Partner Center

Partner Center Administration

Author: Panda Security

Version: 2.90

Date: 31/10/2024

panda

pandasecurity.com

Legal notice

Registered trademarks

Contact information

Corporate Headquarters:

Panda Security

Santiago de Compostela 12

48003 Bilbao (Bizkaia) SPAIN.

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

Author : Panda Security

Version: 2.90

Date: 10/31/2024

About the Partner Center Administration Guide

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

http://documents.managedprotection.pandasecurity.com/AdvancedGuide/PARTNERCENTER-Manual-EN.pdf

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

http://documents.managedprotection.pandasecurity.com/Help/v77000//Partners/en-us/index.htm

Release notes

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

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

Products supported by Partner Center

Panda Adaptive Defense

Administration Guide:

http://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/latest/ADAPTIVEDEFENSEoAP-guide-EN.pdf

Product online help:

https://www.pandasecurity.com/enterprise/downloads/docs/product/help/adaptivedefense/latest/en/index.htm

Product support articles:

https://www.pandasecurity.com/en/support/adaptive-defense-aether.htm

Panda Adaptive Defense 360

Administration Guide

http://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/latest/ADAPTIVEDEFENSE360oAP-guide-EN.pdf

Product online help:

https://www.pandasecurity.com/enterprise/downloads/docs/product/help/adaptivedefense360/latest/en/index.htm

Product support articles:

https://www.pandasecurity.com/en/support/adaptive-defense-360-aether.htm

Panda Endpoint Protection

Administration Guide:

http://www.pandasecurity.com/rfiles/enterprise/solutions/endpointprotection/latest/ENDPOINTPROTECTIONoAP-guide-EN.pdf

Product online help:

https://www.pandasecurity.com/enterprise/downloads/docs/product/help/endpointprotection/latest/en/index.htm

Product support articles:

https://www.pandasecurity.com/en/support/endpoint-protection-aether.htm

Panda Endpoint Protection Plus

Administration Guide:

http://www.pandasecurity.com/rfiles/enterprise/solutions/endpointprotection/latest/ENDPOINTPROTECTIONPLUSoAP-guide-EN.pdf

Product online help:

https://www.pandasecurity.com/enterprise/downloads/docs/product/help/endpointprotection/latest/en/index.htm

Product support articles:

https://www.pandasecurity.com/en/support/endpoint-protection-plus-aether

Panda Systems Management

Administration Guide:

https://www.pandasecurity.com/rfiles/enterprise/documentation/pcsm/docswebpage/SYSTEMSMANAGEMENT-Guide-EN.pdf

Release notes:

https://www.pandasecurity.com/en/support/card?id=300121

Product support articles:

https://www.pandasecurity.com/en/support/cloud-systems-management.htm

Panda Fusion 360

Panda Systems Management Administration Guide:

https://www.pandasecurity.com/rfiles/enterprise/documentation/pcsm/docswebpage/SYSTEMSMANAGEMENT-Guide-EN.pdf

Panda Adaptive Defense 360 Administration Guide:

https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/ADAPTIVEDEFENSE360-manual-EN.pdf

Product support articles:

https://www.pandasecurity.com/en/support/#panda_fusion_360

Panda Fusion

Panda Systems Management Administration Guide:

https://www.pandasecurity.com/rfiles/enterprise/documentation/pcsm/docswebpage/SYSTEMSMANAGEMENT-Guide-EN.pdf

Panda Endpoint Protection Plus Administration Guide

https://www.pandasecurity.com/rfiles/enterprise/solutions/endpoint2015/ENDPOINTPROTECTION-AdvancedGuide-EN.pdf

Panda Email Protection

Administrator's Manual

https://www.pandasecurity.com/rfiles/enterprise/documentation/pcep/EMAILPROTECTION-AdministratorManual-4.3.2-2-EN.pdf

Domain Administrator's Manual

https://www.pandasecurity.com/rfiles/enterprise/documentation/pcep/EMAILPROTECTION-DomainAdministratorManual-4.3.2-2-EN.pdf

Quick Configuration Guide:

https://www.pandasecurity.com/rfiles/enterprise/documentation/pcep/EMAILPROTECTION-TechDoc-ConfigGuide-EN.pdf

User's Manual:

https://www.pandasecurity.com/rfiles/enterprise/documentation/pcep/EMAILPROTECTION-UserManual-4.3.2-2-EN.pdf

Product support articles:

https://www.pandasecurity.com/en/support/cloud-email-protection/

Technical information about modules and services compatible with Partner Center

Advanced Reporting Tool

https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/ADVANCEDREPORTINGTOOL-AETHER-Guide-EN.pdf

Panda Data Control

http://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/DATACONTROL-AETHER-Guide-EN.pdf

Panda Patch Management

You can find more information in the **Panda Patch Management settings** chapter of the Panda Adaptive Defense, Panda Adaptive Defense 360, Panda Endpoint Protection, and Panda Endpoint Protection Plus online help files.

Product support articles:

https://www.pandasecurity.com/uk/support/patch-management.htm

Panda Full Encryption

You can find more information in the **Panda Full Encryption settings** chapter of the Panda Adaptive Defense , Panda Adaptive Defense 360 , and Panda Endpoint Protection Panda Endpoint Protection Plus online help files.

Product support articles:

https://www.pandasecurity.com/uk/support/full-encryption.htm

Panda SIEMFeeder

Infrastructure Guide:

http://resources.pandasecurity.com/enterprise/solutions/adaptivedefense/SIEMFeeder- Manual-EN.PDF

Event Description Guide:

https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/SIEMFeederAD-EventDescriptionGuide-EN.pdf

Product support articles:

https://www.pandasecurity.com/en/support/siemfeeder.htm

Table of contents

Chapter 1

Preface

The Administration Guide contains basic information and procedures to help you get the most out of Panda Partner Center.

CHAPTER CONTENTS

Audience

This guide is primarily aimed at partners (distributors) with a contractual relationship with Panda, in order to aid remote provisioning and management of security solutions for their clients.

What is Partner Center?

Partner Center is a cloud-based solution that offers partners simple and centralized management of the lifecycle of clients, from assigning trial versions and renewing contracted services 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

Partner Center basic information

Partner Center is a service for partners and service providers who wish to manage their clients' security products centrally and with maximum vendor autonomy. Partner Center provides a single, Web-based console available anytime, anywhere, which partners can use to centralize operations, simplify client lifecycle management, and streamline processes while saving time.

CHAPTER CONTENTS

Partner Center benefits

Partner Center is a service that Panda Security makes available to its partners 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.
- Increases efficiency of operations.
- Aids the sale and adoption of Panda Security security products.
- Improves recognition and satisfaction of clients.

Simplifies monitoring of clients

- 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 with a system of roles and groups. Sets different access permissions for the Web console user and levels of visibility of clients.
- Sends alerts proactively whenever systems are unprotected, displaying key status information in real time about clients: products and assigned modules, licenses used or about to expire, renewals pending, etc.
- Helps decision making and the implementation of new security strategies by providing lists with information about client activity.

Increased operation efficiency

- Offers volume licensing discounts. Partners are assigned a pool of licenses they purchase in advance at a lower cost and which they later sell to clients according to their needs.
- 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 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.

Aids the sale and adoption of Panda Security security products

- **Greater turnover of sales assets**: enabling assignment of trial licenses of Panda Security 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 Panda Security product licenses.
- **Greater flexibility**: it is possible to work with different license durations and cross-sell Panda Security solutions.
- **Greater profitability**: it is possible to recover unused licenses from clients canceling their service subscription and assign them to other clients, maintaining the value of purchased assets.

Increases client satisfaction and loyalty

The benefits obtained from using Partner Center are felt by clients:

- Greater peace of mind for clients, who feel protected and properly managed at all times.
- More satisfied clients, 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.

Partner Center features

License management

All licenses purchased by a partner are incorporated into a stock or pool of licenses, from which they can be directly assigned to clients. There is a history available to view all license movements. In addition to renewing and canceling licenses, it is also possible to change and group licenses, as well as recovering those not used by clients in order to assign them to other clients. They can also assign trial licenses to clients.

MSSP Command integration

Partner Center integrates with WatchGuard's MSSP Points system. Partners can manage, from their MSSP Command console, the conversion of their MSSP Points to monthly licenses of Panda Security products which they will be able to assign to their clients from the Partner Center console.

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.

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

Partner Center 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.

License assignment, renewal and recovery

Delete clients and their services, and proportionally recover the unused commercial licenses assigned to clients, and assign them to other clients.

With the aid of email notifications, the Web console user will be able to know which clients have licenses that expire in the coming days and deal with the situation.

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 clients you manage. Streamline deployment of security policies by centrally pushing settings to groups of clients with the same needs.

Centralized sending of scan and Panda Patch Management tasks

Create scan tasks and install operating system and third-party software updates on all computers in the branch offices managed by the main office. Get a consolidated view of task results.

Access to each client's Web console

Access all the Web management consoles of the security products installed on each client's network 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 . 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.

Detailed lists

See the security status of your clients' networks and the detections made by the protection modules included in the service.

Customization of clients' consoles (Co-branding)

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

Supported products

Panda Adaptive Defense 360

https://www.pandasecurity.com/en/business/adaptive-defense/

Panda Adaptive Defense 360 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, Panda Adaptive Defense 360 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 Aether platform), Linux, iOS and Android devices, as well as with persistent and non-persistent VDI environments (on the Aether platform).

Panda Adaptive Defense 360 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.

Panda Adaptive Defense

https://www.pandasecurity.com/en/business/adaptive-defense/

Panda Adaptive Defense 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, Panda Adaptive Defense 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, Panda Adaptive Defense doesn't require new IT infrastructures on the company's premises for management and maintenance, significantly reducing the solution's TCO.

Panda Endpoint Protection Plus

https://www.pandasecurity.com/en/business/solutions/#ep

Panda Endpoint Protection Plus is a security solution that leverages multiple protection technologies, allowing organizations to replace the on-premises or standalone antivirus solution installed on their network with a complete, cloud-based managed security service.

It combines an extremely lightweight security software installed on network computers for centralized, continuous protection, with a single Web management console accessible anytime, anywhere and from any device. Additionally, it provides the following features:

- User productivity control: the service can prevent access to Web resources unrelated to the company's activity and filters corporate email to prevent performance loss.

- Simple, centralized management from a single Web console, without the need to install new infrastructure to operate the service and thereby reducing the total cost of ownership (TCO).
- Compatible with Windows, macOS, Linux, iOS and Android devices, as well as with persistent and non-persistent VDI environments. One single tool is enough to respond to the security needs of all computers on the corporate network.

Panda Endpoint Protection

https://www.pandasecurity.com/en/business/solutions/#ep

Panda Endpoint Protection Plus is a security solution that leverages multiple protection technologies, allowing organizations to replace the on-premises or standalone antivirus solution installed on their network with a complete, cloud-based managed security service.

It combines an extremely lightweight security software installed on network computers for centralized, continuous protection, with a single Web management console accessible anytime, anywhere and from any device. Additionally, it provides the following features:

- Simple, centralized management from a single Web console, without the need to install new infrastructure to operate the service and thereby reducing the total cost of ownership (TCO).
- Compatible with Windows, macOS, Linux, iOS and Android devices, as well as with persistent and non-persistent VDI environments. One single tool is enough to respond to the security needs of all computers on the corporate network.

Panda Systems Management

https://www.pandasecurity.com/en/support/cloud-systems-management.htm

Panda Systems Management is a cloud-based solution for IT departments that need to provide professional remote monitoring and management services while minimizing user disruption.

Panda Systems Management increases efficiency through task automation and centralized, straightforward management of devices. The solution provides the following benefits that help reduce the overhead costs dedicated to serving each user:

- It is hosted in the cloud. Hence, it requires no additional infrastructure in the company or department providing the service, or on the managed network.
- It has a smooth learning curve for support technicians, providing value from the outset.
- It is accessible anytime, anywhere, and from any device, which means technicians do not have to be at their desktop to provide the service. Also, there is no need to visit clients' premises thanks to the remote device control feature.
- It enables task automation. Tasks can be set to be launched immediately as a response to preconfigured alerts, preventing failures before they occur.

Panda Systems Management fosters collaboration among support technicians and minimizes the time spent interacting with users to determine the root cause of problems.

Panda Email Protection

https://www.pandasecurity.com/en/support/cloud-email-protection.htm

Panda Email Protection is a cloud-based solution designed to protect clients against malicious email messages. It provides immediate protection and effective filtering technologies against spam, malware, and phishing attacks. The solution detects and stops unwanted email messages before they arrive in the email client inbox, by leveraging multiple layers of protection with spam detection rates of 99.9% and known malware detection rates of 99.99%. Panda Email Protection gives full visibility into its filtering activity thanks to real-time monitoring. Furthermore, it ensures business continuity by enabling secure access to email with 24x7 service availability The solution is easy to use, does not require additional infrastructure, and can be managed at any time from anywhere through its web console.

Panda Fusion 360

https://www.pandasecurity.com/en/support/card?id=50120

Panda Fusion 360 is a holistic solution that provides automated advanced security, centralized IT management, and remote support for all workstations, laptops and servers on the corporate network, including mobile devices and tablets. As it is a cloud solution, it is deployed rapidly without the need for maintenance or costly investments in IT infrastructure.

Panda Fusion 360 combines the best of two worlds: the advanced adaptive security provided by Panda Adaptive Defense 360 against all types of cyber-threats, and the monitoring, management and remote support capabilities delivered by Panda Systems Management. The key benefits of Panda Fusion 360 are:

- Automated prevention, detection, containment and response against any present or future advanced threat, zero-day malware, ransomware, phishing, memory exploit or malwareless attack.
- Cost savings thanks to centralized control and automation of infrastructure management tasks.
- The best support experience with proactive troubleshooting and remote, non-intrusive access to devices, wherever they are.

Panda Fusion

https://www.pandasecurity.com/en/support/card?id=50120

Panda Fusion is a complete product able to protect, manage and deliver remote support to all your IT devices, including smartphones and tablets. As it is a cloud solution, it is deployed rapidly without the need for maintenance or costly investments in server infrastructure.

Accessible online anytime, anywhere, through a simple Web browser, Panda Fusion provides:

- Maximum protection against malware and other unknown threats.
- Cost savings thanks to centralized control and automation of infrastructure management tasks.
- The best support experience with proactive troubleshooting and remote, non-intrusive access to devices, wherever they are.

Advanced Reporting Tool module

https://www.pandasecurity.com/en/mediacenter/products/advanced-reporting-tool/

Panda Adaptive Defense allows all the information collected from the client's computers to be automatically and seamlessly sent to Advanced Reporting Tool, a service designed to store and leverage security knowledge.

All actions triggered by the processes run across the IT network are sent to Advanced Reporting Tool, 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.

Advanced Reporting Tool module

https://www.pandasecurity.com/es/business/solutions/#datacontrol

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

Panda Data Control 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, Panda Data Control generates an inventory showing the evolution of the number of files with personal data found on each computer on the network.

Advanced Reporting Tool module

https://www.pandasecurity.com/en/business/solutions/#patchmanagement

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, Panda Patch Management allows organizations to roll back/uninstall those patches that support this feature, or exclude them from installation tasks, preventing them from being installed.

Panda Full Encryption module

https://www.pandasecurity.com/en/support/card?id=700067

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. Panda Full 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.

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

Advanced Reporting Tool 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. Panda SIEMFeeder for 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.

Panda SIEMFeeder for 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 (Partner Center) that enables partners to configure Panda SIEMFeeder for 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 Panda 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.

Partner Center product user profile

Partner Center is aimed at partners and service providers who wish to manage their clients' security simply and effectively, from a single console and with maximum vendor autonomy.

Types of Partner Center users

- **Resellers**: Partners who purchase Panda product licenses and sell them to their clients without adding value.
- **Managed Service Providers (MSP)**: Partners who sell Panda products to their clients and manage their security proactively.
- **ISP**: Partners who integrate their back-office into Panda's back-office to register clients and their licenses automatically. Both clients and their licenses will be visible in the Partner Center Web console.
- **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.

Chapter 3

Management console

Partner Center 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 Panda's Web console, products can be managed centrally, remotely and with a single tool.

Centralized management for all clients and roaming users

The Partner Center Web console is hosted in the cloud, so there is no need to perform additional installations on users' premises, 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 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 Partner Center 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

How to access Partner Center:

- **Partners belonging to the Panda Security security provider**: directly from Panda Cloud (**https://www.pandacloudsecurity.com**) by entering their partner credentials.
- **Partners belonging to the WatchGuard security provider** : from the link **https://watchguard.com** by entering their partner credentials.

To log in to the Panda Cloud site, you need the email address you provided when contracting the service, and the associated password. Next, you must accept the terms and conditions of the License Agreement (you will only be asked to do this the first time that you access the web console)

Account information and logout

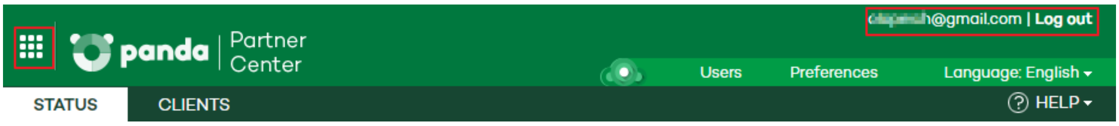


Figure 3.1: Logged-in user, logout option and access to Panda Cloud

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 Panda Cloud page. Refer to chapter **The Panda account** on page **175** 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 Panda Cloud login page.

Web console general structure

The Partner Center 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.

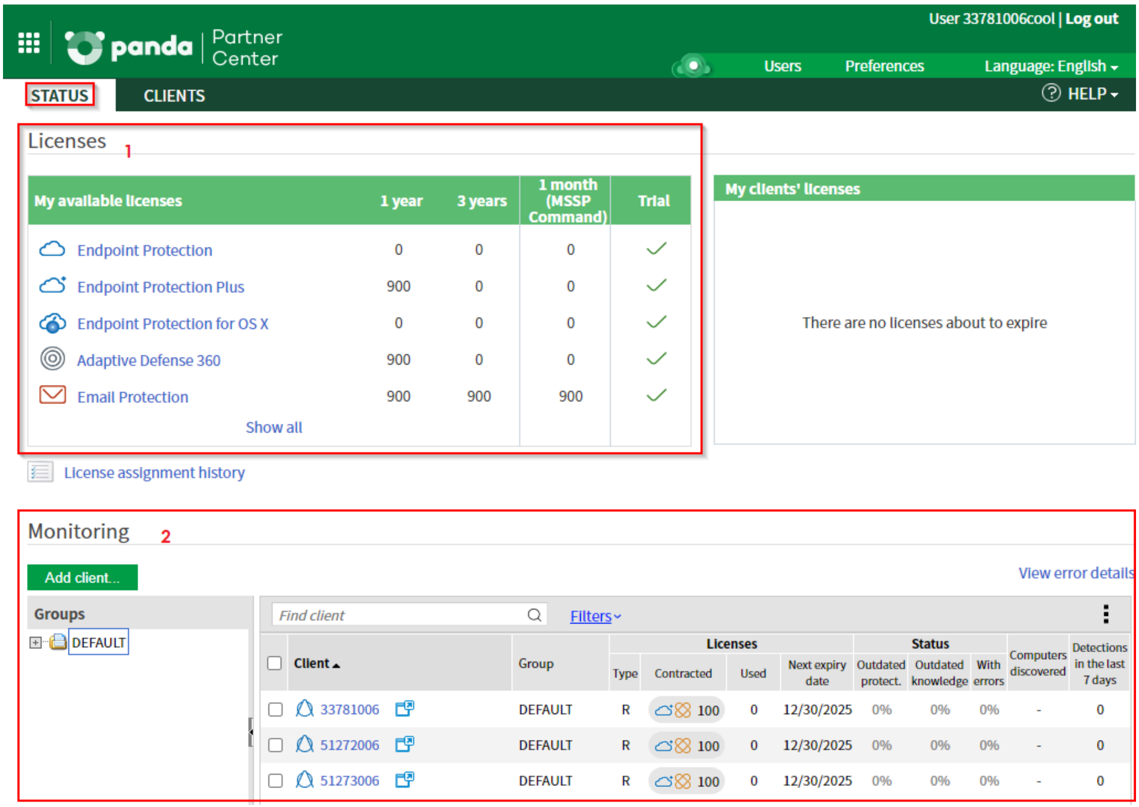
Below is a description of the console's basic features and how to use them:

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)



Licenses

My available licenses	1 year	3 years	1 month (MSSP Command)	Trial
Endpoint Protection	0	0	0	✓
Endpoint Protection Plus	900	0	0	✓
Endpoint Protection for OS X	0	0	0	✓
Adaptive Defense 360	900	0	0	✓
Email Protection	900	900	900	✓

Show all

My clients' licenses

There are no licenses about to expire

License assignment history

Monitoring

Add client...

View error details

Groups

DEFAULT

Find client

Filters

□	Client ▲	Group	Licenses				Status			Computers discovered	Detections in the last 7 days
			Type	Contracted	Used	Next expiry date	Outdated protect.	Outdated knowledge	With errors		
□	33781006	DEFAULT	R	100	0	12/30/2025	0%	0%	0%	-	0
□	51272006	DEFAULT	R	100	0	12/30/2025	0%	0%	0%	-	0
□	51273006	DEFAULT	R	100	0	12/30/2025	0%	0%	0%	-	0

Figure 3.2: Main Web console window

Top menu

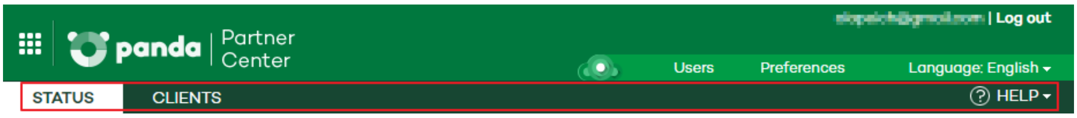


Figure 3.3: Top menu

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 as well as virtual licenses bought from Panda and which haven't yet been assigned to clients.

Click the **Status** tab to:

- Show information about the licenses purchased that are still not in use.
- 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 manually or automatically.
- Group license contracts.
- Create security settings profiles and push them to clients' workstations.

Refer to chapter ***Client management*** *on page* ***41*** *for more details.*

Help

This menu provides:

- Access to the Partner Center Web help.

http://documents.managedprotection.pandasecurity.com/Help/v77000//Partners/en-us/index.htm#t=049.htm

- Access to the Partner Center Administration Guide.

http://documents.managedprotection.pandasecurity.com/AdvancedGuide/PARTNERCENTER-Manual-EN.pdf

- Information about new features in Partner Center.

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

- Access to the license agreement
- Information about the Partner Center version available.

Other options menu

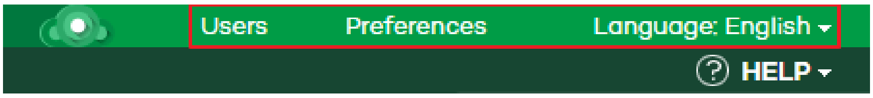


Figure 3.4: Other options menu

Users

Create users and assign them access permissions to the Web console. For more information, refer to chapter **Access and authorization in Partner Center** on page **31**.

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 **77** for more information.

Access permission for Panda

Allows Panda'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

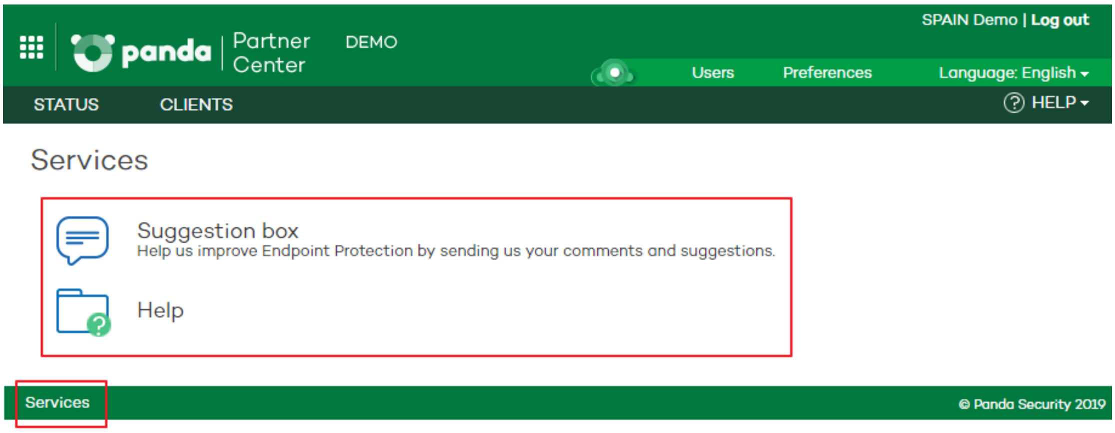


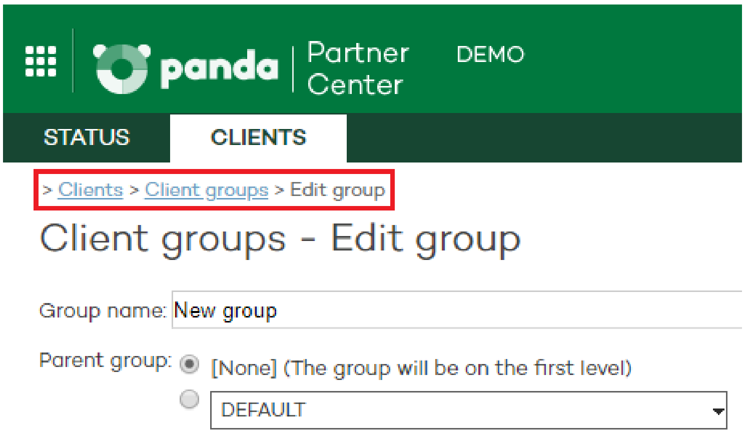
Figure 3.5: Partner Center services

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

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

Breadcrumb bar

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



panda Partner Center DEMO
STATUS
CLIENTS
> Clients > Client groups > Edit group

Client groups - Edit group

Group name: New group

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

○ DEFAULT

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:

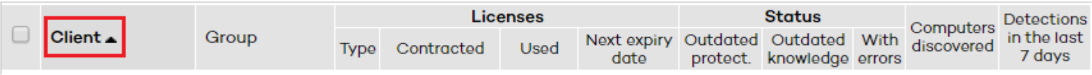
- Drop-down lists
- Combo boxes
- Buttons
- Text boxes
- Lists

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

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

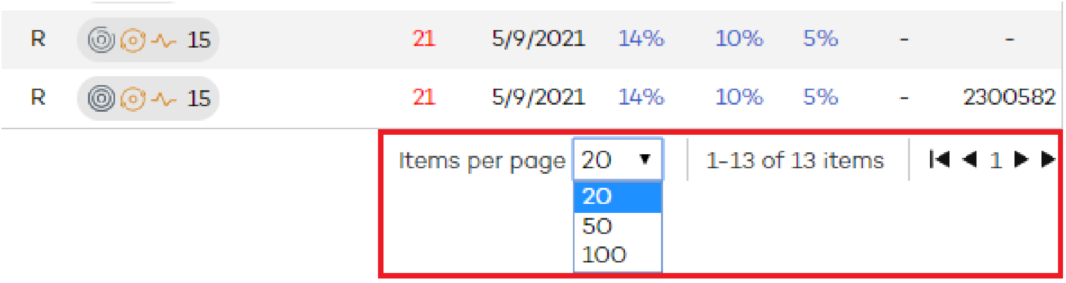


□	Client ▲	Group	Licenses				Status			Computers discovered	Detections in the last 7 days
			Type	Contracted	Used	Next expiry date	Outdated protect.	Outdated knowledge	With errors		

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 ▼

20
50
100

1-13 of 13 items

⏮ ◀ 1 ▶ ⏭

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 Partner Center

This chapter describes the resources implemented in Partner Center 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 Partner Center, 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 Partner Center 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 Panda Security. 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 Partner Center.

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 Partner Center. For more information, refer to chapter **Endpoint security product settings management** on page **91***

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.

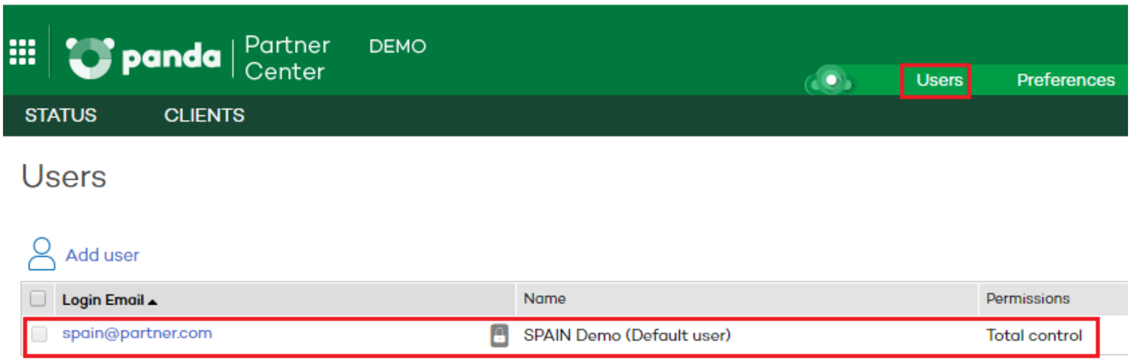
These criteria can overlap, generating a flexible, easily-established, and low-maintenance settings matrix which enables console features to be defined perfectly to ensure accessibility to each technician based on the user account they use to access the system.

Total control role

All Partner Center 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:



☐	Login Email ▲	Name	Permissions
☐	spain@partner.com	SPAIN Demo (Default user)	Total control

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

- **For partners belonging to the Panda Security security provider**: To edit the name, password, email address, or two-factor authentication status of a user, go to Panda Cloud (**https://www.pandacloudsecurity.com**).
- **For partners belonging to the WatchGuard security provider**: To edit the name, password, email address, or two-factor authentication status of a user, go to **https://watchguard.com**.

For more information, see chapter **The Panda account** on page **175**.

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 Partner Center 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 Partner Center 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 Panda Cloud:
  - For partners belonging to the Panda Security security provider: Enter your partner credentials at **https://www.pandacloudsecurity.com**.
  - For partners belonging to the WatchGuard security provider: Enter your partner credentials at **https://watchguard.com**.
- 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.

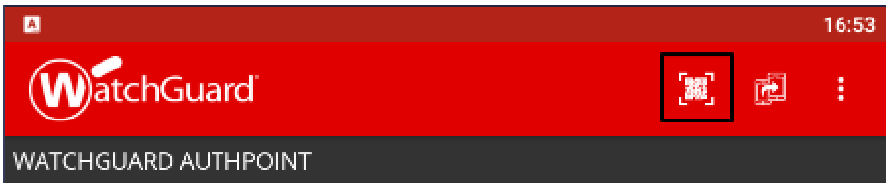


Figure 4.2: Scan QR code

- Point the camera on your device at the QR code in the Partner Center 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 Partner Center 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

Partner Center 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 **71**.
- 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 **71**.
- 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.
- View the profiles of those clients they have access to, and assign profiles to them.

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 assigned to clients in groups they have access to.
- 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 Partner Center is built around the concept of the Client, an entity that represents each company that has contracted security services through the partner.

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.

CHAPTER CONTENTS

Creating and deleting clients

Here we describe the process for Partner Center 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* ***34*** *for more information about how to create and delete users, edit their details and assign permissions. Refer to section* ***Types of permissions*** *on page* ***37*** *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**.

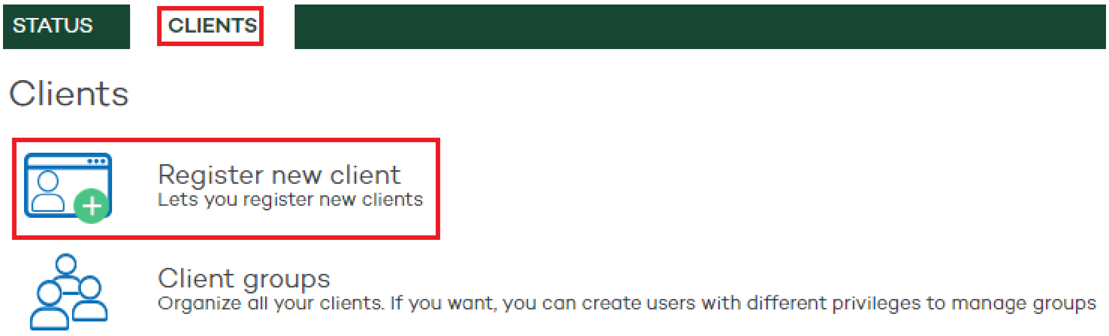

STATUS
CLIENTS
Clients
Register new client
Lets you register new clients
Client groups
Organize all your clients. If you want, you can create users with different privileges to manage groups

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**.

*Refer to **Annual license pool (1, 2, or 3 years)** on page **56** for more information about the various license validity periods based on their source (WatchGuard's MSSP Command console or Panda Security licenses).*

- **The license duration**: 1, 2, 3 years, 1 month (MSSP Command).
- **The quantity of licenses to assign**: If the number exceeds the number of licenses available in the license pool, a warning will be displayed. Refer to section **Annual license pool (1, 2, or 3 years)** on page **56**.
- **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 **16**.*

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

From the Add client button

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

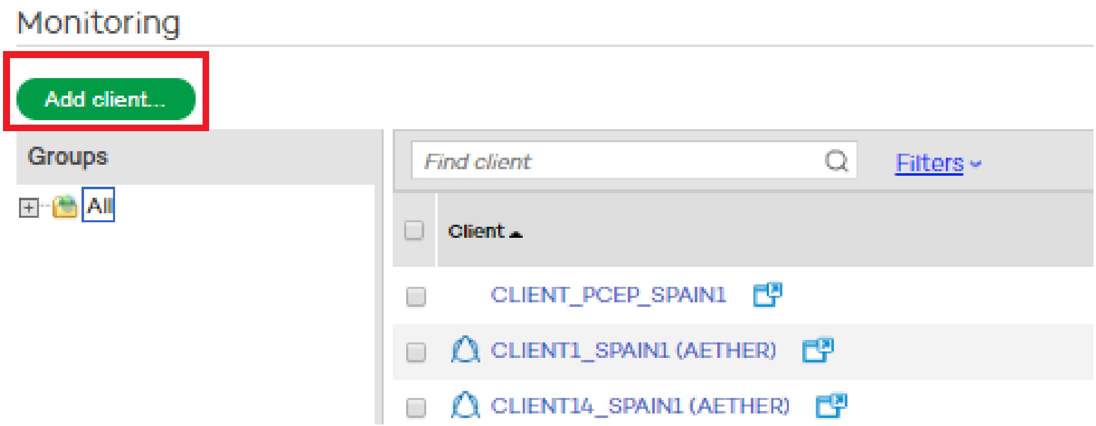


Figure 5.2: Add client

- 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 licenses will be taken from the license pool shown in the **Status** window, 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 Panda products and modules.

*For more information on managing licenses, refer to chapter **Product and license management** on page **53**.*

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.

License recovery

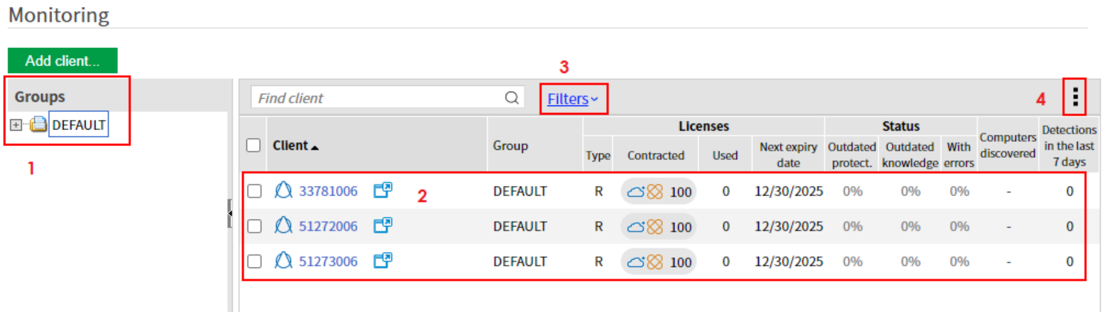
Deleting a client can in some cases involve the partial recovery of licenses that the client had assigned for modules and services, so that they may be reused and assigned to other clients.

*To know when and how licenses are recovered after a client is deleted, refer to section **Annual license recovery process** on page **82**.*

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)**


Monitoring

Add client...

Groups

DEFAULT

Find client

Filters

□	Client ▲	Group	Licenses				Status			Computers discovered	Detections in the last 7 days
			Type	Contracted	Used	Next expiry date	Outdated protect.	Outdated knowledge	With errors		
□	33781006	DEFAULT	R	100	0	12/30/2025	0%	0%	0%	-	0
□	51272006	DEFAULT	R	100	0	12/30/2025	0%	0%	0%	-	0
□	51273006	DEFAULT	R	100	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:

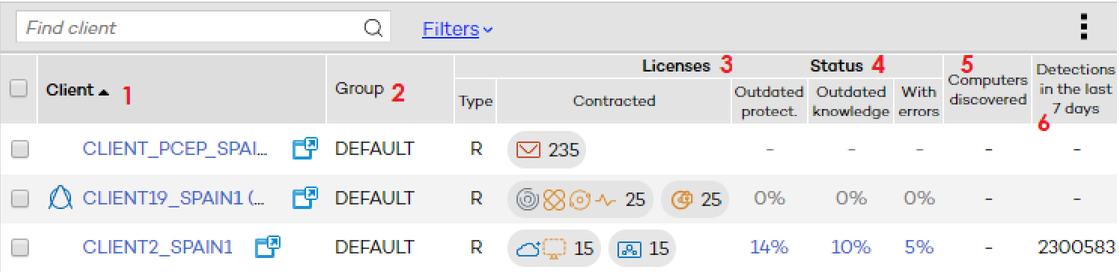
- Click **Filters (3)**.
- Select the **Show clients without active services** checkbox. Click **Filter**.

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:


Find client

Filters

□	Client ▲	Group	Licenses		Status			Computers discovered	Detections in the last 7 days
			Type	Contracted	Outdated protect.	Outdated knowledge	With errors		
□	CLIENT_PCEP_SPAI...	DEFAULT	R	235	-	-	-	-	-
□	CLIENT19_SPAIN1 (...	DEFAULT	R	25 25	0%	0%	0%	-	-
□	CLIENT2_SPAIN1	DEFAULT	R	15 15	14%	10%	5%	-	2300583

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 Panda 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 **70**.
Management mode	Indicates whether the product is centrally managed or not. For more information, see chapter **Endpoint security product settings management** on page **91**
Group (2)	Name of the group the client belongs to.
Type	Indicates whether the client has Trial or Release products. If the client has 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.

Field	Description
	• 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.
  - **Client-managed products**: For Panda Email Protection, Panda Systems Management and all bundles that include this product (Panda Fusion and Panda Fusion 360). See section **Email and RMM service management models** on page **63**
  - **Partner- managed products**: For Panda Email Protection, Panda Systems Management and all bundles that include this product (Panda Fusion and Panda Fusion 360). See section **Email and RMM service management models** on page **63**
  - **Centrally managed products:** For Panda Endpoint Protection, Panda Endpoint Protection Plus, Panda Adaptive Defense and Panda Adaptive Defense 360. See

section **Security product settings** on page **96**.

- **Non-centrally managed products**. See section **Security product settings** on page **96**.

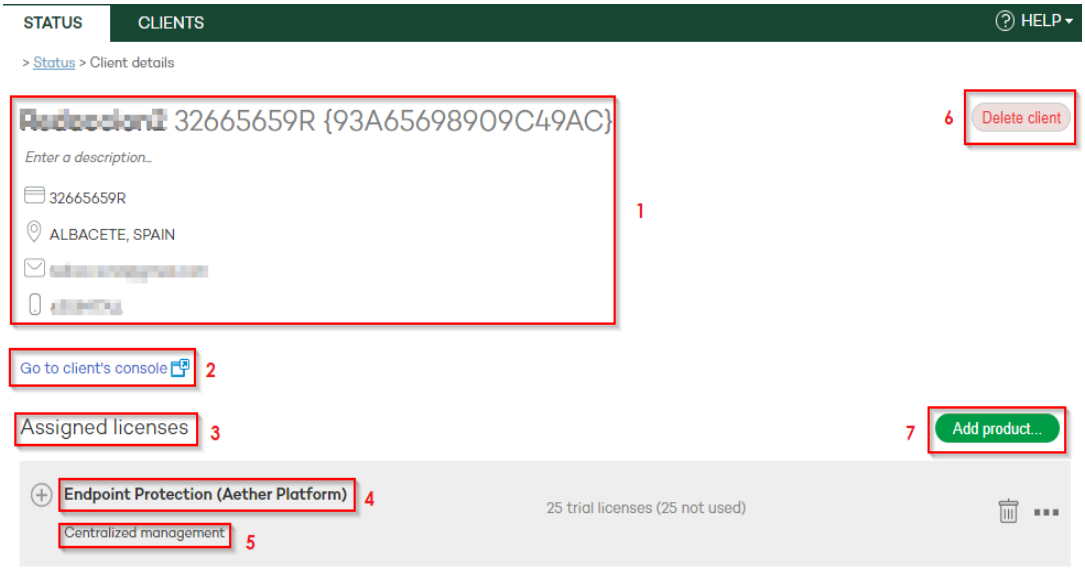
Exporting the client list

- 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:



> Status > Client details

[redacted] 32665659R {93A65698909C49AC}

Enter a description...

32665659R

ALBACETE, SPAIN

[redacted]

[redacted]

25 trial licenses (25 not used)

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 **Email and RMM service management models** on page **63**
- **Delete client** button (**6**)
- **Add product** button (**7**)

Creating and managing client groups

Why use client groups?

Partner Center 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 **33** for information on the various reasons for organizing clients into groups.

Partner Center 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.

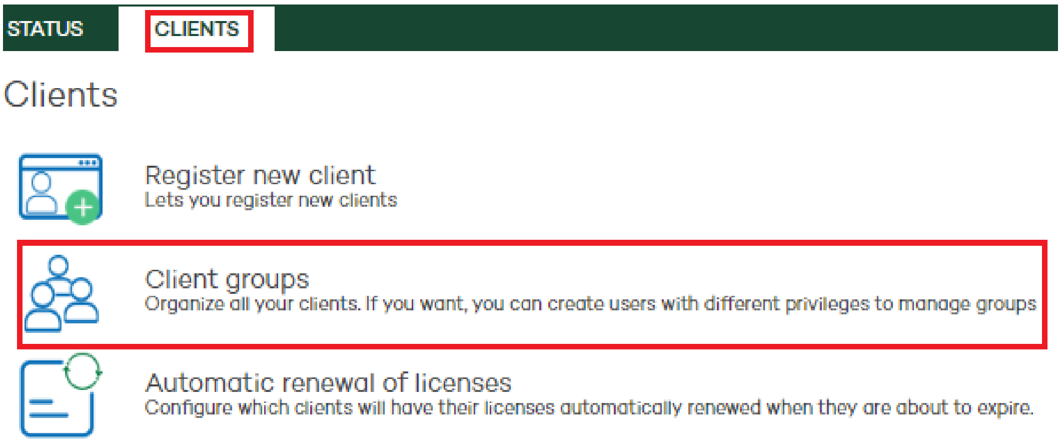
Applying configuration profiles

By assigning and sending profiles, Partner Center enables you to apply configuration profiles to client groups in order to save time. See chapter **Endpoint security product settings management** on page **91** for details of the configuration profiles supported by Partner Center.

Creating client groups

To create a client group:

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



Clients

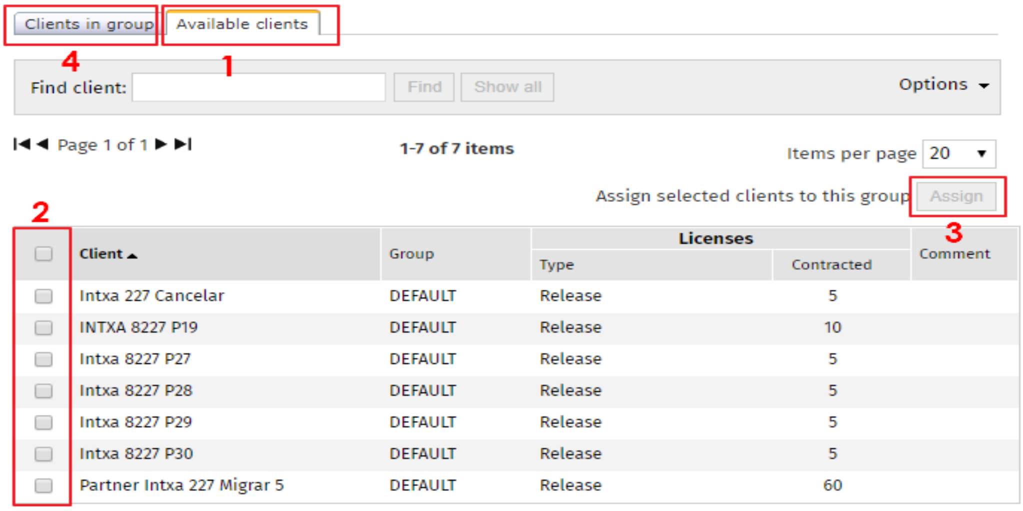
Register new client
Lets you register new clients

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

Partner Center 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 the technical departments of partners or large companies, clients and Panda Security with respect to the assignment of products, modules and licenses.

With Partner Center, 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.
- The pool/stock of licenses contracted.
- The recovery of licenses not used by clients.
- 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* ***37****.*

CHAPTER CONTENTS

Basic concepts

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

- **License pool**: Also called 'license stock' this is a repository that temporarily stores the licenses of the various products that partners buy from Panda Security to later assign to clients.
- **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 Panda Security's portfolio and compatible with Partner Center. 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.

- **Product family**: Products belong to product families in accordance with the type of product and their features. One client cannot have more than one assigned product belonging to the same family, unless one of them is a trial version.
- **Module**: A product component that adds additional functions or features.
- **License**: Each Panda Security product can be used/installed on as many devices as there are licenses in the license contract assigned to the client.
- **Virtual license**: This is the license in the license pool and which has yet to be assigned to a client. These licenses can be partially recovered in some cases if, for example, having been assigned to a client, the client does not use the service for the contracted period.
- **MSSP Points**: A 'virtual currency' that partners can exchange for product licenses. They are available to WatchGuard partners or Panda Security partners that have migrated to WatchGuard and who are signed up to the MSSP Points program.
- **MSSP Command**: This area of the WatchGuard website enables partners to exchange MSSP Points for security product licenses.
- **Management model**: Some Panda Security solutions permit 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.

Products and modules available in Partner Center

Available products and product families

The table below shows the product families available in Partner Center and the products they include:

Family	Products
Endpoint	• Panda Endpoint Protection • Panda Endpoint Protection Plus • Panda Adaptive Defense 360 • Panda Adaptive Defense • Panda Fusion (Panda Endpoint Protection Plus + Panda Systems Management • Panda Fusion 360 (Panda Adaptive Defense 360 + Panda Systems Management)
macOS	• Panda Endpoint Protection for OS X

Family	Products
Email	• Panda Email Protection
RMM	• Panda Systems Management

Table 6.1: Products supported by Partner Center classified by family

⚠ *One client cannot have more than one assigned product belonging to the same family, unless one of them is a trial version. For example, it is not possible to assign Panda Endpoint Protection and Panda Adaptive Defense to the same client.*

Modules available

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

Modules available in Partner Center are:

- Advanced Reporting Tool (ART)
- Panda Data Control (DC)
- Panda Full Encryption (FE)
- Panda Patch Management (PM)
- Panda SIEMFeeder for Partners (SF4P)

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.

License pool management

Partners have access to different types of license pools depending on the security provider to which they are associated (Panda Security or WatchGuard):

- Annual license pool (1, 2, or 3 years).
- Monthly license pool (MSSP Command).

Annual license pool (1, 2, or 3 years)

To assign products to clients, a sufficient number of product licenses must be acquired with the corresponding duration.

Partner Center supports several types of annual license pools, depending on the security provider to which the partner is associated:

- **1- and 3-year license pools**: Accessible to both Panda Security and WatchGuard partners.
- **2-year license pools**: Accessible to Panda Security partners.

The license pool is a repository where licenses are stored before being assigned to end clients. These licenses are called 'virtual licenses' and are different from normal licenses in the following ways:

- Virtual licenses do not expire as long as they are in the license pool. This offers the flexibility to maintain licenses in order to respond immediately to the needs of clients.
- Virtual licenses are acquired in blocks, with progressive volume discounts.
- Virtual licenses can be recovered totally or partially if they have been assigned to clients that have not used the product for the entire license period. After the process of recovering the license has been completed, they are available to be assigned to clients again.

Monthly license pool (MSSP Command)

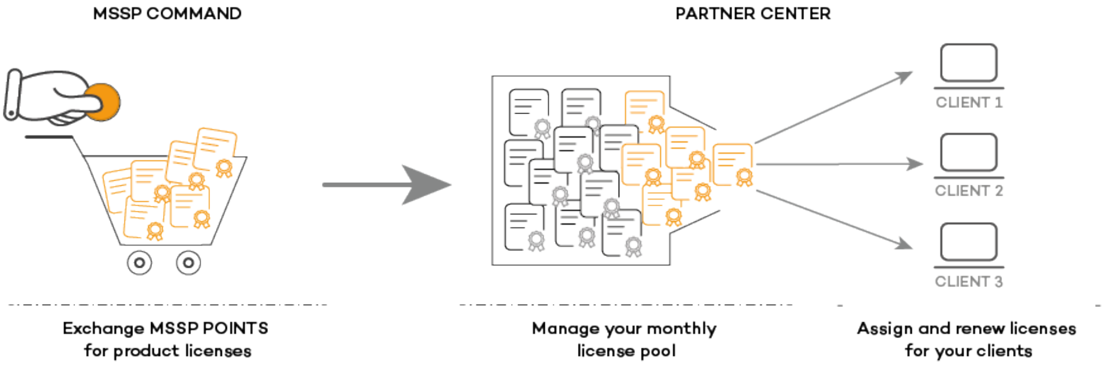

MSSP COMMAND
PARTNER CENTER
CLIENT 1
CLIENT 2
CLIENT 3
Exchange MSSP POINTS for product licenses
Manage your monthly license pool
Assign and renew licenses for your clients

Figure 6.1: Exchange of MSSP Points for Panda licenses and assignment to clients

To assign monthly licenses (MSSP Command) to a partner's clients, MSSP Points must first be exchanged for Panda Security product licenses. After this is complete, a license pool is created in Partner Center with monthly licenses with these features:

- When a partner assigns licenses to a client, they expire on the first of each month. See **Automatic renewal of one-month licenses (MSSP Command)**.
- The duration of monthly licenses (MSSP Command) is 30 days. If a license is assigned to a client after the first of the month, Partner Center recalculates the total number of licenses used in the pool (see **Process for exchanging MSSP Points in the MSSP Command console** for more details).
- Monthly licenses (MSSP Command) require continual renewal in order to keep protecting clients' systems. See **Process for exchanging MSSP Points in the MSSP Command console**)
- Monthly licenses are renewed automatically when they expire. If there are insufficient

licenses available, the logic described in **Renewal logic for clients with monthly licenses (MSSP Points)** will be applied to discount computers belonging to certain clients.

Process for exchanging MSSP Points in the MSSP Command console

Partners assigned to WatchGuard have the option of exchanging MSSP Points for Panda Security product licenses, which can then be managed later in the Partner Center.

> ⚠ *The Panda Security product licenses obtained with MSSP Points expire on the first of each month, and must therefore be renewed in order for the protection to remain active. Partners must exchange a sufficient number of MSSP Points **every month** to meet the protection needs of clients. See **Renewal logic for clients with monthly licenses (MSSP Points)** for more information about assigning licenses if there is an insufficient number of licenses to renew all assigned services.*

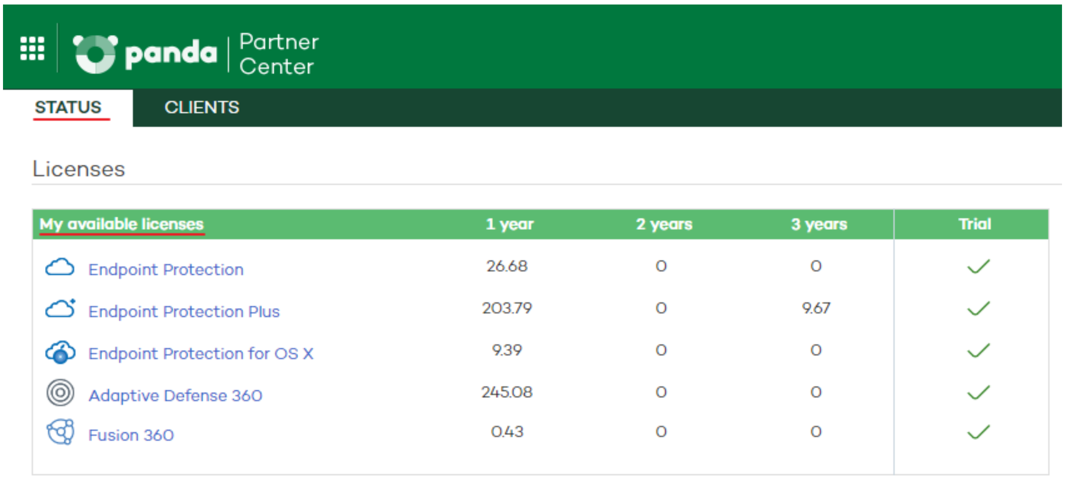
Licenses acquired by the partner always have a fixed 1-month duration. If the date the license was exchanged for points is not the first of the month, partners will require proportionally fewer licenses (and therefore fewer MSSP Points) to protect all their clients' devices. Below are two examples of how this is calculated:

- A partner has **100 MSSP Points** and needs **30 Panda Adaptive Defense 360** licenses to meet the protection needs of clients, and each Panda Adaptive Defense 360 license costs **3 MSSP Points**.
- If the partner exchanges points for licenses on the first of the month, **90 MSSP Points** are used **(30 Panda Adaptive Defense 360 licenses x 3 MSSP Points / license = 90 MSSP Points)**. In Partner Center, a monthly license pool is created (MSSP Command) with **30 Panda Adaptive Defense 360 licenses**.
- If the partner makes the exchange after the month has begun, **for example on the 23rd**, they will need fewer MSSP Points as the monthly licenses always expire on the first of the month:
  - The total number of protection days required is **270 days (9 days until the end of the month x 30 devices = 270 days)**
  - If to protect **30** devices for a whole **month (30 days) 90 MSSP Points are required**, to protect **30 devices for 9 days** requires **27 points (90 MSSP Points / 30 days = 3 MSSP Points / day. 3 MSSP Points / day * 9 days = 27 MSSP Points)**. In Partner Center a monthly license pool is created (MSSP Command) with **9 Panda Adaptive Defense 360 licenses (27 MSSP Points / 3 MSSP Points / license = 9 licenses)**.
  - The partner assigns the 9 licenses obtained to the 30 devices to be protected, which are distributed proportionally as only 9 days of protection for each device are required, and not the full month.

- In the following month, the Partner Center automatic renewal process will require 30 licenses from the monthly pool, so the partner will need to exchange 90 points for 30 Panda Adaptive Defense 360 licenses, as after the first month, full licenses will be consumed

Accessing the license pool

To access the license pool, select **Status** in the top menu. You can see the **My available licenses** section.



Licenses

My available licenses	1 year	2 years	3 years	Trial
Endpoint Protection	26.68	0	0	✓
Endpoint Protection Plus	203.79	0	9.67	✓
Endpoint Protection for OS X	9.39	0	0	✓
Adaptive Defense 360	245.08	0	0	✓
Fusion 360	0.43	0	0	✓

Figure 6.2: License pool

In the **My available licenses** panel, the virtual licenses that have not yet been assigned to clients are classified by product and duration. You can also see whether it is possible to assign trial licenses of the product to clients. See **Assigning trial licenses** for further information about trial licenses.

To add new virtual licenses to the pool, contact your assigned salesperson to place an order. After the process has been completed, the licenses will appear in the ***My available licenses*** *section.*

Migrating licenses to WatchGuard Cloud

Partners that have started to move client accounts from Panda Security infrastructure to WatchGuard infrastructure can manually migrate pools of licenses they have not already used.

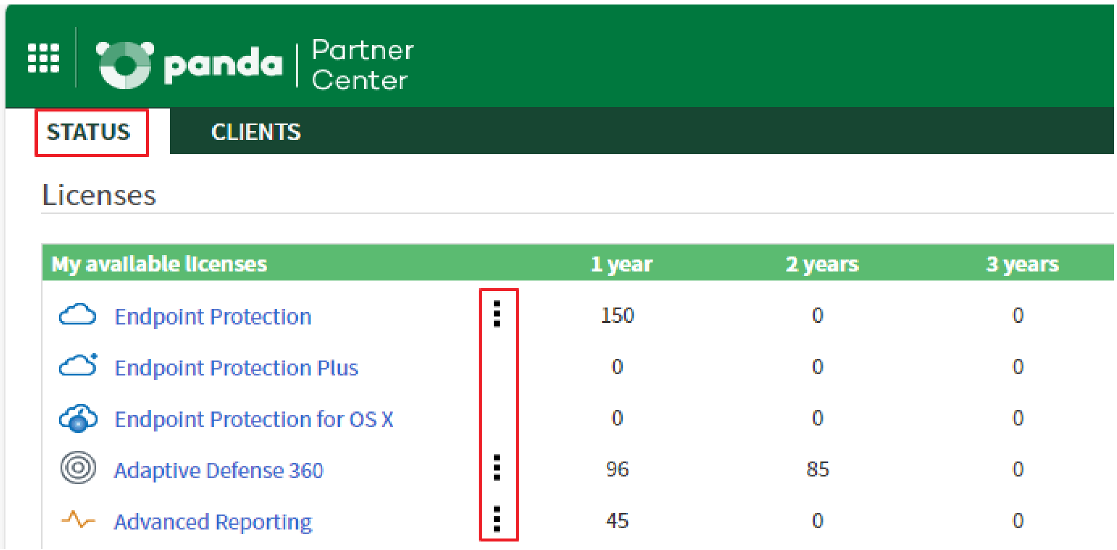
To migrate a pool licenses to WatchGuard Cloud, the partner must generate a package for each operation. This package consists of one or more license keys. A license key contains one or more licenses of a single product. These license keys are subtracted from the associated license pool and are imported from the WatchGuard Cloud portal.

License pool migration requirements and limitations

- The product associated with the license pool you want to migrate must have an equivalent product in WatchGuard Cloud:
  - Panda Endpoint Protection (is migrated to Panda Endpoint Protection Plus)
  - Panda Endpoint Protection Plus
  - Panda Adaptive Defense 360
  - Panda Adaptive Defense
  - Panda SIEMFeeder
  - Panda Patch Management
  - Panda Data Control
  - Panda Full Encryption
  - Advanced Reporting Tool
  - MDR
- One- or three-year license pools are migrated to one- or three-year license keys. For other durations:
  - License pools with durations over three years or with MSSP Points require regularization before the start of the migration process. Contact your Panda sales representative.
  - Two-year license pools are converted to two one-year license keys, with the same number of assigned licenses. Example: A license pool with 10 two-year licenses is converted to two license keys, each with 10 one-year licenses.
- The license pool you want to migrate cannot exceed 200 licenses.
- The maximum number of product licenses that can be assigned to a license key is 50.
- The user account that logs in to the Partner Center console must have the Total Control or License and Security Administrator permission. See **Types of permissions** on page **37**.

Migrating a license pool

- From the top menu, select **Status**.
- In the **Licenses** section, click the ⋮ icon for the product for which you want to migrate a license pool. A context menu opens.

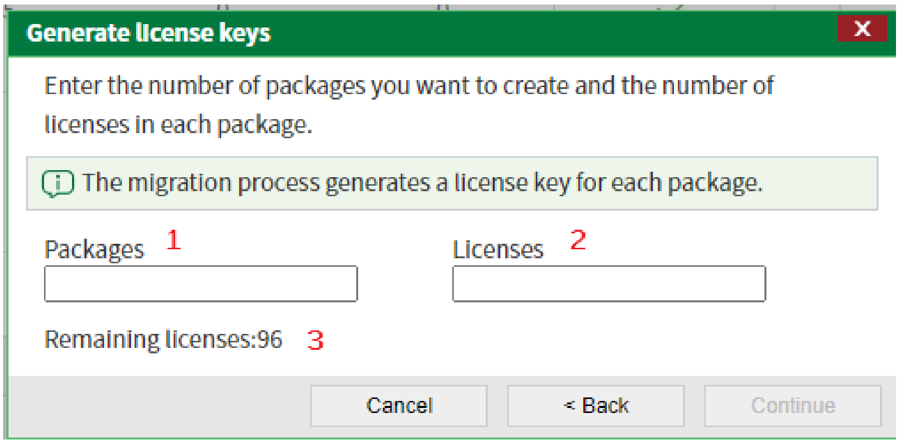


Licenses

My available licenses		1 year	2 years	3 years
Endpoint Protection	⋮	150	0	0
Endpoint Protection Plus		0	0	0
Endpoint Protection for OS X		0	0	0
Adaptive Defense 360	⋮	96	85	0
Advanced Reporting	⋮	45	0	0

Figure 6.3: Accessing license pool management

- From the context menu, select **Migrate to WatchGuard product licenses**. The **Migrate <Product Name> licenses** dialog box opens.
- From the **License Pool** drop-down menu, select the duration for the license pool you want to migrate. The menu shows only the license pools you can migrate. See **License pool migration requirements and limitations**. Click **Continue**. The **Generate license keys** dialog box opens.



Generate license keys

Enter the number of packages you want to create and the number of licenses in each package.

The migration process generates a license key for each package.

Packages 1

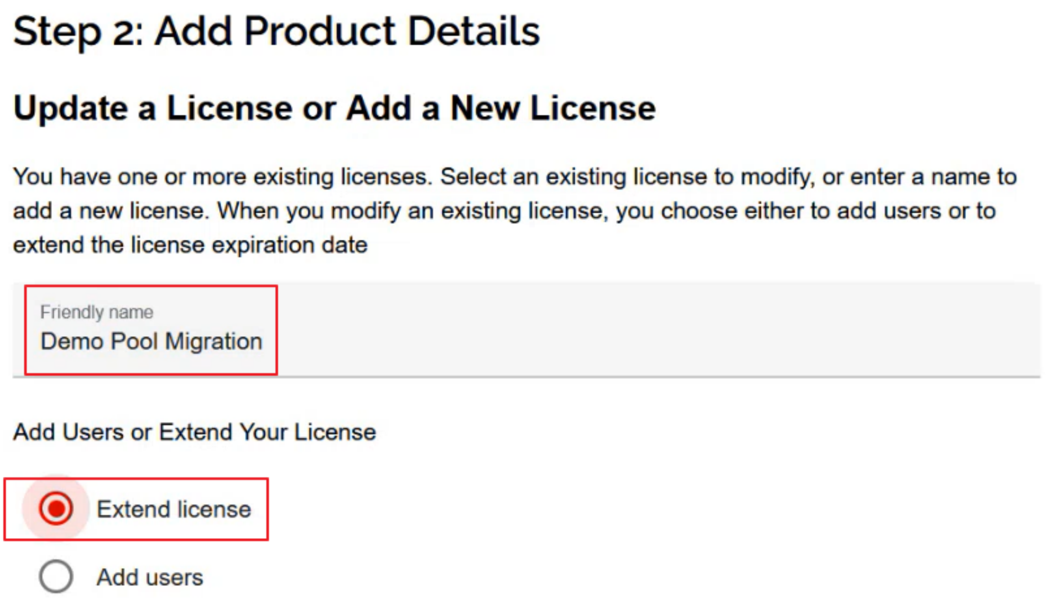
Licenses 2

Remaining licenses:96 3

Figure 6.4: Configuring a license key

- In the **Packages** text box **(1)**, type the number of license keys you want to generate.
- In the **Licenses** text box **(2)**, type the number of licenses you want to assign to each license key. For information about limitations related to the number of licenses, see **License pool migration requirements and limitations**.
- In **Remaining licenses (3)**, the console shows the rounded-up total number of licenses that are available for migration.
- Click **Continue**. The **Migration Complete** dialog box opens and shows the license keys.

- To copy the generated license keys to the clipboard, click the **Copy license keys** link.
- To activate the licenses in WatchGuard Cloud, click the **Go to WatchGuard.com** button. A new browser tab opens at **https://myproducts.watchguard.com/activate**.
- To log in to the WatchGuard portal, enter your user name and password. Click **Continue**. The **Activate Products** page opens.
- In the **Enter a Serial Number or License Key** text box, enter a license key. Click **Next**. The **Add Product Details** page opens and shows information about the package you want to activate (product name and duration) in the **Product Details** section.
- If the license key was generated from a one- or three-year license pool, or it is the first of the two license keys generated from a two-year license pool, type the license name in the **Friendly Name** text box.
- If the license key is the second of the two license keys generated from a two-year license pool, in the **Friendly Name** text box, select the name of the license created in the previous step, and select **Extend License**. The expiration information updates to the new date (2 years), keeping the number of users.



Step 2: Add Product Details

Update a License or Add a New License

You have one or more existing licenses. Select an existing license to modify, or enter a name to add a new license. When you modify an existing license, you choose either to add users or to extend the license expiration date

Friendly name: Demo Pool Migration

Add Users or Extend Your License

● Extend license

○ Add users

Figure 6.5: Configuring a two-year license key

- Click **Activate**. The total number of licenses appears, as well as the associated product, and the expiration date of the licenses that are assigned to the account.

Viewing generated license keys

- From the top menu, select **Status**. Click **License assignment history**. The **License assignment history** page opens.

- Click the **Options** drop-down menu. Select **Show filter**. A pane opens that shows the filtering criteria for the list.
- From the **Assignment type** drop-down menu, select **License migration**.
- Click **Search**. The list shows all license migration operations and their license keys, number of migrated licenses, product, operation date, and other associated information. For more information about the **License assignment history** list, see **License assignment history**.

List of license keys generated from a two-year license pool

Because two-year license pools automatically generate two one-year license keys, the **License assignment history** list shows this information in this way:

- The **Period** column shows the pool original duration (2 years).
- The **No. of licenses** column shows the number of licenses in the generated package divided by two.

Example: If the pool had seven two-year licenses, the **License assignment history** list shows two entries, each with 3.5 two-year licenses.

Service management models

Email and RMM service management models

Partner managed model

The Partner Center user manages the service. The client cannot access the product console.

Client managed model

You provide the solution to your clients, and it is each client who manages the service as they deem appropriate. For that reason, the Partner Center user cannot access the product console.

Products supported by these management models

- Panda Systems Management
- Panda Email Protection

The aforementioned management models also apply to the bundles that include any of the above products.

- Panda Fusion
- Panda Fusion 360

Assigning a management model to a new email or RMM service

- Select **Status** from the top menu. Select the client you want to assign the service to. The **Client details** page opens. This pages shows the client data and the products they have purchased.
- Click **Add product**. The **Add product**dialog box opens.
- Fill in the form. Indicate the license type, the number of licenses, and the product. The solution then checks the number of available licenses. Click **Add**. A dialog box opens for you to select the management model.
- Select a management model. Click **Add**.
  - **Managed by me**: You manage the service. The client cannot access the product console.
  - **Managed by the client**: The client manages the service. You cannot access the product console.

Changing the management model for a new email or RMM service

- Select **Status** from the top menu. Select the client whose service you want to modify. The **Client details** page opens. This pages shows the client data and the products they have purchased.
- Point to the ■■■ icon. A context menu opens.
- Select **Convert to partner-managed service** or **Convert to client-managed service**. A warning message appears.
- Click **Convert**. After a few seconds, the product management model changes.

Accessing a client’s product console

Required permissions

To access the managed product console directly from Partner Center, the partner account must have one of these permissions:

- Total control
- License and security administrator
- Security administrator

For more information about the permission system implemented in Partner Center see **Types of permissions** on page **37**.

Accessing the client's console

- Select **Status** from the top menu. Select the client whose service you want to access. The **Client details** page opens. This pages shows the client data and the products they have purchased.
- Click the **Go to client's console** link. A page opens in a new tab in your browser. This page shows the client's console. If the client has multiple managed services, the page shows the Panda Cloud site.

Information about the partner managed model for Panda Email Protection

- The Partner Center user accesses a single console that hosts all clients you manage.
- The Partner Center account visibility applies to the managed Panda Email Protection console. Nevertheless, the user must select the client to manage from the Panda Email Protection console.
- Partner Center enables you to change the management model assigned to the client's product.
- Only one access mode to the Panda Email Protection console is supported. Therefore:
  - If the Panda Email Protection user account was created from the Panda Email Protection console, this account can access the service only through the direct link **https://emailprotection.watchguard.com**, not from Panda Cloud.
  - If the Panda Email Protection user account was created from Partner Center, this account can access the service only through Panda Cloud.

Information about the partner managed model for Panda Systems Management

- The Partner Center user accesses a single console that hosts all clients you manage.
- The Partner Center account visibility does not apply to the managed Panda Systems Management console. The user must group clients manually and assign the required permissions to the account from the product.
- After you have configured the management model when assigning the product to a client, Partner Center does not enable you to change the management model from the web console.

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 Partner Center

Not centrally managed

The product is configured solely from the client's Web console. Partner Center does not apply centralized settings to the product.

Centrally managed from Partner Center

The client's product is assigned centralized settings from Partner Center.

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* ***94***
> *For more information about how Partner Center behaves with regard to centralized management, see* ***Security product settings*** *on page* ***96***.

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 Partner Center.

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 Partner Center.

> *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 Partner Center 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 Panda Security, 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 **41**.
- **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* ***44***

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 Partner Center 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. If you select Panda Systems Management, a message will be displayed asking you to choose the management model to apply to the product. See

Field	Description
	Email and RMM service management models.
Quantity	Select the number of licenses to assign. If you select an amount higher than the number of licenses available in the pool, a warning will be displayed.
Period	Select the license duration (1, 2 or 3 years). If you select a period you have no licenses for, a warning will be displayed.
Additional modules	Depending on the product selected, you can assign additional module licenses. Other than with Panda Full 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**. If the product to be added is Panda Systems Management, Panda Fusion or Panda Fusion 360, a window will appear to select the type of management: client managed or partner managed. If the product is compatible with the Aether platform, a window will appear to choose the type of management: with or without centralized management.

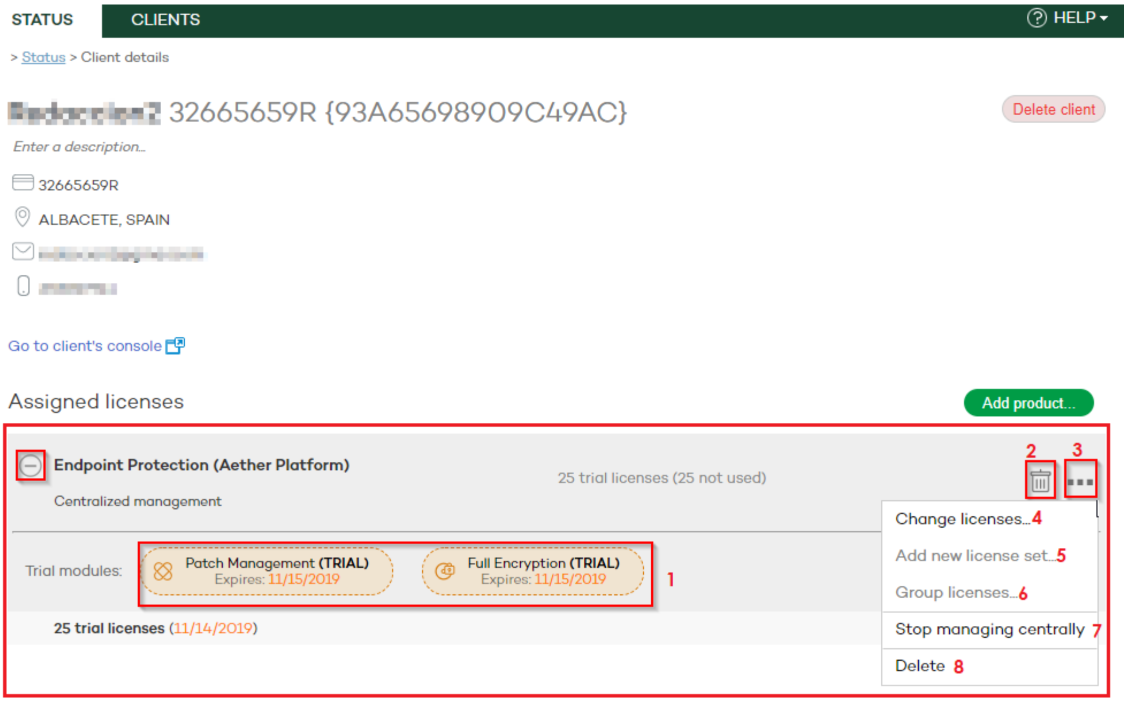
As a result of this process, the number of licenses in the pool will drop proportionally and the new license contract will be visible in the client's details. The license assignment operation will be reflected in the **My available licenses** section of the **Status** menu. See **Viewing license status**.

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 **Email and RMM service management models** for Panda Systems Management, Panda Fusion or Panda Fusion 360 or the **Default management model assigned to security products** section if it is a product managed from Aether.*

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



STATUS
CLIENTS
HELP
> Status > Client details
[redacted] 32665659R {93A65698909C49AC}
Delete client
Enter a description...
32665659R
ALBACETE, SPAIN
[redacted]
[redacted]
Go to client's console
Assigned licenses
Add product...
Endpoint Protection (Aether Platform)
Centralized management
25 trial licenses (25 not used)
2
3
Change licenses... 4
Add new license set... 5
Group licenses... 6
Stop managing centrally 7
Delete 8
Trial modules:
Patch Management (TRIAL) Expires: 11/15/2019
Full Encryption (TRIAL) Expires: 11/15/2019
1
25 trial licenses (11/14/2019)

Figure 6.6: Assigned product details

- Additional modules contracted (**1**): number of contracted licenses, license duration and expiration date.
- Context menu options (**3**):
  - Change licenses (**4**)
  - Add new license set (**5**)
  - Group licenses (**6**)
  - 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. A confirmation dialog box opens that shows the licenses that will be returned to the virtual license pool.
- Click **Delete service**. The product licenses are freed up and returned to the license pool. The client loses the protection services 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. A dialog box opens that shows the licenses you will recover. Click **Delete** . The modules licenses are freed up and returned to the license pool. The client loses the protection services immediately.

Consequences of deleting products and modules

For clients

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.

For partners

If the deletion process entails recovering licenses that have not been used by the client, those licenses automatically become virtual licenses and are included in the license pool. Later, you can assign those licenses to other clients.

For more information about how Partner Center converts released licenses to virtual licenses, see ***Formula for calculating virtual licenses***

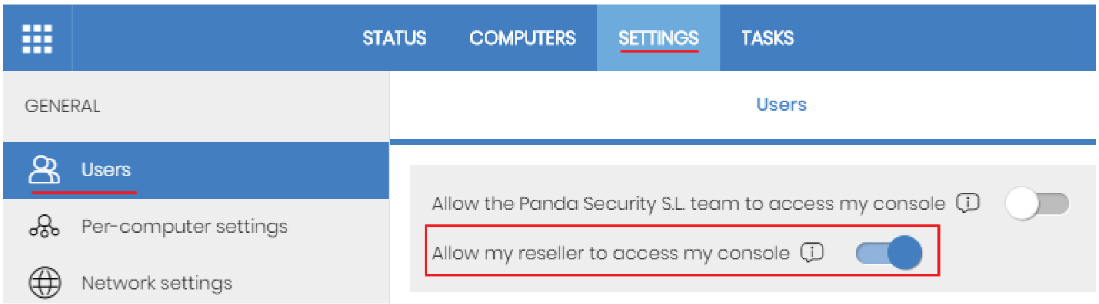
The licenses recovered are added to the total number of licenses the partner has. These licenses appear in the **My available licenses** on the **Status** page.

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 Panda Security S.L. team to access my console

Allow my reseller to access my console

Figure 6.7: Accessing the Allow my reseller to access my console option from the client's console

Accessing the client's console from Partner Center

- 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 Panda Cloud 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 Partner Center 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 the licenses acquired by partners. This area of the Web console is essential for daily management tasks, as it groups all the licenses of the different products that they have purchased, and also allows lets you know which of the licenses assigned to clients are expired or about to expire.

The license life cycle begins with the assignment of licenses to clients. These licenses can be then be modified, renewed or canceled. All actions taken are reflected in the **Licenses** area and, in addition, to offer greater control, Partner Center provides a history of 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 client removes computers from the network**: You can reduce the number of licenses assigned to the client manually.
- **When the number of computers the client has installed exceeds the number of licenses assigned**: If the client is classified as 'self-assignable', they can take the licenses they need

directly from the pool. Otherwise, you can manually increase the number of licenses assigned to them.

- **When a client removes computers from the network**: You can reduce the number of licenses assigned to a client and, in some cases, recover them in the pool.

Assigning trial licenses

Partner Center 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:

- The trial period is one month. This can be changed only for WatchGuard partners. See **Extending trial license periods**.
- The number of licenses assigned depends on the product family. This cannot be changed:
  - Panda Endpoint Protection, Panda Endpoint Protection Plus, and **Panda Fusion**: 25 licenses.
  - **Panda Adaptive Defense**, **Panda Adaptive Defense 360**, and **Panda Fusion 360**: 100 licenses.
  - **MacOS, RMM, and Email family products**: 25 licenses.
- If the client has a product, and the trial product you want to assign them belongs to the same family as that product, the trial product must provide more features than the product they already have. This condition applies only to product families that include several products, such as Endpoint Security. The product list ordered in terms of features (fewer features to more features) is as follows:
  - Panda Endpoint Protection
  - Panda Endpoint Protection Plus
  - Panda Fusion
  - Panda Adaptive Defense
  - Panda Adaptive Defense 360
  - Panda Fusion 360
- 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.
- Trial licenses for Panda Fusion are always ‘unmanaged’. See **Service management models**.

Extending trial license periods

Partners can extend the trial license period by an additional 30 days, assigning licenses to clients with a total duration of 30 + 30 days. The conditions required for requesting an extension are:

- The partner must belong to WatchGuard. This option is not available to Panda Security.partners.
- You can request the trial period extension at any time, even after the original trial period has expired.
- You can extend the trial period only once.
- You must have these permissions:
    - Total control
    - License and security administrator
    - Security administrator
- If you extend the trial period of the main product, the period of the associated modules is also extended.

To extend the trial period of a product assigned to a client:

- From the top menu, select **Status**. In the **Monitoring** area, select the client whose trial period you want to extend.
- Click the ■■■ icon associated with the trial license contract you want to extend. A drop-down menu opens.
- Select **Change licenses**. The **Change licenses** page opens.
- Click **Extend trial**. Select 30 days.
- Click **Change**. An additional 30-day period is added to the contract.

Assigning license sets

After you assign licenses for a product, you can extend their duration through the license renewal process (see **Renewing licenses**). Additionally, you can change the number of licenses through the license modification process (see **Modifying assigned products and licenses**). In both cases, the license contract associated with the client updates with the new information. For clients for which you prefer to generate an additional license contract to increase the number of licenses assigned or to extend the duration without modifying the original contract, Partner Center provides the option to **Add a new license set** to the assigned product.

> *Panda recommends that you use the feature for modifying and renewing licenses rather than creating a new license contract for an existing product.*

When you assign a new license set, bear this in mind:

- You create an independent license contract for the assigned product with a separate expiration date that depends on the start date of the license contract and the chosen license period (1 year, 2 years, 3 years, or monthly (MSSP Command)).
- License sets are only permitted for products that do not have modules assigned.
- You cannot modify license contracts with license sets later. This applies to changes of products, early renewals, changes to the number of licenses, or adding product modules.
- You can group several license contracts into one, using the process for grouping licenses. In this case, all the aforementioned restrictions do not apply. See **Grouping licenses**.

To add a license set:

- From the top menu, select **Status**. In the **Monitoring** area, click the name of the relevant client.
- The **Details** page opens. In the **Assigned licenses** section, click the ■■■ icon for the relevant product.
- A drop-down menu opens. Select **Add new license set**.
- Enter the number of licenses and the duration: 1 year, 2 years, 3 years, or monthly (MSSP Command). Click **Add**.
- If the license set belongs to Panda Fusion , Panda Fusion 360 , or Panda Systems Management, the management model is the same model as you selected for other license contracts of the product.

When the process is complete, a new license contract is created with the number of licenses specified and the expiration date corresponding to the license duration and the date it was created.

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

> ⚠ *If a client has multiple license contracts for the same product, each with a different expiration date, you must group the licenses before starting the renewal process. See **Grouping 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 and the corresponding number of licenses is subtracted from the license pool.

Automatic renewal of licenses

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

Partner Center 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.

You can automatically renew these products and modules:

- Panda Endpoint Protection
- Panda Endpoint Protection Plus
- Panda Endpoint Protection for OS X
- Panda Email Protection
- Panda Systems Management

- Panda Adaptive Defense
- Panda Adaptive Defense 360
- Panda Fusion
- Panda Fusion 360
- Panda Patch Management
- Advanced Reporting Tool
- Panda Data Control
- Panda Full Encryption

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 **48**. 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.

Field	Description
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. • **1-month licenses (MSSP Command)**: When the client's licenses expire on the first of the month, they are automatically renewed for one more month.

Table 6.4: Options in the automatic renewal list

Automatic renewal of one-month licenses (MSSP Command)

With these licenses, you enable the automatic renewal process in the same way as with other licenses. See **Configuring automatic renewal of licenses**. The differences in the renewal process with respect to one-, two-, and three-year licenses are:

- When you assign one-month licenses (MSSP Command) to a product, Partner Center automatically configures the renewal process.
- The automatic renewal process runs every day to detect clients that require renewals for not having enough licenses.

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, Partner Center 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.

⚠ *This email message does not contain information about one-month licenses (MSSP Command).*

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. Also, partially used and reduced licenses are NOT returned to the license pool.*

- 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 number of licenses in use appear along with the number of licenses released and returned to the virtual license pool. See **Formula for calculating virtual licenses**.

Changing annual licenses to monthly licenses (MSSP Points)

To change the license type from annual to monthly (MSSP Points) with automatic renewal, 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.
- Change the type of license to **1 month (MSSP Points)**. Click **Change**. The new license usage is shown.

The license type change will be made as soon as the partner requests it in the Partner Center console, though only if the client's conditions are improved:

- If the date of the license change is in the same month as when the previously assigned licenses expire:
  - The monthly licenses begin when the annual licenses expire.
  - A proportional part of the monthly licenses is consumed.
  - From the 1st of the following month, the number of licenses consumed is the same as the number of protected devices the client has.
  - Partner Center configures the automatic renewal process. See **Automatic renewal of one-month licenses (MSSP Command)**.
- If the date the licenses are to be changed is in the month prior to the month in which the previously assigned licenses expire, the change cannot take place as the client's conditions are not improved.

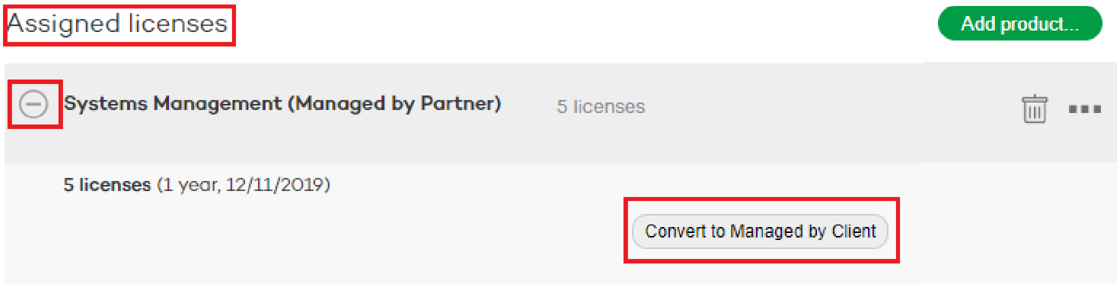
Changing trial licenses (converting from trial to commercial licenses)

With Partner Center, 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**: If the trial product does not coexist with a commercial product in the same family, you can change the trial license product to another one in its family. The licenses will continue to be trial licenses.
- **Changing from a trial product to a commercial one:**:

    - If the trial product does not coexist with an inferior commercial product, you can change the trial product to a commercial one, select additional services and the number and duration of the licenses.
    - If the trial product coexists with a commercial product in the same family, you cannot change the trial product to a commercial one as it is not possible for one client to have two commercial products from the same family. In this case, you would have to change the main product assigned to the client.

Changing the Panda Systems Management model


Assigned licenses

Add product...

⊖ Systems Management (Managed by Partner) 5 licenses

5 licenses (1 year, 12/11/2019)

Convert to Managed by Client

Figure 6.8: Information about the licenses assigned to a product

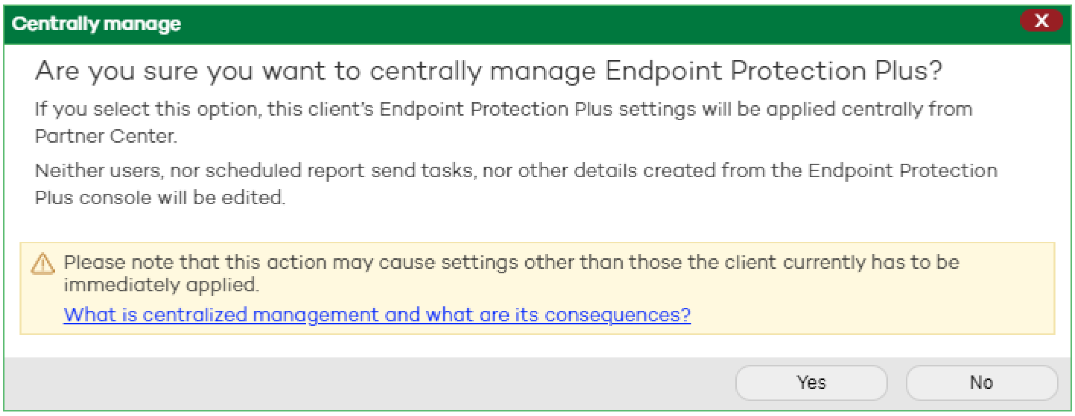
- Go to the **Status** menu at the top of the console, and click the client with the Panda Systems Management product to be changed.
- In the **Assigned licenses** section, use the icon ⊕ to display the product information.
- Click the context menu ▮▮▮ and select **Convert to managed by client** or **Convert to managed by partner**. A message appears informing you of the consequences of the action.
    - You must reinstall the service on all computers.
    - The only person with access to the Panda Systems Management console will be the person responsible for managing the service (partner or client).
- Click **OK**. The change takes place instantly.

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 **94**.
- 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 Endpoint Protection Plus?

If you select this option, this client's Endpoint Protection Plus settings will be applied centrally from Partner Center.

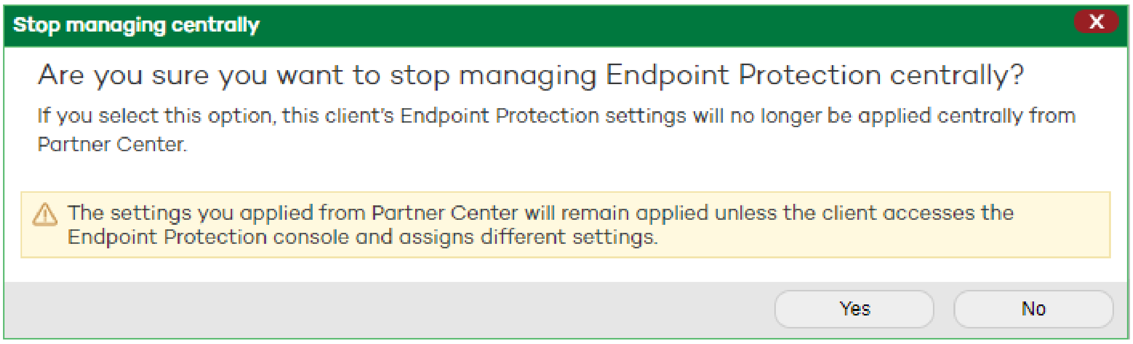
Neither users, nor scheduled report send tasks, nor other details created from the Endpoint Protection Plus console will be edited.

⚠ 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 6.9: 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 Endpoint Protection centrally?

If you select this option, this client's Endpoint Protection settings will no longer be applied centrally from Partner Center.

⚠ The settings you applied from Partner Center will remain applied unless the client accesses the Endpoint Protection console and assigns different settings.

Figure 6.10: 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 Partner Center

- The client's product is centrally assigned settings from Partner Center.

See chapter ***Endpoint security product settings management*** *on page* ***91*** *for more information about the interaction between the settings configured by the client and by the Partner Center user.*

Not centrally managed:

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

Annual license recovery process

Recovering licenses is a process that involves returning to the virtual license pool those licenses assigned to clients that have not been used entirely. The process is triggered automatically in the following cases:

- **When a product assigned to a client is deleted**: The proportional part of the licenses that the client hasn't used is returned to the license pool. If the product had associated modules, they too are recovered.
- **When changing a product assigned to client for another**: In this process, the licenses assigned with the original product are deleted.

Formula for calculating virtual licenses

Given that the virtual license pool can only contain licenses with periods of 1, 2 and 3 years, and in most cases the licenses to be recovered have been partially used by clients, an intermediate standardization process is required. This process transforms partially consumed licenses into licenses compatible with the license periods supported by the license pool. In general terms, the process follows the logic shown below:

- The expiration date of the license contract that is to be deleted is compared with the current date, to calculate the **number of days remaining**.
- The **number of days remaining** is multiplied by the number of product licenses to be canceled, in order to obtain the **total number of days remaining**.
- The **total number of days remaining** is divided by 365 x N, where N is the duration in years of the canceled product's licenses, to obtain the **number of licenses to recover**.

At the end of the process, a total number of licenses less than those canceled but with the same duration as the licenses originally assigned to the client (1, 2 or 3 years) will be restored to the license pool.

Example of license recovery

Below is a complete example of a license recovery process.

Current licenses on July 2, 2019

Client with the products and modules shown below:

- 100 1-year licenses of Panda Adaptive Defense 360.
- 100 1-year licenses of Panda Data Control.

License expiration date: December 17, 2019

Web console user's action: Change product and renew for one year

The user wants to change the current licenses of Panda Adaptive Defense 360 into 1-year licenses of Panda Fusion 360, while keeping the additional modules and renewing the entire service for one year.

Calculations made by Partner Center

- The number of unused licenses of the previous Panda Adaptive Defense 360 product are recovered on applying the formula:

```
No. of previous product licenses x No. of days until product
expiration / 365 x license period (years)
```

- **100 licenses x 169** (days remaining from July 2 to December 17) / **365 = 46.3** 1-year licenses of Panda Adaptive Defense 360, which will be added to the license pool.
- **46.3 product licenses of** Panda Fusion 360 will be taken from the license pool to service the client from July 2 to December 17, plus **100 Panda Fusion 360 product licenses** dedicated to the renewal from December 17.
- Module licenses will be unaltered, so **100 Panda Data Control module licenses** will be taken from the pool to service the client from December 17.
- All licenses assigned will have the new renewal date of: **December 17, 2020**.

Grouping licenses

In cases where a web console user has created multiple license contracts for the same product using the **Add new license set** option (see **Assigning license sets**) and needs to assign modules to the product and/or wants to set the same expiration date for all contracts, you can generate a single contract by grouping licenses.

You cannot group annual or monthly (MSSP Command) license contracts.

License grouping process

Follow these steps:

- In the top menu, select **Status**. In the **Monitoring** section, find the client whose licenses you want to group. In the **Client** column, click the client name.
- On the **Client details** page > **Assigned licenses** section, click ▮▮▮. Select **Group licenses**. A confirmation dialog box appears.

At the end of the process, there is one license contract with all licenses and a pro-rata expiration date for all licenses.

Formula for calculating the new license period

In the grouping process, we use the number of licenses in each license contract and its expiration date to calculate the final result. The result is a single license contract with the total sum of licenses and a shorter license period. In general terms, the process follows this logic:

- We compare the expiration date of each license contract to the current date to calculate the **number of days remaining on each license contract**.
- We multiply the **number of days remaining on each license contract** by the number of licenses in the contract to get the **total number of days remaining on each license contract**.
- We calculate the **total number of days remaining** for the client by adding up the **total number of days remaining on each license contract**.
- We calculate the **total number of licenses** by adding up the licenses assigned in each license contract.
- We divide the **total number of days remaining** by the **total number of licenses** to get the **total number of days of service**.

Example of a license grouping operation

A client has four Panda Endpoint Protection Plus license contracts with these licenses and license periods:

- License contract A: 5 licenses with 18 days remaining.
- License contract B: 1 license with 44 days remaining.
- License contract C: 1 license with 75 days remaining.
- License contract D: 4 licenses with 159 days remaining.

Calculation of the number of license days remaining:

- **Total number of days remaining**: (5 licenses x 18 days) + (1 license x 44 days) + (1 license x 75 days) + (4 licenses x 159 days)= 845 days.
- **Total number of licenses**: 5 + 1 + 1 + 4 = 11 licenses across four license contracts.
- **Number of days of service**: 845 / 11 = 76.8 days.

At the end of the license grouping process, the client has a single license contract which expires in 77 days and covers the 11 computers on their network.

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 and analytics carried out by Partner Center. Computers affected by this situation will automatically revert to their protected status as soon ass the client has a sufficient number of licenses.

Renewal logic for clients with monthly licenses (MSSP Points)

- Renewals apply to the complete client. If there are not enough licenses available for all the client's devices, then none are renewed.
- Clients' licenses are renewed in chronological order: the first to acquire monthly licenses (MSSP Command) have priority of renewal over more recent clients.

Actions to take for clients with annual licenses

If there are new, unprotected devices on the network.

- **The client has several license contracts**: The Web console user must create a new license contract with the same number of licenses as new computers. See **Assigning license sets**.
- **The client has one license contract**: The Web console user must change the number of licenses to include the new computers. See **Modifying assigned products and licenses**.

If there are previously protected computers on the network with annual licenses that have expired.

- **The client has several license contracts**: The Web console user must create a new license contract with the same number of licenses as computers with expired licenses exist on the network. See **Assigning license sets**.
- **The client has one license contract**: The Web console user must renew the license contracts affected. See **Renewing licenses**.

Panda Security recommends migrating to a single license contract per product to better adapt to clients' needs. To do this, use the license grouping feature. See ***Grouping licenses***

Actions to take for clients with monthly licenses (MSSP Command)

If there are new, unprotected devices on the network.

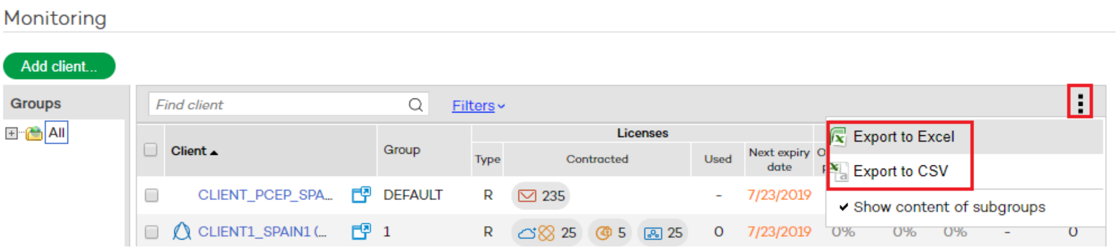
- The Web console user must exchange enough MSSP Points in the MSSP Command console.
- **The client has several license contracts**: The Web console user must create a new license contract with the same number of monthly licenses (MSSP Command) as new devices. See **Assigning license sets**.
- **The client has one license contract**: The Web console user must change the number of monthly licenses (MSSP Command) to include the new devices. See **Modifying assigned products and licenses**.

If there are previously protected devices on the network with monthly licenses (MSSP Command) that have expired:

- The Web console user must exchange enough MSSP Points in the MSSP Command console. Partner Center will check every day for new monthly licenses (MSSP Command) and assign them to devices with expired licenses.

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:



Monitoring

□	Client ▲		Group	Licenses									
				Type	Contracted	Used	Next expiry date						
□	CLIENT_PCEP_SPA...		DEFAULT	R	235	-	7/23/2019						
□	CLIENT1_SPAIN1 (...		1	R	25 5 25	0	7/23/2019	0%	0%	0%	-	0	

Figure 6.11: Exporting client lists

- 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.

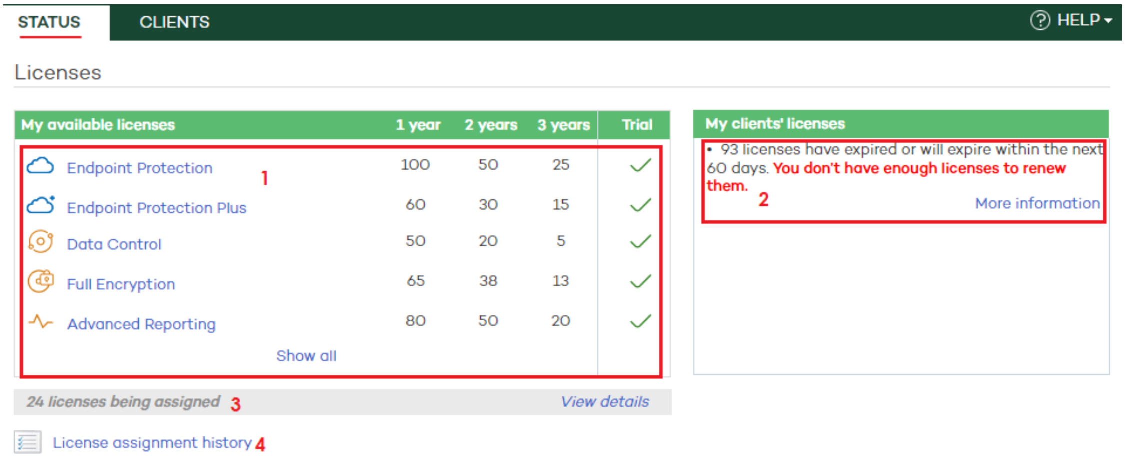
Email list of computers with expired licenses

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 Partner Center web console.



My available licenses	1 year	2 years	3 years	Trial
Endpoint Protection	100	50	25	✓
Endpoint Protection Plus	60	30	15	✓
Data Control	50	20	5	✓
Full Encryption	65	38	13	✓
Advanced Reporting	80	50	20	✓

Show all

My clients' licenses

- 93 licenses have expired or will expire within the next 60 days. You don't have enough licenses to renew them.

More information

24 licenses being assigned *View details*

License assignment history

Figure 6.12: 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	Indicates the license period (one, two, or three years).
Trial	Indicates whether Partner Center enables you to assign trial licenses for this product.
Show all	Shows all products or only products for which there are virtual licenses.

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)

Partner Center 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 **48** window.
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.
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**.

Field	Description
Service cancellation	See **Deleting products and modules**.
Grouping	See **Grouping licenses**.

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.
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 **44** for more information. • **Service change** See **Modifying assigned products and licenses**. • **License contract renewal** See **Renewing licenses**. • **Grouping license contracts**: See **Grouping licenses**.

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

Chapter 7

Endpoint security product settings management

Partner Center 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 Aether.

CHAPTER CONTENTS

Partner Center 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 Partner Center 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 Partner Center with respect to the Aether 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 Partner Center 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 Partner Center are inherited from the Aether 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 Partner Center, along with a link to the associated guide:

Product / Module	Product guide
Panda Adaptive Defense 360	Panda Adaptive Defense 360 Administration Guide **http://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/latest/ADAPTIVEDEFENSE360oAP-guide-EN.pdf**
Panda Adaptive Defense	Panda Adaptive Defense Administration Guide **http://www.pandasecurity.com/rfiles/enterprise/solutions//adaptivedefense/latest/ADAPTIVEDEFENSEoAP-guide-EN.pdf**
Panda Endpoint Protection	Panda Adaptive Defense 360 Administration Guide **http://www.pandasecurity.com/rfiles/enterprise/solutions/endpointprotection/latest/ENDPOINTPROTECTIONoAP-guide-EN.pdf**
Panda Endpoint Protection Plus	Panda Adaptive Defense 360 Administration Guide **http://www.pandasecurity.com/rfiles/enterprise/solutions/endpointprotection/latest/ENDPOINTPROTECTIONoAP-guide-EN.pdf**
Panda Full Encryption	Installed product administration guide.
Panda Data Control	Installed product administration guide.
Panda Patch	Installed product administration guide.

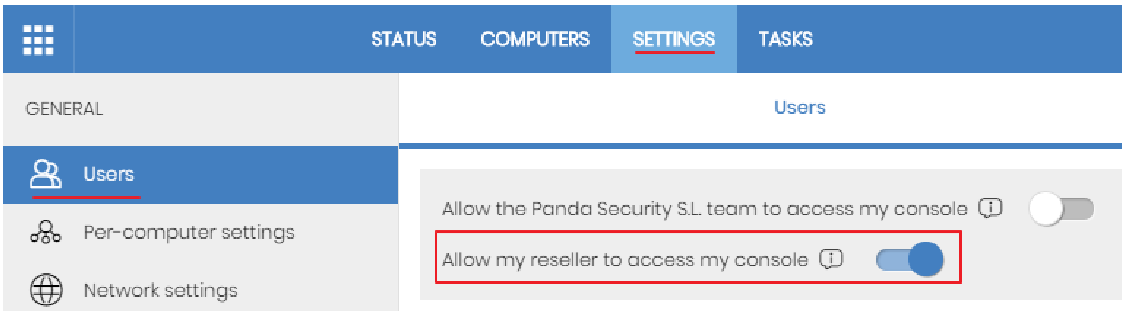
Product / Module	Product guide
Management	
Panda SIEMFeeder for Partners	Infrastructure Guide. **https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/SIEMFeeder-Manual-EN.PDF** Event Description Guide. **https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/SIEMFeederAD-EventDescriptionGuide-EN.pdf**

Table 7.1: Products supported by Partner Center and the corresponding administration guide.

Requirements for assigning centralized settings

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

- The Partner Center Web console user must have previously created the client and assigned a security product to them. Refer to **Supported products and modules**.
- The Partner Center Web console user must have chosen the option to manage the product centrally. Refer to **Assigning products to clients** on page **67**
- The Partner Center 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 Partner Center** on page **31** for more information about permissions in Partner Center.
- 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**.



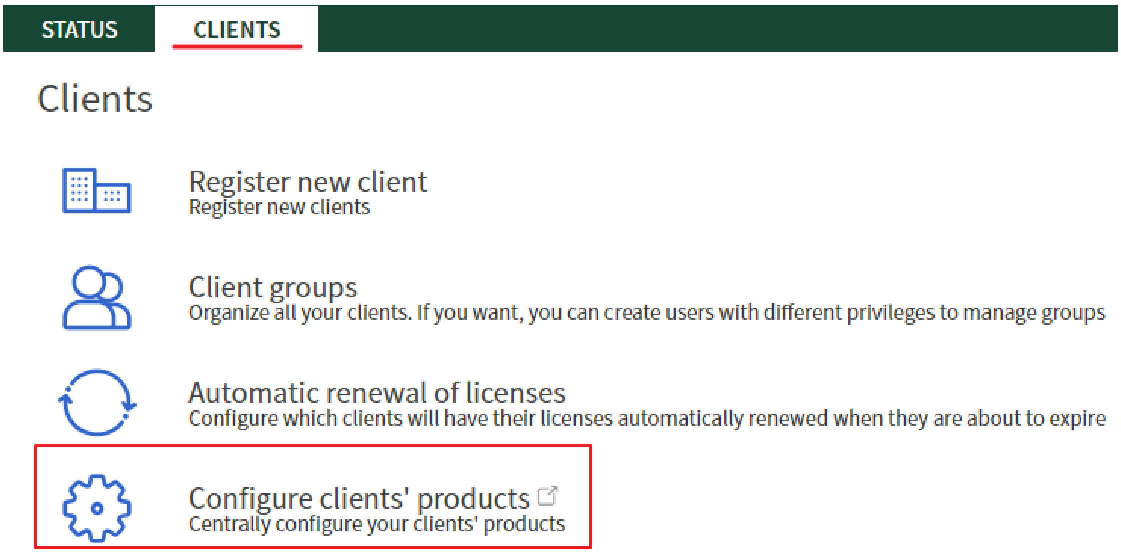
Allow the Panda Security S.L. team to access my console

Allow my reseller to access my console

Figure 7.1: Accessing the ‘Allow my reseller to access my console’ option from the client’s Aether 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 Panda SIEMFeeder for 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 Partner Center

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 Partner Center** in the relevant product administration guide.

Partner Center 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: • 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 Partner Center, 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**.
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.

Settings	Description
	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 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 Panda 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 Aether 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.

Settings	Description
	See **Full Encryption settings**.
Panda SIEMFeeder for Partners	Configure unified settings to receive all the telemetry generated on your clients' computers. For more information about how to configure the module, see section **Panda SIEMFeeder for Partners settings**.

Table 7.2: Settings profiles available in Partner Center

Settings profiles editable by clients

By default, clients cannot edit or delete the settings profiles inherited from a service provider. Nevertheless, Partner Center 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 Partner Center:

- 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 Aether console

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

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

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

Patching test computers

When configuring Panda Patch Management in the Aether 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 Aether console, create a Panda Patch Management settings profile.
- In the settings profile, select **Designate as test computers and install patches** from the **Patch installation** drop-down menu.
- In the Partner Center 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 Partner Center , see **Creating tasks** on page **159** and **Configuring Panda Patch Management tasks (4)** on page **164**.

*For more information about how to configure Panda Patch Management in the Aether 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 **37**.*

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.

Panda SIEMFeeder for 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 Panda Security 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://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/SIEMFeederAD-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

Partner Center allows settings to be assigned to clients with Aether 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 Partner Center 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 Partner Center 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

Partner Center 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 Partner Center, 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:

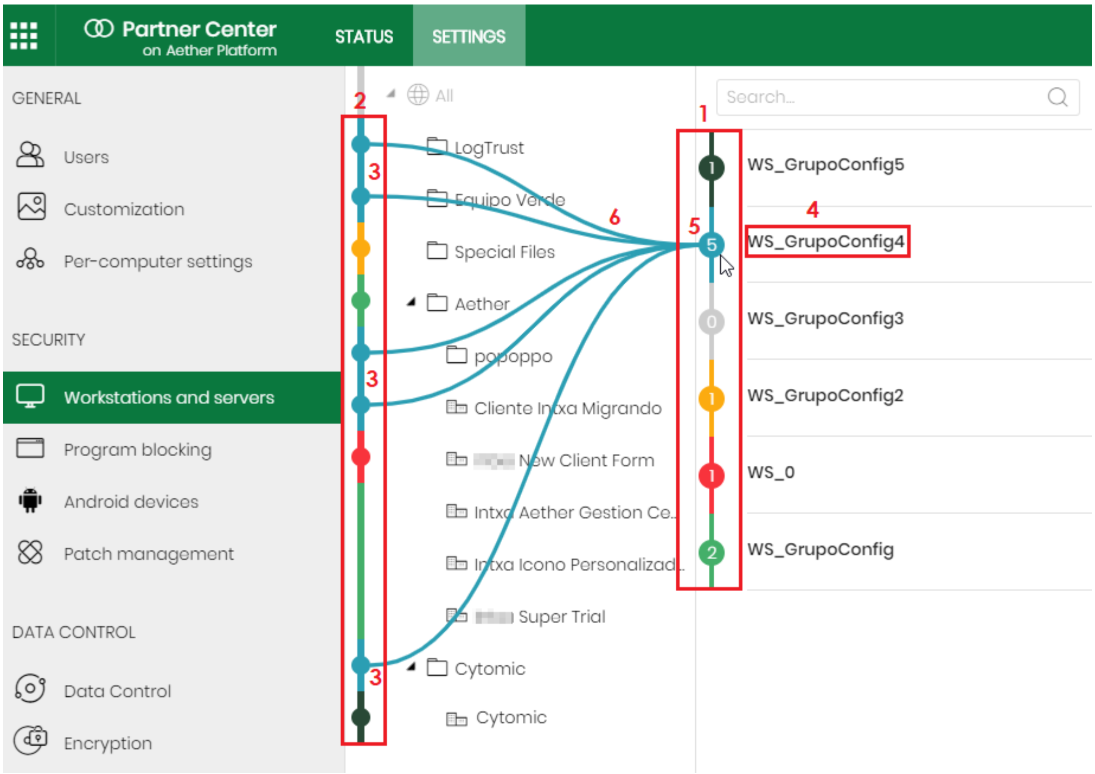


Figure 7.3: Viewing assigned settings

- **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, Panda Partner Center 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.

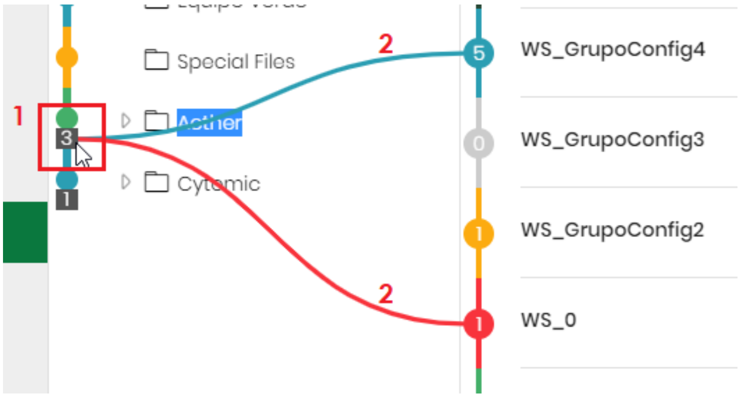


Figure 7.4: Viewing the settings assigned to nodes with exceptions

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 Partner Center console user. For this reason, Partner Center 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 Partner Center and centrally sent to a client are owned by Partner Center.
- Settings created and sent from the Partner Center Web console whose recipients are later edited in the client's console are co-owned.

The implemented rules are as follows:

- **Settings owned by Partner Center**: 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 Partner Center 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 Partner Center Web console.
- **Co-owned settings**: these settings can be edited (synced) from the Partner Center 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 Partner Center. Just like settings owned by Partner Center, these settings appear in the client's console with a green label with the text "Partner Center".

Creating settings in clients' consoles

When the Partner Center 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 Partner Center 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 Partner Center 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 Partner Center Web console to the settings sent or assigned to clients are automatically synced in the clients' consoles. This synchronization is unidirectional, from Partner Center 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 Partner Center Web console are as follows:

- The Partner Center 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 Partner Center 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 Partner Center 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 Partner Center Web console user are not deleted. They are kept in the client's console.
- Even after a settings profile is deleted from the Partner Center 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 Partner Center Web console through inheritance or, if there are no settings available for that client in Partner Center, 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 Partner Center 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 Partner Center to access their console (see **Requirements for assigning centralized settings**).
- The client is removed from the Partner Center web console after the contractual relationship ends.
- The product management mode is changed from the Partner Center web console. See **Assigned product details** on page **68**.

When that happens, all settings owned by the Partner Center web console or co-owned with the client, excluding settings associated with the Panda SIEMFeeder for 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 Partner Center 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 Panda SIEMFeeder for Partners

Because the Panda SIEMFeeder for 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 Partner Center/client relationship

If the Partner Center/client relationship is restored after it is broken, Partner Center 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 Partner Center*** *on page* ***31***.

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 Partner Center to access their consoles and have been configured as centrally managed in the Partner Center 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.

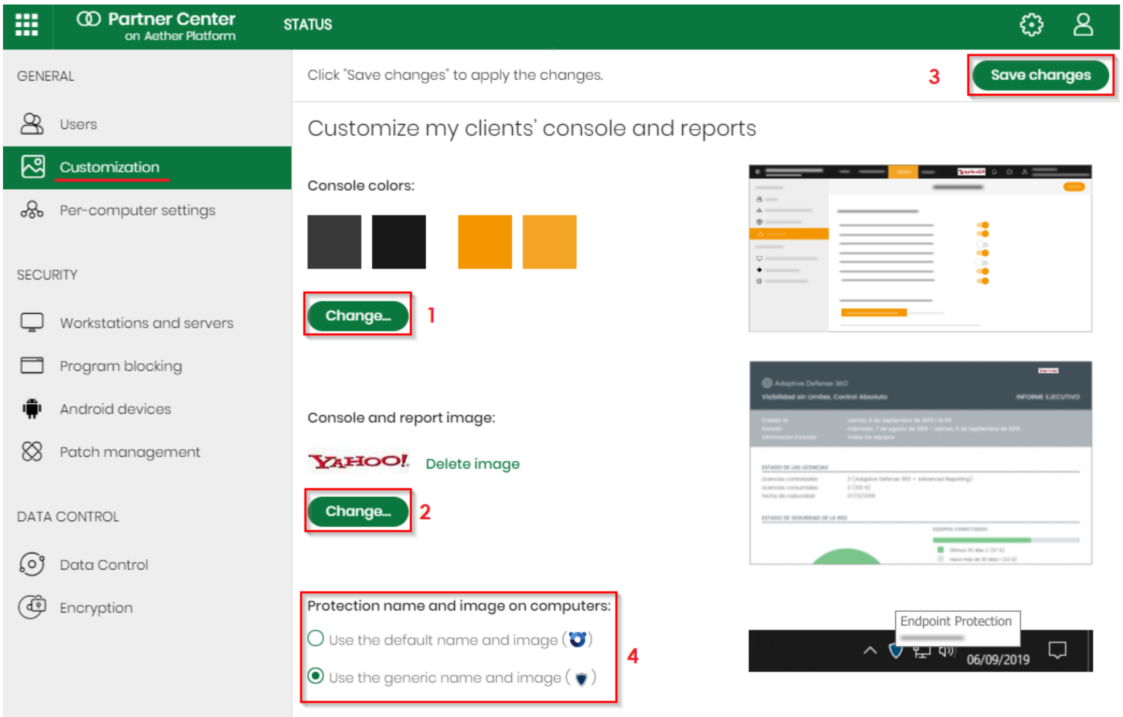
You can delete only settings profiles that do not have clients assigned. To unassign a settings profile from a client, the user account must have permissions on the client.

Customizing clients' consoles (Co-branding)

Partner Center 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:

Delete image

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).

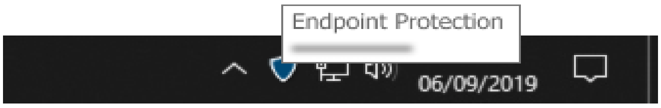


Figure 7.6: Security product generic name and image

- 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 "Panda" name. For example, Panda Endpoint Protection will appear as "Endpoint Protection".

Clients' security status

Panda Partner Center 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 Partner Center** on page **31**.*

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.

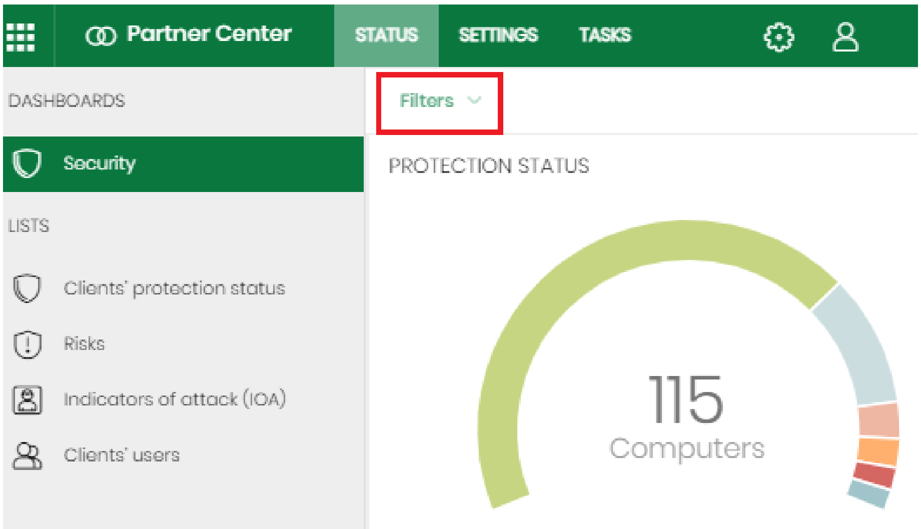


Figure 7.7: Selecting the security dashboard filters

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

Protection status

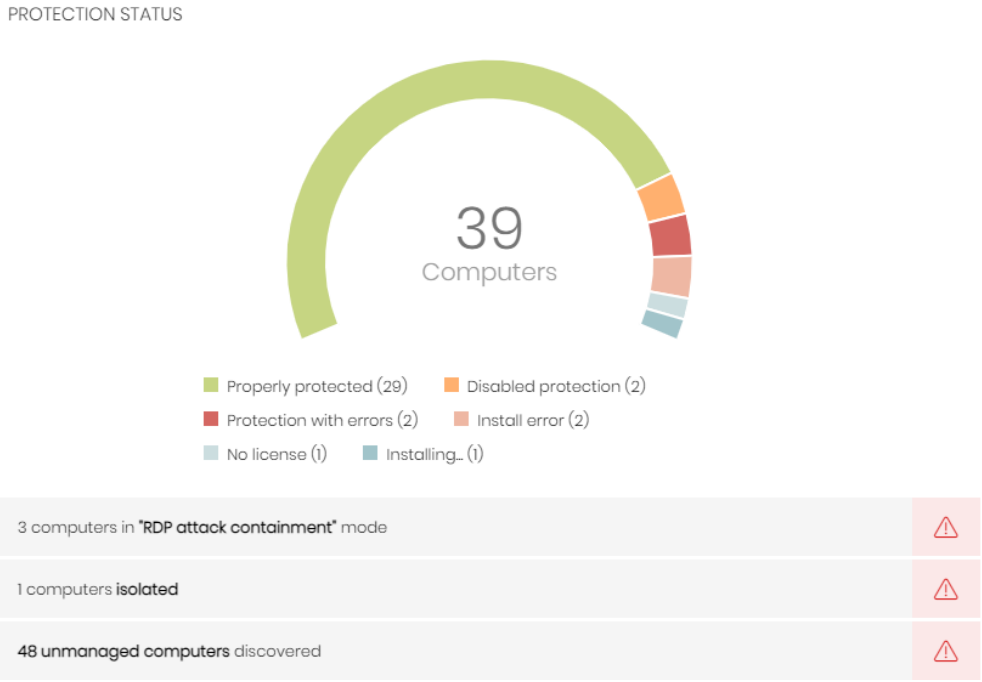
This widget provides a graphical representation and percentage of clients' computers with the same status. It shows the clients' computers where the security software works correctly and where it does not, and computers with installation errors or problems The status of the network computers is represented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

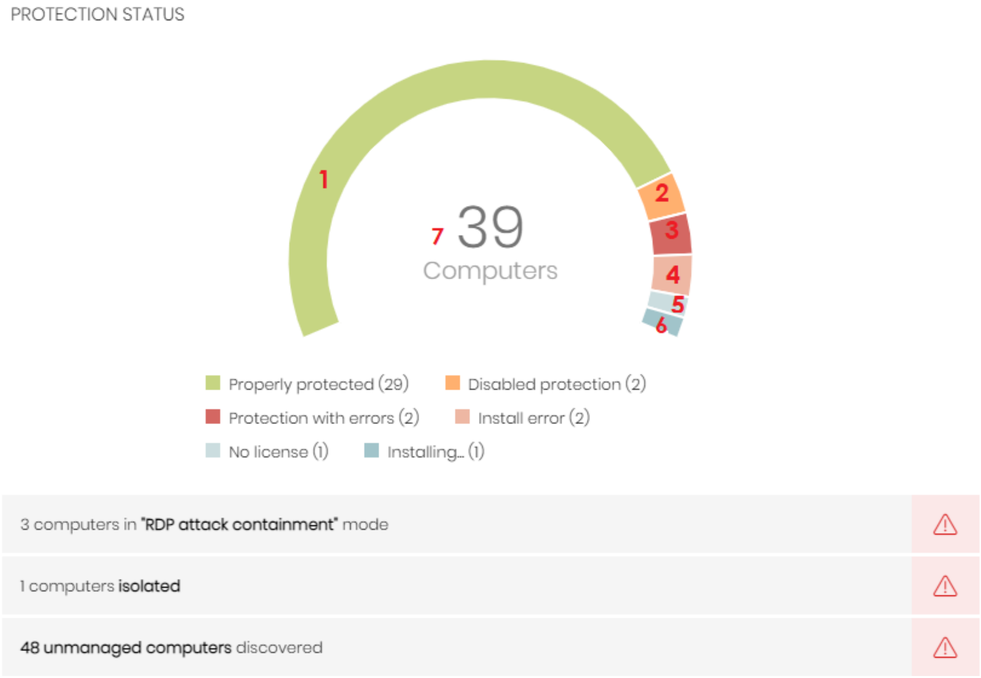
Meaning of the data displayed

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 Panda Security servers.
Install error	Number of clients' computers on which the security

Data	Description
	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.
(2)	Protection status = Disabled protection.
(3)	Protection status = Protection with errors.

Hotspot	Filter
(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 Panda Security 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 Aether knowledge servers.

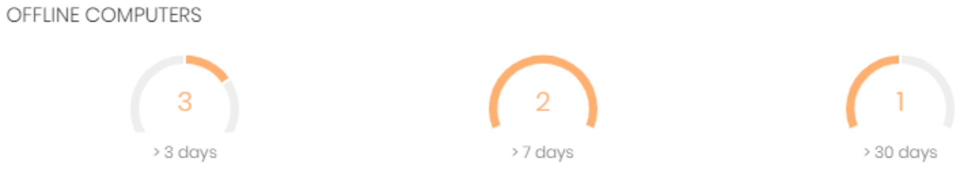


Figure 7.10: Offline computers panel

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.
> 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

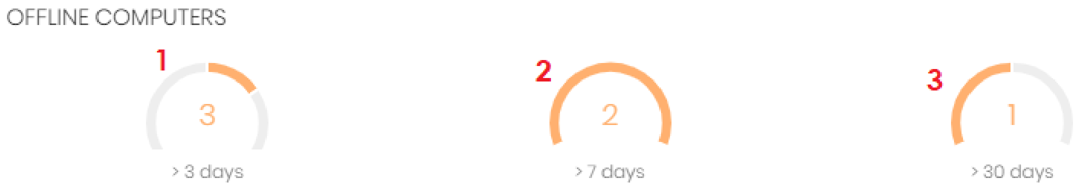


Figure 7.11: Hotspots in the offline computers panel

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.

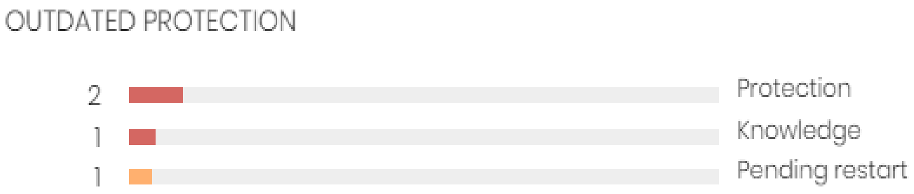


Figure 7.12: Outdated protection panel

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

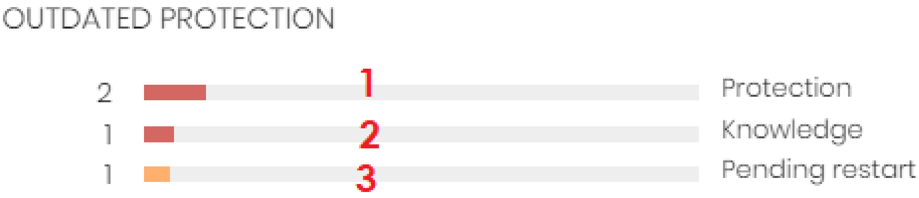


Figure 7.13: Hotspots in the outdated protection panel

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.
(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

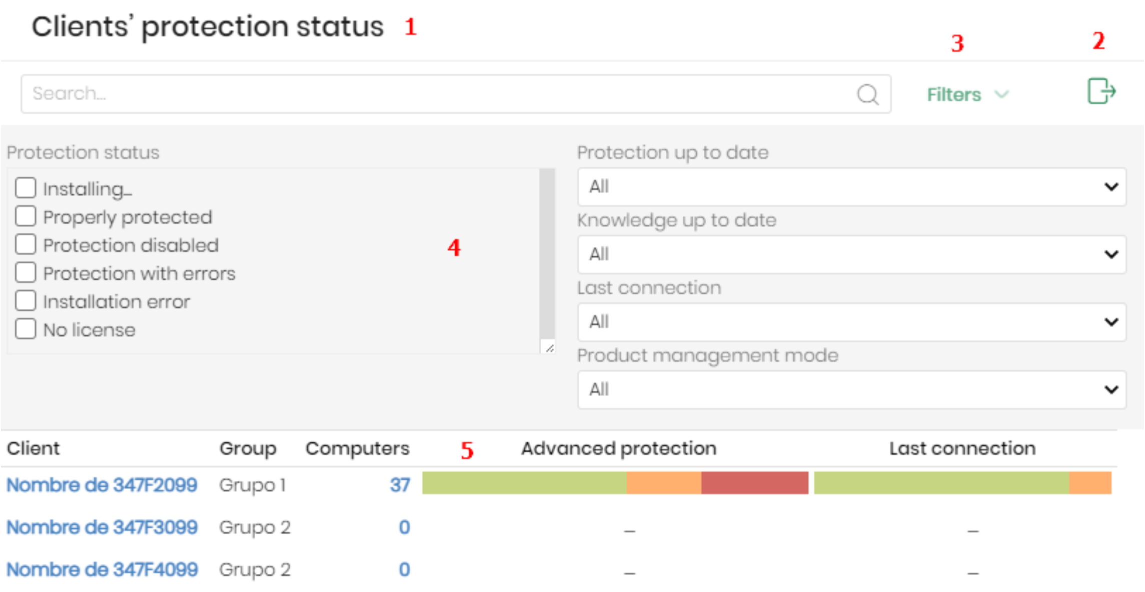
> *For more information about user accounts and permissions, see chapter* ***Access and authorization in Partner Center*** *on page* ***31****.*

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 Partner Center** on page **31**.

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 Partner Center user. See **Web console user permissions and visibility** on page **109**.

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 Partner Center console users with permissions higher than read-only.	Numeric value
Managed computers	The total number of computers and devices with Aether 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 Partner Center 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 Panda Security 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 Aether 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 Panda 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 Aether 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 Panda 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 Panda cloud in the specified time interval.	Numeric value
Last connection - More than 30 days ago	The number of computers that last connected to the Panda cloud in the specified time interval.	Numeric value

Table 7.12: Fields in the Protection Status exported file for clients with Aether 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 Panda Security 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 Panda Security 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 Aether 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 Panda 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 Aether 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 Aether 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 centrally managed clients that have the Panda Patch Management module. See **Service management models for endpoint security products** on page **65**.*

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 Panda Patch Management.	Character string

Field	Description	Values
Computers with required restart	The total number of computers and devices that must restart to complete installation or uninstallation of patches.	Numeric value
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 Panda Patch Management 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

Field	Description	Values
Computer	The computer name.	Character string
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-

Field	Description	Values
		related) - Unspecified (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 Panda Patch Management.	• All clients • Only clients with patch management
Date	The time period when the Panda Patch Management 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 the	• Other patches (non-

Field	Description	Values
	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 data for centrally managed clients only. See ***Service management models for endpoint security products*** *on page* ***65****.*

This list shows details of all patches that are available for each client that has the Panda Patch Management 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 Partner Center 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	Character string

Field	Comment	Values
	number, etc.).	
Release date	Date when the patch was released for download and application.	Date
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

Table 7.23: Fields in the Available Patches list

Filter tool

Field	Comment	Values
Search	Client name or folder in the Partner Center group tree.	Character string
Platform	Operating system installed on the computer.	• All • Windows • Linux • macOS

Field	Comment	Values
Patch release	Date when the patch was released and is available to download.	• All • Less than 7 days ago • Less than 14 days ago • 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

Field	Comment	Values
		- Test computer for patch installation - Patch installation disabled
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
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 Panda Patch Management cannot directly download because there are additional requirements set by the vendor (EULA acceptance, login credentials, CAPTCHA, etc.).	Boolean

Field	Comment	Values
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

Field	Comment	Values
		(security-related) - Low (security-related) - Unspecified (security-related) - Service Pack
CVEs (Common Vulnerabilities and Exposures)	CVE (Common Vulnerabilities and Exposures) ID that describes the vulnerability associated with the patch.	Character string
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 Partner Center console. For more information about user accounts and permissions, see chapter **Access and authorization in Partner Center** on page **31**.*

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	• **Gray**: Number of connections that meet the Unmanaged/Unavailable

Field	Description	Values
	information, see section **Security characteristics of connecting computers** 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 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.	condition. • **Blue**: Number of connections that meet the Managed by Another Account condition. • **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.

Field	Description	Values
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:	Numeric value

Field	Description	Values
	- 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).	
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 or equal to Critical. See chapter **Risk assessment** in the product administration guide.	Numeric value
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

Field	Description	Values
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**	• All • Unmanaged/Unavailable • Managed by another account • Protection not enabled

Field	Description	Values
	computers in chapter **Endpoint Access Enforcement** in the product administration guide.	• 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
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

Field	Description	Values
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 Partner Center 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 Partner Center 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
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 Partner Center 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
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
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

Field	Description	Values
		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 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 Partner Center console user can centrally define and send tasks to their clients' security products that are compatible with the Aether platform:

- Panda Adaptive Defense (for patch installation tasks only)
- Panda Adaptive Defense 360

- Panda Endpoint Protection
- Panda Endpoint Protection Plus

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 "Partner Center" and is assigned the **All** group so that it runs on all computers on the network. Tasks sent from Partner Center 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 Partner Center, 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**: Partner Center collects and consolidates the results generated by the clients' computers where the task was run.

Task types

Partner Center 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 Panda Patch Management 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

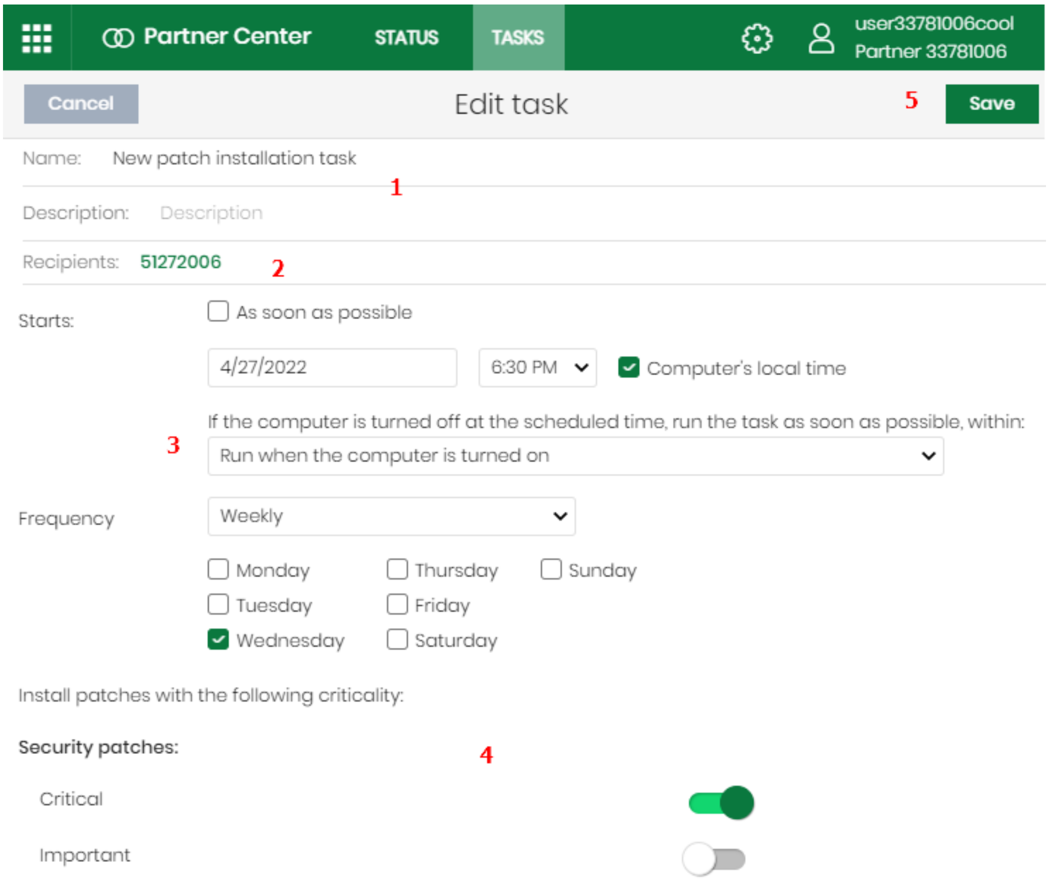
- You must have one of these permissions:
    - Total control
    - License and security administrator
    - Security administrator
- You must have permissions on the clients you want to assign to the task.

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: 51272006

Starts: □ As soon as possible

4/27/2022 6:30 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 **Panda Patch Management (Updating vulnerable programs)**, section Panda Patch Management **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 Partner Center server time.
If the computer is turned off	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 task expires immediately if the computer is not available) to infinite (the task is

Value	Description
	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: • Run the task on a specific day of each month. If you select the 29th, 30th, or

Value	Description
	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	• **The 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 suspicious files	Scheduled scans can scan computer software statically without the need to run the software. This reduces the likelihood that the scan detects some

Value	Description
	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 Panda Patch Management tasks (4)

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

> *For more information about how to edit the Panda Patch Management settings profile assigned to clients' computers to allow or deny patch installations, see chapter* ***Panda Patch Management (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 • Unspecified

Value	Description
	• 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 Panda Patch Management 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, Panda Patch Management 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 Panda Patch Management 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 Panda Patch Management 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. • **Automatically restart servers only**: This option behaves in the same way as

Value	Description
	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, Partner Center takes the following actions:

- The task is added to the Partner Center 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 Partner Center label. This label indicates that the task is read only.

Creating a Panda Patch Management quick task

Partner Center enables you to create installation tasks for individual patches for the Panda Patch Management 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. Partner Center deploys the tasks to the consoles of the selected clients for immediate execution.

Quick patch installation tasks create a single task in Partner Center 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. Partner Center 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 **141**.
- From the action bar, click **Schedule installation**. The task page opens and Partner Center 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, Partner Center 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.

Partner Center 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, Partner Center does not create a task to install that patch in the client's console.

- Click **Save**. Partner Center sends the task configuration changes to the affected clients' consoles.
- To delete the task, click **Cancel**. Because Partner Center 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 Partner Center. 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 Partner Center 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 Partner Center 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 Partner Center 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 **136**.*

Automatic adjustment of task recipients

If the Partner Center 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 Partner Center 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 Partner Center 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, Partner Center 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 Partner Center breaks: the task is no longer read only and the "Partner Center" label is removed.

Partner Center 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.

Partner Center deletes the results generated by the clients that left the group from the task.

Task synchronization and relationship between Partner Center and clients

As long as there is a relationship between Partner Center 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 Partner Center console and clients' consoles.

Interruption of the relationship between Partner Center and the client

For Partner Center 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 endpoint security products** on page **65**.
- 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 **94**.

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

The way Partner Center 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 Partner Center.
- In-progress tasks are kept in clients' consoles. However, the Partner Center 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 Partner Center.

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 Partner Center.
- Tasks sent by Partner Center before the relationship was interrupted and which were not modified or deleted by the client become read-only and show the Partner Center label.
- Tasks sent by Partner Center before the relationship was interrupted and whose recipients were modified by the client maintain those recipients and add the **All** group.
- Tasks sent by Partner Center before the relationship was interrupted and whose settings were modified by the client are resent, thus creating new tasks.

The Panda account

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

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

CHAPTER CONTENTS

Creating a Panda account for Panda Security partners

Follow the procedure described below to create a Panda account.

Receiving the email

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

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

- Find the message in your inbox.
- Click the activation button. By doing this, the address provided when creating your Panda 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 Panda 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 Panda Cloud account home page. From there, you will be able to access Partner Center's Web console. To do this, click the solution's icon you will find in the '**My Services** section.

Modifying Panda account

If your associated security provider is Panda Security, click the **Edit account** option in Panda Cloud.

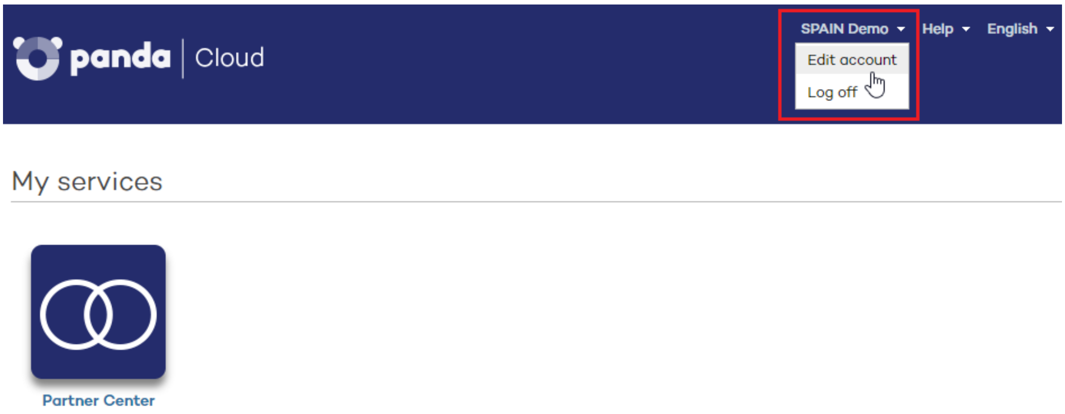


Figure 7.17: Editing the user account

Creating and linking a Panda account to WatchGuard

For more information on how to activate and link a Panda account when activating a commercial license, refer to ***https://www.pandasecurity.com/support/card?id=300001***

To manage Panda Security products from Partner Center, WatchGuard partners must meet the following requirements:

- They must have a WatchGuard partner account. For more information, refer to >**https://secure.watchguard.com/BecomeAPartner**.
- They must have a Partner Center account.
- They must link both accounts.

WatchGuard partners can create a Panda account in Partner Center in two ways:

- When assigning a trial license for a Panda Security product for the first time.
- When activating a commercial license for a Panda Security product for the first time.

Creating a Panda account when assigning a trial license for a Panda Security product

- Go to **https://www.watchguard.com** and enter your WatchGuard partner credentials.
- Click the **Support Center** link. In **My WatchGuard**, click **Manage Products**.
- Click the name of the Panda Security product that you want to activate a trial license for. Then, click the **Manage your Panda product** button.
- Click **I need a Panda account**. A page opens with the account name and ID. We recommend that you save this information. You need this information if you contact Support.
- Click **Submit** and **Continue**. The Panda Cloud page opens.
- To accept the End User License Agreement, click **Accept and continue**.
- Click Partner Center to access the management console.

Creating a Panda account when assigning a commercial license for a Panda Security product

- Go to **htps://watchguard.com/activate** and enter the license key for the Panda Security product.
- Click **I need a Panda account**. A page opens with the account name and ID. We recommend that you save this information. You need this information if you contact Support.
- Click **Submit** and **Continue**. The **WatchGuard Support Center** page opens.
- If prompted, enter the license key for the Panda Security product again. The **Activate product** wizard opens.
- Click **Next** to accept the End User License Agreement.
- From the **Select a license** drop-down menu, select **New license** and click **Next**.
- Type a name for your license that will help you easily identify the product on the WatchGuard website. Click **Next**.

- Select the **I accept the end user license agreement** checkbox and click **Next**. The **Activation Complete** page opens and your license is added to the relevant license pool in Partner Center.
- To access Partner Center, click **Manage Your Panda Product**. Click **Accept and continue** to accept the End User License Agreement.

Linking accounts when assigning a trial license

- Go to **https://www.watchguard.com** and enter your partner credentials.
- Click the **Support Center** link. In **My WatchGuard**, click **Manage Products**.
- Click the name of the Panda Security product that you want to activate a trial license for. Then, click the **Manage your Panda product** button.
- Click **Link my Panda account**. The Panda Cloud page opens. Enter your Partner Center login credentials.
- Click the **Log in** button. A page opens indicating that both accounts are linked.
- Click **Continue**. The Panda Cloud control panel appears.
- Click Partner Center to access the management console.

Linking accounts when assigning a commercial license

- Go to **htps://watchguard.com/activate** and enter the license key for the Panda Security product.
- Click **Link my Panda account**. A Panda login page opens.
- Type your Panda account user name and password. Click **Log in**. Your Panda account is linked to your WatchGuard account.
- Click **Continue**. The WatchGuard Support Center opens.

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 assignment of licenses

This mode of assignment means that clients themselves automatically take the licenses from the partner's pool as they are needed.

Automatic renewal of licenses

An automatic process implemented by Partner Center 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 Panda Security 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 Panda Security partner.

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 Panda Security‘s back-office in order to register clients and their licenses automatically. Both clients and their licenses will be visible in the Partner Center Web console.

L

License

Mechanism for controlling use and access to the products developed by Panda Security. 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.

License pool

Also called ‘stock of licenses’, this term refers to the repository where the product licenses purchased from Panda Security are temporarily stored, before being assigned to clients.

License recovery

A process aimed at returning to the pool of virtual licenses those licenses assigned to clients which have been canceled before the end of the contract date. This process is triggered automatically when a product assigned to a client is deleted or when a client’s product is replaced with a different one.

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.

Migration

The set of actions required to move a product from the Traditional platform to the Aether platform.

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 Partner Center 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

Panda Security

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.

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.Panda Security has two separate platforms: Aether 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 Partner Center 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 Panda Security, 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 Panda Security‘s portfolio and compatible with Partner Center, and therefore can be managed by partners or 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 Aether-based products allow for real-time communication with Panda Security's servers. This results in immediate deployment of the settings configured by the Partner Center 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 Panda Security 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 Panda Patch Management 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, Partner Center 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.

Virtual license

These are the licenses included in the pool of licenses and which haven't been assigned yet to any clients. The licenses assigned to clients can be recovered in some cases and returned to the pool of licenses if, for example, the client cancels the service before the end of the contract period due to a change of product.

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 Partner Center to regulate technicians' access to the Web console and establish the actions they can take on the computers on the network.