines for used license types, with the correct quantity and price.

Integrating with payment platforms

Advanced Automation (PSA) enables you to integrate with various payment platforms (currently only PayPal and Stripe are supported). This enables you to send invoices that include links that customers can click to pay using the relevant platform.

To access the payment platform integrations, go to **Integrations**. In the displayed left menu, select **Automation** > **Payment processing**.

Integrating with PayPal

Advanced Automation (PSA) integration with the PayPal payment gateway enables you to automate the collection and tracking of payments from customers.

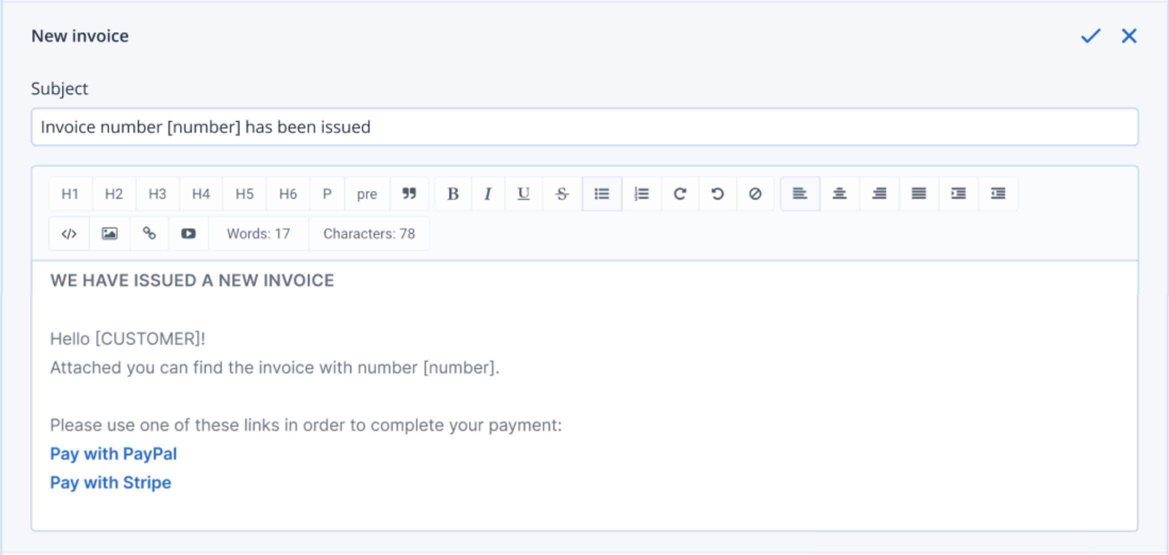
For information about additional payment platforms that integrate with Advanced Automation (PSA), see "Integrating with payment platforms" (p. 353).

To integrate with PayPal

1. Go to **Integrations**, and then select **Automation** > **Payment processing**.
2. On the PayPal tile, click **Configure**, and then click **Activate**.
3. Enter the following PayPal credentials:
   - API Username
   - API Password
   - Signature

   For more information about getting the above credentials from PayPal, see "How to access your PayPal API username, password, and signature information" (p. 354).
4. Click **Save**.

   You can now include a link to pay by PayPal in invoices sent to customers, as shown below. For more information about defining this link in the "New invoice" email template, see "Managing email templates" (p. 299).



Invoice number [number] has been issued

WE HAVE ISSUED A NEW INVOICE

Hello [CUSTOMER]!
Attached you can find the invoice with number [number].

Please use one of these links in order to complete your payment:
Pay with PayPal
Pay with Stripe

To modify your PayPal integration settings

1. Go to **Integrations**, and then click the **Integrations in use** tab.
2. On the PayPal tile, click **Manage**, and then select **Settings**.
3. Modify the settings as required (see above).

To deactivate your PayPal integration

1. Go to **Integrations**, and then click the **Integrations in use** tab.
2. On the PayPal tile, click **Deactivate**.
3. In the displayed confirmation message, click **Delete**.

How to access your PayPal API username, password, and signature information

In order to integrate Advanced Automation (PSA) with PayPal (see "Integrating with PayPal" (p. 353)), you need to define the PayPal API username, password, and signature in the integration settings. These credentials are located in your PayPal account settings, as described below.

To get your PayPal API username, password and signature information

1. Login to your PayPal account.
2. From the main menu, go to **Tools > All Tools**.
3. Scroll down the page and click **API Credentials**.
4. Click **NVP/SOAP integration**.

> **Note**
> If this is your first time creating API credentials, a **Request API credentials** link is displayed under the NVP/SOAP API integration. Complete the API Credential Request form, select the agreement check box, and click **Submit**.

5. Click the **Show** link on each corresponding entity and take note of the displayed credentials. They can then be used when defining your integration settings, as described in "Integrating with PayPal" (p. 353).

Integrating with Stripe

Advanced Automation (PSA) integration with the Stripe payment gateway enables you to automate the collection and tracking of payments from customers.

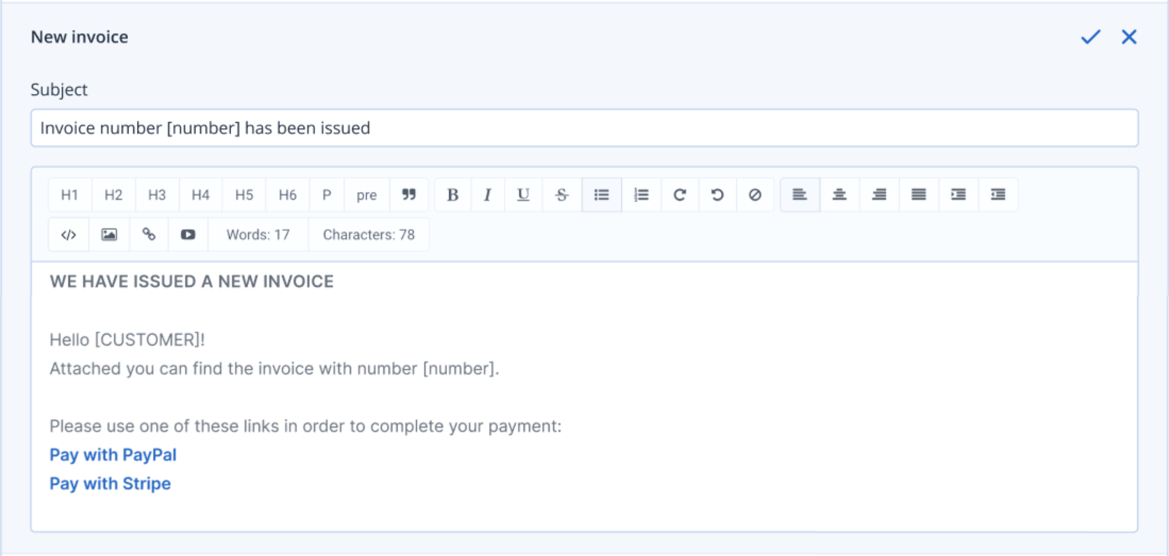
For information about additional payment platforms that integrate with Advanced Automation (PSA), see "Integrating with payment platforms" (p. 353).

To integrate with Stripe

1. Go to **Integrations**, and then select **Automation** > **Payment processing**.
2. On the Stripe tile, click **Configure**, and then click **Activate**.
3. Enter the following Stripe credentials:
   - Secret Key
   - Publishable Key

   For more information about getting the above credentials from Stripe, see "How to access your Stripe secret and publishable keys" (p. 356).
4. Click **Save**.

   You can now include a link to pay by Stripe in invoices sent to customers, as shown below. For more information about defining this link in the "New invoice" email template, see "Managing email templates" (p. 299).



New invoice

Subject

Invoice number [number] has been issued

WE HAVE ISSUED A NEW INVOICE

Hello [CUSTOMER]!
Attached you can find the invoice with number [number].

Please use one of these links in order to complete your payment:
Pay with PayPal
Pay with Stripe

To modify your Stripe integration settings

1. Go to **Integrations**, and then click the **Integrations in use** tab.
2. On the Stripe tile, click **Manage**, and then select **Settings**.
3. Modify the settings as required (see above).

To deactivate your Stripe integration

1. Go to **Integrations**, and then click the **Integrations in use** tab.
2. On the Stripe tile, click **Deactivate**.
3. In the displayed confirmation message, click **Delete**.

How to access your Stripe secret and publishable keys

In order to integrate Advanced Automation (PSA) with Stripe (see "Integrating with Stripe" (p. 355)), you need to define the Stripe secret key and publishable key in the integration settings. These credentials are located in your Stripe account settings, as described below.

To get your Stripe secret and publishable keys

1. Login to your Stripe account.
2. Go to **Developers > API keys**.
3. If this is your first time getting your secret key, click **Reveal test key token** to generate the key.
4. Take note of the displayed credentials. They can then be used when defining your integration settings, as described in "Integrating with Stripe" (p. 355).

Deactivating the Advanced Automation (PSA) service

You can deactivate the Advanced Automation (PSA) service if you no longer want to use the functionality included in Advanced Automation (PSA).

Deactivation is immediate. However, you can select to immediately delete the settings and data stored in Advanced Automation (PSA), or schedule their deletion in 30 days.

Important
If you select to delete all Advanced Automation (PSA) data immediately, all Advanced Automation (PSA) data and settings are removed from the system. If you later decide to start using Advanced Automation (PSA) again, you will need to activate the Advanced Automation (PSA) service, and redo the onboarding. For more information, see "Setting up Advanced Automation (PSA)" (p. 190).

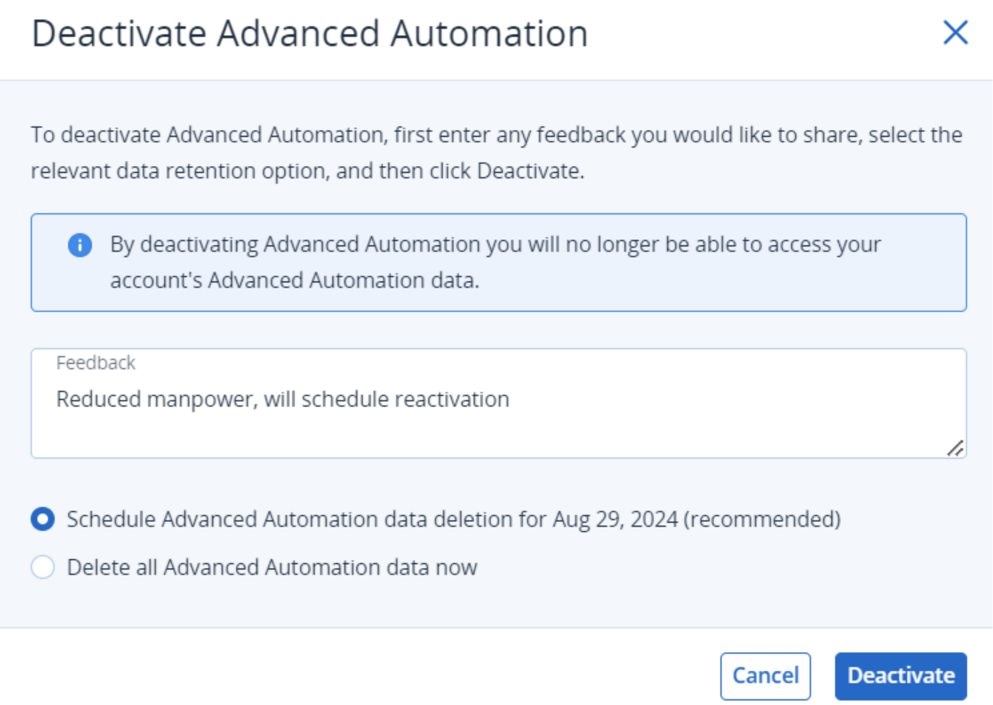
If you select to schedule the deletion of Advanced Automation (PSA) data in 30 days, your settings and data are preserved and you can reactivate Advanced Automation (PSA) at any time in the next 30 days. You are not charged for Advanced Automation (PSA) usage during this 30-day retention period. For more information about reactivating, see the procedure below.

To deactivate the Advanced Automation (PSA) service

1. In Management Portal, click **Settings** > **Billing and quoting**, and then select **Advanced Automation (PSA) service**.

   The displayed screen includes details on the number of current Advanced Automation (PSA) users.
2. Click **Deactivate Advanced Automation (PSA) service**.
3. In the displayed dialog, enter any feedback you would like to share.
4. Select one of the following options:

- Schedule the deletion of Advanced Automation (PSA) data for 30 days from now (the actual deletion date is shown). This option enables you to reactivate Advanced Automation (PSA) at any time during the next 30 days, as described in the procedure below.
- Delete all your Advanced Automation (PSA) data now. This option immediately deletes all Advanced Automation (PSA) data and settings, and cannot be reversed.



Deactivate Advanced Automation

To deactivate Advanced Automation, first enter any feedback you would like to share, select the relevant data retention option, and then click Deactivate.

By deactivating Advanced Automation you will no longer be able to access your account's Advanced Automation data.

Feedback: Reduced manpower, will schedule reactivation

● Schedule Advanced Automation data deletion for Aug 29, 2024 (recommended)

○ Delete all Advanced Automation data now

5. Click **Deactivate**.

   If you selected to schedule the deletion of Advanced Automation (PSA) data in 30 days, the main Advanced Automation (PSA) landing page is displayed. You can click **Reactivate** at any time in the next 30 days to reactivate the service. For more information about reactivating, see the procedure below.

   If you selected to delete all Advanced Automation (PSA) data now, the main Advanced Automation (PSA) landing page is displayed, but only with the option to **Activate** the Advanced Automation (PSA) service. You will need to complete the onboarding process if you want to activate Advanced Automation (PSA) again.

To reactivate the Advanced Automation (PSA) service

1. In the management portal, click **Settings > Advanced Automation (PSA)**.
2. Click **Reactivate**.

   Note

   The **Reactivate** option is only available if you selected to schedule the deletion of Advanced Automation (PSA) data in 30 days, as described in the above procedure.

3. In the confirmation dialog, click **Reactivate**.

Note
If you did not previously complete the onboarding process, the onboarding wizard screen is displayed. Configure the relevant Advanced Automation (PSA) options (see "Activating Advanced Automation (PSA)" (p. 190)).

Although the Advanced Automation (PSA) service is now reactivated and most of your settings are restored, you will need to manually perform the following:

- Review and update Advanced Automation (PSA) roles for the users in your tenant.
- Review and activate accounting and payment platform integrations, if previously in use.
- Review and configure RMM integrations, if previously in use. You should update all active RMM integrations to enable third-party alerts for ticket synchronization.
- Review and configure incoming and outgoing email servers.
- Check expiration dates in contracts, and update as required.
- Your tenant's users may also need to manually enable Outlook for calendars.

Integrations

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

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

Integrations are listed on the integration catalogs.

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

Integration catalogs

The integration catalogs list the available integrations:

- The Application Catalog.

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

  If one of your customers sees an integration they want to use, they should contact you to activate it for them.
- Data center (DC) catalogs.

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

  Partner-level Management Portal administrators can:

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

  Customer-level Management Portal administrators can:

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

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

Catalog entries

Catalog entries consist of two parts:

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

Opening your data center integration catalog

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

- The **Learn more** link

  Each integration catalog entry has a page with integration details including, for example, a full functional description, screenshots, videos, a feature list, contact details, links to integration resources, etc.

  Click this link to open the integration detail page.
- The **Configure** button

  Click this button to activate the integration.

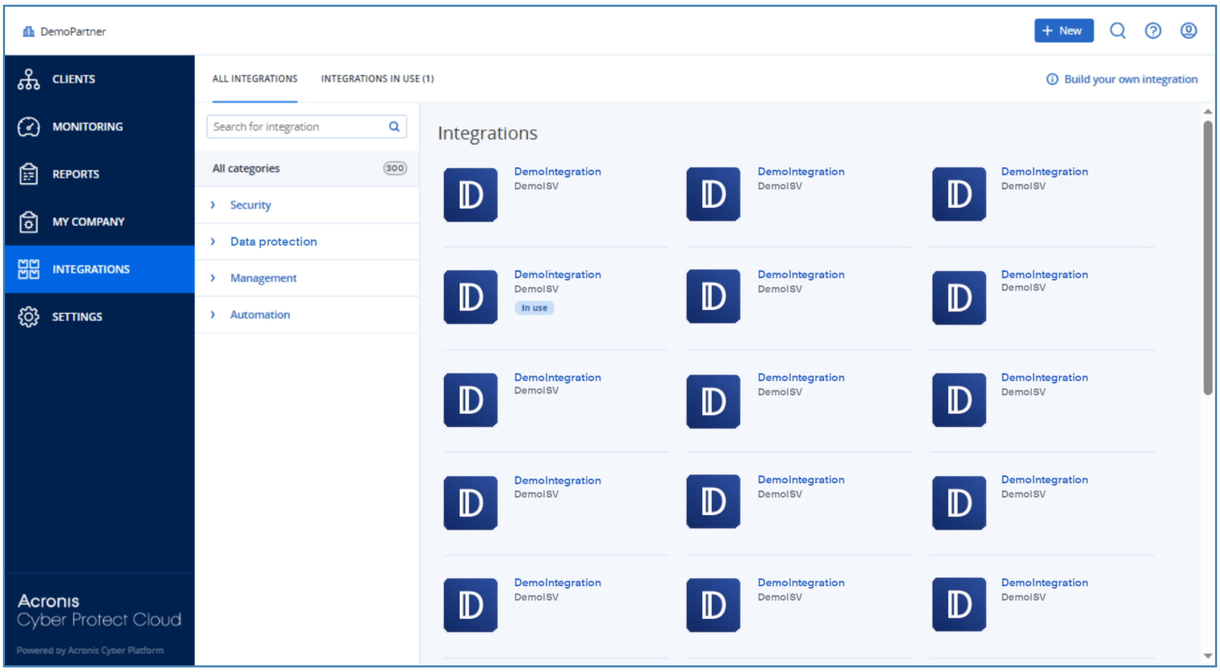
Note

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

To open your DC integration catalog

1. Open Management Portal.
2. Select **Integrations** from the main menu.

   The **All integrations** tab is opened by default. This displays the catalog cards for the integrations which are currently available on your DC.
3. [Optional] Choose a category and enter text in the search field to filter the catalog cards.

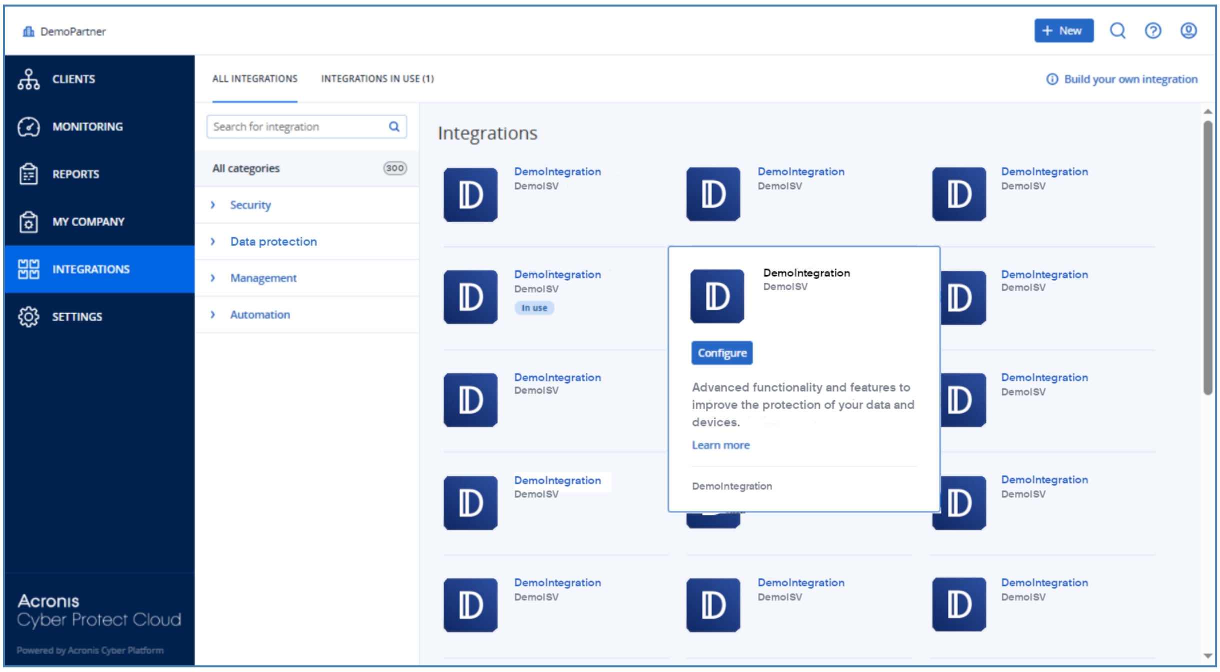


Opening an integration detail page

To open an integration detail page

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

The integration detail page opens.

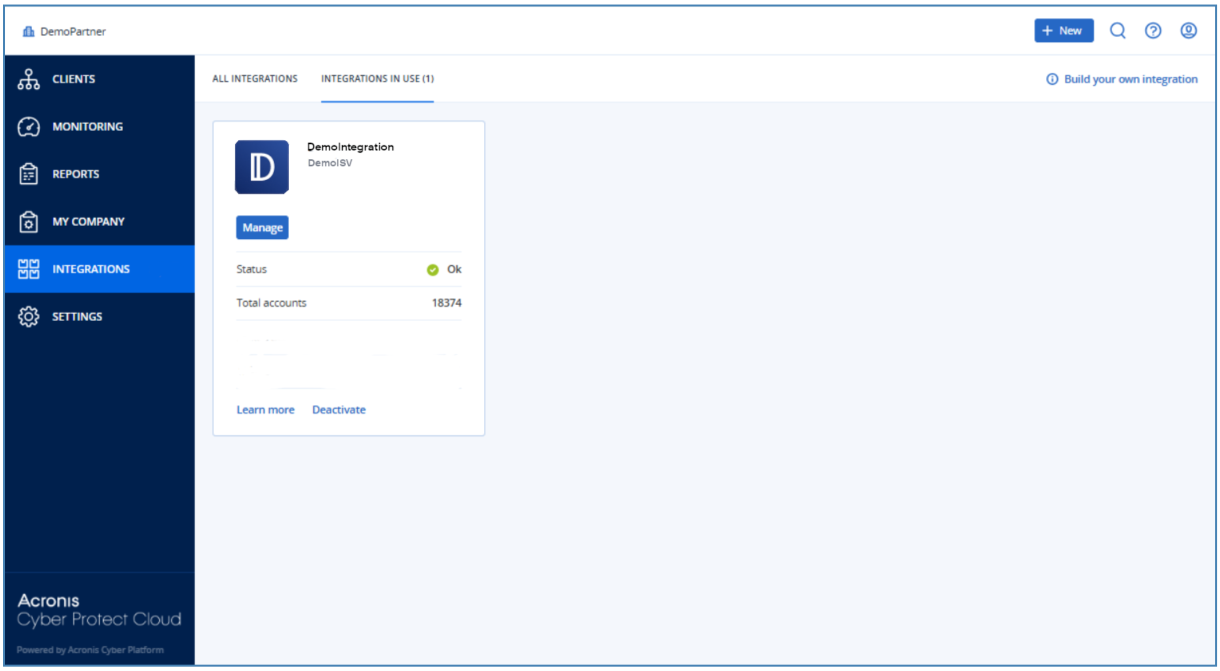


Viewing your activated integrations

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

To view your actived integrations

1. Open the integration catalog on your data center.
2. Select the **Integrations in use** tab.



Status: Ok

Total accounts: 18374

Opening Application Catalog

Application Catalog lists all Cyber Protect Cloud integrations.

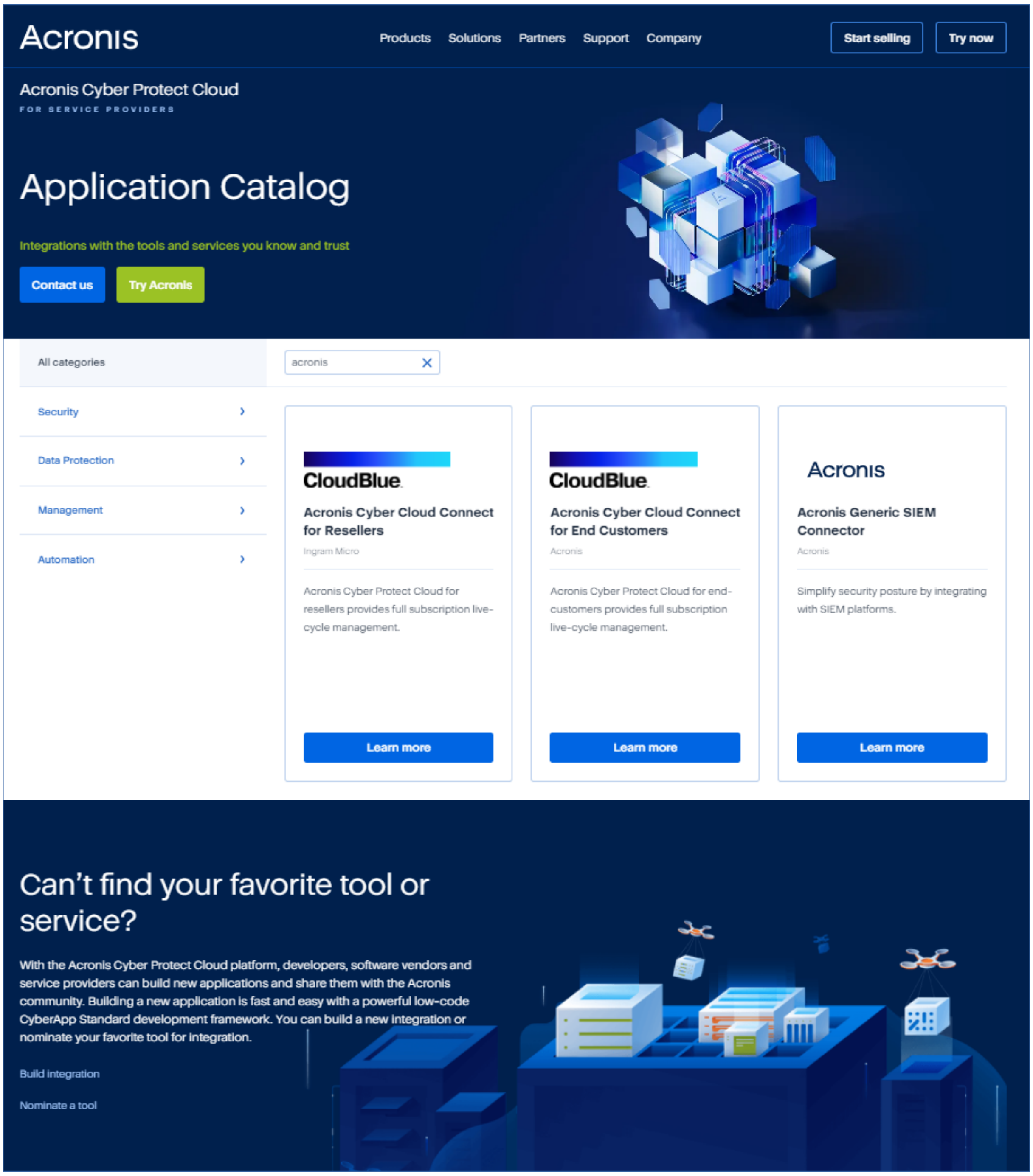
Note

Application Catalog is for reference only: integration enablement is not available from this catalog. You can activate an integration from the data center integration catalog on Management Portal.

To open Application Catalog

1. Visit solutions.acronis.com.

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



Acronis Cyber Protect Cloud
FOR SERVICE PROVIDERS

Application Catalog

Integrations with the tools and services you know and trust

Acronis Cyber Cloud Connect for Resellers
Ingram Micro
Acronis Cyber Protect Cloud for resellers provides full subscription live-cycle management.

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

Acronis Generic SIEM Connector
Acronis
Simplify security posture by integrating with SIEM platforms.

Can't find your favorite tool or service?

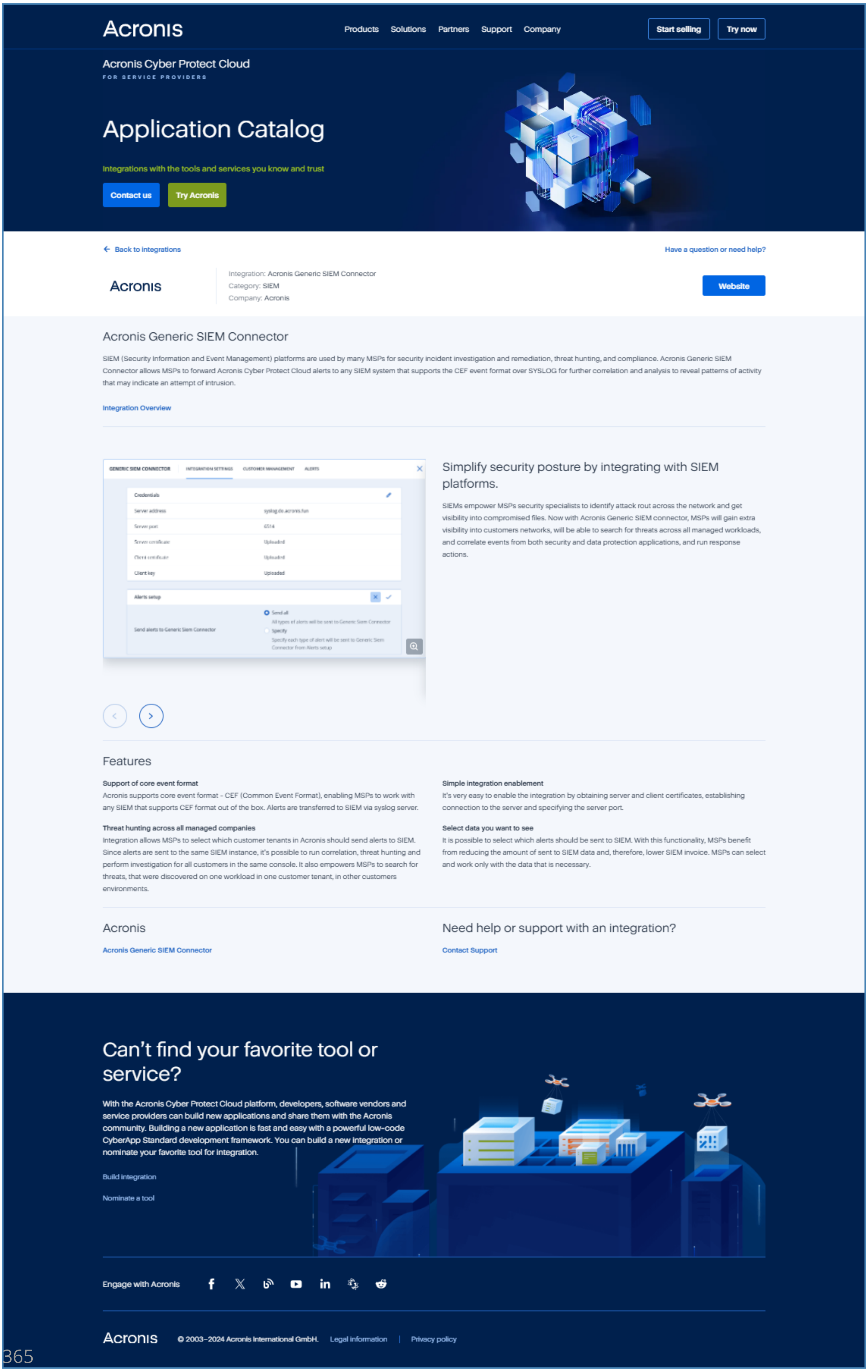
With the Acronis Cyber Protect Cloud platform, developers, software vendors and service providers can build new applications and share them with the Acronis community. Building a new application is fast and easy with a powerful low-code CyberApp Standard development framework. You can build a new integration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

Opening an integration detail page

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

To open an integration detail page

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



Acronis Cyber Protect Cloud
FOR SERVICE PROVIDERS

Application Catalog

Integrations with the tools and services you know and trust

Integration: Acronis Generic SIEM Connector
Category: SIEM
Company: Acronis

Acronis Generic SIEM Connector

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

Integration Overview

Credentials

Server address	syslog.do.acronis.fun
Server port	6514
Server certificate	Uploaded
Client certificate	Uploaded
Client key	Uploaded

Alerts setup

Send alerts to Generic Siem Connector
● Send all
All types of alerts will be sent to Generic Siem Connector
○ Specify
Specify each type of alert will be sent to Generic Siem Connector from Alerts setup

Simplify security posture by integrating with SIEM platforms.

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

Features

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

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

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

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

Acronis

Acronis Generic SIEM Connector

Need help or support with an integration?

Contact Support

Can't find your favorite tool or service?

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

Build integration

Nominate a tool

Engage with Acronis

Legal information | Privacy policy

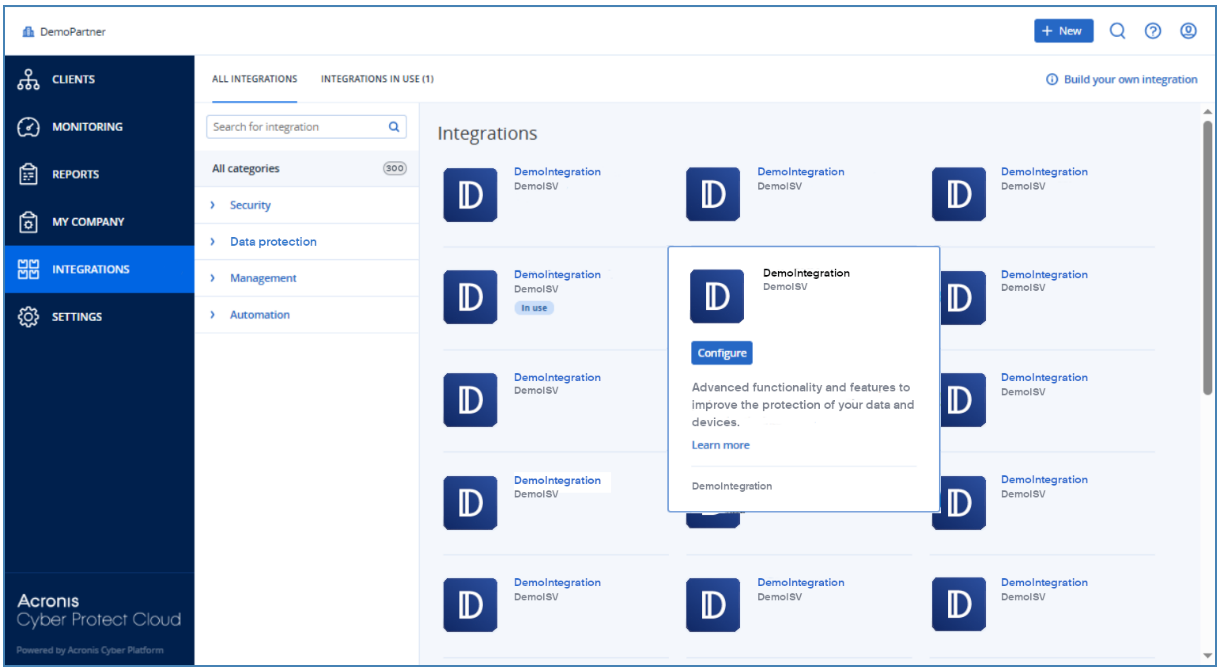
Activating an integration

To activate an integration

1. Open the integration catalog on your data center.
2. Locate the catalog card for the integration you want to activate.

   To filter the integrations:

   - [Optional] Select a category.
   - [Optional] Type a string in the search field.
3. Hover over the catalog card.
4. Click **Configure**.
5. Follow the on-screen instructions.



Advanced functionality and features to improve the protection of your data and devices.

Configuring an active integration

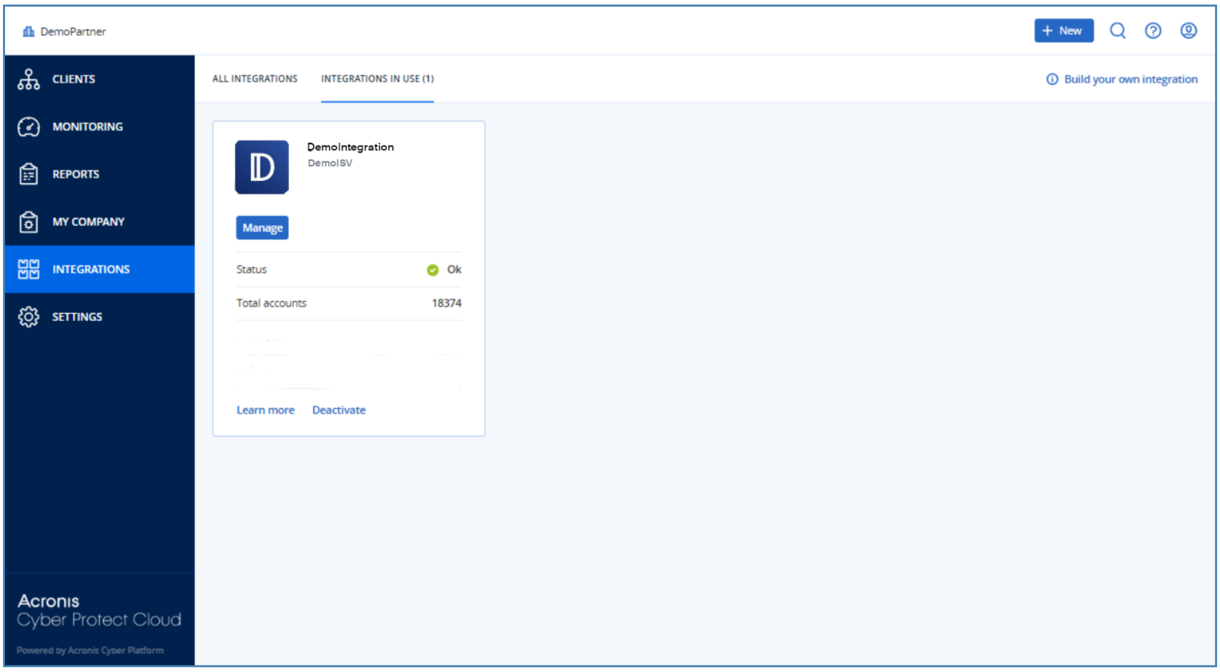
To configure an active integration

1. Open the integration catalog on your data center.
2. Select the **Integrations in use** tab.
3. Locate the catalog card for the integration you want to configure.
4. Click **Manage**.

   The integration configuration screen opens.
5. Follow the on-screen instructions or consult the integration documentation.

Note

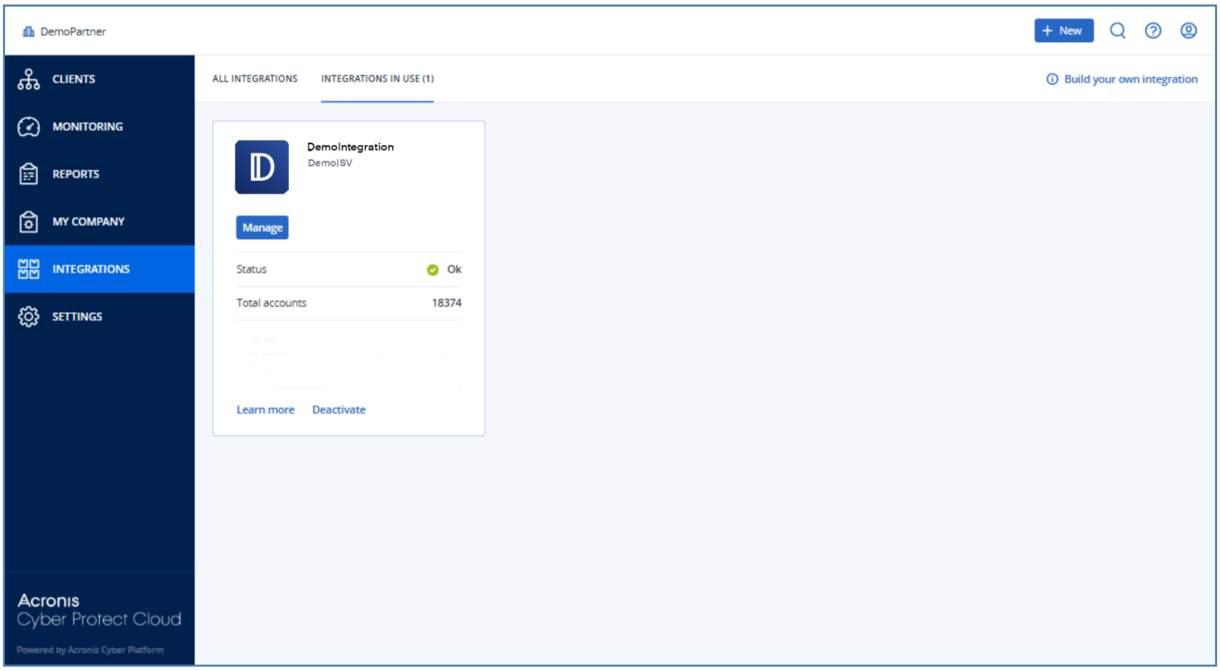
Documentation is usually available in the catalog detail page. For more information, see Opening an integration detail page.



Deactivating an active integration

To deactivate an integration

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



Status: Ok

Total accounts: 18374

API clients

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

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

Note
The API client inherits the service roles of the administrator account, and these roles cannot be changed later. Changing roles of the administrator account or disabling it does not affect the client.

API client credentials

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

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

API client flow

1. A Management Portal administrator creates an API client.
2. An administrator enables the OAuth 2.0 client credentials flow in the third-party system.

3. According to this flow, before accessing the tenant and its services via the API, the system must first send the API client credentials to the platform, using the authorization API.
4. The platform generates and sends back a security token- the unique cryptic string assigned to this specific client.
5. The third-party system must add this token to all API requests.

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

Creating an API client

To create an API client

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

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

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

Resetting an API client secret value

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

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

To reset an API client secret value

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

4. Click •••, and then click **Reset secret**.
5. Click **Next** to confirm your decision.
6. Copy and save the new API client secret value.

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

7. Click **Done**.

Disabling an API client

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

> **Note**
> Disabling the client does not affect tokens' expiration time.

You can re-enable the API client at any time.

To disable an API client

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

Enabling a disabled API client

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

To enable a disabled API client

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

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

Deleting an API client

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

Important
There is no way to recover a deleted client.

To delete an API client

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

Creating an integration

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

CyberApp

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

Note
For more information about CyberApps and Vendor Portal, see the Integration Guide.

API integrations

There is a full suite of APIs for integrations.

Note
For more information about APIs, see the platform APIs chapter of the Integration Guide.

Integrating Cyber Protect Cloud with VMware Cloud Director

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

The integration includes the following steps:

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

   RabbitMQ provides single sign-on (SSO) functionality, so that you can use your VMware Cloud Director credentials to log in to the Cyber Protect console.

   In Cyber Protect Cloud version 23.05 (released in May 2023) and older, RabbitMQ is also used for synchronizing the changes in the VMware Cloud Director environment to Cyber Protect Cloud.
2. Deploying a management agent.

   During the deployment of the management agent, a plug-in for VMware Cloud Director is also installed. The plug-in adds Cyber Protection to the VMware Cloud Director user interface.

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

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

   Note
   Only Organization Administrators with unique email addresses in VMware Cloud Director are mapped to Cyber Protect Cloud.
3. Deploying one or more backup agents.

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

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

Limitations

- Integration with VMware Cloud Director is possible only for partner tenants in the **Managed by service provider** management mode, whose parent tenant (if any) also uses the **Managed by service provider** management mode. For more information about the types of tenants and their management mode, see "Creating a tenant" (p. 39).

  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.
- If two-factor authentication is enabled for your tenant, you must use a partner administrator account that is marked as a service account. Otherwise, the agent will not be able to authenticate to Cyber Protect Cloud.

  We recommend that you use a dedicated account for the agent. For more information about how to create a service account, see "To convert a user account to a service account" (p. 58).
- 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 Protect console opens in a new tab.

Software requirements

Supported VMware Cloud Director versions

VMware Cloud Director 10.4 and 10.5 require RabbitMQ message broker. For more information, see "Configuring RabbitMQ message broker" (p. 373). When upgrading to VMware Cloud Director 10.6, you must update the management and backup agents to their latest versions. For more information, see "Updating the agents" (p. 381).

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

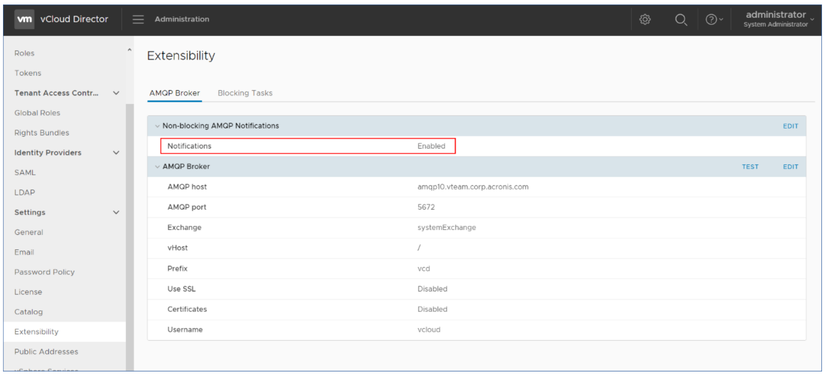
This procedure depends on the version of Cyber Protect Cloud. A simplified procedure is used for version 23.06 (released in June 2023) and later.

To configure RabbitMQ

For version 23.06 and later

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.



Non-blocking AMQP Notifications

Notifications	Enabled

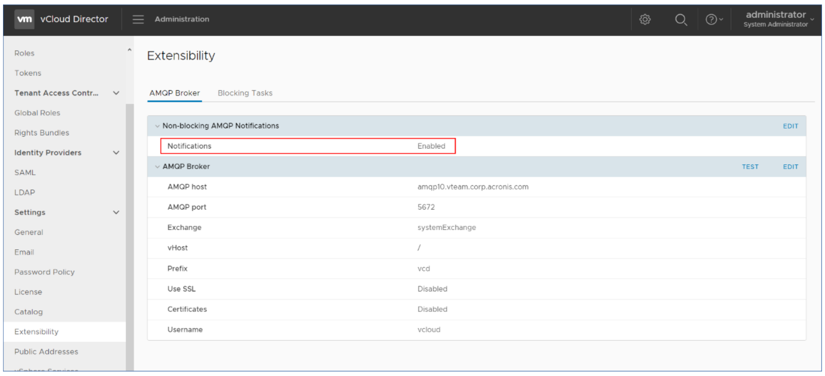
AMQP Broker

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

For version 23.05 and older

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.



Non-blocking AMQP Notifications

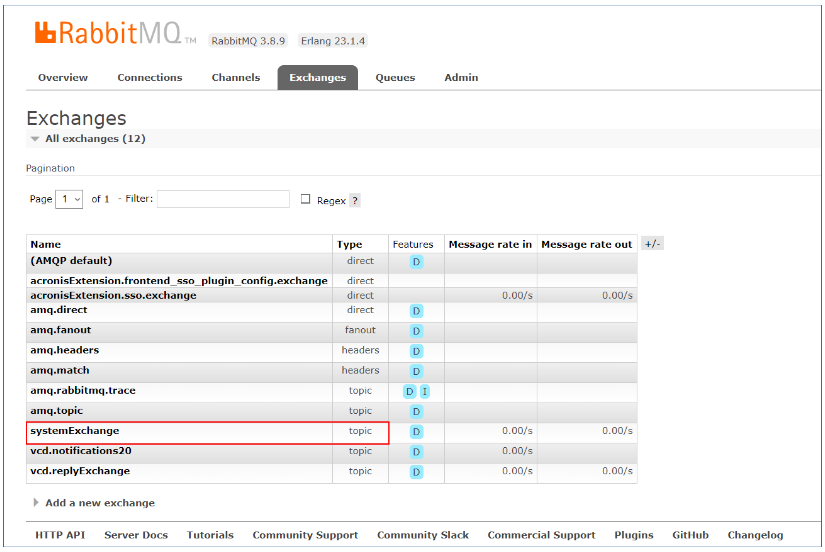
Notifications	Enabled

AMQP Broker

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

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

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



Exchanges

All exchanges (12)

Pagination

Page 1 of 1 - Filter: □ Regex ?

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

Installing and publishing the plug-in for VMware Cloud Director

The plug-in for VMware Cloud Director is automatically installed when you install the management agent.

However, you need to manually publish the plug-in to the tenants that will use Cyber Protection.

To publish the plug-in for VMware Cloud Director

1. Log in to the VMware Cloud Director provider portal as a system administrator.
2. From the navigation menu, select **Customize Portal**.
3. On the **Plugins** tab, select the **Cyber Protection** plug-in, and then click **Publish**.
4. Configure the scope of the publishing:
    a. In the **Scope to** section, select only the **Tenants** check box.
    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.
5. Click **Save**.
6. Click **Trust**.

Installing a management agent

1. Log in to Cyber Protect Cloud Management Portal as a partner administrator.
2. Go to **Settings** > **Location**, and then click **Add VMware Cloud Director**.
3. From the **Release channel** drop-down list, select the version of the agent. The following options are available:

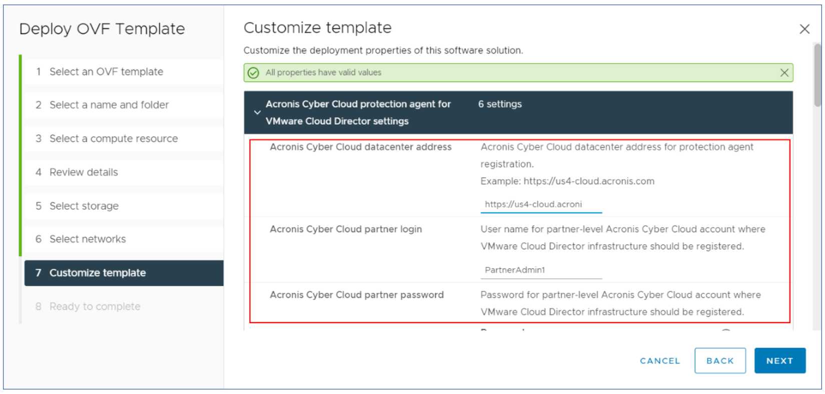
- **Latest** – the latest available version.
- **Previous stable** – the most recent stable version of the protection agent from previous releases.

4. Click the **Management Agent** link and download the ZIP file.
5. Extract the management agent template file `vCDManagementAgent.ovf` and the virtual hard disk file `vCDManagementAgent-disk1.vmdk`.
6. 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.

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



Deploy OVF Template

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

Customize template

Customize the deployment properties of this software solution.

All properties have valid values

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

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

https://us4-cloud.acroni

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

PartnerAdmin1

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

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

Note

If two-factor authentication is enabled for your tenant, you must use a partner administrator account that is marked as a service account. Otherwise, the agent will not be able to authenticate to Cyber Protect Cloud.

We recommend that you use a dedicated account for the agent. For more information about how to create a service account, see "To convert a user account to a service account" (p. 58).

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. 82).

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

Note

The selected billing mode applies to all new customer tenants that will be created.

e. VMware Cloud Director parameters: infrastructure address, system administrator login, and password.

f. [If you use VMware Cloud Director 10.5 or older] RabbitMQ parameters: administrator login and password.

g. The password for the `root` user on the virtual machine with the agent.

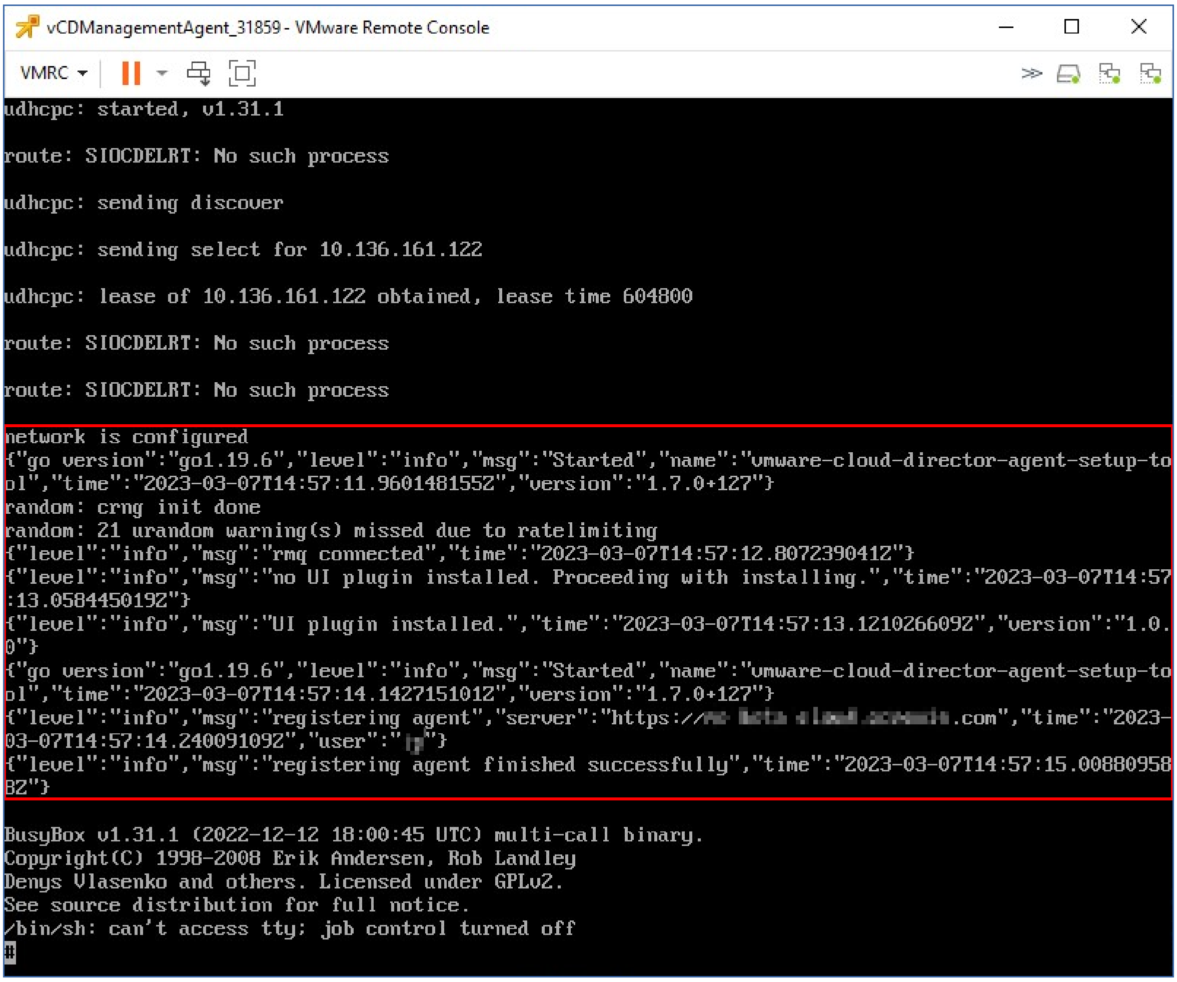
h. Network parameters: IP address, subnet mask, default gateway, DNS, DNS suffix.

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

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

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

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

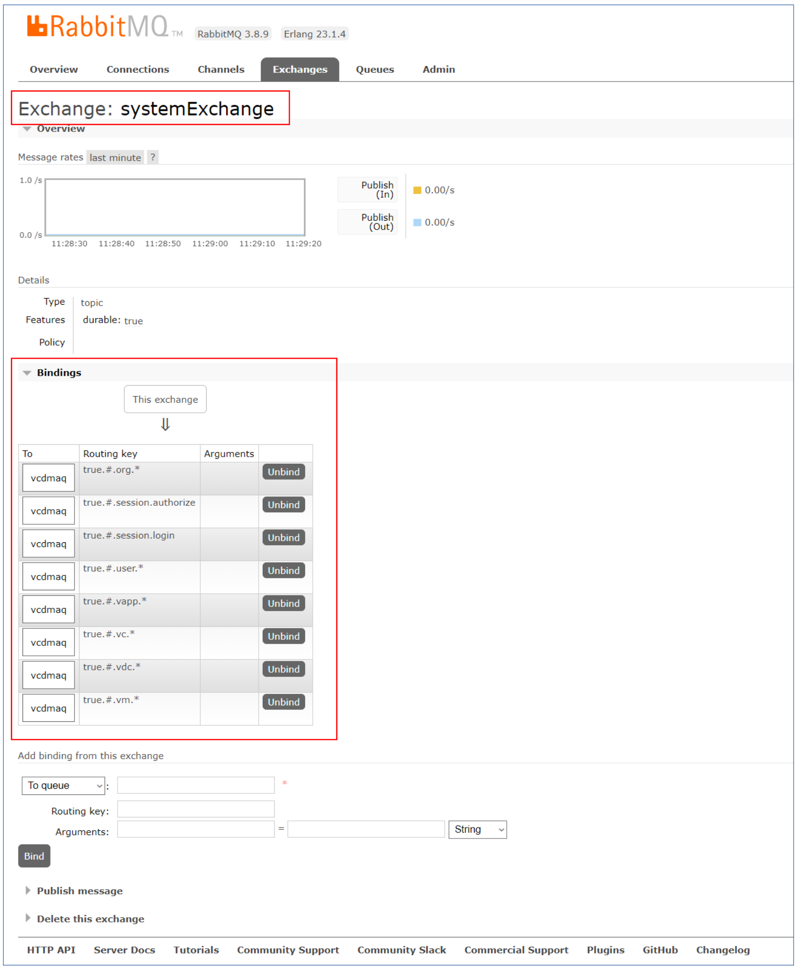


```
udhcpc: started, v1.31.1

route: SIOCDELRT: No such process

udhcpc: sending discover

udhcpc: sending select for 10.136.161.122

udhcpc: lease of 10.136.161.122 obtained, lease time 604800

route: SIOCDELRT: No such process

route: SIOCDELRT: No such process

network is configured
{"go version":"go1.19.6","level":"info","msg":"Started","name":"vmware-cloud-director-agent-setup-to
ol","time":"2023-03-07T14:57:11.960148155Z","version":"1.7.0+127"}
random: crng init done
random: 21 urandom warning(s) missed due to ratelimiting
{"level":"info","msg":"rmq connected","time":"2023-03-07T14:57:12.807239041Z"}
{"level":"info","msg":"no UI plugin installed. Proceeding with installing.","time":"2023-03-07T14:57
:13.058445019Z"}
{"level":"info","msg":"UI plugin installed.","time":"2023-03-07T14:57:13.121026609Z","version":"1.0.
0"}
{"go version":"go1.19.6","level":"info","msg":"Started","name":"vmware-cloud-director-agent-setup-to
ol","time":"2023-03-07T14:57:14.142715101Z","version":"1.7.0+127"}
{"level":"info","msg":"registering agent","server":"https://[redacted].com","time":"2023-
03-07T14:57:14.240091092Z","user":"[redacted]"}
{"level":"info","msg":"registering agent finished successfully","time":"2023-03-07T14:57:15.00880958
8Z"}

BusyBox v1.31.1 (2022-12-12 18:00:45 UTC) multi-call binary.
Copyright(C) 1998-2008 Erik Andersen, Rob Landley
Denys Vlasenko and others. Licensed under GPLv2.
See source distribution for full notice.
/bin/sh: can't access tty; job control turned off
#
```

9. a. Log in to the RabbitMQ management console as an administrator.

   b. In the **Exchanges** tab, select the exchange that you set during the RabbitMQ installation. By default, its name is **systemExchange**.

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



Exchange: systemExchange

Details

Type	topic
Features	durable: true
Policy	

Bindings

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

What to do next

If your agent build is 24.12.39185 or later and your environment is VMware vSphere 8.x or later, you can enable the FIPS compliance mode. See "Enabling the FIPS compliance mode for VMware Cloud Director" (p. 380).

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. From the **Release channel** drop-down list, select the version of the agent. The following options are available:
   - **Latest** – the latest available version.
   - **Previous stable** – the most recent stable version of the protection agent from previous releases.

4. Click the **Backup Agent** link and download the ZIP file.
5. Extract the backup agent template file `vCDCyberProtectAgent.ovf` and the virtual hard disk file `vCDCyberProtectAgent-disk1.vmdk`.
6. In vSphere Client, deploy the backup agent template to the desired ESXi host.

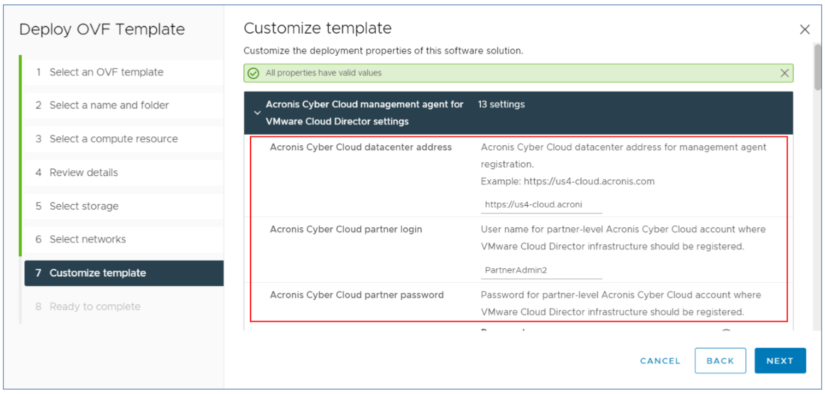
   You need at least one backup agent per host. By default, the backup agent is assigned 8 GB of RAM and 2 CPUs, and can process up to 5 backup or recovery tasks simultaneously.

   To process more tasks or to distribute the backup and recovery traffic, deploy additional agents to the same host. Alternatively, to avoid failures related to insufficient memory, we recommend that you assign 16 GB of RAM and 4 vCPUs to the existing agent.

   Note

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

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



Customize template

Customize the deployment properties of this software solution.

All properties have valid values

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

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

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

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

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

      If two-factor authentication is enabled for your tenant, you must use a partner administrator account that is marked as a service account. Otherwise, the agent will not be able to authenticate to Cyber Protect Cloud.

      We recommend that you use a dedicated account for the agent. For more information about how to create a service account, see "To convert a user account to a service account" (p. 58).
   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. The password for the `root` user on the virtual machine with the agent.
   e. 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 check box next to **Enable eth1**.

> **Note**
> Ensure that your network settings will allow the backup agent to access both the vCenter Server and your Cyber Protect Cloud data center.

f. 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.

g. 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.

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

What to do next

If your agent build is 24.12.39185 or later and your environment is VMware vSphere 8.x or later, you can enable the FIPS compliance mode. See "Enabling the FIPS compliance mode for VMware Cloud Director" (p. 380).

Enabling the FIPS compliance mode for VMware Cloud Director

FIPS compliance mode can be enabled for agent builds 24.12.39185 and later, in VMware vSphere 8.x and later. In this mode, the backup agent uses FIPS 140-2 compliant cryptographic library for all encryption operations. For more information, see FIPS-compliant mode.

> **Important**
> To operate as expected, FIPS mode must be enabled on both the management agent and the backup agents.

To enable FIPS compliance mode for Cyber Protect agents in a Cloud Director instance

1. In the vSphere Client, locate the vCD Management Agent virtual machine, open the remote console, and then run the following command:

   ```
   fips-mode-setup --enable
   ```

2. Back in the vSphere client, locate the vCD Cyber Portect Agent virtual machine on which you want to enable the FIPS compliance mode, open the remote console, and then run the following command:

```
fips-mode-setup --enable
```

3. Run the command on all other vCD Cyber Portect Agent virtual machines on which you want to enable the FIPS compliance mode.

Updating the agents

To update a management agent

1. Log in to the Cyber Protect Cloud management portal as a partner administrator.
2. Go to **Settings** > **Location**, and then click **Add VMware Cloud Director**.
3. Click the **Management Agent** link, and then download the ZIP file with the latest agent.
4. Extract the management agent template file `vCDManagementAgent.ovf` and the virtual hard disk file `vCDManagementAgent-disk1.vmdk`.
5. In vSphere Client, power off the virtual machine with the current management agent.
6. Deploy a virtual machine with the new management agent by using the latest `vCDManagementAgent.ovf` and `vCDManagementAgent-disk1.vmdk` files.
7. Configure the management agent by using the same settings as in the old one.
8. [Optional] Delete the virtual machine with the old management agent.

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

To update a backup agent

1. Log in to the Cyber Protect Cloud management portal as a partner administrator.
2. Go to **Settings** > **Location**, and then click **Add VMware Cloud Director**.
3. Click the **Backup Agent** link and download the ZIP file with the latest agent.
4. Extract the management agent template file `vCDCyberProtectAgent.ovf` and the virtual hard disk file `vCDCyberProtectAgent-disk1.vmdk`.
5. In vSphere Client, power off the virtual machine with the current backup agent.
6. 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.
7. Deploy a virtual machine with the new backup agent by using the latest `vCDCyberProtectAgent.ovf` and `vCDCyberProtectAgent-disk1.vmdk` files.
8. Configure the backup agent by using the same settings as in the old one.
9. Delete the virtual machine with the old backup agent.

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 and publishing the plug-in for VMware Cloud Director" (p. 375).

4. In the VMware Cloud Director tenant portal, click **Users**.
5. Select a user, and then click **Edit**.
6. Assign this user the new role that you created.

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

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

System report, log files, and configuration files

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

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

To enable the SSH connection to a virtual machine

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

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

To run the `sysinfo` tool

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

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

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

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

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

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

To access a log or configuration file

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

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

   You can find the log files in the following locations:
   - Backup agent: `/opt/acronis/var/log/vmware-cloud-director-backup-service/log.log`
   - Management agent: `/opt/acronis/var/log/vmware-cloud-director-management-agent/log.log`

   You can find the configuration files in the following locations:
   - Backup agent: `/opt/acronis/etc/vmware-cloud-director-backup-service/config.yml`
   - Management agent: `/opt/acronis/etc/vmware-cloud-director-management-agent/config.yaml`

Accessing the Cyber Protect 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. 382).

Administrators can access the custom Cyber Protect 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 Protect 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 Protect consoles of their customer tenants and can manage backup and recovery on their behalf.

Performing backup and recovery

Creating a protection plan

To configure the backup settings, you must create a protection plan.

You can apply a protection plan to more than one machine. Also, you can apply multiple protection plans to the same machine.

Limitations

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

To create a protection plan

1. In the Cyber Protect console, go to **Devices** > **VMware Cloud Director**.
2. Select the machines that you want to protect, and then click **Protect**.
3. [If there are already applied plans] Click **Add plan**.
4. Click **Create plan**.
5. In **Encryption**, configure the encryption settings.
6. [Optional] To rename the protection plan, click the pencil icon, and then enter the new name.
7. [Optional] To change the backup scheme or schedule, click **Schedule**, and then configure the settings.
8. [Optional] To change the retention rules, click **How many to keep**, and then configure the settings.
9. [Optional] To change the backup options, click **Backup options**, and then configure the settings.
10. Click **Apply**.

Recovering a machine

You can recover a backup to the original virtual machine or to a new virtual machine.

Limitations

- File-level recovery is not supported.
- You can recover backups to new virtual machines in VMware Cloud Director 10.4 and later.

  To recover a backup to a new virtual machine, the backup must be created by an agent version 24.02 or later. You can check the agent version in the `ProductVersion.conf` file, which is located in the `/etc` directory of the virtual machine with the agent.
- After you recover a backup to a new machine, the new machine appears in **Devices** > **VMware Cloud Director** > Organization > virtual data center > **Standalone VMs**. You cannot select a specific vApp as a recovery target.

To recover a machine

To the original machine

1. In the Cyber Protect console, select the recovery point in one of the following ways:
   - Go to **Devices** > **VMware Cloud Director**, select a backed-up machine, click **Recovery**, and then select a recovery point.
   - Go to **Devices** > **VMware Cloud Director**, select a backup archive, click **Show backups**, and then select a recovery point.
2. Click **Recover machine**.
3. Click **Start recovery**.

To a new machine

1. In the Cyber Protect console, select the recovery point in one of the following ways:
   - Go to **Devices** > **VMware Cloud Director**, select a backed-up machine, click **Recovery**, and then select a recovery point.
   - Go to **Devices** > **VMware Cloud Director**, select a backup archive, click **Show backups**, and then select a recovery point.
2. Click **Recover machine**.
3. Click **Target machine**, and then select **New machine**.
4. Select the virtual data center for the new machine.
5. Specify a name for the new machine.

   By default, the name of the original machine is suggested.
6. Click **OK**.
7. [Optional] Click **VM settings** to change any of the following settings for the new machine, and then click **OK**:
   - RAM size
   - Number of virtual processors
   - Number of cores per socket
   - Storage profile
   - Network adapters and assigned networks

8. [Optional] Click **Disk mapping** to change the disk mapping or the storage profile for a disk, and then click **OK**.
9. Click **Start recovery**.

Removing the integration with VMware Cloud Director

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

Using the partner portal

The partner portal is designed for service providers, distributors, and resellers participating in the #CyberFit partner program.

With the partner portal, you can access   content, tools, and training.

To start using the partner portal

1. Access the partner portal in one of the following ways:
   - Click **Become a partner** in the bottom-left corner of the management portal.
   - Visit the partner portal website.
2. Register your company in the partner program.
3. Receive the access details via email.

Partner portal roles

Partner portal includes a number of roles, which can be assigned to your users as required.

The table below describes each of the available roles, and the rights assigned to each role within the Partner portal:

Role	Description
Basic	The default role applied to all users. This role grants access to essential features of the Partner portal, including the Dashboard, Partner Program, Content Hub, and Training.
Training	Users with this role can access training materials. Other features of the Partner Portal will not be available to these users.
Marketing	This role grants access to features of the Partner portal necessary for a marketing specialist, including the Dashboard, Partner Program, Marketing, Content Hub, Training, Datacenter Status, and Database Management.
Sales	Users with this role can access features of the Partner portal necessary for a sales specialist, such as the Dashboard, Partner Program, Sales, Content Hub, Training, Datacenter Status, and Database Management.
Sales and Marketing	This role grants access to the necessary features of the Partner portal for a unified sales and marketing specialist, including the Dashboard, Partner Program, Sales, Marketing, Content Hub, Training, Datacenter Status, and Database Management.
Administrator	Administrators have access to all features of the Partner portal, including Dashboard, Partner Program, Sales, Marketing, Content Hub, Training, Datacenter Status, and Database Management. Additionally, administrators can manage permissions for partner users and modify company information.

Index