CYTOMIC

CYTOMIC Nexus Administration Guide_

Legal notice

Registered trademarks

Contact information

Corporate Headquarters:

Cytomic (Business Unit of Panda Security)

Calle Santiago de Compostela 12

Bilbao (Bizkaia) 48003 Spain.

https://www.pandasecurity.com/uk/about/contact/

Author : Cytomic

Version: 1.90

Date: 10/31/2024

About the Cytomic Nexus Administration Guide

To get the latest version of this guide, go to:

http://nexus-documents.cytomic.ai/AdvancedGuide/Nexus-Manual-EN.pdf

For more information about a specific topic, see the product online help, available at:

http://nexus-documents.cytomic.ai/Help/v77000/Partners/en-us/index.htm

Release notes

To find out what's new in the latest version of Cytomic Nexus, go to:

http://documents.managedprotection.pandasecurity.com/ReleaseNotes/v77000//Partners/en-us/ReleaseNotes.html

Products supported by Cytomic Nexus

Advanced EDR

Administration Guide:

https://info.cytomicmodel.com/resources/guides/EDR/latest/en/EDR-guide-EN.pdf

Product online help:

https://info.cytomicmodel.com/resources/help/EDR/latest/en/index.htm

Advanced EPDR

Administration Guide

https://info.cytomicmodel.com/resources/guides/EPDR/latest/en/EPDR-guide-EN.pdf

Product online help:

https://info.cytomicmodel.com/resources/help/EPDR/latest/en/index.htm

Technical information about modules and services compatible with Cytomic Nexus

Cytomic Insights

https://info.cytomicmodel.com/resources/guides/Insights/en/INSIGHTS-guide-EN.pdf

Cytomic Data Watch

https://info.cytomicmodel.com/resources/guides/DataWatch/en/DATAWATCH-guide-EN.pdf

Cytomic Patch

You can find more information in the **Cytomic Patch settings** chapter of the Advanced EDR and Advanced EPDR online help files.

Cytomic Encryption

You can also see the **Cytomic Encryption (device encryption)** chapter of the Advanced EDR and Advanced EPDR Administration Guides.

Cytomic SIEMConnect

Infrastructure Guide:

https://info.cytomicmodel.com/resources/guides/SIEMConnect/en/SIEMCONNECT- Manual-EN.pdf

Event Description Guide:

https://info.cytomicmodel.com/resources/guides/SIEMConnect/en/SIEMCONNECT-EventDescriptionGuide-EN.pdf

Table of contents

Chapter 1

Preface

The Administration Guide contains basic information and procedures to help you get the most out of Cytomic Nexus.

CHAPTER CONTENTS

Audience

This document is aimed at all audiences:

- Partners (distributors) with a contractual relationship with Cytomic, in order to aid remote provisioning and management of security solutions for their clients.
- Large organizations with IT security management delegated in each department or office, and who wish to have centralized control over compliance with security regulations across the whole organization.

What is Cytomic Nexus?

Cytomic Nexus is a cloud-based solution that offers partners and large organizations simple and centralized management of the lifecycle of clients and users, from assigning trial versions to remotely configuring products. All this in a very simple way and from a single centralized Web console available anytime, anywhere.

Icons

The following icons are used in this guide:

Explanations and additional information, such as an alternative method for performing a certain task.

Suggestions and recommendations.

See other chapter or section in the guide for more information.

Chapter 2

Cytomic Nexus basic information

Cytomic Nexus is a product aimed at service providers and large companies that want to manage clients' and users' security solutions centrally with a single tool.

In addition, Cytomic Nexus helps configure and monitor IT security for large companies with offices where the security service has been delegated to local technicians.

CHAPTER CONTENTS

Cytomic Nexus benefits

Cytomic Nexus is a service that Cytomic makes available to its partners and key accounts in order to help them manage their clients and the security products purchased by them. The service provides the following benefits:

- Simplifies monitoring of clients as well as remote offices and departments.
- Increases efficiency of operations.
- Aids the sale and adoption of Cytomic security products.
- Improves recognition and satisfaction of clients and users.
- Re-centralizes security services.

Simplifies monitoring of clients and remote offices or departments

- Streamlines the partner's relationship with clients by storing all information required for daily client management (contact information, etc.) in a single tool.
- Improves the organization and efficiency of partners and the technical departments of large companies with a system of roles and groups. Sets different access permissions for the Web console user and levels of visibility of clients or remote offices.
- Sends alerts proactively whenever systems are unprotected, displaying key status information in real time about clients and remote offices: products and assigned modules, licenses used or about to expire, renewals pending, etc.

Increased operation efficiency

- Reduces the need to go to clients' premises as it allows for remote installation and maintenance, as well as providing automatic product updates.
- Reduces the time spent managing security of clients and remote offices as it allows for central assignment of the same settings to multiple clients.
- Reduces costs and minimizes the learning curve for technicians by providing a single tool for managing the entire sales cycle and the security of clients and remote offices.

Aids the sale and adoption of Cytomic security products

- **Greater turnover of sales assets** and faster adoption of new technologies: enabling assignment of trial licenses of Cytomic products during the same call as they are offered to the client.
- **Greater operational simplicity** : it is no longer necessary to request approval from the software vendor when assigning Cytomic product licenses.
- **Greater flexibility**: it is possible to work with different license durations and cross-sell Cytomic solutions.

Increases client and user satisfaction and loyalty

The benefits obtained from using Cytomic Nexus are felt by clients and users:

- Greater peace of mind for clients and users, who feel protected and properly managed at all times.
- More satisfied clients and users, which results in recommendations to new clients.
- Make the partner's or company's technical department visible to the client by customizing the management console and protection with their brand image.

Recentralization of the security service

In large companies where the security service has been delegated to each office or department, Cytomic Nexus ensures that management can be centralized in a single console with the following benefits:

- Greater control over the security service offered globally in the company.
- Homogenized security criteria by centrally establishing the basic security guidelines to be applied in all offices.
- Increased security by centrally monitoring the results of security policies applied across the company's offices.
- Management of specific cases through centralized access to the Web console of each department / office.

Cytomic Nexus features

Flexible model for managing product licenses

Support for multiple licensing models based on the requirements of the key account or the business model that the partner has implemented.

- **Monthly licensing model:** The licenses assigned to clients are invoiced to the partner monthly. The licenses don't expire and they last until the partner withdraws them from the client.
- **Annual licensing model**: Licenses are assigned to clients for 1, 2, or 3 years, and they are invoiced to the partner at the beginning of the period. They can be renewed manually whenever required or automatically when they expire.
- **Simplified licensing model**: The partner or key account does not want to manage the commercial licenses of clients or users and delegates this task to Cytomic. They can only assign trial licenses from the Cytomic Nexus Web console. Other operations are carried out by phone or email through the assigned salesperson.

Product lifecycle management

Create and assign trial versions directly from the Web console. Automatically renew client and user licenses to enhance options for cross-selling and upselling.

Security management

Install and deploy services remotely, saving travel costs and optimizing staff time. Configure the security solution installed on clients' computers individually or massively for all computers, reducing management time.

In large companies where security management has been delegated to the different offices or departments, Cytomic Nexus enables centralization of protection guidelines.

Client and client group creation and management

Register new clients and organize them into groups to configure and manage their security service faster.

Centralized management from a single Web console

Cytomic Nexus is configured through a Web console. As a cloud service, it can be accessed from anywhere, at anytime, from a supported Web browser. As such, there is no need for going out on-site or for specific network configurations.

Assigning and renewing licenses

Create and delete clients and their contracted services. Automatically renew the assigned licenses depending on the chosen license model.

Centralized deployment of settings from the Web console

Design flexible, detailed security policies by creating all settings required to cover the diverse needs of the branch offices in your company. Streamline deployment of security policies by centrally pushing settings to groups of clients with the same needs.

Centralized sending of scan and Cytomic Patch tasks

Create scan tasks and install operating system and third-party software updates for all clients you manage. Get a consolidated view of task results.

Access to each branch office Web console

Access all the Web management consoles of the security products installed at each branch office to manage specific situations or provide special treatment to specific users.

Security monitoring

Monitor and check through a single integrated view the status of the protection installed on the computers of clients and remote offices. This allows you to:

- Monitor protected computers and the groups they belong to.
- View purchased licenses, used licenses and the next expiration date of client's licenses.
- Check the status of the protections installed on computers.
- View the percentage of computers where the antivirus engine or the signature file is out of date, and the percentage of computers with errors, including errors that may have occurred during the protection installation process.
- Visualizar la distribución de los riesgos detectados en los equipos de cada cliente.

Customization of clients' consoles (Co-branding)

Change the look and feel of clients' products to reinforce brand image.

Supported products

Advanced EPDR

Advanced EPDR is a solution based on multiple protection technologies that replaces and fills the gaps of traditional antivirus solutions, protecting computers against all types of malware, including APTs (Advanced Persistent Threats) and other advanced threats. To do that, Advanced EPDR monitors and classifies all processes run on IT networks based on their behavior and nature. The service protects workstations and servers by allowing only those programs classified as trusted to run. Additionally, the product provides the following features:

- User productivity control: The service can prevent access to Web resources unrelated to the company's activity and filter corporate email to prevent spam-related performance loss.
- Application control, firewall, intrusion detection system, and anti-theft system for mobile devices (smartphones and tablets).
- Monitoring, forensic analysis and remediation tools to determine the scope of detected issues and resolve them.
- Cloud-based, cross-platform service compatible with Windows, macOS (on the Cytomic platform), Linux, iOS and Android devices, as well as with persistent and non-persistent VDI environments (on the Cytomic platform).

Advanced EPDR covers the security needs of all types of devices with a single tool. Additionally, it doesn't require new IT infrastructures on the company's premises for management and maintenance, significantly reducing the solution's TCO.

Advanced EDR

Advanced EDR is a solution based on multiple protection technologies that complements traditional antivirus solutions, protecting computers against all types of malware, including APTs (Advanced Persistent Threats) and other advanced threats. To do that, Advanced EDR monitors and classifies all processes run on IT networks based on their behavior and nature. The service protects workstations and servers by allowing only those programs classified as trusted to run. Additionally, it incorporates monitoring, forensic analysis and remediation tools to help determine the scope of detected issues and resolve them.

Finally, Advanced EDR doesn't require new IT infrastructures on the company's premises for management and maintenance, significantly reducing the solution's TCO.

Cytomic Insights module

Advanced EDR allows all the information collected from the client's computers to be automatically and seamlessly sent to Cytomic Insights , a service designed to store and leverage security knowledge.

All actions triggered by the processes run across the IT network are sent to Cytomic Insights, where they are analyzed and correlated in order to extract security intelligence. This provides administrators with additional information about threats and the way users use corporate computers. This information is delivered in the most flexible and visual way to make it easier to understand.

Cytomic Insights module

This module is designed to help organizations comply with the data protection regulations governing the storage and processing of personally identifiable information (PII).

Cytomic Data Watch discovers, audits and monitors the entire lifecycle of PII files in real time: from data at rest to data in use (the operations performed on personal data) and data in motion (data exfiltration). With this information, Cytomic Data Watch generates an inventory showing the evolution of the number of files with personal data found on each computer on the network.

Cytomic Insights module

This service reduces the attack surface of the Windows workstations and servers in the organization by updating the vulnerable software found on the network (operating systems and third-party applications) with the patches released by the relevant vendors.

Additionally, it finds all programs on the network that have reached their EOL (End of Life). These programs pose a threat as they are no longer supported by the vendor and are a primary target for hackers looking to exploit known unpatched vulnerabilities. Administrators can easily locate all EOL programs in the organization and design a strategy for the controlled removal of this type of software.

Also, in the event of compatibility conflicts or malfunction of the patched applications, Cytomic Patch allows organizations to roll back/uninstall those patches that support this feature, or exclude them from installation tasks, preventing them from being installed.

Cytomic Encryption module

The ability to encrypt the information held in the internal storage devices of computers is key to protecting the data they contain. This additional protection is critical in case of loss or theft of devices or when systems are disposed of without properly deleting data. Cytomic Encryption leverages BitLocker technology to encrypt hard disk contents at sector level, centrally managing recovery keys in the event of loss or hardware configuration changes.

Cytomic Encryption lets you use the Trusted Platform Module (TPM), if available, and provides multiple authentication options, adding flexibility to computer data protection.

Cytomic Insights module

This module centralizes, in the partner’s SIEM solution, all detections, processes, and programs run on the partner’s clients’ devices.

To detect the appearance of malware, security service providers need a high level of visibility into the activity that occurs on clients’ computers. This enables them to anticipate the problems caused by the advanced threats that proliferate in corporate environments. Cytomic SIEMConnect fo Partners provides the following features to help security service providers achieve that objective:

- Anticipates potential security problems by finding run programs that have not yet been classified as goodware or malware, and getting information about how they reached computers (infection vector).
- Receives IOA (Indicators of Attack) alerts and detects suspicious activity, such as Windows registry modifications or driver installations.
- Monitors the execution of legitimate software often exploited by attackers to go unnoticed on clients' networks, such as scripting or remote access tools.

Cytomic SIEMConnect fo Partners simplifies operations for the partner's SOC and provides the following benefits:

Comprehensive visibility of everything that is run on clients' devices

This module helps monitor and manage security. It detects anomalies continuously in each client's execution environment.

Centralized configuration

Centralized management console (Cytomic Nexus) that enables partners to configure Cytomic SIEMConnect fo Partners settings for clients easily and visually.

Easy to install, secure, and scalable

Configure the telemetry download service only once and add new clients without having to deploy or install any additional components on their infrastructures. Safe downloads via secure TLS (Transport Layer Security) connections from the Cytomic cloud.

Reduced SIEM storage costs

It filters required events before they reach the security service provider's infrastructure, minimizing storage costs.

Compatible with most SIEM solutions on the market

It downloads telemetry in the LEEF and CEF formats, compatible with the leading SIEM solutions on the market such as QRadar, AlienVault, Splunk, Devo, etc., and natively with ArcSight.

Cytomic Nexus product user profile

Cytomic Nexus is aimed at partners or technical departments in large companies who wish to manage their clients' and offices' security simply and effectively, from a single console and with maximum vendor autonomy.

Types of Cytomic Nexus users

- **Resellers**: Partners who purchase Cytomic product licenses and sell them to their clients without adding value.
- **Managed Service Providers (MSP)**: Partners who sell Cytomic products to their clients and manage their security proactively.
- **Distributors**: Partners who buy large numbers of licenses. They then sell those licenses among their partners, who in turn sell them to end clients. Distributors keep a stock of licenses to quickly respond to the everyday license needs of their partners.
- **IT departments**: These are teams that normally operate from the head offices of large companies. They define, implement and monitor the security policies that are applied in all the company's offices and departments.

Chapter 3

Management console

Cytomic Nexus uses Web technology to provide partners with a cloud-based, easy-to-use centralized management console.

CHAPTER CONTENTS

Benefits of the Web console

The management console, also called ‘Web console’, or simply ‘console’ is the main tool used to assign and manage clients’ services. As it is a centralized Web service, it offers a series of features that improve the user experience.

A single tool for complete product management

The Web console enables you to configure security policies for your clients, centrally assign protection settings to users’ computers, and customize clients’ services. It also enables you to generate detailed lists about security status and configure their content.

All these features can be accessed from the Web console, eliminating the complexity of having to use various management tools from different vendors. With Cytomic‘s Web console, products can be managed centrally, remotely and with a single tool.

Centralized management for all clients and roaming users

The Cytomic Nexus Web console is hosted in the cloud, so there is no need to perform additional installations on users' premises or remote offices, nor configure VPNs or change corporate router settings.

Neither is it necessary to invest in hardware or database/operating system licenses, or take care of maintenance/warranty management tasks to ensure the service stays operational 24/7.

Security management from anywhere at anytime

As this is a cloud service, the Web console user can manage clients' products and security and remote offices from anywhere at any time from a compatible Internet browser.

Web console requirements

To access the Web management console, the following requirements must be met:

- Have valid credentials (user name and password).
- Supported browser.
- Internet connection and communication through port 443.

Supported browsers

To access the Cytomic Nexus Web console, we recommend that you use the latest version of any of the following supported browsers:

- Chrome
- Internet Explorer
- Microsoft Edge
- Firefox

Other browsers not listed may also be supported, such as Safari, Opera, etc.

Accessing the Web console

Cytomic Nexus is accessed from Cytomic Central (**https://central.cytomic.ai**), the centralized access point for all Panda Security's cloud-based services.

Account information and logout

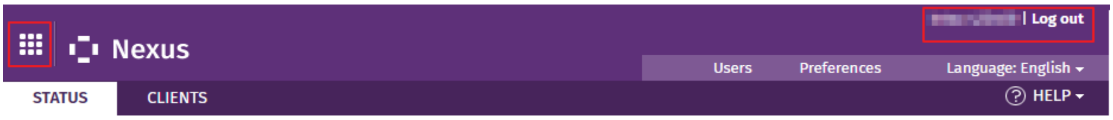


Figure 3.1: Logged-in user, logout option and access to Cytomic Central

At the top of the window you can see at all times the name of the account that is logged in to the Web console, and the option to log out:

- ▦ Takes you back to the Cytomic Central page. Refer to chapter **The Cytomic account** on page **153** for more details.
- **User name**: This shows the Web console user who logged in to the service.
- **Log out**: This logs you out and takes you back to the Cytomic Central login page.

Web console general structure

The Cytomic Nexus Web console is an easy-to-use tool that allows users to centrally and remotely manage the products assigned to their clients and the security of their devices.

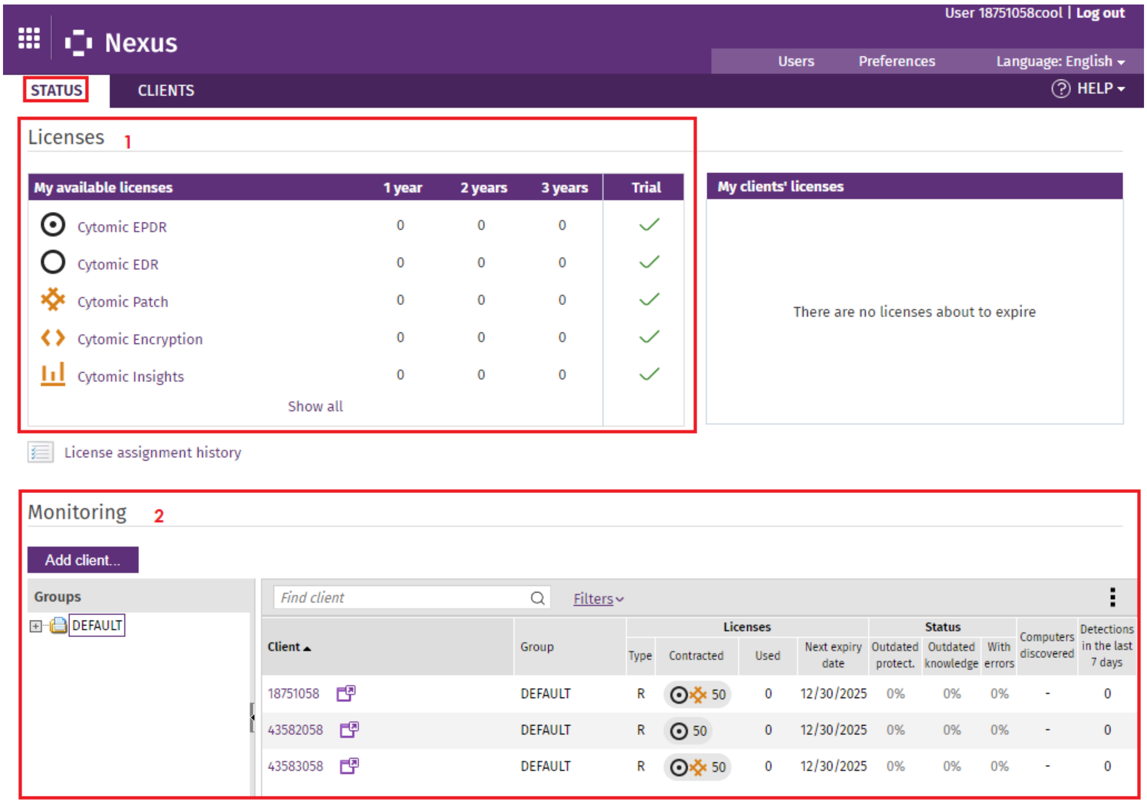
Below is a description of the console's basic features and how to use them:

Introduction

When accessing the Web console, the first thing you'll see is the main window, which corresponds to the **Status** tab in the top menu.

The main window provides a summary of the general status of clients, as well as the number of licenses available which have not yet been assigned. The main window is divided into two areas:

- The **Licenses** area (1)
- The **Monitoring** area (2)



User 18751058cool | Log out

Nexus

Users Preferences Language: English

STATUS CLIENTS HELP

Licenses 1

My available licenses	1 year	2 years	3 years	Trial
Cytomic EPDR	0	0	0	✓
Cytomic EDR	0	0	0	✓
Cytomic Patch	0	0	0	✓
Cytomic Encryption	0	0	0	✓
Cytomic Insights	0	0	0	✓

Show all

My clients' licenses

There are no licenses about to expire

License assignment history

Monitoring 2

Add client...

Groups

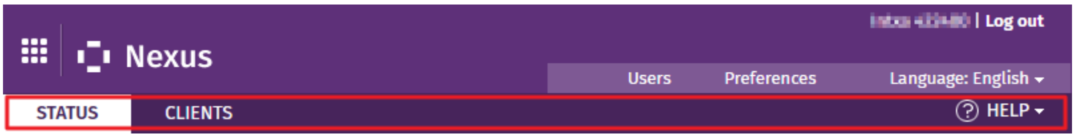
DEFAULT

Find client Filters

Client	Group	Licenses: Type	Licenses: Contracted	Licenses: Used	Licenses: Next expiry date	Status: Outdated protect.	Status: Outdated knowledge	Status: With errors	Computers discovered	Detections in the last 7 days
18751058	DEFAULT	R	50	0	12/30/2025	0%	0%	0%	-	0
43582058	DEFAULT	R	50	0	12/30/2025	0%	0%	0%	-	0
43583058	DEFAULT	R	50	0	12/30/2025	0%	0%	0%	-	0

Figure 3.2: Main Web console window

Top menu



[redacted] | Log out

Nexus

Users Preferences Language: English

STATUS CLIENTS HELP

Figure 3.3: Top menu

This is the main menu of the Web console. It lets you navigate the main sections of the product:

Status

View a summary of the client status. The information displayed about the licenses that can be sold or assigned to clients or offices will depend on the licensing model chosen by the partner or the organization.

Click the **Status** tab to:

- Show information about the licenses available.
- Access the license assignment history.
- Monitor licenses in the process of being assigned.
- Check the status of the protections installed on computers.

Clients

Lets you manage clients, as well as products, modules and licenses.

Use the **Clients** tab to:

- Register new clients.
- Organize clients into groups.
- Assign, change and renew licenses.
- Group license contracts.
- Create security settings profiles and push them to clients' workstations.

Refer to chapter ***Client management*** *on page* ***39*** *for more details.*

Help

This menu provides:

- Access to the Cytomic Nexus Web help.

http://nexus-documents.cytomic.ai/Help/v77000//Partners/en-us/index.htm

- Access to the Cytomic Nexus Administration Guide.

http://nexus-documents.cytomic.ai/AdvancedGuide/Nexus-Manual-EN.pdf

- Information about new features in Cytomic Nexus.

http://documents.managedprotection.pandasecurity.com/ReleaseNotes/v77000/Partners/ReleaseNotes.html

- Access to the license agreement
- Information about the Cytomic Nexus version available.

Other options menu

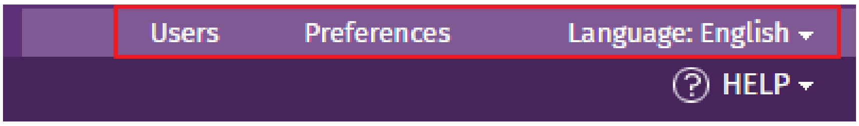


Figure 3.4: Other options menu

Users

Create users and assign them access permissions to the Web console. For more information, refer to chapter **Access and authorization in Cytomic Nexus** on page **29**.

Preferences

Configure general aspects of the Web console.

Default views

Defines the way clients and computers are displayed in the Web console.

Email notifications

Sends a report, on the 1st of each month, with the number of clients' licenses that have expired or are due to expire shortly. Refer to section **Email alerts about licenses about to expire** on page **60** for more information.

Access permission for Cytomic

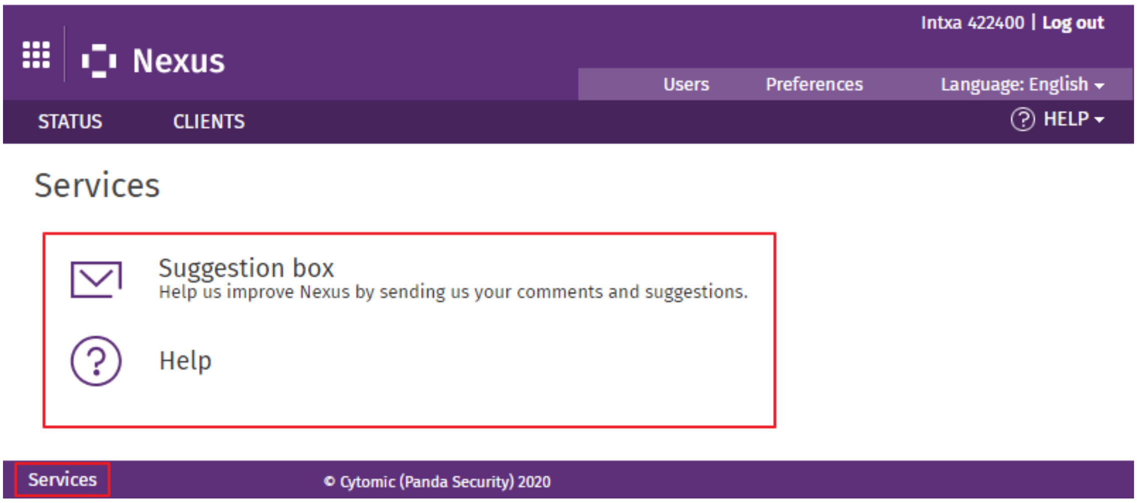
Allows Cytomic's technical staff to access the user's Web console for troubleshooting purposes.

Language

Select the language of the Web console. Supported languages are:

- German
- English
- Spanish
- French
- Italian
- Portuguese
- Swedish
- Polish
- Japanese
- Simplified Chinese
- Traditional Chinese

Services



Help us improve Nexus by sending us your comments and suggestions.

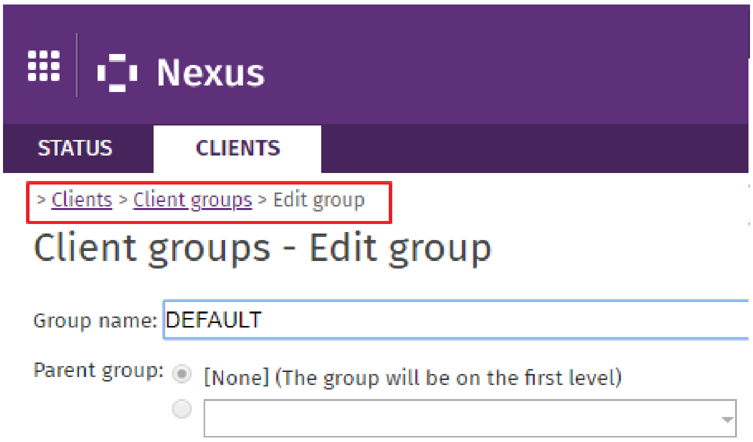
Figure 3.5: Cytomic Nexus services

Click the **Services** link at the bottom of the Web console and select:

- **Suggestion box:** Send suggestions to the Cytomic team responsible for designing and developing Cytomic Nexus.
- **Help:** Access the Cytomic Nexus Web help.

Breadcrumb bar

This is a navigational element that shows the full path to the current window in the Web console.


Nexus
STATUS
CLIENTS
> Clients > Client groups > Edit group
Client groups - Edit group

Group name: DEFAULT

Parent group: ● [None] (The group will be on the first level)
○

Figure 3.6: Breadcrumb bar

The breadcrumb bar shows the names of the windows the user has gone through to reach the current location, separated by the symbol “>”.

Hyperlinks are used to allow the user to jump directly to any previous window without the need to go back to the starting point.

Other interface elements

The web console uses standard interface elements for configuring settings, such as:

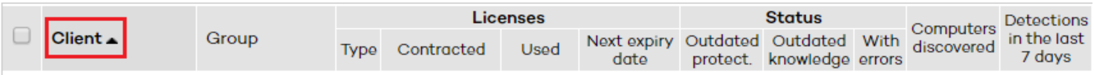
- Drop-down lists
- Combo boxes
- Buttons
- Text boxes
- Lists

Text boxes

On many occasions, the console checks the text you enter in text boxes to verify it has the right format (presence of the "@" character in text boxes for entering email addresses, checking of numeric data, etc.).

Lists

Cytomic Nexus uses tables to present data in lists. All tables have headers for sorting the items in the list:

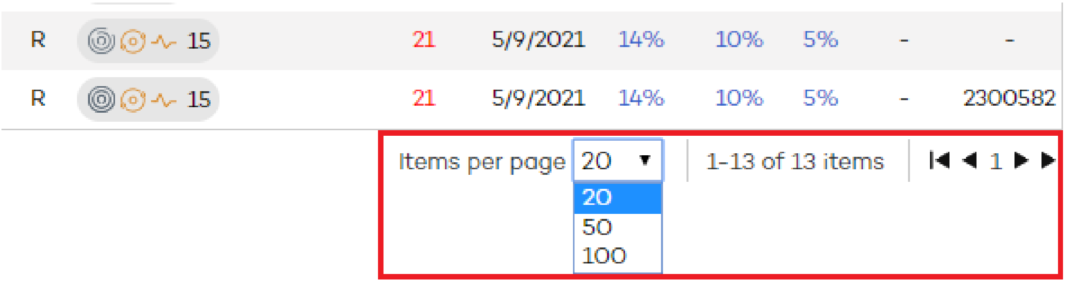


☐	Client ▲	Group	Licenses				Status			Computers discovered	Detections in the last 7 days
			Type	Contracted	Used	Next expiry date	Outdated protect.	Outdated knowledge	With errors		

Figure 3.7: Table header

Click a header in the list to sort the information in the table in ascending order based on the data contained in that particular column. Click the same header a second time to switch between ascending and descending order.

The bottom of the table shows a pagination tool.



R	15	21	5/9/2021	14%	10%	5%	-	-
R	15	21	5/9/2021	14%	10%	5%	-	2300582

Items per page 20 ▼ | 1-13 of 13 items | ⏮ ◀ 1 ▶ ⏭

20
50
100

Figure 3.8: Pagination tool

The features included in the pagination tool vary depending on the table:

- Rows per page selector
- Shortcuts to specific pages
- Next page link
- Previous page link

- Last page link
- First page link

Chapter 4

Access and authorization in Cytomic Nexus

This chapter describes the resources implemented in Cytomic Nexus to control and monitor the actions taken by users of the Web management console.

This monitoring and control is implemented through the following two resources:

- User account.
- Roles assigned to user accounts.

CHAPTER CONTENT

What is a user account?

A user account is a resource managed by Cytomic Nexus, comprising a set of data which the system uses to control users' access to the Web console and to determine which actions they can perform on clients and the managed computers.

User accounts are used only by those accessing the Cytomic Nexus Web console. Each user will need at least one user account to access the console, although they can have more than one account with different access levels.

User account structure

A user account consists of the following items:

- **Account login name**: Assigned on creating the account, its aim is to identify the user accessing the console.
- **Account password:** Assigned once the account is created, its aim is to control access to the management console.
- **Assigned permissions**: Assigned once the user account is created, they determine which actions the user can take using the Web console.
- **Visibility**: Establishes which client groups the administrator can act upon with the user account.

Primary user

This is the first user account created through the welcome email received from Cytomic. It has the following structure:

- **Account name**: Contact email address of the user who contracted the service.
- **Account password**: Set through the activation email.
- **Assigned permissions**: **Total control**, explained in section **Types of permissions**.
- **Client groups**: Shows the console user's visibility of client groups.

What are permissions?

Permissions are a specific configuration for accessing the console, applied to one or more user accounts. They regulate the resources a technician or sales representative can view or edit, based on the permissions assigned to the user account with which they accessed Cytomic Nexus.

Each user account is assigned a unique set of permissions, although this set of permissions can be assigned to one or more user accounts.

The permissions discussed in this chapter also affect management of Endpoint family clients from Cytomic Nexus. For more information, refer to chapter ***Endpoint security product settings management*** *on page* ***69***

Structure of a set of permissions

A set of permissions consists of the following items:

- **Name**: Provides a brief summary of the Web console features accessible to the user accounts with these assigned permissions.
- **Groups the permissions grant access to**: Lets you restrict access to certain clients. Select the folders in the group tree that the user account will have access to.
- **Type of permissions**: Determines which actions the user accounts with these assigned permissions can perform on clients.

Why are permissions necessary?

In a small department, all technicians will typically access the console as administrators without any type of restriction. However, in mid-sized or large departments with a wide network of clients to manage, it is highly likely that it will be necessary to organize or segment access to clients, based on some or all of the following criteria:

Based on the size of the clients to manage.

Mid-sized or large clients may need to have dedicated teams of technicians exclusively assigned to them. This is so that the devices managed by a particular technician are invisible to technicians managing other clients' devices.

Based on the type of client

It may be necessary to set access restrictions to certain clients based on their type of business, or based on whether they handle confidential information. The latter case often requires careful assignment of the technicians who will be able to access devices with such data.

Based on the technology used by the client to manage.

Based on the infrastructure deployed at the client's premises, it may be necessary to assign the client technicians specialized in a specific technology: for example, clients using Exchange mail servers can be assigned expert technicians in that field, whereas clients with Android devices can be assigned a different team of technicians.

Based on the knowledge or profile of the technician.

Based on each technician's skills or role, you can assign monitoring/read-only permissions to them, or more advanced permissions that allow them to edit the services contracted by clients. For example, large departments often have groups of technicians dedicated exclusively to configuring the security solutions installed on their clients' devices. Whereas other employees with a more salesoriented profile assign trial licenses to potential clients in order to expand their client base, or modify the license contracts of existing clients, renewing them when their expiration dates approach.

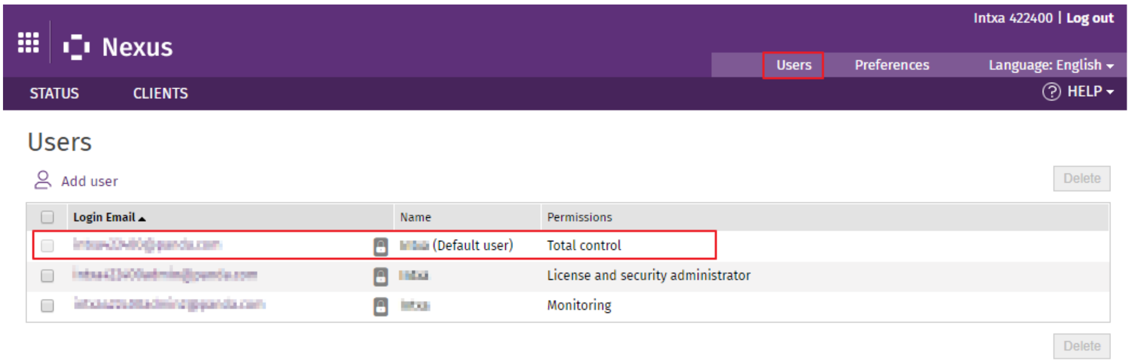
These criteria can overlap, generating a flexible, easily-established, and low-maintenance settings matrix which enables console features to be defined perfectly to ensure accessibility to each technician based on the user account they use to access the system.

Total control role

All Cytomic Nexus licenses come with the **Total control** role assigned. The default administration account also has this role assigned. This account makes it possible to perform absolutely every action available in the Web console on all clients.

User management

To manage users and their permissions, select **Users** from the **Other options** area:



Users

☐	Login Email ▲	Name	Permissions
☐	[redacted]	[redacted] (Default user)	Total control
☐	[redacted]	[redacted]	License and security administrator
☐	[redacted]	[redacted]	Monitoring

Figure 4.1: Users list

Adding a user

To create a user:

Select **Users** from the **Other options** area. Click the **Add user** link and enter the required data:

- **Login email**: This is used as the user name.
- **Comments**: Here you can add additional information.
- **Permissions**: Select the permissions you want to assign to the user. For more information, see section **Types of permissions**.
- **Client groups**: Select the client groups/subgroups the user will be able to take action on. Users with total control permissions can act on all groups.

If you create a user with permissions on a group and all of its subgroups, and later you add a new subgroup to it, the user is automatically granted permissions on that subgroup as well. If you create a user with permissions on some subgroups in a group, and later you add a new subgroup to it, the user is NOT automatically granted permissions on the new subgroup.

- Click **Add**. A message appears informing you that an email message has been sent to the address specified when you created the user.

After you create the user, it appears on the list shown in the **Users** section.

Editing a user data

Select **Users** from the **Other options** area. Click the name of the user whose data you want to edit. The **Edit users** page opens. You can edit this data:

- The text entered in the **Comments** field.
- The type of permissions.
- The group the user belongs to.

*In the case of the primary or default user, you can edit only the contents of the **Comments** field.*

Editing a user account authorization information

To edit the name, password, email address, or two-factor authentication status of a user, go to Cytomic Central (**https://central.cytomic.ai**). For more information, see chapter **The Cytomic account** on page **153**.

Deleting a user

To delete a user:

- Select **Users** from the **Other options** area. Select the checkbox next to the user you want to delete.
- To delete all users, select the checkbox located at the top of the table, next to the **Login email** column.
- Click the **Delete** button.

Note that you cannot delete either the default user or the active user (the user whose credentials you have used to access the web console).

Requiring two-factor authentication

From the moment you require two-factor authentication in the organization, the console user must have an additional device and a code generator program, such as WatchGuard AuthPoint, to access the console.

To require two-factor authentication for all users that access the Cytomic Nexus console:

- From the top menu, select **Users**. A page opens that shows a list of all users created in Partner Center.
- Select the checkbox **Require users to have two-factor authentication enabled to access this account** . If the user account that enables the feature does not have two- factor authentication enabled, a warning message appears. See **Enabling two- factor authentication**.

When you enable two-factor authentication, any user that is logged in to the console is logged out and must log back in using two-factor authentication.

Enabling two-factor authentication

To enable two-factor authentication in a Cytomic Nexus user account:

- Download the WatchGuard AuthPoint app for free from **https://play.google.com/store/apps/details?id=com.watchguard.authpoint** (for Android) or from **https://apps.apple.com/app/watchguard-authpoint/id1335115425** (for iOS).
- Go to Cytomic Central:
  - Enter your company credentials at **https://central.cytomic.ai**.
- Click the 👤 icon in the upper-right corner of the page. A menu appears.
- Select **Set up my profile**. The **Panda Account** page opens.
- From the left panel, select **Login** . Click the **Enable** link. The **Synchronization using an authentication app** dialog box opens.
- If this is your first time using the WatchGuard AuthPoint app on your mobile device, tap the **Activate** button. If you have used it before, tap the QR icon in the upper-right corner. Your device camera opens.

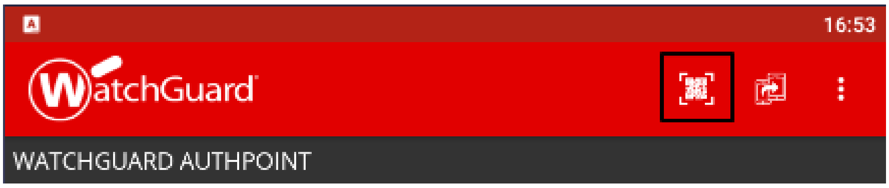


Figure 4.2: Scan QR code

- Point the camera on your device at the QR code in the Cytomic Nexus console. A new entry is added in WatchGuard AuthPoint and the app generates a one-time token every 30 seconds.
- Enter the code generated by WatchGuard AuthPoint in the Cytomic Nexus console to link the device to your user account. Click the **Verify** button. A dialog box opens that shows the message **Two-factor authentication is enabled**.
- Click **OK**. After this, the console user is required to enter an email address, a password, and the token generated by WatchGuard AuthPoint before they are able to access the console.

Types of permissions

Cytomic Nexus supports four types of permissions:

- Total control
- License and security administrator
- Security administrator
- Monitoring (read-only)

Depending on the permissions assigned to a user, they will be able to perform more or fewer actions via the Web console.

The actions a user can take are related to various aspects of the protection's basic and advanced settings. They range from creating and editing their own user credentials to configuring and assigning profiles to groups and computers, etc.

Total control

This user is authorized to perform all actions available in the Web console on all of the partner's clients. This is the only permission in the Web console that allows users to create other users.

User, group and client management

This user can:

- Create, edit and delete any user except for deleting the default user and the active user.
- Create, edit and delete any group except for the DEFAULT group.

- Create, edit and delete any client.
- Assign clients to groups and move clients from one group to another.

License management

This user can:

- Edit the license assignment type for any client. Refer to section **Assigning and modifying licenses** on page **57**.
- Access the license assignment history and view the licenses assigned to any client. Clear the history for any client.
- Assign, change and delete licenses for any client.
- Assign, change and delete products / services for any client.

Profile management

This user can:

- Access all clients' Web consoles with total control permissions.
- Manage automatic updates of any client's profile.
- View all clients' profiles and assign profiles to any client.

License and security administrator

This user has the same permissions as a **Total control** user (authorization to perform all actions available in the Web console), but limited to those clients the user has access to. This user cannot create other users.

User, group and client management

This user can:

- Edit their own credentials.
- Manage and delete those groups they have access to, except for the DEFAULT group.
- Create, delete and edit those clients they have access to.
- Use the **Comments** field to enter additional data about clients. Additionally, view other data they have permissions on (name, contact phone, fax, etc.)
- Access the Web consoles of those clients they have access to, with total control permissions.

License management

This user can:

- Edit the license assignment type for those clients they have access to. Refer to section **Assigning and modifying licenses** on page **57**.
- Access the license assignment history and view the licenses assigned to those clients they have access to. Clear the history for those clients.
- Assign, change and delete licenses for those clients they have access to.
- Assign, change and delete products for those clients they have access to.
- Assign, change and delete services for those clients they have access to.

Profile management

This user can:

- Access the Web consoles of those clients they have access to, with total control permissions.
- Manage automatic updates of the profiles of those clients they have access to.
- View the profiles of those clients they have access to and assign profiles to them.

Security administrator

Users with this permission assigned can manage the security of those clients they have access to. However, they can't manage their licenses, they can only view them. Nor can they create users via the Web console.

User, group and client management

This user can:

- Edit their own credentials.
- Manage and delete those groups they have access to, except for the DEFAULT group.
- Use the **Comments** field to enter additional data about clients. View other data related to the clients they have permissions on (name, contact phone, fax, etc.)

License management

This user can:

- Access the license assignment history and view the licenses assigned to clients belonging to groups they have access to. However, they cannot clear the assignment license list.

Profile management

This user can:

- Access the Web consoles of those clients they have access to, with total control permissions.
- Manage automatic updates of the profiles of those clients they have access to.

Monitoring (read-only)

Users with monitoring permissions cannot create, delete or modify any information in the Web console.

User, group and client management

This user can:

- Edit their own credentials.
- Access the groups assigned to them, and view the clients in those groups as well as their profiles.
- View the contents of the **Comments** field as well as other data related to the clients they have access to (name, contact phone, fax, etc.)

License management

This user can:

- View the licenses automatically renewed to clients in groups they have access to.
- Access the license assignment history and view the licenses assigned to clients belonging to groups they have access to. However, they cannot clear the assignment list.

Chapter 5

Client management

All the functionality provided by Cytomic Nexus is built around the concept of the Client, an entity that represents two groups of users.

- Companies that have contracted security services through the partner.
- Branches, departments or remote offices within a large organization with delegated security management.

The 'client' entity is used to organize all the data as well as to enable monitoring, thereby freeing up resources in technical departments that can be used on more productive tasks.

> *Cytomic Nexus simplified licensing mode does not allow clients to be managed through the Web console. See chapter* ***Product and license management*** *on page* ***49*** *for more details of available licensing modes and their features.*

CHAPTER CONTENTS

Creating and deleting clients

Here we describe the process for Cytomic Nexus users to register clients, assigning a trial version or full product version. The process for deleting clients is also described.

Required permissions

To register and delete clients, the user account has to have Total control or License and security administrator permissions.

> *Refer to section **Adding a user** on page **32** for more information about how to create and delete users, edit their details and assign permissions. Refer to section **Types of permissions** on page **35** to find out the different management levels possible in accordance with the permissions assigned.*

Registering clients

There are two ways to register a client:

- The **Register new client** option in the **Clients** window.
- The **Add client…** option in **Status** > **Monitoring**.

From the Register new client option

- Click **Clients**, and then **Register new client**.

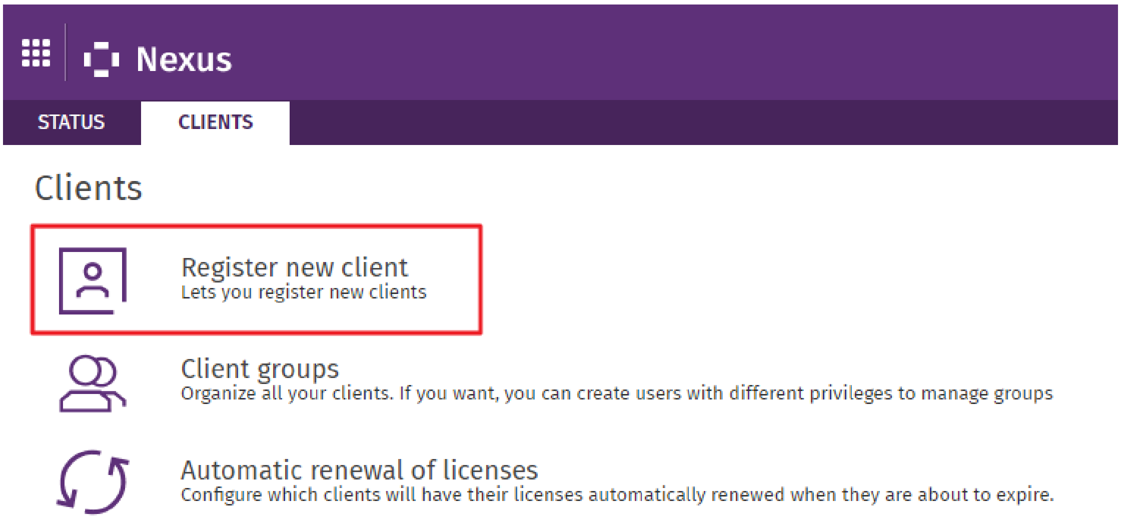

Nexus
STATUS
CLIENTS
Clients
Register new client
Lets you register new clients
Client groups
Organize all your clients. If you want, you can create users with different privileges to manage groups
Automatic renewal of licenses
Configure which clients will have their licenses automatically renewed when they are about to expire.

Figure 5.1: Register new client

- In the registration form, complete the necessary fields to register the client and click **Next**.
- Select the group in which you want to include the client. If no group is configured, select the default group.
- Use the drop-down menus to select:
  - **The type of license you want to assign to the client**: trial or commercial license.
  - **The product**.
  - **The license duration**: 1, 2, 3 years, 1 month.
  - **The quantity of licenses to assign**: If the number exceeds the number of licenses available, a warning will be displayed. .
  - **Additional modules**: Depending on the selected product, it may be possible to assign commercial or trial licenses for modules that offer additional security and features.

> *All the information about the modules available and their features is in section* ***Supported products*** *on page* ***15***.

- To complete the process, click **Add client**.

From the Add client button

- In the **Monitoring** section of the **Status** window, click **Add client**.

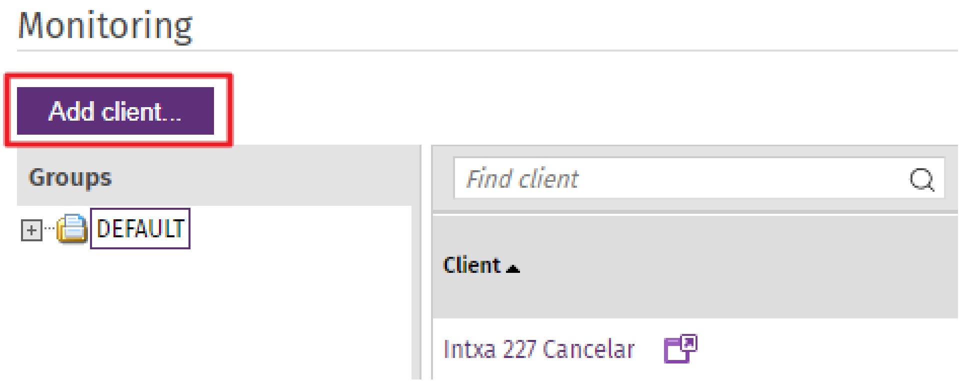


Figure 5.2: Add client

- Complete all the fields in the registration form.
- Use the drop-down menus to assign licenses to the client, as explained above in section **From the Register new client option**.

Once the process is complete, the license contract will automatically be created, and the license validity period will commence.

> *If assignment is not immediate, the following text is displayed on the status screen: **XX licenses being assigned**. **View details**. Clicking the **View details** link will display the details of the license assignments in progress.*

Once licenses have been assigned to a client, they can be modified and others assigned for other Cytomic products and modules.

> *For more information on managing licenses, refer to chapter **Product and license management** on page **49**.*

Deleting clients

During the daily management of clients, there could be times when it is necessary to delete a client.

Consequences of deleting clients

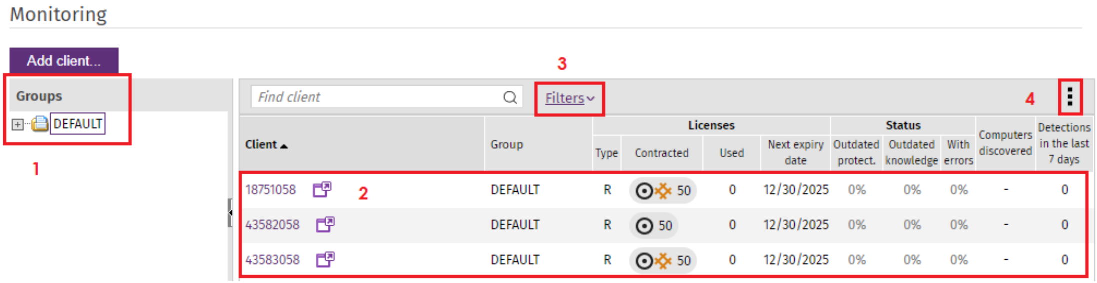
After deleting a client, it will not be possible to:

- Recover their data 90 days after the date the client is deleted.
- Access the console from which the client's services were managed.

Monitoring clients

To see the clients created in the console, select **Status** from the top menu. This information is availble in the **Monitoring** section, which is divided into three main areas:

- The group tree **(1)**
- The list of clients **(2)**
- The filter tool **(3)**



Client ▲		Group	Licenses				Status			Computers discovered	Detections in the last 7 days
			Type	Contracted	Used	Next expiry date	Outdated protect.	Outdated knowledge	With errors		
18751058		DEFAULT	R	50	0	12/30/2025	0%	0%	0%	-	0
43582058		DEFAULT	R	50	0	12/30/2025	0%	0%	0%	-	0
43583058		DEFAULT	R	50	0	12/30/2025	0%	0%	0%	-	0

Figure 5.3: Monitoring clients

For the list to also show the clients that have been inactive for the last 90 days:

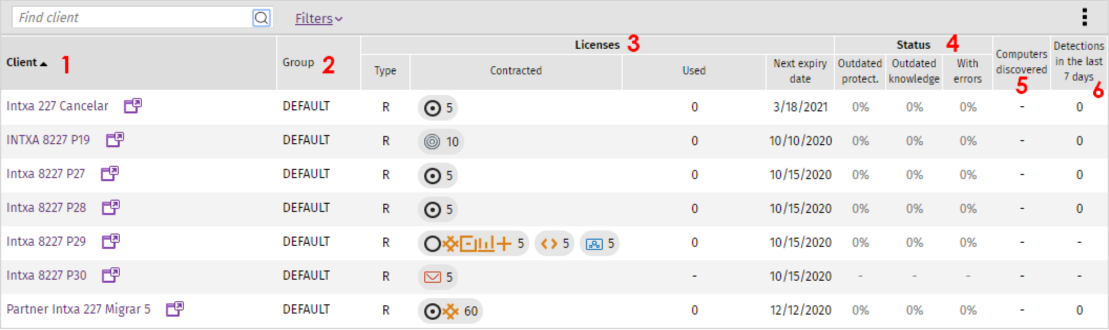
- Click **Filters (3)**.
- Select the **Show clients without active services** checkbox. Click **Filter**.

To show only clients belonging to a specific group, select the group in the tree.

To show all clients in the subgroups that belong to the selected group, click the ⋮ icon **(4).** Select the **Show content of subgroups** option.

Client list

The client list provides the following information:



Client ▲ 1	Group 2	Licenses 3				Status 4			Computers discovered 5	Detections in the last 7 days 6
		Type	Contracted	Used	Next expiry date	Outdated protect.	Outdated knowledge	With errors		
Intxa 227 Cancelar	DEFAULT	R	⊙ 5	0	3/18/2021	0%	0%	0%	-	0
INTXA 8227 P19	DEFAULT	R	◎ 10	0	10/10/2020	0%	0%	0%	-	0
Intxa 8227 P27	DEFAULT	R	⊙ 5	0	10/15/2020	0%	0%	0%	-	0
Intxa 8227 P28	DEFAULT	R	⊙ 5	0	10/15/2020	0%	0%	0%	-	0
Intxa 8227 P29	DEFAULT	R	○✲ + 5 <> 5 5	0	10/15/2020	0%	0%	0%	-	-
Intxa 8227 P30	DEFAULT	R	✉ 5	-	10/15/2020	-	-	-	-	-
Partner Intxa 227 Migrar 5	DEFAULT	R	⊙✲ 60	0	12/12/2020	0%	0%	0%	-	0

Figure 5.4: Client list information

To view complete information about a client, point the mouse to the client name. A label appears that shows the client details.

Field	Description
Client (1)	The name or ID Cytomic assigns the client at registration time. This ID is sent to clients in the welcome email and is requested in all communications between clients and the support department for incident management. : Icon for accessing the client's console if the client has the **Allow my reseller to access my console** option enabled in their product console. See **Accessing the client's console** on page **56**.
Management mode	Indicates whether the product is centrally managed or not. For more information, see chapter **Endpoint security product settings management** on page **69**
Group (2)	Name of the group the client belongs to.
Type	Indicates whether the client has Trial or Release products. If the client has

Field	Description
	both types of products, Release is shown.
Licenses (3)	• **Contracted**: Products or modules purchased by the client and number of licenses. • **Used**: Number of licenses assigned to the client's computers. • **Next expiry date**: Next date on which some or all of the client's licenses expire. • **Outdated protect.**: Percentage of user computers whose protection is out of date.
Status (4)	**Status (4)**: Shows percentages that indicate the status of the protection installed on clients' computers. • **Outdated knowledge**: Percentage of computers whose signature file is out of date. • **With errors**: Percentage of computers with errors in the security software installed. • **Computers discovered**: Percentage of computers found on the network that do not have security software installed.
Detections in the last 7 days (6)	Detections made in the last 7 days in: • File system. • Email. • Web browsing activity. • Instant messaging apps. • Items blocked by the firewall.

Table 5.1: Client list information

> *To access the **Client details** page, click a client's name. For more information, see section **Client details***

Client filter

The filter tool consists of a series of drop-down menus with filter options that determine the search results.

To use the filters, click **Filters** and use the menus to select:

- **Product**: Choose the product to narrow the search by.
- **License type**: Commercial or trial licenses.
- **License status**:
  - Valid.
  - Expired.
  - Licenses that expire in one week, two weeks, or two months.
  - Percentage of licenses used (more than 80% or 100%).
- **Licenses contracted**: Here you can enter a number of licenses as a search parameter.
- **Product management mode**:
  - **All**. All products are shown, regardless of the management mode.
  - **Non-centrally managed products**. See section **Security product settings** on page **73**.

Exporting the client list

- To export the client list, click the icon and select a format.
  - **Export to Excel**
  - **Export to CSV**
- For the list to include information about clients belonging to second-level groups in the client tree, select **Show content of subgroups**.

Client details

- To access this window, click a client name where it appears as a link.

The **Client details** screen shows the following information:

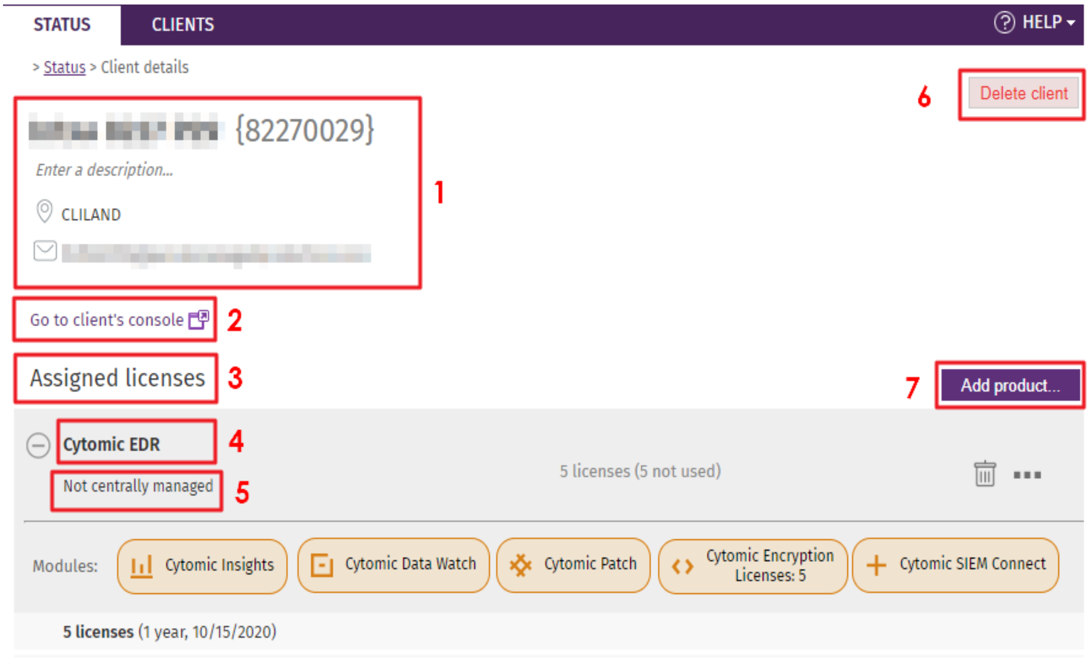


Figure 5.5: Client details

- **Client details (1)**:
  - Name and description of the client.
  - Contact details (fax number, phone number, email address, etc.).
- **Go to client's console (2)**: To access the console, click the ⧉ icon.
- **Assigned licenses (3)**
- Use ⊖ and ⊕ to expand or close the information in each part of the report.
- **Products contracted by the client (4)**: The number of licenses contracted and those not used.
- **Product management model (5)**. Refer to section **Service management models** on page **52**
- **Delete client** button (**6**)
- **Add product** button (**7**)

Creating and managing client groups

Why use client groups?

Cytomic Nexus lets you group clients in order to use two features aimed at improving the management of clients:

- Restricting the visibility of Web console users with regard to the clients they are permitted to manage.

- Making it easier to apply configuration profiles to clients.

Restricting the visibility of Web console users

Technical departments with large, complex internal structures, or who manage a large number of clients, may need to group their clients in order to assign their management to specific technicians. Refer to section **Why are permissions necessary?** on page **31** for information on the various reasons for organizing clients into groups.

Cytomic Nexus allows you to restrict the visibility of Web console users by assigning them certain client groups. As such, they can only see clients who belong to those groups.

Applying configuration profiles

By assigning and sending profiles, Cytomic Nexus enables you to apply configuration profiles to client groups in order to save time. See chapter **Endpoint security product settings management** on page **69** for details of the configuration profiles supported by Cytomic Nexus.

Creating client groups

To create a client group:

- From the top menu, select **Clients**. Select **Client groups**.

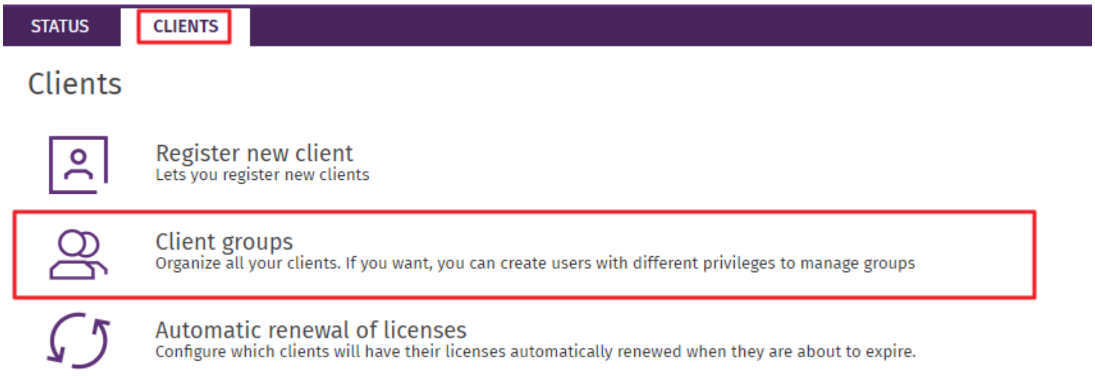
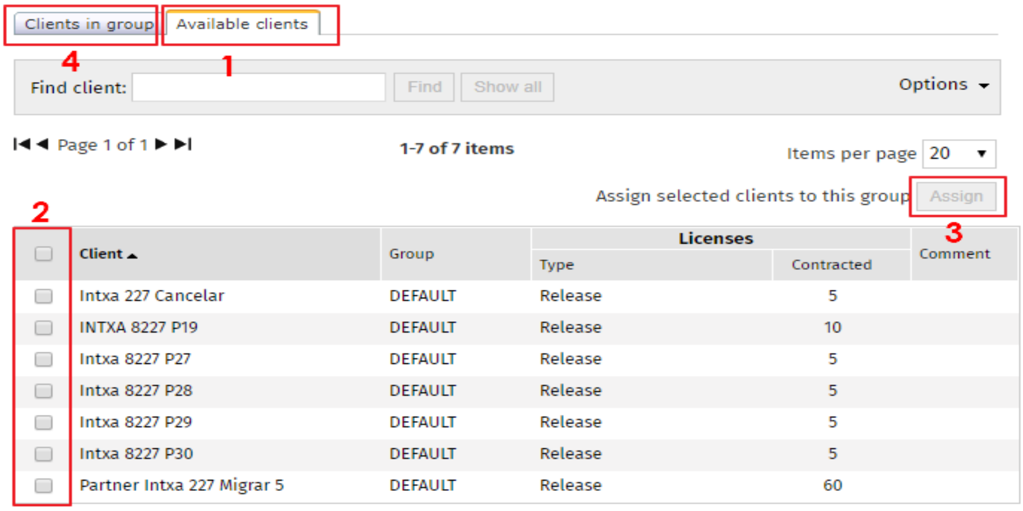

STATUS
CLIENTS
Clients
Register new client
Lets you register new clients
Client groups
Organize all your clients. If you want, you can create users with different privileges to manage groups
Automatic renewal of licenses
Configure which clients will have their licenses automatically renewed when they are about to expire.

Figure 5.6: Creating client groups

- Click the **Create new group** link. The **Client groups - Edit group** page opens. Complete these fields:
  - **Group name**: Specify the name of the new group. You can create multiple client groups with the same name provided they do not belong to the same parent group.
  - **Parent group**: Specify the group to which the new group will belong. For the group to appear at the top level of the group structure, use the option **None (the group will be on the first level)**. For the group to belong to an existing group, select the group using the drop-down menu.



□	Client ▲	Group	Licenses		Comment
			Type	Contracted	
□	Intxa 227 Cancelar	DEFAULT	Release	5	
□	INTXA 8227 P19	DEFAULT	Release	10	
□	Intxa 8227 P27	DEFAULT	Release	5	
□	Intxa 8227 P28	DEFAULT	Release	5	
□	Intxa 8227 P29	DEFAULT	Release	5	
□	Intxa 8227 P30	DEFAULT	Release	5	
□	Partner Intxa 227 Migrar 5	DEFAULT	Release	60	

Figure 5.7: Controls for selecting the clients that will be part of a new group

- Select the clients that will be part of the new group: The **Available clients** tab **(1)** shows a list of clients that you can see depending on your permissions and which do not belong to the group that you are editing/creating. Along with the client name, you can also see the number and type of licenses they have, and any associated comments. To select a client you want to include in the group, use the checkbox **(2)** next to the client name. To include multiple clients, select the checkbox for each client.
- Click **Assign (3)**. Verify the clients appear on the **Clients in group (4)** tab.

Moving clients from one group to another

- Select the **Clients in group** tab **(4)** and select the client or clients that you want to move by selecting the relevant checkboxes.
- Use the drop-down menu to select the target group and click **Move**.

To check whether the newly created group appears at the corresponding level in the group structure, go back to the **Client groups** main window.

Deleting client groups

To delete a group, the group must first be empty, i.e. it cannot include clients or subgroups. Select the group and click **Delete**.

Chapter 6

Product and license management

Cytomic Nexus offers a set of tools that provides considerable autonomy when it comes to delivering services and choosing the optimum type of service that adapts to clients' needs. This enables a fluent service relationship between partners' technical departments, clients and Cytomic with respect to the assignment of products, modules and licenses.

Depending on the license mode, with Cytomic Nexus Web console users can manage:

- Products assigned to clients, including changes or cancellations.
- The duration and number of licenses assigned for each product.
- Service renewals and cancellations.
- Assignment of trial versions.
- How to manage clients' services: centrally or non-centrally.

To manage and assign products and licenses, the user account used to access the Web console should have Total control or License and security administrator permissions. See ***Types of permissions*** *on page* ***35****.*

CHAPTER CONTENTS

Basic concepts

To efficiently manage products and licenses, it is important to bear in mind the following concepts:

- **License contract**: This is the assignment of a specific number of licenses of a given duration of a product or module to a client.
- **Product**: A security solution belonging to Cytomic's portfolio and compatible with Cytomic Nexus. These solutions can be managed by the technical department.
- **Service**: This is a group of one or more license contracts associated to the same product.
- **Module**: A product component that adds additional functions or features.
- **License**: Each Cytomic product can be used/installed on as many devices as there are licenses in the license contract assigned to the client.
- **Management model** :Some Cytomic products allow the total delegation of product management. This model frees clients from the need to manage the service themselves, thereby increasing the added value provided to clients.

Licensing models and features available

Depending on the licensing model chosen by partners or by the technical department of a large company, certain features of Cytomic Nexus relating to client management will be disabled in the Web console, and will be available through an assigned salesperson:

Feature	Monthly subscription	Annual subscription	Simplified model
Create and delete clients	Web console	Web console	Assigned salesperson
Assigning commercial licenses to clients	Web console	Web console	Assigned salesperson
Assigning trial licenses to clients	Web console	Web console	Web console
Monitoring clients' status	Web console	Web console	Web console
Filtering and exporting clients	Web console	Web console	Web console
Creating client groups	Web console	Web console	Web console

Table 6.1: Client and license management features corresponding to the licensing models

Products and modules available in Cytomic Nexus

Available products

- Advanced EPDR
- Advanced EDR

Modules available

Web console users can assign additional modules to clients to complement certain aspects of the products.

Modules available in Cytomic Nexus are:

- Cytomic Insights
- Cytomic Data Watch
- Cytomic Encryption
- Cytomic Patch
- Cytomic SIEMConnect fo Partners

By default, modules are assigned to the product with the same number of licenses and the same expiration date, though these values can be changed later.

Service management models

Service management models for endpoint security products

When assigning an endpoint security product to a client, you must choose the associated management model:

- Not centrally managed
- Centrally managed from Cytomic Nexus

Not centrally managed

The product is configured solely from the client’s Web console. Cytomic Nexus does not apply centralized settings to the product.

Centrally managed from Cytomic Nexus

The client’s product is assigned centralized settings from Cytomic Nexus.

To enable centralized management, certain requirements must be met. Also, it is very important to understand and bear in mind the consequences of centrally managing a product.

*For more information about the requirements necessary to enable centralized management, see **Requirements for assigning centralized settings** on page 72*
*For more information about how Cytomic Nexus behaves with regard to centralized management, see **Security product settings** on page 73.*

Default management model assigned to security products

Assigning new products to clients

The option **Not centrally managed** is selected by default. Later, you can change the management model.

Assigning a trial version of a superior product to a client who already has centrally managed products

The trial version inherits the management model of the product the client already has. Therefore, the trial is managed centrally from Cytomic Nexus.

Assigning a trial version of a superior product to a client who has non-centrally managed products

The trial version inherits the management model of the product the client already has. Therefore, you cannot manage the trial version centrally from Cytomic Nexus.

> *See **Service management models for endpoint security products***

Setting and changing the management model

The management model is set when you assign a product to a client through the Cytomic Nexus console. See **Adding a product to an existing, expired or canceled client**.

To change a previously set management model, see **Assigned product details**.

Product and module management

Assigning products to clients

In order for clients to use the services provided by Cytomic, a Web console user first has to assign at least one product from one of the available families.

The process of assigning products and modules varies depending on whether it is a new client or an existing one.

- **For new clients**: Assigning products is part of the client registration process. See **Creating and deleting clients** on page **40**.
- **For existing clients, as well as those expired or canceled within the last 90 days:** See **Adding a product to an existing, expired or canceled client**.

> *If the client to whom you want to assign licenses does not appear in the list, it may be because their services have been inactive for the last 90 days. See **Monitoring clients** on page **42***

In the process of assigning a product you can also add any supported modules required.

Adding a product to an existing, expired or canceled client

- Click the **Status** menu at the top of the console, and go to the client's details by clicking their name in the list in the **Monitoring** section.

- If the client was canceled less than 90 days ago, or the product was canceled or has expired, they will continue to appear in Cytomic Nexus in case the Web console user wants to reassign the product.
- Click **Add product**.
- Select the characteristics of the product to be added to the client:

Field	Description
License type	Use the drop-down menu to select a trial license or commercial license.
Product	Select the product to assign to the client.
Quantity	Select the number of licenses to assign.
Period	In the annual subscription model, select the license duration (1, 2 or 3 years). If you select a period not enabled for use by Cytomic a notice will appear.
Additional modules	Depending on the product selected, you can assign additional module licenses. Other than with Cytomic Encryption, it is not possible to specify the number of licenses for the additional modules as it will be the same number as for the main product.

Table 6.2: Fields defining the type of product to assign to clients

- Click **Add**. A window will appear to choose the type of management: with or without centralized management.

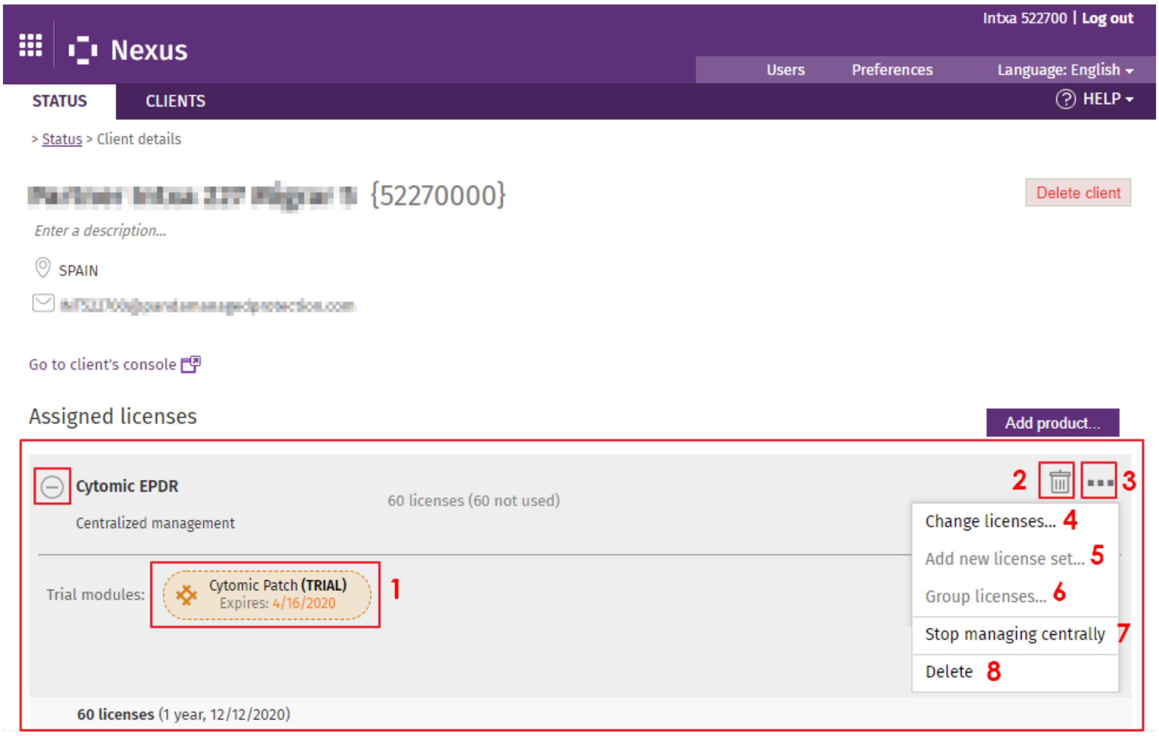
As a result of this process, the license contract will be displayed in the client's details.

Assigned product details

Once you assign a product to a client, the client's **Details** window will show the product name and the management model applied to it.

> *See **Default management model assigned to security products**.*

Click ⊖ and ⊕ to display or close details on each line of information and ▮▮▮ (**3**) for the context menu options:



> Status > Client details

[redacted] {52270000}

Enter a description...

SPAIN

[redacted]

Go to client's console

Assigned licenses

Cytomic EPDR

Centralized management

60 licenses (60 not used)

Trial modules: Cytomic Patch (TRIAL) Expires: 4/16/2020

60 licenses (1 year, 12/12/2020)

Figure 6.1: Assigned product details

- Additional modules contracted (**1**): number of contracted licenses, license duration and expiration date.
- Context menu options (**3**):
  - Change licenses (**4**)
  - Centrally manage/Stop centrally managing (**7**)
  - Delete option (**8**) to delete services.

Deleting products and modules

Deleting a product

- In the top menu, select **Status**. In the list of clients, click the name of the client whose product you want to delete. The **Client details** page opens.
- Click the 🗑 icon for the service you want to delete.
- Click **Delete service**. The client loses the protection service immediately.

Deleting modules

- In the top menu, select **Status**. In the list of clients, click the name of the client whose module you want to delete. The **Client details** page opens.

- Click the ▮▮▮ icon for the product whose module you want to delete. Select **Change licenses**. A page opens that shows details of all of the client's licenses,
- Clear the checkbox for the module you want to delete. Click **Delete**. The client loses the protection services immediately.

Consequences of deleting products and modules

When you delete a product, you also delete its associated modules. Clients cease to have access to the service.

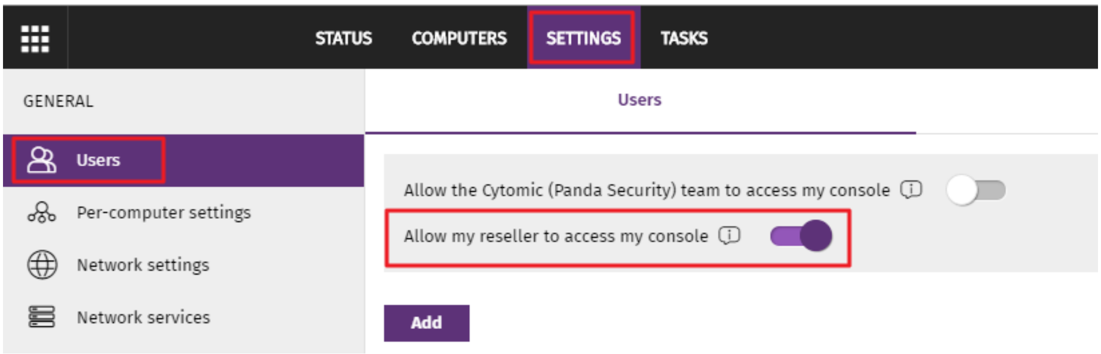
When you delete only the modules associated with a product, the service remains active but the client ceases to have access to the modules.

Accessing the client's console

Requirements for accessing the client's console

The client must enable the **Allow my reseller to access my console** option in their product console. This options is enabled by default. If it is not, the client must follow the steps below from their product's management console:

- Click **Settings** in the menu at the top of the console. Click **Users** in the side menu.
- On the **Users** tab, click the **Allow my reseller to access my console** option.



Allow the Cytomic (Panda Security) team to access my console ○

Allow my reseller to access my console ●

Figure 6.2: Accessing the Allow my reseller to access my console option from the client's console

Accessing the client's console from Cytomic Nexus

- Click **Status** in the menu at the top of the console.
- In the **Monitoring** list, click the ⧉ icon next to the client's name. The Cytomic Central page opens. This page shows all products contracted by the client.
- Select the client's product to manage. The client's management console opens.

You access the client's console with the account you used to access the Cytomic Nexus console, and with the Full Control role assigned.

License management

In the **Licenses** area, which can be accessed from the **Status** menu, you can see details of the licenses. This information varies depending on the license model agreed with Cytomic:

- **Monthly subscription model**: This indicates the product licenses that can be assigned to clients, both commercial and trial. In this model, the license duration is not established beforehand, as it is the Web console user that determines the end of the service period when licenses are manually withdrawn from users.
- **Annual subscription model:** This indicates the type of licenses and which products can be assigned to clients: 1,2 or 3-year licenses or trial licenses.
- **Simple license model**: No information is reported as the licenses are managed via telephone through the assigned salesperson.

The license panel indicates the licenses that have expired or are about to expire and also to offer greater control, Cytomic Nexus provides a history of the licenses assigned to clients.

Assigning and modifying licenses

You can assign and/or modify the number of product licenses a client has at different times during the license life cycle:

- **When you assign the product to a client**: You must specify the number and type of licenses when you assign a product to a client. See **Assigning products to clients**.
- **When the number of installations exceeds the number of licenses assigned**: You can manually increase the number of assigned licenses.
- **When the client removes computers from the network**: You can reduce the number of licenses assigned to the client manually.

Assigning trial licenses

Cytomic Nexus allows product up-selling and cross-selling, as well as gaining new clients by enabling you to assign trial licenses. Trial licenses provide clients with all the features of products for a limited time period. After the trial period expires, access to the product is automatically disabled.

To provide trial licenses to a client, you must assign a new product to the client with a **Trial license**. See **Assigning products to clients**.

When you assign trial licenses, bear this in mind:

-
-
- You cannot assign a trial license to a client who has had a trial version of the same product or a full version of the product during the previous three months.

Renewing licenses

License renewal extends the duration of product licenses assigned to a client. You can renew licenses before they expire (manually) or automatically. Below is an explanation of both renewal methods.

Early (manual) renewal of annual licenses

When you learn that a client's licenses are about to expire, you can begin the early renewal process to make sure that no computers are left unprotected.

> ⚠ *Early renewal can be applied only to products with less than one year remaining on the license.*

To renew a license contract before it expires (early renewal):

- From the top menu, select **Status**. In the **Monitoring** section, click the name of the client. The **Client details** page opens.
- Click the ▮▮▮ icon. From the context menu, select **Change licenses**. A dialog box opens where you can see the products whose licenses you want to renew
- In the **Renew for** field, choose the duration of the licenses that you want to assign to the product when it expires. Click **Change**.

After the process is complete, the license contract updates with the new expiration date.

Automatic renewal of licenses

> ⓘ *You cannot automatically renew security product licenses assigned to clients you are migrating to WatchGuard Cloud.*

Cytomic Nexus allows the automatic renewal of product and module licenses assigned to clients. This helps simplify management tasks because you do not have to continually monitor which clients have products with licenses close to expiring to start a manual/early renewal process.

When setting up the process, you can choose to automatically renew only the main product. When the renewal date arrives, the product is renewed, and if there are additional services or modules, they are automatically renewed as well.

Configuring automatic renewal of licenses

From the top menu, select **Clients**. Select **Automatic renewal of licenses**. The **Automatic renewal** page opens. This page is divided into a **search area** and a **client list**:

Search area

Find clients for which you want to configure automatic renewal. To show the search options, click **Options** > **Show filter**. If you select multiple search criteria, the logical operator 'AND' is applied.

Field	Description
Find client	Filters the list by client name. It allows partial searches and is not case sensitive.
Group	Filters the list by client groups. It allows partial searches and is not case sensitive.

Table 6.3: Search options in the automatic renewal list

Client list

This section shows a list of clients, specifying whether or not they support automatic renewal. If they support this feature, you can enable it. This information appears:

Field	Description
Client	Shows the client name and a link to the **Client details** page. For more information, see **Client details** on page **45**. Under the client name, this information appears: product name, number of contracted licenses, and expiration date for the licenses that are closest to expiring. Point to the product name or the number of licenses for additional information.
Group	Shows the group to which the client belongs.
Product	A drop-down menu where you can select the automatic renewal action: • **Not available**: The product does not support automatic renewal. • **Do not automatically renew**: The client's licenses are renewed early/manually. • **1-year licenses**: When the client's licenses expire, they are automatically renewed for 1 year. • **2-year licenses**: When the client's licenses expire, they are automatically renewed for 2 years. • **3-year licenses**: When the client's licenses expire, they are automatically renewed for 3 years.

Table 6.4: Options in the automatic renewal list

Email alerts about licenses about to expire

To eliminate the need to constantly check the web console for clients with licenses that are about to expire, Cytomic Nexus sends an email alert to you. This message is sent on the first day of every month, and contains a list of clients whose licenses have expired or are about to expire, along with the number of licenses. This information is also available in the **My clients' licenses** panel in the **Licenses** section of the **Status** page.

The email message includes a spreadsheet with this data:

- Additional licenses needed for renewals (if there is enough stock to renew all clients' licenses).
- Clients with licenses that are about to expire.

To enable the sending of this email message, follow these steps:

- From the **Other options** menu, select **Preferences**. The **Preferences** page opens.
- In the **Email notifications** section, select the **Send an email message with the licenses that will expire within the next 60 days** option. Complete these fields:
    - **Message subject**
    - **Email address**: To send the message to multiple recipients, use the ";" character.

Modifying assigned products and licenses

As part of the daily management of clients, the web console user might need to change the licenses or even upgrade the products assigned to adapt the service to the changing needs of clients.

The following restrictions apply when you change the number of licenses or the products assigned to clients:

- You cannot reduce the number of licenses in use individually. You can reduce the number of licenses only if you do it along with an early renewal during the last three months of the license period. For more information, see **Early (manual) renewal of annual licenses**.

> ⚠ *Reductions and changes to the license period are applied instantly to clients.*

- You can only change from a product to a superior product in the same product family.

Acquiring a superior product and/or increasing the number of commercial licenses

To increase the number of licenses and improve the assigned product, follow these steps:

- In the top menu, select **Status**. In the list of clients, click the client whose licenses you want to change.
- Click the ■■■ icon for the relevant product. Select **Change licenses**. A page opens that shows the details of the current license contract.
- Make the changes to the product, number of licenses, and access to modules. Click **Change**. The new license usage is shown.

Changing trial licenses (converting from trial to commercial licenses)

With Cytomic Nexus, you can convert a trial license to a commercial license and even change the trial product. These restrictions apply when you change trial licenses:

- You cannot change the number of trial licenses established per product (see **Assigning trial licenses**) nor their duration.
- **Changing from one trial product to another**: You cannot change from one trial product to another.
- **Changing from a trial product to a commercial one**: You can change the trial product to a commercial one, select additional services and the number and duration of the licenses.

Changing the Panda Systems Management model

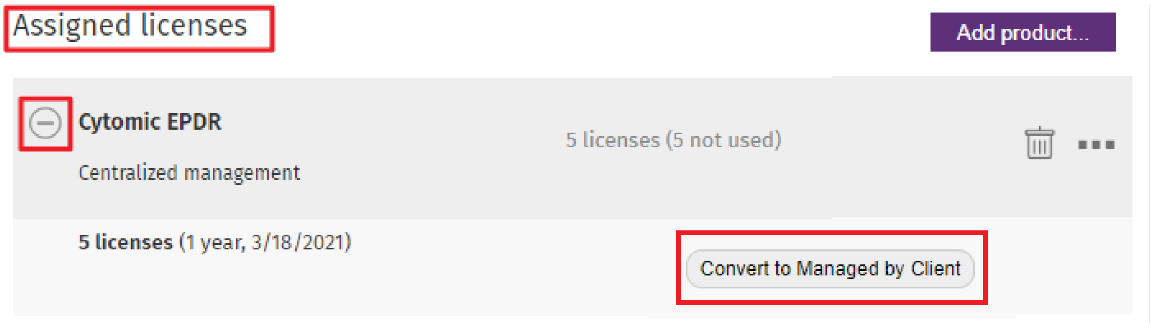


Figure 6.3: Information about the licenses assigned to a product

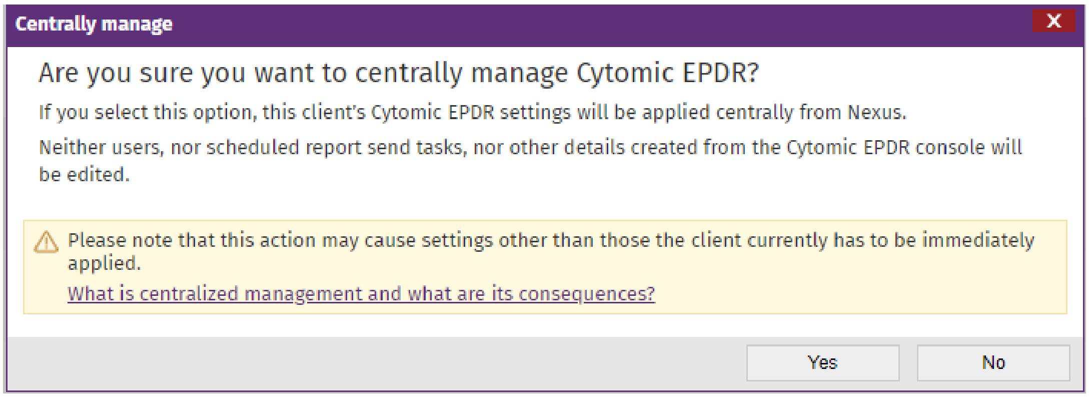
Changing the security product management model

*See **Consequences of changing the management model** for a summary of the effects of changing the management model of a client's products on their security settings.*

To centrally manage a client's security product:

- See **Requirements for assigning centralized settings** on page **72**.
- In the top menu, select **Status**. In the list of clients, click the client for whom you want to change the management model.

- On the **Client details** page, click the context menu ⋮.
- Select **Centrally manage**. A message appears indicating the consequences of applying the new management model, and a link to more information. If you are sure you want to apply the change, click **Yes**.



Centrally manage

Are you sure you want to centrally manage Cytomic EPDR?

If you select this option, this client's Cytomic EPDR settings will be applied centrally from Nexus.

Neither users, nor scheduled report send tasks, nor other details created from the Cytomic EPDR console will be edited.

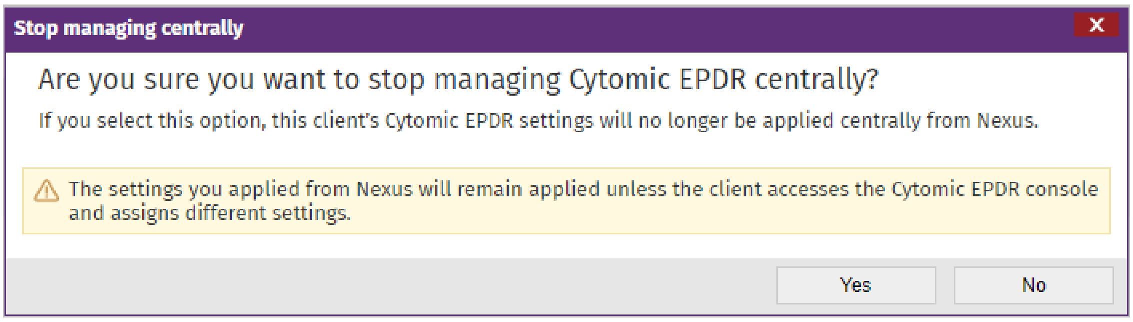
⚠ Please note that this action may cause settings other than those the client currently has to be immediately applied.

What is centralized management and what are its consequences?

Figure 6.4: Centrally manage a product

To stop managing a client's product centrally:

- In the client list, select the client whose management model you want to change.
- On the **Client details** page, click the context menu ⋮.
- Select **Stop managing centrally** and click **Yes**.



Stop managing centrally

Are you sure you want to stop managing Cytomic EPDR centrally?

If you select this option, this client's Cytomic EPDR settings will no longer be applied centrally from Nexus.

⚠ The settings you applied from Nexus will remain applied unless the client accesses the Cytomic EPDR console and assigns different settings.

Figure 6.5: Stop managing a product centrally

Consequences of changing the management model

When a client's management model is changed, settings other than those previously assigned by the client might be immediately applied to their products. It is therefore important to understand the consequences of changing the management model.

Centrally managed from Cytomic Nexus

- The client's product is centrally assigned settings from Cytomic Nexus.

See chapter ***Endpoint security product settings management*** *on page 69 for more information about the interaction between the settings configured by the client and by the Cytomic Nexus user.*

Not centrally managed:

- The product's settings are managed solely from the client's product Web console.
- Settings previously assigned from Cytomic Nexus remain in effect until they are changed by the network administrator from the product console.

Managing unprotected computers

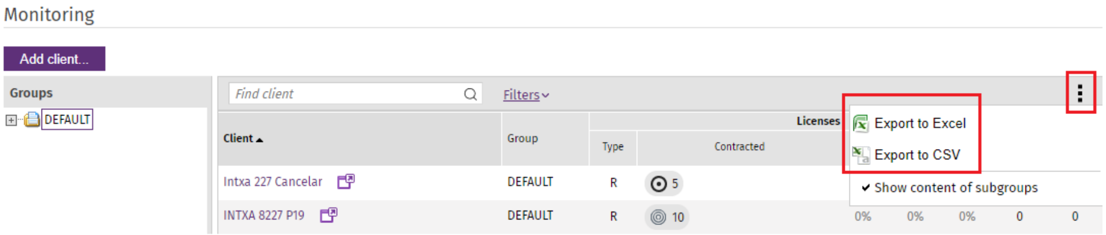
When a client does not have enough licenses to protect all their computers, some of them will be left unprotected. This means that their protection will not be updated and that the information coming from these devices will not be taken into account for the purpose of statistics, reports and analytics carried out by CYTOMIC Nexus .

The computers affected by this situation will automatically revert to their protected status when a client has sufficient licenses. To achieve this, the Web console user must perform one of the following actions:

- If there are new computers on the network that are unprotected because the client doesn't have unassigned licenses, the Web console user will have to change the number of licenses to add new the client's new computers. See **Modifying assigned products and licenses**.
- If there are previously protected computers on the client's network with licenses that have expired, the Web console user must renew the corresponding license contracts.

Viewing computers with expired licenses in the Web console

To see the devices a client has without licenses you have to export the client list:



Client ▲	Group	Licenses Type	Contracted					
Intxa 227 Cancelar	DEFAULT	R	5					
INTXA 8227 P19	DEFAULT	R	10	0%	0%	0%	0	0

Figure 6.6: Exporting client's list

- Click the **Status** menu at the top of the console. In the **Monitoring** section, click the context menu and select a format: Excel or CSV.

- Open the report. Computers with expired license are displayed in the **Computers without a license** column.

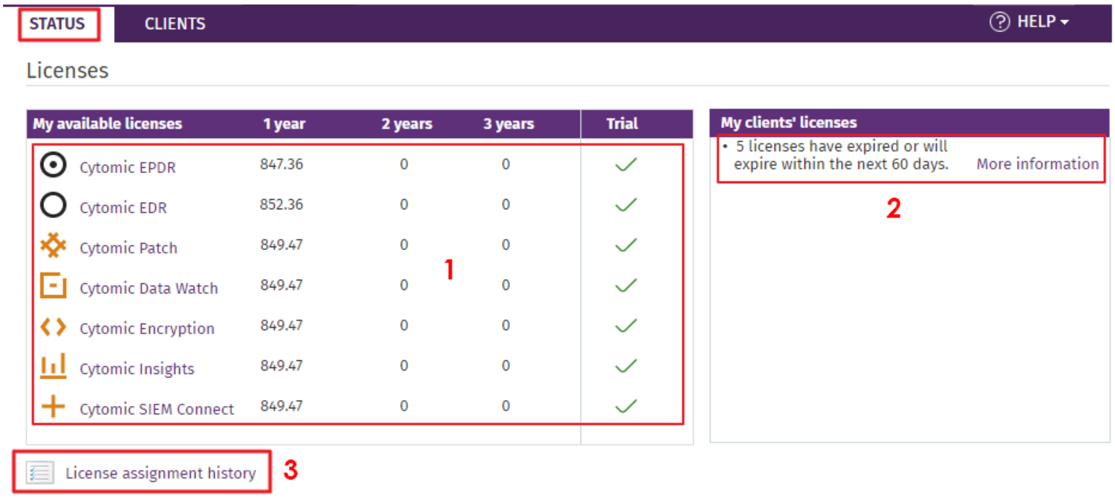
Email list of computers with expired licenses

See **Email alerts about licenses about to expire** for more information about configuring the sending of emails with a list of clients with expired or soon to expire licenses.

Viewing license status

Licenses area

The Licenses area is the first thing you see when you log in to the Cytomic Nexus web console.



Licenses

My available licenses	1 year	2 years	3 years	Trial
Cytomic EPDR	847.36	0	0	✓
Cytomic EDR	852.36	0	0	✓
Cytomic Patch	849.47	0	0	✓
Cytomic Data Watch	849.47	0	0	✓
Cytomic Encryption	849.47	0	0	✓
Cytomic Insights	849.47	0	0	✓
Cytomic SIEM Connect	849.47	0	0	✓

My clients' licenses

- 5 licenses have expired or will expire within the next 60 days. More information

License assignment history

Figure 6.7: Licenses area

The information is organized as follows:

My available licenses (1)

This section shows the licenses available for the different products. It includes:

Field	Description
Product name	Click the product name for more detailed information.
License duration	Based on the licensing model selected, this panel shows this information: • **Monthly licensing model**: The products available for sale appear. • **Annual licensing model**: The types of licenses (one, two, or three years) appear as well as the products available for sale. • **Simple licensing model**: The panel does not show any relevant details.

Field	Description
Trial	Indicates whether Cytomic Nexus enables you to assign trial licenses for this product.

Table 6.5: Fields in the My Available Licenses list

My clients' licenses (2):

This section shows the number of your clients' licenses that have expired or are about to expire. It includes:

- Warnings related to licenses assigned to clients.
- **More information** link: Click it to generate a report about expired licenses.

> ⚠ *The number of licenses that are about to expire does not include licenses for security products assigned to clients that you are migrating to WatchGuard Cloud.*

Licenses being assigned (3)

This section shows the number of licenses that are in the process of being assigned. For more information, click the **View details** link.

License assignment history (4)

Cytomic Nexus provides a history of all the license assignment operations that occurred.

Licenses being assigned

When licenses are assigned to clients, if the assignment is not immediate, you will see the text **XX licenses being assigned**. **View details** in the Licenses area. Click **View details**, and you will see the **Licenses being assigned** window with the following information:

Field	Description
Type	Name of the product.
Service period	Duration of the licenses (1, 2 or 3 years).
Quantity	Number of licenses being assigned.
Client	Name of the client to whom the licenses are being assigned. Click the name to go to the **Client details** on page **45** window.

Field	Description
Group	Group to which the client belongs.

Table 6.6: Fields in the 'Licenses being assigned' window

License assignment history

The license assignment history enables you to monitor all the operations that involve changes to the licenses assigned to clients.

To access the history, select **Status** in the top menu. Click the **License assignment history** link.

The **License assignment history** page is divided into two main areas:

- The search area
- The list of assigned licenses

The search area

The search are shows these fields:

Field	Description
Options > Show filter	Shows all the search fields.
Find	Enter the name of the client, group, or user of the web console for whom you want to see licenses. It allows partial searches and is not case sensitive.
Assignment type	Use the drop-down menu to select the type of assignment used to assign the licenses to the client. See table **Types of assignments**.
Product	Select the product that corresponds to the assigned licenses.
From	Click the icon to use the calendar to select a date for the beginning of the search period.
To	Click the icon to use the calendar to select a date for the end of the search period.
Show all	This displays all the clients to whom licenses have been assigned, without applying any search criteria.

Field	Description
Export to	Exports the list as an Excel or .CSV file.
Clear history	Deletes all records from the history. The information cannot then be recovered.

Table 6.7: Search area filter criteria

Types of assignments:

Field	Description
Manual assignment	See **Assigning and modifying licenses**.
Renewal	See **Early (manual) renewal of annual licenses**.
Automatic renewal	See **Automatic renewal of licenses**.
Service change	See **Modifying assigned products and licenses**.
Service cancellation	See **Deleting products and modules**.

Table 6.8: Types of assignments

The list of assigned licenses

This area shows the filtered search results. The information is shown as follows:

Field	Description
Date	Date and time of the operation.
Product	Name of the product.
Period	Duration of the licenses.
No. of licenses	Number of licenses affected.
Client	Name of the client.
Group	Group to which the client belongs.

Field	Description
Assigned by	Web console user account that carried out the operation.
Assignment type	Type of registered operation: • **Manual**: the licenses were manually assigned from the Web console by the administrator. See **Assigning and modifying licenses**. • **Automatic renewal**: The licenses were automatically renewed. See **Automatic renewal of licenses** • **Cancellation of license contracts, services and clients**: See sections **Deleting products and modules** and **Deleting clients** on page **42** for more information. • **Service change** See **Modifying assigned products and licenses**. • **License contract renewal** See **Renewing licenses**.

Table 6.9: Fields in the 'License assignment history' list

Chapter 7

Endpoint security product settings management

Cytomic Nexus provides advanced capabilities for managing the security of clients with endpoint security products:

- Configure the operation of all security products installed on clients' networks.
- Customize the look and feel of clients' consoles. Change colors and logos to reflect your company's brand.
- Minimize management time. Streamline the deployment of settings by leveraging the advanced inheritance features implemented in Cytomic.

CHAPTER CONTENTS

Cytomic Nexus Web console and client's Web console

The ability to configure products centrally opens up the possibility that a settings profile configured by the partner can conflict with another settings profile previously configured by the client. To resolve such situations, there is a system of priorities in place regarding settings which depends on the settings source (the console where they were created):

- The settings configured by the partner are always created and sent from the Cytomic Nexus Web console.
- The settings configured by the network administrator are always created from the client's Web console.

Access from a partner to a client's console and the subsequent creation of settings in that console fall outside the centralized settings management dynamics discussed in this section. For this reason, that scenario is not contemplated when describing the priorities governing the settings created by the partner and by the user.

Centralized product configuration

The functionality of Cytomic Nexus with respect to the Cytomic products that clients have installed is as follows:

- Creation and assignment/display of the security product settings profiles for one, multiple, or all clients managed by the user of the Web console.
- Advanced configuration of the appearance of the client console, in order to adapt it to the brand image.
- Use of the tree structure and inheritance feature to assign and deploy settings to clients.

- Integration with the Cytomic Nexus permissions system: the client tree structure adapts, limiting the information displayed based on the permissions assigned to the Web console user account. The ability to edit settings is also defined by the account permissions.

Supported products and modules

Many of the concepts required for managing Cytomic Nexus are inherited from the Cytomic platform and are familiar to the Web console user, and the administration guides for the managed products can serve as a reference.

The following table shows the security products supported by Cytomic Nexus, along with a link to the associated guide:

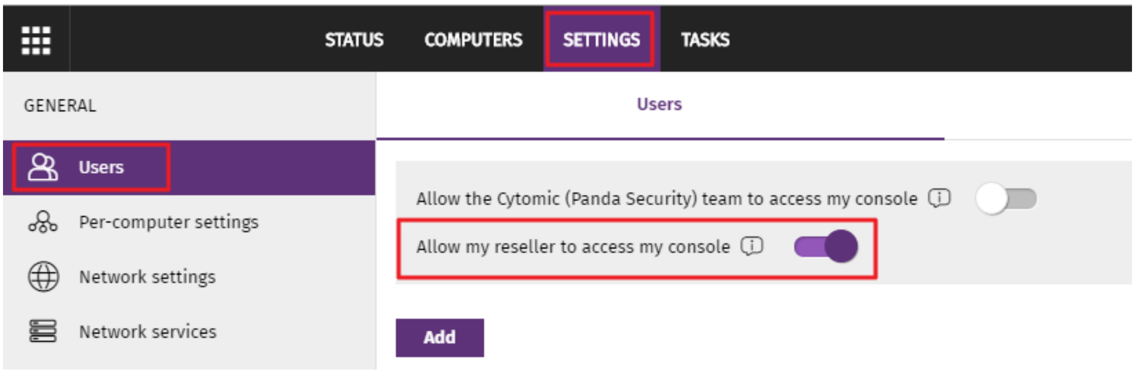
Product / Module	Product guide
Advanced EPDR	Advanced EPDR Administration Guide **https://info.cytomicmodel.com/resources/guides/EPDR/latest/en/EPDR-guide-EN.pdf**
Advanced EDR	Advanced EDR Administration Guide **http://info.cytomicmodel.com/resources/guides/EDR/latest/en/EDR-guide-EN.pdf**
Cytomic Encryption	Installed product administration guide.
Cytomic Data Watch	Installed product administration guide.
Cytomic Patch	Installed product administration guide.
Cytomic SIEMConnect fo Partners	Infrastructure Guide. **https://info.cytomicmodel.com/resources/guides/SIEMConnect/en/SIEMCONNECT-Manual-EN.pdf** Event Description Guide. **https://info.cytomicmodel.com/resources/guides/SIEMConnect/en/SIEMCONNECT-EventDescriptionGuide-EN.pdf**

Table 7.1: Products supported by Cytomic Nexus and the corresponding administration guide.

Requirements for assigning centralized settings

For Cytomic Nexus Web console users to assign settings to the security products installed on clients' systems, the following requirements must be met:

- The Cytomic Nexus Web console user must have previously created the client and assigned a security product to them. Refer to **Supported products and modules**.
- The Cytomic Nexus Web console user must have chosen the option to manage the product centrally. Refer to **Assigning products to clients** on page **53**
- The Cytomic Nexus Web console user must have visibility and the permissions required to assign settings to the client or group of clients. Refer to chapter **Access and authorization in Cytomic Nexus** on page **29** for more information about permissions in Cytomic Nexus.
- The version of the security product installed on the client's network must be at least 3.50. To find this information in the client's console, go to the general settings menu and select the Release Notes option.
- The client must have the option **Allow my reseller to access my console** enabled. This option should be enabled by default. If it is not enabled, the client must follow these steps from their product management console:
  - In the **Settings** menu, click **Users** in the side bar and then the **Users** tab.
  - Click the option **Allow my reseller to access my console**.



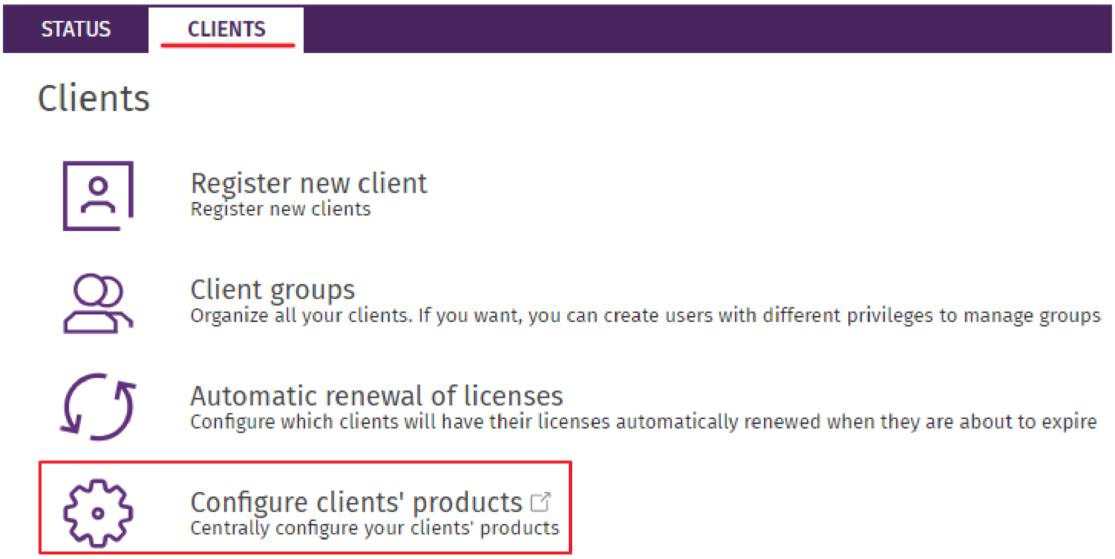
Allow the Cytomic (Panda Security) team to access my console ○

Allow my reseller to access my console ●

Figure 7.1: Accessing the 'Allow my reseller to access my console' option from the client's Cytomic console

Accessing settings management

- Select **Clients** in the top menu. Select **Configure clients' products**. A new tab opens. This tab looks the same as the console used by clients to manage their products.



Clients

Register new client
Register new clients

Client groups
Organize all your clients. If you want, you can create users with different privileges to manage groups

Automatic renewal of licenses
Configure which clients will have their licenses automatically renewed when they are about to expire

Configure clients' products
Centrally configure your clients' products

Figure 7.2: Accessing the product settings

- Select the **Settings** menu at the top of the console. Two tabs appear in the side panel: **Clients** and **Management.**
- Click the **Settings** tab to change the way the security product and the modules installed on clients' networks work.
- Click the **Management** tab to manage the appearance of clients' consoles and the telemetry data received by the security service provider through the Cytomic SIEMConnect fo Partners product.

Security product settings

Managing settings

For more information about how to create, delete, and edit settings profiles, see **Creating and managing settings profiles**.

Types of settings supported by Cytomic Nexus

Depending on the product a client has installed, some or all of the settings profiles you configure will take effect on the security software on the client's systems. To configure a settings profile, see the chapter specified in table **Settings profiles available in Cytomic Nexus** in the relevant product administration guide.

Cytomic Nexus supports these types of settings profiles for the endpoint security products:

Settings	Description
Per-computer settings	Configure these features of the security software installed on user computers:

Settings	Description
	- Show/hide the system tray icon. See **Configuring the agent visibility**. - Update the security software installed. See **Protection engine updates**. - Configure protection against tampering of the security software (anti-tamper protection), protection for computers that start in Safe Mode, and enable two-factor authentication (2FA). - See **Configuring the agent remotely**. - For specific details about Cytomic Nexus, see **Two-factor authentication (2FA) and password to perform management tasks from computers**. - Manage shadow copies of files stored on user computers. See **Configuring Shadow Copies**.
Remote control	Establish a remote connection from the console of the product purchased by the client to the computers on the client's network to check their status or for troubleshooting. See **Remote computer control**.
Workstations and servers	Configure how the security software must handle threats, and define administrator rules to access network resources and minimize the attack surface. See **Security settings for workstations and servers**.
Indicators of attack (IOA)	Detect targeted cyberattacks used by hackers to try to break through security defenses by running series of coordinated actions. These actions take place over long periods of time and use multiple strategies and infection vectors simultaneously. See **Indicators of attack settings**.
Advanced indicators of attack	Perform in-depth monitoring of the applications on clients' computers to detect suspicious behavior. The events generated by the applications installed on computers are analyzed to determine whether the event is an attack. This type of settings profile applies only.to Windows computers. See **Indicators of attack settings**.
Program blocking	Increase the security of the Windows computers on clients' networks by preventing the use of programs you consider dangerous or not

Settings	Description
	compatible with the work of their organizations. See **Program blocking settings**.
Authorized software	Prevent inconvenience and delay to users when the advanced protection blocks the execution of programs that are unknown to the Cytomic intelligence until a classification is returned. See **Authorized software settings**.
Mobile devices	Configure how the security software must handle threats on Android and iOS smartphones and tablets. See **Security settings for mobile devices**.
Patch management	Keep installed applications and operating systems up to date by automating installation of the security patches published by software vendors. • See **Selective patching of computers of clients managed from a single Cytomic console**. • See **Patching test computers**. • See **Updating vulnerable programs**.
Endpoint Access Enforcement	Endpoint Access Enforcement monitors inbound connections to computers on the corporate network to check whether they originate from managed, protected computers. See **Endpoint Access Enforcement settings**.
Data Control	Comply with data protection regulations, such as the GDPR, and see and monitor Personally Identifiable Information (PII) stored in IT infrastructures. See **Personal data monitoring**.
Encryption	Encrypt the content of internal and external storage devices to minimize the exposure of corporate data in the event of data loss or theft, as well as when users remove storage devices. See **Full Encryption settings**.
Cytomic SIEMConnect fo	Configure unified settings to receive all the telemetry generated on your clients' computers.

Settings	Description
Partners	For more information about how to configure the module, see section **Cytomic SIEMConnect fo Partners settings**.

Table 7.2: Settings profiles available in Cytomic Nexus

Settings profiles editable by clients

By default, clients cannot edit or delete the settings profiles inherited from a service provider. Nevertheless, Cytomic Nexus enables the service provider to configure certain settings profiles to be editable. In this case, clients can add items to the settings profile, but cannot delete the items defined by the service provider.

The types of settings profiles that clients can edit are:

- **Workstations and servers**: Clients can add exclusions to these lists, but cannot delete or edit the exclusions defined by the service provider:
  - File, folder, and extension exclusions, in the general settings. For more information, see **General settings**.
  - AMSI technology. See **Anti-Malware Scan Interface**.
  - Code injection exclusions, in the anti-exploit protection. For more information, see **Advanced protection**.
- **Authorized software**: Clients can add authorized software rules to the list of rules defined by the service provider. However, clients cannot delete or edit the existing rules. See **Authorized software settings**.
- **Endpoint Access Enforcement**: Clients can add new allowed IP addresses to the protocols defined by the service provider. See **Endpoint Access Enforcement settings**.

Configuring settings profiles to be editable

To access editable settings profiles managed from Cytomic Nexus:

- From the top menu, select **Clients**. Select **Configure clients' products**. A page opens in a new tab in your browser.
- From the top menu, select **Settings**. From the side menu, select **Clients**.

To configure a **Workstations and servers** settings profile to be editable:

- From the side menu, select **Workstations and servers**. A list appears and shows all settings profiles created so far.
- Select the settings profile you want to configure to be editable.

- Select **Allow Client Exclusions**. Click **Save**. The settings profile shows the **Exclusions editable by clients** label.

To configure an **Authorized software** settings profile to be editable:

- From the side menu, select **Authorized software**. A list appears and shows all settings profiles created so far.
- Select the settings profile you want to configure to be editable.
- Select **Settings editable by clients**. Click **Save**. The settings profile shows the **Settings editable by clients** label.

To configure an **Endpoint Access Enforcement** settings profile to be editable:

- From the side menu, select **Endpoint Access Enforcement**. A list appears and shows all settings profiles created so far.
- Select the settings profile you want to configure to be editable.
- Select **Protocols editable by client**. Click **Save**. The settings profile shows the **Settings editable by clients** label.

Changing the status of a settings profile from editable to non-editable and vice versa

If the service provider changes the status of a settings profile from editable to non-editable, the items the client added will no longer apply.

If the service provider changes the configuration again to be editable, then the items the client added are restored and applied.

None of these changes affect the items the service provider added. These items are always visible, albeit dimmed, and in force as long as the settings profile is kept.

Selective patching of computers of clients managed from a single Cytomic console

As a general rule, a service provider assigns each client a separate Cytomic console to manage the security products the client purchased. However, if the service provider manages the security of multiple clients from a single Cytomic console, there is the possibility that some clients have Cytomic Patch and others do not. In this case, to prevent a patch installation task sent by the service provider from the Cytomic Nexus console from running on all computers indistinctively, you must create different patch installation settings profiles in the Cytomic console to install patches on computers or not.

To configure Cytomic Patch to allow or deny patch installations on clients' computers:

- In the Cytomic console, create a settings profile for clients' computers with a Cytomic Patch license.

- In the Cytomic console, create another settings profile for clients' computers without a Cytomic Patch license**.**
- In the settings profile for computers with a Cytomic Patch license, select **Install patches** from the **Patch installation** drop-down menu.
- In the settings profile for computers without a Cytomic Patch license, select **Do not install patches** from the **Patch installation** drop-down menu.
- In the Cytomic Nexus console, create a single patch installation task whose recipient is the console that contains computers from multiple clients.

Patching test computers

When configuring Cytomic Patch in the Cytomic console, you can designate computers as test computers for patch installation.

By installing patches on test computers, you add an additional layer of security because you can verify the installation results before you install the patches on other computers on the network.

To install patches on test computers only:

- In the client's Cytomic console, create a Cytomic Patch settings profile.
- In the settings profile, select **Designate as test computers and install patches** from the **Patch installation** drop-down menu.
- In the Cytomic Nexus console, create a patch installation task whose recipients are clients that have test computers. For more information about how to create patch installation tasks in Cytomic Nexus, see **Creating tasks** on page **137** and **Configuring Cytomic Patch tasks (4)** on page **142**.

For more information about how to configure Cytomic Patch in the Cytomic console, see ***Configuring the discovery of missing patches****.*

Two-factor authentication (2FA) and password to perform management tasks from computers

For more information about this feature, see ***Configuring security against protection tampering****.*

Permissions and visibility

- To view the QR code generated in a settings profile or the password to uninstall the security software or locally manage a computer, the console user must have visibility of some of the clients assigned to the profile and a higher permission than Monitoring (read-only).
- To edit the QR code generated in a settings profile or the password to uninstall the security software or locally manage a computer, the console user must have visibility of all the clients assigned to the profile and a higher permission than Monitoring (read-only).

*See **Types of permissions** on page **35**.*

Copying settings profiles in the client's console

If a client copies a settings profile inherited from a service provider and the profile already has a QR code or a password to uninstall the security software or locally manage computers, the client could view the QR code or the password in the copied profile. To prevent security issues, the client's console deletes the existing code and password and generates a new QR code and a password automatically in the copied profile.

Cytomic SIEMConnect fo Partners settings

To enable the settings, click the **Send the following events to my SIEM** toggle and select the groups of events that your SIEM solution will receive from all the telemetry data generated by the computers assigned to the settings.

Configuring groups

The telemetry data sent to Cytomic consists of the relevant events logged when programs are run on clients' computers. These events are grouped based on their type. Each group can be enabled and disabled individually so the MSSP can choose to receive only those events they are interested in.

Group	Description
Threat detections (malware, PUPs, exploits)	Alerts about malware/PUPs, exploits, and items blocked by advanced policies.
Loading and execution of executable (PE) files and scripts	Loading and execution of binary and non-binary (scripts) executable files.
Communications	Socket open and use events.

Group	Description
Access to data	Access to data contained in files and the Windows registry.
Creation and modification of executable (PE) files and scripts	Creation and modification of binary and non-binary (scripts) executable files.
Access to the Windows registry	Events related to access to the Windows Registry.
System events	Events related to access to devices, the WMI engine, as well as logins and logouts.
Threat hunting indicators (only for clients with Cytomic Orion)	Alerts generated by Orion hunting rules.

Table 7.3: Event groups available to partners

For more information about the meaning and definition of the events sent to the service provider's SIEM solution, refer to the Event Description Guide at ***https://info.cytomicmodel.com/resources/guides/SIEMConnect/es/SIEMCONNECT-ManualDescripcionEventos-ES.pdf***

Configuring the event format

- Click the Change sending format link at the bottom of the page. The Select the format of the events sent to your SIEM window opens.
- Select LEEF format or CEF format and click **Save**. The new setting is applied immediately.

Because the MSSP receives all events at a single SIEM server, all events are received in the same format. Therefore, if the Partner Center console user changes the event format in a settings profile, the change will apply to all other settings profiles created.

Default settings

With the default settings, all groups and the **Send the following events to my SIEM** toggle are disabled. Therefore, initially, partners do not receive any events from clients.

Assigning and sending settings

Assigning settings

Cytomic Nexus allows settings to be assigned to clients with Cytomic products. It provides two methods for doing this: direct assignment and indirect assignment of settings. Settings will automatically be applied to the **All** group in the client's console.

*Refer to section **Manual assignment/sending of settings** and **Indirect assignment of settings: Inheritance**.*

Sending settings

This feature enables the Cytomic Nexus console user to send settings to their clients' product consoles, without applying them to the clients' All group. These settings can be assigned later directly when needed by the administrator of each client's console and/or by the Cytomic Nexus Web console user accessing the client's console.

*For more information, see section **Settings assignment/sending methods***

Settings assignment/sending methods

Manual assignment/sending of settings

You can assign settings directly to clients from a settings profile or from the list of settings profiles.

Assigning/sending settings from a settings profile

- In the top menu, select **Settings**. Select the **Clients** tab. From the side menu, select the type of settings you want to assign.
- The panel on the right shows your list of client groups and the existing settings profiles of the selected type.
- Select the settings profile you want to assign or create a new settings profile and click the **Recipients** text field.
- **How to assign a settings profile**: In section **Assign to the "All" group of the following clients**, click the ⊕ icon. From the client tree, select the client or client group you want to assign the settings profile to.
- **How to send a settings profile**: In section **Show in the following clients' console**, click the ⊕ icon. From the client tree, select the client or client group you want to send the settings

profile to.

- Click **Add**.

The clients or client groups you select are shown in the **Client groups** text box on the **Recipients** page, and the new settings profile is immediately sent to your clients' consoles.

When you assign a settings profile, if any of the child nodes of the selected node already has other settings profiles assigned by the web console user, a warning message is shown that asks which settings profile should prevail: the old settings profile or the new one.

Assigning settings from the list of settings profiles (Drag-and-drop)

Select the settings profile you want to assign and drag it to the client or client group to assign it to. The settings profile is automatically assigned to the clients' consoles, and the client group is added to the **Client groups** field on the settings profile **Recipients** page.

Indirect assignment of settings: Inheritance

Cytomic Nexus implements the same inheritance functionality as in the Endpoint Security family products installed on clients' systems. A web console user can indirectly assign settings to whole branches of the client tree, without having to configure each node (clients or client groups) individually.

For more information about this feature and the types of inheritance mechanisms supported in Cytomic Nexus, see section **Indirect assignment of settings: the two rules of inheritance** in chapter **Managing settings** of the product administration guide.

Viewing assigned settings

To view the settings assigned to clients' Aether-based products, go to the **Settings** menu at the top of the console. This window contains the following items:

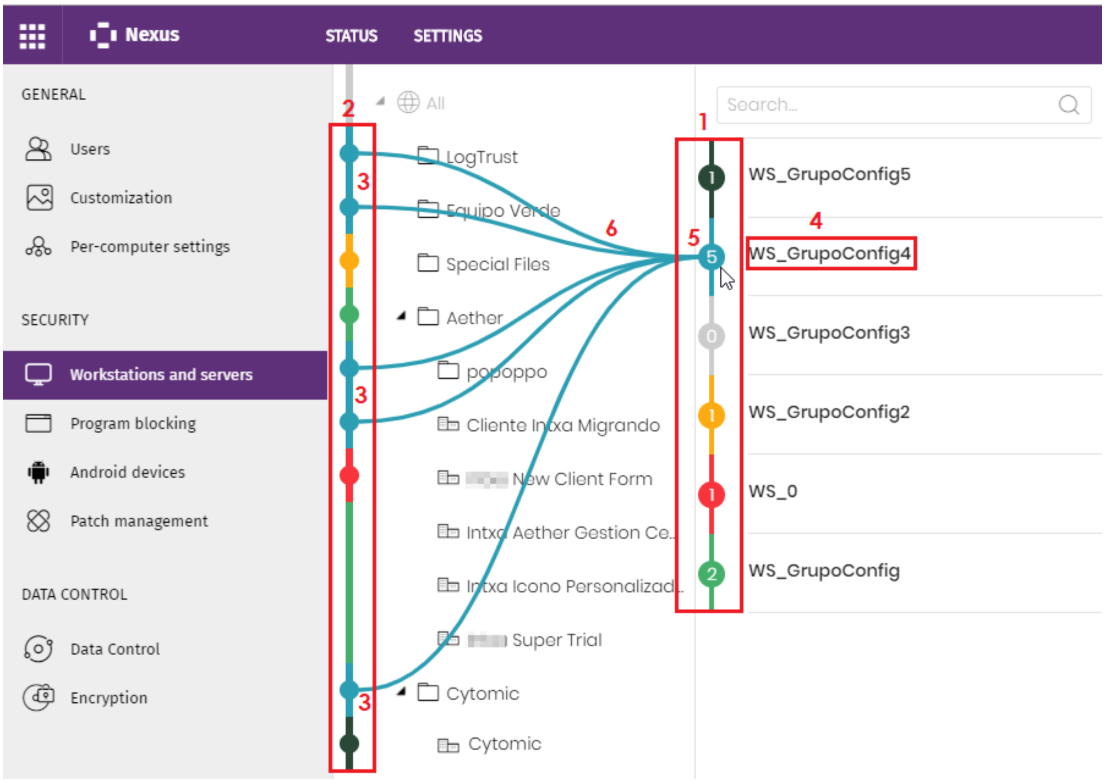


Figure 7.3: Viewing assigned settings

- **Left-hand panel**: Shows the available types of settings.
- **Right-hand panel**: Shows the existing settings of the selected type and the clients they have been assigned to. This panel contains the following items:
    - **Settings vertical bar (1)**: The existing settings appear in different colors. Each settings profile indicates the number of nodes in the client tree that it is assigned to.
    - **Client group tree vertical bar (2)**: Each color indicates the section of the client tree affected by the settings.

When a settings profile is created and assigned, Cytomic Nexus performs the following steps:

- Shows the settings in the list of available settings **(4)**.
- Creates a section in the settings vertical bar and assigns a color to it **(5)**. Each section displays the number of nodes the settings have been assigned to. If the settings have not been assigned to any nodes, the number “0” will be displayed.
- Marks, with the same color as that of the settings, the section of the client tree vertical bar affected by the settings **(3)**. If the same settings are assigned to different nodes in the client tree, all of those nodes will have the same color.
- Shows the relationship between a settings profile and the nodes it affects in the client tree through lines **(6)** visible when placing the cursor on the relevant sections of both vertical bars. The color of the lines will be the same as the color of the settings.

- If the client tree bar shows numbers associated with any of its sections, it means that those sections are collapsed and there are hidden child nodes that have exceptions to the settings.

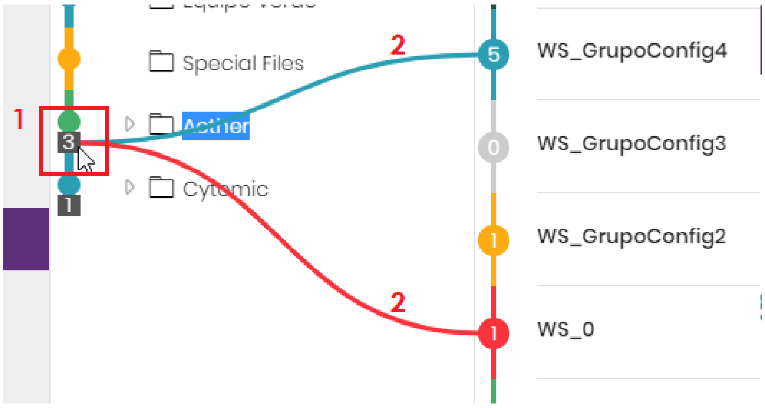


Figure 7.4: Viewing the settings assigned to nodes with exceptions

The number displayed **(1)** indicates the number of hidden child nodes that have specific settings assigned. Placing the cursor on the number in the square will display the color lines corresponding to the specific settings assigned **(2).**

Double-click the square to expand the client group vertical bar and show the hidden nodes.

Impact of assigning/sending settings

Clients' consoles contain both settings created by clients themselves and settings sent to them by the Cytomic Nexus console user. For this reason, Cytomic Nexus implements a number of rules to resolve situations where there can be conflicts or replacements between settings originating from both sources. The priority of a settings profile is determined by its owner, that is, the console from which the settings were created or modified:

- Settings created by a client using their console are owned by the client.
- Settings created in Cytomic Nexus and centrally sent to a client are owned by Cytomic Nexus.
- Settings created and sent from the Cytomic Nexus Web console whose recipients are later edited in the client's console are co-owned.

The implemented rules are as follows:

- **Settings owned by Cytomic Nexus**: these settings appear in the client's console with a green label with the text "Partner Center". They can be deleted and edited (synced) from the Cytomic Nexus Web console. Clients cannot directly delete or edit them, although they can add new recipients or delete any recipients they have added, in which case the settings become co-owned. If the settings are assigned to the **All** group in the client's console, they cannot be directly deleted by the client. Refer to **Causes and impact of changing the**

management mode for clients.

- **Settings owned by the client**: these settings cannot be accessed, viewed, edited, or deleted from the Cytomic Nexus Web console.
- **Co-owned settings**: these settings can be edited (synced) from the Cytomic Nexus Web console, respecting any recipients added by the client, but they cannot be deleted from that console. They cannot be deleted or edited by clients with the exception of adding or removing recipients, just like with settings owned by Cytomic Nexus. Just like settings owned by Cytomic Nexus, these settings appear in the client's console with a green label with the text "Partner Center".

Creating settings in clients' consoles

When the Cytomic Nexus Web console user assigns settings to one or more clients, the user is the owner of the settings. These settings are sent to each client's console and are associated to the **All** group in the client's computer tree to make sure that they are applied to all computers on the network. However, if any of the nodes in the client's computer tree already has settings manually assigned by the client, these settings will prevail over the settings inherited from the **All** group. Therefore, none of the child nodes of that node will receive the new settings.

When the Cytomic Nexus Web console user sends or assigns settings to a client, these settings are shown in the list of available settings in the client's console, with the following features:

- All settings sent or assigned to clients from the Cytomic Nexus Web console are read-only for clients, and appear with a green label and the text "Partner Center" in the client's list of settings. This way, they can be easily differentiated from the settings created by the client's network administrator.
- Clients can only add or remove recipients from a read-only settings profile, in which case the settings become co-owned. Nevertheless, read-only settings can be copied by clients and edited based on their needs, in which case the client becomes the owner of the copy.
- Changes made from the Cytomic Nexus Web console to the settings sent or assigned to clients are automatically synced in the clients' consoles. This synchronization is unidirectional, from Cytomic Nexus to clients. These changes are immediately reflected in clients' consoles and propagate to their devices in real time or within 15 minutes, depending on whether the **Enable real-time communication** option is selected or cleared. Refer to chapter "**Configuring the agent remotely**", section "**Configuring real-time communication**" of the relevant product's administration guide.
- Co-owned settings cannot be directly unassigned from the **All** group by clients.

Deleting settings from clients' consoles

The rules that govern centralized deletion of settings from the Cytomic Nexus Web console are as follows:

- The Cytomic Nexus Web console users can delete only the settings owned by them from clients' consoles. That is, those settings they have previously sent and which have not been edited by the client (these would be co-owned settings).
- Settings owned by the Cytomic Nexus Web console which are deleted are also removed from clients' consoles. Co-owned settings, however, are not deleted. For example, if a settings profile is deleted or a client is moved from one group to another in the Cytomic Nexus Web console, the settings will disappear from the affected client's console. However, if the client added a recipient to the settings, they will not be centrally removed even though they are no longer in use.
- Settings owned by the client which are overridden by settings owned by the Cytomic Nexus Web console user are not deleted. They are kept in the client's console.
- Even after a settings profile is deleted from the Cytomic Nexus Web console, clients will always have a settings profile assigned to the **All** group in their consoles. This might be another settings profile assigned from the Cytomic Nexus Web console through inheritance or, if there are no settings available for that client in Cytomic Nexus, the client's current settings are maintained, in which case the client becomes the owner of the settings.

Changing clients from one group to another

Changing a client from one group to another in the Cytomic Nexus Web console triggers the following actions:

- All settings owned by the Web console user and assigned to the client that is moved from the source group are deleted from the client's list of available settings.
- The client's list of settings will show the settings assigned to the new group.

Causes and impact of changing the management mode for clients

There are many reasons why a client might stop receiving centralized settings from the corresponding partner:

- The client stops authorizing Cytomic Nexus to access their console (see **Requirements for assigning centralized settings**).
- The client is removed from the Cytomic Nexus web console after the contractual relationship ends.
- The product management mode is changed from the Cytomic Nexus web console. See **Assigned product details** on page **54**.

When that happens, all settings owned by the Cytomic Nexus web console or co-owned with the client, excluding settings associated with the Cytomic SIEMConnect fo Partners module, become the property of the client:

- The “Partner Center” label no longer appears in the list of settings in the client’s console.
- The settings are no longer read-only for the client.
- The changes made to the settings in the Cytomic Nexus web console are not synced in the client’s console.
- In order to not disclose information shared by multiple clients, with **Per-computer settings** profiles with two-factor authentication enabled or an uninstall password assigned, the client’s console generates a new QR code and a new random password in the settings profile originally sent by the partner. For more information about how two-factor authentication works in the client’s console, see chapter **Configuring the agent remotely**, section **Configuring the anti-tamper protection and password** of the product administration guide.

Management mode chosen and Cytomic SIEMConnect fo Partners

Because the Cytomic SIEMConnect fo Partners settings do not affect the settings of the security product installed on the client’s network, the management mode you choose has no impact.

Consequences of restoring the Cytomic Nexus/client relationship

If the Cytomic Nexus/client relationship is restored after it is broken, Cytomic Nexus assigns the client the settings that correspond to the group the client belongs to.

Web console user permissions and visibility

*For more information about user accounts and permissions, see chapter **Access and authorization in Cytomic Nexus** on page **29**.*

Client tree visibility

The client tree shows only the clients the web console user has permissions on. If a web console user has permissions on a client group but does not have permissions on an intermediate node, the node does not show any clients.

The client tree in the web console shows only those clients that have allowed Cytomic Nexus to access their consoles and have been configured as centrally managed in the Cytomic Nexus console.

*Clients can authorize web console users to access their endpoint security product web console by going to the **Settings** menu at the top of their console, selecting **Users** from the side menu, and selecting the **Allow my reseller to access my console** checkbox.*

Editing settings

To edit a settings profile, the web console user must meet these requirements:

- The web console user must have Total Control, License and Security Administrator, or Security Administrator permissions. User accounts that have Monitoring permissions only cannot edit settings profiles.
- The web console user who edits a settings profile must have permissions on all clients to which the profile was assigned. If there are clients the user does not have permissions on, the user cannot edit the settings profile. Alternatively, the user can:
  - Assign/unassign or send settings profiles to clients the user has permissions on.
  - Create a new settings profile by copying an existing profile, edit it, and assign it or send it to clients the user has permissions on.

Copying settings

To copy a settings profile, the web console user must have Total Control, License and Security Administrator, or Security Administrator permissions. User accounts that have Monitoring permissions only cannot copy settings profiles.

Except in **Per-computer settings** profiles, when you copy a settings profile, all settings are copied except for the **Recipients** field, which is left empty.

With **Per-computer settings** profiles, the settings profile copied does not include:

- The **Recipients** field.
- The password to uninstall the security software from computers.
- The QR code generated for two-factor authentication.

*For more information, see chapter **Configuring the agent remotely**, section **Security against protection tampering** of the product administration guide.*

Deleting settings

To delete a settings profile, the web console user must have Total Control, License and Security Administrator, or Security Administrator permissions. User accounts that have Monitoring permissions only cannot delete settings profiles.

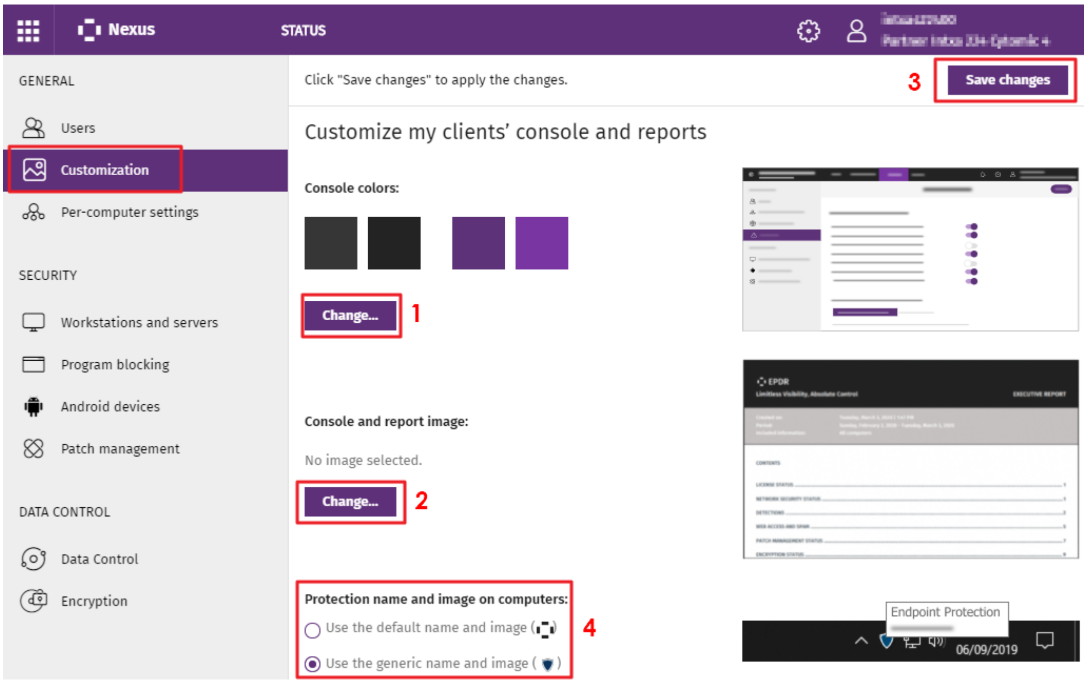
You can delete only settings profiles that do not have clients assigned. To unassign a settings profile from a client, the user account must have permissions on the client.

Customizing clients' consoles (Co-branding)

Cytomic Nexus enables you to change the look and feel of the console of the security products assigned to your clients to reflect your company's brand:

- Change the console colors.
- Change the console logo.
- Change the name of the security product installed on computers to a generic name.
- Change the icon of the security product installed on computers to a generic icon.

Accessing the customization settings



Click "Save changes" to apply the changes.

Customize my clients' console and reports

Console colors:

Console and report image:

No image selected.

Protection name and image on computers:

○ Use the default name and image

● Use the generic name and image

Figure 7.5: Accessing the customization feature for endpoint security products

To change the look and feel of the clients' console for clients with endpoint security products:

- In the top menu, select **Clients**. Select **Configure clients' products**. A page opens in a new tab in your browser.
- In the top menu, select **Settings**. Select the **Management** tab. From the side panel, select **Customization**. The **Customize my clients' console and reports** page opens.

Changing the console appearance

- Click **Change (1)** to select a color scheme from the eight available options.

Changing the image shown in the console and reports

- Click **Change (2)** to upload a new logo that replaces the product image in the client's console. The image must be a .JPG or .PNG file with a resolution of 128 x 48 pixels. Additionally, it must be less than 10 KB in size.
- After you have finished making all the changes, click **Save changes (3)**. The changes are immediately applied to the client's console.

Changing the security product name and icon shown on computers

- Click **Use the generic name and image (4)**.

Consequences of modifying these items:

- The agent name is Panda Endpoint Protection.
- The agent icon is the generic icon (shield).

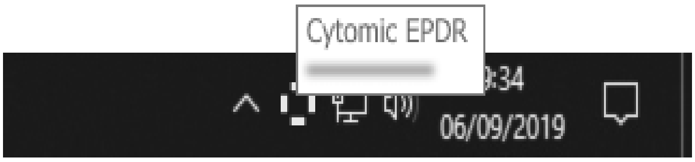


Figure 7.6: Security product generic name and image

- After you have finished making all the changes, click **Save changes (3)**. The changes are applied immediately and are visible in:
    - All windows shown by the agent on clients' computers, both during the installation process and later.
    - The quick launch bar on clients' computers.
    - The local console.

The products installed on clients' computers will not show the "Cytomic" name. For example, Panda Endpoint Protection will appear as "Endpoint Protection".

Clients' security status

Cytomic Nexus provides two large sets of tools that enable you to monitor the security status of your clients' computers:

- The security dashboard, which provides information about the overall status of the security software installed on clients' networks.

- Lists with information about:
    - Status of the security software installed on your clients' computers.
    - Number of risks detected for each of your clients.
    - Indicators of attack (IOA) detected.
    - Result of patch installation tasks on your clients' computers.
    - Available patches for your clients' computers.
    - Inbound connections to your clients' computers.
    - Overall information about users who log in to your clients' management consoles.

*For more information, see **Security dashboard lists**.*

The monitoring and visualization tools help you determine, in real time, the security status of your clients' networks and the impact of any potential security breach to facilitate the implementation of appropriate security measures.

Security dashboard widgets

The security dashboard contains widgets that show the security status of your clients' IT networks. Additionally, it provides a filter tool that enables you to quickly and directly find computers that meet certain characteristics.

Accessing the security dashboard

To access the security dashboard, in the top menu, select **Status**. Select **Security** 🛡. A page opens that contains counters showing the security of the computers managed by the clients that are visible to the user account used to access the partner console.

*For more information about user accounts and permissions, see chapter **Access and authorization in Cytomic Nexus** on page **29**.*

Filters available in the security dashboard

The security dashboard filter tool enables you to quickly and directly find clients' computers that meet certain characteristics.

The filters you select in the security dashboard filter the data shown in widgets. When you click a series in a widget, the filter settings configured in the security dashboard are also applied to the data shown in the **Clients' protection status** list that opens.

The security dashboard filters work in the same way as the filters in the clients' protection status list. For more information, see ***Available lists***

The **Clients' protection status** list enables you to access the security dashboard in each client's product console and the corresponding computer protection status lists with all your selected filters applied.

To access the security dashboard filter tool, click the **Filters** drop-down menu in the upper-left corner of the dashboard.

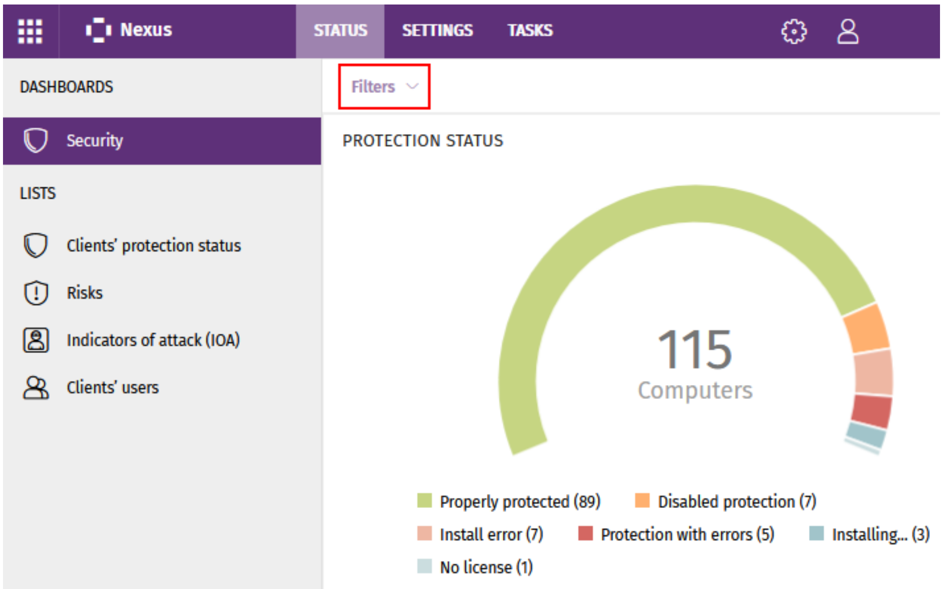


Figure 7.7: Selecting the security dashboard filters

The following is a description of the widgets, their areas and hotspots, and the available filters.

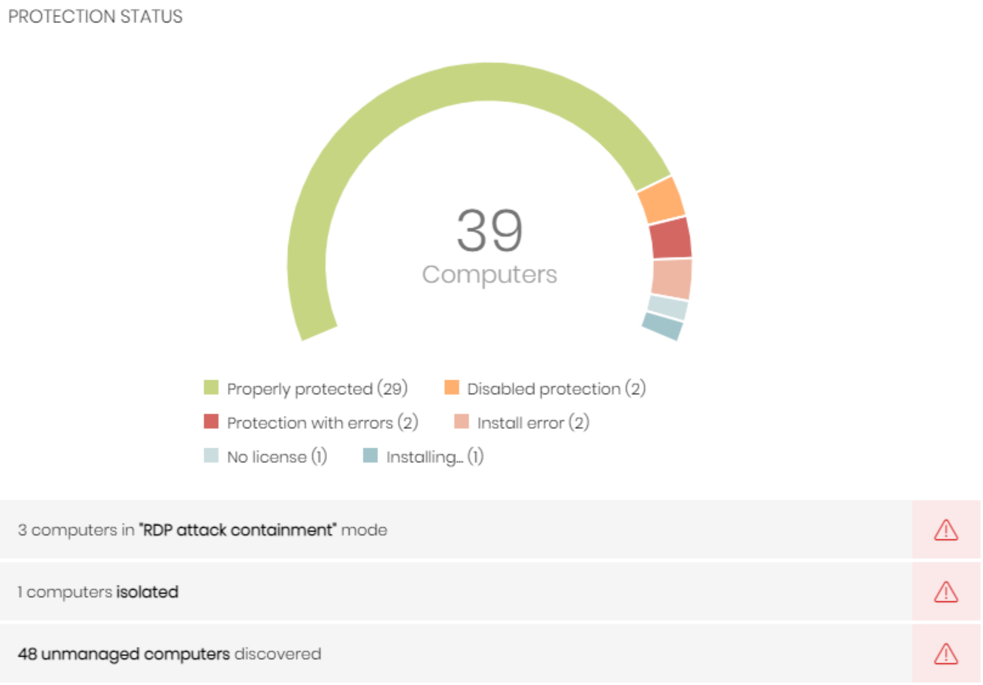
Protection status

This widget provides a graphical representation and percentage of clients' computers with the same status. It shows the clients' computers where the security software works correctly and where it does not, and computers with installation errors or problems The status of the network computers is represented with a circle with different colors and associated counters.

The sum of all percentages can be greater than 100% as the status types are not mutually exclusive. A computer can have different statuses at the same time.

At the bottom of the widget, you can find this information (if any):

- Number of clients' computers in **RDP attack containment** mode. Click the message to open the **Clients' protection status** list, filtered to show the computers that are in **RDP attack containment** mode.
- Number of clients' computers that are isolated. Click the message to open the **Clients' protection status** list, filtered to show isolated computers.
- Number of unmanaged computers discovered. Click the message to open the **Clients' protection status** list, filtered to show the number of unmanaged computers discovered on your clients' networks, in descending order.



3 computers in "**RDP attack containment**" mode ⚠

1 computers **isolated** ⚠

48 unmanaged computers discovered ⚠

Figure 7.8: Protection status panel

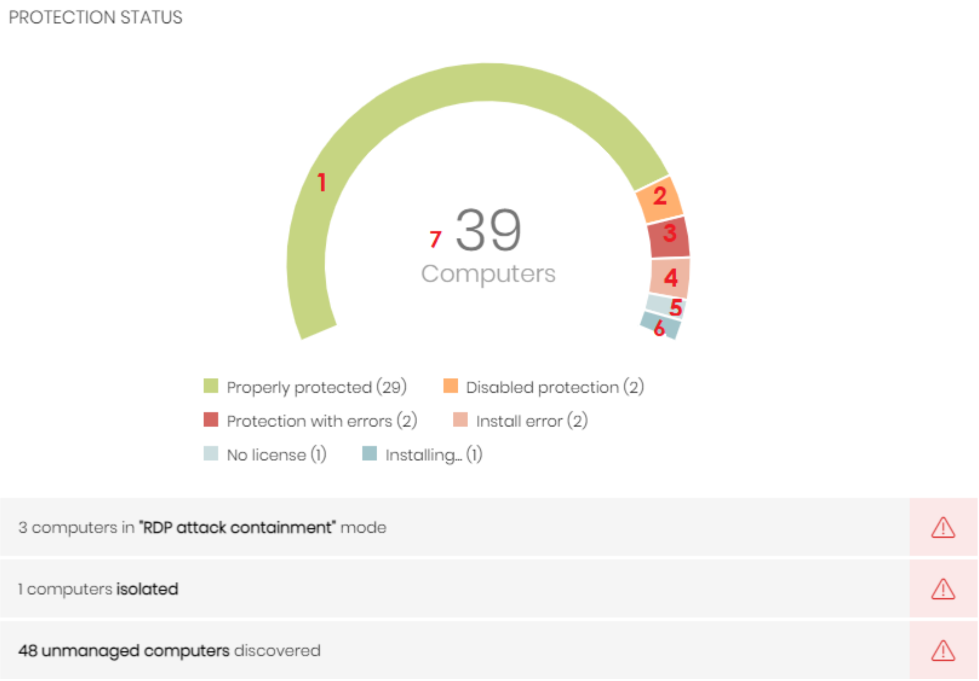
Meaning of the data displayed

Data	Description
Properly protected	Number of clients' computers where the security software installed without errors and is working correctly.
Disabled protection	Number of clients' computers where the antivirus protection or the advanced protection is disabled (the advanced protection will be available depending on the product purchased by the client and the operating system installed on the device).
Protection with errors	Number of clients' computers with the security software installed, but do not respond to the requests sent from the

Data	Description
	Cytomic servers.
Install error	Number of clients' computers on which the security software installation process could not be completed.
No license	Number of clients' computers that are unprotected because there are insufficient licenses or because an available license has not been assigned to the computer.
Installing	Number of clients' computers on which the security software is currently being installed.

Table 7.4: Description of the data displayed in the protection status panel

Lists accessible from the panel



3 computers in "RDP attack containment" mode

1 computers isolated

48 unmanaged computers discovered

Figure 7.9: Hotspots in the protection status panel

Click a hotspot in the panel to open the **Clients' protection status** list with these predefined filters:

Hotspot	Filter
(1)	Protection status = Properly protected.

Hotspot	Filter
(2)	Protection status = Disabled protection.
(3)	Protection status = Protection with errors.
(4)	Protection status = Install error.
(5)	Protection status = No license.
(6)	Protection status = Installing
(7)	No filter.

Table 7.5: Filters available in the clients' protection status list

Offline computers

This widget shows the number of clients' computers that have not connected to the Cytomic cloud for a number of days. These computers might be susceptible to security problems and require attention.

At the bottom of the widget, you can find information about the number of computers (if any) that have had connection problems to the Cytomic knowledge servers.

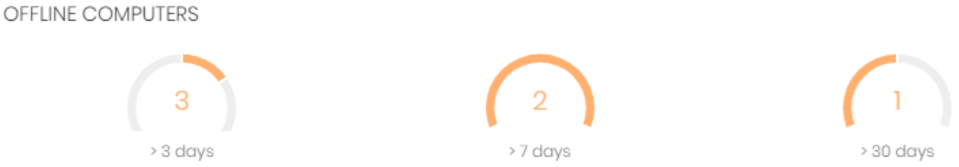


Figure 7.10: Offline computers panel

Meaning of the data displayed

Hotspot	Filter
> 3 days	Number of computers that have not reported their status in the last 3 days.
> 7 days	Number of computers that have not reported their status in the last 7 days.

Hotspot	Filter
> 30 days	Number of computers that have not reported their status in the last 30 days.

Table 7.6: Description of the data displayed in the offline computers panel

Lists accessible from the panel

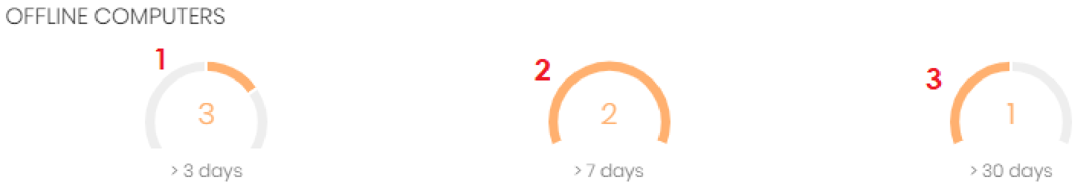


Figure 7.11: Hotspots in the offline computers panel

Click a hotspot in the panel to open the **Clients' protection status** list with these predefined filters:

Hotspot	Filter
(1)	Last connection = More than 3 days ago.
(2)	Last connection = More than 7 days ago.
(3)	Last connection = More than 30 days ago.

Table 7.7: Filters available in the offline computers list

Outdated protection

This widget shows:

- The number of clients' computers with a signature file that is more than three days older than the latest released file.
- The number of clients' computers with an antivirus engine that is more than seven days older than the latest released engine.

These computers might be vulnerable to attacks from threats.

- The number of clients' computers that require a restart to complete the update.

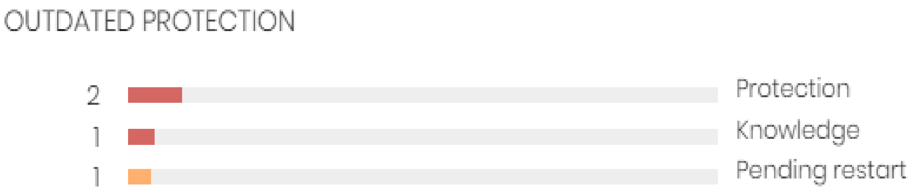


Figure 7.12: Outdated protection panel

Meaning of the data displayed

The widget shows the percentage and number of computers that are vulnerable because their protection is out of date, under three concepts: protection, knowledge, and pending restart. To view the percentage, point the mouse to the bars in the graph.

Data	Description
Protection	For at least seven days, the computer has had a version of the antivirus engine older than the latest released engine.
Knowledge	The computer has not updated its signature file for at least three days.
Pending restart	The computer requires a restart to complete the update.

Table 7.8: Description of the data displayed in the outdated protection panel

Lists accessible from the panel

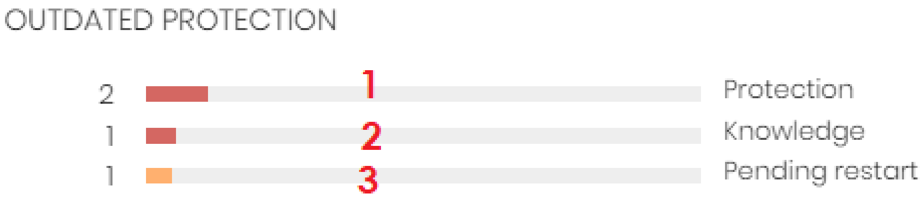


Figure 7.13: Hotspots in the outdated protection panel

Click a hotspot in the panel to open the **Clients' protection status** list with these predefined filters:

Hotspot	Filter
(1)	Protection up to date = No.

Hotspot	Filter
(2)	Knowledge up to date = No.
(3)	Protection up to date = Pending restart.

Table 7.9: Filters available in the clients' protection status list

Security dashboard lists

The security lists contain the data used to generate the widgets. They show detailed information about the security of the computers on the network.

Accessing the clients' security dashboard

- From the top menu, select **Status**. Select **Security** 🛡.
- From the top menu, select **Clients**. Select **Configure clients' products**. A page opens in a new browser tab.
- On the new tab, select **Status** from the top menu. These lists appear:
  - **Clients' protection status**: Shows the threats detected by the different protection modules for each of your clients. It also shows whether or not these modules are updated.
  - **Risks**: Shows the number of risks by computer for each of your clients. See chapter **Risk assessment** in the product administration guide.
  - **Indicators of attack (IOA)**: Shows a summary of the indicators of attack found for each of your clients. An IOA is a sequence of unusual actions found in the events generated on a client's computers and which are highly likely to be an attack. These attacks are typically at an early or exploitation stage and often do not use malware. Adversaries normally leverage the operating system own tools to execute their attacks and thereby hide the traces of their activity.
  - **Patch installation results**: Shows the results of installing program and operating system updates on the computers you manage.
  - **Endpoint Access Enforcement**: Shows information about inbound connections to computers on your clients' networks, which meet the conditions configured in the Endpoint Access Enforcement feature. See chapter **Endpoint Access Enforcement** in the product administration guide.
  - **Clients' users**: Provides overall information about users who log in to the management consoles of the clients you manage. It indicates which user logged in to the console

and when, whether the login password was changed, and whether two-factor authentication (2FA) was required to log in to the console.

Monitoring and access based on the permissions assigned to the user account

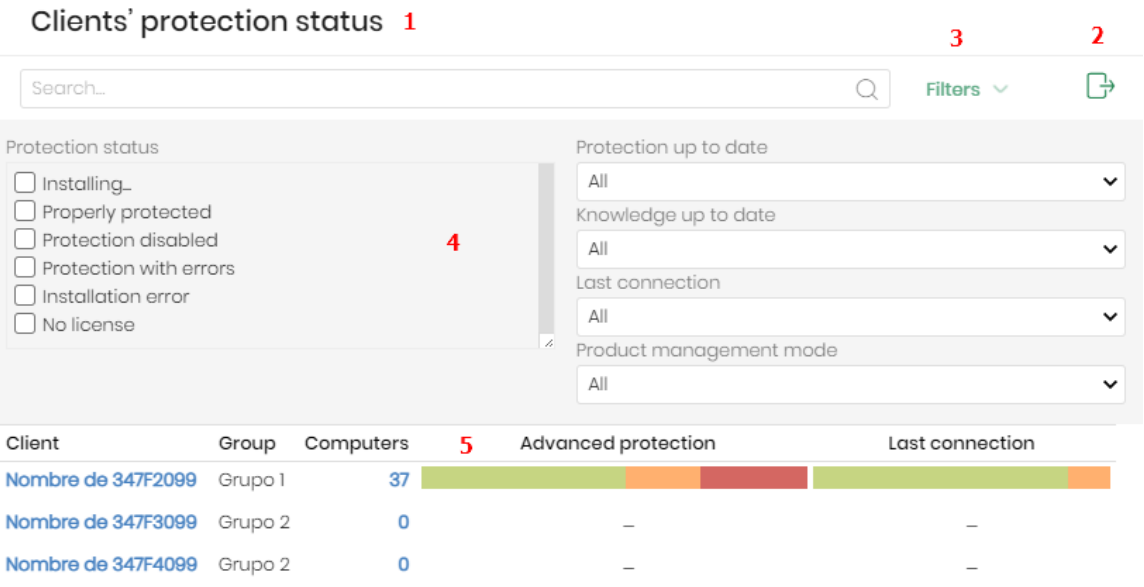
> *For more information about user accounts and permissions, see chapter **Access and authorization in Cytomic Nexus** on page **29**.*

The **Status** page shows only clients visible to the user account used to log in to the console. This visibility is defined when you configure the permissions assigned to the user account. See **Access and authorization in Cytomic Nexus** on page **29**.

Sections of a list

All lists have a number of tools in common to make interpretation easier. This section describes the main elements in a sample list.

- **List name (1)**: Identifies the information in the list.
- **Export (2)**: Generates an Excel file with the content of the list.
- **Filter and search tools (3)**: Click the button to open a panel with the available filter tools. After you configure them, click the **Filter (6)** button.
- **Filter and search parameters (4)**: Enable you to filter the data in the list.
- **Sorting order (5)**: Click a column header to sort the list by that column. Click the same header a second time to switch between ascending and descending order. This is indicated with arrows (a ↑ arrow or a ↓ arrow). If you are accessing the management console from a small-size mobile device, click the ⇩ icon in the bottom-right corner of a list to show a menu with the names of the columns included in the table.



Clients' protection status

Search...

Filters

Protection status

□ Installing...
□ Properly protected
□ Protection disabled
□ Protection with errors
□ Installation error
□ No license

Protection up to date: All

Knowledge up to date: All

Last connection: All

Product management mode: All

Client	Group	Computers	Advanced protection	Last connection
Nombre de 347F2099	Grupo 1	37	🟩🟧🟥	🟩🟧
Nombre de 347F3099	Grupo 2	0	–	–
Nombre de 347F4099	Grupo 2	0	–	–

Figure 7.14: Parts of a list

- **Pagination**: Pagination controls appear at the bottom of the list to help you quickly move from page to page.

Icon	Description
25 rows ⌄	Rows per page selector.
1 to 25 of 67	Number of rows shown out of the total number of rows.
«	First page link.
‹	Previous page link.
1 2 3	Numbered links to access pages directly.
›	Next page link.
»	Last page link.

Table 7.10: Pagination controls

Available lists

Lists show information about the security status of computers belonging to clients visible to the Cytomic Nexus user. See **Web console user permissions and visibility** on page **87**.

Clients' protection status

This list includes detailed information about the status of each client's endpoint security software and includes filters to show clients with unprotected computers.

It enables you to quickly access different sections in each client's management console.

When the list includes a color bar, you can point to it with the mouse to show detailed information:

- The number of computers in each group.
- The percentage of the total number of computers on the network.
- The **Go to client's console** link.

Field	Description	Values
Client	The client name or ID. Click the name of a client to open the client's console on the **Status** page of the security dashboard.	Character string
Group	The name of the group the client belongs to.	Character string
Unmanaged computers discovered	The total number of unmanaged computers and devices on the client's network. Click the number of computers to open the client's console on the **Unmanaged computers discovered** list page with the filters you selected applied. This link is available to Cytomic Nexus console users with permissions higher than read-only.	Numeric value
Managed computers	The total number of computers and devices with Cytomic products installed. Click the number of computers to open the client's console on the **Computer protection status** list page with the filters you selected applied. This link is available to Cytomic Nexus console users with permissions higher than read-	Numeric value

Field	Description	Values
	only.	
Advanced protection	A color bar that indicates the advanced protection status of the computers and devices.	• **Red**: Computers with protection errors, with disabled protection software, with installation errors, or without a license. • **Green**: Computers where the protection software is OK or in the process of installation. • **Hyphen** [-]: The client's endpoint security product does not include this feature.
Antivirus	A color bar that indicates the antivirus protection status of the computers and devices.	• **Red**: Computers with protection errors, with disabled protection software, with installation errors, or without a license. • **Green**: Computers where the protection software is OK or in the process of installation. • **Hyphen** [-]: The client's endpoint security product does not include

Field	Description	Values
		this feature.
Protection up to date	A color bar that indicates the update status of the security software on the client's computer or device.	• **Red**: Computers with out-of-date protection software. • **Orange**: Computers that require a restart to complete the update. • **Green**: Computers with up-to-date protection software.
Knowledge	A color bar that indicates the update status of the signature file on the client's computer or device.	• **Red**: Computers with an out-of-date signature file. • **Green**: Computers with an up-to-date signature file.
Last connection	A color bar that indicates the date when connection status was last sent to the Cytomic cloud.	• **Green**: Less than 3 days ago. • **Orange**: More than 3 days ago. • **Darker orange**: More than 7 days ago. • **Red**: More than 30 days ago.

Table 7.11: Fields in the Protection Status list for clients with Cytomic products

Fields displayed in the exported file

Field	Description	Values
Client	The name of the client account the service belongs to.	Character string
ID	The ID Cytomic assigned the client at registration time. This ID is requested in all communications between the client and the support department for incident management.	Character string
Group	The name of the group the client belongs to.	Character string
Centralized management	Indicates whether or not the product is centrally managed. For more information, see chapter **Endpoint security product settings management**	• **Yes**: Centrally managed • **No**: Not centrally managed
Used licenses	The total number of licenses used by the client.	Numeric value
Unmanaged computers discovered	The total number of unmanaged computers and devices on the client's network.	Numeric value
Managed computers	The total number of computers and devices with Cytomic products installed.	
Advanced protection - Installing	The number of computers that reported the relevant status.	Numeric value
Advanced protection - Properly protected	The number of computers that reported the relevant status.	Numeric value
Advanced protection - Protection disabled	The number of computers that reported the relevant status.	Numeric value

Field	Description	Values
Advanced protection - Protection with errors	The number of computers that reported the relevant status.	Numeric value
Advanced protection - Installation error	The number of computers that reported the relevant status.	Numeric value
Advanced protection - No license	The number of computers that reported the relevant status.	Numeric value
Antivirus - Installing	The number of computers that reported the relevant status.	Numeric value
Antivirus - Properly protected	The number of computers that reported the relevant status.	Numeric value
Antivirus - Protection disabled	The number of computers that reported the relevant status.	Numeric value
Antivirus - Protection with errors	The number of computers that reported the relevant status.	Numeric value
Antivirus - Installation error	The number of computers that reported the relevant status.	Numeric value
Antivirus - No license	The number of computers that reported the relevant status.	Numeric value
Protection up to date	The number of computers that reported the relevant status.	Numeric value
Protection out of date	The number of computers that reported the relevant status.	Numeric value

Field	Description	Values
Protection pending restart	The number of computers that reported the relevant status.	Numeric value
Knowledge	The number of computers that reported the relevant status.	Numeric value
Knowledge out of date	The number of computers that reported the relevant status.	Numeric value
Last connection - Less than 3 days ago	The number of computers that last connected to the Cytomic cloud in the specified time interval.	Numeric value
Last connection - Between 3 and 30 days ago	The number of computers that last connected to the Cytomic cloud in the specified time interval.	Numeric value
Last connection - More than 30 days ago	The number of computers that last connected to the Cytomic cloud in the specified time interval.	Numeric value

Table 7.12: Fields in the Protection Status exported file for clients with Cytomic products

Filter tool

Field	Description	Values
Computer type	The type of device.	• Workstation • Laptop • Server • Mobile device
Platform	The operating system installed on the computer.	• All • Windows • Linux • macOS • iOS

Field	Description	Values
Product management mode	Indicates whether or not the product is centrally managed.	• All • Not centrally managed • Centrally managed
Protection up to date	The protection module installed on the computer is the latest published version.	• All • Up to date • Pending restart • Out of date
Knowledge	The signature file on the computer is the latest published version.	• All • Up to date • Out of date
Last connection	The last time the client status was sent to the Cytomic cloud.	• All • Less than 24 hours ago • Less than 3 days ago • Less than 7 days ago • Less than 30 days ago • More than 3 days ago • More than 7 days ago • More than 30 days ago
Connection to knowledge servers	Indicates the result of the last connection between the computer and the Cytomic knowledge servers.	• All • OK • With problems

Field	Description	Values
Protection status	Indicates the protection status.	• Installing • Properly protected • Protection disabled • Protection with errors • Installation error • No license
Isolation status	Indicates the isolation status of the computer.	• Not isolated • Isolated • Isolating • Stopping isolation
"RDP attack containment" mode	Indicates whether or not the computer is in "RDP attack containment" mode.	• All • No • Yes

Table 7.13: Filters available in the Protection Status list for clients with Cytomic products

Risks by client

This list shows the risk level for each client.

*For more information, see chapter "**Risk assessment**" in the product administration guide.*

When the list includes a color bar, you can point to it with the mouse to show detailed information:

- The number of computers at each risk level.
- The percentage over the total number of computers on the client's network.
- The **Go to client's console** link.

Field	Description	Values
Client	The client name or ID. Click it to open the client's console on the **Status** page of the risk assessment module.	Character string
Group	The name of the group the client belongs to.	Character string
Computers	The total number of computers and devices with detected risks.. Click it to open the client's console on the **Risks by computer** list page.	Numeric value
Risk by computer	A distribution graph that shows the risk level by computer (Critical, High, Medium, or No Risk). When you point the mouse to the color bars, a label appears with detailed information. Click the percentage shown in the label to go to the **Risks by computer** list in the client's console, filtered by the relevant risk.	• **Red**: The number of computers that have a critical risk level. • **Orange**: The number of computers that have a high risk level. • **Yellow**: The number of computers that have a medium risk level. • **Green**: The number of computers with risks that have no impact on security.

Table 7.14: Fields in the Risks by Client list

Fields displayed in the exported file

Field	Description	Values
Client	The name of the client account the service belongs to.	Character string
ID	The ID Cytomic assigned the client at registration time. This ID is requested in all communications between the client and the support department for incident management.	Character string
Group	The name of the group the client belongs to.	Character string
Computers with critical risks	The number of computers that have a critical risk level.	Numeric value
Computers with high risks	The number of computers that have a high risk level.	Numeric value
Computers with medium risks	The number of computers that have a medium risk level.	Numeric value
Computers with no risk	The number of computers with risks that have no impact on security.	Numeric value

Table 7.15: Fields in the Risks by Client exported file

Filter tool

Field	Description	Values
Search for client	Filters clients by name or group.	Character string
Computer type	Filters computers by type.	• Workstation • Laptop • Server • Mobile device

Field	Description	Values
Platform	The operating system installed on the computer.	• All • Windows • Linux • macOS • Android • iOS
Risk level	The risk level assigned.	• Critical • High • Medium • No risk

Table 7.16: Filters available in the Risks by Client list

Indicators of attack (IOA)

This list shows the total number of indicators of attack detected for each client, regardless of whether they were reviewed or not, and the number of indicators that were not reviewed by you or the client's administrator.

It enables you to quickly access different sections in each client's management console.

Field	Description	Values
Client	The client name or ID. Click it to open the client's console on the **Status** page of the security dashboard.	Character string
Group	The name of the group the client belongs to.	Character string
Computers	The total number of computers and devices with Cytomic products installed. Click it to open the client's console on the **Computers** page and view a list of computers with an endpoint security product installed.	Numeric value
Detected	The total number of indicators of attack detected on the	Numeric

Field	Description	Values
indicators of attack (IOA)	client's computers and devices. Click it to open the client's console on the **Indicators of attack (IOA)** page, with the **Status** filter set to **All**, to view a history of all IOAs detected on the client's network.	value
Pending indicators of attack (IOA)	The total number of unconfirmed indicators of attack detected on the client's computers and devices Click it to open the client's console on the **Indicators of attack (IOA)** page, with the **Status** filter set to **Pending**, to view all the IOAs that were not reviewed or resolved by you or the client's administrator.	Numeric value
Last detection	The date and time when the last indicator of attack was detected.	Date

Table 7.17: Fields in the Indicators of Attack list

Fields displayed in the exported file

Field	Description	Values
Client	The client name or ID.	Character string
Group	The name of the group the client belongs to.	Character string
Computers	The total number of computers and devices with Cytomic products installed.	Numeric value
Detected indicators of attack (IOA)	The total number of indicators of attack detected on the client's computers and devices.	Numeric value
Pending indicators of attack (IOA)	The total number of unconfirmed indicators of attack detected on the client's computers and devices	Numeric value
Last detection	The date and time when the last indicator of attack	Date

Field	Description	Values
	was detected.	

Table 7.18: Fields in the Indicators of Attack exported file

Filter tool

Field	Description	Values
Status	• **Archived**: The IOA no longer requires administrator attention because it was a false positive or was resolved. • **Pending**: The IOA was not investigated by the administrator.	Enumeration
Risk	The impact of the IOA detected.	• Critical • High • Medium • Low • Unknown
Indicator of attack (IOA)	The name of the rule that detected the pattern of events that triggered the IOA. The drop-down menu shows only the names of the IOA rules displayed in the list.	Enumeration
Action	The type of action taken by the security software installed on the computer.	• Reported • Attack blocked
Tactic	The category of the attack tactic that generated the IOA, mapped to the MITRE matrix. The drop-down menu shows only the tactics associated with the IOAs displayed in the list.	Enumeration
Technique	The category of the attack technique that generated the IOA, mapped to the MITRE matrix. The drop-down menu shows only the techniques associated with the IOAs displayed in the list.	Enumeration

Field	Description	Values
Last detection	The time period when the indicators of attack were detected.	• Last 24 hours • Last 7 days • Last month

Table 7.19: Filters available in the Indicators of Attack (IOA) list

Patch installation results

This list shows data only for clients that have the Cytomic Patch module. See ***Service management models for endpoint security products****.*

This list provides a summary of the patch installation history for each client and shows the results of patch installation tasks, following these criteria:

- If there are multiple failed attempts to install a patch on a computer, only the last attempt is logged.
- If there are multiple failed attempts to install a patch on a computer but installation finally succeeds, the solution logs only one successful installation.
- If a patch installs successfully on two computers, the solution logs two successful installations.

Field	Description	Values
Client	The client name or ID.	Character string
Group	The name of the group the client belongs to.	Character string
Patch management	Indicates whether the client purchased Cytomic Patch.	Character string
Computers with required restart	The total number of computers and	Numeric value

Field	Description	Values
	devices that must restart to complete installation or uninstallation of patches.	
Patch installation results	A color bar that indicates the status of the last patch installation attempt on clients' computers.	• **Green**: The number of installed patches. • **Yellow**: The number of patches that require a computer restart for installation. This count does not include patches that require a computer restart for uninstallation, therefore this number might not match the number in the **Computers with required restart** field. • **Orange**: The number of patches with installation errors. • **Red**: The number of patches with download errors. • **Gray**: There are no items for the client for the selected criteria.

Table 7.20: Fields in the Patch Installation Results list

Fields displayed in the exported file

The exported file logs the operations performed on each client's computers with Cytomic Patch licenses assigned. It logs patch installations and uninstallations, as well as errors. The file logs only the last operation of each type on each computer.

Field	Description	Values
Client	The client name or ID.	Character string
Computer type	The type of device.	• Workstation • Laptop • Server
Computer	The computer name.	Character string

Field	Description	Values
IP address	The computer IP address.	Numeric value
Domain	The domain the computer belongs to.	Character string
Description		Character string
Platform	The operating system installed on the computer.	• Windows • Linux • macOS
Group	The name of the group the computer belongs to.	Character string
Date	The date of the last operation performed on the patch.	Date
Program	The name of the program or Windows operating system version involved in the patch operation.	Character string
Version	The version of the program involved in the patch operation.	Numeric value
Patch	The name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Criticality	The update severity and type.	• Other patches (non-security-related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified

Field	Description	Values
		(security-related) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	The CVE (Common Vulnerabilities and Exposures) ID that identifies the vulnerability associated with the patch	Character string
KB ID	The ID of the Microsoft Knowledge Base article that describes the vulnerability fixed by the patch and its requirements (if any).	Character string
Release date	The date when the patch was released for download and application.	Date
Installation	The status of the patch.	• Installed • Requires restart • The patch is no longer required • Uninstalled (requires restart) • Error
Installation error	The specific type of error occurred.	• Installation error • Uninstallation error • Download error
Download URL	URL to download the patch individually.	Character string
Result code	The operation result code: success or failure reason. For more information about the result code, see the vendor documentation.	Numeric value
Task name	The name of the task associated with the operation performed.	Character string

Field	Description	Values
Task launch date	The date when the task was scheduled to run.	Date
Task start date	The date when the task started to run.	Date
Task end date	The date when the task finished to run.	Date

Table 7.21: Fields in the Patch Installation Results exported file

Filter tool

Field	Description	Values
Search	Filters by client name or group.	Character string
Show	Shows all clients or only clients that purchased Cytomic Patch.	• All clients • Only clients with patch management
Date	The time period when the Cytomic Patch operation occurred.	• Last 24 hours • Last 7 days • Last month
Platform	Filters by the operating system installed on the client's computers.	• All • Windows • Linux • macOS
Computer type	The type of device.	• Workstation • Laptop • Server
Installation	Filters by the patch installation task result on the client's computers.	• Installed • Requires restart • Download error • Installation error
Criticality	Filters by the severity of the patch installed on	• Other patches (non-

Field	Description	Values
	the client's computers.	security-related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related)

Table 7.22: Filters available in the Patch Installation Results list

Available patches

This list shows details of all patches that are available for each client that has the Cytomic Patch module. Each row in the list corresponds to a patch-client pair.

Field	Comment	Values
Client	Name of the client with outdated software.	Character string
Group	Folder in the Cytomic Nexus group tree to which the client belongs.	Character string
Occurrences	Number of computers the patch is available for.	Numeric value
Program	Name of the outdated program or operating system version with missing patches.	Character string
Version	Version number of the outdated program.	Numeric value
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Release date	Date when the patch was released for download and application.	Date
Criticality	Update severity rating and type.	• Other patches (non-security-

Field	Comment	Values
		related) - Critical (security-related) - Important (security-related) - Moderate (security-related) - Low (security-related) - Unspecified (security-related) - Service Pack

Table 7.23: Fields in the Available Patches list

Filter tool

Field	Comment	Values
Search	Client name or folder in the Cytomic Nexus group tree.	Character string
Platform	Operating system installed on the computer.	- All - Windows - Linux - macOS
Patch release	Date when the patch was released and is available to download.	- All - Less than 7 days ago - Less than 14 days ago

Field	Comment	Values
		• Less than 1 month ago • Less than 2 months ago • More than 7 days ago • More than 14 days ago • More than 1 month ago • More than 2 months ago
Computer type	Type of device.	• Workstation • Laptop • Server
Patch type	Type of patch.	• App patches • Operating system patches
Program	Name of the outdated program or operating system version with missing patches.	Character string
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.)	Character string
Patch installation	Patch installation option.	• Patch installation enabled • Test computer for patch installation • Patch installation disabled
Criticality	Update severity rating and type.	• Other patches

Field	Comment	Values
		(non-security-related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
Installation	Shows patches that are in the process of installation, filtering them by the installation stage they are in.	• Pending • Requires manual download • Pending (manually downloaded) • Pending restart
Show non-downloadable patches	Shows patches Cytomic Patch cannot directly download because there are additional requirements set by the vendor (EULA acceptance, login credentials, CAPTCHA, etc.).	Boolean
CVE	CVE (Common Vulnerabilities and Exposures) ID that describes the vulnerability associated with the patch.	Character string

Table 7.24: Filters available in the Available Patches list

Detected patch page

Click a row in the list. The **Detected patch** page opens and shows details of the patch. This data might vary depending on the operating system installed on the client's computers.

Field	Comment	Values
Patch	Name of the patch or update and additional information (release date, Knowledge Base number, etc.).	Character string
Program	Name of the outdated program or operating system version with missing patches.	Character string
Program version	Version number of the outdated program. Not available for macOS or Linux patches.	Character string
Family	Name of the product with patches pending installation or a reboot. Not available for macOS or Linux patches.	Character string
Vendor	Company that created the outdated program. Not available for macOS or Linux patches.	Character string
Criticality	Update severity rating and type.	• Other patches (non-security-related) • Critical (security-related) • Important (security-related) • Moderate (security-related) • Low (security-related) • Unspecified (security-related) • Service Pack
CVEs (Common	CVE (Common Vulnerabilities and Exposures) ID	Character string

Field	Comment	Values
Vulnerabilities and Exposures)	that describes the vulnerability associated with the patch.	
Client	Name of the client with outdated software.	Character string
Occurrences	Number of computers the patch is available for.	Numeric value
Release date	Date when the patch was released for download and application.	Date
Download size	Patch size, in a compressed format. Applying the patch or update might require more space on the target computer storage media than indicated in this field.	Numeric value
KB ID	ID of the Microsoft Knowledge Base article that describes the vulnerability fixed by the patch and the patch requirements (if any). Not available for macOS or Linux patches.	Character string
Download URL	URL to download the patch individually.	Character string
File name	Name of the file that contains the patch.	Character string
Description	Information about the impact the vulnerability could have on computers. Not available for macOS or Linux patches.	Character string

Table 7.25: Fields on the Detected Patch page

Connections identified by Endpoint Access Enforcement

This list shows the clients where Endpoint Access Enforcement has identified connections to computers that meet the conditions defined in the settings. For more information, see chapter **Endpoint Access Enforcement** in the product administration guide.

The data in the list refers to clients visible to the user account used to log in to the Cytomic Nexus console. For more information about user accounts and permissions, see chapter ***Access and authorization in Cytomic Nexus*** *on page* ***29****.*

The list provides information about managed and unmanaged clients, as well as clients that do not have the Endpoint Access Enforcement feature available because they do not meet the minimum requirements. For more information about minimum requirements, see chapter **Endpoint Access Enforcement settings** in the product administration guide.

Field	Description	Values
Client	The client name or ID. Click it to open the client's console on the **Status** page of the **Endpoint Access Enforcement** dashboard.	Character string
Group	The name of the group that the client belongs to.	Character string
Identified connections	The number of connections detected on the client's computers that have Endpoint Access Enforcement enabled. Click it to open the client's console on the **Connections identified by Endpoint Access Enforcement** list page. For more information, see section **Endpoint Access Enforcement module lists** in chapter **Endpoint Access Enforcement** in the product administration guide.	Numeric value Hyphen: The feature is not available for the client.
Connections by condition	Conditions in connections to computers on the network. For more information, see section **Security characteristics of connecting computers** in chapter **Endpoint Access Enforcement** in the product administration guide.	• **Gray**: Number of connections that meet the Unmanaged/Unavailable condition. • **Blue**: Number of connections that meet the Managed by Another Account condition.

Field	Description	Values
	Point to the bar to show a list of the number of identified connections for each condition. Click the **Go to client's console** link to go to the **Connections identified by Endpoint Access Enforcement** list in the client's console. For more information, see section **Endpoint Access Enforcement module lists** in chapter **Endpoint Access Enforcement** in the product administration guide.	• **Purple**: Number of connections that meet the Protection Not Enabled condition. • **Red**: Number of connections that meet the Critical Risk condition. • **Orange**: Number of connections that meet the High Risk condition. • **Yellow**: Number of connections that meet the Medium Risk condition.
Connections by monitored protocol	Monitored protocols identified in connections to computers on the network. For more information, see section **Monitoring inbound connection protocols** in chapter **Endpoint Access Enforcement** in the product administration guide. Point to the bar to show a list of the number of identified connections for each protocol. Click the **Go to client's console** link to go to the **Connections identified by Endpoint Access Enforcement** list in the client's console. For more information, see section **Endpoint Access Enforcement module lists** in chapter **Endpoint Access Enforcement** in the product administration guide.	• **Gray**: Number of connections over the SMB protocol. • **Blue**: Number of connections over the RDP protocol. • **Purple**: Number of connections over other protocols.

Table 7.26: Fields in the Connections Identified by Endpoint Access Enforcement list

Fields displayed in the exported file

Field	Description	Values
Client	The client name or ID.	Character string
Group	The name of the group that the client belongs to.	Character string
Identified connections	The number of connections detected on the client's computers that have Endpoint Access Enforcement enabled.	Numeric value
Unmanaged/Unavailable	The number of connections received from computers that meet one of these conditions: • Do not have a supported security software installed. See chapter **Minimum requirements** in the product administration guide. • Do not have the minimum required version of the security software installed. See chapter **Minimum requirements** in the product administration guide. • Are unavailable for connection (a firewall prevents the connection).	Numeric value
Managed by another account	The number of connections received from computers managed by an account other than the account used to manage the target computer.	Numeric value
Protection not enabled	The number of connections received from computers whose security software is up to date but disabled. See chapter **Minimum requirements** in the product administration guide.	Numeric value
Critical Risk	The number of connections received from computers whose risk level is greater than	Numeric value

Field	Description	Values
	or equal to Critical. See chapter **Risk assessment** in the product administration guide.	
High Risk	The number of connections received from computers whose risk level is greater than or equal to High. See chapter **Risk assessment** in the product administration guide.	Numeric value
Medium Risk	The number of connections received from computers whose risk level is greater than or equal to Medium. See chapter **Risk assessment** in the product administration guide.	Numeric value
Protocols	The number of connections detected on computers, over the different protocols monitored by Endpoint Access Enforcement. For more information, see section **Monitoring inbound connection protocols** in chapter **Endpoint Access Enforcement** in the product administration guide.	Numeric value
Custom	The number of connections detected on computers, over custom protocols entered by the administrator. For more information, see section **Monitoring inbound connection protocols** in chapter **Endpoint Access Enforcement** in the product administration guide.	Numeric value

Table 7.27: Fields in the Connections Identified by Endpoint Access Enforcement exported file

Filter tool

Field	Description	Values
Search for client	Filters clients by name.	Character string
Search for group	Filters clients by group.	Character string
Dates	Set a time period, from the current moment back.	• Last 24 hours • Last 7 days • Last month
Condition	Filters the list of detected connections by the condition assigned by Endpoint Access Enforcement. For more information, see section **Security characteristics of connecting computers** in chapter **Endpoint Access Enforcement** in the product administration guide.	• All • Unmanaged/Unavailable • Managed by another account • Protection not enabled • Risk level greater than or equal to: ◦ Medium ◦ High ◦ Critical
Action	Filters the list by the action taken by Endpoint Access Enforcement on the connection.	• Allowed • Blocked • All
Protocol	Filters the list by the connection protocol monitored by Endpoint Access Enforcement.	• All • SMB • RDP • Other protocols

Table 7.28: Filters available in the Connections Identified by Endpoint Access Enforcement list

Clients' users

This list provides global information about users who log in to the management consoles of the clients you manage. This data is very useful for large networks, because it specifies which users logged in to the console and when. Additionally, it shows when the console login password was last changed and whether two-factor authentication was required to log in to the console.

*For a client's users to appear in the list, you must be able to access the client's console. In the client's console, click **Settings**. From the side menu, select **Users**. Select the **Allow my reseller to access my console** checkbox.*

Field	Description	Values
Client	The client name or ID.	Character string
Group	The name of the group that the client belongs to.	Character string
User	The first name and last name for the user. If the user did not provide a first name and last name, the text before the @ symbol in the user's email address appears. Example: If the user's email address is *my.user@gmail.com*, *my.user* appears. When you click it, the client's console opens on the **Users** page (this feature is not available if the user who accesses the Cytomic Nexus console has read-only permissions only).	Character string
Email	The user's email address. When you click it, the client's console opens on the **Users** page (this feature is not available if the user who accesses the Cytomic Nexus console has read-only permissions only).	Character string
Role	The role assigned to the user account.	Character string
Status	Indicates whether the user account is activated or blocked.	Character string

Field	Description	Values
2FA required	Indicates whether two-factor authentication (2FA) is required to log in to the management console. When you click it, the client's console opens on the **Security** page. There you can enable or disable 2FA (this feature is not available if the user who accesses the Cytomic Nexus console has read-only permissions only).	Character string
2FA enabled	Indicates whether the user has two-factor authentication (2FA) enabled.	Character string
Password changed	Indicates the day and time the management console login password was last changed.	Character string
Last access	Indicates the day and time the user last logged in to the management console.	Numeric value

Table 7.29: Fields in the Clients' Users list

Fields displayed in the exported file

Field	Description	Values
Client	The client name or ID.	Character string
Group	The name of the group that the client belongs to.	Character string
User	The first name and last name for the user. If the user did not provide a first name and last name, the text before the @ symbol in the user's email address appears. Example: If the user's email address is *my.user@gmail.com*, *my.user* appears.	Character string
Email	The user's email address.	Character string
Role	The role assigned to the user account.	Character string

Field	Description	Values
Status	Indicates whether the user account is activated or blocked.	Character string
2FA required	Indicates whether two-factor authentication (2FA) is required to log in to the management console.	Character string
2FA enabled	Indicates whether the user has two-factor authentication (2FA) enabled.	Character string
Password changed	Indicates the day and time the management console login password was last changed.	Character string
Last access	Indicates the day and time the user last logged in to the management console.	Numeric value

Table 7.30: Fields in the Clients' Users exported file

Filter tool

Field	Description	Values
Search for client	Filters clients by name.	Character string
Search for group	Filters clients by group.	Character string
Search for user	Filters users based on the contents of the **User** or **Email** fields.	Character string
Email	Filters users by email address.	Character string
Status	The user account status.	• All • Activated • Blocked
2FA required	Filters users based on whether 2FA is required to log in to the management console.	• All • No • Yes

Field	Description	Values
2FA enabled	Filters users based on whether 2FA is enabled.	• All • No • Yes
Password changed	Filters users based on when the console login password was last changed.	• All • More than 1 month ago • More than 2 months ago • More than 3 months ago • More than 4 months ago • More than 5 months ago • More than 6 months ago • More than 1 year ago
Last access	Filters users based on when they last logged in to the management console.	• All • Less than 1 month ago • Less than 2 months ago • Less than 3 months ago • More than 1 month ago • More than 3 months ago • More than 6 months ago • More than 1

Field	Description	Values
		year ago

Table 7.31: Filters available in the Clients' Users list

Tasks

A task is a resource implemented in Partner Center that enables you to configure two additional aspects for the execution of a process: repetition interval and execution time.

- **Repetition interval**: You can configure tasks to be performed only once, or repeatedly through specified time intervals.
- **Execution time**: You can configure tasks to be run immediately after being set (immediate task), or at a later time (scheduled task).

CHAPTER CONTENTS

Introduction to the task system

Compatible security products

The Cytomic Nexus console user can centrally define and send tasks to their clients' security products that are compatible with the Cytomic platform:

- Advanced EDR (for patch installation tasks only)
- Advanced EPDR

Accessing the task system

- In the top menu, select **Clients**.
- Select **Configure clients' products**. A page opens in a new tab.
- In the top menu, select **Tasks**. A page opens that shows the list of all configured tasks.

Steps to launch a task

The process to launch a task consists of these steps:

- **Create and configure the task**: Select the clients that will be affected by the task, and configure the task, the date/time it will be launched, and its frequency. After the task has been created, it is sent to the clients you selected as recipients. When the task is received in the client's console, it appears with the label "Cytomic Nexus" and is assigned the **All** group so that it runs on all computers on the network. Tasks sent from Cytomic Nexus cannot be modified by the client, unless the relationship between Partner Center and the client's product is broken.
- **Publish the task**: When you publish a task in Cytomic Nexus, it is added to the process scheduler of the products purchased by the clients who receive it.
- **Run the task**: When the configured conditions are met, the scheduler runs the task on the client's computers.
- **Collect the results**: Cytomic Nexus collects and consolidates the results generated by the clients' computers where the task was run.

Task types

Cytomic Nexus enables you to run these types of tasks:

- File scanning and disinfection: See **Configuring scan tasks (4)**.
- Patch installation: Updates the operating system and the programs installed on clients' computers. See **Configuring Cytomic Patch tasks (4)**.

Permissions associated with task management

- Console users with read-only permissions cannot create, copy, delete, cancel, or publish tasks.
- All users can see the list of configured tasks, regardless of the permissions they have.
- To publish, delete, or cancel a task, the user must have permissions on all clients assigned to the task.
- To add or delete task recipients, the user must have permissions on them.

Creating tasks

Required permissions

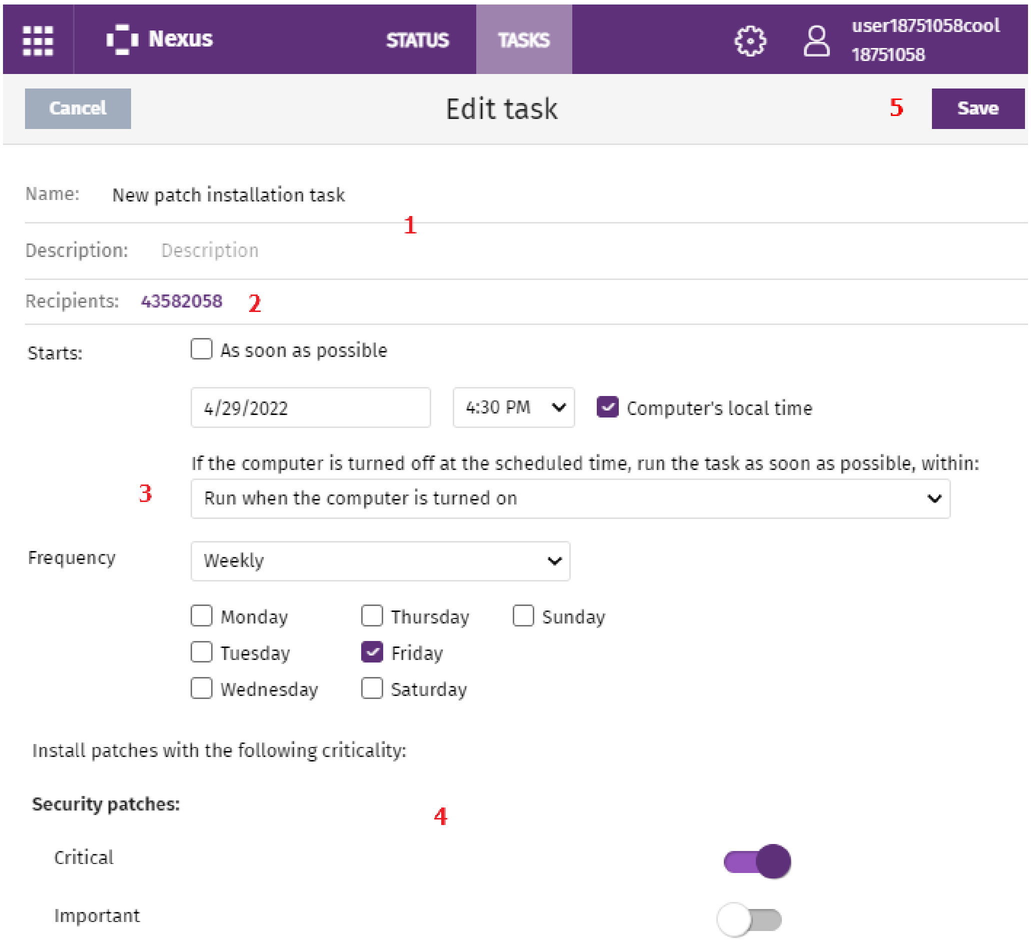
- You must have one of these permissions:
    - Total control
    - License and security administrator
    - Security administrator
- You must have permissions on the clients you want to assign to the task.

Creating a task

From the top menu, select **Tasks**. A page opens that shows a list of all created tasks and their status.

Click **Add task**. From the drop-down menu, select the task type. The **New task** page opens. This page shows the task settings, divided into different sections:

- **Overview (1)**: Task name and description.
- **Recipients (2)**: Computers that receive the task. See **Task recipients (2)**.
- **Schedule (3)**: Task schedule (when you want the task to run).
- **Settings (4)**: The actions the task must take. This section varies based on the task type and is described in the documentation associated with the relevant module.



Edit task

Name: New patch installation task

Description: Description

Recipients: 43582058

Starts: □ As soon as possible

4/29/2022 4:30 PM ☑ Computer's local time

If the computer is turned off at the scheduled time, run the task as soon as possible, within:

Run when the computer is turned on

Frequency Weekly

□ Monday □ Thursday □ Sunday
□ Tuesday ☑ Friday
□ Wednesday □ Saturday

Install patches with the following criticality:

Security patches:

Critical ●

Important ○

Figure 7.15: Creating a task

Task recipients (2)

Select the clients or client groups you want to receive the task.

- On the **New task** page, click the **Recipients: No recipients selected yet** link. The **Recipients** page opens.

> *To access the client selection page, you must first save the task. If you did not save the task, a warning message appears.*

- Click the ⊕ icon. The **Add clients** dialog box opens.
- Select the clients or client groups you want to receive the task. Click **Add**. The **Recipients** page shows the recipients you selected.
- By default, the task is assigned to all computers and devices belonging to the clients and client groups you select. To run the task only on a particular type of computer and device, in

Run the task only on computers of the following types, click the **Workstation** and **Laptop** links.

- In the **Device type** dialog box, select the types of devices on the client's network you want to receive the task. Not all types of devices can receive all types of tasks:
  - **Scan tasks**: Workstation, server, laptop, mobile device.
  - **Patch installation tasks**: Workstation, server, laptop.
- To assign patch installation tasks to test computers only, in **Run the task only on test computers**, select **Yes**. Otherwise, the task is sent to all computers, including test computers.

> *You designate a computer as a test computer in the settings profile assigned to the computer in the client's console. For more information, see chapter* ***Cytomic Patch (Updating vulnerable programs)****, section Cytomic Patch* ***features*** *in the product administration guide.*

- To add clients or client groups, click the ⊕ button. To remove them, click 🗑.
- On the **Tasks** page, click the **View computers** button to review the computers that will receive the task.

Configuring tasks

Task schedule and frequency (3)

You can configure the following three parameters:

- **Starts**: Select when the task will start.

Value	Description
As soon as possible (selected)	The task is launched immediately provided the computer is available (turnedon and accessible from the cloud), or as soon as it becomes available withinthe time interval specified **if the computer is turned off.**
As soon as possible (cleared)	The task is launched on the date selected in the calendar. To specify the time based on the time on the target computer or device, select the **Computer's local time** checkbox. If you do not select this checkbox, the time is based on the Cytomic Nexus server time.
If the computer is	If the computer is turned off or cannot be accessed, the task will not run. The task scheduler enables you to establish the task expiration time, from 0 (the

Value	Description
turned off	task expires immediately if the computer is not available) to infinite (the task is always active and waits indefinitely for the computer to be available): • **Do not run**: The task is canceled immediately if the computer is turned off or is not available at the scheduled time. • **Run the task as soon as possible, within XX**: Define a time interval during which the task will be run if the computer becomes available. • **Run when the computer is turned on**: There is no time limit. The system waits indefinitely for the computer to be available to launch the task. If the value you select is lower than the run frequency, a warning message appears in red text.

Table 7.32: Task launch parameters

- **Maximum run time** (available only **for Scheduled scan** tasks): Select the maximum time that the task can take to complete. After that time, the task is canceled returning an error.

Value	Description
No limit	There is no time limit for the task to complete.
1, 2, 8, or 24 hours	There is a time limit for the task to complete. After that time, if the task has not finished, it is canceled returning an error.

Table 7.33: Task duration parameters

- **Frequency**: Select how often you want the scan to run (One time, Daily, Weekly, Monthly) from the date specified in the **Starts**: field.

Value	Description
One time	The task is run only once at the time specified in the **Starts**: field.
Daily	The task is run every day at the time specified in the Starts: field.
Weekly	Specify the day or days of the week to run the task each week, at the time specified in the **Starts**: field.
Monthly	Choose an option:

Value	Description
	• Run the task on a specific day of each month. If you select the 29th, 30th, or 31st of the month, and the month does not have that day, the task is run on the last day of the month. • Run the task on the first, second, third, fourth, or last Monday to Sunday of each month.

Table 7.34: Configuring the frequency of a task

Configuring scan tasks (4)

The scan options enable you to configure the scan engine parameters in order to scan the computers' file system:

Value	Description
Scan type	• T**he entire computer**: Runs an in-depth scan of the computer that includes all connected storage devices. This scan type might take several hours to complete. • **Critical areas**: Runs a quick scan of the computer. It takes minutes. It scans the following: • %WinDir%\system32 • %WinDir%\SysWow64 • Memory • Boot system • Cookies • <![CDATA[ ]]>**Specific items**: Runs a scan of a selected storage device. This option supports environment variables. The solution scans the specified path and every folder and file it contains.
Detect viruses	Detects programs that enter computers with malicious purposes. This toggle is always enabled.
Detect hacking tools and PUPs	Detects potentially unwanted programs, as well as programs that hackers can use to carry out actions that cause problems for the user of the affected computer.
Detect	Scheduled scans can scan computer software statically without the need

Value	Description
suspicious files	to run the software. This reduces the likelihood that the scan detects some types of threats. Enable this toggle to use heuristic scan algorithms and improve detection rates. The security software classifies as suspicious only programs detected by the heuristic protection.
Scan compressed files	Decompresses compressed files and scans their contents.
Exclude the following files from scans	• **Do not scan files excluded from the permanent protections**: Select this checkbox to not scan files that the administrator allowed to execute, as well as any file that is globally excluded in the console. • **Extensions**: Enter multiple file extensions separated by commas. • **Files**: Enter multiple file names separated by commas. • **Folders**: Enter multiple folders separated by commas.

Table 7.35: Scan options

Configuring Cytomic Patch tasks (4)

The patch installation options enable you to configure Cytomic Patch module parameters to update the components installed on clients' computers.

> *For more information about how to edit the Cytomic Patch settings profile assigned to clients' computers to allow or deny patch installations, see chapter* ***Cytomic Patch (Updating vulnerable programs)****, section* ***Configuring the discovery of missing patches*** *of the product Administration Guide.*

Value	Description
Security patches	Select the criticality or importance of the patches to install. • Critical • Important • Moderate • Low

Value	Description
	- Unspecified - Other patches (non-security-related) - Service Pack
Install patches for the following products	Use the checkboxes to specify which operating system and products to install patches for. Because the product tree is a dynamic resource that changes over time, keep these considerations in mind when you select items from the tree: - When you select a node, you also select all of its child nodes and all items they contain. For example, if you select Adobe, you also select all nodes below it. - If you select a node, and Cytomic Patch automatically adds a child node to that branch, that node is selected as well. For example, as previously explained, when you select Adobe you also select all of its child nodes. If, later, Cytomic Patch adds a new node (a program or program family) to the Adobe group, that node is selected as well. Conversely, if you manually select a number of child nodes from the Adobe group, and later Cytomic Patch adds a new child node to the group, this is not automatically selected. - The programs to patch are evaluated at the time when the task is run, not at the time when the task is created or configured. For example, if Cytomic Patch adds an entry to the tree after you have created a patch task, and that entry is selected automatically in accordance with the aforementioned mechanism, the task installs the patches associated with that new program when run.
Install patches for the following products	Configure the restart option in case the target workstations or servers require a restart to finish installing the patch. - **Do not restart automatically**: A restart dialog box appears on the target computer. The available options are: **Restart now** and **Remind me later**. If the latter is selected, a reminder appears 24 hours later. - **Automatically restart workstations only**: A restart dialog box appears on the target computer. The available options are **Restart now, Minimize**, and there is **4-hour countdown timer**. This dialog box is maximized every 30 minutes as a reminder to the user. Less than one hour before the restart, the minimize button is disabled. When the countdown finishes, the computer restarts automatically.

Value	Description
	• **Automatically restart servers only**: This option behaves in the same way as **Automatically restart workstations only**, but applies to servers only. • **Automatically restart both workstations and servers**: This option behaves in the same way as **Automatically restart workstations only**, but applies to both workstations and servers.

Table 7.36: Patch installations options

Saving tasks (5)

When you save the task, Cytomic Nexus takes the following actions:

- The task is added to the Cytomic Nexus task list with status **Unpublished**.
- The task is sent to all clients selected as recipients of the task.
- In each of the clients' consoles, the task is added to the **All** group so that it is run on all computers on the network.
- In the client's console, the task is marked with the Cytomic Nexus label. This label indicates that the task is read only.

Creating a Cytomic Patch quick task

Cytomic Nexus enables you to create installation tasks for individual patches for the Cytomic Patch module without having to follow all the steps in **Creating tasks**. With this type of task, you only need to select the patches that you want to install in the **Available patches** list. Cytomic Nexus deploys the tasks to the consoles of the selected clients for immediate execution.

> ⚠ *Quick patch installation tasks create a single task in Cytomic Nexus with all the clients and patches you select in the* ***Available patches*** *list. If, for example, you select two different patches and each patch is associated with a different client. Cytomic Nexus creates a single task that installs the two patches on the two clients. To make sure that each patch installs only on the devices of the clients you want, create as many quick tasks for a single patch as you need.*

To create a quick patch installation task:

- From the top menu, select **Status**.
- From the side menu, select the **Available patches** list.

- Select the checkboxes for the patches you want to install. The list shows the patches available for each client. For more information about this list, see **Available patches** on page **119**.
- From the action bar, click **Schedule installation**. The task page opens and Cytomic Nexus sends the task automatically to the consoles of the assigned clients. The task status is **Unpublished**. See **Status**.
- Edit the settings based on your needs. By default, Cytomic Nexus creates a single task with the settings:
    - **Recipients** contains all clients associated with all the patches you selected in the **Available patches** list. The task installs all the patches you selected in the **Available patches** list on all the clients associated with the task.
    - The **Frequency** is **One time**. If a client's computer is turned off, the task does not expire. It runs when the computer is back on again.

> *Cytomic Nexus automatically sends the task to the console of clients with computers that have the selected patch available for installation. If no computers in a client have the selected patch, Cytomic Nexus does not create a task to install that patch in the client's console.*

- Click **Save**. Cytomic Nexus sends the task configuration changes to the affected clients' consoles.
- To delete the task, click **Cancel**. Because Cytomic Nexus has already sent the task to clients (with the status **Unpublished**) but the task is no longer required, the task is deleted from their consoles.

Old versions of the security software

If the recipient computers have an old version of the security software installed, they might not correctly interpret the frequency settings defined from Cytomic Nexus. Computers with old versions of the security software interpret the taskfrequency settings as follows:

- **Daily tasks**: Unchanged.
- **Weekly tasks**: Recipient computers ignore the days selected in the task by the administrator. The first run occurs on the specified start date and then runs again every 7 days.
- **Monthly tasks**: Recipient computers ignore the days selected in the task by the administrator. The first run occurs on the specified start date and then runs again every 30 days.

Task list

Required permissions

All Cytomic Nexus users can see the task list, regardless of the permissions and visibility assigned to their accounts.

Accessing the task list

From the top menu, select **Tasks**. A page opens that shows a list of all created tasks, along with their type, status, and other relevant information.

Field	Comment	Values
Icon	Task type.	• Patch installation task • 🔍 Scan task
Name	Task name.	Character string
Schedule	Date the task is set to run.	Character string
Status	• **No recipients**: The task cannot run because there are no recipients assigned to it. Assign one or more clients to the task. • **Unpublished**: The task cannot run because it has not been added to the clients' scheduler queue. Publish the task to send it to clients and add it to the process scheduler for execution. • **In progress**: The task is running or has finished on some or all of the clients' computers. • **Canceled**: The task was manually canceled. This does not mean that all processes that were running on the target computers have stopped.	Character string

Table 7.37: Fields in the Tasks list

Filter tool

Field	Comment	Values
Type	The task type.	• Scan • Patch installation • All
Search for task	Task name.	Character string
Schedule	Task repeat frequency.	• All • Immediate • Once • Scheduled
Sort list	Task list sort order.	• Sort by creation date • Sort by name • Ascending • Descending

Table 7.38: Filters available in the Tasks list

Task management

Required permissions

- The console user must have one of these permissions:
  - Total control
  - License and security administrator
  - Security administrator
- Permissions on all clients assigned to the task to be able to modify the available parameters.
- Permissions on the recipients the user wants to add or remove from the task.

Access to task management

From the top menu, select **Tasks**. A page opens where you can publish, delete, copy, cancel, or view the results of tasks.

Publishing a task

After you create and configure a task, and add recipients to it, it appears in the list of configured tasks. The status shows as **Unpublished** and the task is not yet active. To publish a task, click the **Publish** button. Partner Center adds the task to the scheduler queue in the client's product, which runs it based on its settings.

A task must have recipients assigned to be published. You cannot publish a task if it has client groups assigned but they are empty.

Editing a task

To edit a task, click the task name. Based on the status of the task and your permissions, you can edit the task overview, recipients, schedule, or settings. To see the elements that make up a task, see Creating tasks.

- **Unpublished tasks**:

To modify any of the task parameters (overview, recipients, schedule, or settings), you must have permissions on all of the task recipients.

- **Published tasks without a recurring schedule**:
  - You cannot edit any task parameters (overview, recipients, schedule, or settings).
  - To edit the task parameters, create a copy of the task and make changes to the copy.
- **Published tasks with a recurring schedule**:
  - You can edit the task name and description if you have permissions on all of the task recipients.
  - You can add or delete recipients if you have permissions on them.
  - You cannot edit the task schedule or settings.
- **Canceled or failed tasks**: You cannot edit any task parameters (overview, recipients, schedule, or settings).

Canceling a published task

You can cancel a task if the status is **In progress**. Additionally, you can cancel a task only if you have permissions on all clients assigned to the task.

- Select the checkbox for each task you want to cancel. In the toolbar, click the **Cancel** icon. A confirmation dialog box opens.
- Click **OK**. This cancels the task, but does not delete the task from the Tasks page. You can still see the task results.

Deleting a task

When a task is published and executed, it is not automatically deleted from the Tasks page.

To delete a task:

- Verify you have permissions on all the clients that have the task assigned. Otherwise, the **Delete** 🗑 icon is disabled.
- Verify the task status is one of these:
    - **In progress**: You must cancel the task before you can delete it.
    - **Unpublished**.
    - **Canceled**.
- Select the checkbox for each task you want to delete. A toolbar appears at the top of the page.
- Click the 🗑 icon. A confirmation dialog box opens that informs you that the tasks will be deleted for all clients' accounts that have them assigned.
- If you confirm the action, the tasks are deleted from the clients' consoles.
- The tasks are deleted from Cytomic Nexus along with all of the results collected from client accounts.

Copying a task

From the top menu, select **Tasks**. Click the icon for the task you want to copy. A menu opens. Select a copy type.

> *You can copy any task regardless of its status. For more information about the statuses of tasks, see **Task list**.*

Figure 7.16: Copy task icon menu

- If you select **Copy with recipients**, the **Copy task** page opens with the recipients configured in the original task.

  > *The recipients shown are the clients and client groups you have visibility of.*

- If you select **Copy without recipients**, the **Copy task** page opens.
  - To assign recipients, click the **No recipients selected** link. The **Recipients** page opens.
  - Select the task recipients. Click **Save** in the upper-right corner of the page.

Task results

To view the current results of any published, finished, or canceled task, on the **Tasks** page, click **View results**.

Field	Description	Value
Client	Name of the client associated with the task execution result. Click it to access the dashboard that corresponds to the task type in the client's console.	Character string
Group	Folder in the Cytomic Nexus folder tree that the computer belongs to.	Character string
Installed patches	This field appears only in patch installation tasks. Number of patches installed on the client's computers the last time the task ran. Click it to access the task details in the client's console. See the administration guide for the product installed on the client's network.	Character string
Detections	This field appears only in scan tasks. Number of detections made on the client's computers the last time the task ran. Click it to access the task details in the client's console. See the administration guide for the product installed on the client's network.	Character string

Table 7.39: Fields in the task results list

*For more information about the results of patch installations on clients' computers, see **Patch installation results** on page **114**.*

Automatic adjustment of task recipients

If the Cytomic Nexus console user selects a client group as the recipient of a task, the clients that finally run the task may vary from those initially selected. This is because groups are dynamic entities that the Cytomic Nexus user can change.

For example: A task defined at a specific time (T1) and assigned to a group has the clients in the group as recipients. However, at the time the task is run (T2), the clients in the group may have changed. These are the ways Cytomic Nexus and the product installed on the client's network behave when the members of a group set to run a task change.

Unpublished tasks

When a client enters or leaves a group assigned to the task, Cytomic Nexus updates the list of recipients. When you publish the task, it is sent to the clients that are currently part of the group.

Published tasks

Clients added to a group assigned to a one-time scheduled task

The task is not created for the new clients.

Clients added to a group assigned to a recurring scheduled task

The changes made to the group members are applied the next time the task is run. The clients that were added to the group receive the task in their product consoles.

Clients added to a group assigned to a canceled task

The task is not created for the new clients because it is canceled and will not run again.

Clients added to a group assigned to an unpublished task

The task is created for the new clients so that it runs when scheduled.

Clients removed from a group assigned to an in-progress task

The task created in the client's console continues to run, but its relationship with Cytomic Nexus breaks: the task is no longer read only and the "Cytomic Nexus" label is removed.

Cytomic Nexus deletes the results generated by the clients that left the group from the task.

Clients removed from a group assigned to an unpublished or canceled task

The task and its results (if any) are deleted from the client's console.

Cytomic Nexus deletes the results generated by the clients that left the group from the task.

Task synchronization and relationship between Cytomic Nexus and clients

As long as there is a relationship between Cytomic Nexus and the clients it manages, task creation, status changes, and task results are synchronized between the Partner Center console and clients' consoles. If that relationship changes, there will be a number of changes in both the Cytomic Nexus console and clients' consoles.

Interruption of the relationship between Partner Center and the client

For Cytomic Nexus to send tasks to clients and synchronize the status of created tasks:

- There must be a contractual relationship with the client.
- The client's product must be configured as managed. See **Service management models for Cytomic-based products**.
- The client must have the Allow my reseller to access my console option enabled in their product console. See **Requirements for assigning centralized settings** on page **72**.

If any of the above conditions are not met, the tasks configured in Cytomic Nexus are not sent or synchronized.

The way Cytomic Nexus behaves with respect to synchronization of tasks already sent to clients is as follows:

- Unpublished, finished, or canceled tasks are automatically deleted from clients' consoles. The results generated by the clients are deleted from the task in Cytomic Nexus.
- In-progress tasks are kept in clients' consoles. However, the Cytomic Nexus label is removed and the tasks can be edited or canceled from the client's console. The results generated by the clients are deleted from the tasks in Cytomic Nexus.

Resumption of the relationship between Partner Center and the client

When a client resumes the relationship with Partner Center after it was interrupted, the following actions are taken:

- The client receives all previously assigned tasks. Previous results are restored in Cytomic Nexus.
- Tasks sent by Cytomic Nexus before the relationship was interrupted and which were not modified or deleted by the client become read-only and show the Cytomic Nexus label.
- Tasks sent by Cytomic Nexus before the relationship was interrupted and whose recipients were modified by the client maintain those recipients and add the **All** group.
- Tasks sent by Cytomic Nexus before the relationship was interrupted and whose settings were modified by the client are resent, thus creating new tasks.

The Cytomic account

The Cytomic account provides administrators with a safer mechanism to self- manage login credentials and access the Cytomic services purchased by their organization than the standard method of receiving credentials by email.

With a Cytomic account, it is the administrator who creates and activates the access method to Cytomic Nexus's web console.

CHAPTER CONTENTS

Creating a Cytomic account

Follow the procedure described below to create a Cytomic account.

Receiving the email

- When purchasing Cytomic Nexus, you will receive an email from Cytomic.
- Click the link in the message to access a site from which you will be able to create your Cytomic account.

Filling out the form

- Enter your information in the form shown.
- Use the drop-down menu located in the bottom-right corner if you wish to display the page in a different language.
- Access the License Agreement and Privacy Policy by clicking the relevant links.
- Click **Create** to finish and receive an email sent to the address indicated in the form. Use that message to activate your account.

Activating the Cytomic account

Once created, it is necessary to activate your Cytomic account. To do this, you must use the message received at the email address you specified when creating your Cytomic account.

- Find the message in your inbox.
- Click the activation button. By doing this, the address provided when creating your Cytomic account will be confirmed as valid. If the button doesn't work, copy and paste the URL included in the message into your browser.

- The first time you access your Cytomic account, you will be asked to confirm your password. Set it and click the **Activate account** button.
- Enter the necessary information and click **Save data**. If you prefer to provide your data at another time, use the **Not now** option.
- Accept the License Agreement and click **OK**.

Once the activation process is successfully finished, you will be redirected to the Cytomic Central account home page. From there, you will be able to access Cytomic Nexus‘s Web console. To do this, click the solution's icon you will find in the '**My Services** section.

Modifying Cytomic account

If your associated security provider is WatchGuard, go to **https://watchguard.com/**

Click the **Edit account** option.

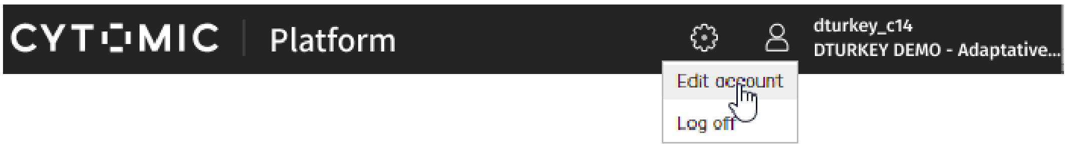


Figure 7.17: Editing the user account

Glossary

A

Antivirus

Protection software that relies on traditional technologies (signature files, heuristic scanning, anti-exploit techniques, etc.) to detect and remove computer viruses and other threats.

APT (Advanced Persistent Threat)

A set of strategies implemented by hackers and aimed at infecting clients' networks through multiple infection vectors simultaneously. Advanced Persistent Threats are designed to go undetected by traditional antivirus programs for long periods of time. Their main aim is financial (through theft of confidential information or intellectual property for blackmail, etc.).

Automatic renewal of licenses

An automatic process implemented by Cytomic Nexus to renew the licenses of the products and modules assigned to clients when they are close to expiring. This helps simplify management tasks as they don't need to monitor on a daily basis which clients have products with licenses close to expiring in order to start a manual/early renewal process.

Automatic/indirect assignment of settings

See Inheritance.

B

Backup

Storage area for non-disinfectable malicious files, as well as spyware specimens and hacking tools detected. All programs classified as threats and removed from the system are temporarily moved to the backup/quarantine area for a period of 7/30 days based on their type.

C

Client

Company contracting security products and services from a Cytomic partner.

Co-branding

A feature aimed at remotely configuring the look and feel of the Web management console used by clients to manage the products provided by the Cytomic partner.

Cytomic

Self-management mechanism provided by that allows Web console users to generate their login credentials for the services purchased by the organization, in contrast to the standard method of receiving credentials by email.

D

Distributor

Partners who buy large volumes of licenses. They then sell those licenses among their partners, who in turn sell them to end clients.

Distributors keep a stock of licenses to quickly respond to the everyday license needs of their partners.

E

Early/manual renewal of licenses

A type of license renewal process in which the partner monitors clients' licenses manually and gets notified whenever there are licenses due to expire. The partner can then renew the affected clients' licenses early so they aren't left unprotected.

EDR (Endpoint Detection & Response)

The term 'EDR' refers to a type of security software developed to fill the gaps of traditional antivirus solutions, which are incapable of stopping all cyber-attacks. EDR solutions work under the assumption that a number of threats will be able to bypass prevention mechanisms, and focus on monitoring computers with the aim of detecting behaviors that may indicate malicious activity and collecting data for security investigations. Most EDR solutions provide a certain level of automated response to threats. Nevertheless, depending on the dwell time of threats, manual remediation initiatives may be required.

End of Life (EOL)

A term used to indicate that the product is in the end of its useful life. Once a product reaches its EOL, it stops receiving updates or fixes from the vendor, leaving it vulnerable to hacking attacks.

Exploit

Generally speaking, an exploit is a sequence of specially crafted data aimed at causing a controlled error in the execution of a vulnerable program. Once the error occurs, the compromised process will mistakenly interpret certain parts of the data sequence as executable code, triggering dangerous actions that may compromise the security of the targeted computer.

F

Filters

A set of values and criteria used to exclude, from a list, those entries that bear no interest for the user of the management console.

G

Group

Static container that groups together one or more clients. Clients are assigned to groups manually. Groups simplify the assignment of security settings and facilitate management of clients.

Group tree

Hierarchical structure made up of static groups. Its purpose is to help organize clients, assign settings and set permissions for technicians.

I

ISP

Partners who integrate their back-office into Cytomic's back-office in order to register clients and their licenses automatically. Both clients and their licenses will be visible in the Cytomic Nexus Web console.

L

License

Mechanism for controlling use and access to the products developed by Cytomic. Licenses enable the use of the product for which they were issued for a period of time ranging from 1 to 3 years based on the license type.

License contract

This is the assignment, to a client, of a specific number of licenses of a product or module with a specific duration.

M

Malware

Generic term used to refer to programs containing malicious software (MALicious softWARE), whether it be a virus, a Trojan, a worm or any other threat to the security of IT systems. Malware tries to infiltrate and damage computers, often without users' knowledge, for a variety of reasons.

Managed model

Management model in which the client delegates product management to the partner. This model frees clients from the need to manage the service themselves. The service is maintained by the partner, thus increasing the added value provided to clients.

Managed Service Providers (MSP)

Partners who sell products to their clients and manage their security proactively.

Manual assignment of licenses

Procedure used to assign a specific number of licenses to clients' computers so they can activate the purchased product. If a client integrates into their infrastructure a number of computers greater than the number of licenses assigned by the Web console user, the excess computers will be left unprotected.

Module

A product extension that adds additional features to it. The available modules vary based on the platform and the product.

MyTerm

N

Notifications

Alert system implemented in Cytomic Nexus to inform Web console users, via the Web console and email, of situations that may require their intervention.

O

On-premises software

A type of software in which the computing resources are located within the client's own facilities. It usually requires additional resources (servers, licenses, etc.), and associated maintenance. That's why on-premises solutions have a higher TCO and provide less flexibility for uses to access their features from remote locations.

P

Permission

Specific access settings applied to one or more user accounts, and which authorize users to view and edit certain resources of the console.

Phishing

A technique for obtaining confidential information from a user fraudulently. The targeted information includes passwords, credit card numbers and bank account details.

PII (Personally Identifiable Information)

Information that can be used to identify or locate an individual.

Platform

Environment where products from the Endpoint family are hosted in the cloud.Cytomic has two separate platforms: Cytomic and Traditional. There are significant differences between the two platforms in terms of features and product management for both partners and clients.

Primary user

This is the first user created after purchasing the Cytomic Nexus service. This user has access to all resources and all clients.

Private-label product

This is a special version of a security product developed by Cytomic, stripped off any reference to the original manufacturer (logos, brand, etc.). Those items are replaced with the logo and brand of a third party, usually the partner that sells the software and provides maintenance.

Product

A security solution belonging to Cytomic's portfolio and compatible with Cytomic Nexus, and therefore can be managed by partners or large companies client.

Product family

A group of products with similar features. Two or more products of the same family cannot be simultaneously installed on the same computer.

Q

Quarantine

See Backup.

R

Ransomware

A type of malware that prevents access to users' data or devices, and demands a ransom payment in exchange for restoring access to the files or compromised system.

Real-time communication

Clients' computers protected with Cytomic-based products allow for real-time communication with Cytomic's servers. This results in immediate deployment of the settings configured by the Cytomic Nexus Web console user or the client's network administrator.

Renewal

A process consisting of extending the duration of the product licenses assigned to a client by 1, 2 or 3 years.

Resellers

Partners who purchase Cytomic product licenses and sell them to their clients without adding value.

RMM (Remote Monitoring and Management)

A type of software designed to help managed service providers (MSPs) monitor the performance of clients' computers and networks, and take corrective actions to resolve problems

Rollback

The process of uninstalling those patches installed by Cytomic Patch that cause malfunctions or compatibility issues.

RWD (Responsive Web Design)

An approach to Web design that makes Web pages render well on a variety of devices and window or screen sizes.

S

Service

A set of one or more license contracts associated with a single product.

Settings profile

Specific settings governing the protection or any other aspect of the managed software. Once configured, profiles are assigned to one or multiple client groups and applied to all the computers in the group(s).

Signature file

File that contains the patterns used by the antivirus to detect threats.

Standalone software

Software that requires the computer to be accessed locally for configuration purposes.

T

TCO (Total Cost of Ownership)

An estimate of all direct and indirect costs associated with a purchase, capital investment or acquisition of a product or system.

TPM (Trusted Platform Module)

The TPM is a chip that's part of the motherboard of desktops, laptops and servers. It aims to protect users' sensitive information by storing passwords and other information used in authentication processes. Additionally, the TPM is responsible for detecting changes to a computer's boot chain, preventing, for example, access to a hard disk from a computer other than the one used to encrypt it.

Trial licenses

They provide clients with the full functionality of a product but only for a limited time, after which access to the product is automatically disabled.

U

Unmanaged model

Management model in which clients themselves manage the product they have purchased. If this model is selected, Cytomic Nexus will prevent the Web console user from accessing the product management console so as not to interfere with the client's activity.

User account

See Web console user.

V

VDI

Desktop virtualization technology that hosts virtual machines in a data center accessed by users from a remote terminal with the aim to centralize and simplify management and reduce maintenance costs.

Visibility

This concept is used to limit the Web console user's access to particular user groups.

VPN (Virtual Private Network)

A network technology that is used to interconnect private networks (LANs) across a public network, such as the Internet.

W

Web console user

Data set used by Cytomic Nexus to regulate technicians' access to the Web console and establish the actions they can take on the computers on the network.