Panda Systems Management

# Panda Systems Management Administration guide

**Version**: 9.02.00-00

**Author**: Panda Security

**Date**: 04/11/2021

panda

pandasecurity.com

## Legal notice.

## Registered trademarks.

## Contact information.

Corporate Headquarters:
Panda Security
Calle Santiago de Compostela 12
Bilbao (Bizkaia) 48003 España.
**https://www.pandasecurity.com/spain/about/contact/**

## About the Administration guide

- You can find the most recent version of this guide at:

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

## Release notes

To find out what's new in the latest version of Panda Systems Management following URL:

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

## Technical Support

Panda Security provides global support services aimed at responding to specific questions regarding the operation of the company's products. The technical support team also generates documentation covering technical aspects of our products. This documentation is available in the eKnowledge Base portal.

- To access specific information about the product, please go to the following URL:

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

- The eKnowledge Base portal can be accessed from the following link:

**https://www.pandasecurity.com/uk/support/#enterprise**

## Survey on the Administration Guide

Rate this guide and send us suggestions and requests for future versions of our documentation:

**https://www.pandasecurity.com/uk/support/#enterprise**

# Contents

## Part 1: Introduction to Panda Systems Management

## Part 2: Device installation and organization

## Part 3: Automatic process configuration on devices

## Part 4: Device visibility

## Part 5: Resolution of incidents and technical support

## Part 6: Panda Systems Management service security

## Part 7: Appendix

Part 1

# Introduction to Panda Systems Management

**Chapter 1:** Preface

**Chapter 2:** Basic information about Panda Systems Management

**Chapter 3:** Basic components of the Console

**Chapter 4:** Getting started with Panda Systems Management

Chapter 1

# Preface

This guide contains basic information and procedures of use to get maximum benefit from the product Panda Systems Management.

CHAPTER CONTENT

## Target audience

The purpose of this guide is to provide technical information about the product to the technical staff in charge of offering support services to network users at:

- The IT Department which wishes to professionalize the internal support it provides to the rest of the company.
- The Managed Service Provider (MSP) which provides technical support services to its customer accounts onsite or remotely, reactively or proactively.

## Icons

This guide contains the following icons;

| | |
|---|---|
| ⓘ | Additional information, for example, an alternative method for performing a particular task. |
| 💡 | Suggestions and recommendations. |
| ⚠ | Important and/or useful tips for using Panda Systems Management. |

🔍 Additional information available in other chapters or sections of the guide.

Chapter 2

# Basic information about Panda Systems Management

Panda Systems Management is a cloud-based remote device monitoring and management solution for IT departments that want to offer a professional service while minimizing user disruption.

Panda Systems Management increases efficiency through centralized and straightforward management of devices, while promoting task automation. The overhead costs dedicated to serving each user are reduced as Panda Systems Management:

- Is hosted in the cloud. Hence, it requires no additional infrastructure on the part of the company or department providing the service, or on the managed network.
- Has a very gentle learning curve for technical support, allowing you to deliver value from day one.
- Tools accessible from anywhere, anytime, allowing you to manage support remotely and avoiding wasted time and money by eliminating the need to travel to those sites.
- Task and response automation triggered by configurable alerts that prevent failures before they occur.

Panda Systems Management is a product that promotes collaboration among the technicians in charge of providing support, and minimizes or completely eliminates the time spent interacting with the user to determine the cause of problems.

CHAPTER CONTENT

# Main features of Panda Systems Management

The following are the most important features of the product:

| Feature | Description |
|---|---|
| **Cloud-based solution** | No additional infrastructure at the customer or the MSP/IT Department site. Manage all your devices anytime, anywhere. |
| **Agent-based management for compatible devices** | Extremely light Agent for compatible devices with Windows, Linux, Mac OS X, Android and iOS. |
| **Agentless management** | Simple management using the SNMP protocol and configuration templates for those devices where it is not possible to install the Agent, such as printers, routers, switches, scanners, switchboards, etc..<br>Management of VMware ESXi servers (VMware vSphere Hypervisor 4.1, 5.0, 5.5, 6.0 and 6.5) and Microsoft Hyper-V servers on Window Server. |
| **Automatic detection of devices** | An Agent installed on a single device can detect other devices connected to the same network and start an unattended installation. |
| **Scheduled and custom audits** | Track all changes to the device (hardware, software and system). |
| **Software license management** | Keep track of all software licenses installed. |
| **Computer security monitoring** | Shows the status of the antivirus protection installed on each device. |
| **Alerts and monitoring** | CPU, memory and disk utilization monitors, queues, performance graphs, dashboard alerts, etc., for any device and in real time. Recommended quick-start monitors. |
| **Monitoring common applications** | Monitor common applications such as Exchange, SQL and IIS, backup services, network devices, etc., with monitors that are free from the product's ComStore. |
| **Script and quick job creation** | Create your own scripts, download our pre-configured scripts from the online ComStore, and deploy either on a scheduled basis or as an automatic response to an alert. All at a click. |
| **Patch management** | Automated deployment of updates and patches for the Windows systems on the network. |
| **Software deployment** | Centralized software deployment to Windows, Linux, macOS and iOS computers. |
| **Software Management** | Make sure your managed devices comply with the software installation policies set by your company and update your programs to the latest versions published by software vendors. |
| **Policies** | Define a set of common configurations to manage your IT environment faster and more effectively. |

Table 2.1: Panda Systems Management feature list

| Feature | Description |
|---|---|
| **Remote access** | Task manager, file transfer, registry editor, command prompt, event log viewer, etc. All of these integrated tools enable you to troubleshoot issues without impacting users.<br>Panda Systems Management supports the PowerShell command interpreter, enabling you to troubleshoot and configure your Windows devices in an advanced way. The administrator will be able to connect to a full PowerShell interface on remote devices, from anywhere. The agent is designed to work with PowerShell 2.0 and later versions. |
| **Remote control** | Shared access to the user's desktop or full control through the PCSM agent or directly from the web management console. Supports firewalls and NAT. |
| **Remote management of network devices** | Access management tools for the network computers, printers and other devices that don't support installation of the PCSM Agent. This feature allows administrators to manage all network devices from their computer. |
| **Secure communications** | All communications between the Agents and the Systems Management Server are encrypted (SSL). |
| **Service access control** | Ensuring secure access to the Console by the service administrator with two-factor authentication and with other resources that restrict access from devices to the Systems Management Server. |
| **Reports** | Flexible reporting system in PDF and CSV formats. Multi-language support. Ability to extend the scope of reports to the entire IT network by using aggregate reports. |
| **Collaborative environment** | Manage incident allocation, status and documentation with the ticket system. Simplify creation of an intervention history with device notes. Communicate live with the end user through the IM messaging service. |
| **Activity log** | History of all administrators' activities in the Console. |
| **ComStore** | Complements and extends the capabilities of the platform, allowing administrators to select and download the components they need at any time. All components are provided free of charge. |
| **Mobile Device Management (MDM)** | Supports iOS and Android, allowing monitoring and management of smartphones and tablets, configuring settings and user policies, geolocation of devices, and safeguarding of data should the device be stolen or lost. |

Table 2.1: Panda Systems Management feature list

# Panda Systems Management user profile

Panda Systems Management is designed for two groups of IT professionals with a medium-to-high level of technical knowledge:

- **In-house IT technicians**

Subcontracted or in-house technicians offering company-wide support service for devices and end-users. This scenario often includes remote offices to which access is restricted so technicians must use monitoring and remote access tools, and roaming users or users who work outside the office, which makes them vulnerable to all types of problems with their devices.

- **Managed Service Provider (MSP) technicians**

Technical staff employed by a company to provide a professional service to customer accounts that have decided to outsource or subcontract the IT Department for maintenance of their devices.

# Main components of Panda Systems Management

- **Panda Systems Management console**

A Web portal accessible via compatible browsers, from anywhere, anytime with any Web enabled device.

Most of the daily tracking and monitoring tasks will be performed from this console via a browser.

This resource is available to technical support only.

- **PCSM agent**

This is a small program (less than 10 MB in its Windows version) installed on all supported devices to be managed. After installing the Agent on the device, its information will become directly accessible through the Console.

> *For devices, such as printers, switches or ESXi servers, on which it is impossible to install an Agent, Panda Systems Management can collect status information and display it in the console using the SNMP protocol. For more information, see Chapter 5: Devices, section Management of devices not supported by the Agent. For more information refer to section "**Integrating network devices**" on page 55.*

The Agent supports two execution modes:

- User Mode or Monitor Mode: In this mode, which is the usual mode, the Agent is barely noticeable to the end-user and access to some specific settings can be delegated to the user by the administrator.
- Administration Mode: After entering valid credentials, the network administrator can use the Agent to access remote devices on the network.

> *Install the Agent on all devices you want to manage and also on those used by technicians to manage the hardware and software assets in your IT infrastructure.*

- **Panda Systems Management server**

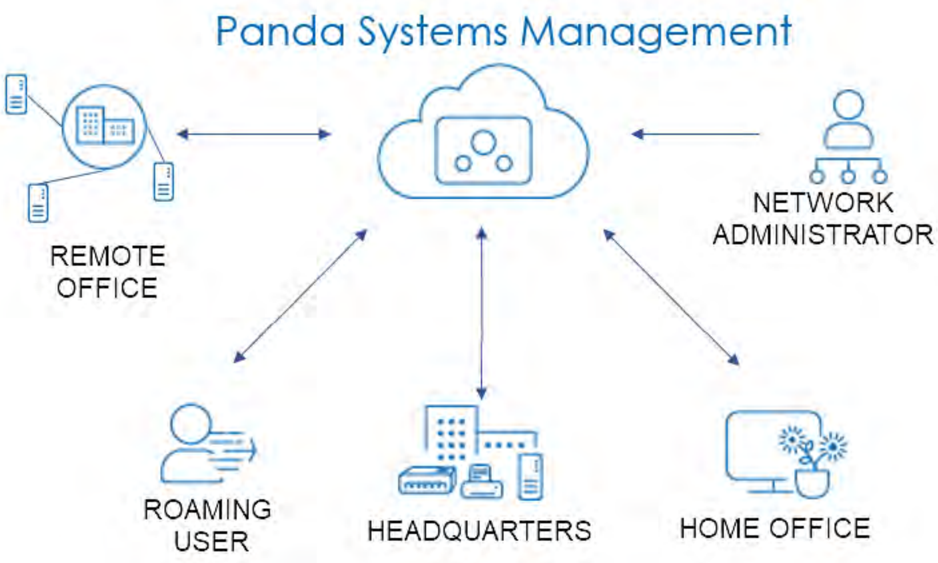


Figure 2.1: Panda Systems Management basic operation diagram

The console, the processes required to collect, synchronize and redirect the messages, events, and information flows generated by the agents, and the databases that store them are all hosted on a cloud-based server farm available 24 hours a day, 365 days a year.

The status information that flows from each of the devices to the Server is highly optimized so that the impact on the customer's network and the latency are negligible. This information is sorted and consolidated in the Server so that it is displayed as a flow of events to diagnose and even efficiently foresee problems on managed devices.

# Key players of Panda Systems Management

- **IT Administrator / Administrator / Managed Service Provider / MSP / IT Department / Support Technician / Technical Team**

These terms include all those who have access to the Console, regardless of the privilege level associated with the credentials supplied.

These are the technical staff from the IT department of the company that opts for Panda Systems Management to manage and monitor its systems, or the MSP staff who access the customer's devices to manage and monitor them.

- **Panda Systems Management administration account / Main administration account**

Each customer or company using Panda Systems Management will be given a Main admin account. An Account with the highest level of privileges that can manage all the resources of the product.

> *Refer to "**User accounts and security levels**" on page **275** to know how to create new users and security levels in order to restrict the access of system technicians to key Panda Systems Management resources.*

Each Main administration account belongs to a secure and separate product instance. Therefore, all of the settings of a Panda Systems Management customer and all of the devices managed will not be accessible or visible to other administration accounts.

- **Customer account / Customer**

A customer account is a contract between the Managed Service Provider and a company that comes to them with the intention of outsourcing their day to day IT Support needs.

Except in Chapter 16: User account and security levels, in this manual, account has an organizational meaning: for the MSP, it is equivalent to a set of devices related to one another for belonging to the same customer network that will require maintenance.

- **User**

The person who uses one or more devices and requires direct support from the MSP or IT department. In this guide, the user of the management console is referred to as "administrator" in order to differentiate them from the user of the managed device.

- **Device**

A device is a computer that has the role of either client or server, which has an Agent installed or is managed indirectly via SNMP.

Chapter 3

# Basic components of the Console

The management Console is structured in an intuitive and visual manner, so that most management resources are just a click away, enabling easier and faster navigation.

The goal is a Console which is clean, quick and convenient to use, while avoiding, wherever possible, full page reloads and offering a gentle and short learning curve for the IT Department. This way, both MSPs and administrators will be able to deliver value to their customers from the outset.

The management console is divided into the following components:

- General menu.
- Tab bar.
- Icon bar and context menus.
- Dashboards.
- Groupings panel.
- Selection controls.
- Lists.
- Sections.

CHAPTER CONTENT

# Management console components

## General menu

The menu at the top of the window. It is accessible from anywhere in the console and allows the administrator to access all of the features provided by Panda Systems Management It is divided into the following eight areas.

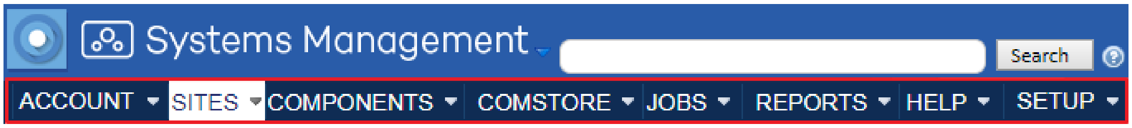


Figure 3.1: general menu

When you mouse over each of the areas of the general menu, a drop-down window will be displayed that allows you to quickly access the tabs that divide the functionality of each area, shown in the following point.

| Menu | Description |
|---|---|
| **Account** | Access to Account Level. For more information about the different levels implemented in Panda Systems Management, refer to section "**Hierarchy of levels within the Management Console**". |

Table 3.1: general menu items

| Menu | Description |
|---|---|
| **Sites** | Access to components downloaded by and accessible to the administrator. "**Hierarchy of levels within the Management Console**". |
| **Components** | For more information, refer to chapter "Components and ComStore" on page "**Components and ComStore**" on page **131**. |
| **ComStore** | Repository of components created by Panda Security that extend the capabilities of Panda Systems Management. For more information, refer to chapter "**Components and ComStore**" on page **131**. |
| **Scheduled Jobs** | List of active and finished jobs. For more information, refer to chapter "**Jobs**" on page **123**. |
| **Scheduled Reports** | List of configured and default reports. For more information, refer to chapter "**Reports**" on page **187**. |
| **Help Center** | Help center with links to Panda Security resources. |
| **Setup** | Access to the details of the Main administration account and to resources for creating new security levels and users. For more information, see Chapter "**User accounts and security levels**" on page **275**. |

Table 3.1: general menu items

## Tab bar

The tab bar provides access to the tools available in the console for generating and presenting consolidated lists on-screen. It also allows configurations to be defined and viewed.

The options displayed on the tab bar will vary depending on the area selected from the general menu.

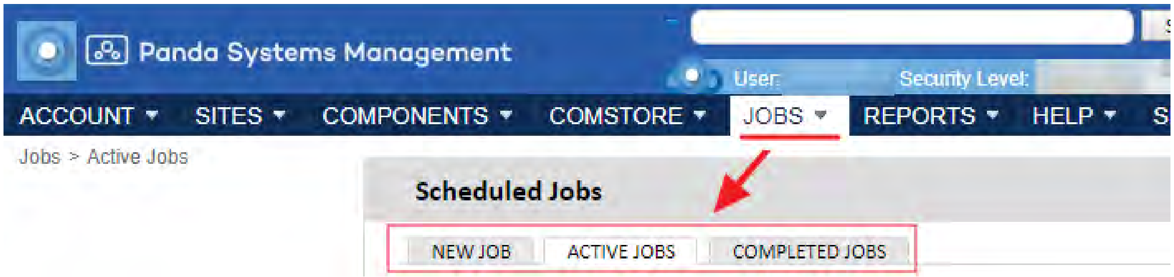


Figure 3.2: tab bar for general menu Jobs

## Icon bar

The icon bar allows the administrator to access actions for changing the status of the items selected from the associated list of devices. Both the look of the icon bar and the options presented will vary depending on where in the management console it is accessed from and the items it affects.

### Icon bar affecting multiple items

Use the checkboxes **(1)** to select the items that will receive the action. Then, click the relevant icon **(2)** under the tab bar.

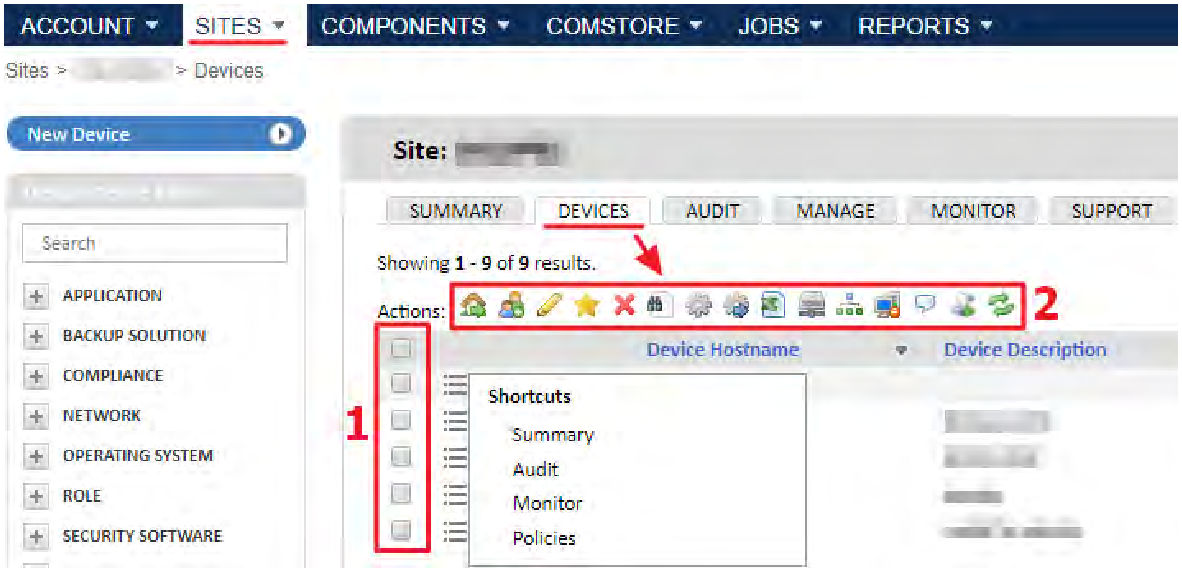
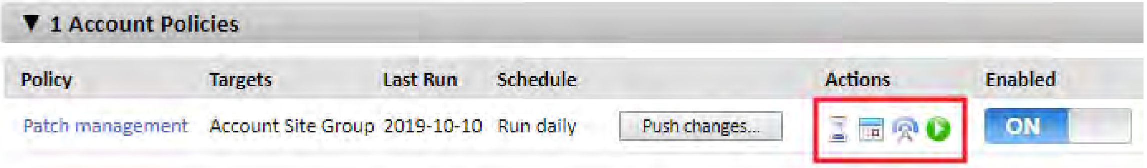


Figure 3.3: icon bar for general menu Sites, tab menu Devices

### Icon bar affecting one item

The position and shape of the icon bar can vary based on the item that will receive the action. Thus, the icon bar may appear as a context menu or a standard icon bar.



| Policy | Targets | Last Run | Schedule | | Actions | Enabled |
|---|---|---|---|---|---|---|
| Patch management | Account Site Group | 2019-10-10 | Run daily | Push changes... | | ON |

Figure 3.4: icon bar in the shape of a standard icon bar associated with an item

## Drop-down menu

Some lists in the console display a drop-down menu icon ☰ next to their checkboxes. This icon provides access to different features and tools based on the screen where it is located:

- In the list of **Sites** of an account, it displays the items on the tab bar..
- Within a **Site**, when located in a device's row, it shows the device's tab bar (1). Additionally, if the

device is online, it displays the available remote tools (2).

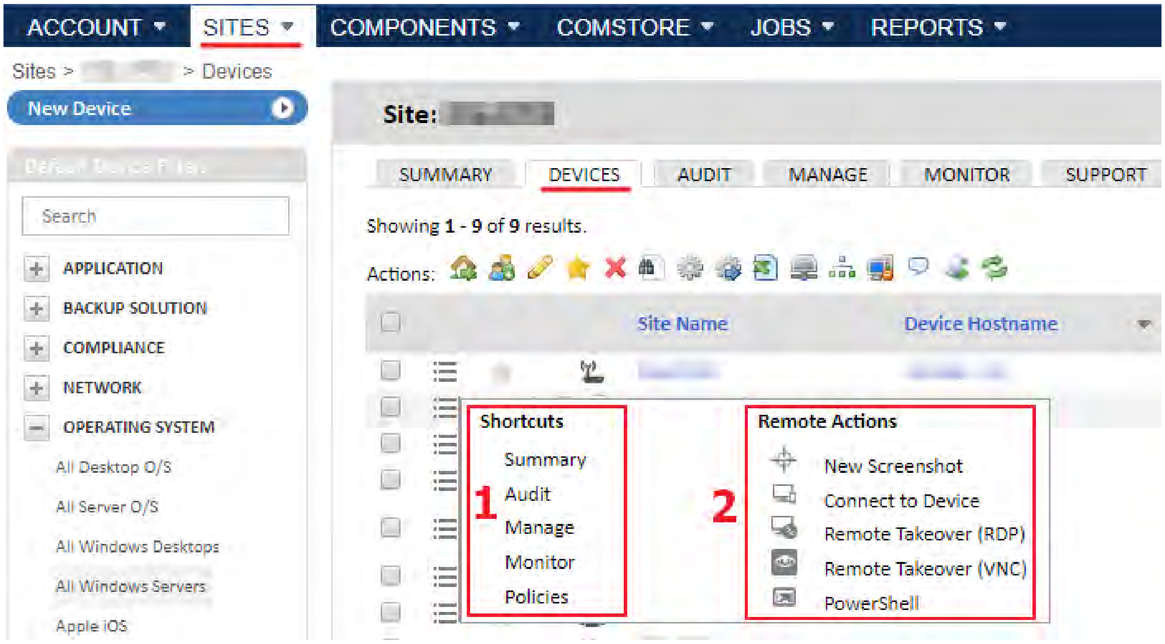


Figure 3.5: icon bar in the shape of a context menu

## Filters and groups panel

*Refer to section “**Device groupings**” on page **69** to get a description of the different device groupings available in Panda Systems Management.*

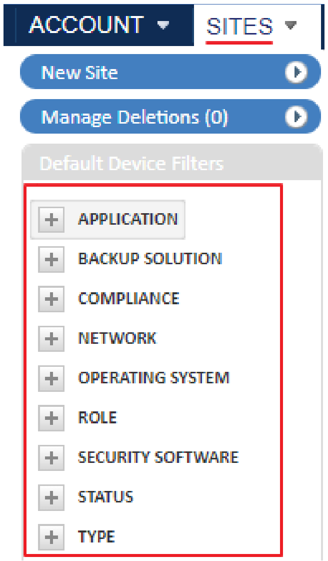


Figure 3.6: side panel with the grouping and filtering tools

The left side of the console displays various panels with different types of groupings available in Panda Systems Management. These grouping will vary depending on the area selected from the general menu, and the tab selected from the tab bar.

# Dashboards

The dashboards reflect the status of a set of devices with different levels of detail. There are three types of dashboards:

- Account level dashboard.
- Site level summary dashboard.
- Device level summary dashboard.

*Refer to chapter "**Device visibility and status**" on page **167** for more information about the information displayed on each dashboard. Refer to section "**Hierarchy of levels within the Management Console**" in this chapter for more information about the levels available in the management console.*

## Account level dashboard

From general menu Account, click Dashboard from the tab bar.

This dashboard gives an overview of the status of the network devices: notifications, jobs, alerts, etc.

## Site level summary dashboard

From general menu Sites, click a site and then Summary from the the tab bar. This dashboard provides information about the status of all devices in the site. Each site has its own summary dashboard.

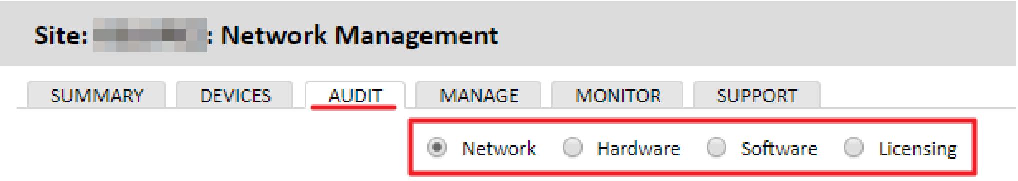
## Device level summary dashboard

Reflects the status of a specific device and is accessible from each device integrated into Panda Systems Management. Follow the steps below to access the device level summary dashboard:

- From general menu Sites, click the site that the device whose details you want to view belongs to.
- Click Devices from the tab menu. Select the relevant device and click the Summary tab.

# Selection controls

A single window can contain multiple settings screens accessible via selection controls located in the top right corner of the window.



● Network ○ Hardware ○ Software ○ Licensing

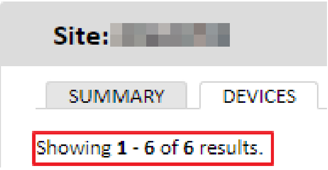
Figure 3.7: selection controls on the Audit tab.

# Lists

Panda Systems Management provides lists of items such as jobs, devices, or configurations, along with standard controls for sorting or configuring them based on the administrator's needs. These controls are:

- Items counter.
- Column settings.
- Items per page settings.
- Pager.
- Filter and search settings.

## Items counter

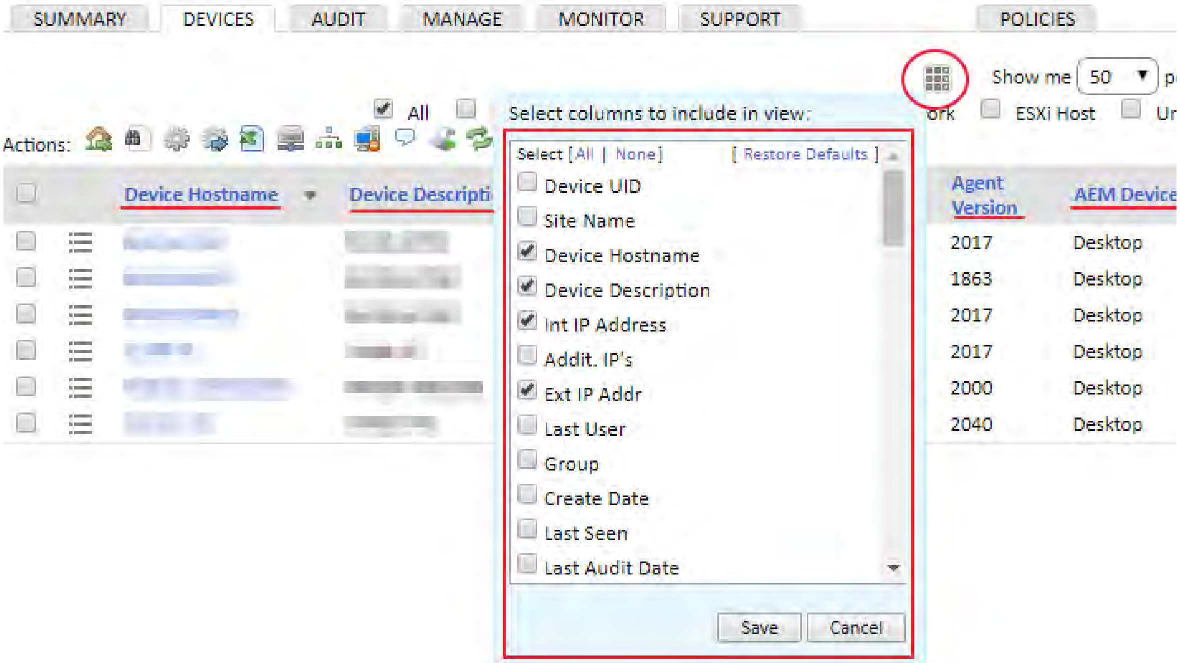


Showing **1 - 6 of 6** results.

Figure 3.8: item counter shown

Located in the top left corner of the screen, under the tab menu. It shows the number of items displayed out of the total number of available items available items.

## Column settings



Select columns to include in view:

Select [All | None] [ Restore Defaults ]

- □ Device UID
- □ Site Name
- ☑ Device Hostname
- ☑ Device Description
- ☑ Int IP Address
- □ Addit. IP's
- ☑ Ext IP Addr
- □ Last User
- □ Group
- □ Create Date
- □ Last Seen
- □ Last Audit Date

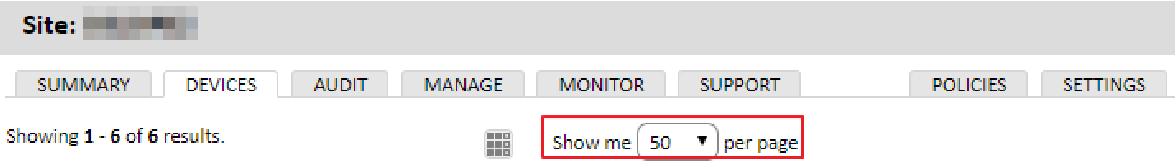
| Agent Version | AEM Device |
|---|---|
| 2017 | Desktop |
| 1863 | Desktop |
| 2017 | Desktop |
| 2017 | Desktop |
| 2000 | Desktop |
| 2040 | Desktop |

Figure 3.9: Column settings in device listings

Click the ▦ icon in the top-right corner of the screen to display a window with all available columns for the list. This window allows to customize the list view to their specific needs.

## Items per page settings

Located in the top left or top right corner of the screen, these controls allow administrators to select the number of items to be displayed per page (10, 25, 50 or 100 items).



Showing **1** - **6** of **6** results.

Show me 50 per page

Figure 3.10: Pagination element

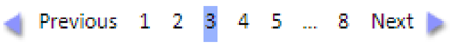


Figure 3.11: Pagination control

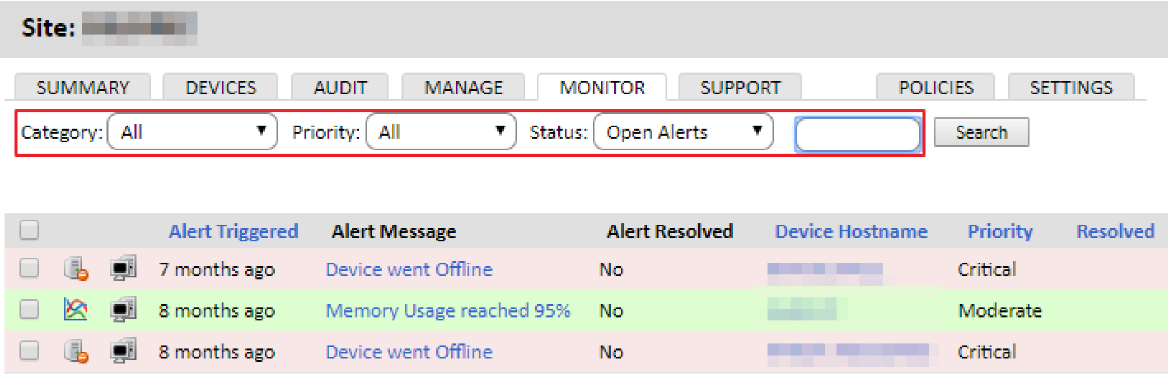
## Pager

Located at the bottom of the screen. these controls indicate the current page, and allow you to move to the next or previous page by using the arrow icons and, or jump directly to a page number ▶ and ◀.

## Filter and search settings

Some particularly long lists provide controls to filter results quickly:

- Drop-down menus: let you select one item from a drop-down list.
- Free search boxes: let you perform free text searches.
- Checkboxes: let you select different search options simultaneously.



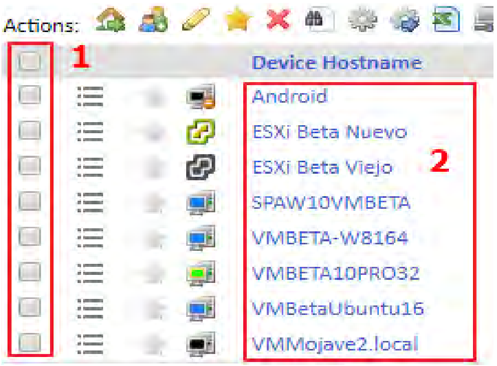
Category: All Priority: All Status: Open Alerts

| □ | | | Alert Triggered | Alert Message | Alert Resolved | Device Hostname | Priority | Resolved |
|---|---|---|---|---|---|---|---|---|
| □ | | | 7 months ago | Device went Offline | No | [redacted] | Critical | |
| □ | | | 8 months ago | Memory Usage reached 95% | No | [redacted] | Moderate | |
| □ | | | 8 months ago | Device went Offline | No | [redacted] | Critical | |

Figure 3.12: Filters and searches in listings

## Checkboxes

Let you select multiple items from a list in order to act on all of them simultaneously via the icon bar. Refer to figure 3.13 **(1)**.



Actions:

| 1 | Device Hostname |
|---|---|
| □ | Android |
| □ | ESXi Beta Nuevo |
| □ | ESXi Beta Viejo |
| □ | SPAW10VMBETA |
| □ | VMBETA-W8164 |
| □ | VMBETA10PRO32 |
| □ | VMBetaUbuntu16 |
| □ | VMMojave2.local |

Figure 3.13: Checkboxes (1) and links (2))

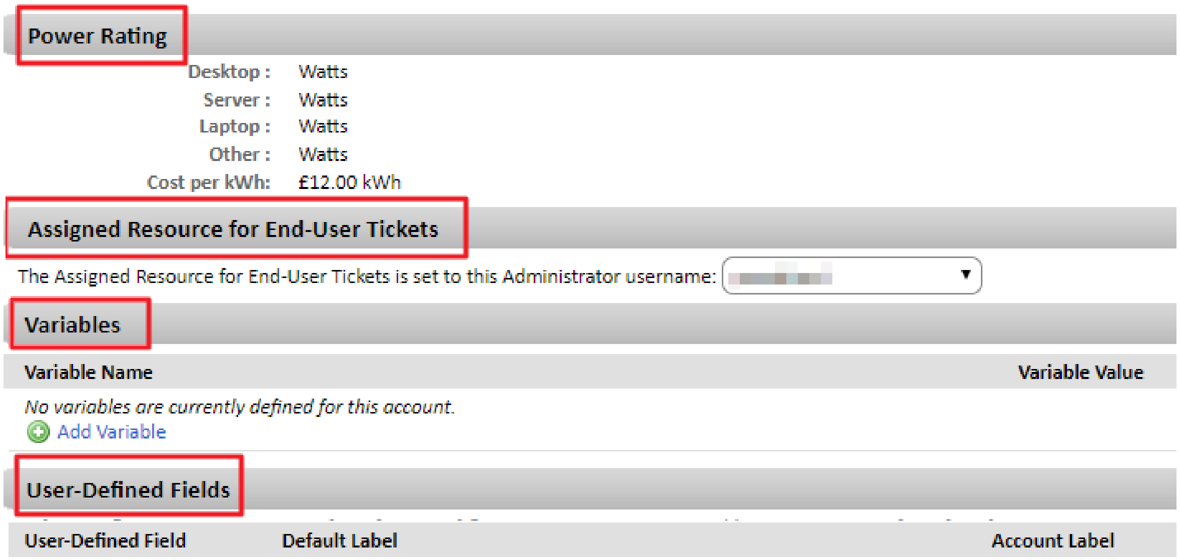
## Links

Many of the items displayed on lists have a link associated (2) that allows you to move to a different level for further details (refer to section "**Hierarchy of levels within the Management Console**" for more information about levels and how they are used in the Panda Systems Management console). That is, while lists contain summary information about items, clicking a specific item will let you access more specific information about the item in question.

*Lists support two types of actions: selecting one or more items to act on them via the icon bar, and moving to a different level in the console by clicking an item's associated link. In this guide, when referring to the first type of action we use the verb "to select" (as in "select one or more devices from the list"), while the second type of action is denoted with the verb "to click" (as in "click the device") to move from one level to another.*

# Sections

Throughout the entire Panda Systems Management interface, and especially on settings screens (general menu **Setup** and tab **Settings**), the information is divided into sections that group all related features together.



**Power Rating**

Desktop : Watts
Server : Watts
Laptop : Watts
Other : Watts
Cost per kWh: £12.00 kWh

**Assigned Resource for End-User Tickets**

The Assigned Resource for End-User Tickets is set to this Administrator username: [redacted] ▾

**Variables**

| Variable Name | Variable Value |
|---|---|

*No variables are currently defined for this account.*
Add Variable

**User-Defined Fields**

| User-Defined Field | Default Label | Account Label |
|---|---|---|

Figure 3.14: settings divided into sections

# Hierarchy of levels within the Management Console

Panda Systems Management divides the management console into three entities/levels in order to simplify use and facilitate reusing the procedures defined by technical staff in the console. From the most general to the most specific, these levels are the following:

- Account level.
- Site level.
- Device level.

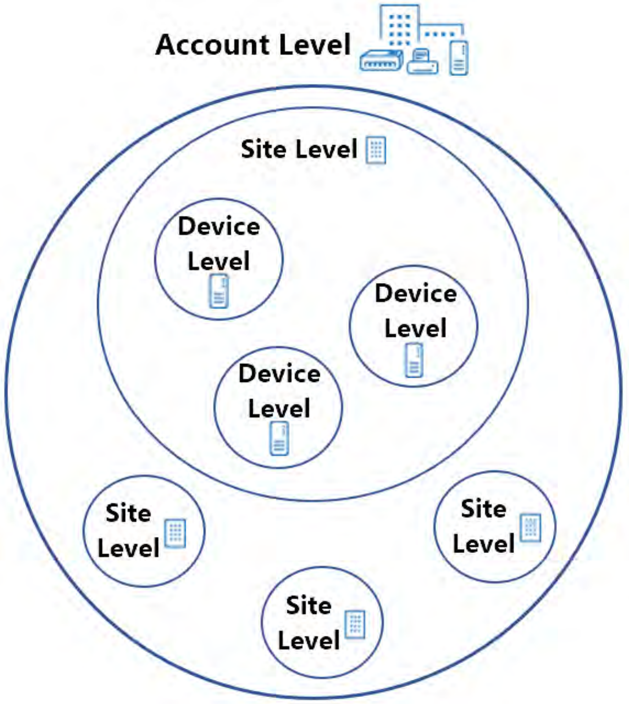


Figure 3.15: level hierarchy

## Account Level

### What is it?

Account Level is the most general and highest entity cluster available, and is also unique for each MSP/IT Department. It automatically groups all devices managed by the MSP/IT Department belonging to their customers and users with an Agent installed and integrated in Panda Systems Management.

### Scope

The actions performed on this level will affect all devices registered on the account, although they can be limited to a subset of devices using filters and groups, described in chapter "**Device groupings**" on page **69**.

### Access

The Account level resources are accessed from general menu **Account** and general menu **Sites**.

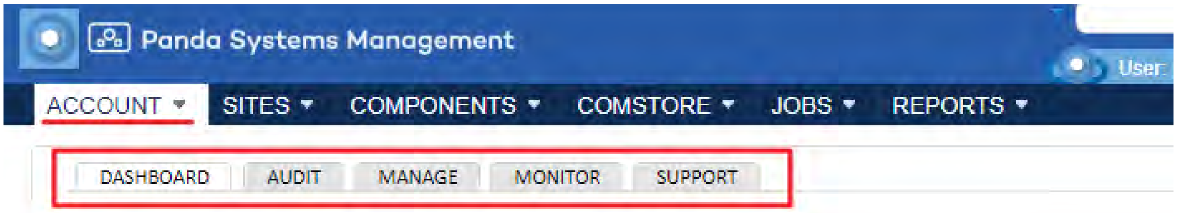


Figure 3.16: Account Level Resources accessible from the general menu

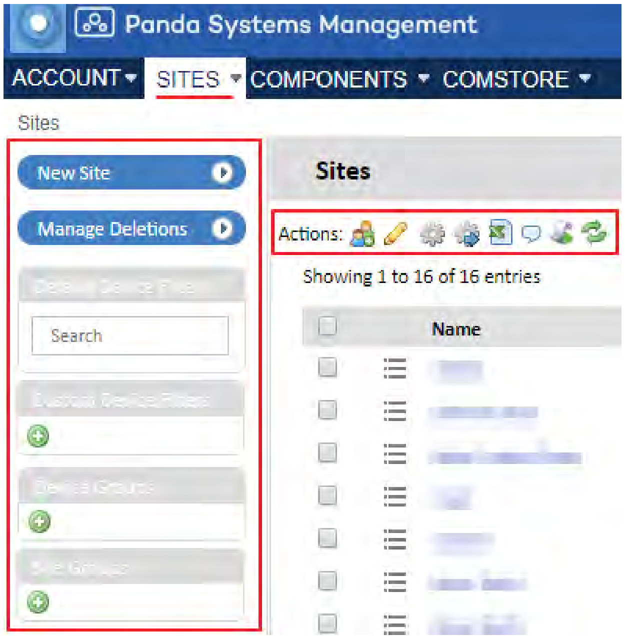


Figure 3.17: Account level resources accessible from the general menu Sites

### Functionality

Account Level can perform global actions. Therefore, you can obtain the status of all managed devices, consolidated reports on your environment, and actions on all or part of the registered devices.

### Settings

The Account Level settings include a wide range of parameters that are dealt with in several chapters throughout this guide.

Below you will find a complete list of all the options in the general menu **Setup**, **Account Settings** and a short description of each one.

## Site Level

### What is it?

Site Level is a grouping entity immediately below Account level. It is a logical grouping that contains the devices that belong to the same branch office/office/network. This way, a company with many branch offices or individual networks will generally establish a site for each of them. Each of these sites will group devices with specific connectivity settings.

The sites list can be accessed from the general menu **Sites**.

Each site includes the Internet connection settings of the devices that comprise it. To view these settings, go to general menu **Sites**, click the relevant site and click **Settings** from the tab bar. These settings are added to the Systems Management Agent that the device user will install on their computer, and are applied automatically without any administrator intervention.

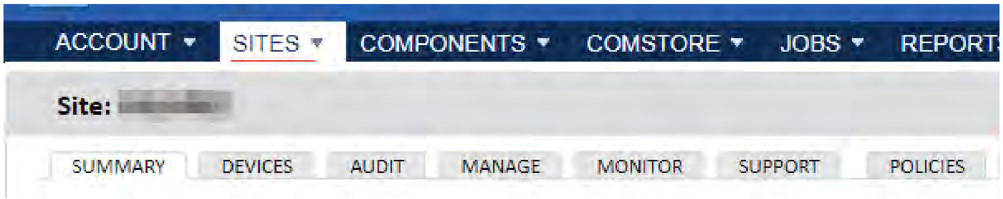


Figure 3.18: accessing general menu Sites. Settings

## Scope

The procedures triggered at Site Level can affect all devices belonging to that site, while some actions can be restricted to a subset of devices using filters and groups, described in chapter "**Device groupings**" on page **69**.

Unlike Account Level, which is unique, the administrator can create as many site groups as needed.

## Membership

Membership of a given device to a site is determined when installing the PCSM agent, even though it is possible to move a device from one site to another through the console once the agent has been installed on the user's device. Refer to section "**Moving computers from one site to another**" on page **71**.

⚠ *Download the Agent directly from the chosen site page so that when installed on the user's device, it will be automatically added to the site in question in the Console. For further details, see "**Deploying and managing devices**" on page **43**.*

ⓘ *To minimize the number of tasks in the deployment phase it is advisable to first create the site in the management Console and then download the Agent from the created site. This way, membership of managed devices to the site will be automatic.*

## Functionality

Site Level can perform actions on all of the devices it contains. This way, you can obtain lists with the status of devices, consolidated reports, and tasks to perform on all or some of the devices which make up the site.

## Settings

The Site Level settings also include a wide range of parameters that are described in several chapters in this guide, some of these coincide with some of the parameters defined at Account Level, in which case the latter shall have priority.

To access a site's settings, go to general menu **Sites**, click the site and then click the **Settings** tab.

# Device Level

## What is it?

This is the logical representation of a single managed device in the management Console. Device Levels are automatically created in the Console, as one is added for each customer device with an Agent installed or managed indirectly through SNMP.

## Scope

All actions performed at this level affect only the selected device.

## Functionality

Device Level can perform actions on a particular device. This way you can get detailed lists from the device as well as reports and actions.

Chapter 4

# Getting started with Panda Systems Management

This chapter shows, via examples, the typical tasks that administrators must perform to deploy the agent across all systems on the network, integrate devices into the Panda Systems Management console and manage them. Additionally, it provides a basic description of many resources necessary to make the most of Panda Systems Management. Further details about those resources are provided in later chapters of the guide. We recommend that you follow the instructions provided step by step in order to become familiar with the product.

In short, we'll cover the following tasks necessary to integrate a Windows computer into Panda Systems Management and manage it

- Creating and configuring the first site.
- Manually installing the Panda Systems Management agent on a Windows device.
- Finding devices quickly using filters.
- Viewing devices.
- Performing hardware, software and license audits
- Monitoring devices.
- Managing patches and updates.
- Deploying software.
- Resolving incidents remotely.

The description of each of these tasks includes a link to the chapter that presents that aspect of Panda Systems Management in more details.

CHAPTER CONTENT

# Creating and configuring the first site

*Refer to chapter "**Device groupings**" on page 69 for more information about the different types of groupings supported by Panda Systems Management.*

Sites are a basic type of grouping that allows administrators to separate the devices integrated into Panda Systems Management for better and more efficient management.

From a management perspective, sites allow devices to be organized in the Panda Systems Management console while, from a technical perspective, a site contains the Internet connectivity settings of all devices it comprises. As a general rule, if two devices have the same proxy settings for accessing external resources, it won't be necessary to create two different sites. However, if they have different proxy settings, it is recommended to create different sites, each with its own connectivity settings.

## Creating a site and configuring its Internet connection settings

- In general menu **Sites**, click **New site** from the left-side panel.
- Enter a **Name** and **Description**.
- If the devices to be integrated into the site have direct Internet access, select **Proxy type None**. If they access the Internet through a proxy, select the relevant type of proxy and enter the proxy details.

- Click **Save**.

*All devices that are integrated into the created site will automatically inherit the Internet connection settings defined.*

### Changing a site's Internet connection settings

- From general menu **Sites**, click the site whose settings you want to edit.
- Click **Settings** from the tab menu.
- In the Proxy section, click the Edit link on the right-hand side of the window and enter the proxy details.

*The proxy settings of a computer with the PCSM agent installed won't change when updating the proxy settings of the site to which the computer belongs. To change them, it will be necessary to download the PCSM agent again or manually edit the settings of the agent installed on the computer. For more information, refer to section "***Connection information***" on page* **45**.

## Manually installing the agent on a Windows computer

*Refer to chapter "***Deploying and managing devices***" on page* **43** *for more information about the various deployment methods implemented in Panda Systems Management and the requirements that target devices must meet.*

The agent to be installed on a customer's device requires certain basic information in order to operate:

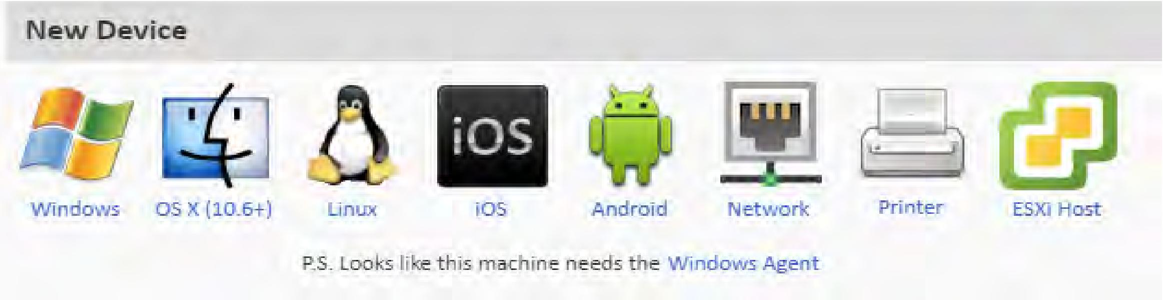
- The site in the management console to which it will belong.
- The minimum information required to access the Internet from the device and connect to the Panda Systems Management server.

When generating the installation package from the site, Panda Systems Management automatically incorporates the aforementioned information into the installer, freeing the administrator from having to configure any settings on the end user's computer.

### Download the PCSM agent for Windows systems

- In general menu **Sites**, click the newly created site.
- Click **New device** from the left-side panel. A pop-up window will appear with all supported

platforms. Select Windows.


New Device

P.S. Looks like this machine needs the Windows Agent

Figure 4.1: platform selection window for downloading the PCSM agent

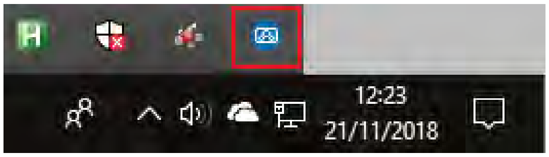


Figure 4.2: PCSM agent in the notifications area of the taskbar

- This will download the installation package to the administrator's computer. Copy the installer to a USB device, share it over the network, or email it to the target user.
- Once the agent has been received at the Windows computer to integrate, double-click the installer. The installation process takes place silently in the background. After a short while, the Panda Systems Management icon will appear in the notifications area of the taskbar.

### Make sure the computer is correctly integrated

- Click general menu **Sites** and then click the site created in the previous step.
- Click **Devices** from the tab menu. A list will be displayed with all computers integrated in the site, along with hardware and status information.

## Finding devices quickly using filters

*Refer to chapter "**Device groupings**" on page **69** for more information about the different types of groupings supported by Panda Systems Management.*

Panda Systems Management provides different types of groupings to streamline device management. These groupings can be static and dynamic. We have already explained how to use a static grouping: sites. Now, we'll discuss how to use a dynamic grouping: filters.

By default, Panda Systems Management incorporates a large number of predefined filters that allow administrators to quickly find managed devices.

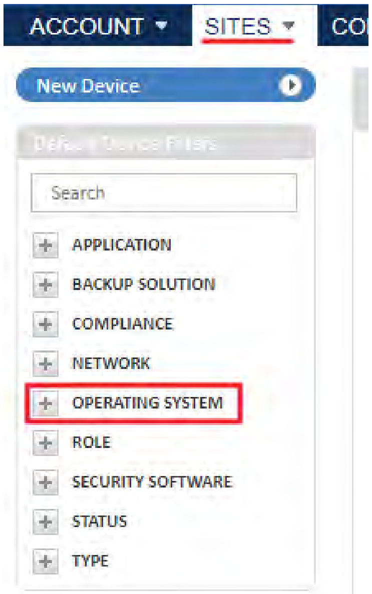


Figure 4.3: Filters side panel

### Filters side panel

Follow the steps below to use the filter system:

- Click general menu **Sites**. Then, click the site created in the first step.
- The panel on the left (**Default Device Filters**) groups all predefined filters into multiple categories. Click the ⊞ button to expand the **Operating System** section and find the filter that corresponds to the operating system version installed on the integrated device.
- Clicking the filter will update the list displayed in the right-hand panel, showing only those devices that match the criteria defined in the filter. Changing a device's operating system will cause it to automatically move to the relevant filter. That's why filters are dynamic groupings.

# Viewing devices

> *Refer to chapter "**Device visibility and status**" on page **167** for more information about the resources implemented in Panda Systems Management to view the status of managed devices.*

Panda Systems Management provides several views for displaying more or fewer details about managed devices.

## Overview of a site's devices

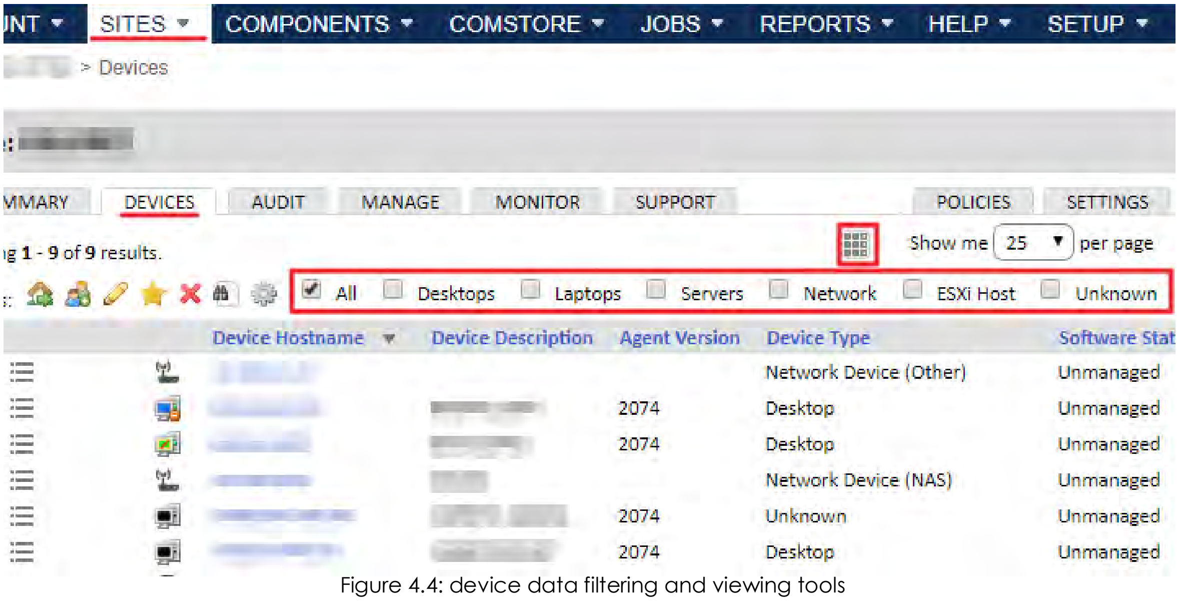
Follow these steps to get an overview of the status of all devices in a site:

- Click general menu **Sites** and then click the previously created site.
- Click **Summary** from the tab menu. A dashboard will be displayed with consolidated information about all devices in the site.
- This window displays information about the general status (online, offline), energy usage, antivirus status, and patch status of those devices.

## Details of a site's devices

- Click general menu **Sites** and then click the previously created site.
- Click **Devices** from the tab menu. A list will be displayed with all devices integrated in the site. Each line contains a series of columns with specific information about the relevant device.
- To add or remove columns from the list, click the select columns icon ▦ **(1)**.

- To filter the list by device type, use the checkboxes above the icon bar **(2)**.



g 1 - 9 of 9 results.

Show me 25 per page

☑ All ☐ Desktops ☐ Laptops ☐ Servers ☐ Network ☐ ESXi Host ☐ Unknown

| Device Hostname | Device Description | Agent Version | Device Type | Software Stat |
|---|---|---|---|---|
| [redacted] | | | Network Device (Other) | Unmanaged |
| [redacted] | [redacted] | 2074 | Desktop | Unmanaged |
| [redacted] | [redacted] | 2074 | Desktop | Unmanaged |
| [redacted] | [redacted] | | Network Device (NAS) | Unmanaged |
| [redacted] | [redacted] | 2074 | Unknown | Unmanaged |
| [redacted] | [redacted] | 2074 | Desktop | Unmanaged |

Figure 4.4: device data filtering and viewing tools

### Details of a specific device

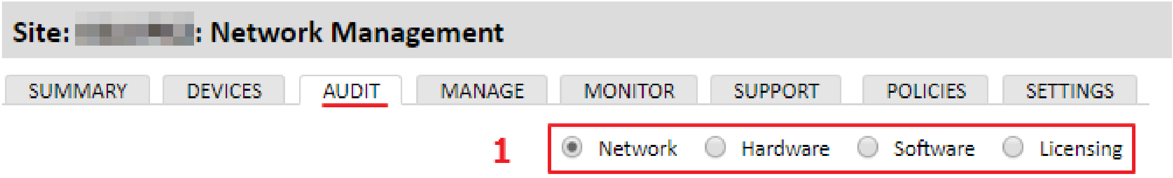
- Click general menu **Sites** and then click the previously created site.
- Click **Devices** from the tab bar and click the name of the device whose details you want to view.
- Click Summary from the tab menu. A window will be displayed with detailed information about the device: operating system information, status, desktop screenshot, and CPU, hard disk and memory usage charts.

## Performing hardware, software and license audits

*Refer to chapter "**Assets Audit**" on page* **151** *for more information about the hardware, software and license auditing resources.*

The auditing tool provides a large amount of useful information about all managed devices and the company's network.

### Accessing the auditing tool


Site: [redacted]: Network Management

● Network ○ Hardware ○ Software ○ Licensing

Figure 4.5: types of details collected by the auditing tool

- Click general menu **Sites** and then click the created site. A list will be displayed with all devices integrated into the site.

- Click a device and then click **Audit** from the tab menu.
- Click a selection control **(1)** to display the information you require:
  - **Hardware**: information about the hardware installed on the device.
  - **Software**: information about the software installed on the device.
  - **Services**: information about the services installed on the device's operating system and their status.
  - **Change log**: information about the hardware, software and system changes made to the device.
  - **Activity log**: list of the actions taken on the device, both those taken by Panda Systems Management and those taken by the administrator.

# Monitoring Windows devices

*Refer to chapter "***Monitoring***" on page* **105** *for more information about the monitoring resources implemented in Panda Systems Management. Refer to chapter "***Alerts and tickets***" on page* **247** *for more information about the alerts and tickets generated by monitors.*

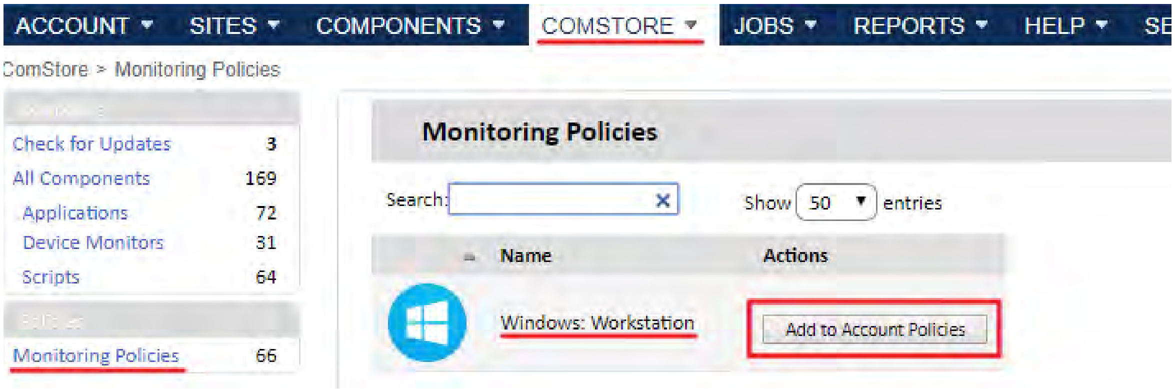
Panda Systems Management enables administrators to continuously and automatically monitor the status of the network devices, triggering alerts if certain values fall under the established thresholds. The monitoring system is flexible as it can be extended by means of proprietary components or components developed by Panda Security and published in the ComStore.

## Monitoring Windows workstations

Follow the steps below to access the predefined monitors:

- Click general menu **ComStore** to access Panda Security's free component store.
- From the side menu, choose the type of component to display: **Monitoring policies**.
- Find the Windows: Workstation component and click the Add to Account Policies button. A window will be displayed with details of the monitoring policy to add: targets (all Windows workstations) and

monitors included in the policy.

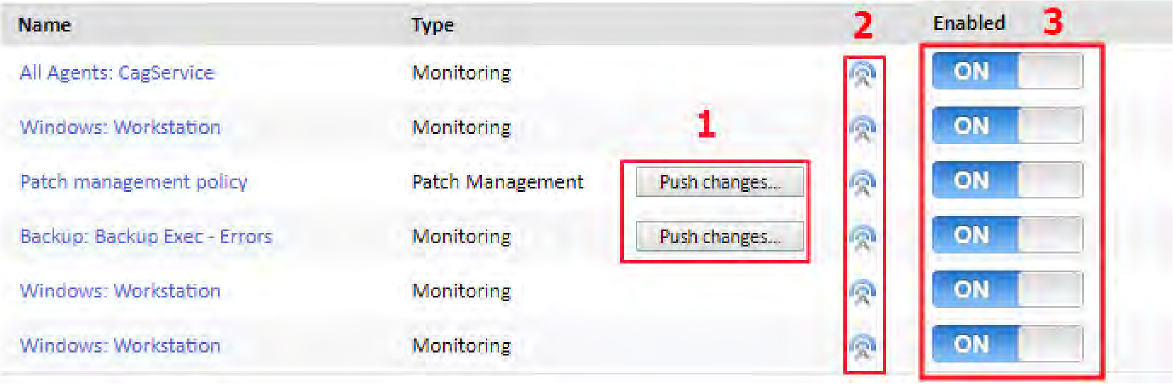


| | |
|---|---|
| Check for Updates | 3 |
| All Components | 169 |
| Applications | 72 |
| Device Monitors | 31 |
| Scripts | 64 |
| Monitoring Policies | 66 |

| Name | Actions |
|---|---|
| Windows: Workstation | Add to Account Policies |

Figure 4.6: adding a monitoring component to Panda Systems Management

- Click **Save**. A window will be displayed with all assigned policies. Click **Push changes (1)** to deploy the policy to all targeted devices. Wait a few minutes for the 📡 icon **(2)** to turn blue. Make sure the Enabled for this site setting is set to **ON (3)**.



| Name | Type | | | Enabled |
|---|---|---|---|---|
| All Agents: CagService | Monitoring | | 📡 | ON |
| Windows: Workstation | Monitoring | | 📡 | ON |
| Patch management policy | Patch Management | Push changes... | 📡 | ON |
| Backup: Backup Exec - Errors | Monitoring | Push changes... | 📡 | ON |
| Windows: Workstation | Monitoring | | 📡 | ON |
| Windows: Workstation | Monitoring | | 📡 | ON |

Figure 4.7: list of policies assigned to the Site

Once the monitoring policy has been deployed, follow the steps below to check all triggered alerts:

- Click general menu **Sites** and then click the previously created site.
- Click **Devices** from the tab bar and click the name of the previously integrated device.
- Click **Monitor** from the tab bar. Click the **Monitor Alerts** selection control in the top right corner of the window.
- In the search filter, select Status: All Alerts. This will display both resolved and open alerts.

> *When a new account is created in Panda Systems Management, a Windows: Workstation monitoring policy and a Windows: Server monitoring policy are automatically applied to it.*

# Deploying software using quick jobs

> *Refer to chapter "***Centralized software deployment and installation***" on page* **225** *for more information about the different strategies by Panda Systems Management to centrally deploy software.*

Panda Systems Management allows organizations to centrally and remotely deploy software packages published in the ComStore, or created by the network administrator, without the need to configure servers that act as repositories in the IT infrastructure. In this example, we'll show you how to deploy a software package containing the Firefox web browser.

## Deploying the Firefox browser

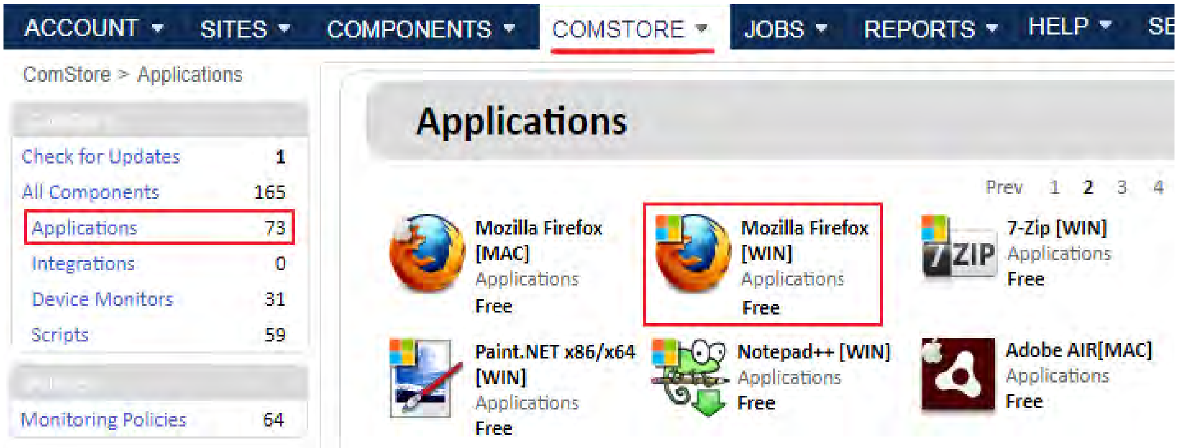
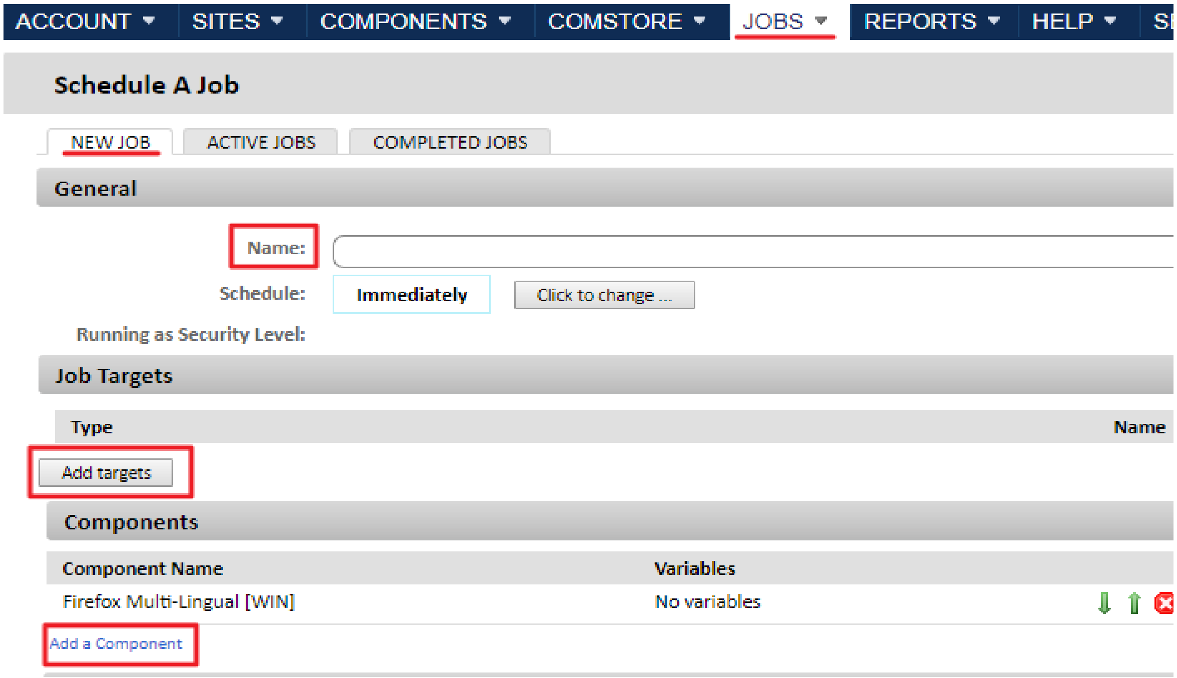


Figure 4.8: downloading the Firefox package from the ComStore free component store

- Click general menu **ComStore** to access Panda Security's free app and component store.
- From the **ComStore** side menu, click **Applications**. The panel on the right will show a list of all available applications.
- Find and click on the `Firefox Multi-lingual [WIN]` application. A window will appear with a description of the component.
- Click the **Add to my Component Library** button. Panda Systems Management will download the package to the administrator's component repository, in the **Components** area. This step is required to use any component published in the ComStore.
- Click general menu **Components** to make sure `Firefox Multi-lingual [WIN]` has been added to the list.

Once the component has been added to the administrator's repository, a job must be created to deploy the installation package to all targeted devices:



General

Name:

Schedule: Immediately

Running as Security Level:

Job Targets

| Type | Name |
|---|---|

Components

| Component Name | Variables |
|---|---|
| Firefox Multi-Lingual [WIN] | No variables |

Figure 4.9: configuring a new job

- Click general menu **Jobs**, and click **New Job** from the tab menu.
- Enter a descriptive name for the job in the **Name** field, and add a target in section **Job Targets** by using the **Add Targets** button. A window will be displayed with the **Target type** drop-down menu. This will show all grouping types supported by Panda Systems Management. To install the component in all devices included in one or multiple sites, select **Sites** from the drop-down menu, select the created site and click the **Add** button.
- From the **Components** section, click the **Add a Component** link. A window will be displayed with all application-type components stored in the administrator's repository. Select the `Firefox Multi-lingual [WIN]` component and click **Save**.
- Click **Save**.

Once the job has been created, it will be run immediately. To view the status of the job, click general menu **Jobs**, and then click **Active Jobs** from the tab menu.

# Managing patches

*Refer to chapter “**Patch Management**” on page **203** for more information about the strategies implemented in Panda Systems Management to keep all managed Windows computers up to date.*

Panda Systems Management lets administrators centrally keep all devices on the network up to date via patch management policies.

## Configuring and deploying Windows Update policies

- Click general menu Sites, select the created site and click Policies from the tab bar.
- Click **New site policy**, select **Windows Update** in the **Type** field and click **Next**.
- Click the Add a target button and select Default Device Filter from the Target type drop-down menu. A list will be displayed with all predefined filters included by default in the console. Refer to section “**Device filters**” on page **75** for a full description. Select the All workstations filter to enable the patch management feature on all workstations.

*The patch management feature is only available for Microsoft Windows devices.*

- From section **Windows Update Policy Options**, select **Automatically detect recommended updates for my computer and install them**.
- In the **Restart behavior** option, select the **No auto-restart with logged on users for scheduled Automatic Updates installations** checkbox to prevent users' computers from being automatically restarted.
- Click **Save**. A window will be displayed with all assigned policies. Click **Push changes** to deploy the policy to all targeted devices. Wait a few minutes for the 📡 icon to turn blue. Make sure the **Enable for this site** setting is set to **ON**.

# Resolving incidents remotely

*Refer to chapter “**Remote access tools**” on page **257** for more information about the remote access and troubleshooting tools provided by Panda Systems Management.*

Panda Systems Management lets administrators access managed devices remotely. This requires the computer from which the administrator accesses another computer remotely to also have the PCSM agent installed.

Out of all the remote management tools provided by Panda Systems Management, only a few may interfere with users' activities. Most tools are run in the background are completely seamless to users. Some of these tools can be accessed directly from the management console, while others must be launched from the PCSM agent.

## Remote takeover via VNC for Windows devices

This tool allows administrators to connect remotely to a computer and access programs, files, and network resources as though they were sitting at it. It may momentarily interrupt user activity. This tool is accessed from the management console.

- Click general menu Sites, select the created site and click Devices from the tab menu.
- From the target device's context menu, select Remote takeover (VNC). The Panda Systems Management agent will appear, with the admin credentials already entered, and connected to the targeted device.

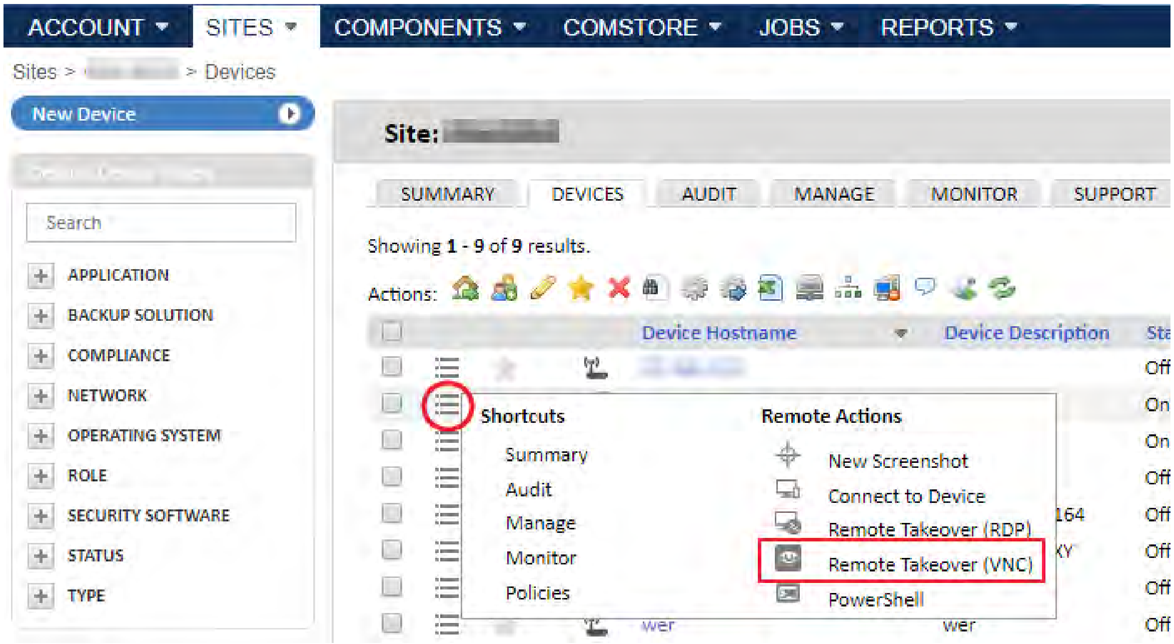


Figure 4.10: accessing the Remote Takeover tool from the management console

## Resource monitor and remote command shell

This tool allows administrators to perform tasks such as remotely accessing a Windows device's task manager, or opening a command shell for troubleshooting purposes, without interfering with the user's activities.

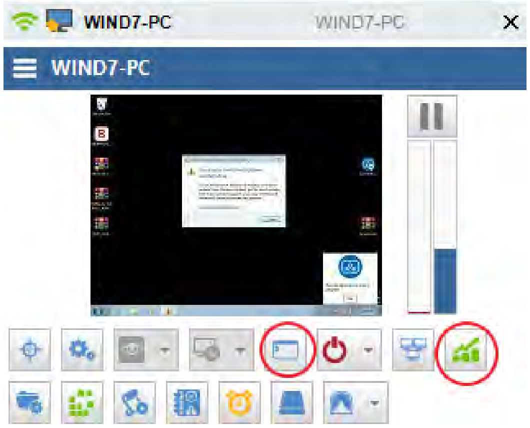


Figure 4.11: PCSM agent and available tools

- Click general menu Sites, select the created site and click Devices from the tab menu.
- From the target device's context menu, select **Connect to Device**. The Panda Systems Management agent will appear, with the admin credentials already entered, and connected to the targeted device.
- Click the button bar in the left-hand side panel to launch the troubleshooting tools shown in figure 4.11.

# Part 2

# Device installation and organization

**Chapter 5:** Deploying and managing devices

**Chapter 6:** Device groupings

# Chapter 5

# Deploying and managing devices

In an environment managed by Panda Systems Management, a device is a computer that can be accessed from the web management console for remote management and support.

All devices managed by Panda Systems Management send and receive information that the PCSM server collects, catalogs, and displays in real time in the console.

There are three possible forms of communication between the Panda Systems Management server and any given device:

- Directly by installing the PCSM agent on supported platforms. In this scenario, the agents connect directly to the Internet and communicate with the server without proxies.
- Indirectly via a proxy for those devices compatible with the PCSM agent that don't have direct Internet access.
- Indirectly via SNMP or other proprietary protocols (ESXi) for those devices that are not compatible with the PCSM agent.

For devices on which it is not possible to install the agent, another device with the agent installed and the Network Node role enabled can be used as a gateway and communicate with the device via auxiliary protocols.

In that case, the Network Node receives the commands from the Server and converts them to a protocol that the agentless device can understand. In the response from the managed device, the Network Node undoes the changes to deliver information from the incompatible device to the Panda Systems Management server.

CHAPTER CONTENTS

# Before integrating devices into the service

Before adding a device to Panda Systems Management, certain basic information is required:

- Make sure the device is compatible with PCSM.
- The site to which the agent will belong.
- Information regarding the device's Internet connection.

## Device compatibility with PCSM

The PCSM agent is compatible with the following operating systems: Windows, Linux, macOS, Android, and iOS. Refer to chapter "**Supported platforms and requirements**" on page **295** to find out if the operating system installed on the target device is supported by Panda Systems Management. If the device doesn't have an operating system compatible with PCSM, or doesn't support the installation of external devices, as is the case with routers, printers, or other network devices, refer to section "**Integrating network devices**".

## Site to which the agent belongs

In order to keep all managed devices organized, they must be put in the appropriate site within the console. For desktop platforms (Windows, Linux, and macOS), the site to which the device belongs is set automatically when the agent generated from the site is installed. This avoids having to manually configure the agent on each of the user's devices.

For mobile platforms (tablets and smartphones), the site that the agent belongs to must be entered manually through a configuration file provided by the server. See section "**Installing the agent on Android and iOS**".

## Connection information

In addition to belonging to the site designated by the administrator, the newly installed agent requires certain Internet connection information in order to communicate with the server.

In most IT infrastructures, Internet access only requires a basic TCP/IP configuration established by the operating system installed on the user's device, which the agent will use for communications. However, in network configurations that have a proxy for Internet access, the agent will require the proxy settings in order to access the proxy server.

The proxy server settings can be entered in two ways:

- **Manually in each installed agent**: from the device, right-click the Panda Systems Management icon in the notifications area of the taskbar. Next, select **Settings** from the drop-down menu and click the **Network** tab. Enter the proxy data in the fields displayed.
- **Globally in each site**: from the management console, click general menu **Sites**, and select the site to which the newly installed device will belong. Then, select the **Settings** tab and enter the required

data in the **Proxy** section. Once this information has been entered, all agents installed from this site will have this proxy data.

# Deploying the PCSM agent via email

This deployment method is compatible with:

- Windows, Linux, and macOS desktops, servers, and laptops.
- iOS and Android smartphones and tablets.

This method is recommended in the following scenarios:

- When a domain infrastructure is not available that allows for centralized deployment via GPO or equivalent third-party tools.
- When there are no other PCSM agents installed on the network.
- When the network is small and it is not worth it for the administrator to configure a centralized deployment job.

Follow these steps to send the PCSM agent installation package via email:

- Go to general menu **Sites**, and select the site to which the devices to integrate will belong.
- Click **Devices** from the tab bar. Then, click the **New Device** button in the upper left corner of the window. You will see a dialog box with all the platforms supported by the agent: Windows, macOS, Linux, iOS, and Android, as well as those devices not compatible with the agent (network devices, printers, and ESXi servers).

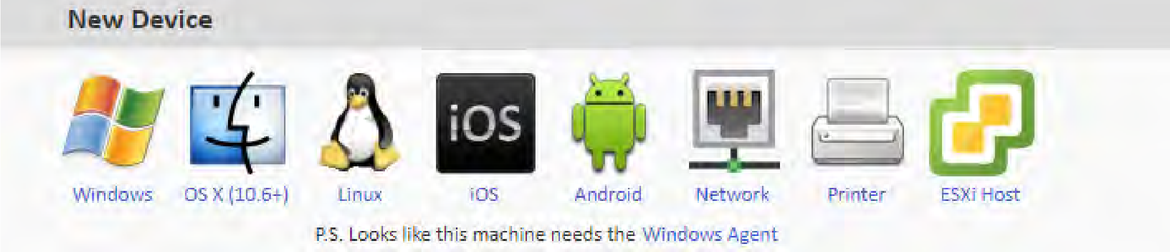


Figure 5.1: platforms supported by Panda Systems Management

- Click the appropriate platform and enter the email addresses of the users of the devices to be managed, separated by a semi-colon ";". Depending on the platform, the user will receive an email with the agent in an attachment (Windows, macOS, and Linux), or with a link to download it from Google Play or Apple Store.

*Unmodified mobile platforms only allow apps to be downloaded from the corresponding app store. For this reason, the only certified method for delivering the agent to tablets and smartphones is by emailing the URL for the app in the app store.*

- To send a message containing the download URL to the Windows, macOS, or Linux installation package using the email client installed on your computer, click the link **Send the link from your email client instead** at the bottom of the window.

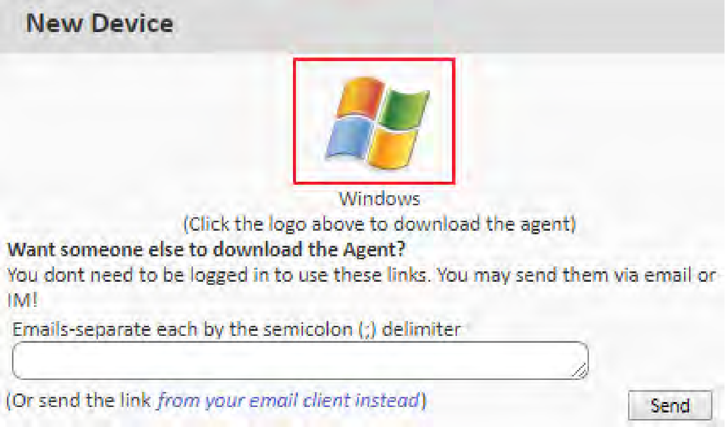
# Deploying the PCSM agent centrally using a deployment tool

This deployment method is compatible with:

- Windows, Linux, and macOS desktops, servers, and laptops.

This method is recommended in the following scenarios:

- When there is a third-party software deployment tool already integrated into your company's IT infrastructure.



New Device

Windows

(Click the logo above to download the agent)

**Want someone else to download the Agent?**

You dont need to be logged in to use these links. You may send them via email or IM!

Emails-separate each by the semicolon (;) delimiter

(Or send the link *from your email client instead*)

Figure 5.2: direct download of the PCSM agent

Administrators can download the PCSM agent from the console, then distribute it manually or using distribution tools such as Active Directory. To do this, follow the procedure described in section "**Deploying the PCSM agent via email**", but, instead of sending an email message, click the platform icon to download the PCSM agent to the administrator's computer. Once downloaded, place the installation package on a network share that is accessible by your network computers, or configure a software installation job via an Active Directory GPO.

# Deploying the PCSM agent remotely via another PCSM agent

This deployment method is compatible with:

- Windows, Linux, and macOS desktops, servers, and laptops.

This method is recommended in the following scenarios:

- When the number of computers to integrate is large and you don't have a third-party software deployment solution.

## Device discovery requirements

For a network computer to be discovered by a Network Node device, the following conditions must be met:

- **If the Network Node is scanning its subnet**: The computer to be found must respond to the `ping`.
- **If the Network Node is scanning different subnets from its local subnet**:
  - The computer to be found must respond to the ping.
  - "The computer to be found must allow TCP connections on any of the following ports: `22 - SSH`,

`80 - HTTP, 8080 - HTTP, 443 - HTTPS.`

## Deploying the PCSM agent remotely

Installing the agent on networks with many devices is a long and tedious process if you have to carry it out for each device independently. The remote installation feature allows you to speed up the deployment process. Follow the steps below:

- Send the agent to the first Windows or macOS device on the network using any of the above-mentioned procedures.
- Designate the installed agent as a Network Node (with network scanning).
- Run a computer discovery task on the network:
  - From the console (Windows and macOS).
  - From the installed agent (Windows only).
- Install the agents remotely:
  - From the console (Windows and macOS).
  - From the installed agent (Windows only).

1. Designate the installed agent as a Network Node (with network scanning).

To discover network active devices, it is necessary to assign the Network Node role to one of the devices with the Systems Management agent installed. Refer to section "**Configuring a Network Node**" in this chapter for more information on how to assign the Network Node role to a device.

2. Run a computer discovery task from the console.

To discover network computers, it is necessary to launch an audit of the computer designated as the Network Node (with network scanning). For that, in the general menu Sites, Devices, select the device and click the binoculars icon on the icon bar.

By default, the discovery task will be limited to those devices connected to the same subnet as the computer nominated as Network Node. Follow the steps below to extend the search scope:

- From the general menu **Sites**, click **Settings** on the tab bar.
- In section **Additional Subnets for Network Discovery**, enter the IP address ranges to explore.
- To limit the total number of IP addresses explored for each subnet, go to general menu **Setup**, **Account Settings** tab, section **Custom Agent Settings**. Set the **Network Subnet Limit** and **Network Scan Limit** values.

3. Install the agents remotely from the console.

Within 15 minutes after the launch of the discovery task, follow the steps below:

- Go to general menu **Sites**, click **Audit** from the tab bar, and select the **Network** radio button in the top-right corner to display all discovered computers grouped by type.
- Select the computers on which you want to install the agent and click the **Manage computers** icon

➡.

- A dialog box will be displayed for you to choose the agent type to install.
- After you select the platform, a dialog box will be displayed prompting you to enter the necessary credentials on the target devices to install the agent. Given that remote installation of an agent is a process that creates services on the device and needs to be configured in order to be launched whenever the operating system is started, remote installation has to be done with administrator (or equivalent) permissions.
  - Click the **Settings** tab of the site the devices that will receive the PCSM agent belong to, or click general menu **Setup** and then click **Account Settings** from the tab bar.
  - In the **Agent Deployment Credentials** section, click **Edit**. Text boxes will be displayed for you to enter the domain administrator credentials (username and password).
  - Use the **ON/OFF** buttons to select at which level you want the entered credentials to be used. ON (default settings): the platform will use the available credentials at **Account** and **Site** levels. OFF: the credentials will be used at **Site** level.

> ⚠ *An installed PCSM agent can only deploy agents that are compatible with its platform. That is, a Windows agent will deploy the agent to Microsoft compatible devices, and a macOS agent will deploy agents to Apple devices.*

4. Run a computer discovery task from the PCSM agent (alternative method).

Instead of using the management console, it is possible to start the deployment process from the PCSM agent installed on a Windows computer. To do this, follow the steps below:

- Click general menu **Sites**, and then click the site where the computer that will perform the discovery task is located.
- Click **Devices** from the tab menu. Then, click **Connect to Device** from the context menu of the device that will deploy the PCSM agent. This will open the PCSM agent installed on the administrator's computer.
- Go to the PCSM agent's **Tools** menu. Click **Agent Deployment** and then **Device Discovery**. This will display all computers connected to the same subnet as the device, indicating whether or not they already have a Panda Systems Management agent installed and its version

.

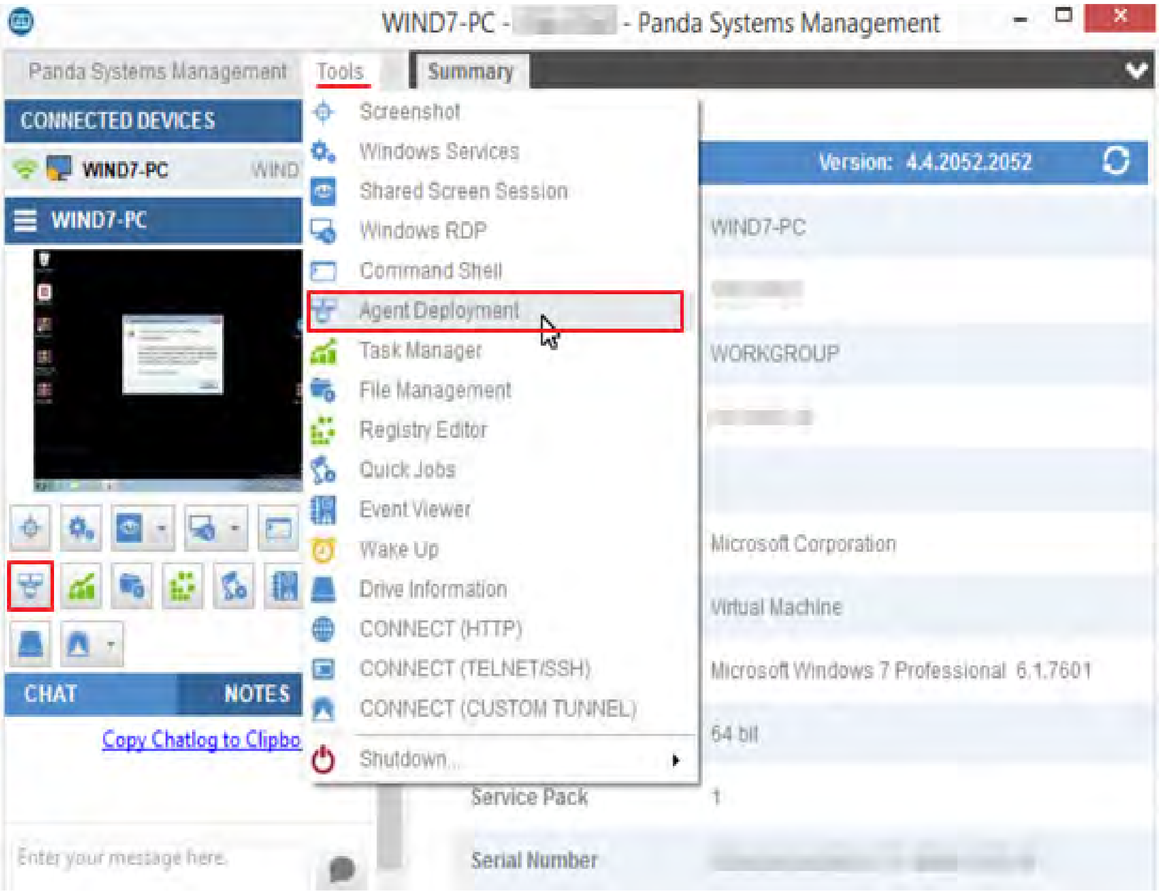


Figure 5.3: accessing the deployment tool from the PCSM agent

- When the discovery process is completed, select the computers that will receive the agent and click the ⊕ icon.
- Before the deployment process is launched, a window will be displayed to enter the necessary user credentials to install the agent and create the required services on the target computers.

# Deploying the agent using image cloning

Each PCSM agent installed on a device generates a unique ID that is used by the Panda Systems Management server to identify it. That ID is stored on the device's record.

In large computer networks where homogeneous hardware is used, one of the basic strategies that is used to expedite deployment to new computers on the network consists in cloning or obtaining an image of the entire operating system along with all installed programs. In the case of Panda Systems Management, you can speed up the PCSM agent deployment process by generating a base image from a computer with the agent installed. However, this implies that the ID generated for the computer will be replicated to all computers that receive the image, resulting in all computers having the same

ID. To avoid this problem, follow these steps on the computer from which the base image will be generated:

### Windows computers

- Isolate the computer from the network.
- Open the Windows registry (regedit.exe), and browse to branch `HKEY_LOCAL_MACHINE/Software/CentraStage`
- Delete the CentraStage folder, including its ID.
- Start the cloning process.

### MacOS computers

- Isolate the computer from the network.
- Open a terminal window and run the following commands:

```
sudo su

cd /var/root/.mono/CurrentUser/software/centrastage

rm -f values.xml
```

- Start the cloning process.

# Installing the agent on workstations and servers

### Installing the PCSM agent on Windows computers

- To install the PCSM agent on a Windows computer other than Windows Server Core, double-click the installation package. The PCSM agent will install silently on the background, automatically connecting to the Panda Systems Management server without requiring any sort of user interaction.

  When the installation process is completed, the Panda Systems Management icon will appear in the notifications area of the Windows taskbar. The color of the icon will be blue, meaning that the agent is connected to the PCSM server.
- To install the PCSM agent on a Windows Server Core computer, make sure the .NET Framework is already installed and the computer has been restarted. From the Command Prompt window, access the folder where the `agent.exe` file is located, and run it.

### Installing the PCSM agent on macOS computers

- Decompress the `.zip` file and open the `AgentSetup` created folder.
- Double-click the `CAG.pkg` file and follow the instructions in the installation wizard. When the installation process is completed, the PCSM icon will appear on the device's menu bar.

### Installing the PCSM agent on Linux computers

- Open a Linux terminal and access the folder where the `AgentSetup.sh` file is located.
- Type `sudo sh AgentSetup.sh` and enter the administrator password when prompted.

# Installing the agent on Android and iOS

This deployment method is compatible with:

- Mobile devices such as Android and iOS smartphones and tablets.

Follow the steps below to manage mobile devices from the Systems Management console:

- Enable the console's MDM feature.
- Import the certificate into the console (for iOS-based devices only).
- Send the PCSM agent download URL via email.
- Associate the device with a site.

1. Enable the console's MDM feature

To be able to interact with your mobile devices from the console, you need to enable the MDM feature. To do this, import the free component Mobile Device Management directly from the ComStore.

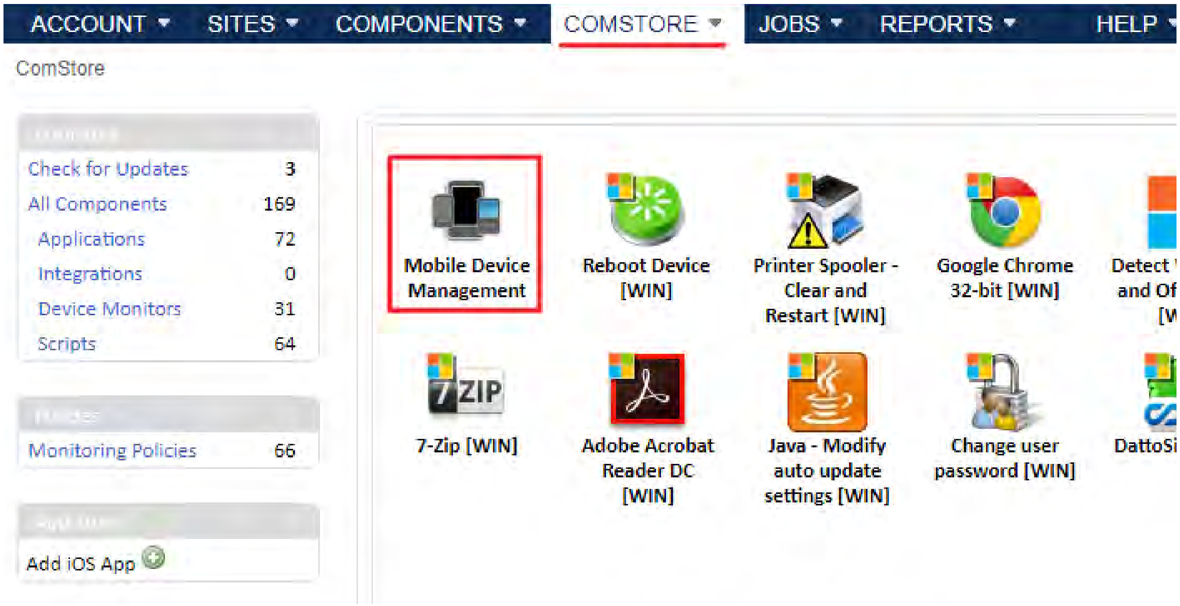


Figure 5.4: Mobile Device Management component

Follow the steps below to import the Mobile Device Management component:

- Go to general menu **ComStore** and click the `Mobile Device Management` component.

- Click the **Add to my Component Library** button.

*Even though the Mobile Device Management component is free, every mobile device with an agent installed will count as a regular license for the purpose of counting the total number of purchased licenses.*

Once the component is added, the iOS and Android operating systems will appear in **Add Devices**.

2. Import the certificate into the console (for iOS-based devices)

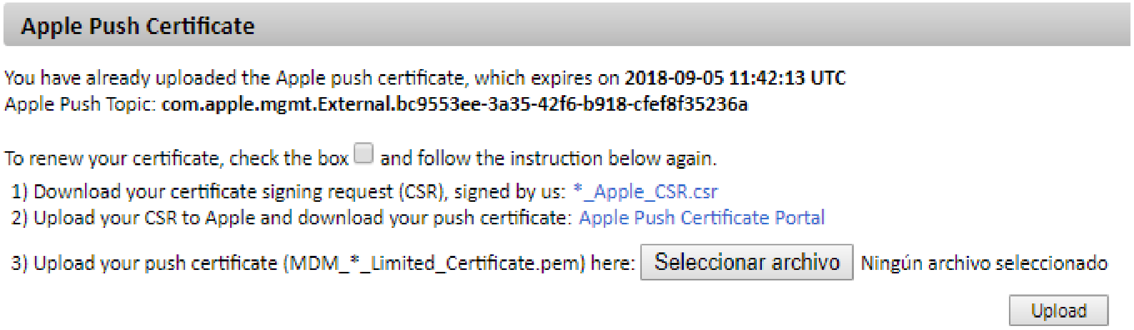
It will also be necessary to incorporate -into the console- the certificate generated by Apple for iOS devices to be able to connect to the server.

*Importing the Apple certificate is a mandatory, one-time process for each customer/ partner who wants to manage one or multiple iOS-based devices.*

*Installing the certificate is a requirement from Apple to ensure the integrity, authenticity and confidentiality of all communications between the server and the user's device.*

To do so, follow the steps below:

- Browse to **Setup**, **Account Settings** to access the Apple certificate settings (Apple Push Certificate section).



**Apple Push Certificate**

You have already uploaded the Apple push certificate, which expires on **2018-09-05 11:42:13 UTC**
Apple Push Topic: **com.apple.mgmt.External.bc9553ee-3a35-42f6-b918-cfef8f35236a**

To renew your certificate, check the box □ and follow the instruction below again.

1) Download your certificate signing request (CSR), signed by us: *_Apple_CSR.csr
2) Upload your CSR to Apple and download your push certificate: Apple Push Certificate Portal
3) Upload your push certificate (MDM_*_Limited_Certificate.pem) here: Seleccionar archivo Ningún archivo seleccionado

Upload

Figure 5.5: certificate upload window

- Download the certificate signing request (CSR), signed by Panda Security (`*_Apple_CSR.csr`).
- Upload the CSR file to the Apple Push Certificate Portal.
  - To access the Apple Push Certificate Portal, you must have an Apple account. Any iTunes account will be enough. However, if you want to generate new Apple credentials, go to **https://appleid.apple.com/**, click **Create an Apple ID** and follow the on-screen instructions.
  - Go to **https://identity.apple.com/pushcert**, and sign in with your Apple credentials. Click Create Certificate and follow the on-screen instructions. Load the CSR file you downloaded in the previous step.
  - Download the new Apple signed certificate (`.PEM`) to your computer.
  - Go back to the PCSM console. Browse to the Apple signed certificate (`.PEM file`) downloaded

from the Apple Push Certificate Portal, and upload it. The following message will be displayed: `You have already uploaded the Apple push certificate, which expires on XXXX`.

3. Send the download URL via email

Due to security restrictions, customers can only receive an email containing a direct download link for Apple Store or Google Play, and an `.MDM` file containing the information about the site associated to the device.

*As the Agent is downloaded from the official app store for each mobile platform (Google Play or Apple Store), information about the site is not part of the downloaded package, as this would mean changing the content of the package in the store. This information is therefore kept in the .MDM file delivered in the email.*

4. Associate the device to a site

After the iOS or Android agent has been installed on the customer's device, the user must take the following steps to associate it to the selected site. There are two ways to associate a device to a site:

- **Option 1: Capturing the QR code using the device's camera**

Click general menu **Sites** and select the site the device will be integrated into. Click the QR code icon in the top-right corner of the window to expand it.

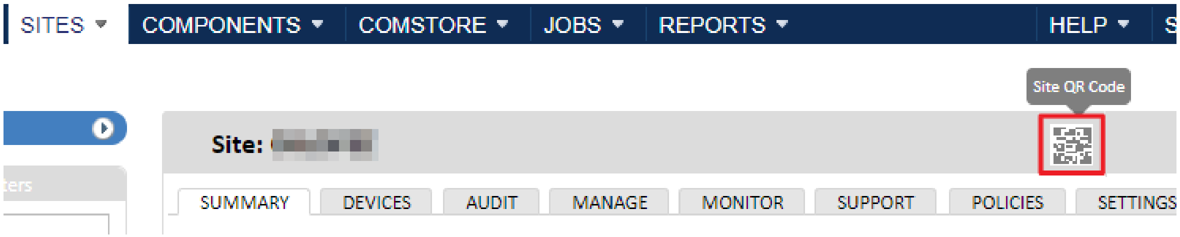


Figure 5.6: generating the QR code

Then, the user must tap the wheel icon on their device to launch the camera and capture the QR code on the screen.

After reading the code, the agent will display the message **Connected** on the user's device, and appear in the console.

- **Option 2: Importing into the agent the .MDM file attached to the email.**

On cell phones without camera, it is possible to open the .MDM file from the email message by simply tapping the file.

After loading the .MDM file, the agent will display the message **Connected** on the user's device, and appear in the console.

*MDM file import is only supported from the device's native email client.*

# Integrating network devices

> *Although not strictly necessary, it is advisable for administrators to familiarize themselves with the basic concepts of SNMP (OID, MIB, NMS, etc.), as well as having a MIB browser to be able to browse the OIDs structure of the device. We recommend using Mibble. Mibble is a MIB browser available for free from the Mibble website.*

This deployment method is compatible with:

- Devices that don't support software installation such as printers, routers, scanners, switchboards, etc.

Follow these steps to manage network devices using Panda Systems Management:

- Add the network device.
- Assign a Network Node computer to the device.

1. Integrating network devices

Adding devices separately:

- Go to the general menu **Sites** and choose the site that the devices to manage belong to.
- In tab bar, **Devices**, click **Add a Network Device** and select **Printer** or **Network Device**.

In both cases, a window will open for the network administrator to enter the device details.

Adding several devices at once:

- From general menu **Sites**, select the site that the devices to manage belong to.
- Click **Audit** from the tab menu, and then click the **Network** selection control from the top-right corner of the window. The **Network**, **Printer,** and **Unknown** groups contain all devices that don't support the PCSM agent.
- Select the network devices to add and click the ➔ button. A window will open for you to enter the necessary information to manage the new devices.
    - **Deploy from**: Select the Network Node assigned to the devices.
    - **Device type**: Select the device type to appear in the console.
    - **Set credentials**: Select the **SNMP credentials** configured in section **SNMP Credentials** of tab **Settings** at Site Level, or in general menu **Setup**, **Account Settings** at **Account Level**.

> *Each device added to the console uses a license from the total number of licenses contracted by the customer.*

2. Assigning a Network Node computer to a device

Since it is not possible to install a PCSM agent on a router, a switch, and other types of network devices, it will be necessary to use another computer as a bridge between the Systems Management server and the device to manage. That computer must be designated as a Network Node.

To assign a device to Network Node, refer to section "**Configuring a Network Node**".

# Managing ESXi servers

ESXi servers are systems that use a specially modified and simplified Linux kernel to run the manufacturer's hypervisor, which will provide the virtualization service to every virtual machine hosted on the system. ESXi systems do not support the PCSM agent, as their only purpose is to run the virtual machines created with the lowest possible impact on the server resources.

ESXi servers are managed with Panda Systems Management through a PCSM agent installed on a Windows machine. The PCSM agent will connect to the ESXi server to manage, and will collect all necessary information to send it to the PCSM server and show it in the management console.

*It is important to draw a distinction between managing the ESXi server and managing the virtual machines it hosts. Managing the ESXi server allows administrators to manage the resources of the physical machine and the hypervisor, whereas managing the various virtual machines allows administrators to manage the status of the virtualized resources for a specific virtual machine. To manage a specific virtual machine, it is necessary to install a PCSM agent on it in the same way as with physical machines.*

## Assigning a Network Node computer to an ESXi server

Since it is not possible to install a PCSM agent on an ESXi server, it will be necessary to use another computer as a bridge between the Systems Management server and the device to manage. That computer must be designated as a Network Node. To assign a Network Node to an ESXi server, follow the steps indicated in section "**Configuring a Network Node**".

## Setting the ESXi credentials

The ESXi server credentials can be set individually for each ESXi server to integrate, or they can be inherited from the general settings defined at Account or Site level.

Follow these steps to set the credentials at Account level:

- Go to general menu **Setup** and click **Account settings** from the tab bar.
- Scroll down to the **ESXi Credentials** section, and click the **Edit** link.
- Enter the following information: **Name**, **CIM Port**, as well as the **Username**, **Port**, and **Password** for the vSphere management tool.

Follow these steps to set the credentials at Site level:

- Click general menu **Sites** and then click the site you want to set the  ESXi credentials for.
- Click **Settings** from the tab menu. Scroll down to the **ESXi Credentials** section, and click the **Edit** link.
- Specify if the credentials must be inherited from the Account level by selecting the **Use Account level credentials for ESXi hosts** option.
- Otherwise, enter the following information: **Name**, **CIM Port**, as well as the **Username**, **Port,** and **Password** for the vSphere management tool.

### Adding ESXi servers individually

- From the general menu **Sites**, select the site that the devices to manage belong to
- On the **Devices** tab, click **Add a device**. A dialog box will be displayed with the platforms that are supported.
- Click the ESXi icon.
- Enter the necessary data to communicate with the ESXi server.

Since ESXi servers do not support the PCSM agent, it is necessary that a PCSM agent on the network acts as a gateway (Network Node). For that, it will be necessary to enter the appropriate connection credentials.

To define the specific credentials to connect to the ESXi server, click **New ESXi Credentials**. To inherit the configuration established at Account or Site level, click **Use Account/Site ESXi Credentials.**

### Adding multiple ESXi servers at the same time

- From general menu **Sites**, click the site that the ESXi servers will be integrated into.
- Click **Audit** from the tab menu, and then click the **Network** selection control from the top-right corner of the window. A list of all the devices discovered on the network will be displayed.
- Click the ESXi grouping to list all the ESXi servers found across the network.
- Click the **Manage Devices** icon ➡ from the icon bar, and select **ESXi** as device type. A form will be displayed similar to the one described in the previous section for you to enter the required credentials.

## Managing Hyper-V servers

Hyper-V servers are Windows Servers with the Hyper-V role enabled, which can run Microsoft's hypervisor subsystem to host virtual machines.

Since Panda Systems Management supports the Windows Server family, it is not necessary to execute a procedure other than that detailed in section "**Installing the agent on workstations and servers**" for

Windows systems. Once the PCSM agent has been installed, it will be possible to audit the Hyper-V server and the virtual machines it hosts.

# Approving devices

Service administrators can also ask for manual approval of devices when integrating a new one with the recently installed agent. This process may be necessary to monitor which devices are added to the service, particularly in environments where the agent is freely accessed from within the company (mapped drive or shared resource).

## Enabling manual approval of devices

- Go to general menu **Setup**, and click **Account Settings** from the tab bar.
- From the **Access Control** section, click the **Require new device approval** button.

## Checking devices pending approval

*Unapproved devices use licenses despite they cannot receive jobs or deployed components.*

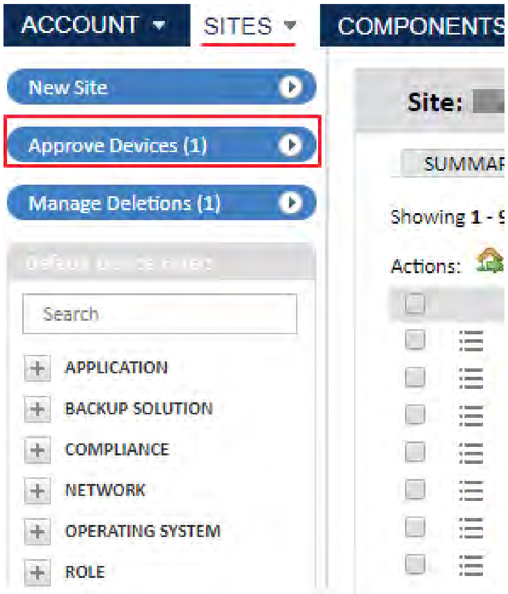


Figure 5.7: Approve Devices button

- Go to general menu **Sites**, and click **Approve Devices** from the left-side panel.
- Select the devices to approve and click the ✓ icon from the icon bar.

Unapproved devices are also shown in inventories and can be accessed via remote takeover.

Unapproved devices are indicated with a message on the list of devices of the site they belong to.

# Uninstalling the agent and deleting devices

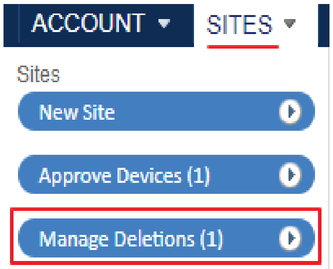


Figure 5.8: Deleted devices

When a device stops being supported by the organization's IT department, or is removed from the company's managed environment, it must be deleted from the Panda Systems Management platform in order to recover the license that was assigned to it and be able to use it on another device.

Every device that is connected to the server, and deleted from the management console, has its PCSM agent automatically uninstalled by Panda Systems Management.

However, if a device is offline when it is deleted, it will be moved to the **Deleted Devices** area and its PCSM agent will be removed the next time that it connects to the server.

To view a list of all deleted devices, click general menu **Sites** and then click **Deleted Devices** from the side menu.

### Recovering deleted devices

When deleting a device that is not currently connected to the Panda Systems Management server, the device is moved to the **Deleted Devices** area. Once there, it can be recovered so that the next time that the device connects to the server the process to automatically uninstall the PCSM agent is not launched. To do this, follow the steps below:

- From the **Deleted Devices** area, select the devices to recover and click the ✖ icon. All selected computers will disappear.
- The computers to recover will reappear in the sites where they were originally integrated the next time that they connect to the server.

## Uninstalling the PCSM agent from the management console

Follow the steps below to delete one or more devices:

- From general menu **Sites**, click the site where the devices to delete are located, and then click **Devices** from the tab bar.
- Use the checkboxes to select the devices to delete and click the ✖ icon.

## Uninstalling the PCSM agent from the target device

### Windows devices

- Click the Windows Start button (lower left corner of the desktop), and then click Settings, Applications.

- Select Panda Systems Management in the list of programs installed.
- Click the Uninstall button.

### MacOS devices

- Open a terminal window and run the following command:

```
sudo bash /Applications/AEM\ Agent.app/Contents/Resources/uninstall.sh
```

### Linux devices

- Open a terminal window and run the following command:

```
sudo /bin/bash /opt/CentraStage/uninstall.sh
```

## Other agent connection parameters

> *With the exception of NetAssets Subnet Limit, these parameters should only be altered with the express permission of the Panda Security Support Dept. Any modification could result in the loss of connection with the agents.*

If you want to change the PCSM agent connection settings, go to general menu **Setup**, **Account Settings**, **Custom Agent Settings**. There, you can configure the following options:

| Field | Description |
|---|---|
| **Use Connection Brokers** | Use the button to enable or disable the feature. |
| **Use alternative settings for Agent** | Lets you manually set a number of parameters to configure a Connection Broker. |
| **Control Channel Address** | Use restricted to the Panda Security Support Dept. |
| **Control Channel Port** | Use restricted to the Panda Security Support Dept. |
| **Web Service Address** | Use restricted to the Panda Security Support Dept. |
| **Tunnel Server Address** | Use restricted to the Panda Security Support Dept. |
| **Network Subnet Limit** | Restricts the device scanning range of the Connection Broker within a network segment to the specified number (0-65535). Enter a value of 0 to prevent network devices from being scanned. |
| **Network Scan Limit** | Restricts the number of devices scanned by the agent within its subnet to the specified number (0-1024). Enter a value of 0 to prevent network devices from being scanned. |

Table 5.1: configuration parameters for the connections used by the PCSM agent

# Configuring a Network Node

A Network Node is a device with a Systems Management agent installed that performs additional tasks on the customer's network. These tasks are related to computer discovery and the configuration of devices managed via SNMP and ESXi.

## Requirements for configuring a Network Node

- Only servers, workstations, and laptops can be designated as a Network Node
- The device must have a Windows, macOS, or Linux operating system installed compatible with the PCSM agent.

> *Only devices with a Windows or macOS operating system can run device discovery tasks.*

- Only devices with a Windows or macOS operating system can run device discovery tasks.
- Due to the activities it will have to perform, it is recommended that the Network Node device be always online. Computers nominated as Network Node will automatically receive an Online Status Monitor. Refer to section "**Online Status Monitor**" on page **109** for more information about this type of monitor. If a Network Node computer is offline for more than 5 minutes, Panda Systems Management will trigger a **Critical** alert and will send an email notification to the predefined accounts.

> *Since Network Node computers perform more tasks than those assigned to a regular computer, it is recommended that you create additional CPU and memory monitors to monitor resource consumption on those devices. In overload situations, the Network Node device may go offline, affecting the connections established with other managed devices.*

## Requirements for configuring a Network Node as SNMP monitor

For an agent with the Network Node role to monitor devices using the SNMP protocol, the .NET Core 3.1 package needs to be downloaded and installed. For that, the PCSM agent checks to see if the operating system meets the necessary requirements and, if it does, it starts downloading the NET Core 3.1 package automatically.

> *PCSM agents with the Network Node role assigned are not compatible with already installed .NET Core 3.1 packages. The PCSM agent itself must download a specific version when the operating system requirements are met. To do that, when it is started and every 2 hours subsequently, the PCSM agent checks to see if the system requirements are met and, if they are, it will download the package automatically and restart.*

Next is a list of the operating systems that support .NET Core 3.1 and the requirements they must meet:

- **Native support (downloading the .NET Core 3.1 package is not required)**:
  - Windows 10
  - Windows Server 2016
  - Windows Server 2019
- **Patches KB2999226 and KB2533623 must be already installed:**
  - Windows 7 SP1
  - Windows Server 2008 R2 SP1
- **Patch KB2999226 must be already installed:**
  - Windows 8.1
  - Windows Server 2012 R2

*KB2999226 is packaged with Microsoft Visual C++ 2015 Redistributable Update 3 or above, including Microsoft Visual C++ 2017 Redistributable.*

- **macOS and Linux**: these systems require that the .NET Core 3.1 package be previously installed in order to manage SNMP-enabled devices.

## Types of Network Nodes

There are two types of Network Nodes:

- **With network scanning**

These nodes allow discovery of neighboring nodes or nodes connected to the same network segment.

Every time there is an audit of the computer with the Network Node role (with network scanning), the agent sends out a device discovery broadcast message. All discovered devices will appear on the **Audit, Network** tab.

Additionally, these devices can send and receive SNMP commands to manage those devices on which it is impossible to install a **Systems Management** agent.

- **Without network scanning**

These devices are capable of sending and receiving SNMP and ESXi commands, but cannot perform computer discovery tasks.

### Designating a Network Node

In the general menu **Sites**, **Devices**, select the device that will be designated as Network Node. To do that, click the checkbox next to the device's name, click the 🖧 icon on the icon bar and select Network Node.

Once the device has taken the new role, its icon will change to 🖥.

### Removing the Network Node assignment from a device

Go to general menu **Sites**, and click the relevant site. Click **Devices** from the tab bar and select the device whose Network Node assignment you want to remove. Next, click 🖧 from the icon bar and select the **Remove as Network Node** option.

### Assigning a Network Node to devices

Follow the steps below to assign a Network Node to a single device not compatible with the PCSM agent:

- Click general menu **Sites**, select the site that the device to manage belongs to, and click **Summary** from the tab bar.
- Click the **Edit** link in the **Network Node** field. A drop-down menu will be displayed with all accessible Network Nodes. Select one and click **Save**.

Follow the steps below to assign a Network Node to multiple devices:

- Click general menu **Sites**, and then click the site where the devices are located.
- Select the devices and click the 🖧 icon from the icon bar.
- Select the **Assign Network Node** option from the drop-down menu displayed. A window will be displayed for you to select a Network Node from all available nodes.

## Device discovery (network scanning)

During audits, Network Nodes will attempt to authenticate network devices automatically. A Network Node is able to scan its own subnet by default, however, additional subnets can also be added for device discovery.

### Device discovery process

The automated device discovery process consists of the following steps:

- When the Network Node scans its own subnet:
  - Ping all IP addresses on the subnet.
  - Create a record for each discovered device, with its IP and MAC address.

- Connect to each device via SNMP to determine if it is a network device or a printer.
- Connect to port 902 to determine if it is an ESXi server.
- Connect via NetBIOS and check the TTL to determine if it is a Windows device.

- When the Network Node scans a user-specified additional subnet:
  - Ping all IP addresses on the additional subnet. Refer to section "**Additional subnets for device discovery**" later in this chapter.
  - Create a record for each device that responds to the ping and where a TCP connection could be established to any of the following ports: 22, 80, 8080, 443.
  - Connect to each device via SNMP to determine if it is a network device or a printer.
  - Connect to port 902 to determine if it is an ESXi server.
  - Connect via NetBIOS and check the TTL to determine if it is a Windows device.
- To avoid duplication in the discovered device records, the following de-duplication logic is applied:
  - Check if the new device to be added to the discovered devices has a MAC address. If the new device does have a MAC address, check if there is another discovered or managed device with the same MAC address in the entire account or in the same site. If a match is found, reject the new device as a duplicate.
  - If the new device does not have a MAC address, because it is on a different network segment, check if there is another discovered or managed device with the same IP address in the same site. If a match is found, reject the new device as a duplicate.

## Additional subnets for device discovery

To add additional subnets to the network discovery settings of a Network Node, follow the steps below:

- Click general menu **Sites**, select the site where the Network Node is located, and click **Settings** from the tab bar.
- In section **Additional Subnets for Network Discovery**, enter the start IP address and the end IP address.
- Click **Save**.

> *You can add additional subnets to scan only at Site level.*

## Limiting device discovery within a subnet

To reduce the number of scanned devices in a device discovery task, follow the steps below:

- Go to general menu **Setup**, and select the **Use alternative settings for Agent** checkbox from the **Custom Agent Settings** section.
- In the **Network Scan Limit** field, enter the number of devices that the Network Node will attempt to discover.

How to disable device discovery:

- Go to general menu **Setup**, and select the **Use alternative settings for Agent** checkbox from the **Custom Agent Settings** section.
- In the **Network Scan Limit** field, enter 0.

### Improving device discovery via SNMP

By default, the PCSM agent uses anonymous SNMP connections (SNMPv2c protocol, public community string) to connect to devices and identify them:

To improve the SNMP authentication phase at Account level, follow the steps below:

- Go to general menu **Setup**, and click **Account Settings** from the tab bar.
- From the **SNMP Credentials** section, click the **Add SNMP Credentials** link and set the credentials for each SNMP device.

To improve the SNMP authentication phase at Site level, follow the steps below:

- From general menu **Sites**, click the site whose settings you want to edit, and then click **Settings** from the tab bar.
- From the **SNMP Credentials** section, click the **Add SNMP Credentials** link and set the credentials for each SNMP device.

Panda Systems Management uses the list of credentials on each device in the order defined at Account level until a set of credentials allows the connection to be established. If no set of credentials are accepted, the solution will start to use the list of credentials defined at Site level.

## Configuring a local cache node

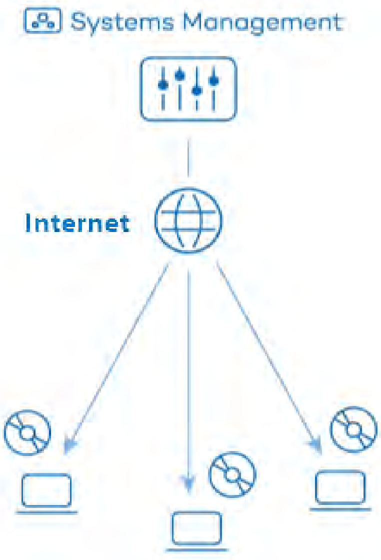


Figure 5.9: Deploying packages individually

The PCSM agent installed on each device checks the PCSM server for downloads every 60 seconds and if there are any available, it is run individually for every agent. In this way, for a 50 megabyte installation package and a network of 50 devices, the download result will be 2.4 gigabytes.

To reduce the total download size, Panda Systems Management uses the Peer-to-Peer Sharing technology, which allows a PCSM agent to download a component from a different PCSM agent in the same site.

Also, to cache patches in addition to components, you can nominate one of the network devices as a local cache. By doing this, only this device will download the package from the server and then deploy it to all of the affected network devices.

*If a component is cached on a device designated as a local cache, the Peer-to-Peer Sharing technology will not be used.*

# Designating a local cache

## Minimum system requirements

Local cache devices must meet the following requirements:

- They must be a desktop, server, or laptop computer.
- They must have a Windows operating system.
- They must have enough free disk space to store the components and patches downloaded from the Panda Systems Management server.
- Port 13229 must be available for inbound communications

## Designating a local cache

To designate a repository/cache on your network, follow the steps below:

- Go to general menu **Sites**, and click the site to which the device you want to designate as a local cache belongs.
- Click **Devices** from the tab menu, and select the checkboxes of the devices to be designated as local cache.
- Click the 🖴 icon. If there are devices that do not meet the minimum system requirements, a warning message will be displayed.
- **Select the types of items to cache**: components and/or patches, as well as the drive on the device that will host the cached components.

## Configuring the behavior of local cache devices

- Click general menu **Sites** and then click the site for which you want to configure the behavior of local cache nodes. Next, click **Settings**.
- In section **Local Caches**, indicate the priority of each local cache node by dragging it from one position to another in the list.
- Specify the time that cached patches will remain on the local cache node.

## Removing a local cache

In addition to following the steps described in section “**Designating a local cache**”, you can also follow the steps discussed in section “**Configuring the behavior of local cache devices**” in order to quickly remove a local cache by clicking the ✖ icon.

# Chapter 6

# Device groupings

To streamline the management of mid-size to large networks, Panda Systems Management provides a flexible device grouping system based on the following resources:

- Sites
- Groups
- Filters
- Favorites

These resources differ from one another in their characteristics:

- The static or dynamic membership of the devices that comprise them.
- Device grouping scope.
- Ease with which the grouping can be modified and used along with other visualization and troubleshooting tools, such as monitors, jobs and status reports.

CHAPTER CONTENT

# Sites

All devices with the same network settings are susceptible of being grouped together within the same site. In geographically distributed companies with remote offices, each work center may have its own network resources, such as proxies, which modify the Internet connection methods of computers. These network settings are necessary for both the computers on the network and the PCSM agents installed on them to connect to resources outside the local network, including the Panda Systems Management server.

*Refer to section "**Hierarchy of levels within the Management Console**" on page **22** for more information on the Site level.*

## Creating a site

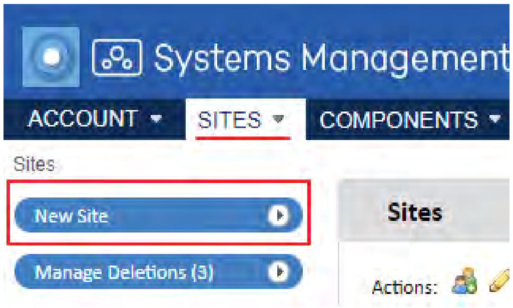


Figure 6.1: creating a site

- From general menu **Sites**, click the **New Site** button in the left-hand side panel.
- Enter a name and description for the site
- Configure the type of connection to be used by the devices in the site to access external resources. The selected proxy will be configured by default with the data provided on the **Settings** tab. Refer to "**Configuring a site's connectivity**" later in this chapter.
- Select the security levels that will be allowed to

access the site Refer to chapter "**User accounts and security levels**" on page **275** for more information about the user and security level structure in Panda Systems Management.

- Select the groups of sites to which the newly created site will be added. Use this option if there are devices at various geographically-distributed offices that require similar management procedures.

## Deleting a site

Go to general menu **Sites** and click the ✖ icon displayer to the right of the site to delete when hovering it with the mouse pointer.

> *Deleting a site with devices will deletes all those devices from the management console.*

## Moving computers from one site to another

- Click general menu **Sites** and select the site where the devices to move are located.
- Select the checkboxes next to the devices to move and click the **Move device(s) to different site** icon 🏠 A window will be displayed with all sites in the account and a text box for filtering and finding sites.
- Select a site and click the **Move** button.

## Configuring a site's connectivity

When you configure a site's Internet connectivity options, all computers in the site will automatically inherit the site's settings.

> *Configuration changes are not automatically inherited by a site's devices if they are made after the devices have been integrated into the site.*

- From general menu **Sites**, click the site whose settings you want to configure.
- Click **Settings** from the tab bar. In the **Proxy** section, configure the connection method and the credentials required to connect to resources outside the company network.
- Click **Save**.

### Listing created sites

To obtain a list of all created sites, click general menu **Sites**. A list will be shown of all sites in the console with the following information:

| Field | Description |
|---|---|
| **Name** | The site name. Clicking the link will take you to the Site level and all its resources. |
| **Description** | The site's description entered by the network administrator. |
| **ID** | Internal ID used by Panda Systems Management to identify the site. |
| **Devices** | Number of devices in the site. Clicking the link will take you to the Site level and all its resources. |
| **Offline** | Number of devices that have the PCSM agent installed but are not connected to the Panda Systems Management server. Click the link to view all offline devices in the site. |
| **Proxy** | Proxy settings assigned to the site. |

Table 6.1: fields in the Sites list.

# Groups

Groups are static device groupings. The membership of a device to a group is defined manually by the administrator (direct assignment). A single device can belong to more than one group.

The following types of groups are supported:

- **Site Device Groups / Site Device Filters**: These are groups created within a specific site. They can only contain devices that belong to the selected site.
- **Device Groups / Custom Device Filters**: These are groups created at Account Level. They can contain devices that belong to one, various or all sites.
- **Site Groups**: Created at Account Level, they are groups of full sites.

*Groups are often used as policy, monitor and job targets. If a group that is being used by any of those resources is deleted, the policies, monitors and jobs that are using it won't be able to resolve the target devices and therefore won't be run.*

## Site device groups

Site device groups contain devices belonging to the same site.

### Creating a site device group

- Go to general menu **Sites** and click the site in which you want to create the site device group.
- From the **Site Device Groups** panel on the side, click the **+** icon. A window will be displayed for you to enter the group name.

- Click **Save**.

### Assigning a device to a site device group

- From general menu **Sites**, click the site where the relevant device is located.
- Select the device by clicking the relevant checkbox.
- Click the **Add device(s) to group** 👥 icon. A window will be displayed, listing all available groups.

### Deleting a site device group

- From general menu **Sites**, click the site that the site device group belongs to.
- From the **Site Device Groups** panel on the side, click the ✖ icon displayed when hovering the mouse pointer over the group to delete.
- Click **OK**.

### Editing a site device group

- From general menu **Sites**, click the site where the site device group to edit is located.
- From the **Site Device Groups** panel on the side, click the ✏ icon displayed when hovering the mouse pointer over the group to edit.
- Enter a new name for the group, and its members.
- Click **Save**.

## Device groups

Device groups contain devices belonging to different sites.

### Creating a device group

- In general menu **Sites**, click the **+** icon from the **Site Groups** left-hand side panel. A window will be displayed for you to enter the group name.
- Click **Save**.

### Assigning a device to a device group

- From general menu **Sites**, click the site where the relevant device is located.
- Select the device by clicking the relevant checkbox.
- Click the **Add device(s) to group** 👥 icon. A window will be displayed, listing all available device.

### Deleting a device group

- Go to general menu **Sites**.
- From the **Device Groups** panel on the side, click the ❌ icon displayed when hovering the mouse pointer over the group to delete**.**
- Click OK.

### Editing a device group

- Go to general menu **Sites**.
- From the **Device Groups** panel on the side, click the ✏ icon displayed when hovering the mouse pointer over the group to edit.
- Enter a new name for the group and its members.
- Click **Save**.

## Site groups

Site groups contain all devices belonging to the sites included in a group.

### Creating a site group

- In general menu **Sites**, click the ⊕ icon from the **Site Groups** left-hand side panel. A window will be displayed for you to enter the group name.
- Click **Save**.

### Assigning a site to a site group

- Click general menu **Sites**, and use the checkboxes to select the sites to be included in the group.
- Click the **Add site(s) to site group** 👥 icon from the icon bar. A window will be displayed, listing all available groups.

### Deleting a site group

- Go to general menu **Sites**.
- From the **Site Groups** panel on the side, click the ❌ icon displayed when hovering the mouse pointer over the group to delete.
- Click **OK**.

### Editing a site group

- Go to general menu **Sites.**
- From the Site **Groups panel** on the side, click the ✎ icon displayed when hovering the mouse pointer over the group to edit.
- Enter a new name for the group, and its members.
- Click **OK**.

# Filters

The filters are dynamic groups of devices. Whether a device belongs to a certain filter or not is determined automatically when the device in question meets the criteria established by the administrator for that specific filter. A device can belong to more than one filter.

The following types of filters are supported:

- **Site Device Groups / Site Device Filters**: These are groups created within a specific site. They can only contain devices that belong to the selected site.
- **Device Groups / Custom Device Filters**: These are groups created at Account Level. They can contain devices that belong to one, various or all sites.
- **Device filters**: these are predefined groupings available at both Account and Site level.

*Filters are often used as policy, monitor and job targets. If you attempt to delete a filter that is being used by any of those resources, the management console will display a warning message. If the filter is finally deleted, the policies, monitors and jobs that are using it won't be able to resolve the target devices and won't be run.*

## Device filters

Panda Systems Management includes a set of predefined filters that simplify the organization and location of devices registered in the service.

*The filters listed below refer to devices managed by Panda Systems Management. That is, they only show devices already integrated in the management Console.*

Predefined devices are grouped into the following categories:

| Group | Description |
|---|---|
| **Application** | Shows devices with the following applications installed: Adobe Flash, Java, Microsoft Office and others. |
| **Backup Solution** | This group contains filters for backup solutions such as Backup Exec, StorageCraft, Veeam. |
| **Compliance** | These are filters that display the devices that need to be checked by the administrator due to a shortage of memory space, disabled antivirus, pending restarts, etc. |
| **Network** | Shows filters displaying network resources (routers, switches, firewalls, NAS and SAN devices, etc.) from the most popular vendors. |
| **Operating System** | These filters display devices in accordance with the operating system they have installed. |
| **Role** | These filters display servers in line with their role. |
| **Security Software** | These filters display devices in accordance with the security solution installed. |
| **Status** | This group identifies devices according to their status (switched on/off, network node, etc.). |
| **Type** | These filters identify devices by their type (ESXi servers, smartphones, tablets, etc.). |

Table 6.2: Predefined filters type

Below you will find a detailed description of each filter.

| Category | Filter | Use |
|---|---|---|
| **Application** | **Adobe Flash** | Shows devices with the Adobe Flash plugin installed. |
| | **Box.Net** | Shows devices with Box.net installed. |
| | **Dropbox** | Shows devices with Dropbox installed. |
| | **Google Chrome** | Shows devices with Google Chrome installed. |
| | **Java** | Shows devices with Java framework installed. |
| | **Microsoft Office** | Shows devices with the Microsoft Office suite installed. |
| | **Mozilla Firefox** | Shows devices with the Mozilla Firefox browser installed. |
| | **SQL Express** | Shows devices with the Microsoft SQL Express personal database installed. |

Table 6.3: List of predefined filters

| Category | Filter | Use |
|---|---|---|
| Backup Solution | Acronis TrueImage | Shows devices with file backup system installed. |
| | Ahsay | Shows devices with file backup system installed. |
| | Backup Exec | Shows devices with file backup system installed. |
| | StorageCraft | Shows devices with file backup system installed. |
| | Veeam | Shows devices with file backup system installed. |
| Compliance | < .NET 4.0.3 | Shows Windows devices with .NET Framework installed, versions 1.x, 2.x, 3.x, 4.0.0, 4.0.1 and 4.0.2. |
| | < 2 GB Free Space | Shows devices with less than 2 Gigabytes of free space on any of their hard disks. |
| | < 2 GB Free Memory | Shows devices with less than 2 Gigabytes of RAM free. |
| | Antivirus Disabled | Shows devices with the antivirus disabled. |
| | No MS Office | Shows devices that don't have Microsoft Office installed. |
| | Reboot Required | Shows the devices that require a reboot in order to complete an action, such as the installation of security patches, etc. |
| | Suspended Devices | Shows suspended devices. |
| Network | Firewalls | Shows firewall devices from the following vendors: Fortigate, SonicWall and pfSense. |
| | NAS devices | Shows network-connected storage devices from the following vendors: QNAP and Synology. |
| | Routers | Shows router devices from the following vendors: Cisco, Huawei, Juniper, Netgear and ZyXEL. |
| | SAN devices | Shows storage area networks from the following vendors: Dell, EMC, HP and NetApp. |
| | Servers | Shows network-connected servers from the following vendors: Dell, Fujitsu and HP. |
| | Switches | Shows network-connected switches from the following vendors: Cisco, HP and Juniper. |
| | UPS devices | Shows network-connected uninterrupted power supply systems from the following vendors: APC. |

Table 6.3: List of predefined filters

| Category | Filter | Use |
|---|---|---|
| Operating System | All Desktop O/S | Shows all desktop devices. |
| | All Server O/S | Shows all server devices. |
| | All Windows Desktops | Shows desktop devices running Windows operating systems. |
| | All Windows servers | Shows servers running Windows operating systems. |
| | Apple iOS | Shows all devices with iOS (tablets and smartphones). |
| | Google Android | Shows all devices with Android (tablets and smartphones). |
| | Linux | Shows all devices with the Linux operating system. |
| Operating System | MS Win 10 | Shows all devices with Microsoft Windows 10. |
| | MS Win 7 | Shows all devices with Microsoft Windows 7. |
| | MS Win 8 | Shows all devices with Microsoft Windows 8. |
| | MS Win Server 2003 | Shows all devices with Microsoft Windows 2003. |
| | MS Win Server 2008 | Shows all devices with Microsoft Windows 2008. |
| | MS Win Server 2012 | Shows all devices with Microsoft Windows 2012. |
| | MS Win Server 2016 | Shows all devices with Microsoft Windows 2016. |
| | MS Win Vista | Shows devices running Microsoft Windows Vista operating systems. |
| | MS Win XP | Shows all devices with Microsoft Windows XP. |
| | mac OSX | Shows all devices with MAC OS X. |

Table 6.3: List of predefined filters

| Category | Filter | Use |
|---|---|---|
| Role | **DHCP Server** | Shows all devices that operate as a DHCP server on the network. |
| | **DNS Server** | Shows all devices that operate as a DNS server on the network. |
| | **Domain Controllers** | Shows all devices that operate as a domain controller on the network. |
| | **Exchange Servers** | Shows all devices that operate as an Exchange server on the network. |
| | **Hyper-V Server** | Shows all devices on the network that act as hosts for virtual machines, based on Microsoft Hyper-V technology. |
| | **IIS Webservers** | Shows all devices on the network that act as Web servers running Internet Information Server. |
| | **SQL Servers** | Shows all servers with SQL Server or Microsoft SQL Server Express on the network. |
| | **Share Point Servers** | Shows all devices on the network that act as Share Point servers. |
| | **WSUS Servers** | Shows all devices on the network that act as WSUS update servers. |
| Security Software | **AVG** | Shows all devices with AVG security software installed. |
| | **Avira** | Shows all devices with Avira security software installed. |
| | **ESET** | Shows all devices with ESET security software installed. |
| | **Kaspersky** | Shows all devices with Kaspersky security software installed. |
| Security Software | **McAfee** | Shows all devices with McAfee security software installed. |
| | **Panda** | Shows all devices with Panda security software installed. |
| | **Sophos** | Shows all devices with Sophos security software installed. |
| | **Symantec** | Shows all devices with Symantec security software installed. |
| | **Trend Micro** | Shows all devices with Trend Micro security software installed. |
| | **Webroot** | Shows all devices with Webroot security software installed. |

Table 6.3: List of predefined filters

| Category | Filter | Use |
|---|---|---|
| Status | Last Seen > 30 Days | Shows all devices that haven't been contacted in over 30 days. |
| | Network Node | Shows all devices that have the role of network node. Refer to section "Configuring a Network Node" on page 61 for more information about the Network node role. |
| | Offline > 1 Week | Shows switched off devices or devices that have been offline for more than one week |
| | Offline Desktop O/S | Shows all switched off or offline desktop computers. |
| | Offline Devices | Shows all switched off or offline devices. |
| | Offline Server O/S | Shows all switched off or offline servers. |
| | Online Desktop O/S | Shows all switched off or offline desktop devices. |
| | Online Devices | Shows all switched on or online device. |
| | Online Server O/S | Shows all switched on or online servers. |
| | Reboot > 30 Days | Shows all devices that haven't been rebooted in over 30 days. |
| Type | All Devices | Shows all devices managed by PCSM. |
| | All Laptops | Shows all laptop devices managed by PCSM. |
| | All Mobiles | Shows all smartphones managed by PCSM. |
| | All NAS devices | Shows all network storage devices managed by PCSM. |
| | All Network Devices | Shows all network devices managed by PCSM. |
| | All Network Printers | Shows all printers installed on the network and managed by PCSM. |
| | All Network Routers | Shows all routers installed on the network and managed by Panda Systems Management. |
| Type | ESXi | Shows the ESXi hosts (ESXi servers) managed by PCSM. |
| | Physical Servers | Shows all physical servers (not virtual) |
| | Virtual Machines | Shows all virtual servers managed by PCSM |

Table 6.3: List of predefined filters

*The predefined filters are not editable.*

## Account filters

Account filters can contain devices from any site.

### Creating an account filter

- In general menu **Sites**, click the ⊕ icon from the **Account filters** left-hand side panel. A window will be displayed for you to enter the following information:
  - Filter name.
  - Filter definition. Refer to section "**Filter composition**" later in this chapter.
  - Select the **Only select devices in the following sites** option to apply the filter only to those devices in specific sites, or select all sites through option **Select devices in all of my sites**.
  - To specify which management console users can have access to the filter, select the **Share this filter with users with the following security level(s)**: option.

> ⚠ *Console users can view the criteria of all filters shared with them. A filter can only be edited and deleted by the console user who created it.*

- Click **Save**.

### Deleting an account filter

- Go to general menu **Sites**.
- From the **Account filters** panel on the side, click the ✖ icon displayed when hovering the mouse pointer over the filter to delete.
- Click **OK**.

### Editing an account filter

- Go to general menu **Sites**.
- From the **Account filters** panel on the side, click the ✎ icon displayed when hovering the mouse pointer over the filter to edit.
- Edit the filter settings and click the **Save** button.

## Site filters

Site filters contain devices belonging to a single site.

### Creating a site filter

- Go to general menu **Sites**. Click the site the filter will be created in, and then click the + icon from the **Site filters** side panel. A window will be displayed for you to enter the following information:
  - Filter name.

- Filter definition. refer to section "**Filter composition**" for more information.
- To specify which management console users can have access to the filter, select the **Share this filter with users with the following security level(s)**: option**.**

> ⚠ *By default, filters can only be accessed by those users who create them. Users specified though the Share this filter option will only be able to access the lists of devices generated by the filter. They won't be able to edit or delete filters.*

- Click **Save**.

### Deleting a site filter

- In general menu Sites, click the site whose filter you want to delete.
- From the Site filters panel on the side, click the ✖ icon displayed when hovering the mouse pointer over the filter to delete.
- Click **Save**.

### Editing a site filter

- In general menu **Sites**, click the site whose filter you want to edit.
- From the Site filters panel on the side, click the ✎ icon displayed when hovering the mouse pointer over the filter to edit.
- Edit the filter settings and click the **Save** button.

## Filter composition

A filter is made up of one or more attributes which combine with each other through the logical operations AND / OR. A device forms part of a filter if it meets the criteria established in the attributes of the filter.

The general layout of the filter is divided into two blocks:

- **Filter name**. It is advisable for this to be a descriptive name that describes the characteristics of the devices (e.g. "Microsoft Exchange servers", "Workstations with limited disk space, etc.").
- **Criteria**: Here you can select the attributes that will be checked on each device and their value. For each attribute several values can be specified, which are taken into account based on the specified AND/OR values. Similarly, several attributes can be specified in the same filter which also relate to each other in line with the AND/OR values.

The criteria block is broken down into three parts:

- **Attribute**: Specifies the device characteristic that will determine whether it is part of a filter. The main attributes are listed and classified below.

- **Condition**: Establishes the way the device attribute is compared with the reference value set by the administrator.
- **Value**: The content of the attribute. Depending on the attribute the value field can change to allow terms such as dates, text, etc.

Below are the values available for each Criteria condition line:

| Field | Condition | Value |
|---|---|---|
| **String** | • Equals - Does not equal<br>• Empty - Not empty<br>• Contains - Does Not contain<br>• Starts with - Does not start with<br>• Finishes with - Does not finish with | String. Use % as a wildcard. |
| **Integer** | • Greater - Greater than or equal to<br>• Less - Less than or equal to<br>• Includes<br>• Excludes | Numeric. |
| **Binary** | • Enabled / Disabled | |
| **Date** | • Before - After<br>• Older than 30/60/90 days | Date interval. |
| **Selection** | Is a member of, is not a member of | Available Groups. |
| **Status** | The status is - The status is not | Available statuses. |

Table 6.4: Data types for filter attributes

To specify different values for an attribute, you have to click the ⊕ symbol to the right of the value field. This deploys a new control and an **AND**/**OR** button that lets you choose the relation: two values related with **AND** means that the device must have an attribute that complies with both fields. Two values related with **OR** means that the device must have an attribute that complies with at least one of the fields.

Finally, to apply more complex filters that can examine several attributes it is possible to add more Criteria blocks by clicking the ⊕ below, and repeating the process described above: the new Criteria can be related with the same **AND**/**OR** logic.

Below you can see the attributes available to create a Criteria block:

| Attribute | Description |
|---|---|
| **Windows Updates (Enabled/ Disabled)** | Lets you filter devices with the Windows Updates engine enabled or disabled. |

Table 6.5: filter attributes

| Attribute | Description |
|---|---|
| **Privacy Mode** | Lets you filters devices with Privacy Mode enabled. Refer to section "**Privacy Mode Options**" on page **98**. |
| **Display adapter** | Lets you filter by the name, make and model of the graphics card installed on your devices. |
| **Network adapter** | Lets you filter by the make and model of the network card installed on your devices. |
| **Attached device driver file** | Lets you filter by the **Driver file** field of the USB devices connected to your computers. For more information, refer to chapter "**Assets Audit**" on page **151**. |
| **Architecture** | Lets you filter devices by their architecture: 32-bit or 64-bit. |
| **CPU** | Lets you filter devices by the make and model of the CPU installed. |
| **Local cache** | Shows devices with the Network Node role assigned. For more information, refer to section "**Configuring a Network Node**" on page **61**. |
| **User-defined fields** | Lets you filter by the content of the specified user-defined field (1 to 30). Refer to section "**User-Defined fields**" on page **182** for more information on how to manually set the content of user-defined fields, and section "**Labels and user-defined fields**" on page **145** for more information on how to set it automatically. |
| **Disk size** | Lets you filter devices by the size of the hard disk. |
| **Disk freespace** | Lets you filter devices by the free space on the hard disk. |
| **Class** | |
| **Attached device driver modified** | Lets you filter by the Driver modified field of the external USB devices connected to your computers. For more information, refer to chapter "**Assets Audit**" on page **151**. |
| **Description** | Lets you filter devices by the value of the **Description** field. |
| **SNMP description** | Lets you filter by the description field of your devices' SNMP settings. |
| **Site description** | Lets you filter by the **Description** field of the site to which your devices belong. |
| **Disk description** | Lets you filter by the description string of the internal storage devices connected to your devices. |
| **IP address** | Lets you filter by the IP address assigned to your devices' primary network interface. |
| **Additional IP address** | Lets you filter by IP alias. |
| **External IP address** | Lets you filter devices by the IP address used to connect to the server. Generally, this is the public address of the router that implements the proxy and/or traffic NAT processes. |

Table 6.5: filter attributes

| Attribute | Description |
|---|---|
| **MAC address** | Lets you filter by the physical address assigned to your devices' primary network interface. |
| **Managed device** | Not used. |
| **OnDemand Device** | Not used. |
| **Domain** | Lets you filter devices by the domain to which they belong on Microsoft networks. |
| **Site is OnDemand** | Not used. |
| **Status - Online/Offline** | Filters devices connected to the Panda Systems Management server. |
| **Status - Web port OK** | Not used. |
| **Status - Suspended** | Shows those devices that have entered power saving status. |
| **Patch Status** | Lets you filter devices by their patch status: **No Policy**, **No Data**, **Reboot Required**, **Install Error**, **Approved Pending**, **Fully Patched**. |
| **Antivirus Status** | Lets you filter devices by the status of the antivirus product installed: **Running & up-to-date**, **Running & not up-to-date**, **Not running**, **Not detected**. |
| **Manufacturer** | Lets you filter by the name of the manufacturer that assembled your devices. |
| **NIC manufacturer** | Lets you filter by the name of your devices' network interface manufacturer. |
| **Attached device driver manufacturer** | Lets you filter by the Driver manufacturer field of the external USB devices connected to your devices. For more information, refer to chapter "**Assets Audit**" on page **151**. |
| **Favorite** | Lets you filter by those devices marked as favorite. Refer to section "**Favorites**" later in this chapter. |
| **Warranty expiration date** | Lets you filter devices by the expiration date entered. |
| **BIOS release date** | Lets you filter devices by their BIOS release date. |
| **Last seen date** | Shows those devices seen by the Panda Systems Management server on the specified date. |
| **Windows Firewall** | Lets you filter devices by firewall status (enabled/disabled). |
| **Device group** | Lets you filter devices by the name of the device group they belong to. |
| **Site device group** | Lets you filter devices by the name of the site device group they belong to. |
| **Site group** | Shows those devices that belong to the specified site group. |

Table 6.5: filter attributes

| Attribute | Description |
|---|---|
| **Memory** | Lets you filter devices by the amount of memory installed on them. |
| **Model** | |
| **Create date** | Lets you filter devices by the date they were added to the system. |
| **Monitor / Screen** | Lets you filter devices by the manufacturer of the monitor connected to them. |
| **Reboot required** | Lets you filter by those devices that require a restart to complete a program or patch installation job, component update job, etc. |
| **Network node** | Shows devices with the Network Node role assigned. Refer to section "**Configuring a Network Node**" on page **61**. |
| **Bios name** | Lets you filter devices by the BIOS manufacturer name. |
| **Site name** | Lets you filter devices by the name of the site they belong to. |
| **Service Display Name** | Lets you filter devices by the description field of the service installed on them. |
| **Attached device driver name** | Lets you filter devices by the **Driver name** field of the external USB devices connected to them. For more information, refer to chapter "**Assets Audit**" on page **151**. |
| **Attached device name** | Lets you filter devices by the **Name** field of the external USB devices connected to them. For more information, refer to chapter "**Assets Audit**" on page **151**. |
| **Host name** | |
| **Patch Name (approved and pending)** | Filter the devices by the name of patches that have been approved but not yet installed. |
| **Patch Title (installed)** | Lets you filter devices by the name of a patch installed on the device. |
| **Patch Name (not approved)** | Filter the devices by the name of patches that have been excluded. |
| **Antivirus product name** | Filters by the commercial name of the antivirus product installed on the device. |
| **Service name** | Filter by the name of the service installed on the device. |
| **Name / version of the controller of the connected device** | Filter by the field Name of the controller of the external USB devices connected to the equipment. Refer to chapter "**Assets Audit**" on page **151**, for more information. |
| **Physical cores** | Filters by the number of cores that the device microprocessor implements. |
| **Serial number** | Lets you filter by the device serial number. |
| **Software package** | Lets you filter by the software package installed on the device. |
| **Software package/version** | Lets you filter by the software package and version installed. |

Table 6.5: filter attributes

| Attribute | Description |
|---|---|
| **Approved patches pending** | Filters devices that have the specified number of approved patches pending installation. |
| **Patches installed** | Filters devices that have the specified number of patches installed. |
| **Unapproved Patches** | Filters devices that have the specified number of excluded patches. |
| **Motherboard** | Filter by the manufacturer, make and model of the device's motherboard. |
| **Connected device port** | Filter by the Port name field of external USB devices connected to the computer. Refer to chapter "**Assets Audit**" on page **151** for more information. |
| **Service Pack** | Filter by the version of the Service Pack installed on Windows computers. |
| **Operating system** | Filter by the name and version of the operating system installed on the devices. |
| **Device type** | Filter by device type: **Unknown**, **Desktop**, **Laptop**, **Server**, **Smartphone**, **Tablet**, **Printer**, **Network device**, **ESXi Host**. |
| **Type of connected device** | |
| **SNMP location** | Filters according to the contents of the Location SNMP configuration field set on the device. |
| **.NET version** | Filters by the version of the .NET framework installed on the devices. |
| **BIOS version** | Filter by the BIOS version number installed on the devices. |
| **Software version** | Filters by the version of a software package installed on the computer. |
| **Agent version** | Filters by the version of the PCSM agent installed on the device. |
| **Attached device driver type** | Filter by the driver / version field of external USB devices connected to the device. Refer to section "**Assets Audit**" on page **151** for more information. |
| **Last audit** | Date of the most recent hardware/software audit on the device. Refer to Chapter 12: Assets Audit for more details. |
| **Last reboot** | Filters the devices whose last reboot occurred in certain periods of time. |
| **Last user** | Lets you filter devices by the last user to log on to the device. |

Table 6.5: filter attributes

# Favorites

Favorites are a grouping resource that allows administrators to quickly access those devices requiring continuous special attention. This type of grouping cannot be used with jobs, policies, monitors or reports.

## Marking and unmarking a device as favorite

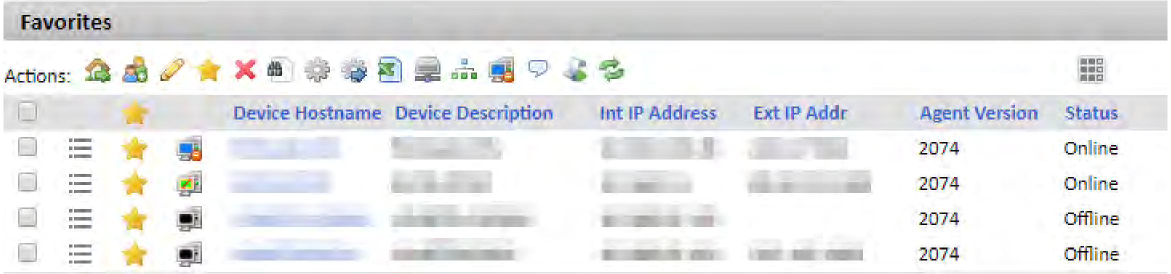
Use the ★ icon on the icon bar to mark or unmark one or more devices as favorite. You can do this from:

- A specific site, by clicking **Devices** from the tab bar.
- A site group, site filter or device filter.

## Accessing devices marked as Favorite

The Favorites section is found on the dashboard displayed at Site level:

- Go to general menu **Sites** and click one of your managed sites.
- Click **Summary** from the tab menu. Scroll down to the Favorites section. This section displays all devices marked as favorite, along with an icon bar for launching jobs, performing audits or generating reports, among other actions.



Favorites

| □ | | ★ | | Device Hostname | Device Description | Int IP Address | Ext IP Addr | Agent Version | Status |
|---|---|---|---|---|---|---|---|---|---|
| □ | ☰ | ★ | | [redacted] | [redacted] | [redacted] | [redacted] | 2074 | Online |
| □ | ☰ | ★ | | [redacted] | [redacted] | [redacted] | [redacted] | 2074 | Online |
| □ | ☰ | ★ | | [redacted] | [redacted] | [redacted] | | 2074 | Offline |
| □ | ☰ | ★ | | [redacted] | [redacted] | [redacted] | [redacted] | 2074 | Offline |

Figure 6.2: access to favorite section

# Managing devices efficiently

The way an MSP with multiple customer accounts or an IT department with various offices organizes managed devices in the Console drastically affects efficiency, as many procedures and actions can be configured to run simultaneously on many devices through the right combination of sites, groups, and filters.

Below is a description of the benefits and limitations of the three grouping methods supported.

## Sites

### Benefits

- They associate the same Agent Internet connection settings to all devices: avoid having to manually configure the Agent for each device locally.
- They link email contact information for sending reports, alerts, tickets, etc.
- They can access the Tab bar and the Icon bar, allowing execution of actions and display lists and consolidated reports that cover all of the devices in the site conveniently and rapidly.

### Limitations

- A device can only belong to one site.
- It is not possible to nest a site within a site.

## Filters and groups

### Benefits

- Groups/filters let you create subsets of devices within one or more sites.
- A device can belong to various groups/filters.

### Limitations

- Groups/filters have limited functionality as the Tab bar is not accessible, so it is not possible to generate lists with consolidated information regarding the members of the group or filter.
- Access to reports is limited; the reports generated will only contain information about one device.

*Groups/filters are actually sites within sites (as many as you like) but have limited access to consolidated reports and the Tab bar.*

# General organization of devices

Apply the following guidelines for generating an organizational structure of devices that simplifies asset management:

- **Group devices in sites to separate the devices belonging to different customer accounts**

Sites do not impose any inherent limitations on generating consolidated reports or lists and allow settings to be applied to all of the devices belonging to a site.

- **Create device groups to group devices with similar hardware / software / configuration / usage**

**characteristics**

For example, configure device groups to separate devices with similar needs (software used, general requirements, printer access, etc.) within a customer account by department or by role (Servers/ Workstations).

- **Create filters to find computers with a common status within a site**

Use filters to quickly and automatically search abnormal conditions that do not fall within predetermined thresholds (insufficient disk space, little physical memory installed, software not allowed, etc.) or to find devices with specific features.

*It is not advisable to use filters for static type groups.*

- **Create groups at Account Level to group sites**

If there are customer accounts or offices with very similar characteristics and a variety of devices, you can group them in the same group at Account Level to ease management.

- **Associate Account Level groups and filters to technical profiles**

If an MSP or company is medium to large in size, a time will come when its technicians will become more specialized. In this case, there will be technicians who only manage certain types of devices, such as Exchange Servers or Windows XP workstations. An Account Level group or filter helps locate and group these devices without having to go site by site to find them. To complete the scenario, it is advisable to create and configure security levels and new user accounts, as described in "**User accounts and security levels**" on page **275**.

- **Mark as favorites those devices you access frequently**

Problematic devices that require constant monitoring by the administrator are more likely to belong to the **Favorites** group. Once those problems are resolved, remove them from the **Favorites** section so that this area is kept as tidy as possible and to ease and expedite access to other problematic devices.

# Part 3

# Automatic process configuration on devices

**Chapter 7:** Policies

**Chapter 8:** Monitoring

**Chapter 9:** Jobs

**Chapter 10:** Components and ComStore

# Chapter 7

# Policies

Policies are specific processes for managing or resolving incidents. They can affect one or more managed devices and can be scheduled to be repeated at regular intervals over a specific period of time, or triggered when certain conditions are met on the targeted device.

Policies are settings templates made up of:

- **Targets**: Groups of devices to which the policy will be applied.
- **Services**: Depending on the policy type, the Agent will perform a specific series of actions on each device.

Policies can be created at the three available levels, based on whether the targeted devices belong to the same site (customer/office) or to multiple sites:

- **Account policy**: Defines an action to apply to Device groups, Site groups or Custom Device Filters.
- **Site policy**: Defines an action to apply to Site Device Filters o Site Device Groups.
- **Device policy**: Defines an action to apply to a specific device.

*Refer to chapter "**Device groupings**" on page **69** for more information about the various types of groupings supported by Panda Systems Management.*

CHAPTER CONTENT

# Managing policies

## Creating policies

Follow the steps below to create a policy:

- Define the scope or level of the policy based on the target devices.
- To create an account policy, go to general menu **Account**, **Policies** tab, and click the **New account policy** button at the bottom of the window.
- To create a site policy, go to general menu **Sites**, select the relevant site, click the Policies tab, and then click the **New site policy** button at the bottom of the window.
- To create a device policy, go to general menu **Sites**, and then click the site where the device is located. Click the device that the policy will be assigned to and click the **Monitor** tab. Then, click the **Monitors** radio button.

> *At Device level you can only add monitor-type policies. Refer to chapter "**Monitoring**" on page **105** for more information on how to create a monitor type policy.*

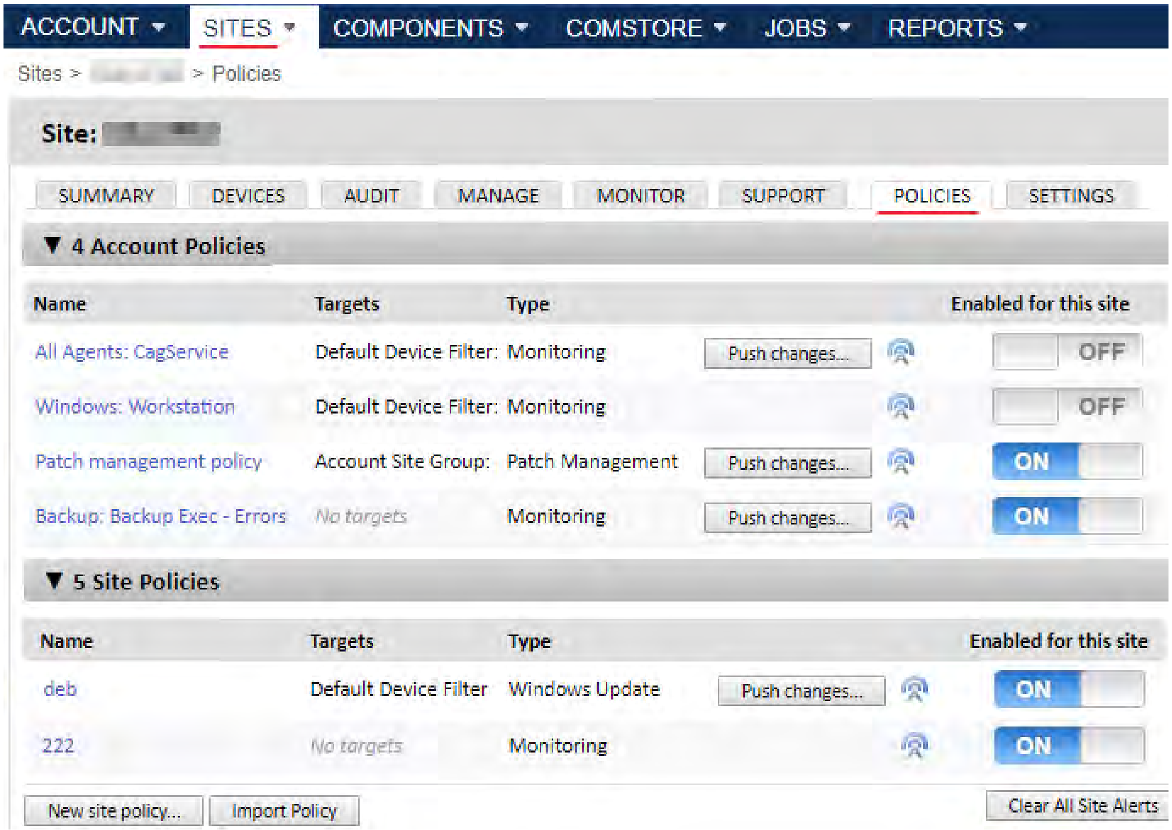
- Enter the name of the policy, its type, and whether it will be based on another policy created earlier to ease the creation process.
- Enter the data required to configure the policy based on the policy type selected. More information about the policy types supported by Panda Systems Management is provided later in this chapter.
- Add the policy target (groups or filters), depending on its Level (Account, Site or Device).
- To complete the policy creation process, click **Save and push changes** to save and run the policy.

## Managing created policies

Since policies can be created at three levels, it may be difficult to determine which groups of devices are being targeted by a specific policy, or if there are overlapping problems between policies created at different levels.

## Managing policies

- To list all policies created at **Account** level, go to general menu Account and click **Policies** from the tab menu.
- To list all policies created for a site (this will include Site-level and Account-level policies), follow the steps below.
    - Click general menu **Sites**, and then click the site whose policies you want to manage.
    - Click **Policies** from the tab menu.
    - To list the monitors assigned to a device and created at Account, Site, and Device level, follow the steps below:
    - Click general menu **Sites**, and then click the site where the device is located.
    - Click the device whose monitoring policies you want to manage.
    - Click **Monitor** from the tab bar. Click the **Monitors** selection control in the top right corner of the window.



▼ 4 Account Policies

| Name | Targets | Type | | Enabled for this site |
|---|---|---|---|---|
| All Agents: CagService | Default Device Filter: | Monitoring | Push changes... | OFF |
| Windows: Workstation | Default Device Filter: | Monitoring | | OFF |
| Patch management policy | Account Site Group: | Patch Management | Push changes... | ON |
| Backup: Backup Exec - Errors | No targets | Monitoring | Push changes... | ON |

▼ 5 Site Policies

| Name | Targets | Type | | Enabled for this site |
|---|---|---|---|---|
| deb | Default Device Filter | Windows Update | Push changes... | ON |
| 222 | No targets | Monitoring | | ON |

Figure 7.1: list of policies assigned at Site level

The list of policies created at Account and Site level includes the fields shown in table **7.1**. To view the fields displayed in the Monitors list at Device level, refer to section "**Managing monitors**" on page **120**.

| Field | Description |
|---|---|
| **Icon** ● | The Patch Management policy defined at Account level is overridden at the current Site level. This only appears with Patch Management policies defined at Account level and managed at Site level. Refer to section "**Overriding the policies defined at Account Level**" on page **217** for more information about policy inheritance. |
| **Name** | The name of the policy. |
| **Targets** | Groups of devices to which the policy will be applied. |
| **Type** | Policy class. Refer to section "**Policy types**" on page **97** later in this chapter. |
| **Edit override** | Lets you edit the policy inherited from the Account Level. This option is only displayed for Patch Management policies defined at Account Level and managed at Site Level. Refer to chapter "**Overriding the policies defined at Account Level**" on page **217** for mere information about the policy inheritance. |
| **Push changes** | Deploys the policy to all devices selected as a target. |
| **Icon** 📡 | Lets you view the devices that will receive the policy. |
| **Enabled for this site** | Enables/disables the policy for the entire site or account. |
| **Delete** ✕ | Deletes the policy. |
| **Enabled** ON | Enables/disables the policy. |

Table 7.1: Policies table columns

## Listing policy targets

Click the 📡 icon to go to the Policy associations screen. There you can view a list of all devices affected by the policy:

| Filter | Description |
|---|---|
| **Site exclusions** | Sites excluded from the policy. |
| **Site manually enabled** | Sites manually enabled for the policy. |
| **All Devices** | Devices associated with the policy. |
| **Devices which currently have the policy applied** | Devices which currently have the policy applied. |
| **Excluded Devices** | Devices which are currently excluded from the policy. |

Table 7.2: policy targets

### Exclude and include zones in an account policy

Account policies can use zone groups as a destination to be distributed across all devices integrated in different zones within the account.

### How to deploy a policy

After a policy has been created, a line will be added to the site's screen.

To deploy the policy to the target devices, click the **Save and push changes** button. This saves the policy and deploys it immediately to all target devices, running it.

# Policy types

There are eight types of policies, summarized below:

| Policies | Description |
|---|---|
| **Agent** | This type of policy allows you to specify the Agent appearance, as well as the functionality features available to the user. |
| **ESXi** | This policy allows administrators to create and assign monitors to ESXi servers to monitor performance, data storage capacity and temperature. |
| **Monitoring Maintenance Window** | Maintenance policies let you define a period of time during which any alerts generated on devices won't create email notifications or tickets. |
| **Mobile Device Management** | Mobile Device Management (MDM) lets you establish policies for iOS devices (tablets and smartphones). These policies allow you to restrict the use of such devices. |
| **Monitoring** | This policy allows you to add device resource monitoring processes. |
| **Patch management** | Patch management is one of the tools available in Panda Systems Management for downloading and installing software patches. |
| **Power** | This policy allows configuration of the power saving settings on the devices that support them. |
| **Windows update** | Windows Update is a transposition of the options available on a WSUS server and allows the most common Patch Management options to be configured for Microsoft systems. |
| **Software management** | Make sure your managed devices comply with the software installation policies set by your company and update your programs to the latest versions published by software vendors. |

Table 7.3: available policies and description

## Agent

This type of policy allows you to specify the Agent appearance, as well as the functionality features available to the user.

## Privacy Mode Options

- **Activate Privacy Mode**: Enabling the privacy mode allows the user of a device to accept or deny the administrator's attempts to remotely access it. Whenever the privacy mode is enabled on a device, it will be necessary to get the user's permission before being able to use the remote management tools (remote desktop, screenshots, remote shell, service management, etc.).

*Once enabled, only the user can disable the privacy mode from the right-click menu of the Agent installed on their device.*

- **Allow connections when no user is logged in**: Provided the privacy mode is enabled, this option allows administrators to connect to a device when no user is logged in to allow or deny the access attempt.
- **Only require permission for Restricted Tools**: Configures the privacy mode so that the customer will only receive confirmation requests when the administrator tries to access the remote desktop, either interactively or to take screenshots. Any other remote management tools will not require permission from the user to be used by the administrator.

## Service options

- **Install service only**: this option hides the icon displayed in the notification area (in the bottom right corner of Windows desktops ), preventing the user from accessing the settings screens.
- **Disable incoming jobs**: Prevents the execution of jobs on the device.
- **Disable incoming support**: Disables remote access to the device.
- **Disable audits**: Prevents selected devices from sending hardware/software audit data.

## Agent Policy Options

- Disable Privacy Options: Prevents users from accessing the privacy options accessible from the Agent's options menu.

*It is not possible to disable the privacy options if the privacy mode is enabled, as the only way to disable the privacy mode is through the Agent's privacy options.*

- **Disable Settings menu**: Prevents users from accessing the Settings menu displayed on right-clicking the Agent's icon.
- **Disable Quit Options**: prevents the user from closing the PCSM agent.
- **Disable Tickets tab**: Disables the Agent's Tickets tab.
- **Agent Browser Mode**: Lets you set the way the Agent is run.

- **Disabled**.
- **User**: The Agent won't show the Support window and therefore will prevent users from logging in administrator mode. This is the normal execution mode of the PCSM agent in order to manage network devices.
- **Admin**: The Agent is run will full permissions. This is the execution mode for network administrators using the PCSM agent to resolve problems with the remote access tools. Refer to chapter "**Remote access tools**" on page **257** for more information.

## ESXi

This policy allows administrators to create and assign monitors to ESXi servers to monitor performance, data storage capacity and temperature.

*Refer to chapter "**Monitoring**" on page **105** for more information.*

## Monitoring Maintenance Window

Maintenance policies let you define a period of time during which any alerts generated on devices won't create email notifications or tickets.

*Emails and tickets are actions generated in response to policies. These actions will be suspended while a Monitoring Maintenance Window is enabled. However, other actions, such as the execution of components will continue to be generated.*

These policies are used when the IT department has to carry out maintenance on the IT network over a long period of time; during this period, the alerts could create unnecessary noise.

## Mobile Device Management policies

In order to manage and control the use of mobile devices, Panda Systems Management offers a set of policies that let you configure iOS-based smartphones and tablets to ensure that, from the outset, users have devices that are ready for use in corporate environment and can be integrated in the company's infrastructure.

*Only one Mobile Device Management policy can be enabled at any given moment.*

### Mandatory and optional policies

At the time of creating the policy, administrators have to establish whether the policy is mandatory or not. This way, in the policy creation screen you can choose between **Allow users to remove this policy** if users will be able to manually disable the policy from their mobile device, or **Require password to remove this policy** if you want to make disabling the policy subject to entering the password set by the administrator.

## Types of Mobile Device Management policies

There are four types of MDM policies available, each of which affecting a series of features and settings on the mobile device.

- **Passcode**: Characteristics of the passwords entered by the user in the mobile device to lock the device, etc.
- **Restriction**: Management of access to device resources.
- **VPN**: VPN settings.
- **Wi-Fi**: Wi-Fi connection settings.

### Passcode

| Field | Description |
|---|---|
| **Passcode strength** | Lets you define the minimum strength for user's passcodes. |
| **Minimum passcode length** | Lets you set the minimum number of characters a passcode must contain. |
| **Minimum Number Of Complex Characters** | Lets you set a minimum number of non-alphanumeric characters for valid passcodes. |
| **Maximum Passcode Age** | Lets you set the maximum valid period for a passcode. |
| **Auto Lock** | Lets you set the maximum number of minutes that the device can be idle before locking the screen. Enter a value between 2 and 5 minutes to apply the policy on both Android and iOS devices. |
| **Passcode History** | The device keeps a history of passcodes used by users to prevent them from being re-used when choosing a new passcode. |
| **Maximum Number Of Failed Attempts** | Lets you set the number of passcode entry attempts allowed before all data on the device will be erased. |

Table 7.4: passcode settings

### Restrictions

| Field | Description |
|---|---|
| **Allow use of camera** | Cameras are completely disabled and the icons are removed from the home screen. Users cannot take photos, video or use FaceTime. |

Table 7.5: usage restrictions settings for iOS devices

| Field | Description |
|---|---|
| **Allow installing apps** | Using this option App store can be disabled and the App store icon will be removed from the home screen. Users will not be able to install or update any apps using App store of iTunes.. |
| **Allow screen capture** | Allows users to capture a screenshot of the display. |
| **Allow voice dialing** | Allows users to use voice dialing. |
| **Allow FaceTime** | Allows users to receive or make FaceTime video calls. |
| **Allow automatic sync when roaming** | Devices while roaming will sync only when an account is accessed by the user. |
| **Allow Siri** | Allows use of Siri. |
| **Allow Siri while locked** | Permits use of Siri when the device is locked. |
| **Allow Passbook notifications while locked** | Permits the use of Passbook while the device is locked. |
| **Allow in-app purchases** | Enables in-app purchases. |
| **Force users to enter iTunes Store password for all purchases** | Prompts for the iTunes password for every download. |
| **Allow multiplayer gaming** | Allows multi-player gaming. |
| **Allow adding Game Center friends** | Allows users to add Game Center friends. |
| **Show Control Center in lock screen (iOS 7)** | Allows users to access Control Center when the device is locked. |
| **Show Notification Center in lock screen (iOS 7)** | Displays Notifications Center when the device is locked. |
| **Show Today view in lock screen (iOS 7)** | Displays the Today view in Notifications Center when the device is locked. |
| **Allow documents from managed apps in unmanaged apps (iOS 7)** | Allows users to share and use the data from a corporate app to a personal app which is not distributed by the company. |
| **Allow documents from unmanaged apps in managed apps (iOS 7)** | Allows users to share and use the data from a personal app to a corporate app which is distributed by the company. |
| **Allow use of iTunes Store** | Allows users to use iTunes Store. |
| **Allow use of Safari** | Allow users to use Safari. |
| **Enable Safari autofill** | Enables the auto-fill option |
| **Force Safari fraud warning** | Safari warns users when visiting fraudulent or dangerous websites. |
| **Enable Safari Javascript** | Allows Javascript. |
| **Block Safari popups** | Enables pop-ups. |
| **Allow iCloud backup** | Enables data backup. |

Table 7.5: usage restrictions settings for iOS devices

| Field | Description |
|---|---|
| **Allow iCloud document sync** | Allows document sync. |
| **Allow iCloud Keychain sync (iOS 7)** | Allows automatic synchronization with iCloud of user names, passwords, credit card numbers, etc. |
| **Allow photo stream** | Enables photo streams. |
| **Allow shared stream** | Enables stream sharing. |
| **Allow diagnostic data to be sent to Apple** | Enables diagnostic data to be sent to Apple. |
| **Allow user to accept untrusted TLS certificates** | Allows the use of untrusted TLS certificates. |
| **Force encrypted backup** | Forces encryption of backup data. |
| **Allow automatic updates to certify trust settings (iOS 7)** | Allows trusted certificates to be updated automatically. |
| **Force limited ad tracking (iOS 7)** | Allows users to limit ad tracking on the device. |
| **Allow fingerprint for unlock (iOS 7)** | Allows users to unlock their devices with their fingerprints. |
| **Allow explicit music and podcasts** | Allows explicit music and podcasts. |
| **Rating Apps** | Allows or blocks apps based on the specified ratings. |
| **Rating Movies** | Allows or blocks movies based on the specified ratings. |
| **Rating Movies** | Allows or blocks movies based on the specified ratings. |
| **Show iMessage** | Allows users to use iMessage. |
| **Allow app removal** | Allows uninstallation of apps. |
| **Allow Game Center** | Allow Game Center. |
| **Allow Bookstore** | Permits the use of iBooks. |
| **Allow Bookstore erotica** | Enables users to download media tagged as erotica. |
| **Allow UI configuration profile installation** | |
| **Allow modifying account settings (iOS 7)** | Allows users to modify their account settings: add or remove mail accounts, modify iCloud feature settings, iMessage feature settings, etc. |
| **Allow AirDrop (iOS 7)** | Allows users to share documents with AirDrop, |
| **Allow changes to cellular data usage for apps (iOS 7)** | Allows users to turn off cellular data for specific apps. |
| **Allow user-generated content in Siri** | Allows Siri to query content from the web (Wikipedia, Bing and Twitter). |

Table 7.5: usage restrictions settings for iOS devices

| Field | Description |
|---|---|
| **Allow modifying Find My Friends settings** | Allows users to change the "Find my Friends" settings. |
| **Allow host pairing** | Allows devices to be paired with other devices. If this option is disabled, it will only be possible to pair the device with a host with Apple Configurator. |

Table 7.5: usage restrictions settings for iOS devices

### VPN

| Field | Description |
|---|---|
| **Connection name** | Name of the VPN connection. |
| **Connection type** | VPN type (L2TP, PPTP, IPSec). |
| **Server** | VPN server IP address. |
| **Shared Secret** | Secret shared between the server and the client. |
| **User Authentication** | Authentication method: password or public/private key. |
| **Account** | User account for authenticating the connection. |
| **Proxy Type** | Proxy to be used with the VPN connection. |

Table 7.6: VPN settings

### Wi-Fi

| Field | Description |
|---|---|
| **SSID** | Sets the Service Set IDentifier. |
| **Security** | Type of Wi-Fi security. |
| **Password** | Wi-Fi password. |
| **Proxy Tipe** | Proxy to be used with the Wi-Fi connection. |

Table 7.7: WiFi connection settings

## Monitoring

This policy allows you to add device resource monitoring processes.

*Refer to chapter "**Monitoring**" on page **105** for more information.*

# Patch management

Patch management is one of the tools available in Panda Systems Management for downloading and installing software patches.

*Refer to chapter "***Patch Management***" on page* **203** *for more information.*

# Power

This policy lets you configure the energy saving settings of the devices that support them.

- **Turn off disk after**: turns off the hard disk after it has been idle for the selected time interval.
- **Turn off display after**: turns off the display after the machine has been idle for the selected time interval.
- **Standby after**: puts the computer into sleep mode after it has been idle for the selected time interval.
- **Schedule**: lets you either disable the Schedule feature, or set a time to put the computer into Sleep, Hibernate or Shutdown each day.

# Windows update

Windows Update is a transposition of the options available on a WSUS server and allows the most common Patch Management options to be configured for Microsoft systems.

*Refer to chapter "***Patch Management***" on page* **203** *for more information.*

# Software management

Lets administrators choose which applications will be installed and updated on the computers on the network in order to comply with the software policies set by the company.

*For more information, refer to chapter "***Software Management***" on page* **233**.

# Chapter 8

# Monitoring

Monitoring is a policy that detects failures on users' devices unattended. This allows the IT administrator to configure monitors on users' devices that warn of abnormal situations and automatically launch alerts or scripts to correct them, all without human intervention.

CHAPTER CONTENT

# Creating monitors manually

## Policies, monitors, and access to the monitoring feature

In most cases, monitors are created within the framework of a monitoring policy, which can contain one or more monitors. Each monitor monitors a specific aspect of the targeted device. Monitors can be grouped in the same policy in order to minimize the number of configurable items for the administrator and simplify management.

As indicated in chapter "**Policies**" on page **93**, policies define a series of services or jobs that are repeatedly run on the targeted devices (in this case, the service to run is a monitor), and those devices. However, it is possible to create monitors outside the framework of a policy at Device level. Therefore, you can manually create monitors at the three levels available in the console, depending on the devices to be monitored:

- Go to the general menu **Account**, click Policies from the tab bar, and click **New account policy**.
- From a specific site, click **Policies** from the tab bar, and click **New site policy**.
- From a specific device, click **Monitor** from the tab bar, and click **Monitors**.

## Monitor composition

A monitor consists of four groups of settings:

- **Monitor type**: Specifies its function.
- **Trigger details**: Monitor parameters that describe the conditions under which a response will be triggered.
- **Response**: Automatic actions that the monitor can trigger. Two types of responses are currently supported:
- Running components.
- Sending emails.

- **Ticket**: Ticket generation (refer to chapter "**Alerts and tickets**" on page **247**).

## Steps to create a monitor

### 1. Select the policy type

As this is a monitor, the policy type will be **Monitoring**.

### 2. Add a target

Add a target group or filter and the monitor.

> *A policy can have more than one associated monitor.*

On adding a monitor, a 4-step wizard appears where you can configure the necessary settings.

### 3. Select the monitor type

In this step, specify the monitor that will be added to the policy, according to the resources on the user's device to be monitored.

### 4. Configure the monitor

Depending on its function, each monitor needs slightly different settings, so this step will vary according to the type of monitor previously selected.

In general, this step requires the following data:

- **Trigger Details**: Complementary monitor settings and conditions to be met to trigger a response.
- **Alert Details**: You can select the priority of the alert that will be generated (**Critical**, **High**, **Moderate**, **Low**, **Information**).
- **Auto Resolution Details**: choose when the alert should auto-resolve itself, i.e., if it's no longer triggered for a certain period of time.

### 5. Set the monitor response

In this step, you can select the response that will be triggered when the limits defined in step 4 are reached.

- **Run the following component**: The drop-down list will show the components imported from the ComStore or developed by the administrator.
- **Email the following recipients**: You can specify the recipients, subject, format and message of the emails. The **Default recipients** checkbox sends the emails to the accounts defined in tab bar, **Settings** in the site to which the monitor created belongs and those defined at global level in the general menu **Account**, **Settings**.

### 6. Create tickets

In this step, you can enable automatic generation of tickets as the response generated by the monitor on reaching the limits defined in step 4.

- **Assignee:** Assigns the tickets generated by the monitor to a technician**.**
- **Severity**: Lets you change the severity of the tickets generated.
- **Ticket Email Notification**: Sends a notification email to the assigned technician's email account.
- **Disable Auto Resolution of Tickets**: Prevents tickets from being automatically resolved when the alert

that generated them ceases to occur.

# Monitoring Windows, Linux, and macOS computers

The available monitors for desktops, laptops, and servers are:

| Monitor name | Function | Available on |
|---|---|---|
| **Component Monitor** | Launches a component monitor from the **ComStore** or designed by the administrator. | Windows, macOS, Linux. |
| **WMI Monitor** | Monitors Windows devices using the Windows Management Instrumentation (WMI) engine. It retrieves hardware and software information for each device on your network: bandwidth consumption, queued processes, outages, etc. | Windows |
| **CPU Monitor** | Monitors CPU usage. | Windows, macOS, Linux. |
| **Online Status Monitor** | Checks to see, every 90 seconds, if the target device has a PCSM agent installed and if it is working properly. | Windows, macOS, Linux, ESXi, network device. |
| **Memory Monitor** | Monitors memory usage. | Windows, macOS, Linux. |
| **Patch Monitor** | Monitors the installation of the patches scheduled using Panda Systems Management's Patch Management module. | Windows |
| **Process Monitor** | Monitors the status of a specific process. | Windows, macOS, Linux. |
| **Windows Performance Monitor** | Monitors certain operating system metrics associated with running processes, triggering alerts if certain values fall under the established thresholds. | Windows |
| **Service Monitor** | Monitors the status of a specific service. | Windows |
| **Software Monitor** | Monitors the software installed on or uninstalled from the device. | Windows |
| **Disk Usage Monitor** | Monitors hard disk usage. | Windows |
| **Security Center Monitor** | Monitors the status of the operating system Security Center. | Windows, macOS, Linux. |
| **Event Log Monitor** | Checks for the presence of certain logs in the event viewer. | Windows |
| **File/Folder Size Monitor** | Monitors the size of files and folders. | Windows, macOS, Linux. |

Table 8.1: List of available monitors

| Monitor name | Function | Available on |
|---|---|---|
| **Ping monitor** | Monitors device connectivity via the ICMP protocol, checking the proper operation of the network. | Windows |

Table 8.1: List of available monitors

The parameters available for each type of monitor are listed below.

## Component Monitor

Refer to section "**Monitoring devices using components**" on page **112**.

## WMI Monitor

- **WMI Namespace**. Run the following command Get `Get-WMIObject -namespace "root" -class "__Namespace" | Select Name` from a PowerShell window. This will list all namespaces available on Windows.
- **WMI Query with WQL**. Click the following link **https://docs.microsoft.com/en-us/windows/desktop/wmisdk/querying-with-wql** or more information about the WQL language used in WMI queries.
- **WMI Property**.
- **Result Calculation (Numeric Values)**: select this checkbox to be able to configure an equation that you can apply the result to. Once the checkbox is selected, you will be able to enter a mathematical operator (+ - * /) and any digits. For example, enter *5 to multiply the result by 5.
- **Result Translation (Texts Values)**: select this checkbox to be able to configure a key to translate the numerical response into a more easily understood string. Use the "," character to separate multiple translations, and the "=" character to set up equivalences. For example `1=OK, 0=NotOK`.
- **Display Name**: it will appear as the description of the monitor on the Monitors page.
- **Format Data as**: select from a drop-down list how you would like to format the data (unit of measure).
- **Alert Settings**: specify the values that will trigger an alert.
- Result calculations are not used to raise alerts. Alerts are raised from the original values. Likewise, result translations are not used to raise alerts. Alerts are raised from the original values.

## CPU Monitor

- CPU usage threshold (percentage).
- How long the device's CPU usage needs to be above the threshold for before an alert is raised.
- Check interval (in minutes).

## Online Status Monitor

- Select whether you want to be alerted if the device goes offline or comes online.

- Specify how long the device needs to be in either of these states for before an alert is raised.

*Online Status Monitors are configured to generate a Critical alert if the device is offline for 5 minutes.*

### Memory Monitor

- What the memory usage threshold should be (percentage) and how long the device's memory usage needs to be above the threshold for before an alert is raised.
- Check interval (in minutes).

### Patch Monitor

The monitor will alert when the device fails to install any patches. Refer to chapter "**Patch Management**" on page **203**.

### Process Monitor

- Process name with or without the file name extension.
- Specify whether an alert should be raised if the process is running or not running OR
- If it has reached a certain CPU or memory usage (percentage).
- Attempt to kill the process if it triggers an alert.

### Windows Performance Monitor

- Specify a counter in the form of `\Category\Counter`. For Example `\TCPv6\Active connections.`

*Run the following command TypePerf.exe -q in a Command Prompt window to list all available counters on the computer.*

- Instance.
- **Alert Settings**: specify the values that will trigger an alert and how long the device needs to be in this state for before an alert is raised.

### Service Monitor

- Service name.
- **Service state**: running or stopped.
- **CPU or memory usage** (percentage).
- Specify how long the service should be in this state AND
- How much time after the device has booted before an alert is raised.

- **Attempt to take remedial action**: start a stopped service or stop a running service.
- Do not alert if service has been manually disabled.

## Software Monitor

- Name of the software package you want to monitor. For more information refer to section "**License audit**" on page **162**.
- **Software status**: is installed, is uninstalled, changes version.

## Disk Usage Monitor

- Drive you want to monitor.
- Threshold that needs to be passed for the alert to be triggered (% disk space used / GB disk space used / GB disk space free).
- **Type of disk to monitor**: fixed drives and/or disks above a certain disk capacity.
- How long the device's disk usage needs to be in this state for before an alert is raised.

## Antivirus Status Monitor

- **Antivirus status**: select the antivirus status you want to monitor (**Not detected, Not running, Running & not up-to-date**).
- How long the device's antivirus status needs to be in this state for before an alert is raised.

## Event Log Monitor

- **Event Log Name (required)**: name of the event viewer branch where the event is stored (Application, Security, System, Installation, Forwarded Events).
- **Event Source Name (required)**: content of the Source field of the device's event viewer. You can use the "%" wildcard character if you do not know the exact name or would like to search for multiple names. The wildcard character search is not case sensitive.
- **Event Codes**: Enter one or more codes separated by a space. Use a minus sign in front of a code to exclude that event from the monitor. E.g. If you set -56 as the event code, the agent will alert for all event codes except 56.
- **Event Types**: **Critical**, **Error**, **Warning**, **Information**, and/or **Verbose**.
- **Event Description**: use the following items to search for strings on the General tab of the event viewer:
  - One or more words.
  - Phrases enclosed in quotes
  - Use a minus sign ("-") in front of a word or phrase to indicate that it should not be present in the event.
  - Use a space between the event descriptions to apply an OR condition.

- If an event description has text within quotation marks, and you want to get an alert based on the information within the quotation marks, you need to add quotation marks around the quotation marks.

- Also specify the number of times this should occur within a certain period of time for the alert to be raised.
- **Auto-Resolution**: specify if you want the alert to be resolved if an event matching a number of characteristics is seen.

> *To avoid generating an excessive number of alerts, Panda Systems Management stops creating alerts after the fifth alert raised within 12 hours. If an event log monitor assigned to a device triggers excessively (over 1,000 times in 12 hours), the monitor will automatically be disabled on that device.*

### File/Folder Size Monitor

- **Item to monitor**: file or folder.
- Full path of the item to monitor.
- Select if the size of the file or folder should be over or under the set threshold.
- Threshold for the file or folder size (MB).
- How long the file or folder needs to be in this state for before an alert is raised.

### Ping Monitor

- IP address of the device you would like to monitor.
- How many ping packets should be sent to the device.
- Check interval.

## Monitoring devices using components

Panda Systems Management developed by the administrator as well as by Panda Security to expand on the capabilities provided by the product and cover virtually all aspects of monitored devices.

To add a component to a monitoring policy, follow the steps below:

- Go to general menu **ComStore**, and click **Device Monitors** from the panel on the left to list all monitoring components. Refer to chapter "**Components and ComStore**" on page **131** for more information about the ComStore.
- Select a component and click the **Add to my Component Library** button. The component will be downloaded and added to the administrator's repository.
- Go to general menu **Components** and click **Device Monitors** from the **My Components** panel on the left. This will display a list of all components added to the administrator's repository.

- Follow the steps in section "**Steps to create a monitor**" In step 3, select **Component Monitor** from the drop-down list.
- Select a monitor from the **Run the Component Monitor** drop-down list.
- Specify when the component monitor should be run.

# Monitoring printers

Panda Systems Management adds a pre-configured monitor automatically as soon as a new printer is incorporated into the management platform. This monitor will be added to the site to which the printer belongs.

This monitor will let you know when printer supplies (toner, ink, etc.) drop below a certain configurable threshold.

# Monitoring network devices using SNMP

*Although not strictly necessary, it is advisable for administrators to familiarize themselves with the basic concepts of SNMP (OID, MIB, NMS, etc.), as well as having an MIB browser to be able to browse the OIDs structure of the device. Mibble is an MIB browser available for free from the Mibble website.*

The process to configure an SNMP monitor is slightly different from configuring other types of monitors. This is due to the fact that SNMP monitors must meet a series of requirements related to the SNMP technology.

## Parameters to monitor

Most SNMP-compatible devices publish, in their MIB, a lot of detailed status information that allows you to monitor many functionality parameters, for example:

- Internal resource usage (memory, internal storage, CPU, etc.).
- Bandwidth consumption.
- Internal device temperature.
- Descriptive information about the device and the manufacturer (model, version, latest firmware update, etc.).
- Detection of specific errors with error codes.
- Changes to the device's configuration.
- Changes to the device status: ports enabled or disabled in a switch via STP, lines available on a switchboard, etc.

Any data published in the device MIB can be read and interpreted by Panda Systems Management, though the manufacturers guide will determine which information can be of use. Similarly, it is important to know the units of measurement used in the published data and to be aware of the thresholds that determine whether a device is in danger of imminent failure and requires intervention from the maintenance department.

## SNMP Throughput Monitor

This monitor is exclusively used to monitor the volume of data sent and received by managed devices. There is no need to configure an MIB since the monitored devices publish this information in a fixed OID (.1.3.6.1.2.1.2.) called IF-MIB. Specify the following parameters to configure this monitor:

- **Check interval**: frequency (in minutes) that the OID values will be checked for.
- **Interface Number (optional)**: number of the interface to monitor.
- **Traffic type**: **Incoming**, **Outgoing**, **Total**.
- **Alert trigger conditions**: indicate the average value required to generate an alert and the sample size.

## Steps to create an SNMP monitor

Follow the steps below to monitor an SNMP device:

### 1. Prepare the devices to monitor

Almost every device connected to a data network can be monitored via SNMP. For that is is usually necessary to enable the SNMP protocol in the specific device's settings and take note of the Community it belongs to (by default it is normally Public).

With some devices it may also be necessary to configure the SNMP protocol version to use (v1/v2), and the IP addresses that the monitored device will receive the SNMP requests from. In this case, the IP address will be that of the device with a Panda Systems Management installed and the Network Node role.

Once SNMP is enabled in the device to monitor, establish the OIDs that need to be monitored. SNMP-compatible devices periodically dump internal status data onto the MIB structure. It will be necessary to consult the manufacturer's documentation to see which OID nodes of the MIB structure contain useful information and make a note of them.

It is also possible to obtain these OID nodes by browsing the MIB structure with Mibble (**https://www.mibble.org**) or similar.

### 2. Designate a device with a Systems Management agent installed as the Network Node

See section "**Configuring a Network Node**" on page **61** for more information about how to assign the Network Node role to a PCSM agent and the requirements needed.

*It is advisable to test communications between the agent designated as the Network Node and the device to monitor on TCP and UDP port 161, in both directions.*

### 3. Add the network device to the management console

See section "**Integrating network devices**" on page **55** for more information about how to add to the management console those devices that do not support installation of the Panda Systems Management agent.

### 4. Configure an SNMP monitoring policy

The OIDs that Panda Systems Management reads from the network devices are established through SNMP monitors created and published by the administrator, or through policies published in the ComStore.

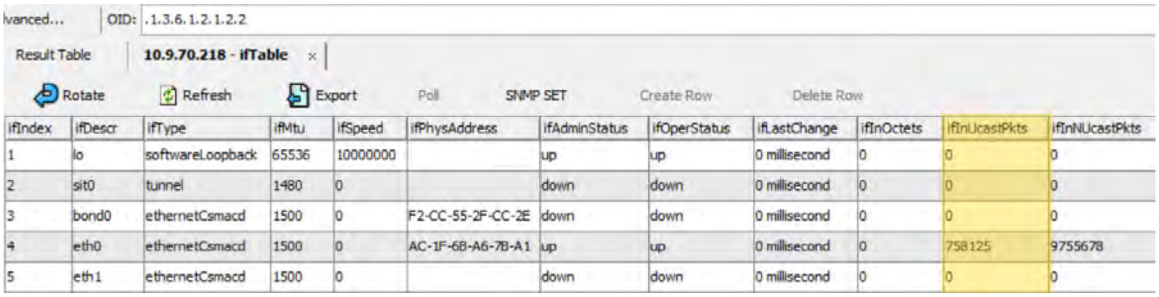
To create an SNMP monitoring policy, follow the steps in section "**Steps to create a monitor**" on page **106** and configure the following parameters:

- **SNMP OID to query:** specify the SNMP OID that you want to monitor.
- In **Alert Settings**, enter the conditions that must be met to consider that a device is malfunctioning.
  - Select the **Alert when OID is not responding** checkbox to have the monitor raise an alert when no response is returned for an OID that has previously returned a response.
- Select the **Alert when OID is Null/NoSuchInstance/NoSuchObject** checkbox to have the monitor raise an alert when Null, NoSuchObject, or NoSuchInstance is returned as a response.
- **Test interval**: indicates how often the monitor will read the configured OID.
- In **Transform Result**, establish a correspondence between the values sent by the device to the Systems Management server, and the text strings or numeric values displayed in the management console. The alerts will be raised from the original values, but the PCSM console will show the transformed data to make it easier to digest.
- In **Format data** as, select how you would like to format the data.

### 5. Configure an SNMP monitoring policy for device groups (optional)

To avoid creating a separate monitor for each value of a device to be monitored, you can monitor OID groups. For example, a common use case for this is monitoring the space of multiple hard disks on the same computer.

In effect, monitoring multiple devices at the same time involves monitoring an OID that contains all the information to be monitored in table format. To select the table cells you are interested in, you must specify the table row and column. To do this, follow the steps below:



| ifIndex | ifDescr | ifType | ifMtu | ifSpeed | ifPhysAddress | ifAdminStatus | ifOperStatus | ifLastChange | ifInOctets | ifInUcastPkts | ifInNUcastPkts |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | lo | softwareLoopback | 65536 | 10000000 |  | up | up | 0 millisecond | 0 | 0 | 0 |
| 2 | sit0 | tunnel | 1480 | 0 |  | down | down | 0 millisecond | 0 | 0 | 0 |
| 3 | bond0 | ethernetCsmacd | 1500 | 0 | F2-CC-55-2F-CC-2E | down | down | 0 millisecond | 0 | 0 | 0 |
| 4 | eth0 | ethernetCsmacd | 1500 | 0 | AC-1F-6B-A6-7B-A1 | up | up | 0 millisecond | 0 | 758125 | 9755678 |
| 5 | eth1 | ethernetCsmacd | 1500 | 0 |  | down | down | 0 millisecond | 0 | 0 | 0 |

Figura 8.1: OID table obtained with a MIB browser

- **SNMP OID to query:** OID string representing the table that contains the device values to be monitored.
- **SNMP table**: select this checkbox if the specified OID contains a table of values that reflect the status of one or more devices. Clear this checkbox if the specified OID only contains one value.
- **Identification column**: number of the column that contains the identifiers of the devices to be monitored. The number of the first column is 0. The device identifiers are character strings that identify the devices to be monitored. They are included in the monitoring process output.
- **Value column:** number of the column that contains the status of the device to be monitored. Use curly brackets around the column number. The number of the first column is 0. In the **Value column** field, it is possible to specify more than one column for simple numeric calculations. For example: if column 10 contains disk size in kilobytes and column 11 contains disk used in kilobytes, you can calculate the disk free space in gigabytes by entering the following calculation: {10}-{11}/1048576.

# Monitoring ESXi servers

The available monitors for ESXi servers are only visible from the Device level associated with the server. For more information, refer to section "**Policies, monitors, and access to the monitoring feature**" on page **106**. The monitors available for ESXi servers are listed below:

| Monitor name | Purpose |
|---|---|
| **ESXi CPU Monitor** | Monitors the ESXi server's CPU usage. |
| **ESXi Memory Monitor** | Monitors the ESXi server's memory usage. |
| **ESXi Data Store Monitor** | Monitors the amount of free/used space in the ESXi server's data stores. |
| **ESXi Temperature Sensor Monitor** | Monitors the ESXi server's temperature. |
| **ESXi Fan Monitor** | Monitors the operation of the server's fans. |

Table 8.2: list of monitors compatible with ESXi servers

| Monitor name | Purpose |
|---|---|
| **ESXi Disk Health Monitor** | Monitors the operation of the hard disks and any failures in the RAID system. You must have CIM providers installed to provide the information this monitor requires. |
| **ESXi PSU Monitor** | Monitors the ESXi power supply. |
| **Online Status Monitor** | Monitors the ESXi power supply. |

Table 8.2: list of monitors compatible with ESXi servers

The parameters you can specify for each type of monitor are listed below.

### ESXi CPU Monitor

- CPU usage threshold (percentage).
- How long the device's CPU usage needs to be above the threshold for before an alert is raised.
- Check interval (in minutes).

### ESXi Memory Monitor

- What the memory usage threshold should be (percentage) and how long the device's memory usage needs to be above the threshold for before an alert is raised.
- Check interval (in minutes).

### ESXi Data Store Monitor

- The threshold that needs to be passed (percentage) for the alert to be triggered.
- How long the data store needs to be in this state for before an alert is raised.

### ESXi Temperature Sensor Monitor

- The temperature threshold that needs to be passed for the alert to be triggered (Celsius (°C)).
- How long the temperature needs to above the threshold for before an alert is raised.

### ESXi Fan Monitor

An alert will be triggered if the status of any fan unit on any targeted device is other than “normal”.

### ESXi Disk Health Monitor

An alert will be triggered if a CIM (Common Information Model) provider registers disk health errors. Devices that do not have CIM providers installed will not raise any alerts.

*Refer to https://code.vmware.com/vmware-ready-programs/management/cim for more information about the CIM standard for VMWare products.*

### ESXi PSU Monitor

An alert will be triggered if the status of any power supply on any targeted device is other than "normal".

### Online Status Monitor

Refer to "**Online Status Monitor**".

## Automatically configuring monitors

*Every time a new account is created, Panda Systems Management assigns a Windows: Workstation monitoring policy and a Windows: Server monitoring policy to it.*

To speed up the monitor configuration process, Panda Security provides more than 50 preconfigured, ready-to-use monitoring policies via its **ComStore** marketplace.

Follow the steps below to import a ComStore monitoring policy:

- Go to general menu **ComStore**, side menu **Monitoring policies**. A list will be displayed showing all available policies.
- Click the **Add to Account Policies** button next to the policies that you want to import.
- Click the **Add a target** button to select the device groups or filters that will receive the policy. Refer to chapter 10 for more information about how to create and monitor policies.
- Click **Save**.
- If you want the policy to be immediately deployed, click **Push changes**.

### Windows: Workstation monitor

The purpose of this monitor is to provide an overview of the status of the Windows operating system installed on the device. This monitor provides Windows metrics only and generates an alert when these metrics are close to the configured thresholds.

This monitor collects the status of the following parameters:

- Disk monitor.
- Service monitor

The Windows: Workstation monitor helps maintenance technicians save time by automatically resolving certain types of common incidents without generating alerts.

### Windows: Server monitor

This monitor provides an overview of the server status by means of a series of charts.

> *This monitor doesn't generate performance alerts when the managed devices get close or exceed the configured threshold. To generate alerts, this monitor's policies must work alongside any other policy set for that purpose.*

This monitor detects the following conditions:

- Event logging.
- Reboot required.
- Reboot as a result of the Blue Screen of Death.
- Disk health.
- Server offline.
- IP conflicts.
- Patching.
- CPU and memory monitoring.

# Importing and exporting a monitoring policy

## Importing monitoring policies

- Go to general menu **Account**, **Policies** tab, to import a policy at Account Level. You can also go to general menu **Sites**, select a site, and click the **Policies** tab to import a policy into a specific site.
- From the list of previously created policies, click the **Import** button at the bottom of the screen. A window will be displayed to select the .pcy file containing the parameters of the policy to import.

## Exporting monitoring policies

To export an already configured monitor type policy as a `Pcy` file:

- Edit the policy to export by clicking its name.
- Click the **Export** button at the bottom of the screen. A window will be displayed for you to enter the name of the .pcy file containing the parameters of the policy to export and the path that the file will be downloaded to.

# Managing monitors

Once you have created and assigned your monitors, you can check their status and results at the Device level associated with each monitored device.

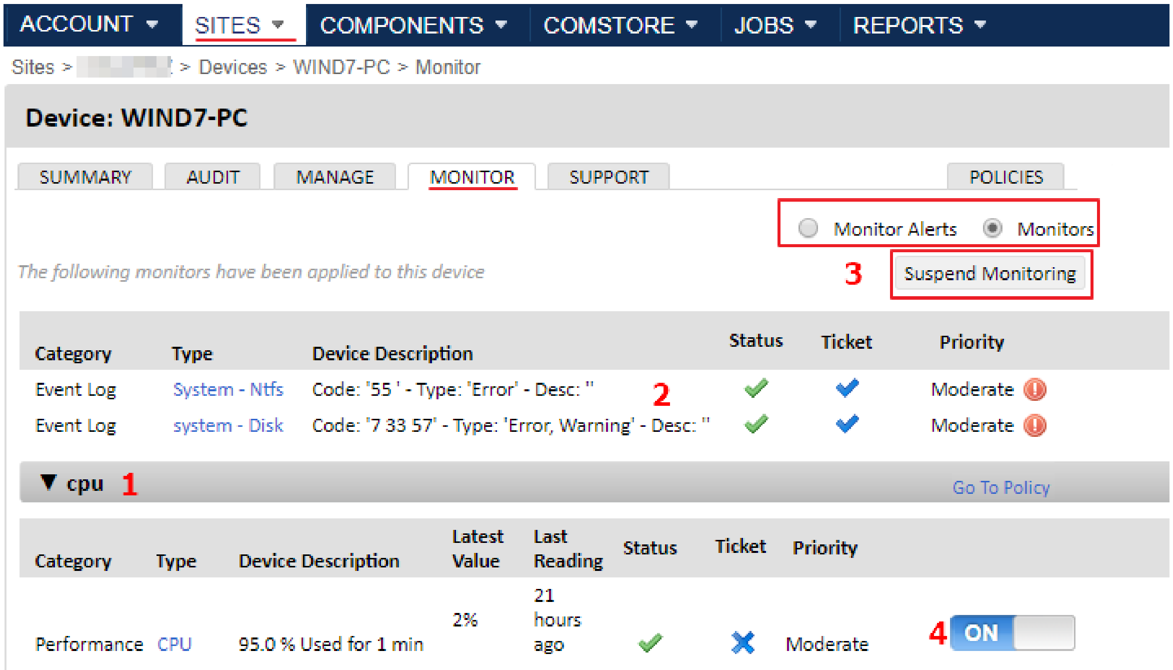
## Accessing the list of monitors

- Click general menu **Sites**, and then click the site where the device is located.
- Click Monitor from the tab menu and then click the Monitors selection control in the upper right corner of the screen. This will list all the monitors associated with the device and their status.

## Description of the columns in the Monitors list

The list shows all monitors grouped by policy **(1)**, since a policy may consist of one or more monitors **(2)**.

Click the ▼ and ▶ icons to hide or show a policy's monitors. Monitors with no associated policies appear under the **No policies** group.



*The following monitors have been applied to this device*

| Category | Type | Device Description | Status | Ticket | Priority |
|---|---|---|---|---|---|
| Event Log | System - Ntfs | Code: '55 ' - Type: 'Error' - Desc: '' | ✓ | ✓ | Moderate ! |
| Event Log | system - Disk | Code: '7 33 57' - Type: 'Error, Warning' - Desc: '' | ✓ | ✓ | Moderate ! |

| Category | Type | Device Description | Latest Value | Last Reading | Status | Ticket | Priority |
|---|---|---|---|---|---|---|---|
| Performance | CPU | 95.0 % Used for 1 min | 2% | 21 hours ago | ✓ | ✗ | Moderate |

Figure 8.2: list of monitors at Device level

You can suspend a device's monitoring altogether **(3)** or disable each monitor individually **(4)**.

| Field | Description |
|---|---|
| **Category** | Shows the type of monitor assigned. |
| **Type** | Shows main parameters that describe the monitor subtype, based on the monitor type and its settings. |
| **Device Description** | Shows secondary parameters that describe the monitor settings. |

Table 8.3: attributes of a monitor

| Field | Description |
|---|---|
| **Latest Value** | Shows the latest value received at the Panda Systems Management server. |
| **Last Reading** | Displays when the value was last measured. |
| **Last 30 Metrics** | Monitors returning numeric data produce a graphical history of the last 30 records. Hover over the graph to see more details. |
| **Status** | Indicates whether or not the device operates within the parameters specified in the monitor. |
| **Respond** | Indicates whether or not an alert response is configured in the monitor. |
| **Ticket** | Indicates if a ticket will be created if an alert is raised through the monitor. |
| **Priority** | Displays the alert priority as configured in the "Alert Details". |
| **Icon bar** | Monitors with no associated policies display an icon bar for editing and deleting them.<br>• ⚠ Deletes all alerts generated by the monitor.<br>• ✎ Lets you edit the monitor.<br>• ✖ Deletes the monitor.<br>To edit or delete the monitor associated with a policy, you must edit the policy. For more information, refer to section "**Managing policies**" on page **94**. |
| ON | Lets you turn the monitor ON or OFF for the device. |
| ❗ | Indicates that the policy associated with the monitor has been disabled at Site level. |

Table 8.3: attributes of a monitor

# Chapter 9

# Jobs

Jobs are groups of operations that are run on devices with a PCSM agent installed. They allow administrators to perform processes one time only or repeatedly at scheduled times. There are two types of jobs based on the schedule:

- **Scheduled jobs**: these jobs are run repeatedly at regular time intervals.
- **Quick jobs**: these jobs are run one time only and on demand by network administrators.

Jobs can be defined at Account, Site or Device level, depending on the targeted devices.

CHAPTER CONTENT

## Job items

Jobs are made up of the following items:

| Item | Description |
|---|---|
| **Associated component** | Contains the process or processes to be deployed to, and run, on the job targets. Refer to "**Configuring a local cache node**" on page **65** for more information on how to minimize the effect on the network of repeatedly downloading one component to multiple devices. |

Table 9.1: job items

| Item | Description |
|---|---|
| **Target** | These are the devices that will receive the job. It can be a filter, group, site or a specific device. |
| **Result** | Every time a job is run, it returns a code indicating whether it was completed successfully or failed, as well as other information associated with the process deployed to the target devices. |
| **Schedule** | Jobs can be quick if they don't require any additional configuration, or scheduled if they are repeated at regular time intervals. |
| **Other options** | Depending on the type of job and where it is executed from, there are a number of advanced options you can configure such as the job's maximum run time, the recipients of the job results, alerts (if required), etc. |

Table 9.1: job items

ⓘ *Jobs are run by default under the Local System account of the target device's operating system.*

### Changing a job's recipients

The time that elapses between when a job is configured and when it is finally executed may vary a lot, and consequently, the job's recipients may change during that time. That is the case, for example, of jobs whose target is a device group or filter whose members change (enter or leave the group) from the time the job was configured, or jobs whose target is a grouping (site, group or filter), which ceases to exist before the job starts running or while it is being executed.

Generally, the members of a device group set to receive a job are resolved just before the job starts executing. This way, a job that has already started executing won't be affected by any change (removal, etc.) in its target (group or filter). However, if a job's target is modified before it starts running, (for example, some of the configured groups are deleted), the job will not be able to find them when resolving its targets and won't be executed on those groups.

## Launching a quick job

A quick job deploys components to the target devices one time only and on demand. There is no need to use the job scheduler to configure a quick job. Quick jobs can be run from the icon bar (quick way) at the level where the targeted devices are, or from the general menu **Jobs**, tab menu **New job** (thorough way).

### Configuring the components to be used in a job

To launch a job that runs a component, you must first enable the component prior to configuring the job. To enable a component downloaded from the Comstore and use it in a job, follow the steps below:

- Go to general menu **Components**.

- Click the favorite icon ★ to the right of the components that you want the job to run.

> *Only script and application components show the favorite icon. Monitor components can only be run by a monitoring policy.*

## Launching a quick job from the action menu (quick way)

Follow the steps below to run a quick job in the faster way:

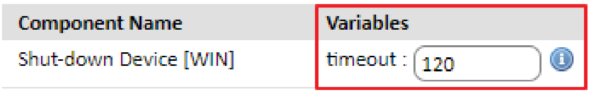
- Define the job targets:
  - If the job is to be run on all devices in one or multiple sites, click the general menu **Sites** and use the checkboxes to select the sites that will receive the job.
  - If the job is to be run on filters or groups at Account or Site level, click the grouping from the panel on the left and select the devices that will receive the job.

- Click the quick job icon ⚙ from the icon bar. A window will be displayed with all components marked as favorite.

- Use the **Search** option to find a specific component from the list, or the **Groups** option to display the components included in a specific group.

> *This method only allows one component to be assigned to one job. Refer to section "**Launching scheduled jobs**" for more information on how to assign two or more components to a quick job.*

- Select the component to run and click **Save**. If the job requires input variables, a text box will be displayed for you to enter the necessary information.



| Component Name | Variables |
|---|---|
| Shut-down Device [WIN] | timeout : 120 ⓘ |

Figure 9.1: component with input variables

- The job will be run immediately. If the **Follow to job list page on submit** checkbox is selected, you will be taken to the **Active jobs** tab.

- A name will be automatically assigned to the quick job, using the following format: "Quick job running Component" [Component name] "`on device`" [Device name].

## Launching a quick job from the general menu Jobs (thorough way)

Go to general menu **Jobs**, tab menu **New job** to configure all of the details of a quick job. This method is equivalent to the method discussed in section "**Launching a quick job from the action menu (quick way)**", however, in this case you must also specify the following details of the quick job:

| Field | Description |
|---|---|
| **Name** | Lets you enter a name to be able to identify the job on the Completed jobs list. |
| **Schedule** | Type of schedule. Immediate in the case of quick jobs. |
| **Job Targets** | Choose the groups, filters or sites that will receive the job. |
| **Components** | Select one or multiple components and define the order of execution by using the green arrows to their right. |
| **Job disabled** | Select this option if you'd like to disable this job without having to delete it. |
| **Expire this job after** | Set an expiration time for the job. Expiration defines the length of time the scheduled job remains available. After this time has elapsed, the expired job will be canceled. |
| **Duration** | Defines the last date and time that a recurring job is available for the scheduler. |
| **Execution** | Select the conditions that must be met to run the component on the user device:<br>• **Only run this job when user is logged in**: select this checkbox to only run the job when the user is logged in.<br>• **Logged in user must have Administrator rights**.<br>• **Execute when user is logged in**: automatically runs the job in the user session.<br>• **Advertise to user but do not execute**: the component is not run automatically. A pop-up message is shown to the user asking for confirmation to run the component. |
| **Alerts** | You can choose to create an alert when the job: succeeds, fails, has warnings, or expires. For more information, refer to chapter "**Alerts and tickets**" on page **247**<br>To view all triggered alerts, go to general menu **Account**, tab menu **Monitor**. |
| **Automatically email StdOut/StdErr options** | You can configure to receive a standard output (`STDOUT`) or standard error (`STDERR`) file via email after the job has run. |

Table 9.2: configuring a job (thorough way)

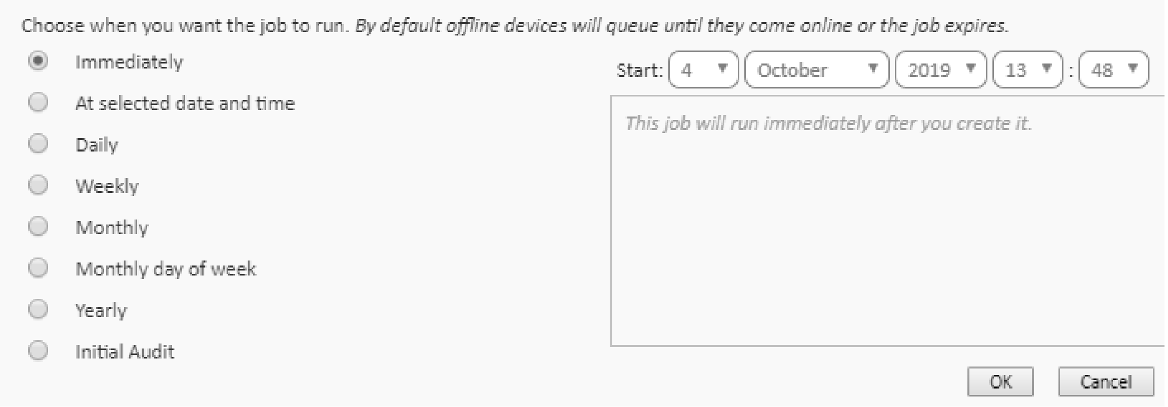
| Field | Description |
|---|---|
| **Job recipients** | Lets you email alerts to the configured accounts.<br>• **To configure the default recipients at Account level**: go to general menu **Setup**, tab menu **Account settings**. Scroll down to section **Email recipients** and select the **Alerts** checkbox. Enter the addresses of your choice by clicking the **Edit recipient** icon.<br>• **To configure the default recipients at Site level**: go to general menu **Sites** and select the relevant site. Click the tab menu **Settings**, and scroll down to section **Email recipients**. Select the **Alerts** checkbox and enter the addresses of your choice by clicking the **Edit recipient** icon. |

Table 9.2: configuring a job (thorough way)

# Launching scheduled jobs

A scheduled job lets you run components repeatedly over time by using the job scheduler. You can launch a scheduled job from the icon bar by clicking the ⚙ icon, or from the general menu **Jobs**, tab menu **New job**. In both cases, a settings screen will be displayed to configure all aspect of the job. The procedure is the same as the one described in "**Launching a quick job from the general menu Jobs (thorough way)**". However, in this case you must configure the job's schedule by clicking the **Click to change** button in section **General**, **Schedule.**

## Job scheduler


Choose when you want the job to run. *By default offline devices will queue until they come online or the job expires.*

● Immediately
○ At selected date and time
○ Daily
○ Weekly
○ Monthly
○ Monthly day of week
○ Yearly
○ Initial Audit

Start: 4 October 2019 13 : 48

*This job will run immediately after you create it.*

Figure 9.2: job scheduler

The job scheduler lets you set the job's repetition interval. The following options are available:

| Field | Description |
|---|---|
| **Immediately** | The job will be run as soon as it is saved. |

Table 9.3: job scheduler settings

| Field | Description |
|---|---|
| **At selected date and time** | The job will run once at the specified date/time. |
| **Daily** | The job will run every day at the specified time. |
| **Weekly** | The job will run every week on the specified days. |
| **Monthly** | The job will run in the specified months on the specified days. |
| **Monthly day of week** | The job will run in the specified months on the specified day of the week. You must specify the day of the week and the job start date/time. |
| **Yearly** | The job will run every year on the specified day. |
| **Initial Audit** | The job will run once an initial audit has completed after the start date configured. |

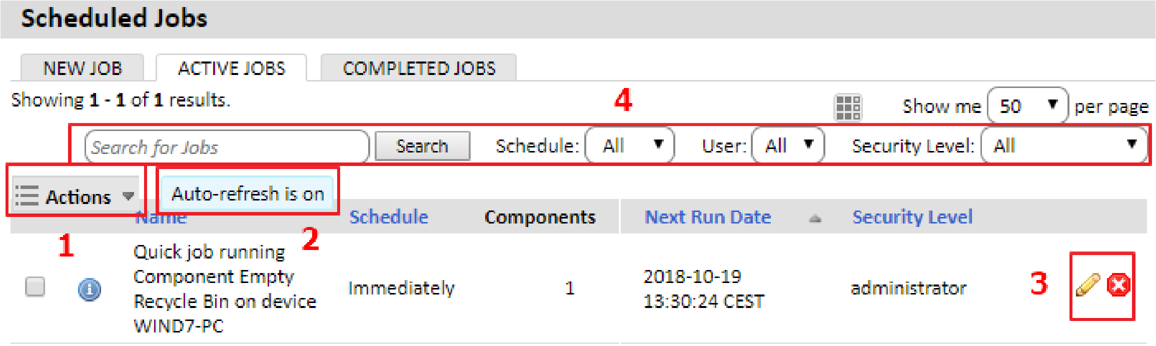
Table 9.3: job scheduler settings

# Managing active and completed jobs

## Active jobs list

Active jobs are jobs that have been created and are waiting to be launched based on the configured schedule, or are underway but have not been completed yet.

To view the list of all active jobs, click general menu **Jobs**, tab menu **Active jobs**.



Scheduled Jobs

Showing 1 - 1 of 1 results.

Show me 50 per page

Schedule: All User: All Security Level: All

| | | Name | Schedule | Components | Next Run Date | Security Level | |
|---|---|---|---|---|---|---|---|
| □ | ⓘ | Quick job running Component Empty Recycle Bin on device WIND7-PC | Immediately | 1 | 2018-10-19 13:30:24 CEST | administrator | ✎ ✖ |

Figure 9.3: Active jobs screen

The Active jobs screen provides resources for checking the status of the jobs and working with them:

| Field | Description |
|---|---|
| **Name** | Job name. If the job is a quick job created from the icon bar, the system will assign a name to it automatically. |
| **Schedule** | Immediately or scheduled. |
| **Components** | The number of components added to the job. |

Table 9.4: fields in the Active jobs list

| Field | Description |
|---|---|
| **Jobs run** | The number of times the job has run. |
| **Next run date** | Date, time, and time zone when the job is next scheduled to be run. A crossed-out date indicates that the job has no future occurrence. |
| **Last run date** | Date, time, and time zone when the job was last run. |
| **User** | The username of the management console user who created the job. |
| **Security level** | The security level of the management console user who created the job. |
| **Icon bar (1) (drop-down menu)** | Lets you export the list, delete a job or refresh the list. |
| **Auto-refresh is on (2)** | The information on the list will be refreshed regularly to reflect the changes in the status of the jobs. |
| **Actions (3)** | Lets you delete or edit the job. |
| **Search tools (4)** | Provides controls to filter the list and make it easier to find a specific job. |

Table 9.4: fields in the Active jobs list

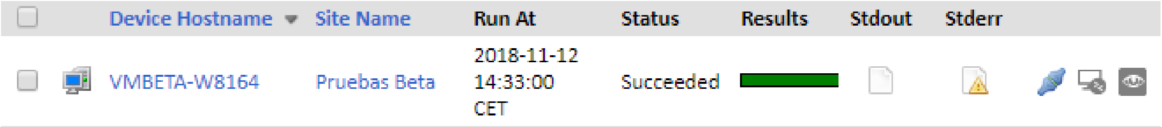
### Completed jobs list

A job is completed when it has finished running, either successfully or with an error.

To view the list of all completed jobs, click general menu **Jobs**, tab menu **Completed jobs**. The fields shown in the Completed jobs list are the same as those in the Active jobs list. These have been discussed in section "**Active jobs list**" on page **128**.

## Job status

To view the status of a job, click its name from the Active jobs or Completed jobs lists (general menu **Jobs**). You'll be taken to a screen with all relevant information about the job:



| □ | Device Hostname ▼ | Site Name | Run At | Status | Results | Stdout | Stderr |
|---|---|---|---|---|---|---|---|
| □ | VMBETA-W8164 | Pruebas Beta | 2018-11-12 14:33:00 CET | Succeeded | 🟩 | | |

Figure 9.4: details of a completed job

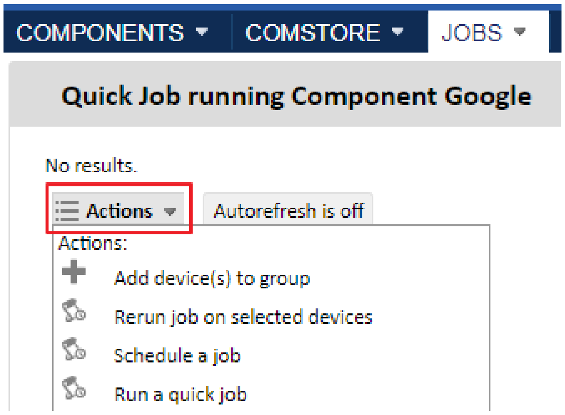
| Field | Description |
|---|---|
| **Device hostname** | The name of the device that received the job. |
| **Site name** | The name of the site the device belongs to. |
| **Run at** | Date/time when the job was run. |
| **Status** | Succeeded, failed, expired. |

Table 9.5: fields on the Job status screen

| Field | Description |
|---|---|
| **Results** | A color indicator of the job result:<br>• **Green**: the job ran successfully.<br>• **Orange**: the job ran but there was a standard output (STDOUT) value found.<br>• **Red**: the job failed. |
| **Stdout** | Standard output message for the device. |
| **Stderr** | Standard error message for the device. |
| **Connect to device** | For more information, refer to chapter "**Remote access tools**" on page **257**. |
| **Remote takeover (RDP)** | For more information, refer to chapter "**Remote access tools**" on page **257**. |
| **Remote takeover (VNC)** | For more information, refer to chapter "**Remote access tools**" on page **257**. |

Table 9.5: fields on the Job status screen

## Available actions for active and completed jobs



Quick Job running Component Google

No results.

Figure 9.5: Actions drop-down menu

When clicking an active or completed job, Panda Systems Management displays an icon bar in the shape of a drop-down menu with multiple options for managing jobs:

- **Rerun job on selected devices**: lets you rerun the job on those devices where it failed.
- **Schedule a job**: lets you schedule a job. For more information, refer to section "**Launching scheduled jobs**".
- **Run a quick job**: lets you run a quick job. For more information, refer to section "**Launching a quick job**".
- **Download selected Standard Output/Error**: launches a window that lets you configure the download options for the Standard Output/Error messages.

# Chapter 10

# Components and ComStore

A component is an extension of the Panda Systems Management platform that allows administrators to add monitoring and troubleshooting features to the PCSM agent.

CHAPTER CONTENT

## Component types

Components can be divided into two groups based on who develops them:

- Components developed by the administrator or IT team of the company that uses Panda Systems Management as a management and remote troubleshooting tool.
- Components developed by Panda Security and offered to all customers for free through the

ComStore.

## Components developed by the administrator

These are divided into three groups based on their purpose, behavior and running method:

- **Applications**

Components used to deploy software across the customer's network. For more information, refer to "**Centralized software deployment and installation**" on page **225**.

These are scripts that are normally executed only once or under very specific circumstances, and may have external files associated to them (in the case of installation components these would be the software to install on the user's device.

- **Monitors**

Monitoring policies always incorporate a component to monitor the user's devices. Panda Systems Management comes with a number of default monitors that monitor many aspects of devices, such as CPU or hard disk usage. However, it is possible that the administrator may need to monitor aspects initially not contemplated by the platform. In that case, it will be necessary to add a component monitor to the policy. Refer to chapter "**Monitoring**" on page **105** for more information about the monitors implemented in Panda Systems Management.

- **Scripts**

These are small programs developed in a scripting language that get run on the customer's devices. They can be run as a one-time job or periodically based on the schedule configured in the task scheduler.

Below you can see a table summarizing the types of components developed by the administrator:

| Component type | Run from | Run every | Purpose |
|---|---|---|---|
| **Applications** | Quick job or scheduled job. | At the time or creating the component or when scheduled. | Centrally deploy and install software. For more information, refer to Chapter 13: Centralized software deployment and installation. |
| **Monitors** | Account policy, Site policy or independently. | 60 seconds (fixed interval). | Monitor devices. |
| **Scripts** | Quick job or scheduled job. | At the time or creating the component or when scheduled. | Run applications developed by the administrator. |

Table 10.1: component type list

*Monitors, applications, and scripts are almost identical with regard to their internal structure. The type of component only determines the way it is integrated into the PCSM console. Thus, jobs use script or application-type components, whereas monitoring policies only use component monitors created by the administrator.*

## Components developed by Panda Security: ComStore

**ComStore** is an online library of components developed and certified by **Panda Security** for **Panda Systems Management** users.

The purpose of the **ComStore** is to make accessing and integrating components easier for the IT team.

*Every component published in the ComStore is provided free of charge and without limitations to all Panda Systems Management customers.*

# Integrating components into the platform

For a component to be used by the administrator it must first be incorporated into the Panda Systems Management platform.

### Adding a component from the ComStore

Go to general menu **ComStore (1)** figure 10.1 to access the library of components developed and certified by Panda Security and made available to the Panda Systems Management customers.

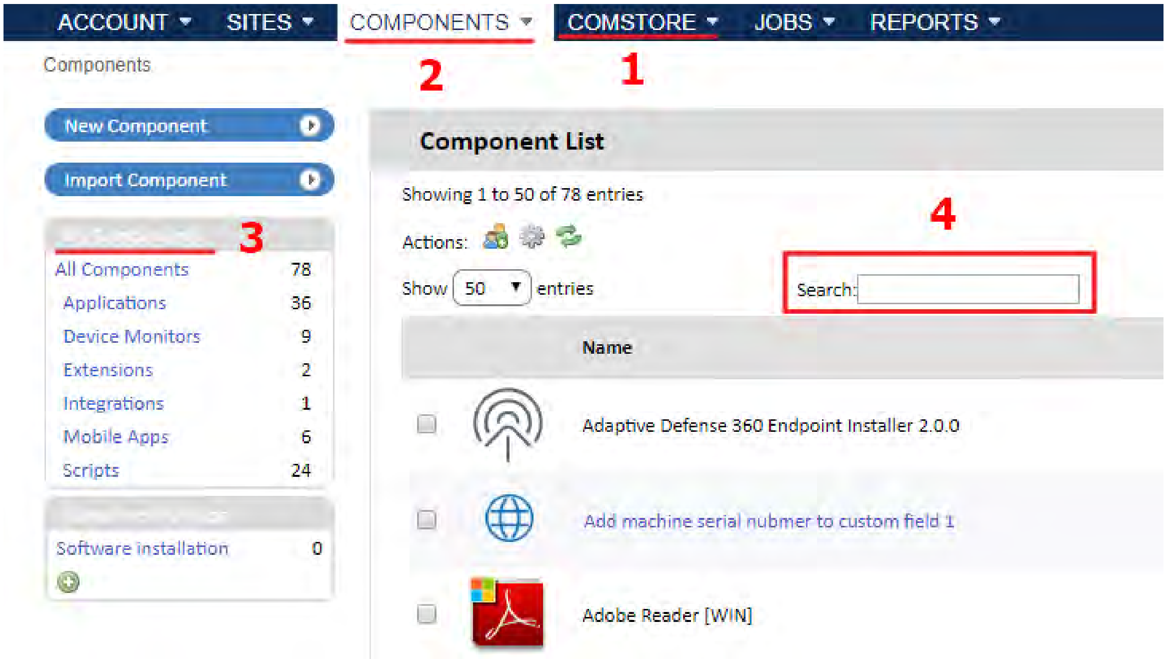
Follow these steps to add a component from the **ComStore** to the administrator's repository:

- Click it. A window will be displayed with the component description, release date, rating, as well as comments from other administrators who used it.
- Click the **Add to my Component Library** button. The component will be downloaded and added to the repository.

To view a list of all components already added to your repository:

- Go to general menu **Components (2)**. The **My Components** panel on the left side **(3)** displays all components added to your repository, grouped into different categories.

- To find a specific component, use the **Search** box on the right side of the window.



Showing 1 to 50 of 78 entries

| | |
|---|---|
| All Components | 78 |
| Applications | 36 |
| Device Monitors | 9 |
| Extensions | 2 |
| Integrations | 1 |
| Mobile Apps | 6 |
| Scripts | 24 |
| Software installation | 0 |

| Name |
|---|
| Adaptive Defense 360 Endpoint Installer 2.0.0 |
| Add machine serial nubmer to custom field 1 |
| Adobe Reader [WIN] |

Figure 10.1: component search tools

## Groups of components in the ComStore

All components published by Panda Security are grouped into seven categories accessible from the left-side panel:

- All Components
- Applications
- Device Monitors
- Extensions
- Integrations
- Mobile Apps
- Scripts

## Importing and downloading components

To import a component:

- Go to general menu **Components** and click **Import Component** from the left-side panel. You can only import components previously exported from the PCSM console.

To export a component:

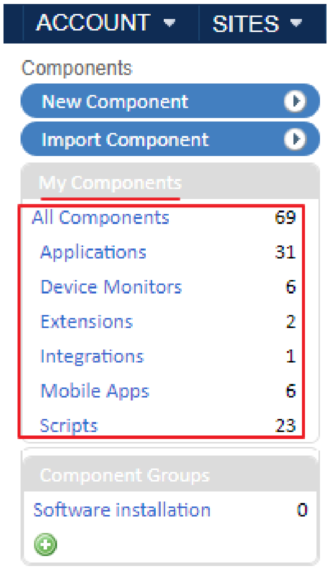
- Go to general menu **Components**, and click the arrow icon in the component list . If the component you want to download doesn't have an associated icon, click to copy the component. The copied component will have the associated icon for download.

## Copying and deleting components

- To copy a component, click the 📄 icon associated with it.
- To remove a component from the **Components** area, click the ✖ icon associated with it. Jobs with that component assigned will be disabled, but not deleted. Deleted components are still available in the **ComStore** area for integration into the administrator's repository.

## Classifying and grouping integrated components

Go to general menu **Components** to view the components already integrated into the platform.



| | |
|---|---|
| All Components | 69 |
| Applications | 31 |
| Device Monitors | 6 |
| Extensions | 2 |
| Integrations | 1 |
| Mobile Apps | 6 |
| Scripts | 23 |

| | |
|---|---|
| Software installation | 0 |

Figure 10.2: My Components side panel

The **My Components** section classifies all integrated components automatically based on their functionality. Seven categories are available:

- All Components
- Applications
- Device Monitors
- Extensions
- Integrations
- Mobile Apps
- Scripts

Additionally, the administrator can create new component groups by using the grouping tool available in the **Component Groups** section in the left-side panel.

Follow the steps below to create a component group:

- Go to general menu **Components**.
- Click the ⊕ icon in the left panel **Component Groups** to give the group a name.
- Select the components to group using the checkboxes in the component list and click the 👥 icon from the icon bar. A window will be displayed listing the component groups previously created.

Select the group to add the selected components to.

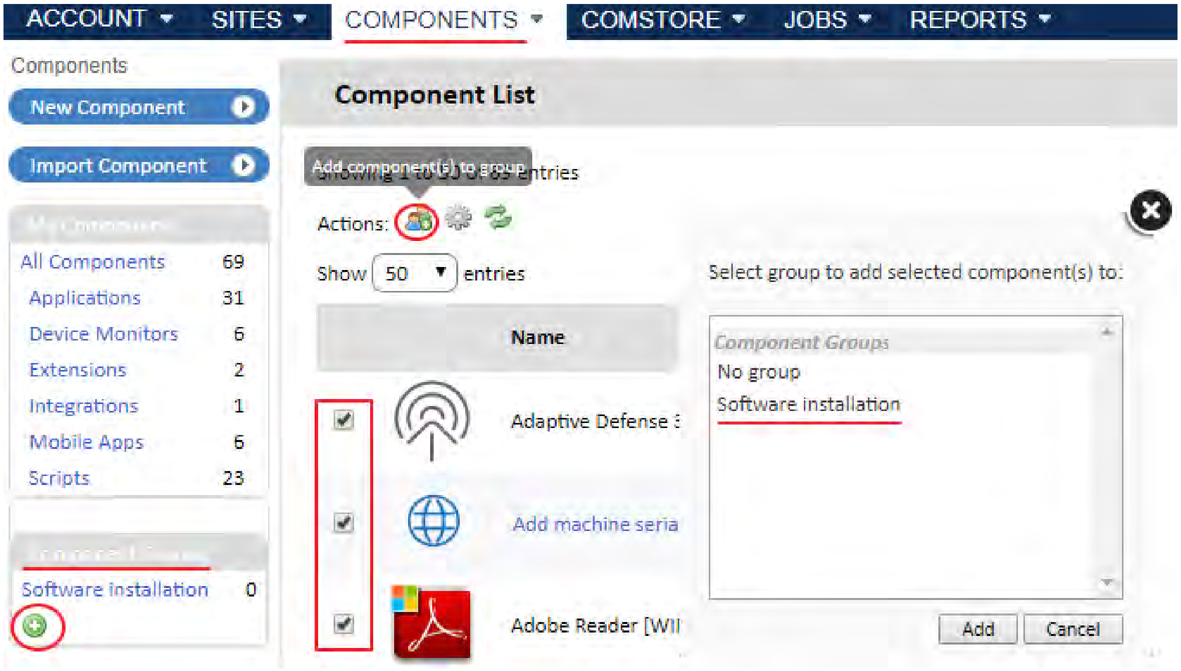


Figure 10.3: adding a component to a component group

## Updating components

Panda Security rolls out updates of the components published in the **ComStore** at regular intervals. These updates are grouped together in section **Check for Updates** of the **ComStore** general menu.

This section shows all of the **ComStore** components that have been updated since being added to **My Components** by the administrator. Click **Update All** to update all of the components included in **My Components**.

*The option **Check for updates** frees administrators from the task of having to manually search for the components they integrated from the ComStore in order to check if they have been updated or not. The option to **Update components** only updates the components included in **My Components**; it doesn't deploy them automatically to the customer's devices. To deploy the updates, you need to run a Quick Job or a Scheduled Job.*

If you don't want to update all components simultaneously, click the **Get Update** button next to each component.

Additionally, administrators can get weekly email notifications with a list of all components added to the ComStore in the last week, as well as of updates to the components included in the **My Components** section.

To enable this weekly notification, go to general menu **Setup**, **Account Settings**, and select **ComStore Components** in **Email recipients**.

# Developing components

Developing components allows the administrator to create new processes to run on users' devices and which add extra functionality to the Panda Systems Management platform.

Although Panda Systems Management provides a default component repository (ComStore) which extends its basic functions, it might be necessary to develop specific components to perform very specific tasks on users' devices or extend the solution's monitoring capabilities to those devices that do not support installation of a Panda Systems Management agent.

## Requirements for developing components

To develop general components, the administrator needs basic knowledge of programming in one of the supported scripting languages:

| Language | Included as standard in | Provider |
|---|---|---|
| **Batch** | All Windows versions | Microsoft |
| **Visual Basic Script** | Windows 98 and later, Windows NT 4.0 Option Pack and later | Microsoft |
| **JavaScript (Jscript)** | Windows 98 and later, Windows NT 4.0 Option Pack and later | Microsoft |
| **PowerShell** | Windows 7 | Microsoft |
| **Python** | macOS 10.3 (Panther) | Python Software Foundation |
| **Ruby** | None | Yukihiro Matsumoto |
| **Groovy** | None | Pivotal & Groovy Community |
| **Unix (Linux, Mac OSX)** | Linux, Mac OSX | Variable |

Table 10.2: programming languages required for component development

Furthermore, the parser associated to the selected scripting language must be installed and running on the user's device.

*Some parsers like Python or Groovy must be installed. Therefore, the components programmed in these languages are not guaranteed to work on recently installed Windows computers.*

*Before running a component developed in a language not supported directly by the user's device, it is advisable to run an automatic job to distribute the parser. Software distribution is described in chapter "***Centralized software deployment and installation***" on page* **225**.

# Creating a component monitor

## Component presentation and purpose

This section provides an example of how to create a monitor from scratch and deploy it to all devices in a specific site.

*Refer to section "**Deploying documents using a script language**" on page **228** to see another example of how to develop a component.*

The purpose of the component in our example is to easily and simply manage the quarantine of the security product Panda Endpoint Protection. The quarantine stores suspicious files that could contain malware and also files detected as a virus. Therefore, it is very important for the administrator to know if there has been an increase in the number of quarantined items. The example also shows how simple it is to adapt and integrate new monitors for other software solutions.

Below is a summary of the component features.

| | |
|---|---|
| **Devices affected** | All Windows 7 devices in the Home site. |
| **Script Language** | Visual Basic Script. |
| **Frequency of sending information** | Every 10 minutes, a notification is sent of whether the number of items in quarantine has increased. |
| **Panda Systems Management actions** | An email is sent to the administrator with the monitoring results. An alert will be generated automatically. |

Table 10.3: features of the component to develop

## Necessary elements

To follow this example, a trial or paid license of Panda Endpoint Protection or PCSM is required. Also, the agent must be installed on a device on the network. However, as the items added to quarantine by Panda Endpoint Protection are files in a specific folder on the device, this example can be used with any other folder on the system.

The component is developed in Visual Basic Script and therefore, the `Wscript.exe` or `Cscript.exe` parser will need to be installed on the user's device. This parser comes as standard on all Windows operating systems.

*The complete source code of the component is found in section "**Quarantine monitor**" on page **299**. It will be necessary to copy and paste the source code later.*

## Communications protocol between the component and the PCSM server

Almost all of the components will need information from the server and will return the result of their execution to the server. All of the information exchanges between the PCSM server and the component will be performed through environment variables created on the device.

These environment variables are automatically created by the PCSM agent when a component is launched. However, it is normal for the script to create environment variables manually to send responses to the server, which it will gather and add to the console.

In this case, three environment variables are required.

| Variable Name | Direction | Purpose |
|---|---|---|
| PCOP_PATH | **Read** | The script recovers from the PCSM server the path where Panda Endpoint Protection stores the quarantine on each user's device. |
| Result | **Write** | Send data to the server every 10 minutes through the standard output. |
| Errorlevel | **Write** | Script error code. If it is 0, the PCSM server concludes that monitoring is correct. If it is 1, Panda Systems Management concludes that monitoring is incorrect. |

Table 10.4: required environment variables

The settings needed to execute the component on the customer's device will be the path to the folder to monitor. This path could be hardcoded in the script source code but, in this example, the values that the administrator has entered in the console will be used in order to add more flexibility to the component.

`Errorlevel` will inform the server whether there has been an error running the script:

- The status code `0` indicates that the script has executed properly.
    - The `Result` variable will display the number of new files detected in the directory. If the number of files in quarantine is the same or lower (emptying of quarantine), the `Result` variable will show the value `0`.
    - However, if the number of files has increased, the `Result` variable will show the result of subtracting the number of files found at the time of running the script minus the number of files found during the previous execution.
- The status code `1` indicates that script execution was not completed. In our example, an error code

is returned as the target folder does not exist on the user's device.

```
Set WshShell=WScript.CreateObject (“WScript.Shell”)
Set objFSO=CreateObject (“Scrpting.FilesSystemObject”)

‘access to environment variable and quarantine path
On error resume Next
   Set WshSysenv=WshShell.Enviroment(“PROCESS”)
   Set objFolder=objFSO.GetFclder(WshSysEnv(“EP_PATH”))

   if err.number<>0 then
      ‘PCSM didn’t send the environment variable
     err.clear
     WScript.Echo”<-StartResult->”
     WScript.Echo”Result=PCOP_PATH variable not defined in PCSM console or path
not found”
     WScript.Echo”<-EndResult->”
     Set WshShell=nothing
     Set WsSysEnvy=nothing
     Set objFolder=nothing
     WScript.Quit(1)
   end if
On error goto 0
```

For the server to correctly interpret the standard output and extract the content of the component's Result variable, the following format must be used:

```
Line 1: <-Start Result->

Line 2: Result=(data to send)

Line 3: <-End Result->
```

*If the script language chosen is Batch, the symbol ^ must be inserted in front of each “<“o “>” character. For example ^<-Start Result-^>.*

Result will be the variable from which the server will extract the data to terminate execution of the component. The string to the right of “=” is the content that the server will store and process.

## Diagnostic summary

With those monitors that require returning several information lines, the following format must be used:

```
Line 1: <-Start Diagnostic->
Line 2: Diagnostic information 1
Line 3: Diagnostic information 2
Line 4: Diagnostic information 3
Line 5: <-End Diagnostic->
```

The information relating to a monitor diagnostic can be viewed in the alert details, specifically, in the **Diagnostic summary** field. For more information, refer to section "**Viewing alert information**" on page **250**.

## How to work with a component monitor

### 1. Loading the component monitor into the Panda Systems Management platform

- Go to general menu **Components** and click **New Component** from the left-side panel. Select **Device Monitors** from the **Category** drop-down list and click the **Save** button.
- Set the **Component** Level. This field determines which users can access this component. For more information, refer to section "**Adding a user account**" on page **278**.
- Select the scripting language to use, in this example VBScript.
- Enter the script source code in the text box. Refer to section "**Quarantine monitor**" on page **299** to get the full script for this example.
- Set the maximum execution time of the component. After this time has elapsed, the agent will interrupt execution.

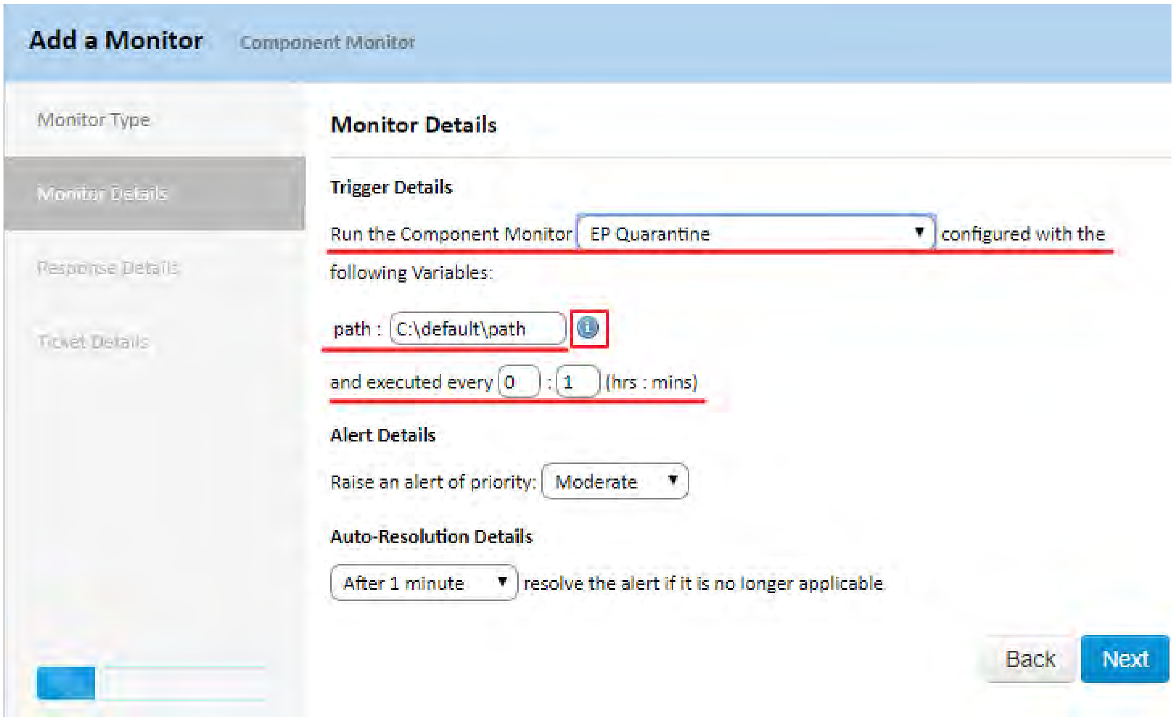
> *It is recommended to develop very light components that are executed very quickly.*

- Click the ⊕ icon to set the **input** and **output variables.**
  - In our example, EP_PATH will be the script input variable defined in the monitor settings by the administrator. It will contain the path to the Panda Endpoint Protection quarantine folder. Choose **Variable Value** from the **Type** drop-down as the variable will contain a character string. If the quarantine path is the same for most user computers, enter it in the **Default** field. If you want a description to be displayed that can guide the administrator as to the type of data to enter when creating the monitor, enter it in the **Description** field.
  - `Result` will be the output variable which will show the script result.
- Click **Save** to add the component to the repository. The new component will be immediately displayed on the list.

### 2. Monitor distribution through account policies or site policies

- If you are developing a monitor, a **monitoring** site policy or account policy must be created.
- Add the **Target** (Windows 7) and a **Component Monitor**.
- From the drop-down list, select the newly created component. This will display the input variables configured when creating the script, in this case EP_Path. It will show the content of the text box associated with the input variable, and the default value specified when creating the monitor (**Default** field) plus the ⓘ icon if a description for the variable was entered (**Description** field). Place

the mouse pointer over the icon to see the description.



Monitor Details

Trigger Details

Run the Component Monitor EP Quarantine configured with the following Variables:

path : C:\default\path

and executed every 0 : 1 (hrs : mins)

Alert Details

Raise an alert of priority: Moderate

Auto-Resolution Details

After 1 minute resolve the alert if it is no longer applicable

Figure 10.4: Configuring a component monitor

- Specify how frequently the script will be run (in our example, every 10 minutes), the severity of the alert that Panda Systems Management must create when the monitor returns an error condition, and whether the alert will be automatically resolved after a certain time or whether it will be resolved manually by the administrator (N/A).
- For the server to generate an email when new items are detected in quarantine, define an email response (`Respond`) with the recipient's address. The content of the `Result` response variable will be copied to the email that will be sent to the administrator.
- After a monitor has been created, a line will be added to the Policies screen. This screen can be accessed from the general menu **Account**, tab **Policies**, or from the general menu **Site**, by selecting the site that the policy was created for, and clicking the **Policies** tab. This will depend on the level that the policy was created at.
- To deploy the monitor, click **Push changes**. This will apply the policy, and the monitor will be deployed to all of the affected devices, triggering its execution.

### 3. Running the component

Once the monitor has been deployed to the devices, it will run every 10 minutes. To do this, it invokes the associated script parser, reads the necessary environment variables and writes the appropriate response.

Line 21 shows the `EP_PATH` environment variable. An object of type `FileSystemObject` is obtained that points to the quarantine folder.

```
Set WshShell=WScript.CreateObject (“WScript.Shell”)
Set objFSO=CreateObject (“Scrpting.FilesSystemObject”)

‘access to environment variable and quarantine path
On error resume Next
   Set WshSysenv=WshShell.Enviroment(“PROCESS”)
   Set objFolder=objFSO.GetFclder(WshSysEnv(“EP_PATH”))

   if err.number<>0 then
      ‘PCSM didn’t send the environment variable
     err.clear
     WScript.Echo”<-StartResult->”
     WScript.Echo”Result=PCOP_PATH variable not defined in PCSM console or path
not found”
     WScript.Echo”<-EndResult->”
     Set WshShell=nothing
     Set WsSysEnvy=nothing
     Set objFolder=nothing
     WScript.Quit(1)
   end if
On error goto 0
```

Lines 23 to 34 control whether the environment variable is defined. If the variable were not defined in the console, an error in the Result variable is returned and execution terminates with `Errorlevel 1` (line 34).

Since the purpose of the monitor is to check whether there is an increase in the number of files located in a directory and each execution calculates the number of files only once, the script will have to be launched at least twice to be able to compare the number of files obtained at two different times (every 10 minutes according to the monitor settings). This creates the need to have a communication mechanism between two successive executions of the script. This way, it will be possible to retrieve the count from the previous execution and compare it with that of the current execution. Since each execution of a monitor is independent from the rest, the ideal method for exchanging data between two executions is to use the device's own resources. It is recommended to use the Windows registry for this purpose, although temporary files can also be used.

Line 42 shows the file count stored in the previous execution. If this data does not exist because this is the first time that the component is executed, the count will be set to 0 (line 45). The current count is stored in the registry in line 49.

```
‘access to registry for saving the count
On error resume Next
    ‘get previous file count
    iCountPast= cint(WshShell.RegRead(“HKLM\Software\Panda Security\Monitor”))
   if Err.Number<>0 then
      ‘if error set to 0
       iCountPast=0
   end if
   iCountNow=colFiles.count
   ‘save the count
   WshShell.RegWrite “HKLM\Software\Panda Security\Monitor”, iCountNow, “REG_SZ”
```

### 4. Sending information and data processing on the platform

After the script finishes running, the PCSM server checks to see if the return code is 0 or 1. If the code is 0, the script execution is considered correct, and the PCSM server will read the standard output in search of the Result variable between the strings "<-Start Result->" and "<-End Result->". With this information, the actions configured in the monitor will be performed. If the return code is 1, the execution will be considered failed.

```
if iCountPast < ICountNow then
  ‘there are more items in the folder, it sends data
  WScript.Echo “<-Start Result->”
  WScript.Echo “Result=” & ICountNow - iCountPast & “new items in PCOP quarantine”
  WScript.Echo “<-End Result->”
  Wscript.Quit (1)
else
  WScript.Quit (0)
```

# How to use global variables

If new scripts are developed frequently, it is highly probably that you will want common data in all of them, such as paths to specific folders on the user's hard disk, the letters of shared drives on servers, or even common credentials to execute certain tasks.

A possible solution is to add all of the data needed to each script, so that if the data changes, every script developed will have to be updated manually and redistributed to the devices.

The most convenient option, however, is to define global variables at site or account level that can be used directly by the scripts.

## Defining global variables

- Go to general menu **Setup** and click **Account settings** from the drop-down list, or go to general menu **Sites**, select a site and click **Settings** from the tab bar, depending on the level at which you want to create the variables. Variables created at Site level will overwrite the variables created at Account level provided they have the same name.

- Scroll down to section **Variable Name**, and click the **Add Variable** link.
- Select the **Mask Value** checkbox if the information to store is sensitive, such as user names and passwords.

When distributing the script, the server will send the content of the variable to the agent, which will create environment variables on the user's device, which will be easily accessible to the scripts you have designed.

## Labels and user-defined fields

In addition to generating alerts and sending emails to administrators when its parameters fall outside the configured threshold, a monitor can automatically populate and update user-defined fields.

*Refer to section "***User-Defined fields***" on page* **182** *for more information on how to access the user-defined fields feature and how to use them.*

Automatically updating **user-defined fields** with a monitor allows you to reflect in the console the status of parameters not directly supported by the PCSM agent.

### Writing user-defined field information to Windows devices

The content of the user-defined fields is taken from the `HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\CustomX` branch in each device's Windows registry, where X is a number between 1 and 30. Each of these branches can contain a string of up to 65534 characters.

A component can freely write to the specified branches, so that the agent will read them on launching an automatic audit (every 24 hours) or manual audit (on-demand) and will send the information to the server, which will display it in the console. Furthermore, the agent will delete this information from the registry of the device once it has been read and sent to the server.

*If the script language used to develop the component monitor does not have access to the write API in the registry, use the following command line to add values:*

*REG ADD HKEY_LOCAL_MACHINE \ SOFTWARE \ CentraStage / v CustomField / t REG_SZ / d "Value" / f*

*Where:*

***CustomField*** *is the name of the field (Custom1, Custom2, Custom3, etc.).*

***Value****: is the content of the field.*

### Accessing the content of user-defined fields

Within the script, Panda Systems Management automatically assigns the content defined in the user-defined fields to the UDF_X variables, where X is the number corresponding to the relevant user-defined field.

### Writing user-defined field information to Linux and macOS devices

The **user-defined field** information on Linux and macOS systems is located in a file called values.xml in the following paths.

- **On macOS**

```
/var/root/.mono/registry/LocalMachine/software/Centrastage/values.xml
```

or

```
/var/root/.mono/registry/CurrentUser/software/Centrastage/values.xml
```

- **On Linux**

```
/root/.mono/registry/LocalMachine/software/Centrastage/values.xml
```

or

```
/root/.mono/registry/CurrentUser/software/Centrastage/values.xml
```

The `values.xml` file has the following format:

```
<values>

<value name="DeviceID" type="string">YourDeviceID</value>

<value name="Custom1" type="string">CustomValue</value>

</values>
```

Where:

- **YourDeviceID**: this is the device's internal ID. It corresponds to the **ID field** located in the **Device Data** section on the **Audit** tab (**Hardware** selection control).
- **CustomValue**: this is the **Custom** field value specified in the Value branch attribute (Custom1 in our example).

## Creating a script component

A script component is created in exactly the same way as a component monitor.

- Go to general menu **Components**, and click **New Component**.
- Select **Scripts**.

- The settings screen for a script component only differs from the settings screen for a component monitor in the information collection section: You cannot define output variables, but instead you can set strings to be searched for in the standard output (stdout) or error output (stderr) to trigger warnings in the console.
- To use a script component, first mark it as favorite in the component list by clicking the star icon. It will then appear in the quick job and scheduled job lists.

# Editing components

Components imported or added from the ComStore cannot be modified directly; Panda Systems Management only allows direct modification of the components developed by the administrator.

To modify a component imported or added from the ComStore, and adapt it to the needs of the network to manage:

- In general menu **Components**, click the documents icon to copy the component.
- The component edit window will open, where you can edit its associated script command, its name, and other features.
- To edit an already copied component, click its name. If you cannot click a component's name it is because it has not been previously copied.

# Part 4

# Device visibility

**Chapter 11:** Assets Audit

**Chapter 12:** Device visibility and status

**Chapter 13:** Reports

Chapter 11

# Assets Audit

Panda Systems Management helps you catalog all your hardware and software assets and monitors the appearance of any new devices and the software installed on them by monitoring the paid licenses that the company has acquired.

CHAPTER CONTENT

# Access and availability of the audit service

The **Audit** tab is available in the three supported levels (Account, Zone and Device) showing information with a variable level of detail from the most generic to the most precise, according to the selected level.

All these features are available through the **Audit** tab in the tab bar.

- To access the auditing features at Account Level, go to general menu **Account, Audit** tab.
- To access the auditing features at Site level, go to general menu Sites, select a site and click the Audit tab.
- To access the auditing features at Device level, go to general menu **Sites**, select the site where the device is located, click the device and click the **Audit** tab.

*The data in the **Audit** tab is refreshed automatically every 24 hours. It can also be refreshed on demand at any time by clicking the icon from the icon Bar.*

The information provided is grouped into several sections depending on the Level and accessible from the upper right of the **Audit** window, by clicking on the appropriate selection control **(1)**:

- **Network**: the network audit is the process by which Panda Systems Management discovers devices on the network and is executed by the teams that have the assigned Network Node role.
- **Hardware**: Devices on the customer's network, installed hardware, etc.
- **Software**: Software on the devices with the Agent installed.
- **Licensing**: Details of the software licenses used.
- **Services**: Shows the services installed on Windows computers and their status.
- **Change log**: logs system, software and hardware changes. Activity logging is considered a security feature and is discussed in chapter **“Activity log” on page 289**.

- **Activity log**: logs the jobs run on the device, regardless of their origin.

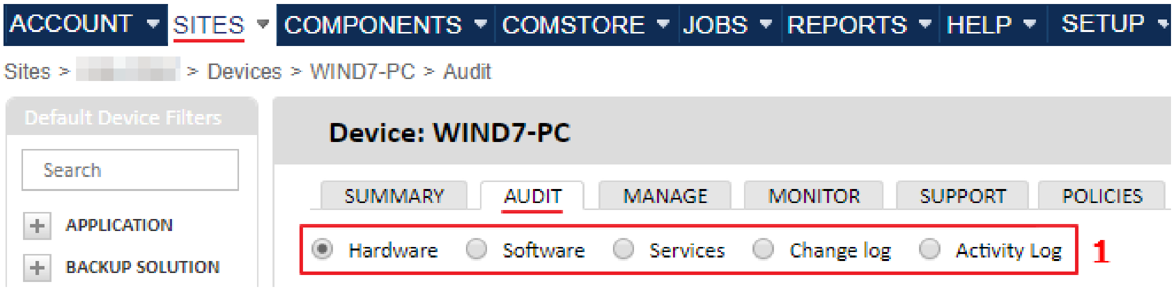


Figure 11.1: audit screen

## Accessing the information depending on the level selected

Certain sections will be available depending on the level selected (Account, Site or Device). Below there is a table with the type of information available in accordance with the level selected.

| Section / Level | Account | Site | Device |
|---|---|---|---|
| Network | YES | YES | NO |
| Hardware | YES | YES | YES |
| Software | YES | YES | YES |
| Licensing | YES | YES | NO |
| Services | NO | NO | YES |
| Changes | NO | NO | YES |
| Activity log | YES | NO | YES |

Table 11.1: auditing features based on the selected level

## Full and delta audits

Panda Systems Management supports various types of audits based on the volume of data and when they are run:

- **Automatic audit**: a device audit is performed automatically at the time the PCSM agent is installed on the device and on a regular schedule. For more information, refer to section "**Frequency of audits**".

- **Manual audit**: every time you click the 🔍 icon from the icon bar, the PCSM agent performs a manual audit.

- **Full audit**: this is a complete inventory audit of a device.

- **Partial audit**: this is a delta audit containing a list of the changes to the audit information on the device since the last audit.

*Delta audits are not available for mobile devices (smartphones and tablets).*

### Frequency of audits

| Device type | Full audit | Delta audit |
|---|---|---|
| **Compatible with the PCSM agent** | • Right after PCSM agent installation.<br>• Anytime by clicking the 🔍 icon from the icon bar when a single device is selected. | • Every 24 hours.<br>• Upon successful completion of a job.<br>• After all patches of a patch policy have been applied. If a reboot is required, the audit will run after the reboot.<br>• Anytime by clicking the 🔍 icon from the icon bar when multiple devices are selected. |
| **Network devices** | • When a device is assigned a Network Node.<br>• When the device's device type is updated.<br>• Anytime by clicking the 🔍 icon from the icon bar.<br>• Every 24 hours. | Not applicable |

Table 11.2: execution frequency of audits

# Network audit

### At Account level

Shows the number of devices discovered in all sites in the account, grouped by type. The table below details the fields on this list:

| Field | Description |
|---|---|
| **Name** | Name of the site. Only displays those sites where devices have been discovered that are not integrated in Panda Systems Management. |
| **Description** | Description of the site. |
| **Windows** | Number of discovered devices identified as Windows. |
| **Mac** | Number of discovered devices identified as macOS. |
| **Network** | Number of discovered devices identified as network devices. |
| **Printer** | Number of discovered devices identified as printers. |

Table 11.3: network audit at Account level

| Field | Description |
|---|---|
| **ESXi** | Number of discovered devices identified as ESXi. servers. |
| **Unknown** | Number of discovered devices that could not be identified. |

Table 11.3: network audit at Account level

### At Site level

Shows all devices discovered in the site, and provides the ability to remotely install the PCSM agent on your devices.

> *Refer to section "**Device discovery (network scanning)**" on page **63** for more information on how to discover devices and integrate them remotely into Panda Systems Management.*

The network audit screen is divided into the following sections:

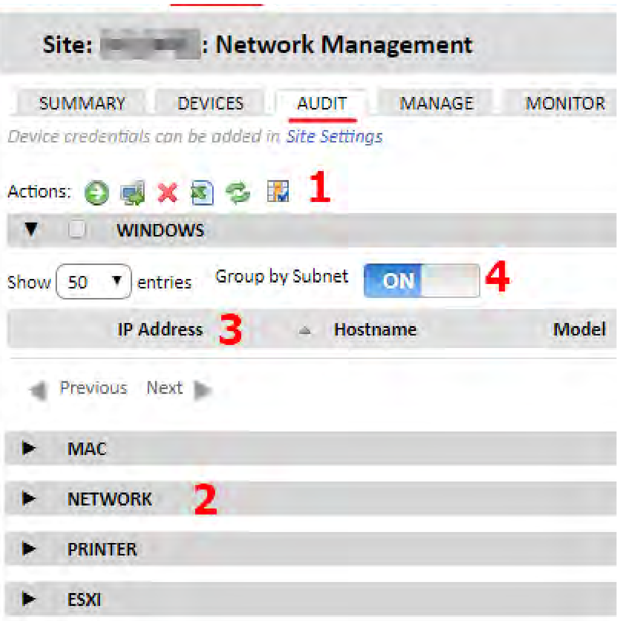


Figure 11.2: network audit at Site level

- **Icon bar (1)**: lets you perform actions on the discovered devices
- **Device groups (2)**: devices are grouped based on the features supported by Panda Systems Management for each type of device. If the group is not empty, it will show the total number of discovered devices of that particular type. Expand a group to display a checkbox to select all devices in the group at once.
- **List fields (3)**: show information about the relevant device. To add or remove a column, click the icon ▦.
- **Group by subnet (4)**: if there are devices that belong to different subnets, use this option to group them by subnet and keep the list of discovered devices organized.

The default fields for discovered devices are as follows:

| Field | Description |
|---|---|
| **Device icon** | The discovered devices are flagged with their corresponding device icon. |
| **IP Address** | The IP address of the device's network interface. |
| **Hostname** | The name of the device. |

Table 11.4: list of devices in a network audit at Site level

| Field | Description |
|---|---|
| **Description** | The description of the device. This can be edited on the **Summary** tab, at Device level. |
| **NIC Vendor** | The network card manufacturer. |
| **Model** | The model of the device. |
| **SNMP V1/V2 public** | Indicates if the device's SNMP credentials are v1/v2c and if the community string is set to public. |

Table 11.4: list of devices in a network audit at Site level

The icon bar allows for the following actions:

| Action | Description |
|---|---|
| **Manage Devices** | Lets you deploy and install the PCSM agent on compatible devices or integrate network devices into the platform. Refer to section "**Deploying the PCSM agent remotely**" on page **48**. |
| **Move Devices** | Lets you move the selected device(s) to another device type group. |
| **Delete Devices** | Lets you delete the selected device(s) from the list of discovered devices. However, the device will appear again next time a network audit is performed. |

Table 11.5: actions available form a network audit

# Hardware audit

## Account level

This shows the hardware platforms (models) used in the managed devices for all the account. A device's platform coincides with the make and model of the motherboard in custom or cloned devices and the trade name and model for assemblers of PCs and devices.

You will also see the number of devices for each platform.

Click the platform to display the devices managed by Panda Systems Management in line with the selected criteria.

## Site level

This displays information about the managed hardware discovered on the customer's network, divided into two different sections:

### Managed devices

Contains a list of the devices managed by Panda Systems Management on the network, grouped by model.

Click **Model** to see a list of the devices grouped according to their model.

### Unmanaged devices

Contains a manually-managed list of the network devices that are not managed by Panda Systems Management, but which the administrator wants to see in the Console for audit purposes.

Click the ⊕ icon from the icon bar to display a form for the administrator to enter relevant information about the unmanaged device.

## Device level

The Device Level audits are the most detailed, displaying all relevant information about the selected device. Some device types have editable fields marked as such on the **Summary** tab.

The content of the **Audit** tab changes depending on the type of device. The information displayed will be as follows:

### General

| Field | Description | Available for |
|---|---|---|
| **Hostname** | Device name. | All |
| **Description** | Character string identifying the device. | All |
| **Operating System** | Operating system installed on the device and internal version. | All |
| **Service Pack** | | Desktops, laptops and servers. |
| **Architecture** | The device's hardware architecture (32-bit or 64-bit). | Desktops, laptops and servers. |
| **Hyper-V Version** | Version of the Hyper-V virtualization engine. | Hyper-V servers. |
| **.NET Version** | .NET framework version installed. | Desktops, laptops and servers. |
| **Domain** | Windows domain the computer belongs to. | Desktops, laptops and servers. |
| **Last Reboot** | Date when the computer was last booted. | Desktops, laptops and servers. |
| **IMEI** | Mobile device ID. | Mobile devices. |

Table 11.6: general information of a device

## Storage

| Field | Description | Available for |
|---|---|---|
| **Disk Drive** | The drive's mount point. | Desktops, laptops and servers. |
| **Drive Type** | Type of storage medium (local disk, removable disk, optical media...). | Desktops, laptops and servers. |
| **Size** | Size of the storage drive. | Desktops, laptops and servers. |
| **Free** | Free space on the storage drive. | Desktops, laptops and servers. |
| **Description** | | Desktops, laptops and servers. |
| **Data Storage** | Name of the data store connected to the ESXi server. | ESXi servers. |
| **Storage** | String character identifying the data store hardware. | ESXi servers. |
| **File System** | The data store file system used by the ESXi server. | ESXi servers. |
| **Capacity** | Total data store space. | ESXi servers. |
| **Free** | Total data store space. | ESXi servers. |
| **Subscription** | Maximum potential capacity occupation of all virtual machines within the data store. Clicking this value displays all created logical drives along with the percentage of space used assigned to each of them. | ESXi servers. |
| **Status** | Storage system status (OK, Not OK). | ESXi servers. |

Table 11.7: storage system information

## Device Data

| Fields | Description | Available for |
|---|---|---|
| **Agent Version** | Internal version of the PCSM agent. | Desktops, laptops and servers. |
| **ID** | The internal ID of the device. | Desktops, laptops, servers, ESXi servers. |
| **Last Seen** | The last time that the PCSM agent contacted the PCSM server. | All |
| **Create Date** | Date when the Device level was created for the device in question. | Desktops, laptops, servers, ESXi servers. |
| **Enrollment Date** | Date when the mobile device was integrated into the PCSM platform. | Mobile devices. |

Table 11.8: Information about the PCSM agent installed on the device

| Fields | Description | Available for |
|---|---|---|
| **Last Audit Date** | Date when the last full audit was run on the device. | All |

Table 11.8: Information about the PCSM agent installed on the device

## Hardware

| Field | Description | Available for |
|---|---|---|
| **Manufacturer** | Name of the manufacturer of the device or the operating system in the case of virtual devices. | All |
| **Model** | Device model or "Virtual machine" string. | All |
| **Serial Number** | Serial number manually assigned to the device. | Desktops, laptops, servers, ESXi servers. |
| **Motherboard** | Device motherboard model. | Desktops, laptops, servers, ESXi servers. |
| **Processor** | Make and model of the installed microprocessor. | Desktops, laptops, servers, ESXi servers. |
| **Physical Cores** | Number of cores installed on the microprocessor. | Desktops, laptops, servers, ESXi servers. |
| **Memory** | Amount of memory installed on the device. | Desktops, laptops, servers, ESXi servers. |
| **Display Adapter** | Manufacturer and model of the video card installed. | Desktops, laptops, servers, ESXi servers. |
| **Monitors** | Make and model of the monitor connected to the device. | Desktops, laptops, servers, ESXi servers. |
| **BIOS Name** | Manufacturer of the device's BIOS. | Desktops, laptops, servers, ESXi servers. |
| **BIOS Version** | Version of the device's BIOS. | Desktops, laptops, servers, ESXi servers. |
| **BIOS Release Date** | Release date of the BIOS. This value is used in reports to determine the device's obsolescence. | Desktops, laptops, servers, ESXi servers. |
| **Power Rating** | | Desktops, laptops, servers, ESXi servers. |
| **ICCID** | SIM card ID. | Mobile devices. |
| **Operator** | Company that provides the telephony service. | Mobile devices. |
| **Number** | Mobile number. | Mobile devices. |

Table 11.9: information about the hardware installed on the device

## Network Adapters

| Field | Description | Available for |
|---|---|---|
| **Adapter** | Name of the network card installed. | All |
| **MAC address** | Physical address of the network card. | All |
| **Speed** | Megabits per second and duplex mode negotiated by the network. | ESXi servers and mobile devices. |

Table 11.10: information about the network cards installed on the device

## Processor

| Field | Description | Available for |
|---|---|---|
| **Name** | Make and model of the physical processor installed on the device. | ESXi servers. |
| **Speed** | The processing speed (measured in Megahertz) of the installed microprocessors. | ESXi servers. |
| **Total Cores** | Number of physical cores available on the ESXi server. | ESXi servers. |

Table 11.11: information about the microprocessor installed on the device

## Guest Info

| Field | Description | Available for |
|---|---|---|
| **Hostname** | Name of the ESXi server that hosts the virtualized system. | ESXi servers. |
| **Guest Name** | Name of the virtualized device. | ESXi servers. |
| **Operating System** | Operating system installed on the virtualized device. | ESXi servers. |
| **Data Storage** | Data storage assigned to the virtual device. | ESXi servers. |
| **CPU** | Virtual CPU assigned to the virtualized device. | ESXi servers. |
| **RAM** | Size of the RAM memory assigned to the virtualized device. | ESXi servers. |
| **Snapshots** | Number of snapshots (restore points) taken from the virtual machine. | ESXi servers. |

Table 11.12: Information about virtual machines

## IP Information

| Field | Description | Available for |
|---|---|---|
| **Internal IP Address** | IP address assigned to the network adapter. | Desktops, laptops, servers, ESXi servers. |
| **Ext IP Address** | IP address with which the device accesses external resources located outside its internal network. | Desktops, laptops, servers, ESXi servers. |
| **Additional IP(s)** | Network aliases. | Desktops, laptops, servers, ESXi servers. |

Table 11.13: information about the TCP/IP connections

## Memory

| Field | Description | Available for |
|---|---|---|
| **Module** | ID of the memory chip made up of the bank it is connected to and the memory implementation technology. | Desktops, laptops, servers, ESXi servers. |
| **Type** | Memory implementation technology. | Desktops, laptops, servers, ESXi servers. |
| **Part Number** | Part number of the memory chip. | Desktops, laptops, servers, ESXi servers. |
| **Serial Number** | Serial number of the memory chip. | Desktops, laptops, servers, ESXi servers. |
| **Capacity** | Memory chip size. | Desktops, laptops, servers, ESXi servers. |
| **Speed** | Internal frequency of the memory chip. | Desktops, laptops, servers, ESXi servers. |

Table 11.14: information about the memory installed on the device

## Attached Devices

| Field | Description | Available for |
|---|---|---|
| **Type** | Type of external device attached to the computer. | Desktops, laptops and servers. |
| **Name** | Volume named of the attached device. | Desktops, laptops and servers. |
| **Driver Name** | Internal name of the driver. | Desktops, laptops and servers. |
| **Driver Manufacturer** | Company that developed the driver. | Desktops, laptops and servers. |

Table 11.15: information about the drivers that manage external storage devices

| Field | Description | Available for |
|---|---|---|
| **Driver Version** | Internal version of the driver. | Desktops, laptops and servers. |
| **Driver File** | Name of the file that contains the driver. | Desktops, laptops and servers. |
| **Driver File Last Modified** | Date the driver was last updated. | Desktops, laptops and servers. |
| **Port Name** | Name of the physical port the device is attached to. | Desktops, laptops and servers. |

Table 11.15: information about the drivers that manage external storage devices

# Software audit

## Account level

This displays all the information about the software installed on the devices found on the customer's network organized by program name and version.

Click on a program name to see the list of devices that have it installed and perform actions on them as a group, such as version upgrades or running scripts to uninstall software packages.

## Site level

The listed programs are those installed on the devices on the selected site. The type of information is the same as that described for Account level in the previous point.

## Device level

The listed programs are those installed on the selected device. The type of information is the same as described for Account level above.

# License audit

## Account level

The aim of the license audits is to determine the number of installations of each program, and as such calculate the number of licenses that the company is using and those that need to be bought.

To this end, it is possible to group several programs together and Panda Systems Management will compare these groups with the software installed on devices.

### Packages

Creating a group or software package makes sense when the programs in the group are licensed or bought as a single entity. For example, the Microsoft Office package comprises several programs which companies would not normally buy separately (Word, Excel, PowerPoint etc.). In this case, the fact that one of these programs is installed would indicate the need to buy licenses for the whole package.

*To add independent programs to the PCSM console, you will have to create a package with just one item.*

Creating packages at Account Level is recommended if common software is used on the various managed sites. This way, the most effective way to avoid duplicating the definition of packages on each site is to define all possible software packages at Account level and activate them on the necessary Site levels.

### Creating a software package

Click the icon from the icon bar to display a window with all the relevant information:

- **Name**: Name of the software package.
- **Search**: Find a certain program in a list of all the programs installed on the devices managed through the Panda Systems Management account.
- **All**: Select all programs that coincide with the criteria selected in the **Search** field.
- **Specific**: Lets you select a specific program (and version) from the list and include it in the package.

Once the package is created it will be displayed in the list of software packages, including the name, the programs that comprise the package and the number of devices in the account that have any of the programs that are included in the package.

*At Account level you can only create and configure packages. To configure alerts that warn the administrator of the absence of licenses, you must go to Site level.*

## Site level

At Site level you can also create packages as with Account level, although only for the software installed on the devices that are included in the site.

Also, at Site level not only can you define software packages or use those defined at Account level, you also have the option to define the maximum number of installations allowed for the site.

This way, when the number of devices that use a certain package exceeds the number of licenses available configured by the administrator in the console, an alert is triggered that will warn the administrator of the need to buy more licenses.

### Creating a software package

The process of creating a software package is the same as that described for Account level.

### Importing a software package created in Account level

Click the icon bar to display all the software packages created in Account level and Site level. Use the checkboxes to select those to import to the Site.

### Configuring a maximum number of licenses

Once you have added the software packages, a table is displayed with the following information:

- **Software package**: Configured software package. Click the name to open a window through which you can edit the package settings.
- **Quantity**: Number of times that the software in the package has been seen on devices in the managed site.
- **Alert**: Maximum number of installations allowed. If the number of installations exceeds this amount an alert will be sent to the administrator.

# Services audit

## Device level

This displays the services installed on a device along with the current status and the startup type.

- **Display Name**: the service name displayed on the list of services installed on the device.
- **Service name**: Internal name of the service.
- **Status at the last audit**: Service status (**running**, **stopped**) the last time the device was audited.
- **Startup type**: Service startup configuration (**Auto**, **manual**, **disabled**).

# Changes audit

## Device level

This displays the changes to hardware and software that have been made on the device along with the date they took place.

This lets administrators diagnose problems on devices that are not operating correctly, as such issues could be related to changes made on the computer.

The changes are grouped in three blocks:

- **System Changes**: This shows the changes to operating system modules on the device.
- **Software Changes**: This shows software installed, updated or deleted from the device.
- **Hardware Changes**: This shows hardware installed or removed from the device.

# Activity audit

## At Account level

Shows those devices that were moved between sites:

| Field | Description |
|---|---|
| **Type** | Device movement between sites. |
| **Device** | Name of the moved device. |
| **Name** | Description of the activity, indicating the start location (site), end location (site) and the management console user who performed the operation. |
| **Started** | Start date of the activity. |

Table 11.16: meaning of the fields that describe device movement between sites

## At Device level

Shows all activities associated with a specific device regardless of its origin:

| Field | Description |
|---|---|
| **Type** | The type of activity represented by its icon. |
| **Name** | The name of the activity. |
| **Started** | Start date of the activity. |
| **Ended** | End date of the activity. |
| **Policy** | If the activity involves applying a policy, the name of the policy that targeted the device. |
| **Status** | The status of the activity (**Running**, **Completed**, **Failed**, etc.). |
| **Results** | Result code returned by the activity. In some cases, a summary icon is displayed for you to access more information. |
| **Progress** | A color indicator of the progress of the activity: green (**completed**), red (**failed**), orange (**warning**). |

Table 11.17: meaning of the fields that describe the activities performed on devices

| Field | Description |
|---|---|
| **Stdout** | Copy of the standard output of the activity. |
| **Stderr** | Copy of the standard error of the activity. |

Table 11.17: meaning of the fields that describe the activities performed on devices

# Chapter 12

# Device visibility and status

Panda Systems Management provides a series of tools to view the status of devices. Depending on the tool, the information is either summarized and consolidated for the group of supported devices (group, filter, site and account) or detailed and individualized for each device on the platform.

CHAPTER CONTENT

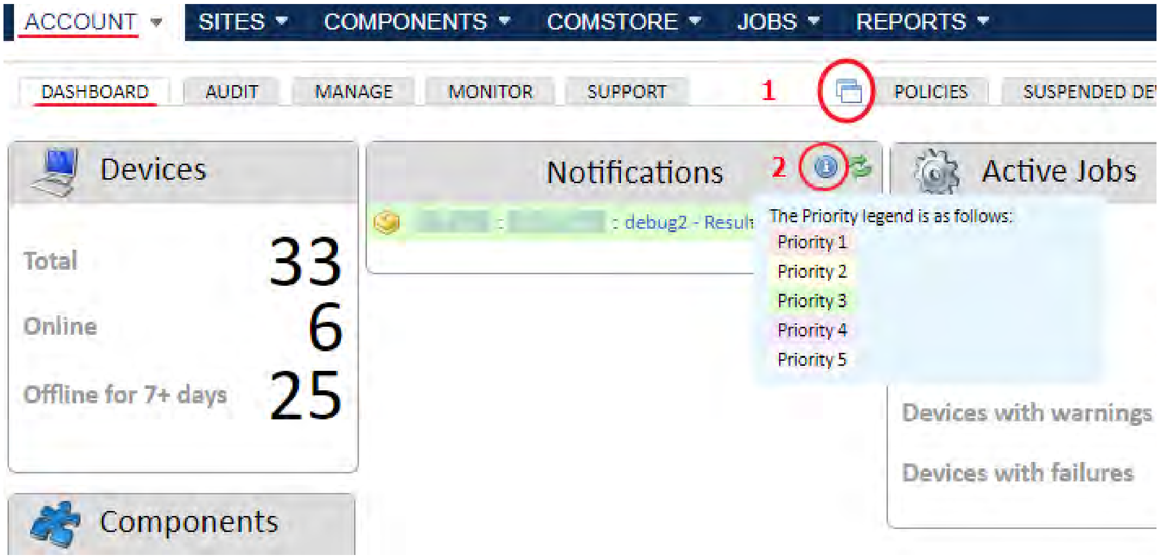
# Device status

The tools available to view the status of devices are as follows:

- **General dashboard**: available at Account and Site level.
- **Site dashboards**: available from the **Summary** tab in a site.
- **Lists of devices and sites**: available from Account level.
- **Device details**: available from the **Details** tab for a device.

# General dashboard

## Aim



[redacted] : [redacted] : debug2 - Result

The Priority legend is as follows:

Figure 12.1: kiosk mode of the general dashboard

Shows a summary of all the devices integrated in the Panda Systems Management platform to analyze the status of the company's IT resources at a glance.

To display the dashboard in kiosk / full screen mode, click the following icon 🗗 **(1)**.

## Access

Go to general menu **Account**, and click **Dashboard** from the tab bar.

## Data displayed

The data is organized into the following sections:

- **Devices**: this displays the number of devices integrated on the platform, grouped by their connection status.
- **Components**: this shows the number of components integrated in the account and in the ComStore.
- **Active jobs**: this shows the number of jobs created, grouped by status.
- **Open alerts**: this shows the number of alerts, grouped by priority.
- **Notifications**: this shows the alerts generated by the devices in the account.

### Devices

| Field | Description |
|---|---|
| **Total** | Total number of devices integrated in Panda Systems Management. |
| **Online** | Total number of devices connected at that moment. |
| **Offline for 7+ days** | Total number of devices that have not connected to the Panda Systems Management server in over a week. |

Table 12.1: number of devices integrated in Panda Systems Management

### Components

| Field | Description |
|---|---|
| **Total** | Number of components added to the account repository and accessible through general menu **Components**. |
| **ComStore** | Number of components published by Panda Security in the ComStore. |
| **Updates** | Number of components with updates released and still to be applied in the account repository. |

Table 12.2: number of components integrated in the account

### Notifications

| Field | Description |
|---|---|
| **Icon** | Type of notification. |
| **Site** | Site of the device that generated the alert. |

Table 12.3: list of account notifications

| Field | Description |
|---|---|
| **Device name** | Device that generated the alert. |
| **Information** | Alert summary. |
| **Time** | Time elapsed since the alert was generated. |
| **Color** | Each notification has a background color according to its priority. For a key to the colors and their priorities, hover the mouse pointer over the ⓘ icon at the top of the notifications table. **(2)** (Figure 12.1). |

Table 12.3: list of account notifications

## Active jobs

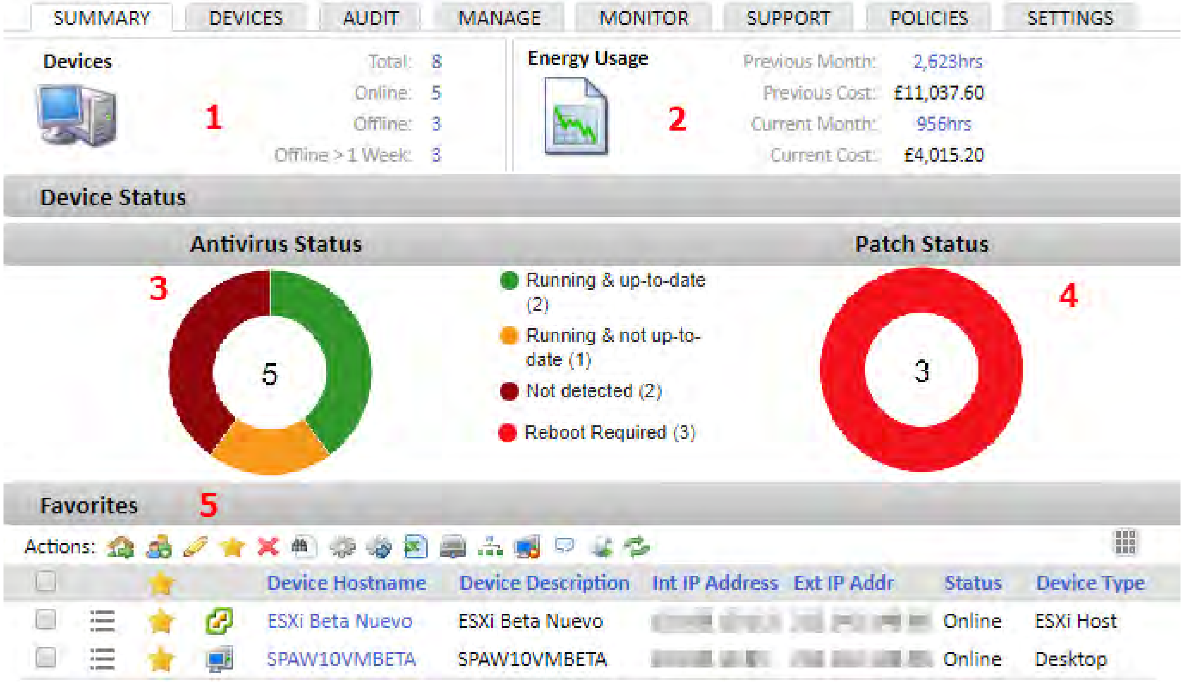
| Field | Description |
|---|---|
| **Devices scheduled** | Number of devices with a scheduled job assigned. If a device has several jobs, it is only counted one. |
| **Devices running** | Number of devices with a scheduled job running. |
| **Devices with warnings** | Number of devices that have sent a post-condition message advising of an alert. |
| **Devices with failures** | Number of devices that have returned an error running a job. |

Table 12.4: information about the alerts generated by jobs

## Open alerts

This shows the number of devices with open alerts, grouped by priority.

# Site dashboards



Devices

| | |
|---|---|
| Total: | 8 |
| Online: | 5 |
| Offline: | 3 |
| Offline > 1 Week: | 3 |

Energy Usage

| | |
|---|---|
| Previous Month: | 2,623hrs |
| Previous Cost: | £11,037.60 |
| Current Month: | 956hrs |
| Current Cost: | £4,015.20 |

Device Status

Antivirus Status

- 🟩 Running & up-to-date (2)
- 🟧 Running & not up-to-date (1)
- 🟥 Not detected (2)
- 🔴 Reboot Required (3)

Patch Status

Favorites

| □ | | ★ | | Device Hostname | Device Description | Int IP Address | Ext IP Addr | Status | Device Type |
|---|---|---|---|---|---|---|---|---|---|
| □ | ☰ | ★ | | ESXi Beta Nuevo | ESXi Beta Nuevo | [redacted] | [redacted] | Online | ESXi Host |
| □ | ☰ | ★ | | SPAW10VMBETA | SPAW10VMBETA | [redacted] | [redacted] | Online | Desktop |

Figure 12.2: site dashboard

## Aim

This shows statistical and status information of the devices in the selected site. The dashboard shows the energy usage of the devices, as well as the status of the antivirus and the patch status of the device.

Use the site dashboard for rapid access to computers marked as **Favorites**, those that require special attention, and the **Notes** tool, which lets you set reminders and enables the exchange of messages between administrators.

## Access

Go to general menu **Sites**, select a site and click the **Summary** tab.

## Data displayed

Each block of information shown is referred to in figure 12.2 on page 171.

## Devices (1)

| Fields | Description |
|---|---|
| **Total** | Total number of devices integrated in the site. |
| **Offline** | Total number of devices integrated in the site connected to the PCSM server at that moment. |
| **Online** | Total number of devices integrated in the site connected to the PCSM server at that moment. |
| **Offline > 1 Week** | Total number of devices integrated in the site that have not connected to the PCSM for over a week. |

Table 12.5: summary of the number of devices integrated in Panda Systems Management and status

## Energy Usage (2)

| Field | Description |
|---|---|
| **Previous month** | Total number of hours that the devices in the site have been switched on during the previous month. |
| **Previous cost** | Cost corresponding to the number of hours that the devices in the site have been switched on in the last month and the price per Kw/h in pounds sterling. |
| **Current month** | Total number of hours that the devices in the site have been switched on during this month. |
| **Current cost** | Cost corresponding to the number of hours that the devices in the site have been switched on in this month and the price per Kw/h in pounds sterling. |

Table 12.6: cost corresponding to the energy consumed by the devices in the site

## Antivirus Status (3)

*See section "**Installed antivirus audit**" on page* **183** *for more information on how to configure Panda Systems Management and get the information about the antivirus installed on the device.*

| Field | Description |
|---|---|
| **Pie chart** | Graphic description of the lists concerning the presence of an antivirus on the site devices, the antivirus status and the signature file status. |
| **Running and up-to-date** | Number of devices in the site with an antivirus installed and running and with an up-to-date signature file. |
| **Running and not up-to date** | Number of devices in the site with an antivirus installed and running but with a signature file more than three days old. |
| **Not running** | Number of devices in the site with an antivirus installed but not running. |

Table 12.7: Antivirus information

| Field | Description |
|---|---|
| **Not detected** | Number of devices in the site without an antivirus installed or with one that is not supported. See section "**Installed antivirus audit**". |

Table 12.7: Antivirus information

### Patch Status (4)

| Field | Description |
|---|---|
| **Pie chart** | Graphic illustration of all the lists regarding patching of the operating systems on the devices in the site. |
| **No policy** | Number of computers in the site without a patching policy. |
| **No data** | Number of computers in the site that have not sent patch information to Panda Systems Management. |
| **Reboot required** | Number of computers in the site that require a restart to complete the patching process. |
| **Install error** | Number of computers in the site with errors in the patching process. |
| **Approved pending** | Number of computers in the site with approved patches pending installation. |
| **Fully patched** | Number of computers in the site up-to-date with patches. |

Table 12.8: patch status

### Favorites (5)

The **Favorites** area can be used to enable a rapid view of problematic devices or those under observation. See section "**Favorites**" on page **88** to select a device as favorite.

The **Favorites** area includes a complete icon bar to take action on selected devices and the column selector discussed in sectio "**Device lists**".

### Notes

You can enter comments or reminders for other administrators in the **Notes** section of the dashboard.

## Site list

### Aim

This shows the sites in which the devices integrated in Panda Systems Management are distributed, and provides basic information about the settings in each site.

### Access

Click **Sites** in the main menu.

### Data displayed

| Field | Description |
|---|---|
| **Name** | Site name. |
| **Description** | Description of the site. |
| **ID** | Internal identifier used by Panda Systems Management. |
| **Devices** | Number of devices in the site. |
| **Offline** | Number of devices in the site that are offline. |
| **Proxy** | The site's proxy settings for accessing the Internet. |

Table 12.9: information about the sites created in the account

# Device lists

### Aim

To show key data about the devices that belong to a specific group and allow you to take action on them.

### Access

Follow the steps below according to the type of group:

- To access the list of devices for a group created at Account level, click **Sites** in the general menu and then the relevant group in the **Groups** side panel.
- To access the list of devices for a group created at Site level, click **Sites** in the general menu and then the relevant site and finally the group in the **Groups** side panel.
- To access the list of devices for a site, click **Sites** in the general menu, then the relevant site and finally select the **Devices** tab.

### Data displayed

To obtain key data regarding devices, the management console displays lists of computers with data fields that can be configured by administrators.

To configure the data displayed in any list of devices, click the ☑ icon. This icon is available from any list of devices (sites, groups or filters). The options available are as follows:

| Field | Description |
|---|---|
| **Checkbox** | Select the devices that will receive the actions indicated in the icon bar. |
| **Shortcuts** | Drop-down menu with the device tab menu and the action menu. |

Table 12.10: device attributes

| Field | Description |
|---|---|
| **Favorite** | Mark or unmark the selected device(s) as favorite for direct access. Refer to "**General organization of devices**" on page **89**. |
| **Device Status** | Icon representing the role and status of the device. |
| **ID** | Internal ID of the device. |
| **Site** | Name of the site the device belongs to. |
| **Hostname** | Name of the device. |
| **Description** | |
| **Int. IP Address** | Local IP address of the device. |
| **Additional IP(S)s** | IP alias(es). |
| **Ext. IP Address** | IP address of the router or the device through which it connects to the Internet. |
| **Last User** | Last user that connected to the device. |
| **Group** | Site device groups the device belongs to. |
| **Create Date** | Date the device was registered in the system. |
| **Last Seen** | Last time the server accessed the device. |
| **Last Audit Date** | Date of the last software and hardware audit. For more details, see chapter "**Assets Audit**" on page **151**. |
| **Session Name** | Currently not used. |
| **Favorite** | Select the device as a favorite for quick access from the system dashboards. |
| **Privacy Mode** | Device privacy mode. |
| **Agent Version** | PCSM agent version number. |
| **Web Port OK** | • **True**: The agent has successfully connected to the server and can send and receive data.<br>• **False**: The agent could not connect to the server. |
| **Network Node** | The agent has the Network Node role assigned. |
| **Status** | Status (**Online**, **Offline**). The **Online** status indicates that the PCSM agent can connect to the Control Channel to send "keep alives". |
| **Model** | |
| **Operating System** | |
| **Service Pack** | |
| **Serial Number** | |
| **Motherboard** | Make and model of the device motherboard. |
| **CPU** | Make, model and speed of the CPU. |

Table 12.10: device attributes

| Field | Description |
|---|---|
| **Physical CPU Cores** | Number of cores in the CPU. |
| **Memory** | Installed memory. |
| **MAC Address(es)** | Network card physical address. |
| **User-Defined Fields 1-30** | Content of the user-defined fields. For more details, see section "**User-Defined fields**" to determine their content manually, and section "**Labels and user-defined fields**" on page **145** to do from a script. |
| **Device Type** | Type of device (**workstation, laptop, tablet, smartphone, printer, network device, ESXi host**). |
| **Domain** | Windows domain the device belongs to. |
| **Disk Drive (total/free)** | Total size and usage of the storage drives installed on the device. |
| **Online Duration (hrs)** | Time that the PCSM agent has been connected to the Panda Systems Management server. |
| **Cost** | Device cost in accordance with its resource usage. |
| **Architecture** | 32 or 64 bits. |
| **Display Adapters** | Make and model of the graphics card installed on the device. |
| **BIOS Name** | BIOS make and model. |
| **BIOS Release Date** | Publication date of the device BIOS. This date is taken as the basis for calculating the obsolescence of devices in reports. See section "**Hardware lifecycle**". |
| **BIOS Version** | |
| **Last Reboot** | Date of the last reboot of the device. |
| **Reboot required** | Indicates whether the device needs to be rebooted to complete the installation process. |
| **.NET Version** | Framework.NET version installed on the device. |
| **Patches Approved Pending** | Number of approved patches pending installation. |
| **Patches Not Approved** | Number of published patches not approved. |
| **Patched Installed** | Number of patches installed. |
| **Patches Status** | Update status of the computer. |
| **Node Assignment** | Name of the Network Node assigned to the device. |
| **SNMP Description** | Description field of the SNMP settings of the device. |
| **SNMP Location** | Location field of the SNMP settings of the device. |
| **NIC Vendor** | Network card vendor. |
| **Manufacturer** | Device manufacturer. |
| **Antivirus Product** | Antivirus name. |

Table 12.10: device attributes

| Field | Description |
|---|---|
| **Antivirus Status** | Antivirus status: **Running and up-to date**, **Running and not up-to date**, **Not running**, **Not detected**. |
| **Warranty Exp. Date** | Warranty expiration date. |

Table 12.10: device attributes

## Search and filter tools

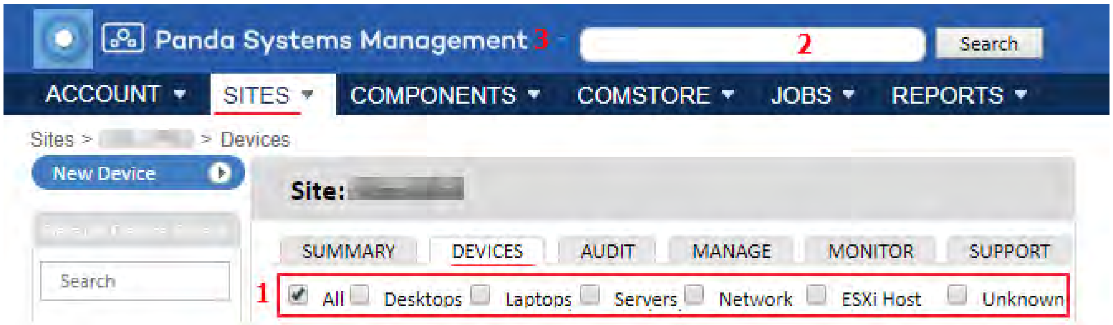


Figure 12.3: Search Tools and device filters

The lists let you search for and filter devices shown using two tools:

- **Filter by type of device (1)**: use the checkboxes to the right of the icon bar to filter the lists by device type (**All**, **Desktops**, **Laptops**, **Servers**, **Network**, **ESXi Host**, **Unknown**)
- **Text search (2)**: use the search bar at the top of the window to run searches of the device description fields. Click the ▼ icon **(3)** to specify the target field:
  - **hostname**: device **hostname** field.
  - **desc**: device **Description** field.
  - **serial**: device **Serial Number** field.
  - **IP**: device **Ext IP Addr**. field.
  - **lastuser**: device **Last User** field.
  - **sitename**: name of the site the device belongs to.
  - **sitedesc**: description of the site the device belongs to.

# Device details

## Aim

This shows the details of the hardware installed on the selected device, as well as its connection status, antivirus status, real-time monitoring status, job status, and resource usage along with other information.

*For more information about device status, click the **More...** link or the **Audit** tab. See section "**Assets Audit**" on page **151** for more details.*

## Access

From the **Sites** menu, select the site to which the device belongs and click the device. You will see the Device level view with the **Summary** tab selected.

## Data displayed

### Device information

| Field | Description | Available for |
|---|---|---|
| **Status Icon** | Shows the role and connection status of the device. | All. |
| **Hostname** | Name of the device and icon indicating the type of device. | All. |
| **Description** | Device description. Click **Edit** to change the description. | All. |
| **ID** | Internal ID. | Network devices. |
| **NIC Vendor** | Network card vendor. | Network devices. |
| **SNMP Name** | Name field of the SNMP protocol configured on the device. | Network devices. |
| **SNMP Description** | Description field of the SNMP protocol configured on the device. | Network devices. |
| **SNMP Location** | Location field of the SNMP protocol configured on the device. | Network devices. |
| **SNMP Contact** | Contact field of the SNMP protocol configured on the device. | Network devices. |
| **SNMP Uptime** | Uptime field of the SNMP protocol configured on the device. | Network devices. |

Table 12.11: Device information section

| Field | Description | Available for |
|---|---|---|
| **Create Date** | Date on which the device was integrated in Panda Systems Management. | Network devices. |
| **Last User** | Name of the user account that last logged in to the device. | Desktops, laptops and servers. |
| **Operating System** | Operating system installed on the device. | Desktops, laptops, servers, ESXi servers, and mobile devices. |
| **Domain** | Windows domain the device belongs to. | Desktops, laptops and servers. |
| **Last Reboot** | Last time the computer was rebooted. | Desktops, laptops and servers. |
| **Last Audit Date** | Date of the last time Panda Systems Management gathered audit information for the device. | Network devices. |
| **Internal IP Address** | Ip address assigned to the device's network card. | Desktops, laptops, servers, ESXi servers, and mobile devices. |
| **Ext. IP Address** | IP address used by the device to connect to resources outside the organization's local network. | Network devices, ESXi servers. |
| **MAC Address** | Physical address of the device network card. | Network devices. |
| **User-Defined Fields 1-30** | These are only displayed if they have been populated with information. See section "**User-Defined fields**" for more information on how to manually enter data into the user-defined fields. See section "**Labels and user-defined fields**" on page **145** to learn how to enter data from a script. | Desktops, laptops, servers, network devices, and ESXi servers. |
| **ESXi Credentials** | Connection credentials assigned to the ESXI server and defined in the Settings tad at Site level or Setup in the main menu. | ESXi servers. |
| **SNMP Credentials** | Connection credentials assigned to the SNMP device and defined in the Settings tab at Site level or Setup in the main menu. See section "**Improving device discovery via SNMP**" on page **65**. | Desktops, laptops, servers, ESXi servers, and mobile devices. |
| **Network Node** | Device with the Network Node role assigned. | Desktops, laptops, servers, network devices, ESXi servers. |
| **Last Seen** | Date on which the mobile device last connected to the Panda Systems Management. | Mobile devices. |
| **Enrollment Date** | Date on which the device enrolled in Panda Systems Management. | Mobile devices. |

Table 12.11: Device information section

| Field | Description | Available for |
|---|---|---|
| **Groups** | Groups to which the device belongs. | Desktops, laptops, servers, ESXi servers, and mobile devices. |
| **Device Type** | • Desktop<br>• Laptop<br>• Server<br>• Smartphone<br>• Tablet | Desktops, laptops, servers, network devices, ESXi servers, mobile devices. |
| **Manufacturer** | Device manufacturer. | Desktops, laptops, servers, network devices, ESXi servers, mobile devices. |
| **Model** | | Desktops, laptops, servers, network devices, ESXi servers, mobile devices. |
| **Serial Number** | | Desktops, laptops, servers, network devices. |
| **Power Rating** | Cost and power rating of the device. | Network devices, ESXi servers. |
| **Service/Asset Tag** | Text string to identify the server. | ESXi servers. |
| **Snapshots** | Number of snapshots taken of the virtual machines hosted on the ESXi server. | ESXi servers. |
| **Object ID** | | Network devices. |
| **Printed Page Count** | Counter of the number of pages printed. | Network devices (printers). |
| **GPS Latitude** | If the device has geo-location hardware, this indicates the latitude. | Mobile Devices. |
| **GPS Longitude** | If the device has geo-location hardware, this indicates the latitude. | Mobile Devices. |
| **GPS Last Update** | If the device has geo-location hardware, this indicates the time of the last known position of the device. | Mobile Devices. |

Table 12.11: Device information section

## Status

| Field | Description | Available for |
|---|---|---|
| **Device Status** | Device connection status: **Online**, **Offline**. | Desktops, laptops, servers, network devices, ESXi servers, and mobile devices. |

Table 12.12: Status section

| Field | Description | Available for |
|---|---|---|
| **Open Alerts** | Number of open alerts on the device. | Desktops, laptops, servers, network devices, ESXi servers, and mobile devices. |
| **Open Tickets** | Number of open tickets assigned to the device. | Desktops, laptops, servers, network devices, ESXi servers, and mobile devices. |
| **Warranty Date** | Expiration date of the device warranty. To enter a date, click **Edit**. | Desktops, laptops, servers, network devices, ESXi servers, and mobile devices. |
| **Patch Status** | Patch status:<br>• No Policy<br>• No Data<br>• Reboot Required<br>• Install Error<br>• Approved Pending<br>• Fully Patched | Desktops, laptops and Windows servers. |
| **AV Product** | Antivirus vendor and name. | Desktops, laptops and servers. |
| **AV Status** | Antivirus engine status:<br>• Running and up-to-date<br>• Running and not up-to-date<br>• Not running<br>• Not detected | Desktops, laptops and servers. |
| **Windows Firewall** | Status of the native Windows firewall (**Enabled**, **disabled**). | Desktops, laptops and Windows servers. |
| **Windows Updates** | Status of the device's Windows Update service (**Enabled**, **disabled**). | Desktops, laptops and Windows servers. |

Table 12.12: Status section

## Screenshot

This displays a screenshot of the device provided that it is a desktop, laptop or server and it is switched on.

Click the ⌖ icon to update the screenshot.

## Notes

You can enter reminders or comments about the device for other administrators in the **Notes** section. A timestamp will be automatically saved for the note.

## Supplies

This section is on only available for network printers to show toner information.

## User-Defined fields

User-defined fields show specific information about the device not supported natively by Panda Systems Management. This information can be used to group devices using Account level filters or Site level filters (see section "**Filters**" on page **75**) and can also show the results of a monitoring component run on the device (see section "**Labels and user-defined fields**" on page **145**).

To define the content of a user-defined field:

- Click the ✎ icon and complete one or more of the 30 custom text fields available.
- Click **Clear** and **Clear user-defined fields** to delete the content of the text boxes.
- Click **Save** to save the content.

The information contained in the custom fields is displayed in the format "`Custom field X: #######`", where `X` is the number of the field (from 1 to 30) and `#######` its content. To show self-explanatory custom fields, Panda Systems Management allows you to change the "`Custom Field X`" string in the Account Level to one that best describes the type of data that will host the field. To do this, follow the steps shown below:

- Click on the general menu **Settings**, tab menu **Account settings**.
- In the **Custom Fields** section, click on the icons ✓ ✗ and ✎ to assign, delete and edit respectively the **Custom Fields X** chains by others that describe their content.

*The procedure shown is also applicable in the Zone level.*

## Guest Info

This section is only displayed when the device is an ESXi or Hyper-V server and hosts virtual machines.

| Field | Description |
|---|---|
| **Hostname** | Name of the ESXi or Hyper-V Server that hosts the virtual machine. |
| **Guest Name** | Name of the virtualized computer. |
| **Operating System** | Operating system installed on the virtualized computer. |
| **Status** | Virtual machine status. (**Online**, **Offline**) |

Table 12.13: Guest Info section

### Real-Time Monitoring Status

This shows the information generated by the monitors assigned to the device and which send data in real time to check that it is operating correctly. This section is included in desktops, laptops and servers as well as network devices and ESXi servers.

| Fields | Description |
|---|---|
| **Monitor** | Name and description of the monitor. |
| **Priority** | Priority configured in the monitor. |
| **Latest Value** | Last value returned by the monitor. |
| **Last Reading** | Date on which the last value was returned by the monitor. |
| **Last 30 Metrics** | Line graph with the last 30 values returned by the monitor. |
| **Status** | This indicates whether the parameters recorded are within the range defined by the monitor, or whether they exceed this range and an alert has been generated by the monitor. |

Table 12.14: Real-time monitoring status' section

### Recent Activity

See section "**Activity audit**" on page **165** for more information about device activity.

### Performance

Here you can see several graphs representing performance on desktops, laptops, servers and ESXi servers.

| Graph | Description |
|---|---|
| **Performance - CPU (% Used)** | Percentage of CPU usage. |
| **Performance - Memory (% Used)** | Percentage of RAM usage. |
| **Disk (% Used)** | Percentage of hard disk usage. |
| **Device Uptime** | Time the device has been switched on. |

Table 12.15: Performance section

## Installed antivirus audit

### Native support

Panda Systems Management automatically detects the status of the antivirus installed on the device and the downloaded signature file. Also, the antivirus detection native feature checks to see if the products based on Aether Platfom are updated or not.

The table below lists the antivirus products that are natively detected by Panda Systems Management on Windows or macOS devices::

| Antivirus | Windows | macOS |
|---|---|---|
| Avast Antivirus | YES | |
| Avast Business Antivirus | YES | |
| Bitdefender Endpoint Security | YES | YES |
| ESET Endpoint Security | YES | |
| Kaspersky Endpoint Security | YES | |
| McAfee Endpoint Security | YES | |
| McAfee VirusScan Enterprise | YES | |
| Sophos Antivirus | YES | |
| Symantec Endpoint Protection | YES | |
| System Center Endpoint Protection | YES | |
| Trend Micro Worry-Free Business Security | YES | |
| Webroot Secure Anywhere | YES | YES |
| Windows Defender Antivirus | YES | |
| Windows System Center Endpoint Protection | YES | |

Table 12.16: detected antivirus product list

### Protection status

Panda Systems Management identifies several protection statuses depending on whether an antivirus is installed, if it is enabled, and whether the signature file is less than three days old or not.

| Detected | Running | Updated | Antivirus status |
|---|---|---|---|
| YES | YES | YES | Running & up-to-date |
| YES | YES | NO | Running & not up-to-date |
| NO | NO | YES | Not running |
| YES | | | Not running |
| NO | | | Not detected |

Table 12.17: installed antivirus statuses

### Increasing the number of antivirus products supported

For antivirus products for which there is no native support or for any antivirus on macOS or Linux, the information has to be sent to the server in a .json file with the following format:

```
{"product":"Override Antivirus","running":true,"upToDate":true}
```

| Field | Description |
|---|---|
| **product** | Name of the antivirus to be displayed in the Panda Systems Management console. |
| **running** | Antivirus status:<br>• “true”: running<br>• “false”: stopped |
| **upToDate** | Signature file status:<br>• “true”: recently updated<br>• “false”: not updated recently |

Table 12.18: fields included in the .json file to extend antivirus support

The `.json` file should be save in:

| Operating System | File path and name |
|---|---|
| **Windows** | `%ProgramData%\CentraStage\AEMAgent\antivirus.json` |
| **macOS** | `/usr/local/share/CentraStage/AEMAgent/antivirus.json` |
| **Linux** | `/usr/local/share/CentraStage/AEMAgent/antivirus.json` |

Table 12.19:  .json file path

*You can develop a component and distribute it to all systems automatically to check the status of the antivirus on all devices and write a .json file periodically. If the .json file has not been edited in 7 days, the PCSM agent will delete it. See section “***Components and ComStore***” on page* **131** *to develop components compatible with Panda Systems Management.*

# Chapter 13

# Reports

The reporting system in Panda Systems Management shows the status of managed devices in various formats (PDF and CSV). These reports are highly configurable in terms of content, and can be adapted according to the target readers. The main features of the reporting system are:

- Options for scheduled and on-demand reports.
- Available in several languages.
- Flexibility in the choice of devices covered in the report.
- Configurable contents for each type of report.
- Reports from several sites can be consolidated in a single document to offer a global perspective of the IT resources.

CHAPTER CONTENT

# Accessing the reports system

All report options can be accessed from the general menu **Reports**. It is possible to generate any type of report from this area. However, to speed up the selection of the devices covered by the report, the reporting tool can be run from the three levels (Account, Site and Device) available in Panda Systems Management. Depending on the level from which a report is generated, the scope of the document will vary. Detailed below are the areas of the management console from which you can generate reports and their scope.

## Reports with data on devices from various sites

- From the general menu **Sites**, select one or more sites and click the icon in the icon bar.
- Generate PDF reports for all devices in the selected site.

## Reports with data on devices from one site

- Click the **Sites** menu and then the site with the devices.
- Select **Devices** in the tab bar and select the devices using the checkboxes.
- Click the icon from the icon bar to generate a PDF report.

## Reports with data from a single device

- Click the **Sites** menu and then the site with the device. Select **Devices** in the tab bar and click the device. Click the icon from the icon bar to generate a PDF report.

## Reports with configurable scope

- From the general menu **Reports**, **New report** option in the tab menu, you can access all the settings of the reporting system. When you access directly, the devices that feed data to the report are not specified in advance, so you have to manually indicate the groups or individual devices from which the report will be made.

# Creating reports

Follow the steps below to create a report:

- Establish the scope of the report and depending on the case, go to the reporting system in one of the ways described in "**Accessing the reports system**" on page **188**.

- Complete the fields in the Reports template:

| Field | Description |
|---|---|
| **Name** | Specify a name for the report. If no name is entered, the field reads: Scheduled Report for `[Username]`. |
| **Schedule** | Specify whether the report is to run immediately, once or several times over a period of time. Refer to "**Job scheduler**" on page **127** for more information.<br>Reports scheduled to run immediately can be downloaded from the console so that the administrator doesn't have to wait for the relevant email to arrive. A pop-up window will be displayed in the top-right corner of the console to download the report. |
| **Aggregate report** | Lets you consolidate, into a single report, the reports generated on devices belonging to different sites. |
| **Individual reports** | Generate a report for each site. |
| **Language** | Select the report language. |
| **Enabled** | By default, the reports created are entered in the job scheduler queue. If the report is not enabled, the settings template is saved but the report is not generated. This prevents having to delete a report when you temporarily don't want to generate it. |
| **Select report** | Select the type of report, the sections it will comprise and the required device filters. See section "**Types of reports available and settings**". |
| **Report targets** | Select the devices displayed in the report. Depending on the way of accessing the reporting system, this field may already be populated. |
| **Email recipients** | Indicate the email addresses and other parameters of the email used to deliver the report:<br>• **Subject**: email subject. If none is specified, one will be added automatically.<br>• **Body**: message body. If none is specified, information will be added about the execution and features of the report.<br>• **Send to default account recipients**: send the email to the accounts defined in the **Setup** menu, **Account settings**, **Email recipients**, provided they have sending of reports enabled.<br>• **Send to default site recipients**: send the email to the accounts defined in **Sites** in the main menu, click on a site, then **Settings**, and **Email recipients**, provided they have sending of reports enabled.<br>• **Additional recipients**: specify additional email addresses to which to send the report. |

Table 13.1: report settings parameters

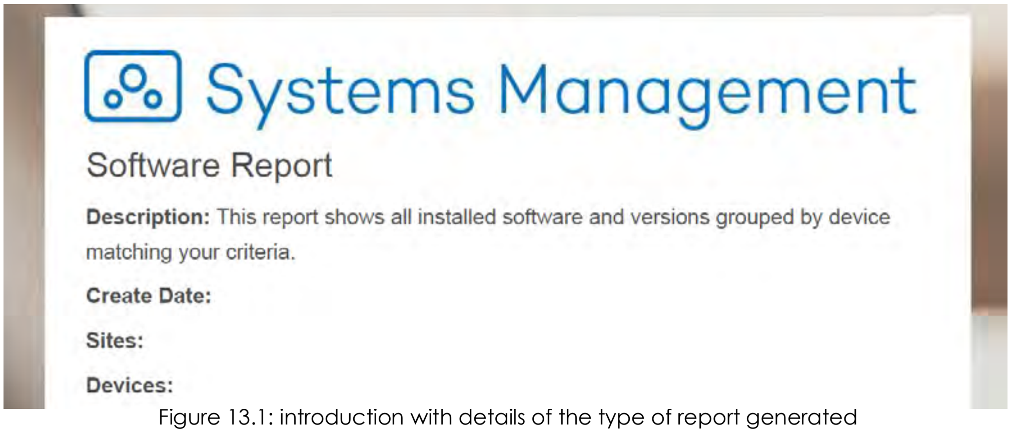
Emails containing a report too large to process will include a link for downloading the report from the management console.

# Report structure

Reports are divided into two clearly distinct sections:

- An introduction with details of the type of report generated.
- The main report section, of varying size, containing the report details.

## Introduction to the report



Systems Management

Software Report

**Description:** This report shows all installed software and versions grouped by device matching your criteria.

**Create Date:**

**Sites:**

**Devices:**

Figure 13.1: introduction with details of the type of report generated

Depending on whether they are defined, the fields included in the report introduction are as follows:

- Panda Systems Management product logo.
- Type of report generated.
- Description of the report.
- Date of creation. The time zone used is the one defined in **Setup**, **My info**.
- Sites covered by the report.
- Filters applied to the devices included in the report.
- Names of the devices included in the report.
- Groups to which the devices included belong.
- Total number of devices included in the report.

## Report body

The reports are divided into sections. Depending on the type of report, you can configure which sections are displayed.

If a report covers sites (see section "**Creating reports**" on page **188** to enable the **Aggregate report** feature), it will have separate sections with the details of each site.

# Types of reports available and settings

Panda Systems Management supports the following types of reports:

- **Executive**: shows the general status of all managed devices.
- **Audit**: shows information on the status of device resources.
- **Monitoring**: shows the status of the monitors assigned to the devices and any active alerts.
- **Patch management**: shows the level of patching on Windows devices.
- **Activity**: shows the activity of administrators on devices.
- **Export**: generates all types of reports with maximum detail, replacing graphics with lists of the activity recorded on the Panda Systems Management platform.

## Executive

### Executive summary

- **Description**: shows the operational status of the managed devices.
- **Options**:
  - **Free space**: sets the threshold in terms of percentage of free space to consider that a device is correct.
  - **RAM**: sets the threshold in terms of the amount of RAM to consider that a device is correct.

The report has six sections that can be included or hidden:

- **Summary**: this includes an explanation of the sections of the report, how measurements are made and how they affect the overall rating.
- **Asset Management:**
  - **Device Type**: table with the number of devices on the network grouped by type.
  - Device Health Check: table with the number of devices that do not exceed the thresholds configured. It also indicates the devices with a Windows operating system not supported by the manufacturer. See **https://www.pandasecurity.com/en/support/card?id=300102**.
- **Monitoring:**
  - Pie chart with the number of alerts triggered, grouped by priority.
  - Pie chart with the number of alerts triggered, grouped by status.
  - Table with the number of alerts grouped by priority and status.
  - Table with the number of alerts grouped by type of device and status.
  - Table of the five servers with most alerts.
  - Table of the five workstations with most alerts.
- **Patch Management:**

  - Pie chart with the number of servers grouped by patch status.
  - Pie chart with the number of workstations grouped by patch status.
  - Table with the total number of servers and the number of them that are fully patched.
  - Table with the total number of workstations and the number of them that are fully patched.
- **Antivirus:**
  - Pie chart with the number of servers grouped by antivirus status.
  - Pie chart with the number of workstations grouped by antivirus status.
  - Table with the total number of servers with the antivirus updated, not updated and not running.
  - Table with the total number of workstations with the antivirus updated, not updated and not running.
- **Proactive Maintenance:**
  - Table with the jobs created for automated maintenance.

## Device health summary

- **Description**: shows the operational status of the managed devices.
- **Options**:
  - **Free space**: sets the threshold in terms of percentage of free space to consider that a device is correct.
  - **RAM**: sets the threshold in terms of the amount of RAM to consider that a device is correct.

The information is divided into several sections:

- **Summary**
  - Pie chart with the total number of devices grouped by whether or not they have passed the tests run by the platform.
  - Pie chart with the total number of devices grouped by type.
- **Device type**: for each type of device there is a table indicating the tests they have passed and failed:
  - **Device name**, **Device description**, **Operating system**: fields to identify the device.
  - **Sufficient disk space**: result of the test of minimum free space available.
  - **Sufficient RAM**: result of the test of minimum RAM available.
  - **Software compliant**: indicates whether all the applications installed on the device are managed by the Software Management module. If they are not, this field will be blank.
  - **Fully patched**: shows whether the computer has patches pending.
  - **Antivirus up to date**: shows whether the antivirus signature file is more than three days out of date.
  - **Under warranty**: shows whether the computer is under warranty.

  - **Online within 30 days**: shows whether the computer has connected within the last 30 days.
  - **No open alerts**: shows whether the computer has any open alerts.

## Hardware lifecycle

- **Description**: this shows the devices managed on the network grouped by site and ordered by the date they were assembled to help administrators locate the oldest computers and therefore most likely to have problems. The assembly date is based on the BIOS release date.
- **Options**:
  - **Free space**: sets the threshold in terms of percentage of free space to consider that a device is correct.
  - **RAM**: sets the threshold in terms of the amount of RAM to consider that a device is correct.

Information in the report:

- **Hardware Replacement Recommendations**: pie chart grouping devices into four categories:
  - **Suitable for 24 months+**: computers less than three years old.
  - **Replacement recommended within 12-24 months**: computers between three and four years old.
  - **Replacement recommended within 12 months**: computers more than four years old.
  - **Unknown**: no information (network devices, printers and other devices without BIOS access).
- **Operating System Support:** pie chart showing the number of devices with a Windows OS supported or not supported by Microsoft. Non-Windows OS are counted as supported. See **https://www.pandasecurity.com/en/support/card?id=300102**.
  - **Operating system is supported**: the manufacturer publishes updates and provides technical support.
  - **Operating system is unsupported unless manufacturer extended support has been arranged**: the manufacturer has recently stopped publishing updates and does not provide technical support any more, unless the customer has purchased an extended support package.
  - **Operating system is unsupported**: the manufacturer stopped publishing updates and does not provide technical support any more. Updating the operating system is recommended.
- **Grouping**: for each group displayed in the pie chart, the corresponding devices are listed.
  - **Device Name**, **Device Description**, **Operating System**: fields to identify the device.
  - **OS Support:** whether the operating system is supported by the manufacturer.
  - **Last User**: user account that last ran a session on the computer.
  - **Serial Number**.
  - **Disk Space**: result of test of minimum free space available.
  - **RAM Quantity**: result of test of minimum RAM available.
  - **Under Warranty**: shows if the computer is under warranty.

- **Online Within Last 30 Days**: shows if the computer has connected in the last 30 days.
- **Build Date**: date the computer was assembled. The Build Date is based on the BIOS release date. While this is the best metric available, the data should not be treated as definitive since the computer may have been assembled at a later date.

# Audits

## Device storage

- **Description**: shows the status of the storage devices connected to the devices.
- **Options**:
  - **Select drive type**: shows a drop-down menu with the types of devices included in the report. Information in the report:
- **Device type**: for each type of device there is a table with the computers and the connected devices:
  - **Device name**, **Device description**: fields that identify the device.
  - **Disk drive**: Letter or mount point that identifies the drive.
  - **Drive type**: Type of storage drive (local, removable, optical, etc.)
  - **Size**: total capacity of the storage device.
  - **Free**: GB of free space of the storage device.
  - **Used (%)**: bar chart showing the percentage of space used on the storage device.

## Detailed computer audit

- **Description**: shows a complete audit of each managed device.
- **Options**:
  - **Select user-defined field for this report**: Displays a drop-down menu with user-defined fields included in the report.

The information contained in this report is a copy of the **Audit** tab at Device level. See chapter "**Hardware audit**" on page **156** for more information about the fields in the report.

## Network audit

- **Description**: shows a complete list of all network devices, including those that are managed as well as those discovered but not managed.
- **Options**:
  - **Managed devices**: the report includes all devices managed by Panda Systems Management.
  - **Discovered devices**: the report includes all devices discovered but not managed by Panda Systems Management.

The information is divided into several sections:

- **Summary**:
  - Pie chart with all devices discovered on the network grouped according to their integration in Panda Systems Management.
- **Managed**: for each type of device there is a table with the following information:
  - **Device name**, **Device description**: fields to identify the device.
  - **IP address**: device IP address.
  - **Vendor**: device manufacturer.
  - **Created**: date the device was integrated in Panda Systems Management.
- **Unmanaged**: For each type of device there is a table with the following information:
  - **Device name**, **Device description**: fields to identify the device.
  - **SNMP description**: description of the SNMP protocol.
  - **IP address**: device IP address.
  - **Vendor**: device manufacturer.
  - **Discovered**: date that Panda Systems Management first discovered the device.

### Software

- **Description**: shows a complete list of the software installed on the devices on the network.
- **Options**: lets you add rules to filter the software or list all the software found. Use "%" as a wildcard to replace characters at the beginning or end of the name of the software.

The information is divided into several sections:

- **Summary**: list of all the software found and the number of times each program occurs.
  - **Software**: name of the program.
  - **Instances found**: number of devices with the program installed.
- **Device**: list of the software found on each device.
  - **Device name**, **Device description**, **Operating system**: fields that identify the device.
  - **Software**: name of the program.
  - **Version**: version of the program.

## Monitoring

### Device monitor status

- **Description**: shows the latest values of the monitors assigned to the devices.
- **Options**:

- **Select monitor statuses**: filters the monitors by status.
- **Select monitor types**: filters the monitors by category. See section "**Monitoring**" on page **105** for more information about the types of monitors available.

Information contained in the report:

- **Device name**: for each device there is a table with the following information:
  - **Device name**, **Device description**, **Operating system**: fields that identify the device.
  - **Monitor type**: type of monitor.
  - **Monitor description**
  - **Priority**
  - **Latest value**: latest value returned by the monitor.
  - **Last reading**: date on which the latest value was received.
  - **Status**: monitor status (**OK**, **Alert**, **No response**)

## Open monitor alerts

- **Description**: shows the current status of the alerts open on the device. The information in the report is a table with the following fields:
- **Device name**, **Device description**: fields that identify the device.
- **Total**: total number of alerts open on the device.
- **Critical**: total number of critically important alerts open on the device.
- **High**: total number of highly important alerts open on the device.
- **Moderate**: total number of moderately important alerts open on the device.
- **Low**: total number of low importance alerts open on the device.
- **Information**: total number of informational alerts open on the device.

## Performance monitoring

- **Description**: shows the performance of the device using graphs accessible at Device level in the management console.
- **Options**:
  - **Select performance options for this report**: select the device resources displayed in the report: **CPU, Memory, Disk**.

The information in the report is a table with the following fields:

- **Device name**, **Device description**: fields that identify the device.
- Line chart representing the memory consumption percentage over the last month.
- Line chart representing the CPU consumption percentage over the last month.

- Line chart representing the percentage of storage space used on internal drives in the last month.

# Patch management

## Patch management activity

- **Description**: shows the patch management activity of Panda Systems Management on the selected devices and for the selected date range.
- **Options**:
  - **Date range**: the report shows information for the selected date range (**Last 7 days**, **Last 30 days**, **Current month**, **Between date range**).
  - **Install status**: includes the patches installed correctly and those that returned an error.

The report contains a table with the following fields:

- **Device name**, **Device description**, **Operating system**: fields that identify the device.
- **Patch name**: name of the patch.
- **Type**: software.
- **Priority**: set by the vendor.
- **Published**: date the patch was published by the vendor.
- **Installed**: date the patch was installed on the device.
- **Install**: patch status (**installed** or **Failed**)

## Patch management details

- **Description**: shows a detailed view of the status of each patch installed on the devices.
- **Options**:
  - **Select patch**: the report will show information about all the patches published or only those selected.
  - **Select patch details options for this report**: filters the patches displayed in the report by status (**Approved**, **Installed**, **Not Approved**).

The report contains a table with the following fields:

- **Device name**
  - **Device name**, **Device description**, **Operating system**: fields that identify the device.
  - **Patch Status**: indicates whether the computer requires a restart to complete the installation of a given patch.
  - **Patch title**: patch name.
  - **Priority**: set by the vendor.
  - **Status**: patch status (**Approved**, **Installed**, **Not Approved**).

### Patch management summary

- **Description**: shows an overview of the patch status of each device.
  The report has several sections:
- **Summary**
  - Pie chart with all computers grouped by patch status (**Fully patched**,
  - **Approved pending**, **Install error**, **Reboot required**, **No data**, **No policy**).
- **Servers**
  - **Device hostname**, **Device description**: fields that identify the device.
  - **Installed**: number of patches successfully installed.
  - **Last reboot**: last device restart.
  - **Approved pending**: number of approved patches pending installation.
  - **Patch status**: patch status of the device (**Fully patched**, **Reboot required**).

## Activity

### Device activity

- **Description**: shows the action taken by the administrator on managed devices.
- **Options**:
  - **Date range**: the report will show information for the selected date range (**Last 7 days**, **Last 30 days**, **Current month**, **Between date range**).
  - **Activity filter**: includes the actions that Panda Systems Management takes on devices.

The report contains a table with the following fields:

- **Device Name**.
  - **Type**: icon representing the type of action taken on the device.
  - **Name**: name of the console user that launched the action.
  - **Activity:** activities performed on the device.
  - **Started**: date the action started.
  - **Ended**: date the action finished.
  - **Duration**: duration of the action.
  - **Status**: specifies whether the action was completed.

## Export

The reports in this category are CSV files that record the different types of activities and actions taken by Panda Systems Management. In this type of report there is a line for each activity, action or change that occurs in the product and they are especially useful when operating automatically with external tools, such as Microsoft Excel, to filter, search and categorize the events.

The reports can be filtered by date and main concept.

The content can be configured with the **Select columns** option to display more or less information in each line.

Below there is a list of the reports available along with an explanation of their purpose.

- **Admin activity**: this shows all the activity for a specified date. The list of lines is filtered by the management console user and not by the devices chosen in the **Report targets** field.
- **Device change log**: this shows all the changes recorded in the device log file. The list of lines is filtered by the type of change: **hardware**, **software**, **system**.
- **Device details**: this shows the information available for each device.
- **Device activity**: this shows the activity specified in the filter that the administrator took on the device for the range of dates configured.
- **Device storage**: this lists all the disks available on the selected devices including their available disk space.
- **Microsoft audit**: this shows the information required to license the Microsoft products installed on audited devices.
- **Monitor alerts**: this shows the alerts generated by the monitors for the specified dates and filters applied.
- **Installed software**: this shows the software installed on the devices in line with the criteria specified.
- **Patch details**: this shows all the patches released by the vendors of the software installed on the computers, filtered by status.
- **Device patch summary**: this shows all devices with patches pending installation.
- **Site device count:** this shows the total number of devices per site grouped by type.

# Part 5

# Resolution of incidents and technical support

# Chapter 14

# Patch Management

The Patch Management tool provides a series of resources for centralized deployment and installation of patches and software updates.

Patch Management not only eases daily updating of the software on your devices but also allows you to perform audits, quickly and easily displaying devices that are not updated or with known vulnerabilities.

With Patch Management, the administrator can strengthen network security and minimize software failures, ensuring that all devices are updated with the latest patches published.

> ⚠ *Patch Management uses the Windows Update API that exists on all Microsoft Windows devices supported by Panda Systems Management. Patch Management supports Microsoft Windows systems.*

CHAPTER CONTENT

# What patches can I deploy/apply?

Panda Systems Management lets you centrally manage the patches and updates published by Microsoft through Windows Update.

Microsoft publishes updates for all the Windows operating systems currently supported and for the software it develops:

- Microsoft Office
- Exchange 2003
- SQL Server
- Windows Live
- Windows Defender
- Visual Studio
- Zune Software
- Virtual PC
- Virtual Server
- CAPICOM
- Microsoft Lync
- Silverlight
- Windows Media Player
- Other...

## Patch Management policies and Feature Updates

From Windows 10, Microsoft has started rolling out all new versions of its operating system in the form of Feature Updates, which are equivalent to a Service Pack. Below is a list of all Windows 10 versions affected by this new policy:

| Version | Code name |
|---|---|
| **1507** | Threshold 1/ First Version |

Table 14.1: Windows 10 versions and codenames

| Version | Code name |
|---|---|
| **1511** | Threshold 2 / November Update |
| **1607** | Redstone 1 / Anniversary Update |
| **1703** | Redstone 2 / Creators Update |
| **1709** | Redstone 3 / Fall Creators Update |
| **1803** | Redstone 4 / April 2018 Update |
| **1809** | Redstone 5 / October 2018 Update |

Table 14.1: Windows 10 versions and codenames

These patches are files of about 5 gigabytes in size which contain either a full image of the new operating system or a delta image with just the changes from the version installed on the user's computer. They are downloaded to the target device and installed during the boot process. Therefore, they are not directly managed by Windows Update.

Due to their characteristics, the Patch Management policies do not show Feature Updates as patches available for installation.

⚠ *To install Feature Updates on Windows 10, use the following ComStore component: 'Windows 10: Upgrade or update to latest Feature Release [WIN]'*

# Patch deployment and installation

Panda Systems Management includes two independent but complementary Patch Management methods. Each of them has different functions to adapt to all possible needs and/or scenarios:

- Windows Update policy.
- Patch Management policy.

⚠ *Windows Update policies and Patch Management policies are mutually exclusive. It is advisable to disable Windows Update when using Patch Management policies to update Windows operating Systems, otherwise there may be unpredictable consequences. See section "***Disabling Windows Update to avoid interference***" on page* **209**.

*The procedures described here can collide with other procedures defined by third-party software, such as Windows Update policies defined in a GPO. It is recommended to disable the policies of third-party manufacturers that interfere with those defined in Panda Systems Management.*

## Patch categories based on the policy used

Depending on the type of policy (Windows Update or Patch Management), Panda Systems Management divides patches into different categories based on their priority:

- **Windows Update policy**: uses the same categories as Windows Update (**Important**, **Recommended**, **Optional**).
- **Patch Management policy**: uses the same categories as the Microsoft Security Response Center (**Critical**, **Important**, **Moderate**, **Low**, **Unspecified**).

## Patch installation order

Panda Systems Management installs patches in an order based on the patch type and priority:

| Order | Category | Priority |
|---|---|---|
| **1** | Security updates | Critical |
| **2** | Security updates | Important |
| **3** | Security updates | Moderate |
| **4** | Security updates | Low |
| **5** | Security updates | Unspecified |
| **6** | Service Packs | Not applicable |
| **7** | Update rollups | Not applicable |
| **8** | Critical updates | Not applicable |
| **9** | Updates | Not applicable |
| **10** | Others | Not applicable |

Table 14.2: patch installation order

## Frequency of patch audits

The Patch Management module scans managed computers for new patches. This process is triggered automatically by the following events:

- When a Patch Management policy is run.
- After the initial full audit (right after agent installation).
- After a regular audit (every 24 hours).
- After a manual audit (when a single device or multiple devices are selected).
- The following events do not trigger a patch scan:
- Quick or scheduled jobs.
- Alert response jobs.

- User tasks.

# Method I: Windows Update policy

Windows Update polices permit centralized configuration of the Windows Update service accessible from the Control Panel of every Windows device on the network.

They allow the administrator to control how all Windows devices across the network will behave with regard to operating system and Microsoft software updates.

As it is a policy, the grouping levels supported by this method are Account Level and Site Level.

## Access to the Windows Update policy method

To access this method, create a **Windows Update** policy at Site Level or Account Level.

A screen appears where you can centrally configure the behavior of Windows Update on all of the devices affected by the policy created.

Windows Update policies are configured in the same way as Windows Update resources on each individual Windows device.

Only important and recommended patches can be automatically installed. The rest of the patches will be installed manually from the user's device or from Panda Systems Management using other patch management methods.

> *All of the settings in this policy are a transposition of the features of Windows Update on Windows devices. Therefore, all of the actions specified refer to the devices and not the agent or the console.*

> *Although the policy settings are the same for all devices, the behavior of Windows Update on each device can vary slightly based on the different operating system versions.*

Below are the settings available for this type of policy:

| Field | Description |
|---|---|
| Microsoft Update | • **Give me updates for Microsoft products and check for new optional Microsoft software when updating Windows**: once selected, updates will be received for Windows as well as for other Microsoft products (Word, Excel, PowerPoint, etc.). |

Table 14.3: options available in the Windows Update policy

| Field | Description |
|---|---|
| **WSUS** | • **Change Endpoint WSUS Settings**: lets you specify the WSUS server to use for patching.<br>• **Do not allow any connections to Microsoft for Patching or Searching when using a WSUS Server**: devices will look for update files on the WSUS server, instead of on external servers.<br>• **Client-side Targeting Group Name**: if a WSUS server is used with client-side targeting enabled, this option lets you specify the target group name or names that should be used to receive updates. If the setting is enabled, you can enter a target group name or names separated by semicolons. |
| **Active Hours** | • **Configure Active Hours**: lets you specify when you usually use your devices. |
| **Update Channel** | • **Change Update Channel settings for applicable devices**:<br>• **Targeted Deployment**: updates are received immediately following general release.<br>• **Broad Deployment**: updates are received later, after receiving community feedback (Current Branch for Business). |
| | • **Defer Feature Updates**: lets you defer feature updates for the maximum time permissible according to the OS build or for a period as close as possible to a specific number of days.<br>• **Defer Quality Updates**: lets you defer performance-enhancing updates for the maximum time permissible according to the OS build or for a period as close as possible to a specific number of days. |
| **Peer Sharing** | • **Permit devices to share Windows Updates within local network**: devices connected to the same network will look for update files on the other devices on the network.<br>• **Permit devices to share Windows Updates outside of local network**: once selected, devices can look for update files on other devices outside their local network. |
| **Fast Startup** | **Disable Windows Fast Startup:** when selected, updates will be installed on shutdown as well as reboot. |
| **Configure Updates** | • **Automatically detect recommended updates for my computer and install them.**<br>• **Download updates for me, but let me choose when to install them.**<br>• **Notify me of updates, but do not automatically install them.**<br>• **Turn off Automatic Updates.** |
| **Install new updates** | Lets you select the day of the week and the time when updates will be installed. |
| **Recommended updates** | **Give me recommended updates the same way I receive important updates.** |

Table 14.3: options available in the Windows Update policy

| Field | Description |
|---|---|
| **Who can install updates** | **Allow non-Administrative Endpoint Accounts to receive update notifications**: once selected, all users on the device will be notified of updates. |
| **Restart behavior** | • **No auto-restart with logged on users for scheduled Automatic Updates installations**.<br>• **Re-prompt for restart with scheduled installations**: if the setting is enabled, the restart will occur the specified number of minutes after the previous prompt for restart was postponed.<br>• **Delay restart for scheduled installations**: if the setting is enabled, the restart will occur the specified number of minutes after the installation is complete. |

Table 14.3: options available in the Windows Update policy

### Disabling Windows Update to avoid interference

Sometimes, third-party programs may exist that set up update policies in Windows Update capable of interfering with Panda Systems Management's patching tool. That is the case, for example, when there is a default Windows Update configuration on each device, aimed at installing important updates from time to time. To avoid any interference caused by patching policies defined by third-party products or local users, follow the steps below:

- Create a Windows Update policy for all devices set to receive updates via Panda Systems Management.
- In **Patch Management policy**, select **Turn off automatic updates**.
- Push the policy to your devices.

### Windows Update method: usage scenarios

- When the administrator needs to make sure that all important patches are automatically installed on all network devices, without the end user obstructing the process.
- When the administrator wants to quickly deploy a centralized Patch Management policy that doesn't require further maintenance.
- When all computers on the network are very similar to one another and there are no circumstances that require a patch exclusion
- When patches classified as Optional do not need to be installed automatically.

## Method II: Patch Management policy.

**Patch Management** policies permit automatic installation of patches, in a similar way to the **Windows Update** policies.

The main difference lies in how the patches to install are managed. Whereas the Windows Update method allows you to apply patches by level (**Important**, **Recommended**, or **Optional**), Patch Management allows you to select the patches to be applied based on very specific conditions, as well as define whether the target device must reboot or not after patch installation.

As it is a policy, the grouping levels supported by this method are Account Level and Site Level.

## General workflow and Patch Management policy override

In medium to large networks, the number of specific circumstances and scenarios that may be incompatible with the general Patch Management policy defined at Account Level may be quite significant. This may force administrators to define as many Patch Management policies as special cases exist on the network. This greatly increases maintenance tasks, especially in the case of heterogeneous networks with multiple devices used by users with different profiles and responsibilities.

For that reason, Panda Systems Management allows a workflow to be established for Patch Management policies completely different from other policies in the system. The purpose of this workflow is to speed up generation of Patch Management policies without sacrificing flexibility to define the patches to be installed on each device on the network.

Figure **14.1** on page **211** shows the workflow phases.

### Establishing a Patch Management policy at Account Level

Specify a Patch Management policy at the most general level that covers all of your devices and applies the default, most common settings. This step won't be necessary if the account only has one site.

Refer to section "**Creating a Patch Management policy**" on page **212** in the guide for information about how to configure a Patch Management policy.

### Overriding a policy at Site Level

Override the policy at Site Level according to your needs. Unlike other policies in the console, the Patch Management policies defined at Account Level can be partially modified. This eliminates the need to create completely new configurations for each site that override the one created at the higher level. The settings inherited from the Account Level can be partially modified keeping the targeted devices at all times.

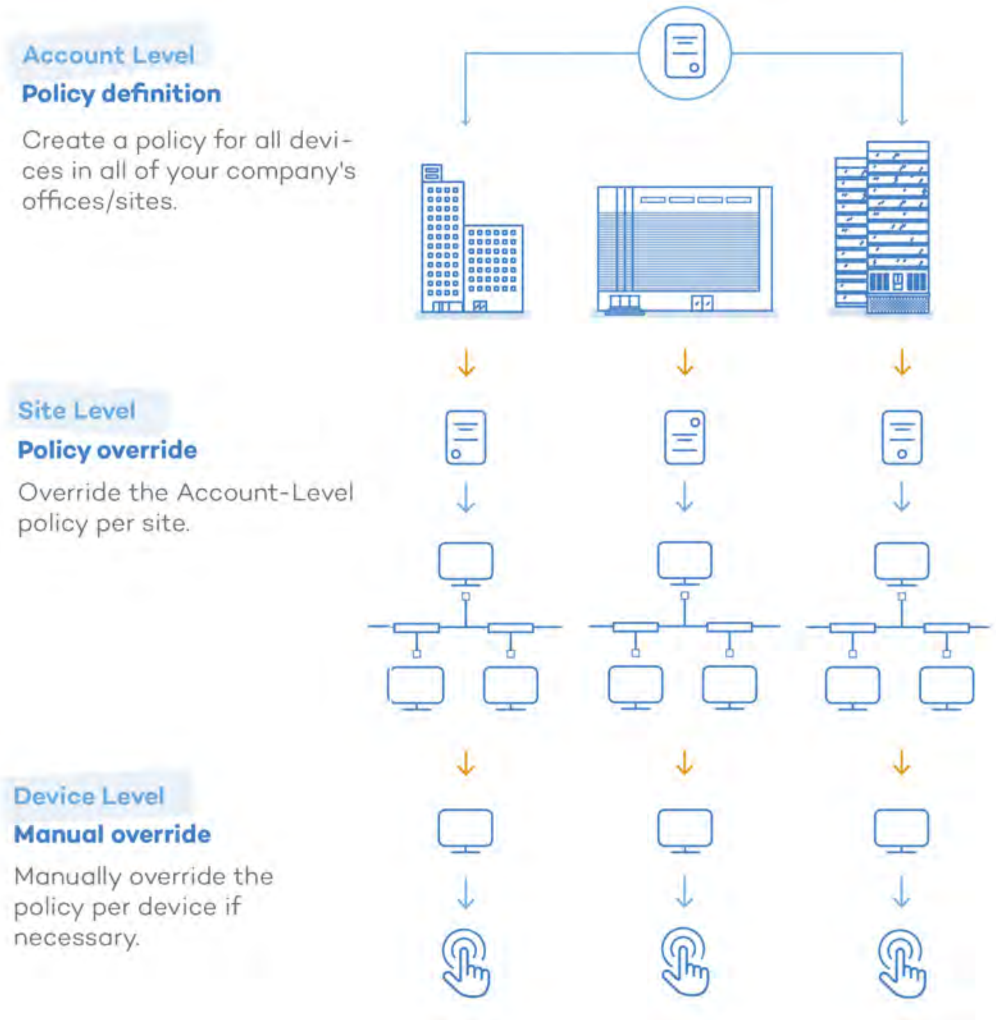

Account Level
Policy definition
Create a policy for all devices in all of your company's offices/sites.
Site Level
Policy override
Override the Account-Level policy per site.
Device Level
Manual override
Manually override the policy per device if necessary.

Figure 14.1: general strategy for defining Patch Management policies

## Patch policy override per device

Finally, you can modify the defined Patch Management policy at Device Level, for those cases in which it may be necessary to make small adjustments for some specific devices.

You can also disable the policy assigned to a specific device, from the **Policies** tab in the site that the device belongs to. This is very useful for those devices that require a Patch Management policy completely different from the one defined for all other devices in the account.

# Creating a Patch Management policy

*Panda Systems Management automatically assigns a Patch Management policy in Audit mode to account devices.*

To create a Patch Management policy at Site Level or Account Level, click the **Policies** tab and select **Patch Management** in policy type.

A screen appears where you can centrally configure the behavior of Patch Management for all of the devices affected by the policy created.

## Patch approval and order of precedence

**Patch Management** policies allow you to set filters and conditions for automatically allowing or denying patch installs. These filters obtain the metadata that accompanies the patches published by Microsoft, and evaluate it in order to decide whether to install them or not.

To allow or deny the installation of a patch or group of patches on one or multiple devices you must approve or deny them. Patches are approved and denied from the **Patch approval** section of a Patch Management policy:

- **Approve patches**: Approving a patch marks it to be installed at the next patch window defined in the policy, on all targeted devices.
- **Do not approve patches**: Disapproved patches are indefinitely excluded from device patch processes.

You can select to approve or not approve:

- **Patch groups**: These groups are defined by the rules created by the administrator to group one or more patches. For example: “All critical patches published”. The console provides a large number of filtering attributes for patches, and logical operators to combine them in order to generate accurate, complex criteria.
- **Individual patches**: You can manually select a specific patch to approve or not approve it.

This results in the following four combinations with the following order of precedence:

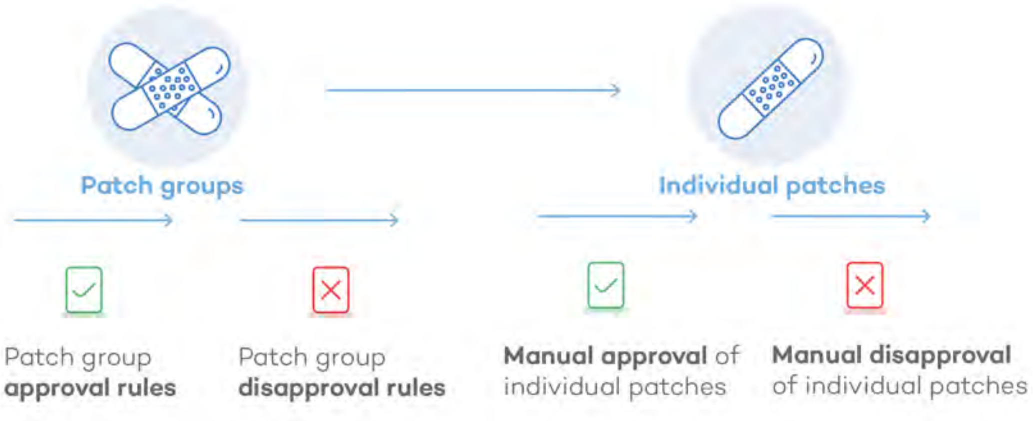

Patch groups
Individual patches
Patch group approval rules
Patch group disapproval rules
Manual approval of individual patches
Manual disapproval of individual patches

Figure 14.2: patch approval/disapproval flows

Each stage takes precedence over the previous one. For example: If a group rule approves a patch that is later denied at individual level, the latter will prevail.

## Configuring a Patch Management policy

These are the settings available for a **Patch Management** policy.

| Section | Field | Description |
|---|---|---|
| **Patch Management policy options** | **Targets** | Lets you add filters or groups that limit the application scope of the policy. Depending on the level at which the policy is created (Site Level or Account Level), different filters and device groups will be displayed. |
| | **Audit only** | Select this option to use the policy for audit purposes only without installing any patches. This will allow you to see missing patches on your devices and problematic patches you may not want to download and apply. |
| | **Schedule** | Lets you define the patch window. Click the **Click to change** button next to **Choose a Schedule** to display a form where you will be able to select the patch installation interval and frequency. See chapter "**Job scheduler**" on page **127**. |
| | **Duration** | Lets you set how long the patch process will last. If the patch process exceeds the set period, the policy will be interrupted with an error. |
| **Patch location** | **Local Cache** | • **Download patches from Windows Update**: The targeted devices will connect to the Windows Update server to download patches.<br>• **Use a local cache**: Allows targeted devices to use the device designated as a local cache to download patches. Refer to "**Designating a local cache**" on page **66**. |

Table 14.4: Patch Management policy settings options

| Section | Field | Description |
|---|---|---|
| Patch Approval | Approve these patches | Refer to "**Patch approval and exclusion criteria**" on page **215** |
| | Do not approve these patches | Refer to "**Patch approval and exclusion criteria**" on page **215** |
| | Available | Refer to "**Configuring individual patches**" on page **216**. |
| | Approve | Refer to "**Configuring individual patches**" on page **216**. |
| | Do Not Approve | Refer to "**Configuring individual patches**" on page **216**. |
| Power | Boot | When selected, wakes all targeted devices compatible with the Wake-On-LAN feature ten minutes before it starts with the patch process. |
| | Reboot | Lets you define how the targeted devices must behave after the patch process.<br>• **Power down**: Shuts down the targeted devices after the patch schedule window.<br>• **Reboot devices**: If necessary, it will reboot the targeted devices after the policy has run. It does not permit rebooting if a USB stick is connected at the scheduled reboot time. This is to prevent systems from rebooting from the operating system stored on a USB device. You can modify this behavior by selecting the option **Permit rebooting**.<br>• **Allow restart when a storage device is connected** to prevent a possible boot from the operating system stored on the USB device.<br>• **Do not reboot**: Stops the targeted devices from rebooting after the patch schedule window. It allows you to show a branded reboot reminder to the end user every 1-12 hours/1 day/2 days, as well as configure how many times the end user is allowed to dismiss the reboot reminder.<br>• **Show personalized reminder:** indicate the number of hours that will pass to show a new notification to the user.<br>• **Allow a maximum number of cancellations**: after the defined number the notification is fixed on the user's screen. |

Table 14.4: Patch Management policy settings options

## Approving patches and creating filters

To select the patches to install on your devices and deny those considered dangerous or unnecessary, go to section **Patch approval** on the Patch Management policy settings screen. To allow or deny a group of patches, define, in sections **Approve these patches** and **Do not approve these patches**, rules similar to those used when creating device filters. These were discussed in chapter "**Filter composition**" on page **82**. In this case, the attributes to configure correspond to the characteristics of the patches to install or deny. Additionally, you can specify individual patches to include or exclude from a patch installation through section **Configure individual patches**.

## Patch approval and exclusion criteria

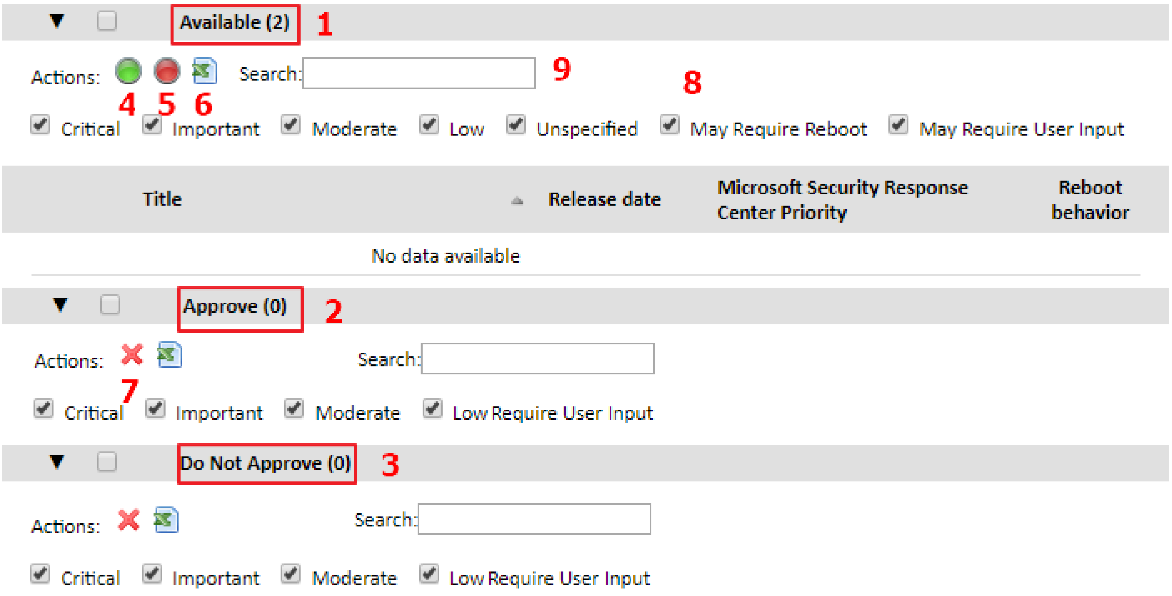
The **Patch approval** section provides resources to define advanced filters to approve patches based on the selected criteria:

| Field | Description |
|---|---|
| **All** | Selects all published patches. |
| **Category** | Selects patches based on their category. |
| **Description** | Allows you to filter by the description of the patch. |
| **Download size** | Specify the size of the download in bytes. For other measures, add G (gigabytes), M (megabytes), or K (kilobytes). |
| **KB Number** | Allows you to search for the specific Microsoft Knowledge Base article number a patch is associated with. |
| **Priority** | Allows you to filter by priority, that is, "severity" as specified in Microsoft Security Bulletins (**Critical**, **Important**, **Moderate**, **Low**, **Unspecified**). The Systems Management Patch Management policies reference the severity of the Security Bulletin classification, not the one in Windows Update. |
| **Restart behavior** | Filters patches based on how they behave after installation: **Never reboots** (0), **Always requires reboot** (1), **Can request reboot** (2). |
| **Release Date** | Date when Microsoft released the patch. |
| **Request user input** | Lets you filter for patches that may require user input (**May require**) or not (**Does not require**). |
| **Title** | Allows you to filter by the name of the patch. |
| **Type** | Allows you to filter by patch type. Select either Software or Driver. |

Table 14.5: patch filter criteria

### Configuring individual patches

To make it easier to find the individual patches to add or exclude from a patch installation, the **Configure individual patches** section is divided into three lists:



▼ □ Available (2) 1

Actions: ● ● 6 Search: 9 8

4 5

☑ Critical ☑ Important ☑ Moderate ☑ Low ☑ Unspecified ☑ May Require Reboot ☑ May Require User Input

| Title | Release date | Microsoft Security Response Center Priority | Reboot behavior |
|---|---|---|---|
| No data available | | | |

▼ □ Approve (0) 2

Actions: ✕ Search:

7

☑ Critical ☑ Important ☑ Moderate ☑ Low Require User Input

▼ □ Do Not Approve (0) 3

Actions: ✕ Search:

☑ Critical ☑ Important ☑ Moderate ☑ Low Require User Input

Figure 14.3: configuring individual patches

- **Available (1)**: this section lists all patches that have been submitted to the platform but have not yet been processed.
- **Approve (2)**: this section lists all patches that have been approved for installation.
- **Do not approve (3)**: this section lists all patches that have been denied. To mark one or more patches as **Approve** or Do not approve, use the icon bar displayed when clicking each of the available groups
- **Approve (4)**: approves the patch for installation, removing it from the **Available** list and placing it in the **Approve** list.
- **Do not approve (5)**: denies the patch, removing it from the **Available** list and placing it in the **Do not approve** list.
- **Export all patches to CSV (6)**: generates a CSV list with all selected patches.
- **Remove from list (7)**: this option is only available for the **Approve** and **Do not approve** lists. It removes the patch from the current list and pushes it into the **Available** list again.

A search bar is available **(8)** to make finding a specific patch easier:

- **Priority**: shows all patches with the selected priority: **Critical**, **Important**, **Moderate**, **Low**, **Unspecified**.
- **May require reboot**: shows all patches that may require a reboot to complete the installation process.
- **May require user input**: shows all patches that may require user interaction to complete the installation process.

- **Search (9)**: lets you perform a free search on all patch attributes.

## Overriding the policies defined at Account Level

To speed up the creation of specific policies for those sites that fall outside the configuration established at Account Level, Panda Systems Management allows administrators to modify or override parts of an Account Level policy, without needing to create a completely new policy. This feature allows administrators to configure the system more quickly and reduce maintenance tasks as there will be fewer policies to manage.

To override an Account-Level policy, go to the **Policies** menu in the site whose policy you want to modify. You will be presented with both Account and Site policies. Locate your Account-Level Patch Management policy. This policy will show an **Override** button, or an **Edit override** button if the patch policy in question already has an active override. An active override is also indicated by a green icon in front of the policy.

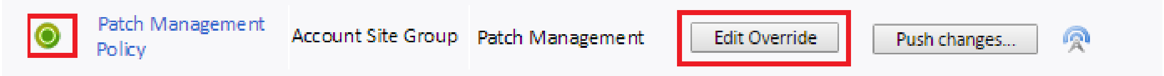
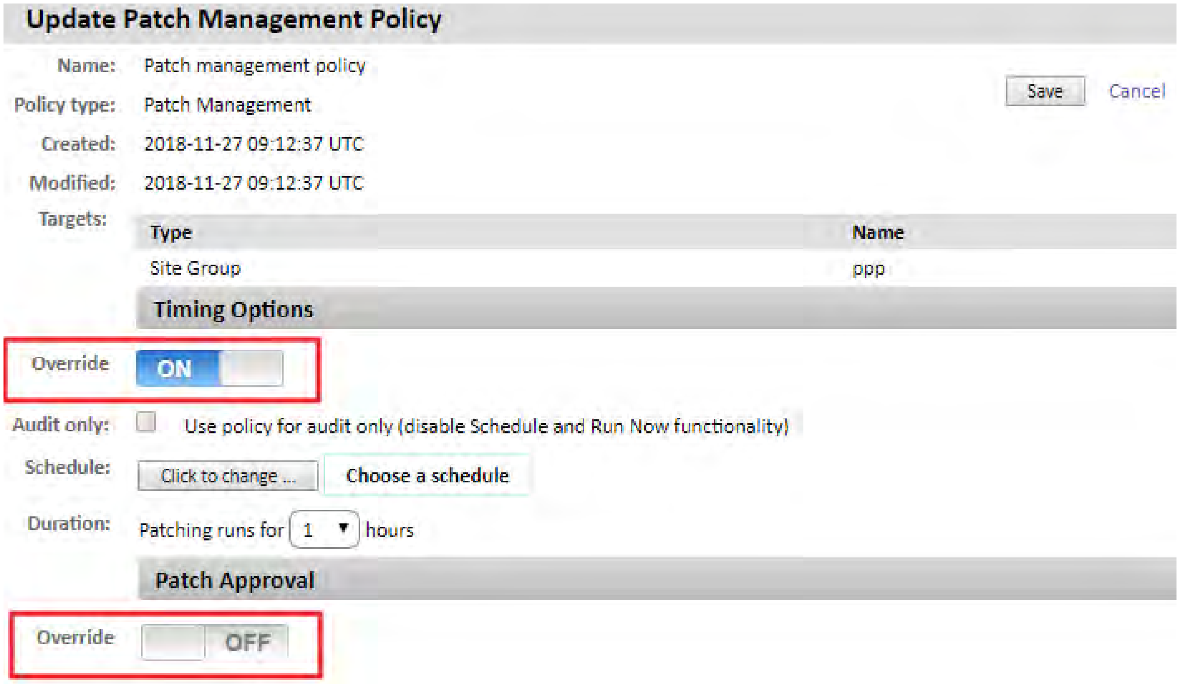


Figure 14.4: Patch Management policy override

Click **Override** or **Edit override**. This will open the Patch Management policy as configured at the Account Level, with **Override** buttons to edit the settings. Also, please note that clicking the policy's name will take you to the policy's original settings.



Update Patch Management Policy

Name: Patch management policy

Policy type: Patch Management

Created: 2018-11-27 09:12:37 UTC

Modified: 2018-11-27 09:12:37 UTC

Targets:

| Type | Name |
|---|---|
| Site Group | ppp |

Timing Options

Override: ON

Audit only: □ Use policy for audit only (disable Schedule and Run Now functionality)

Schedule: Click to change ... Choose a schedule

Duration: Patching runs for 1 hours

Patch Approval

Override: OFF

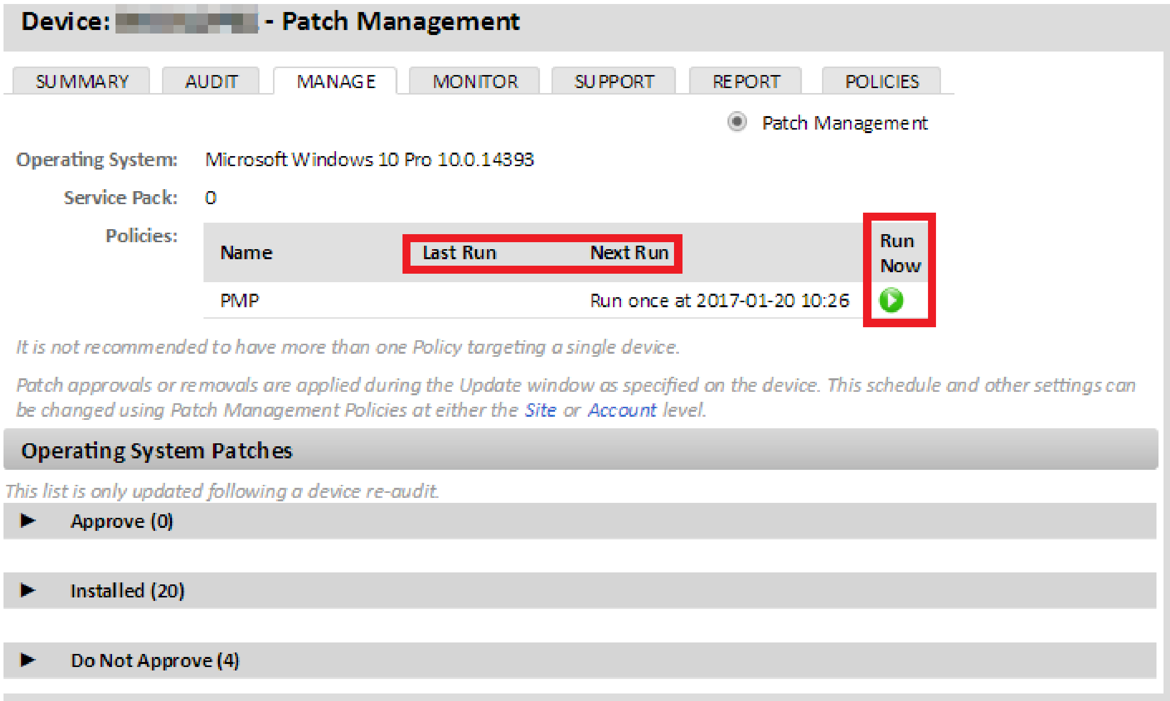
Figure 14.5: Patch Management policy override options

Click those **Override** buttons to edit the policy settings, changing and overriding the original values.

## Modifying Patch Management policies per device

The **Manage** menu at Device Level (which represents each device on the network), lets you modify the patches that have been approved and denied in the previous stages of a Patch Management policy creation process. Furthermore, this screen lets you view the date when the Patch Management policy was run, and force it to run again if necessary.

This screen is divided into two sections: one that lets you view the policies applied to the device, and another one that lets you see the approved and denied patches as per the Patch Management policy assigned to the device.



**Device:** [redacted] **- Patch Management**

Operating System: Microsoft Windows 10 Pro 10.0.14393

Service Pack: 0

Policies:

| Name | Last Run | Next Run | Run Now |
|---|---|---|---|
| PMP | | Run once at 2017-01-20 10:26 | ▶ |

*It is not recommended to have more than one Policy targeting a single device.*

*Patch approvals or removals are applied during the Update window as specified on the device. This schedule and other settings can be changed using Patch Management Policies at either the Site or Account level.*

**Operating System Patches**

*This list is only updated following a device re-audit.*

▶ Approve (0)

▶ Installed (20)

▶ Do Not Approve (4)

Figure 14.6: Patch Management policies applied to a particular device

### Status of the assigned Patch Management policy

This section displays the operating system installed on the device and its Service Pack number. It also displays the policies that are being applied to the device:

- **Name**: The name of the policy.
- **Last Run**: Date when the policy was last run.
- **Schedule**: Date when the policy is scheduled to be run.
- **Run now**: Runs the patch policy now, outside of its schedule.

### Operating system patches

This section allows administrators to further refine the patches to be installed on the specific device.

The following options are available:

- **Approve**: Denotes patches which have been marked for approval on this device. Patches that are approved are pushed to the device during the policy schedule window and, following their installation, are moved to the next list called **Installed**.
- **Installed**: Denotes patches approved and installed on the device.
- **Do not approve**: Denotes patches that have been excluded from being installed on this particular device. If you have a device with no patch policies targeting it, this section will contain all patches published by Microsoft.

*If a patch is manually uninstalled from a computer, but no entry is added to this section indicating that the patch must be excluded from all patch processes, it will be reinstalled in the next patch run.*

*To uninstall a patch remotely, use the component Uninstall Windows Update by KB Number.*

Each of the above-mentioned sections provides search filters that allow you to look for patches based on the following parameters:

- **Severity**: Filters patches by their severity: **Critical**, **Important**, **Moderate**, **Low**, **Unspecified.**
- **May require reboot**: Displays all patches that may require a reboot to complete the installation process.
- **May require user input**: Displays all patches that may require user interaction to complete the installation process.
- **Search**: Lets you perform an unrestricted search on the fields that describe the patches.

## Patch Management method: usage scenarios

- When the administrator requires very accurate supervision of the patches applied on each device.
- When the administrator needs to install all patches without exception, centrally and automatically.
- When the administrator needs to have computers automatically started and shut down before and after installing patches.

# Device patch status

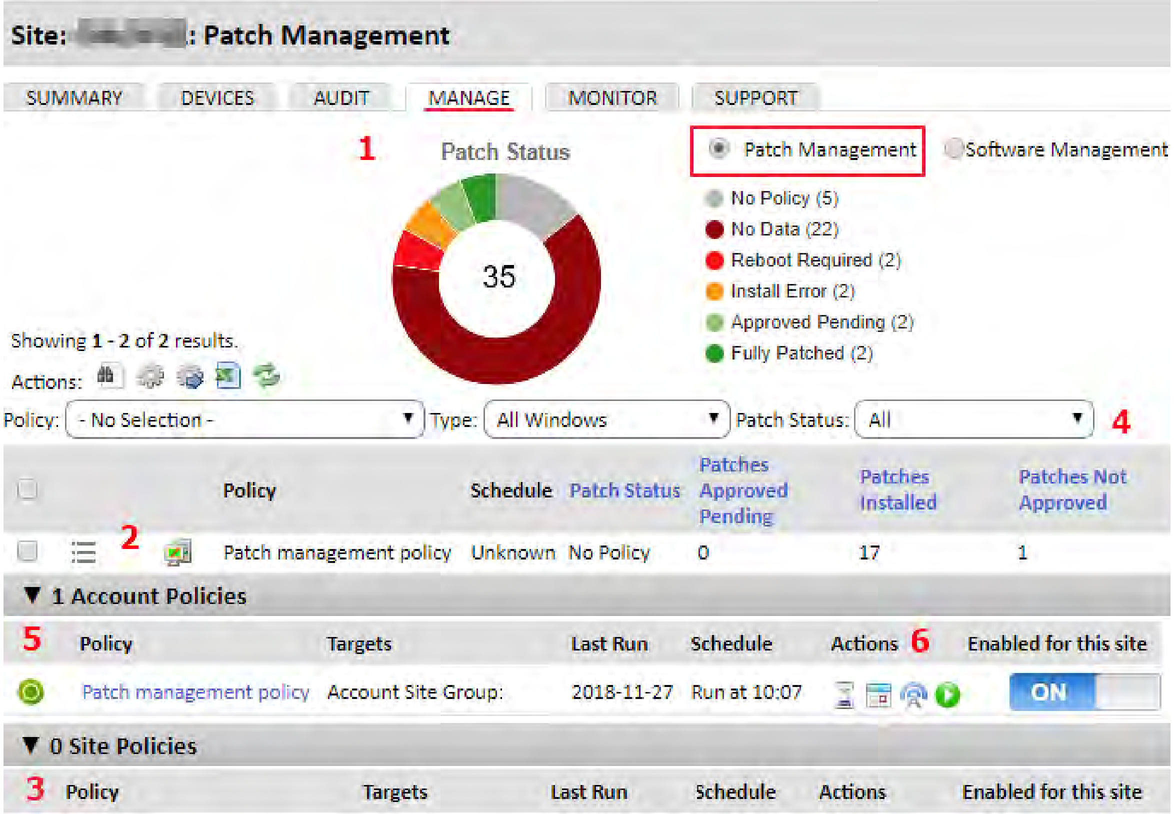
There are two ways for administrators to check the patch status of the IT network:

- **Summary**: shows a pie chart with the percentage of computers in each status category. To view this summary, go to general menu **Sites**, select a site and click **Summary** from the tab menu.
- **Details**: shows the same pie chart as that displayed in section **Summary**, plus a list of the managed devices, their patch status, assigned policies, installed patches, and other relevant information. This information is available at Account and Site level.

- To view the patch status details at Account level, go to general menu **Account**, and click **Manage** from the tab menu. There, click the **Patch Management** radio button on the right-hand side of the screen.
- To view the patch status details at Site level, go to general menu **Sites**, select a site, and click **Manage** from the tab menu. There, click the **Patch Management** radio button on the right-hand side of the screen.

## Managing the device patch status

The **Manage** screen is divided into three areas:



**Site: [redacted]: Patch Management**

SUMMARY | DEVICES | AUDIT | MANAGE | MONITOR | SUPPORT

Showing 1 - 2 of 2 results.

Actions:

Policy: - No Selection - ▾ Type: All Windows ▾ Patch Status: All ▾

| □ | | Policy | Schedule | Patch Status | Patches Approved Pending | Patches Installed | Patches Not Approved |
|---|---|---|---|---|---|---|---|
| □ | | Patch management policy | Unknown | No Policy | 0 | 17 | 1 |

▼ 1 Account Policies

| | Policy | Targets | Last Run | Schedule | Actions | Enabled for this site |
|---|---|---|---|---|---|---|
| ● | Patch management policy | Account Site Group: | 2018-11-27 | Run at 10:07 | | ON |

▼ 0 Site Policies

| Policy | Targets | Last Run | Schedule | Actions | Enabled for this site |
|---|---|---|---|---|---|

Figure 14.7: patch status information on the Manage tab

- **Pie chart (1)**: shows the percentage of fully patched devices and devices with pending patches.
- **Device list (2)**: shows a list of devices and their patch status.
- **List of assigned policies (3)**: helps you locate the Patch Management policies assigned to the devices.

### Patch status pie chart (1)

This chart displays the percentage of computers in each status category. The patch statuses supported are as follows:

- **No policy**: percentage and number of devices with no Patch Management policy assigned.

- **No data**: there is no patch audit data available.
- **Reboot required**: devices with patches downloaded but not installed (they need a reboot to complete the installation process).
- **Install error**: devices where a patch installation error has occurred.
- **Approved pending**: devices with approved patches not installed yet.
- **Fully patched**: fully patched devices.

## Device list (2)

Shows all devices in the selected Account or Site, along with patch status information, and a search bar for finding devices based on their status. You can select the columns to include in the view using the ▦ icon. Below is a description of all columns associated with the patch status of the devices on the screen:

- **Policy**: the name of the Patch Management policy assigned to the device.
- **Last run**: the last run time of the Patch Management policy.
- **Schedule**: the run frequency of the Patch Management policy assigned to the device.
- **Patch status**: **No policy**, **No data**, **Reboot required**, **Install error**, **Approved pending**, **Fully patched**.
- **Last audit date**: the last time the device was audited.
- **Patches approved pending**: the number of patches approved by the assigned policy that have not been installed yet.
- **Patches installed**: the number of patches installed on the device.
- **Patches not approved**: the number of patches marked as excluded in the assigned policy.
- **Last reboot**: shows the date when the device was last rebooted.
- **Reboot required**: indicates whether the device needs a reboot to finish installing patches.

> *The information in this table is updated at device audit time. To update the data, select the device to audit and click the icon from the icon bar.*

The search bar **(4)** lets you filter devices by the following criteria:

- **Account/Site policy**: shows the devices assigned to the selected policy.
- **Type**: shows devices based on their type (All Windows, Windows workstations, Windows servers).
- **Patch status**: **All**, **No policy**, **No data**, **Reboot required**, **Install error**, **Approved pending**, **Fully patched**.
- **Search field**: lets you filter devices by their attributes.

## List of assigned policies (3)

This section displays the list of Patch Management policies created at Account level and Site level.

You will see the following details for each policy:

- **Override Active icon (5)**: this icon only appears if the Account-level policy in question is overridden at Site level. To view/edit the override, click Policies at the Site level. To view the policy's original settings, click its name.
- **Name**: the name of the policy.
- **Targets**: the targets of the policy.
- **Last run**: the last run time of the policy.
- **Schedule**: the run frequency of the Patch Management policy assigned to the device.
- **Push changes**: click this button to immediately push any policy changes to all devices targeted by the policy.
- **Actions**: lets you control certain aspects of the policy.
    - ⌛ : allows you to view results from the last time the policy ran, including: **Patch description**, **Download size**, **Targeted devices**, **Successes**, and **Failures**.
    - 📅: allows you to see what patches would be installed if the policy were run now. It lets you validate the policy, making sure all approved patches are included in the list, and all denied patches are excluded from it.
    - 📡 : shows all sites targeted by the policy. It also displays overridden policies and lets your enable or disable specific sites for the policy.
    - ▶ : clicking this icon displays a dialog box where you can confirm whether you want to run the policy now, outside of its schedule.
- ON : this is a toggle to turn the policy ON or OFF.

# Patch Management method comparison chart

| Method | Patch selection detail level | Automation | Setup time |
|---|---|---|---|
| **Windows Update** | **Low**<br>Patch selection according to the "Important" and "Recommended" groups | **High**<br>The groups of patches to install are configured once. | **Low**<br>Choose whether "important" and "optional" patches are installed. |
| **Patch Management** | **Moderate**<br>Patch selection via multiple configurable criteria. | **High**<br>After creating the filters, the patches will be automatically installed as Microsoft releases them. | **Moderate**<br>Define the filters to select the patches to install. |

Table 14.6: comparison of the Patch Management policies available in Panda Systems Management

# Chapter 15

# Centralized software deployment and installation

The PCSM Server can automatically and remotely deploy files and software packages to all the managed devices across the network. This way, the administrator can make sure that all managed devices have the software and documents that users need to work, without having to go to each device individually or connect via remote access

Automatic software deployment also helps the administrator keep software (Java, Adobe, etc.) vulnerability free, thereby significantly reducing the risk of infection and loss of confidential data.

CHAPTER CONTENT

Software deployment and installation is a process that is executed through application components on Windows, Linux and Mac desktop platforms.

*For more information about how to install apps on iOS smartphones and tablets, refer to the end of the chapter.*

Like the monitor and script components described in "**Components and ComStore**" on page **131**, application components consist of a small script, which in this case simply guides the installation process, and a series of files and/or programs to install.

A separate component must be created for each group of files or programs to install on the user's devices.

# Package deployment and installation procedure

The general procedure consists of several steps:

### 1. Determine the devices on which the software will be installed

The procedure for finding the devices that do not have the necessary files or programs installed will vary depending on whether the Server can perform an audit of the programs installed on the device or not.

If the software to install appears on the list of programs installed kept by the operating system, it will also appear in the Panda Systems Management software audits. Therefore, a filter can be created to filter the devices that already have the software installed.

If the software does not have an installer and therefore does not appear on the list of programs installed or if it is a one-off document, configuration files, etc., the Server will not be able to filter the devices that already have these files installed and the installation script will have to make the appropriate checks manually.

### 2. Check to see if the software to deploy is published in the ComStore

- Click general menu **ComStore** to access Panda Security's free app and component store.
- From the **ComStore** side menu, click **Applications**. The panel on the right will show a list of all available applications.
- Find and click on the `Firefox Multi-lingual [WIN]` application. A window will appear with a description of the component.
- Click the **Add to my Component Library** button. Panda Systems Management will download the package to the administrator's component repository, in the **Components** area. This step is required to use any component published in the ComStore.
- Click general menu **Components** to make sure `Firefox Multi-lingual [WIN]` has been added to the list.

Once the component has been added to the administrator's repository, a job must be created to deploy the installation package to all targeted devices. Refer to chapter "**Jobs**" on page **123** for more information.

### Generate a software installation component

If the software to deploy is not published in the ComStore, you will need to create a software deployment component. The steps involved are the same as those described in the section "**Developing components**" on page **137** for creating script or monitor components.

### 3. Launch a job to push the installation component to the PCSM agent on the affected devices

You can launch a scheduled job for a specific date on which the user is not working with the device, in order to minimize the impact on performance.

### 4. Collect the deployment result in order to identify possible errors

Once the process is complete, an error code and/or message can be collected, which will display the deployment result in the Console.

There are four final statuses:

- **Success**: Deployment execution was completed without errors. The script returns the code `Errorlevel 0`.
- **Success - Warning**: Deployment execution was completed with some unimportant errors. The script returns the code `Errorlevel 0` and a string through the standard output or standard error, which will be interpreted by the Console.
- **Error**: Deployment execution was not completed. The script returns the code `Errorlevel 1`.
- **Error-Warning**: Deployment execution was not completed. The script returns the code `Errorlevel 1` and a string through the standard output or standard error, which will be interpreted by the Console.

# Deployment examples

We'll use a number of examples to illustrate software deployment:

- Deploying documents using a script language.
- Deploying documents without a script language.
- Deploying self-installing software.
- Deploying software without an installer.

*The procedures described here and the third-party tools and script languages used are examples and could vary. Panda Systems Management is designed to be flexible and adapt to the tools with which the administrator feels most comfortable.*

## Deploying documents using a script language

*For the example in this chapter we will use the Deploy_documents.vbs script. The source code of this script is available in chapter “**Source code**” on page **299**.*

The objective of this example is to deploy a folder with three Word documents to the root directory of the targeted user's device. To do this, the following steps are followed:

### 1. Identify the devices to deploy the files to

Panda Systems Management does not have visibility of the content of the file system on users' devices. Therefore, the installation package will be deployed to all the devices which may require the documents, and the script will check to see if the folder containing the files exists or not (lines 25-32).

```
Set objFSO=CreateObject (“Scripting.FileSystemObject”)
Set WshSysEnv=WshShell.Enviroment (“Process”)
Set obj.Folder=objFSO.GetFolger(WshSysEnv(“USERDESKTOP”) & WshSysEnv(“PCSM PATH”)

If err.number<>0 Then
     WScript.Echo ”Deploy unsuccesful: The folder already exist”
     WScript.Quit(1)
End If
```

If the folder does not exist, it is created (line 28), the documents are moved to it (lines 30-32) and a message is sent through the standard output (line 37). However, if the folder exists, it is assumed that the documents have already been deployed and the script ends with an error.

```
‘the folder will be create in the user’s desktop
Set objFolder = objFSO.CreateFolder(WshSysEnv(“USERDESKTOP”)& WshSysEnv(“PCSM
PATH”)
‘the documents will be moved to the folder
objFSO.MoveFile “docl.docs”, objFolder.Path & “\docl.docx”
If Err.Number<> 0 Then
   ‘Wscript.Echo “Deploy unsuccessful: “ & Err.Description
    WScript.Quit (1)
Else
    Wscript.Echo “Deploy OK: All files were copied”
    WScript.Quit (0)
End If
```

### 2. Generate a file deployment component using a script

- Go to general menu **Components**, and click **New Component** from the left-side panel:
- Select **Applications** from the **Category** drop-down list. Enter a name and a description.
- Click the **Add file** button and add the three files you want to deploy.
- In the **Commands** section, add the source code you can find in section “**File deployment**” on page **301** and select **VBScript** from the **Install command** drop-down list.
- In the **Variables** section, click the ⊕ icon and enter, in the **Name** field, the name of the variable that will contain the path to the folder to deploy, in this case `PCSM_PATH`. Then, select **Variable Value**

from the **Type** drop-down list. In **Default**, enter the string to be used if the administrator doesn't specify anything during the script launch process. Finally, in **Description**, enter a description of the purpose of the variable.

- Click Save.

The configured component will run the script which, in turn, will check to see whether the folder with the documents exists on the user's computer. If it doesn't exist, it will create it and move the three documents to it. This operation will be performed on all devices that receive the deployment component.

In **Post-Conditions**, you can specify text strings that the Console will interpret as warnings.

The example specifies that if the standard output (**Resource:stdout**) contains (**Qualifier:is found in**) the string **Deploy unsuccessful**, the result of executing the script will be considered Warning.

### 3. Launch a job to push the software to the agents on the affected devices

> *Refer to chapter "**Jobs**" on page **123** for more information on how to create immediate and scheduled jobs.*

- Click general menu **Jobs**, and click **New Job** from the tab menu.
- Click the **Add targets** button to select the job targets.
- Click the **Add a Component** link. All application components marked as favorites will be displayed.
- Click **Save**.

### 4. Collect the deployment result in order to identify possible errors

The output conditions defined in the example script are three:

- **Success**: The files are copied to the target folder without any errors (lines 30-32). Ends with an `Errorlevel 0` (line 38).
- **Error**: An error occurs when copying the files. Ends with an `Errorlevel 1` (line 35).
- **Success - Warning**: The folder already exists so the files are not copied. Ends with `Errorlevel 0` (line 23) and the string **Deploy unsuccessful** is generated, which the Server will interpret as warning, as configured in the **Post-Conditions** section in step 3.

After the job has been launched, it will appear in general menu **Jobs**, **Active Jobs** tab.

In Tab bar, **Completed Jobs**, you can see the deployment result, in Red if it ended with error, Orange if there was a warning or Green if it was successful.

The **Stdout** and **Stderr** icons show a copy of the standard output and standard error generated by the script.

## Deploying documents without a script language

The installation script can be greatly simplified if previous checks are not required or if warnings do not need to be generated in the Console.

This example deploys the 3 documents from the previous example but in this case, instead of generating the folder structure from the script, a self-extracting .EXE package is created which contains the compressed documents and the folder structure considered necessary. The .EXE package can be generated using many tools. This example uses WinRAR.

*To download a free version of WinRAR, go to http://www.winrar.com*

This example generates a self-extracting .EXE file with the following characteristics:

- Works in Silent mode.
- The folder with the content will be automatically created in `C:\documentation`.
- If the folder already exists, its content will be overwritten without warning.

*It is essential to generate a self-extracting file that works in silent mode, i.e., it does not display dialog boxes or windows and does not require user intervention.*

### 1. Identify the devices on which to install the software.

Follow the steps on point 1 from section "**Deploying documents using a script language**".

### 2. Generate a file distribution component

Follow the steps detailed in section 2 of the "**Deploying documents using a script language**". In this case, the component will need a simple script, so in the field **Installation command** choose Batch and enter the following information.

```
@echo off

pushd %~dp0

name_of_the_self-extracting_file.exe
```

You won't need to define input or output variables as the path to copy the files to is defined in the self-extracting package itself.

## Create a self-extracting file

Follow these steps to generate a silent self-extracting file:

- **Prepare the folder with the documents to deploy.**

Create the root folder `c:\documentacion`, and place all of the files, folders and subfolders to be deployed inside.

- **Generate the executable file.**

With the WinRAR program open, drag the recently created folder ACME Documents and select the option **Create SFX archive** and **Create solid archive**.

- **Configure the behavior of the executable file**

At this point, you must set the file to run silently, that is, no dialog boxes will be shown to the user. Also, the executable file will overwrite all files that already exist on the target computer.

- On the **Advanced** tab, click the **SFX options** button.
- On the **Modes** tab, select Hide all.
- On the **Update** tab, **Update mode** section, select **Extract and replace files**.
- On the **Update** tab, **Overwrite mode** section, select **Overwrite all files**.
- Click **OK**.
- On the **General** tab, specify the path the files will be uncompressed to in section **Path to extract**.

### 3. Launch a job to push the software to the Agents on the affected devices.

Follow the steps in the 3 point from section “**Deploying documents using a script language**”.

### 4. Collect the result in order to identify possible errors.

Follow the steps in the 4 point from section “**Deploying documents using a script language**”.

## Deploying self-installing software

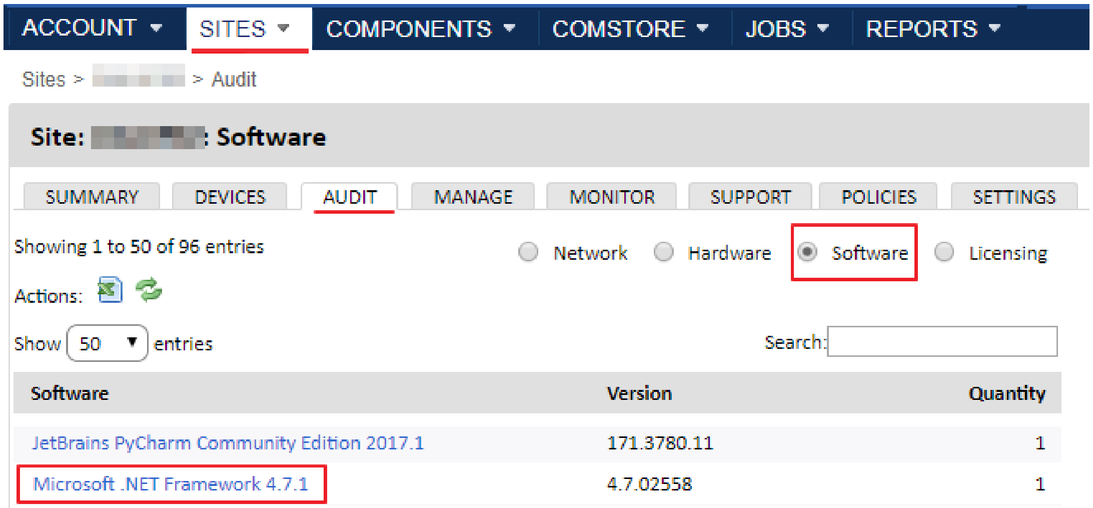
In this example, the Microsoft Framework .NET 4.0 `dotNetFx40_Full_x86_x64.exe` package will be deployed to the devices on which it is not already installed.

To do this, and as Microsoft Framework .NET 4.0 is a program that appears in the program list kept by the device's operating system, we will use a filter to identify those on which it is not installed.

The installation package is a self-extracting .EXE that admits the parameters `/q /norestart` to execute in silent mode and prevent the device from restarting, so no additional special preparation is required.

## 1. Identify the devices on which to install the software.

To filter the devices on which the software is already installed, you need to know which identification string corresponds to the package already installed. This data can be obtained from Tab bar, **Audit**, **Software** on a device on which the package is already installed.



Sites > [redacted] > Audit

Site: [redacted]: Software

Showing 1 to 50 of 96 entries

○ Network ○ Hardware ● Software ○ Licensing

Actions:

Show 50 entries

Search:

| Software | Version | Quantity |
|---|---|---|
| JetBrains PyCharm Community Edition 2017.1 | 171.3780.11 | 1 |
| Microsoft .NET Framework 4.7.1 | 4.7.02558 | 1 |

Figure 15.1: obtaining the installed application ID string

This data is used to create a site filter or an account filter with the following settings:

*Refer to chapter "**Creating a site filter**" on page **81** for more information about creating and managing filters.*

- **Field**: Software package to inspect the software installed on the device
- **Search Item**: Here you can enter the string that identifies the software to install
- **Condition**: **Does not contain** to select the devices that do not contain the content specified in **Search Item** in the **Software package** field.

## 2. Generate a file distribution component

Follow the steps detailed in section 2 of the "**Deploying documents using a script language**" section. As in this case the software package requires parameters to be installed in quiet mode it is necessary to pass them in the field **Installation command**. In this case choose as **Batch** script language:

```
@echo off

pushd %~dp0

dotNetFx40_Full_x86_x64.exe /q /norestart
```

The script only has one relevant line, which is the one that executes the installation package with the necessary parameters to achieve a silent installation.

### 3. Launch a job to push the software to the PCSM agent on the target devices.

Follow the steps detailed in section 3 of the "**Deploying documents using a script language**" section but in the **Group type** field select **Account Filters** and choose the filter created in step 1.

### 4. Collect the result in order to identify possible errors.

A good way of checking the installation result is to check the previously prepared device filter to see if the number of devices on which the deployed software is not installed is lower. All of the devices that continue to appear in the filter will have returned some kind of error.

> *The device audit data containing the hardware and software installed is sent to the Server by the Agent every 24 hours, so the recently installed software list will not be updated until this time has elapsed. However, you can force a manual update using the* ***Request device audit*** *action from the icon bar.*

## Deploying software without an installer

Many programs consist of a single executable file without an associated installer that generates the necessary structure in the Start menu, the desktop shortcuts or the corresponding entries in Add or Remove Programs. These types of programs can be deployed by following the document or self-extracting package example. However, doing it in this way prevents the Server from generating a reliable audit of the programs installed, as they will not appear in the list of programs installed kept by the device's operating system.

For this reason, third-party tools are often used that generate a single MSI package with all of the programs to add, creating the necessary groups in the Start menu and the shortcuts on the user's desktop in order to simplify execution.

To do this, this example will use the program Advanced Installer, the free version of which allows you to easily generate MSI installers.

> *To download EXE to MSI Converter Free, go to: https:// www.exemsi.com/*

Follow these steps to generate the installer:

### 1. Identify the devices to deploy the files to

Follow the steps detailed in point 1 of section "**Deploying documents using a script language**". In this case, the entry that will appear in Add/Remove Programs will be known beforehand, as the `EXE` to `MSI Converter Free` program lets you configure the name of the program that will appear in that section. Therefore, you can enter the name directly in the **Find** field of the filter.

### 2. Generate a file deployment component using an MSI installer

Since, in this case, the software package requires a series of parameters in order to install in silent mode, you must enter them in the **Install command** field. In this case, select **Batch** as the script language:

```
@echo off

pushd %~dp0

MSIEXEC /I "my software.msi" /qn
```

## Create a self-extracting MSI file

Follow these steps to generate a silent self-extracting file:

- Run the program `EXE` to `MSI Converter Free` and click **Next**.
- On the **Executable** screen, enter the name of the executable file in the **Setup Executable Input File Name** text box, enter the name and path of the `.msi` file to generate in the **MSI Output File Name** text box, and click **Next**.
- On the **Security and User Context** screen, click **Next**.
- On the **Application ID** screen, click the **Create new** button and then click **Next**.
- On the **Properties** screen, specify the **Product Name**, **Manufacturer** and **Version** using the following format: `x.x.x.x`. This is the data that will be displayed in the Add/Remove Programs section of the Window operating system.
- On the **More properties** screen, click **Next**.
- On the **Parameters** screen, click **Next**.
- On the **Actions** screen, click **Next**.
- On the **Summary** screen, click **Build**. The `.msi` file will be generated in the specified path.

### 3. Launch a job to push the software to the PCSM agent on the target devices

Follow the steps detailed in point 3 of section "**Deploying documents using a script language**" except for the following: select **Custom Device Filters** from the **Target type** drop-down list and select the filter created in step 1.

### 4. Collect the job result in order to identify possible errors

A good way of checking the installation result is to check the previously prepared device filter to see if the number of devices on which the deployed software is not installed is lower. All of the devices that continue to appear in the filter will have returned some kind of error.

> *The device audit data containing the hardware and software installed is sent to the server by the agent every 24 hours, so the recently installed software list will not be updated until that time has elapsed. However, you can force a manual update using the option **Request device audit(s)** from the icon bar.*

# Bandwidth usage optimization in software deployments

Panda Systems Management implements two mechanisms (Peer Sharing and the local cache role) to prevent downloading the same component multiple times from the PCSM server. Refer to section "**Configuring a local cache node**" on page **65** for more information on the Peer Sharing technology and how to assign the local cache role to a desktop or server.

# Software installation on iOS devices

The procedure to deploy software to iOS tablets and smartphones is different from the aforementioned one as these devices have limitations regarding the origin of the software to install. In the case of iOS devices, every downloaded item must come from Apple Store.

*App installation on Android devices is not supported in this version of Panda Systems Management.*

## Requirements for installing apps on iOS devices

To download apps to iOS devices, follow the steps below:

- Go to general menu **ComStore**.
- Download the Mobile Device Management component.

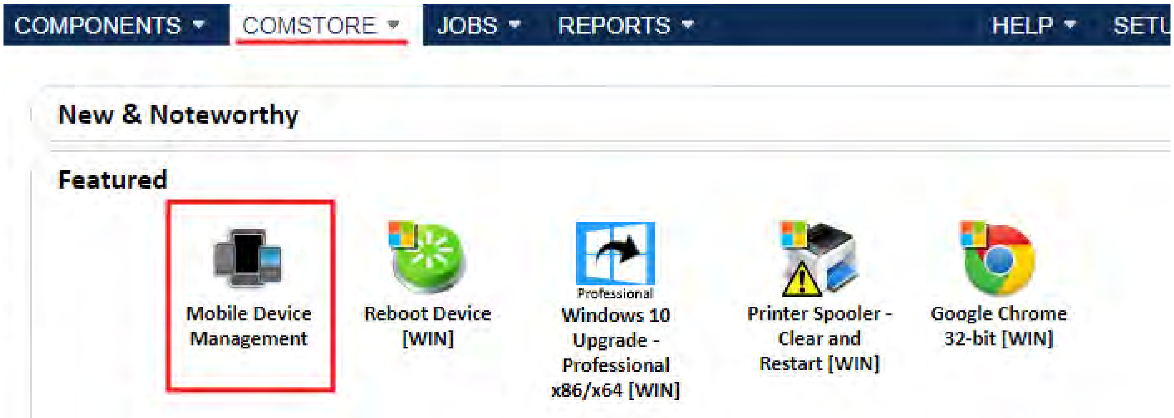


Figure 15.2: mobile Device Management component

- To add the apps to deploy to your iOS devices to the **Application List**, click the **Add iOS App** button from the left-hand side menu of the ComStore. This will take you to the app selection window.
- There you must specify the customer's country and enter the app name in the text box.
- Click **Search** to find the app, along with its price and a basic description.
- Click **Add** to add it to the **Application List**.

## Installing apps from the Application List

Create a software management policy to deploy apps to end users' iOS devices:

- Determine if the software to install will be run on devices belonging to one or multiple sites.
  - Multiple sites: Go to general menu **Account**, **Manage** tab.
  - One site: Go to general menu **Sites**, select a site and click the **Manage** tab.
- Select the **Software Management** radio button and click the **Add site policy** button in the bottom left corner of the screen.
- Select the apps to deploy by clicking **Add an app**, and add the devices that they will be deployed to by clicking **Add target**.
- After selecting the apps to deploy, if any of them is a paid app, click the ✏ icon to enter the relevant **Redemption Code**.
- Finally, click the **Push changes** button to instantly send the configured apps to the devices selected in the policy and which are turned on at the time of pushing the changes.

*If an iOS device is turned off at the time of pushing the changes, it will appear in section Non-Compliant Devices. To set the changes to be automatically applied as soon as the device becomes available, click the ➜ icon.*

# Chapter 16

# Software Management

Keeping the applications installed on systems up-to-date is a key task for IT departments. Many typical applications and libraries contain bugs and vulnerabilities used by viruses and threats, which providers resolve by updating them periodically.

Panda Systems Management ensures that supported applications installed on managed computers can be kept up-to date with no need for action by users or administrators. You can also quickly locate devices that do not comply with any software policies and approve software updates immediately.

Administrators won't have to manually crosscheck new releases of the programs used by users with the Software Management module, nor create or update any components in order to deploy them. Similarly, there will be a snapshot of the status of computers, quickly identifying those that fail to comply with any existing software policies.

Such advantages will deliver time savings and simplification to the management of corporate networks, while improving the security of the applications installed on computers.

CHAPTER CONTENTS

# Software Management workflow

In order to manage the entire range of critical applications on network computers, an administrator's workflow will, in general terms, be as follows:

- Administrators create a software management policy in line with an overall strategy. Refer to section "**Software Management policy**"
- Depending on the selected procedure for approving updates, specified in table **16.3**:
  - Panda Systems Management approves and installs the updates automatically.
  - Panda Systems Management requires manual approval of updates with the button in the application list in the software management panel.
- Administrators check that network computers comply with the software management policies. Refer to section "**Viewing the software management status**" and section "**Creating Software Management reports**".

# How the Software Management module works

## Features

The module has three main functions:

- **Management of third-party software updates:** it keeps computers up-to-date with the latest versions of frameworks and programs.
- **Approval of updates:** it sets the update installation mode so they are carried out either manually or automatically.
- **Compliance reports:** it indicates whether managed computers have the latest versions of applications and frameworks installed.

## Functionality

Panda Systems Management automatically looks for updates for the applications installed and allows them to be approved automatically or manually. The module also provides hands-free, immediate software installation whenever a new version is detected. This installation can also be scheduled for a later time. Refer to "**Creating a Software Management policy**" for more details.

## Supported applications

The main aim of the Software Management module is to ensure that computers on the network have the latest available versions of the software installed.

In addition, Panda Security keeps track of the new versions of supported applications and includes a quality control feature to ensure that updates are correctly installed on users' devices. Consequently, updates will be available for installation within a maximum of 48 hours from their publication by the vendor and in the language of the user's computer.

The Software Management module supports the following applications:

| Applications | Windows | macOS |
|---|---|---|
| 7-Zip | YES | |
| Adobe Acrobat Reader DC | YES | YES |
| Adobe Air | YES | YES |
| Adobe Flash Player | YES | YES |
| Adobe Shockwave Player | YES | |
| Datto File Protection | YES | YES |
| Datto Workplace Classic | YES | YES |
| FilleZilla Client | YES | YES |
| Foxit Reader | YES | |
| Google Chrome | YES | YES |
| Java Runtime Enviroment | YES | YES |
| Microsoft Office 365 | YES | |
| Mozilla Firefox | YES | YES |
| Notepad ++ | YES | |
| Paint.NET | YES | |
| PUTTY | YES | |
| Skype | YES | YES |
| VLC Media Player | YES | YES |
| VMWare Tools | YES | |
| Zoom | YES | |

Table 16.1: applications supported by the Software Management module

*This list is continuously updated. For new programs, please contact Panda Security.*

The Software Management module functionality is unrelated to that of the ComStore. Administrators won't have to deploy the software using components nor check for new versions that would mean altering them.

# Software Management module requirements

## Firewall settings

Panda Systems Management looks for program updates on vendors' web pages, so the corporate firewall and the one installed on the device itself have to allow access and the downloading of content from these pages in order for the updates to take place.

| Application | URL |
|---|---|
| **Adobe Acrobat Reader DC** | https://storage.centrastage.net |
| **Deploy F-Secure Computer Protection** | https://download.sp.f-secure.com |
| **FileZilla Client** | https://filezilla-project.org |
| **Foxit Reader** | https://www.foxitsoftware.com |
| **Mozilla Firefox** | https://download.mozilla.org |
| **Notepad ++** | https://notepad-plus-plus.org |
| **Paint.NET** | https://www.dotpdn.com |
| **PuTTY** | https://the.earth.li |
| **Skype** | https://get.skype.com |
| **Trend Micro Worry-Free Services-Deployment** | https://wfbs-svc-nabu-aal.trendmicro.com<br>or<br>https://wfbs-svc-emea-aal.trendmicro.com |
| **VLC Media Player** | https://www.mirrorservice.org |
| **Windows 10 Upgrade - Professional x86/x64** | https://storage.centrastage.net |

Table 16.2: URLs for updating applications

## Supported platforms

Platforms supported by the Software Management module:

- Windows (32 and 64-bit)
- macOS

*Refer to section "**Supported applications**" for a list of the applications supported by the Software Management module.*

## Permissions

Depending on the level from which the software management policy is run, it may be necessary to create permissions. Refer to section "**Alerts and tickets**" on page **247** on page 269.

# Software Management policy

When a new Panda Systems Management account is created, a Software Management type policy is created automatically. Refer to "**Policies**" on page **93** for more details on the Panda Systems Management policies system.

## Concept of compliant and not compliant devices

Devices managed with a Software Management module policy can have one of three different statuses:

- **Unmanaged**: in this case, no Software Management policies are applied to the device.
- **Not compliant:** this is when one or more of the supported applications have the status 'Not compliant'. This occurs when the device does not have the latest available version installed.
- **Compliant**: this is when all the applications managed by the policy have the latest version installed.

## Creating a Software Management policy

To create a Software Management policy, follow the steps below:

- Establish the environment or level of the policy according to the devices that will be affected.
    - To create an account-level policy, click **Account** in the general menu, then **Policies** from the tab menu, then **New account policy** at the bottom of the panel.
    - To create a site policy, click **Site** in the general menu, then, in the site, click **Policies** from the tab menu and, then **New site policy** at the bottom of the panel.
- Specify the **Name** of the policy in the text box and, in the **Type** drop-down menu, select **Software Management**. Click **Next**.
- In the window for creating policies, add the **Targets** to which the policy will be applied and the **Timing options: Immediately** or **On a schedule**. Refer to "**Launching scheduled jobs**" on page **127** for more details of the job scheduler.
- In the managed applications listed in table **16.3** select how each one will be updated:

| Action | Description | Compliance report |
|---|---|---|
| **Unmanaged** | Default selection. Panda Systems Management will not install or update the application. | The application will always be considered compliant. |
| **Manual approve** | Administrators have to manually approve each update for this application as they become available. If the application is not already installed, it won't be installed. | The application is considered compliant when it is absent or when it is installed and updated. |

Table 16.3: options for approving a Software Management policy

| Action | Description | Compliance report |
|---|---|---|
| **Manual approve + install if not present** | Administrators have to manually approve each update for this application as they become available. If the application is not already installed, installation must be approved. | The application is considered compliant only when it is present and updated. |
| **Auto approve** | Panda Systems Management will automatically update the application without the need for approval. If the application is not already installed, it won't be installed. | The application is considered compliant when it is absent or when it is installed and updated. |
| **Auto approve + install if not present** | Panda Systems Management will automatically update the application without the need for approval. If the application is not already installed, it will be installed automatically. | The application is considered compliant only when it is present and updated. |

Table 16.3: options for approving a Software Management policy

- Click **Save.** The policy created will appear in the list of **Account** or **Site** policies, depending on where it was created.

- To deploy it, select the **Push changes** ▦ option next to it.

*Once installation of an update has been approved, the action cannot be reversed. To stop the installation of applications, the policy will have to be edited accordingly.*

# Viewing the software management status

*Even though the changes to the status of software are displayed automatically in the Software Management screens, these changes may take up to 24 hours to be reflected in the audits.*

## Dashboard

To access from Account level:

- In the general menu, select **Account** and then **Manage** from the tab menu. Then select the **Software Management** radio button to see the software management status.

To access from Site level:

- In the **Sites** menu, choose the site and then click **Manage** from the tab menu. Use the radio button to open the **Software Management** panel **(1).**

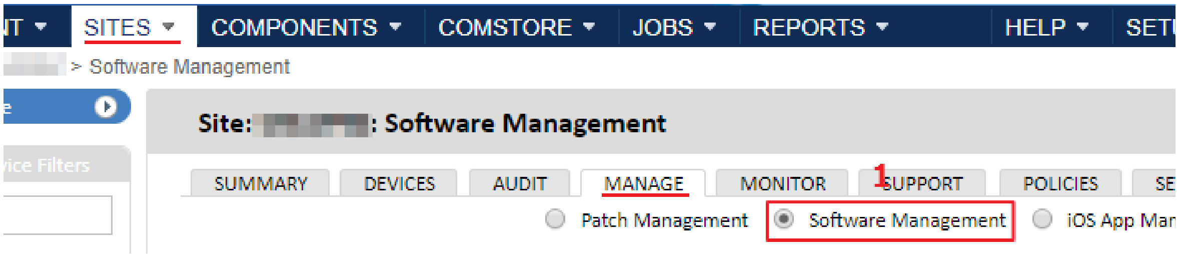
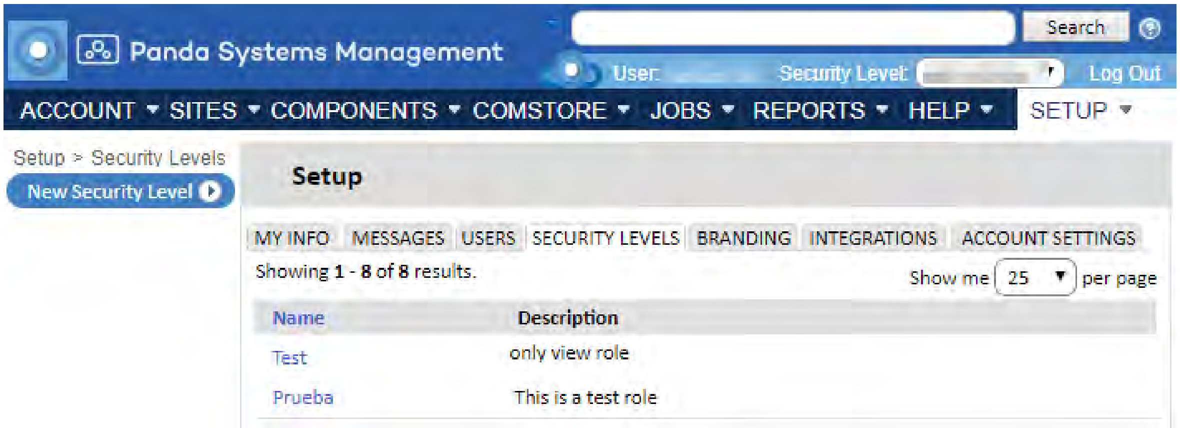


Figure 16.1: Path to Software Management at Site level

The dashboard contains the following components:

- **Pie chart (1)**: here you can see the number of compliant and not compliant devices of those managed by the policy.
    - **Total**: number of devices in the policy.
    - **Compliant**: number of applications whose status is compliant.
    - **Not compliant**: number of applications whose status is not compliant.
- **Search bar (2):** filter devices according to the parameters entered.
- **Device lists (3):** list of all devices managed by the policy.
- **Application lists (4):** list of all applications managed by the policy.



Showing **1 - 8** of **8** results.

| Name | Description |
|---|---|
| Test | only view role |
| Prueba | This is a test role |

Figure 16.2: general dashboard view

## Search bar

By using different criteria for the search you can filter the results displayed to find the devices you want to work on.

| Field | Description |
|---|---|
| **Policy** | List of the Software Management policies. Account-level policies are displayed at both Account and Site level, while Site-level policies are only displayed at Site level. No policy is selected by default. |

Table 16.4: search bar items

| Field | Description |
|---|---|
| **Type** | • All<br>• All Windows<br>• All Mac<br>• All Windows servers<br>• All Windows workstations |
| **Software status** | • All<br>• Not compliant<br>• Compliant<br>• Unmanaged |
| **Search** | Enter a text and click **Search** to filter the results. |

Table 16.4: search bar items

## List of devices

This displays the devices managed by the policy and their status.

| Field | Description |
|---|---|
| **Site name** | Name of the site that the device is associated with |
| **Device hostname** | Device name. |
| **Device description** | Device description. |
| **Policy** | The name of the Software Management policy associated with the device. |
| **Last run** | Date and time the policy was last run. |
| **Schedule** | Next time the Software Management policy is due to run. |
| **Software status** | • Unmanaged<br>• Compliant<br>• Not compliant<br>For more information about the software statuses, refer to "**Concept of compliant and not compliant devices**". |

Table 16.5: items displayed on devices at Account and Site level

## List of applications (Account and Site level)

This is a list of the supported applications, indicating the latest versions released and the action configured.

*Refer to "**Supported applications**" for more details.*

| Field | Description |
|---|---|
| **Application name** | Name of the supported application. |
| **Latest version** | The latest version available for the operating systems:<br>• Windows 32-bit<br>• Windows 64-bit<br>• macOS |
| **Not compliant** | Number of not compliant devices when one or more of the applications don't have the latest available version. |
| **Approve button** | Allows you to approve an update manually. The application will be installed immediately. The button only appears when the policy is set to **Manual Approve** or **Manual approve + install if not present** and the status of the managed application **is Not compliant**. See the table **16.3**. |

Table 16.6: device list items

### List of applications (Device level)

This dashboard is accessible from Device level, through the **Manage** tab to manage each connected device individually. In this case, the module options vary, displaying different fields and actions.

| Field | Description |
|---|---|
| **Name** | Name of the supported application. |
| **Installed version** | Version of the application installed on the device. |
| **Latest version** | Latest version available. |
| **Action** | The action of the software management policy as defined in the policy details. Refer to "**Creating a Software Management policy**" on page **241**. |
| **Status** | One of the following statuses is displayed:<br>• **Compliant**: the version installed is the latest version released by the software vendor.<br>• **Not compliant**: the version installed is not the latest version released by the software vendor.<br>• **Unmanaged**: The policy action is configured as Unmanaged for all supported applications.<br>• **Install error**: the latest attempt to install or update resulted in an error. |
| **Stdout / Stderr** | Click to see the Stdout or Stderr message for the last activity on the device. |

Table 16.7: dashboard items from the device

| Field | Description |
|---|---|
| **Approve button** | Click the button to approve the installation of the software application. The application will be installed immediately. The button only appears when the policy is set to **Manual Approve** or **Manual approve + install if not present** and the status of the managed application is **Not compliant**. |

Table 16.7: dashboard items from the device

# Creating Software Management reports

The software management system supports the creation of reports through the **Executive summary** and **Device health summary** features. To see all the contents and features of the reports, refer to chapter "**Reports**" on page **187**.

## Executive summary

This gives a general view of the status for the level that it has been generated for. In total there are six areas:

- Asset management
- Monitoring
- Patch Management
- Software Management
- Antivirus
- Proactive Maintenance

## Device health summary

This shows the status of the device and can be accessed through each device on the system. It gives an overview of the device's status:

- Disk space
- RAM
- Software compliant
- Patches
- Antivirus
- Under warranty
- Online within last 30 days
- Open alerts

# Chapter 17

# Alerts and tickets

The monitors constantly check the configured parameters on a device. When these parameters are exceeded, the monitor will trigger an alert or ticket to draw the administrator's attention to the issue.

CHAPTER CONTENT

## Alerts and ticket management cycle

Panda Systems Management uses alerts to warn network administrators of a problem affecting managed devices. This way, when a monitor notices that a device is operating outside the established parameters, it will trigger an alert in accordance with the rules below:

- An alert corresponds to a single network computer.
- When an alert is triggered its status is **Open**, to indicate that there is an unresolved problem.
- The status of an alert changes automatically to **Closed**, when the error has disappeared and the time specified in the monitor settings (**Auto-resolution**) has elapsed.

- To prevent having multiple alerts open corresponding to resolved issues, administrators can close them manually.
- If a device triggers an alert that had already been resolved but the error condition reoccurs, Panda Systems Management will trigger a new alert.

Once an alert has been triggered, the administrator can access the description and details to decide on the corrective action to take, either connecting to the device remotely or resetting the monitor parameters if they are too strict. If a lot of similar alerts are being triggered, they can be muted to avoid excessive noise.

Once an alert is resolved, it can be closed to remove it from the list of open alerts and thereby focus attention on the alerts that still require administrators' attention.

The alert management cycle is as follows:

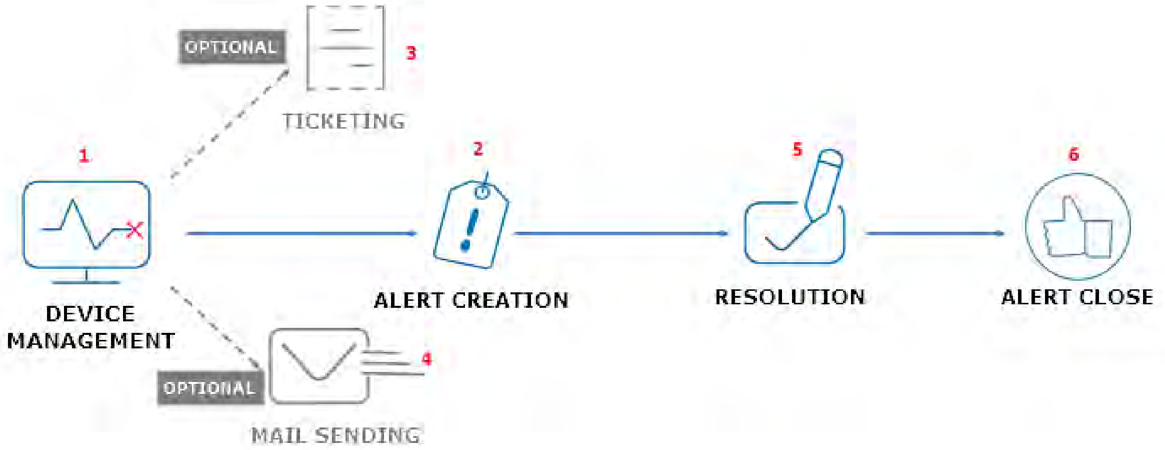


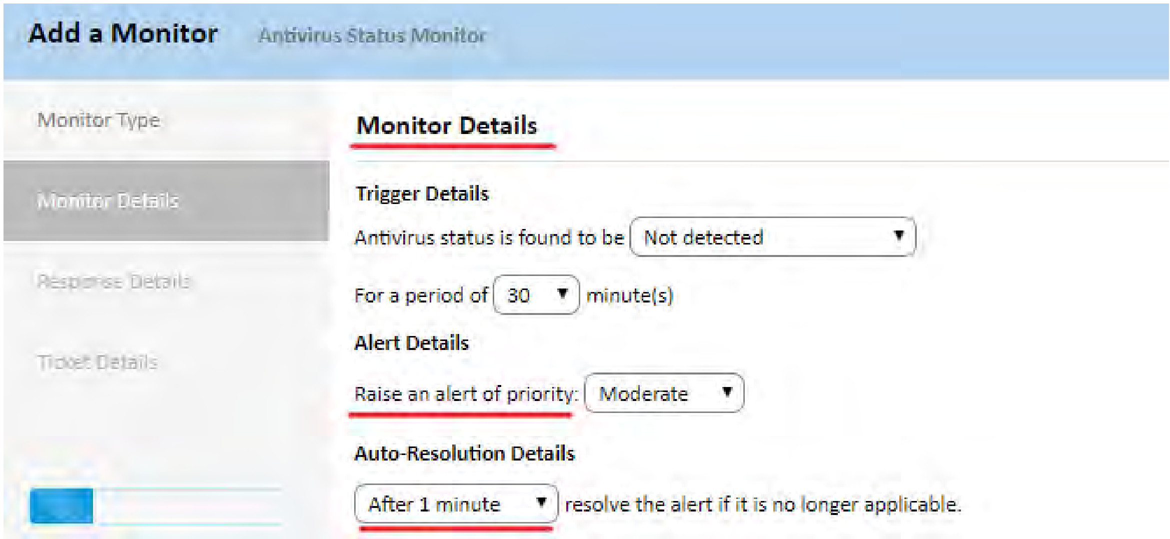
Figure 17.1: alert management flow in Panda Systems Management

- A monitor detects that a parameter has been exceeded on a device **(1)** and generates an entry in the list of alerts **(2)**. The category and priority of the alert will depend on the type of monitor, and the priority settings in the monitor.
- Depending on the monitor settings, the administrator may receive an email **(4)** advising of the existence of the alert, and a ticket is generated **(3)**. These emails include a link to the alert ID.
- The administrator will find details of the alert in the console (priority, type, devices involved, associated monitor and other information).
- If similar alerts are being triggered at the same time, administrators can temporarily stop the emails being sent by muting the alert. They will however continue to be added to the list of alerts.
- Administrators can launch the remedial action required **(5)** (see section "**Remote access tools**" on page **257**) or lower the monitor settings.
- Either the administrator or the system closes the alert manually **(6)** and reactivates the emails, should the alert occur again in the future. Administrators may have configured the triggering of alerts in auto-resolution mode, this means that an alert will close automatically once the time specified in the associated monitor settings has elapsed.

# Alerts

## Alert settings

Only monitor policies can trigger alerts and they are configured from the monitor itself. See section "**Creating monitors manually**" on page **106** to start configuring a monitor-type policy.



Monitor Details

Trigger Details

Antivirus status is found to be Not detected

For a period of 30 minute(s)

Alert Details

Raise an alert of priority: Moderate

Auto-Resolution Details

After 1 minute resolve the alert if it is no longer applicable.

Figure 17.2: alert settings

On the **Monitor Details** screen, specify the following parameters:

- **Alert Details**. **Raise an alert of priority**: indicates the priority of the alerts generated by the monitor. This priority can be used later when ordering and filtering open alerts.
- **Auto-Resolution Details**: specifies the time that has to elapse for the alert to close automatically if the issue that caused it has disappeared.

## Alert management

### Alert rate limit

To avoid raising a massive number of alerts, each configured monitor has a limit of 10,000 alerts per device per day. Once this limit is hit, the following actions are taken automatically:

- The monitor is automatically disabled for the device that exceeded the threshold. The monitor's ON/ OFF toggle on the **Policies** tab is automatically set to OFF. See "**Gestión de monitores**" on page **124**.

A notification email is sent to all administrators (max. 50 users) to inform them that the monitor has been disabled on the device due to rate limiting.

### Viewing the alerts triggered

To display a list of the alerts triggered, go to the **Monitor** tab of the corresponding level, depending on the scope of the information you want:

- To display a list of all alerts triggered in the account:
  - Click **Account** from the main menu and then **Monitor** from the tab menu.
  - In the top right of the screen, click **Monitor Alerts**.
- To display a list of the alerts triggered on a site:
  - Click **Sites** from the main menu, and then the site.
  - From the tab menu, click **Monitor**.
- To display a list of the alerts triggered on a single device:
  - Click **Sites** from the main menu, and then the site.
  - Click **Devices** from the tab menu, and then the device.
  - From the tab menu, click **Monitor**. Then, in the top right of the screen, click **Monitor Alerts**.

## Viewing alert information

Click an alert to display a screen with information.

The available options are as follows:

| Section | Field | Description |
|---|---|---|
| **Device Summary** | **Hostname** | Name of the device that triggered the alert. |
| | **Site** | Site the device belongs to. |
| | **Operating System** | Name and version of the operating system installed on the device. |
| | **Make/Model** | Hardware make and model. |
| | **Last User** | Name of the account that last logged in on the computer. |
| | **User-Defined Fields 1-30** | Content of the user-defined fields if the component associated to the monitor uses them. See section "**Labels and user-defined fields**" on page **145** for more information. |
| | **Description** | Device description. |
| | **IP Address** | IP address of the device's network interface |
| | **Architecture** | 32-bit or 64-bit. |
| | **Serial No** | |
| | **Domain** | Windows domain the device belongs to. |

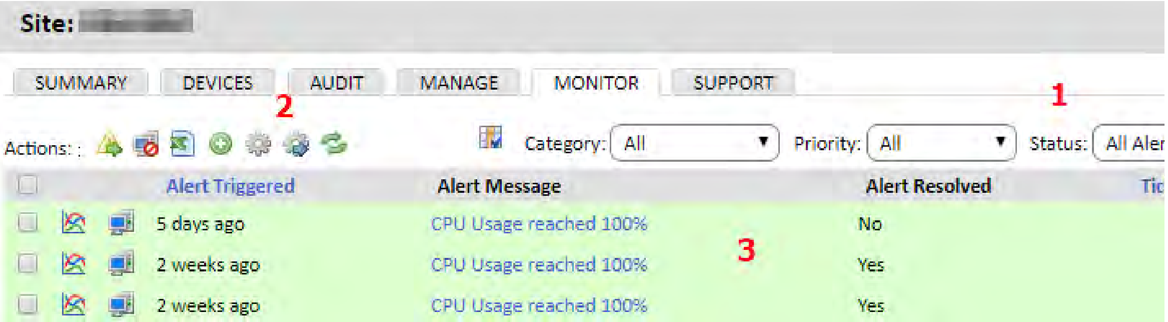
Table 17.1: alert features

| Section | Field | Description |
|---|---|---|
| **Alert Summary** | **Alert UID** | Unique identifier of the alert. |
| | **Policy** | Unique identifier of the alert.<br>Name of the monitor policy that triggered the alert. Click to show the policy definition and the associated monitors. |
| | **Resolved** | The alert remains open unless closed by the administrator or the system. |
| | **Alert Triggered** | Date and time the alert was triggered. |
| | **Message** | Details of the reason why the monitor triggered the alert. |
| | **Trigger** | Rule that triggered the alert. |
| **Alert Summary** | **Muted** | Determines whether or not administrators will receive an email for each alert triggered. |
| | **Alert Received** | Date and time the system displayed the alert on the console. |
| **Diagnostic Summary** | **Diagnostic Summary** | Displays a window with details of the diagnosis generated by the monitor. See "**Diagnostic summary**" on page **140**. |
| **Alert Response** | **Action** | Action taken by Panda Systems Management when the alert is triggered in line with the settings in the monitor (send email and generate ticket). |
| | **Message** | Email subject and the message in the ticket. |

Table 17.1: alert features

## Alert management

Alerts are managed from the icon bar **(1)** below the tab menu from various levels (Figure **17.3**).



| □ | | | Alert Triggered | Alert Message | Alert Resolved |
|---|---|---|---|---|---|
| □ | | | 5 days ago | CPU Usage reached 100% | No |
| □ | | | 2 weeks ago | CPU Usage reached 100% | Yes |
| □ | | | 2 weeks ago | CPU Usage reached 100% | Yes |

Figure 17.3: list of alerts

| Icon | Description |
|---|---|
| **Resolve selected alerts** | Sets the status of the selected alerts to Resolved. |

Table 17.2: icons in the Alerts list icon bar

| Icon | Description |
|---|---|
| **Disable Monitor(s) for Devices** | Prevents the monitors assigned to the devices from sending email notifications. |
| **Un-Mute Monitors for Devices** | It allows re-triggering of email notifications for device monitors. |
| **Export to CSV** | Export the list of alerts to a .CSV file. |
| **New Ticket** | Assign a new ticket. See "**Tickets**". |
| **Schedule a job** | Schedule a job for the device(s) that the selected alerts were created for. |
| **Run a quick job** | Run a quick job on the device(s) that the selected alerts were created for. |
| **Refresh** | Manually refresh the page to see the results. |

Table 17.2: icons in the Alerts list icon bar

## Alert search and filters

To find any alert, Panda Systems Management provides a search filter bar **(2)** (Figure 17.3). The available options are:

| Field | Description |
|---|---|
| **Category** | Filter by the category of the monitor that triggered the alert. |
| **Priority** | Filter by alert priority. The priority is set in the settings of the monitor that triggered the alert. |
| **Status** | Filter by alert status: open, resolved or muted. |
| **Search** | Filter by the content of certain alert fields. |

Table 17.3: alert filter bar

## Alert list fields

The list of alerts can be configured using an icon **(3)** (Figure 17.3) to add or remove columns describing the alert. Below you can see the specific columns.

| Field | Description |
|---|---|
| **Alert Type** | Icon that describes the type of monitor that triggered the alert. |
| **Alert Triggered** | Shows how long ago the alert was triggered. |
| **Alert Message** | Description of the reason why the monitor triggered the alert. |
| **Alert Resolved** | Indicates if the alert has been closed. |
| **Ticket Number** | Identifier of the ticket associated with the alert. |

Table 17.4: alert list fields

| Field | Description |
|---|---|
| **Alert Muted** | Indicates if the administrator has muted the alert to prevent emails from being sent. |
| **Priority** | Importance of the alert in accordance with the monitor settings. |
| **Resolved** | When the alert has been resolved it indicates how long it was open for and who closed it (the agent if the criteria established by the monitor has disappeared or the administrator account name if the alert was closed manually). |

Table 17.4: alert list fields

# Tickets

Tickets add the following functionalities to the alerts:

- They offer technicians the option to add information about the problem detected, the work carried out or the solutions applied.
- They can be created automatically by a monitor, but also manually by a technician or even a network user.

## Ticket settings

### Creating a ticket automatically with the monitor settings

Tickets created automatically from a monitor are associated with the alert that it triggers.

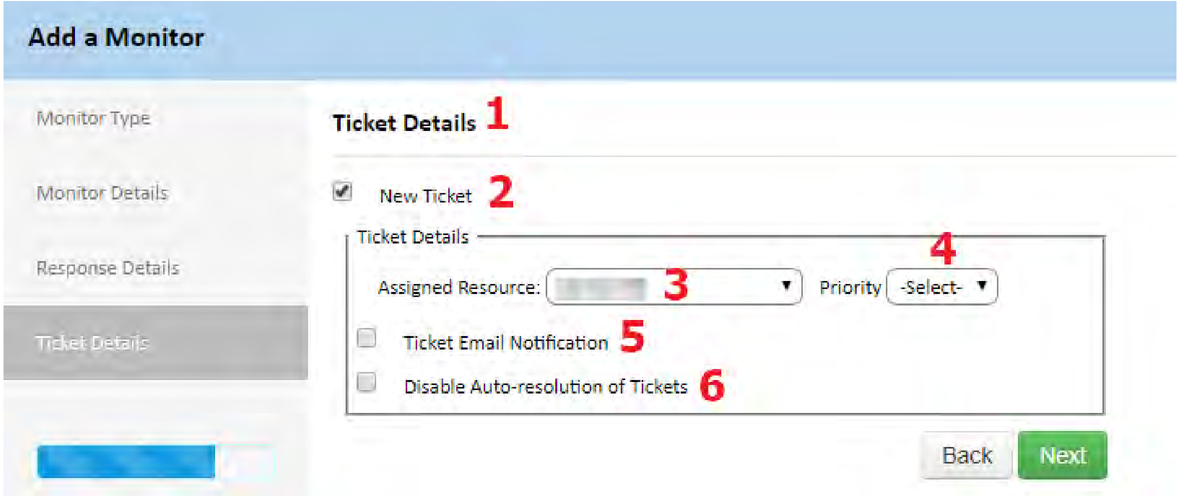


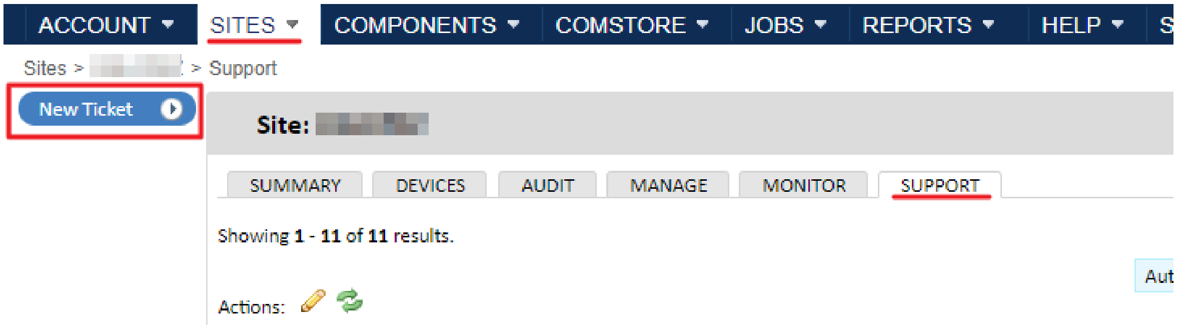
Figure 17.4: generating tickets from a monitor

- See section "**Creating monitors manually**" on page **106** to start configuring a monitor.
- In the **Ticket Details (1)** section of the monitor settings, select the option **New Ticket (2)**.
- Use the **Assigned Resource (3)** box to specify the network administrator responsible for the service monitoring the ticket.

- Select the **Priority (4)** of the ticket.
- Specify if there will be an email notification **(5)** and if the ticket will be resolved automatically. **(6)**

## Creating a ticket from the management console

Tickets generated from the management console do not have an associated alert as they are created manually by the network administrator in response to a situation that has not been triggered by the system.



Showing **1** - **11** of **11** results.

Figure 17.5: creating a ticket from the management console

- Go to general menu **Sites**, choose the site, and then select the **Support** tab.
- Click **New Ticket** in the top left of the screen.
- Enter the summary/title of the ticket, description, priority and the network administrator to whom it will be assigned.
- Click **OK**. The new ticket will be added to the list and will have the status **New**.

## Creating a ticket from the PCSM agent

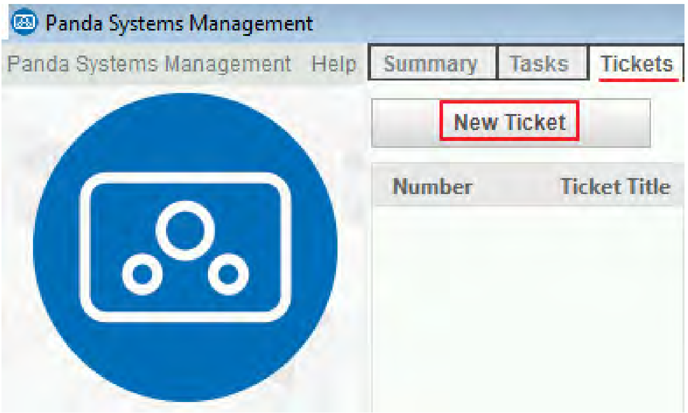


Figure 17.6: creating a ticket from the PCSM agent

For those cases in which a problem on a device does not trigger an alert or the automatic generation of a ticket, users can advise the IT team of the issue. To do so, follow the steps below:

- On the user's device, click the PCSM agent icon in the notification area on the left of the taskbar in the desktop.
- Click **Tickets**, then **New Ticket**.
- Specify the ticket title, the description and the issue, then click **OK**.
- There will automatically be a new entry in the **Support** tab of the administrator's console with the new ticket.

### Creating tickets from an alert

In the event that the monitor settings do not require tickets to be created, but the administrator wants to add information to the alert, follow the steps below:

- Go to general menu **Sites**, click the relevant site and then the **Monitor** tab.
- Use the checkboxes to select the alerts that will be assigned to the ticket. One ticket can only have one alert assigned, so if several alerts are selected, there will be one ticket for each of them.
- From the icon bar, click the ⊕ icon and specify the administrator account to which the tickets will be assigned, the priority and whether an email notification will be generated.
- Click **Save**. The tickets will appear on the **Support** tab and the **Description** will contain the same content as the **Alert Message** field of the alert.

## Ticket management

### Viewing the tickets created

Go to the **Support** tab from the various levels, depending on the scope of the information you want:

- To display a list of the tickets generated for the whole account, click general menu **Account** and then **Support** from the tab menu.
- To display a list of the tickets generated for a site, click general menu **Sites**, click the site and then **Support** from the tab menu.
- To display a list of the tickets generated for a device:
  - Click general menu **Sites**, click the site, and then **Devices** from the tab menu.
  - Select the device in the list, click **Support**, and then, in the top right of the screen, select **Monitor Alerts**.

### Viewing ticket information

Click the **Number** field of a ticket to see a screen with information about the ticket.

The information available is as follows:

| Field | Description |
|---|---|
| **Created by** | The user account that created the ticket from the web console or from a monitor, or the name of the device if the ticket was created by the user of the affected device. |
| **Site** | Site that the device referred to by the ticket belongs to. |
| **Create Date** | Date and time the ticket was created. |
| **Status** | Ticket status. Tickets have the status **New** when they are created and administrators can change this as the incident progresses. |

Table 17.5: ticket details

| Field | Description |
|---|---|
| **Priority** | Incident priority on a scale of 1 to 5. |
| **Assigned to** | Account of the technician assigned to resolve the incident. |
| **Ticket Tittle** | Ticket subject. |
| **Description** | Progress of the ticket. Full description of the issue detected. If the ticket was created by a user or from the management console, there are comments entered manually. If the ticket was created by a monitor, there is an automatic description of the monitor parameter that has been exceeded. |

Table 17.5: ticket details

## Editing tickets

- To edit the status of a ticket, select the ticket and click **Update status of selected tickets** from the icon bar.
- To edit the rest of the ticket fields, click **Number** and edit the corresponding field. Then click **Save**.

## Ticket filters

Use the options **Open Tickets**, **All Tickets**, and **My Tickets** to filter the list of tickets by status.

## Ticket list fields

| Field | Description |
|---|---|
| **Number** | Character string that uniquely identifies the ticket. |
| **Site** | Site that the device referred to by the ticket belongs to. |
| **Created by** | The user account that created the ticket from the web console or from a monitor, or the name of the device if the ticket was created by the user of the affected device. |
| **Ticket Tittle** | Ticket subject. |
| **Description** | Progress of the ticket. Full description of the issue detected. If the ticket was created by a user or from the management console, there are comments entered manually. If the ticket was created by a monitor, there is an automatic description of the monitor parameter that has been exceeded. |
| **Priority** | Incident priority on a scale of 1 to 5. |
| **Status** | Ticket status. Tickets have the status **New** when they are created and administrators can change this as the incident progresses. |
| **Create Date** | Date and time the ticket was created. |
| **Assigned To** | Account of the technician assigned to resolve the incident. |

Table 17.6: attributes of the tickets shown on the tickets list

# Chapter 18

# Remote access tools

Panda Systems Management enables administrators to remotely and seamlessly access IT devices on their network to resolve incidents without interrupting users or having to be physically in front of the affected device.

CHAPTER CONTENT

# Available remote access tools

## Tools integrated into Panda Systems Management

Many of the remote access tools are designed to be run on the background without disrupting users' activities. Table **18.1** shows a list of all available tools along with a description and the type of tool (intrusive or compatible with the user's activity).

| Tool | Description | Background |
|---|---|---|
| **Remote Screen Capture** | Quick viewing of error messages. | YES |
| **Windows Services Tab** | Remote access to stop, start, and restart services without a remote desktop connection. | YES |
| **Screen Share Session** | Remote desktop access via VNC or Web Remote. Available from the PCSM agent and from the management console. | NO |
| **Windows RDP** | Remote desktop access via RDP. It entails shutting down the user's session. In accordance with the group policy (GPO) set by the administrator, users will have to provide an additional password. | NO |
| **Command Shell** | DOS or PowerShell remote command line interface. | YES |
| **Shutdown/Reboot** | Shut downs or restarts the remote device. | NO |
| **Agent Deployment** | Installs the agent remotely across the local network. | YES |
| **Task Manager** | Remote access to the Task Manager without a remote desktop connection. | YES |
| **File Transfer** | Provides full access to the remote device's file system, allowing the administrator to transfer files between their computer and the user's computer, move files, create and delete folders, and rename items. | YES |
| **Drive Information** | Lists all local and network drives currently connected to the remote device, allowing the administrator to add or delete network paths. | YES |
| **Registry Editor** | Remote access to the `Regedit` tool without a remote desktop connection. | YES |
| **Quick Jobs** | Enable administrators to launch jobs on the remote device. | YES |
| **Event Viewer** | Remote access to the Event Viewer without a remote desktop connection. | YES |
| **Wake Up** | Wakes up a remote device on the network by sending it a "magic packet" from a device on the same subnet. | YES |
| **Connect to Network Devices** | Enables administrators to remotely connect to the configuration interface of network devices. | N/A |

Tabla 18.1: remote access tools integrated into Panda Systems Management

## Availability of the PCSM agent tools by platform

The availability of the PCSM agent tools depends on the operating system installed on the remote device. Table **18.2** shows the tools that are available based on the operatingsystem of the remote device.

| Tool | Windows | macOS | Linux |
|---|---|---|---|
| Remote Screen Capture | YES | YES | |
| Windows Services Tab | YES | | |
| Screen Share Session (VNC and Web Remote) | YES | YES | |
| Windows RDP | YES | | |
| Command Shell | YES | YES | YES |
| Shutdown/Reboot | YES | YES | YES |
| Agent Deployment | YES | YES | |
| Task Manager | YES | | |
| File Transfer | YES | YES | YES |
| Drive Information | YES | | |
| Registry Editor | YES | | |
| Quick Jobs | YES | YES | YES |
| Event Viewer | YES | | |
| Wake Up | YES | YES | YES |
| Connect to Network Devices | YES | YES | YES |

Tabla 18.2: remote access tools integrated into Panda Systems Management

## Requirements for accessing the tools

In order to remotely access the resources of a managed device, this device must have a PCSM agent installed, except as described in section "**Accessing devices not compatible with the PCSM Agent**".

Additionally, the device used by the network administrator to access the remote device must also have a PCSM agent installed, except for the following tools, which only require a web browser compatible with Panda Systems Management:

- Remote Screen Capture
- Screen Share Session via Web Remote.

All other tools require that a PCSM agent be installed on the administrator's device.

> *Use a Windows device to manage devices on your network with the PCSM agent.*

## Accessing the tools from the console

The management console includes shortcuts to make the tools included in the PCSM agent easier to use. The benefits of using the console shortcuts are:

- The management console invokes the PCSM agent with the right credentials, enabling the administrator to skip this step.
- The management console invokes the PCSM agent pointing to the selected device. This way, there is no need to browse the computer structure from the computer panel in the PCSM agent in order to find the device to manage.

These shortcuts can be found in the context menus associated with each device on a list of devices, and on the **Summary** tab of any device.

- To access a device's context menu from a list of devices:
  - Go to general menu **Sites**, select a site, and click **Devices** from the tab menu. A list of devices is displayed, with a context menu associated with each line in the table.
  - Place the mouse pointer over the context menu icon ☰ to display the shortcuts available for that particular device based on its type.

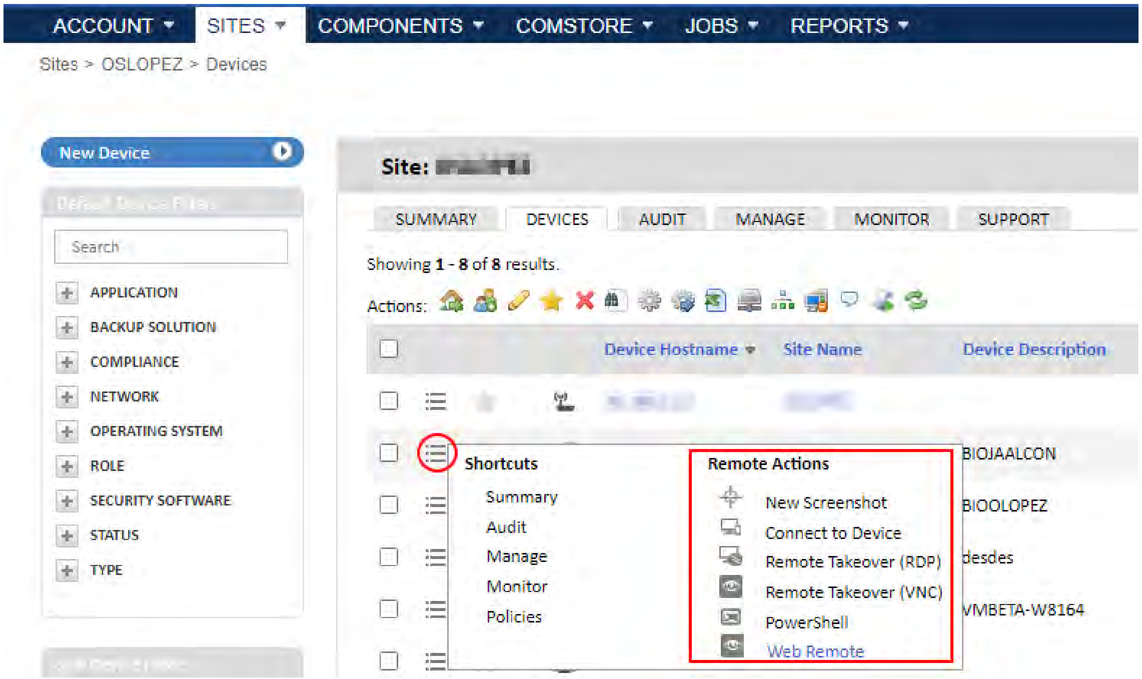
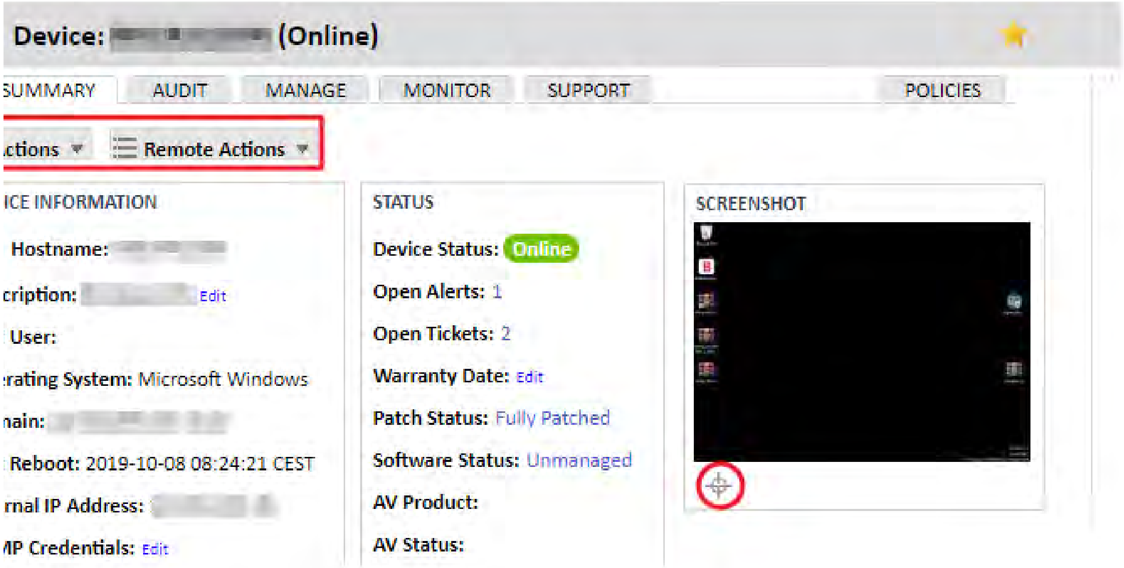


Figura 18.1: accessing the Remote Actions context menu from a list of devices

- To access the remote access tools from the **Summary** tab:

- Go to general menu **Sites**, select a site, and click **Devices** from the tab menu. Click the device that you want to access.
- On the **Summary** tab, place the mouse pointer over the **Actions** and **Remote Actions** context menus, or click the ⌖ icon.



Device: [redacted] (Online)

Hostname: [redacted]

cription: [redacted] Edit

User:

rating System: Microsoft Windows

nain: [redacted]

Reboot: 2019-10-08 08:24:21 CEST

rnal IP Address: [redacted]

IP Credentials: Edit

Device Status: Online

Open Alerts: 1

Open Tickets: 2

Warranty Date: Edit

Patch Status: Fully Patched

Software Status: Unmanaged

AV Product:

AV Status:

Figura 18.2: accessing the remote access tools from the Summary tab

The shortcuts to the PCSM agent tools accessible from the web console are:

| Tool | Description |
|---|---|
| ⌖ | Refreshes the thumbnail image of the desktop of the remote device displayed in the management console. |
| **New Screenshot** | Opens a window with a screenshot of the desktop of the remote device. |
| **Connect to Device** | Connects the PCSM agent installed on the administrator's computer tothe remote device, so the login credentials don't have to be manuallyentered. |
| **Remote Takeover (RDP)** | Establishes a remote desktop connection to the selected device using theRDP protocol. |
| **Remote Takeover (VNC)** | Establishes a remote desktop connection to the selected device using theVNC protocol. |
| **Connect (HTTP)** | Establishes an HTTP tunnel connection to the network device. See "**Accessing devices not compatible with the PCSM Agent**". |
| **Connect (Telnet/SSH)** | Establishes a Telnet/SSH tunnel connection to the network device. See "**Accessing devices not compatible with the PCSM Agent**". |
| **Connect (custom)** | Establishes a custom tunnel connection to the network device. See "**Accessing devices not compatible with the PCSM Agent**". |
| **Send a message to the selected devices** | Shows a pop-up message on the desktop of the remote device. |

Tabla 18.3: remote access tools accessible from the management console

| Tool | Description |
|---|---|
| **PowerShell** | • Establishes one or multiple simultaneous remote connections to the selected device with the PowerShell interpreter.<br>• Requires providing RDP credentials.<br>• Requires configuring the remote device to receive PowerShell remote commands by running the `Enable-PSRemoting` command. |
| **Web Remote** | Establishes a remote desktop connection to the selected device from the management console. On computers where there are multiple users with an interactive session initiated, Web Remote enables you to connect to each session separately. |

Tabla 18.3: remote access tools accessible from the management console

### Accessing the tools from the PCSM agent

Accessing the PCSM agent tools from the management console is much quicker; however, not all tools can be accessed that way. For this reason, the administrator can use the PCSM agent to have access to all tools.

To access the PCSM agent tools, you need to enter administrator credentials in the agent. This can be done directly through the agent itself or from the web console:

- From the web console:
  - From the context menu associated with the device (see section "**Accessing the tools from the console**" en la página **260**), click the **Connect to Device** option. This launches the PCSM agent installed on the administrator's computer with the right credentials.
  - Access the control tools in the upper-left corner of the window.
- From the agent itself:
  - Find and double-click the PCSM agent icon in the notification area of your Windows desktop.
  - Enter the administrator credentials and click the **Log in** button.
  - Click the 🏠 icon to view all sites configured in the account. Select the relevant site and click the device you want to connect to. The panel on the right will display information from the device.
  - Click the device again to open the management tools panel.

# Remote takeover tools

Administrators can establishes a remote desktop connection to a Windows or macOS computer using the following tools:

- **Remote Takeover (VNC)**: establishes a connection to the current remote desktop session using the VNC protocol.
- **Remote Takeover (RDP)**: creates a new remote desktop session on Windows computers using the RDP protocol.

- **Web Remote**: connects to an interactive session directly from the management console.

# Remote takeover via VNC

This tool shares the desktop, mouse, and keyboard of the remote device using the Virtual Network Computing (VNC) protocol. If VNC is disallowed on a target device, the VNC connection will fail. To allow or disallow the use of VNC on a remote device, see "**Configuring VNC for Windows devices**".

*VNC does not allow user switching and will not be able to connect to a device where no user is logged in.*

## Using VNC on macOS devices running Mojave or Catalina

- If connecting to a remote user's macOS device running Mojave, a pop-up notification displays stating the PCSM Agent.app program would like to control this computer using accessibility features. Direct the user to click **Open System Preferences** on the device and to select the application in the **Privacy** panel to allow interaction between their device and the agent's VNC session using Vine Server. Please note that Vine Server is installed during the PCSM agent installation and runs as user (instead of root) so that the above permission can take effect.
- In order for VNC to function properly on macOS devices running Mojave or Catalina, these applications must be listed and checked under **System Preferences**, **Security & Privacy**, **Privacy** in the following sections:
  - **Accessibility**: PCSM Agent, Vine Server.
  - **Full Disk Access**: PCSM Agent, Vine Server.
- If Vine Server is updated, you may need to remove the PCSM Agent application from the list, for any settings within the panels under **System Preferences** > **Security & Privacy** > **Privacy**. Then, on the next activity requiring the PCSM agent, the operating system will display a pop-up notification prompting the user to re-add the application.

## Access in view only mode

If you would like to open a VNC session to share the remote user's desktop but without the ability to control their keyboard or mouse, click the arrow next to the VNC icon and click **Connect in View Only Mode**.

## Configuring VNC for Windows devices

To allow or disable VNC remote takeover at Account level:

- Go to general menu **Setup**, click **Account settings** from the tab menu, and go to the **VNC Settings** section.
- Set **Allow VNC** to **ON** or **OFF**. You can select whether to apply the setting to all sites in the account or selected sites:

- When switched OFF, VNC is disallowed and the VNC service will be removed from all devices along with all associated files.
- When switched ON, VNC is allowed and the agents will download and install the VNC service automatically on all devices.

## Remote takeover via RDP

This tool creates a new, separate remote desktop session on Windows devices using the Remote Desktop Protocol (RDP).

To see what is shown on the remote device's screen using RDP, click on the arrow next to the RDP icon and click **Connect to Console Session**.

### Network Level Authentication (NLA)

Network Level Authentication (NLA) is an authentication tool used in Remote Desktop Services (RDP Server) or Remote Desktop Connections (RDP Client), introduced in RDP 6.0 in Windows Vista and above. NLA requires the connecting user to authenticate themselves before a session can be established with the remote device. This is due to the fact that starting a remote session on a device can use up CPU resources on that device. This can be prevented by requiring the connecting user to authenticate themselves first. Any failed attempt made by an unauthorized user will not allow to establish a connection and, consequently, will not use the device's CPU resources. Requiring user authentication before the remote session also provides a layer of defense against Denial of Service (DoS) attacks.

When a user tries to establish a connection to a device with NLA enabled, NLA will send the user's credentials to the server for authentication before creating a session. Only once the user authentication is successful will the connection be established.

To enable NLA, access one of the paths below:

- **Start menu > Control Panel > System and Security > System > Remote Settings > Remote > Remote Desktop >** select **Allow connections only from computers running Remote Desktop with Network Level Authentication**.
- **Start menu > Control Panel >** right-click on **Computer > Properties > Remote Settings > Remote > Remote Desktop >** select **Allow connections only from computers running Remote Desktop with Network Level Authentication.**

### Opening an RDP session with a device with NLA enabled

- Log in to the PCSM agent and connect to a server.
- Click the RDP icon, enter your user name and password, and select **Use Network Level Authentication**. The option to use NLA will be grayed out on incompatible devices.
- Select **Remember passwords for this device** if you want your password to be remembered for future RDP sessions.

- Click **Login** to establish the connection. The connection will be established if the user authentication has been successful.

## Remote takeover via Web Remote

This tool shares the desktop, mouse, and keyboard of the remote device using HTML5 remote control technology. It features faster connection times and is available as a remote action for online servers, laptops, and desktops.

A Web Remote session can be initiated from any device supported by Panda Systems Management using the latest version of a compatible web browser; a PCSM agent is not required on the administrator's computer. However, only Windows and macOS devices with a PCSM agent installed can be controlled via a Web Remote session.

Web Remote supports simultaneous connections to one device from multiple users. See "**Multi-session support**".

### Using Web Remote on macOS devices running Mojave or later

For Web Remote to function properly on macOS devices running Mojave or later, these applications must be listed and checked under **System Preferences** > **Security & Privacy** > **Privacy** in the following sections:

- **Accessibility**: PCSM agent, Vine Server.
- **Full Disk Access**: PCSM agent, Vine Server.
- **Screen recording**: PCSM agent, Vine Server.

### GPU acceleration on the administrator's computer

Starting from Windows NT 6.2 (Windows 8/Windows Server 2012), hardware acceleration is permitted when screen sharing. Using this technology in Web Remote where possible results in a marked improvement in the quality and responsiveness of the takeover session experience.

GPU acceleration prerequisites:

- Windows NT 6.2 (Windows 8/Windows Server 2012) or above only. Windows NT 6.1 (Windows 7/ Windows Server 2008 R2) or below must use VNC.
- The PCSM agent must use .NET Core. Otherwise, VNC must be used, even on Windows NT 6.2 and above.

⚠ *On hybrid systems (those with two graphics cards: an integrated graphics card and a separate/discrete graphics card), GPU acceleration is not compatible with the discrete graphics card.*

## GPU acceleration on hybrid systems

On hybrid systems with two graphics cards: one integrated into the motherboard and an additional separate graphics card (also known as discrete graphics card), GPU acceleration is not supported on the discrete graphics card. This limitation is due to the Microsoft API. Consequently, in order to use GPU acceleration in this scenario, the Web Remote process must be switched to the integrated graphics card.

With NVIDIA graphics cards:

- Open the NVIDIA Control Panel and navigate to **3D Settings > Manage 3D Settings**.
- Select the **Program Settings** tab and click the **Add** button.
- Choose the RMM.WebRemote process and click **Add Selected Program**.
- Select **Integrated processor** as the preferred graphics processor and then click **Apply** to apply the changes.

With AMD Radeon graphics cards:

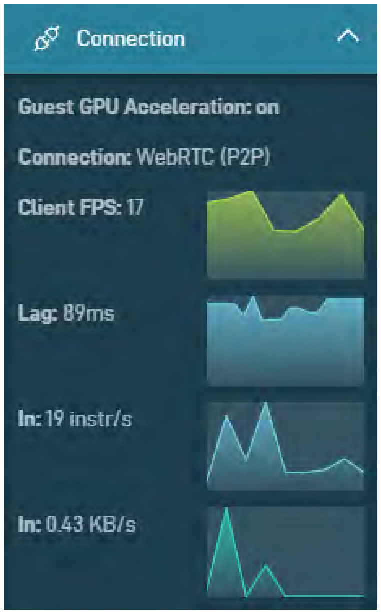
- Open the Radeon Settings panel.
- Navigate to **System** > **Switchable Graphics**.
- Navigate to the RMM.WebRemote process in the list, select it to open its drop-down menu, and select **Power Saving**. The changes will take affect the next time Web Remote is started.

## Requirements for access with WebRTC

WebRTC is an open framework that enables Real-Time Communication (RTC) capabilities in the web browser. Web Remote leverages this technology to allow a fast peer-to-peer (P2P) connection to be established between devices if available. If a P2P route is not possible, WebRTC will fall back to a relay connection via the Panda Systems Management servers.

For additional reliability, a WebSocket connection is automatically attempted in parallel with each WebRTC connection. The following scenarios are possible:

- If WebRTC fails to connect but WebSocket succeeds, the WebSocket channel is used for communication.
- If WebRTC succeeds but then disconnects in the middle of the session, an automatic failover to the WebSocket channel occurs without the user experiencing a disconnect.
- If WebSocket fails to connect and WebRTC succeeds, WebRTC is used.
- WebRTC is always preferred over WebSocket, whether the connection is P2P or Relay.



Connection

Guest GPU Acceleration: on

Connection: WebRTC (P2P)

Client FPS: 17

Lag: 89ms

In: 19 instr/s

In: 0.43 KB/s

Figura 18.3: Connection panel in a takeover connection

To check the type of connection and graphics acceleration of the WebRTC connection established to the user's device, click the right menu **Connection**. A panel opens with all required information:

- **Guest GPU Acceleration**: ON or OFF.
- **Connection**: connection type.
- **Client FPS**: frames received per second.
- **Lag**: communication lag in milliseconds.
- **Ln**: number of graphical primitives received per second.
- **Ln**: bandwidth measured in kilobytes per second.

For Web Remote to be able to establish connections, the following rules are added to the device's firewall to allow inbound and outbound traffic:

- **RMM RTC Proxy**: RMM Web Remote RTC Proxy Service
- **RMM RTO Proxy**: RMM Web Remote RTO Proxy Service
- **RMM Web Remote**: RMM Web Remote Process

## Multi-session support

Web Remote supports multi-session devices such as Windows Virtual Desktops and servers running Remote Desktop Services (RDS). After initiating a Web Remote session on one of these devices, technicians can view a list of users who are logged in to the device and then choose a user session to connect to the device.

## Privacy mode

*For more information about privacy modes, refer to "***Privacy Mode Options***" en la página* **98**

If privacy mode is set on the remote device, the end user will be prompted to accept or decline a connection request by a dialog box displayed by the PCSM agent and which includes the requesting technician's name and email address. If the end user's screen is locked, the prompt will not be displayed, and the technician will be notified on the connection screen.

Once the connection is in progress, a message will be displayed to the end user that a remote takeover is currently in progress. This message will only appear once the end user has accepted the connection request. Web Remote will reconnect with the same session should a brief interruption in

Internet connectivity occur; a second privacy mode prompt will not appear as the end user has already accepted the connection.

*If the privacy mode request message does not display (macOS only), check that the System Events checkbox is selected under* ***System Preferences > Security & Privacy > Privacy > PCSM Agent****.*

# Accessing devices not compatible with the PCSM Agent

Routers, switches, switchboards, and printers are network devices not compatible with the PCSM agent but which incorporate more or less standardized services that allow administrators to remotely access and manage them. However, those services pose a big problem for organizations: They can only be used from inside the corporate network.

In this scenario, it is common practice to configure a computer accessible from the outside that can work as a proxy when the administrator is not directly connected to the corporate network and needs to manage this type of devices. Panda Systems Management automates this operation by means of a network computer designated as Network Node, thereby eliminating the need for manual port forwarding in corporate routers or purchasing and configuring access VPNs.

Panda Systems Management enables the administrator's computer to connect to the device to manage using Telnet, SSH, HTTP, and other protocols, regardless of location. The Network Node computer then manages the administrator's requests and collects the appropriate results, delivering them in real time to the IT staff.

Computer management through a Network Node is as follows:

- The administrator's Systems Management agent creates a tunnel between the administrator's computer and the Network Node device. This tunnel has, at the administrator's end, the IP address 127.0.0.1 on a port randomly assigned by the PCSM agent. This tunnel, which is managed by the Systems Management server, goes through the organization's perimeter firewalls as well as the personal firewall installed on the Network Node computer.
- The administrator then runs a management client application and connects it to the local address assigned by the PCSM agent 127.0.0.1 {port}.
- From then on, all traffic directed to the 127.0.0.1:port address on the administrator's computer is routed through the tunnel and is received by the Network Node computer on the organization's network.
- The Network Node collects this data and forwards it to the service installed on the remote device to manage (via HTTPS, SSH, Telnet, or other).
- The service installed on the remote device collects the administrator's requests, process them, and returns them to the Network Node.
- The Network Node then routes the response through the set tunnel in order to deliver it to the

application connected to 127.0.0.1:port on the administrator's computer.

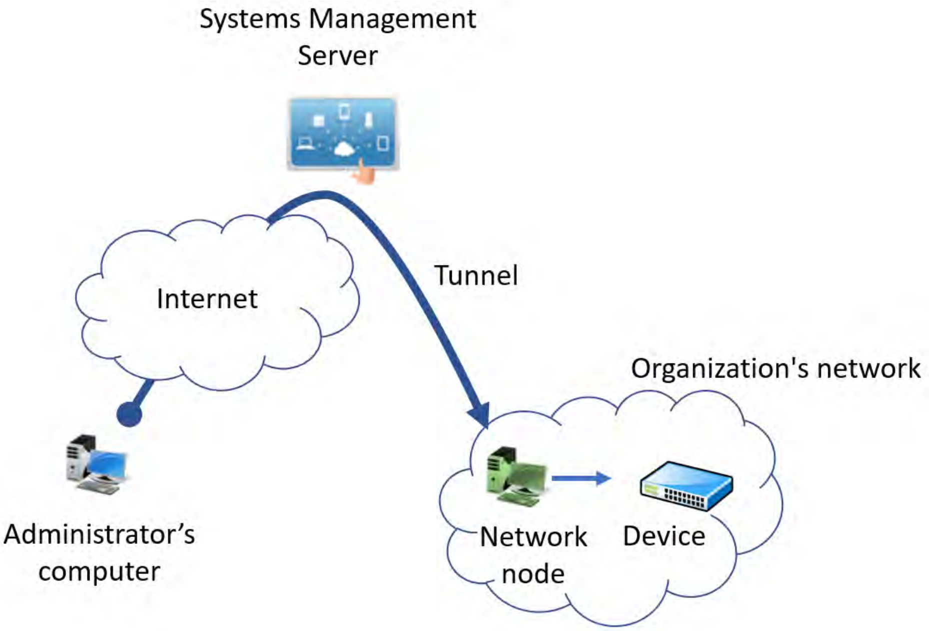


Figure 18.4: connection established between the administrator's computer and the Network Node through the tunnel

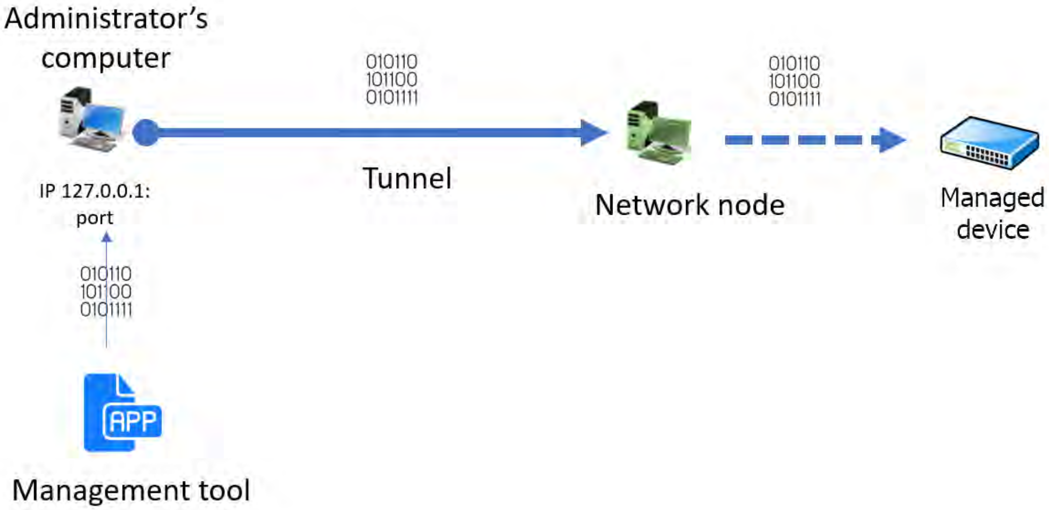


Figure 18.5: access from the management tool to the managed device

## Follow the steps below to access a network device via HTTPS:

- The device to manage must incorporate a web server that receives the request and displays a web management interface.
- From the PCSM agent, select the device to manage.
- Click the icon and select the **Connect (HTTPS)** option.
- Select the **Open browser automatically** checkbox. The administrator's computer must have an Internet browser installed.

- The URL field will be automatically populated with the IP address of the device to access. If the device's web server cannot listen on the default port for HTTP connections (80), enter a new port separated by a colon (:).
- In the **VIA** section, select the Network Node that will act as an intermediary between the administrator's computer and the device to manage.
- Click the **Start** button.

## Follow the steps below to access a network device using SSH

- The device to manage must incorporate a remote command-line server compatible with the Telnet or SSH protocol. This server will collect the requests and display the appropriate results.
- From the PCSM agent, select the device to manage.
- Click the icon and select the **Connect (Telnet/SSH)** option.
- Select the **Open PuTTY automatically** checkbox. The PuTTY program must be installed on the administrator's computer.
- The URL field will be automatically populated with the IP address of the device to access and the port. If the device's Telnet/SSH server cannot listen on the default Telnet port (21)/SSH port (22), enter the new port in the text box.
- In the **VIA** section, select the Network Node that will act as an intermediary between the administrator's computer and the device to manage.
- Click the **Start** button.

## Follow the steps below to access a network device via a third-party application

- From the PCSM agent, select the device to manage.
- Click the icon and select the **Connect (Custom Tunnel)** option.
- To run the management tool automatically once the tunnel has been set, select the **After connected, run the following program** checkbox. The third-party program must be installed on the computer to manage.
- In the URL field, enter the IP address of the device to connect to and the management service port. The device to access must incorporate a server compatible with the management tool chosen by the IT technician and capable of understanding requests, processing them and returning a result.
- In the **VIA** section, select the Network Node that will act as an intermediary between the administrator's computer and the device to manage.

- Click the **Start** button.

*The tunnel between the administrator's computer and the Network Node is established on a single local port. Therefore, the management tool must communicate with the management service through a single port. Services using protocols that establish multiple communication channels simultaneously won't work.*

# Remote mobile device management

This section describes the tools included in Panda Systems Management to manage mobile devices from the console, how they work, and the benefits they provide.

## Accessing the remote mobile device management tools

The mobile device management features included in the console are only available at Device level for the device to manage:

- Go to general menu **Sites**, select the site the mobile device belongs to, and click the device to manage.
- Click **Summary** from the tab menu. The Actions context menu adapts automatically to the type of device, showing the management tools compatible with mobile devices.

## Device Wipe

Click the ⚠ icon to perform a remote factory reset of the device. This feature prevents data theft in the event of device loss, theft, or malfunction.

*Please note that any user data, programs, specific settings, or modifications stored on the device will be irreversibly erased. The device is returned to its factory settings.*

## Geolocation

Click the 📍 icon to view the device's location on a map. The device's coordinates are obtained in different ways depending on the available resources on the device. Accuracy varies greatly from one system to another. The technologies used are (in order of accuracy):

- GPS (Global Positioning System)
- WPS (Wi-Fi Positioning System)

- GeoIP

> *GeoIP may report a location completely different from where the device actually is.*

## Device Lock

Click the 🔒 icon to turn off the device's screen and lock it. This feature turns the device's screen off until a security PIN (if there is one) is entered. This is particularly useful if the device is stolen.

## Device Unlock

Click the 🔓 icon to unlock the device and delete the security PIN should the user forget it.

## Passcode Policy

Click the 🔑 icon to force the user to create a security PIN on the device. Once set, the administrator will be able to lock the device if stolen, prompting the thief for that PIN when the device is powered on.

> *This feature sends a remote request to the user to set the PIN, it doesn't allow the administrator to set it from the console.*

# Part 6

# Panda Systems Management service security

# Chapter 19

# User accounts and security levels

A user account is a resource consisting of information regulating access to the PCSM Console, and the actions that technicians can take on users' devices.

User accounts are only used by the IT administrators who access the PCSM console or other services provided by Panda Systems Management. In general, each IT administrator has a single user account.

Device users do not need any kind of user account as they don't access the PCSM Console. The Agent installed on their devices is configured by default to work in Monitor mode so that it doesn't require any intervention by the end user

⚠ *Unlike the rest of the manual where the "user" is the person who uses the device managed by an administrator with the help of Panda Systems Management, in this chapter, "user" can refer to a user account or Console access account.*

CHAPTER CONTENT

# Main user

The main user is the user account provided by Panda Security to the customer at the time of provisioning the Panda Systems Management service. This account is assigned the **administrator** security level (explained later in this chapter).

For security reasons, it is not possible to change the main user's password or configuration, or access the service by logging in from a PCSM Agent; Nevertheless, the main user account can be used to access the Agent installed on the administrator's computer from the PCSM Console.

# Security levels

A security level is a specific permission configuration for accessing the Console, which is applied to one or more user accounts. This authorizes a specific administrator to view or modify certain Console resources, depending on the security level to which the user account used to access Panda Systems Management belongs.

One or more user accounts can belong to one or more security levels.

*Security levels only affect the access level of IT administrators to the Console resources to manage network devices. They do affect other device users.*

## Security levels: Purpose

In a small IT Department, all technicians access the Console as administrators with no restrictions. However, in a medium or large IT Department or in partners with many customers, access to devices could need to be segmented according to three criteria:

- **The number of devices to manage.**

In medium/large networks or networks belonging to offices of the same company or to different customers of the same partner, it could be necessary to deploy and assign devices to technicians. By doing this, the devices of an office managed by a certain technician will not be visible to the technicians who manage the devices of other offices.

There could also be restricted access to the sensitive data of specific customers, which requires precise control of the technicians who can handle the devices that contain it.

- **The purpose of the device to manage.**

Depending on the function of a device, an expert technician in this field can be assigned. For example, a group of specialized technicians could be assigned to the database server of one or all of the customers managed by the partner and, in the same way, other services like mail servers might not be visible to this group.

- **Technical knowledge.**

Depending on the knowledge of the technicians or their security level in the IT Department, they might only need monitoring/validation (read-only) access to the Console, or more advanced access, such as modification of device settings.

The three criteria can overlap, creating a very powerful configuration matrix that is flexible and easy to define and maintain, which allows you to perfectly restrict the Console features accessible to each technician according to their profile and responsibilities.

## The administrator security level

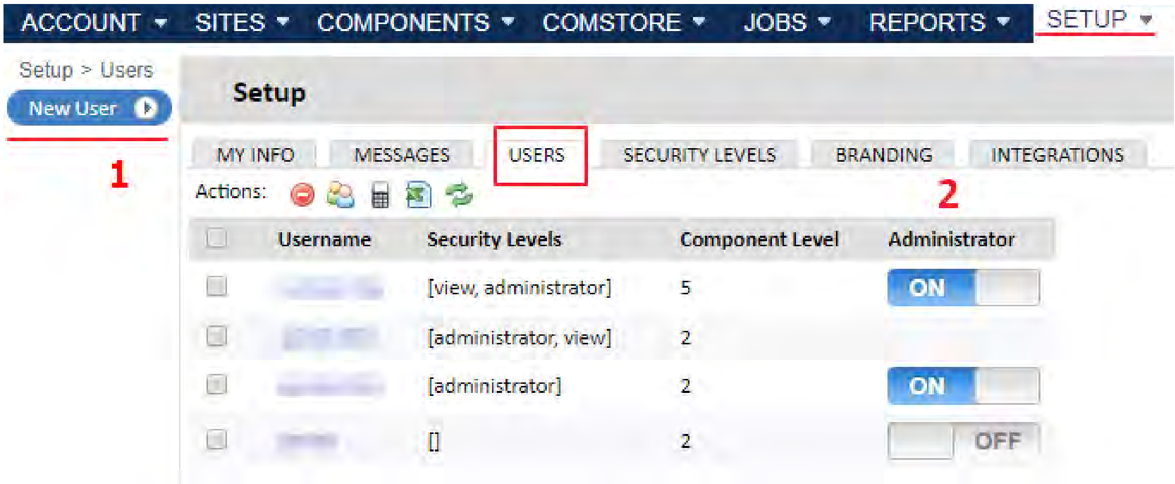
A Panda Systems Management user license comes with a default total control security level, called administrator. The default administration account belongs to this security level and it allows absolutely every action available on the Console to be performed. **Administrator** is also the only security level that can create new security levels and users and modify existing security levels.

The administrator security level cannot be deleted from the Server, and any user account can belong to this security level after it has been assigned through the Console.

> *All of the procedures described in this chapter require an account that belongs to the administrator security level.*

# Creating, configuring and deleting user accounts

## Adding a user account



| □ | Username | Security Levels | Component Level | Administrator |
|---|---|---|---|---|
| □ | [redacted] | [view, administrator] | 5 | ON |
| □ | [redacted] | [administrator, view] | 2 | |
| □ | [redacted] | [administrator] | 2 | ON |
| □ | [redacted] | [] | 2 | OFF |

Figure 19.1: access to the user management window

Follow the steps below to add a user account:

- Go to general menu **Setup**, and click **Users** from the tab bar.
- Click the **New User (1)** button from the side panel.
  - Enter the username, password, email address and full name (first name and last name) of the technician who will use the account.
  - Specify when you want the user account to expire.
  - Set the **Component Level** of the account (1 to 5). This will prevent access to those components imported from the ComStore whose **Component Level** is higher than the level configured for the account. Refer to section "**Loading the component monitor into the Panda Systems Management platform**" on page **141**.
  - Select the security roles you want to assign to the account as well as the default security role.

## Editing a user account

- Click the name of the account to edit. A window will open with the editable fields in the user account.
- Click **Save**.

## Deleting a user account

- Hover the mouse pointer over the user account to delete. The ✗ icon will be displayed at the end of the row. Click the icon. A confirmation window will be displayed.
- In the confirmation window, select the **Assign data to user** checkbox to copy the user settings before deleting the user. The following items will be copied:

- Scheduled jobs
- Scheduled reports
- Filters
- Tickets

- Select the **I understand that this action is irreversible** checkbox and click the **Permanently Delete User** button to finish deleting the user account.

> *When deleting a user, administrators have the option to assign the user settings to another user.*

## Inactivating a user account

- Use the checkboxes to select the user accounts to inactivate.
- Click the ⊖ icon from the icon bar.

## Exporting the user list

- Select the checkboxes next to the user accounts to export.
- Click the 📊 icon from the icon bar.

## Assigning and unassigning the administrator security level from a user account

Click the **ON/OFF (2)** button to assign and unassign the administrator security level from a user account.

## Changing the effective security level of a user account

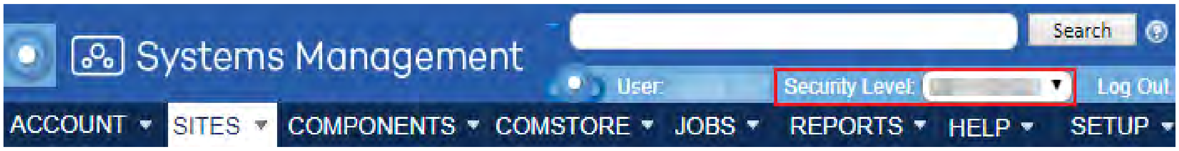


Figure 19.2: Security level change with a session already started

A user account can belong to one security level or more. In the latter case, the console will display a drop-down list through which you can choose the security level with which the user account will operate. That is, there is no need to log out of the console and then log in again to change the security level.

# Creating, configuring and deleting security levels

## Adding a security level

Follow the steps below to add a security level:

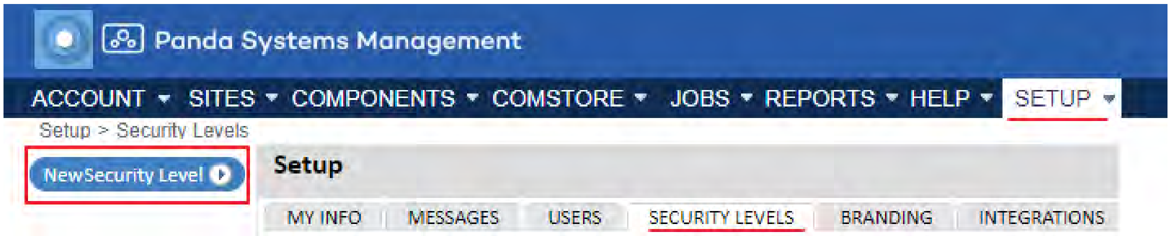


Figure 19.3: Security level management window

- Go to general menu **Setup** and click **Security Levels** from the tab bar. Then, click **New Security Level** from the left side panel.
- Enter a name, a description and an existing security level if you would like to use it as a template.
- Click **Save**. A window will open for you to configure the security level details. Refer to section "**Configuring security levels**" on page **280** for more information about the permissions assigned to a security level.

## Deleting a security level

Click the ✖ icon to he right of the security level to delete.

> *If user accounts are assigned to a security level that you want to delete, you will be prompted to assign a new security level to those accounts.*

## Configuring security levels

The configuration of a security level is divided into four sections:

- **Device visibility**: Enables or restricts access to device groups.
- **Permissions**: Enables or restricts access to the Console features.
- **Agent Browser Tools**: Enables or restricts access to the Agent features.
- **Membership**: Specifies the user accounts that belong to the security level configured.

### Device visibility

This setup group lets you specify the network devices that will be visible to the Console users who belong to a certain security level.

Panda Systems Management´s security levels allow you to specify and limit the access users have to the four types of static groupings available in the Console:

- Sites
- Site device group
- Device group
- Site group

More specifically, the security levels allow you to define access to the individual items contained in each type of device grouping. To allow access to all items contained in a grouping, select **ON** next to it. A settings window will be displayed.

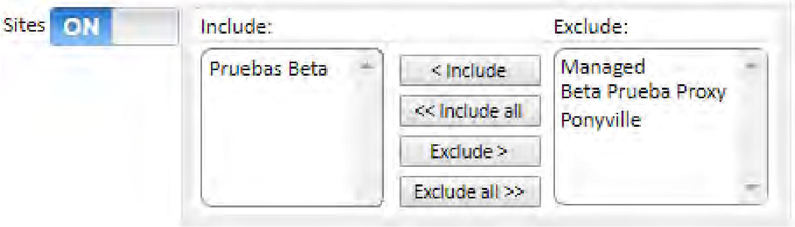


Figure 19.4: configuring the items accessible to a security level

A group listed in the **Include** textbox will be visible to all of the user accounts that belong to this security level. Similarly, if the group is listed in the **Exclude** textbox, this device group will not be visible in the Console.

## Filter visibility

Panda Systems Managements lets you create filters to view different types of devices. However, access to those filters is not configured via the **Security Levels** tab, but is configured when creating or editing the relevant filter. Follow the steps below to modify access to a filter:

- Go to general menu **Sites** to access the account filters, or click a specific site to access the site filters.
- Create a new filter or edit an existing one. For more information, refer to "**Filters**" on page **75**.
- In the settings window, select the **Share this filter with users with the following security level(s)** checkbox and use the **Include** and **Exclude** buttons to allow or prevent security levels from accessing the filter.

## Permissions

The **Permissions** section lets you set the access level to each resource in the console. For that, it first shows the list of areas available in the console, which coincide with the entries in the general menu.

To set the access level of the security level to each area in the console (tabs in the general menu), move the switch to the ON position. This will display the resources associated with each area (tab menu. For example, move the switch to the **ON** position in **Account** to display the area's resources and to specify the access level to each one of them.

The access levels are:

- **None**: The resource is not displayed in the console.
- **View**: The resource is displayed in the console, but it is not possible to configure or modify any of its parameters.
- **Manage**: The resource is displayed in the console, and can be accessed with full permissions.

### Agent Browser Tools

This setup group allows you to specify access to the remote administration tools available in the Agent.

*Any change made in Agent Browser Tools requires the Agent to be restarted.*

*These restrictions apply to the Agent's local Console, on logging on to manage remote devices (Administrator Mode).*

### Membership

Allows you to configure the user accounts that belong to the security level configured.

## Strategies for generating security levels

You can generate as many security levels as necessary, bearing in mind that the objective of a security level is to restrict administrator access to the devices or Console resources in order to provide higher security and protection against human error. However, this higher security comes with lower flexibility when reusing technical staff among various customers or tasks, so that the exact number of security levels on a system will be the result of the weighting of two variables: flexibility vs. security.

### Horizontal security levels

In general, a company with several offices and an independent IT team in each one will want a total control security level limited to the devices in each office.

In this way, the devices managed by office A will not be visible to office B and vice versa.

In a company with several offices, the following configuration will be needed in each office:

- A site or device group that groups the office's devices.
- A security level that allows access to the devices in the site and denies access to the rest.
- An account for each technician, assigned to the security level that covers the designated office.

The same schema can be used by a partner who wants to segregate customers and assign specific technicians to them.

### Vertical security levels

For devices largely aimed at specific tasks, such as print, database, mail servers, etc., you can create security levels that restrict access to this type of device.

This will allow a company or partner with many offices or customers with mail servers to group them and assign a group of technicians to manage them, whist the rest of the technicians with a more general profile manage user devices.

The following general configuration will be required:

- A Device group that groups all mail servers, regardless of the site/customer/office to which they belong.
- A security level A that allows access to the devices in the Device group and denies access to the rest of the devices.
- A security level B that denies access to the devices in the Device group and allows access to the rest of the devices.
- A security level A user account for every technician performing maintenance on the company or partner's mail servers.
- A security level B user account for every technician performing maintenance on the company or partner's user devices.

## Resource access security levels

In accordance with each technician's profile or level of experience, the IT Department manager can share the work among the members of the department. This allows you to create groups of technicians with complementary responsibilities:

- **Monitoring and report generation technicians:** With full access to the **Reports** tab and read-only access to the rest of the Console.
- Script development and software deployment technicians: With access to general menus **Components** and **ComStore**.
- **Support technicians**: With access to the **Support** tab and to the resources on the user's device through the Agent.

You can also restrict access to certain components in the **ComStore** or developed by the IT Department that perform sensitive operations on the user's devices, assigning higher Component levels than those set in the user account.

Chapter 20

# Service security and access control

Administrators have several tools to improve the security of access to the Panda Systems Management service, including:

- Two-factor authentication.
- Password policies.
- IP address restrictions to grant or deny access to the Console.
- IP address restrictions to grant or deny access from the Agent to the Server.

CHAPTER CONTENT

## Two-Factor Authentication (2FA)

Two-Factor Authentication (2FA) makes it necessary to use a second device to verify the administrator credentials entered in the console login screen. So, in addition to entering the credentials, the administrator must also enter a personal code generated automatically every minute on their phone.

*Two-Factor Authentication only affects access to the Console and is therefore aimed only at network administrators. Neither network administrators nor users that access other devices through the Agent are affected by these settings.*

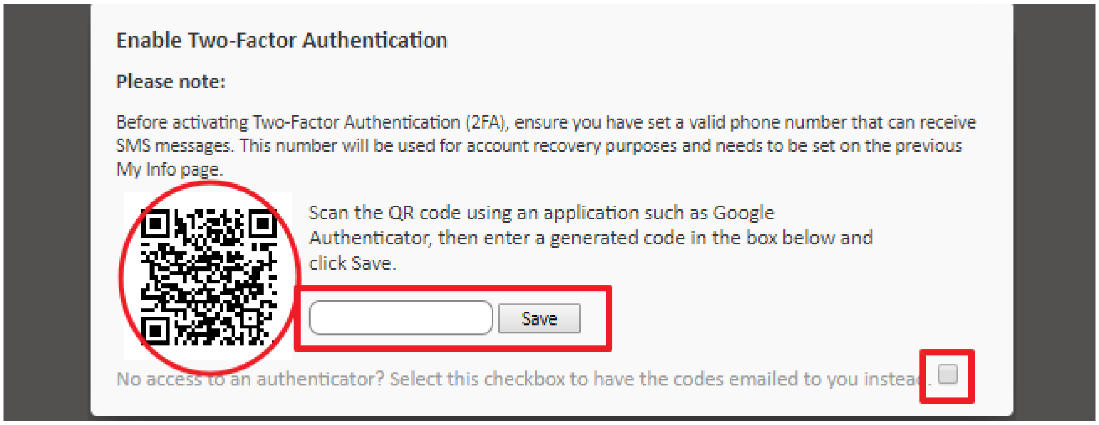
## Essential requirements

- A mobile device that supports the token generating application.
- The free app `Google Authenticator` or other compatible app installed on the mobile device.

## Settings

Below we describe the steps necessary to enable Two-Factor Authentication in the account of the administrator that has logged in to the Console:

- Go to general menu **Setup**, **My Info** tab. Scroll down to the **Security settings** section and click **Enable Two-Factor Authentication**.



Enable Two-Factor Authentication

Please note:

Before activating Two-Factor Authentication (2FA), ensure you have set a valid phone number that can receive SMS messages. This number will be used for account recovery purposes and needs to be set on the previous My Info page.

Scan the QR code using an application such as Google Authenticator, then enter a generated code in the box below and click Save.

No access to an authenticator? Select this checkbox to have the codes emailed to you instead. □

Figure 20.1: token generation and mailing

- You will see a QR Code on the screen and a space to enter the token. This token is generated by `Google Authenticator`. If you don't have an authentication application that can read a QR Code, you can select the checkbox that allows the system to send a QR Code to the administrator's email address specified on the same page.
- Install `Google Authenticator` from Google Play on the mobile device of the administrator accessing the Console (see "**Installing Google Authenticator**" en la página **286**).
- Tap **Begin setup** and **Scan barcode** to scan the code displayed in the Console. If there is no barcode scanner installed, the app will suggest installing the free program `ZXing Barcode Scanner`.
- After scanning the QR code, the application starts generating tokens every 30 seconds. You have to generate a token and enter it in the corresponding space in the Console login screen to fully enable Two-Factor Authentication.
- From then on, the administrator will only be able to access their account if they enter the credentials correctly along with a valid token.

## Installing Google Authenticator

To install `Google Authenticator` on an Android-compatible mobile device, follow the steps below:

- Download the app from Google Play.

- Once the app has started, tap **Begin Setup**.
- Tap **Scan a barcode** to scan the QR code displayed in the Console.
- The app will start to generate tokens automatically. Each token is valid for 30 seconds.

### Enabling Two-Factor Authentication for all accounts

Once Two-Factor Authentication is enabled for the administrator account, it is possible to force it to be used for the other administrator accounts created in the console. To do this, click general menu **Setup**, **Account Settings**, **Require Two-Factor Authentication**.

*To force use of Two-Factor Authentication for the other accounts, the account used for configuration must already have Two-Factor Authentication enabled.*

Whenever a user without Two-Factor Authentication configured accesses the console, they will see a warning message and they won't be able to use the console.

### Disabling Two-Factor Authentication from the login screen

It is possible to disable Two-Factor Authentication from the login screen. To do this, you have to enter the user name and password correctly, and you will see the screen asking for the token. At the bottom there's a link to **Disable TOTP**. Click the link and the Server will send an SMS with a code that is valid for 10 minutes to the phone number configured in the system. Enter the code to disable the Two-Factor Authentication service.

## Password policy

In order to reinforce security regarding access to the Console, administrators can establish a password policy which means that all passwords will have to meet certain requirements.

To configure the password policy, go to **General menu**, **Accounts**, **Settings** and enter the relevant values in the following fields:

- **Password expiration**: Sets the maximum duration of the password (30, 60, 90 days or never expires).
- **Unique passwords**: The system stores a list of passwords for each account so administrators cannot reuse them when a password is changed. The password history will have a value of 0 (never) to 6 entries.

### Resetting 2FA

You can reset 2FA for a user if they lose their mobile device. To do that, follow the steps below:

- Go to general menu **Setup** and click **Users** from the tab bar.

- There, you will find the 📱 icon, from which you can reset a user's 2FA status.
- Select the checkboxes next to the users you want to reset 2FA for and click the aforementioned icon.
- Observe the message stating that 2FA has been disabled (reset) for the users. To re-enable it, follow the steps in section "**Enabling Two-Factor Authentication for all accounts**".

# IP address restrictions for accessing the Console

To restrict access to the Console to a set of known IP addresses, go to general menu **Account**, **Setup**, and enable the option **PSM Console IP Address Restriction**. Then, in **Restricted IP List**, set the list of IPs from which it will be possible to access the Console.

# IP address restrictions for accessing the Server from Agents

To restrict access from the Agents to the service, go to general menu Account, Setup and  enable the option Agent IP Address Restriction. Then, in Restricted IP List, set the list of IPs from which Agents can access the Server.

Chapter 21

# Activity log

Panda Systems Management keeps a log of the actions taken by service administrators. This log records the changes carried out on users' devices, who made the changes and when.

The activity log is divided into three sections in the console, depending on the level of detail required.

CHAPTER CONTENT

## Account level activity log

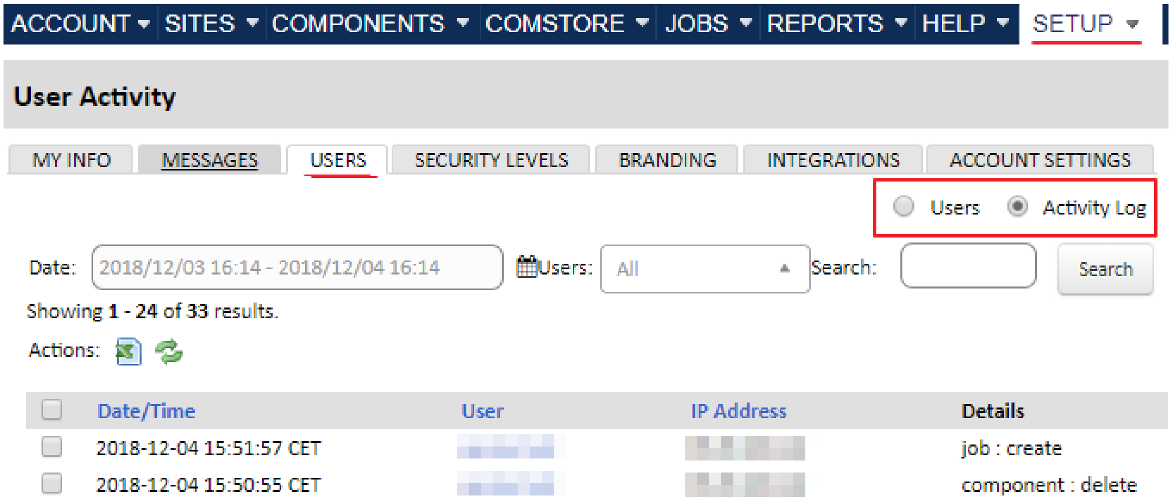
This is accessed through the general **Account** menu by clicking the **Reports** tab and then **Activity log**.

The activity log at Account level only displays the movement of devices between sites, specifying the date and time of the movement.

## General activity log

The general activity log lets you see the most important actions taken by network administrators on the administration console.

The user's general activity log can be accessed from the general **Setup** menu by clicking **Users** and selecting **Activity log**.



○ Users ● Activity Log

Date: 2018/12/03 16:14 - 2018/12/04 16:14 Users: All Search:

Showing **1 - 24** of **33** results.

| □ | Date/Time | User | IP Address | Details |
|---|---|---|---|---|
| □ | 2018-12-04 15:51:57 CET | [redacted] | [redacted] | job : create |
| □ | 2018-12-04 15:50:55 CET | [redacted] | [redacted] | component : delete |

Figure 21.1: list of actions taken by the administrator

## List of activities

This consists of a table -list of activities-, with the following information for each action:

- **Checkbox**: This lets you select activities from the list to take actions such as export to Excel.
- **Date/time**: Date, time and time zone of the action.
- **User**: Panda Systems Management user used by the administrator to carry out the action.
- **IP Address**: IP address from which the administrator connected to the console.
- **Details**: Shows the Panda Systems Management entity on which the action was taken and the type of action taken.
- **Parameters**: Shows the fields and values that the action applied to the unit.

## Activity filter and searches

The following tools are designed to help you search for activities:

### Date

This offers several options for selecting a time period:

- **Quick**: Select one of the default periods: Last 24 hours, Last 2 days, Last 2 weeks, Last month, Last two months, Last 6 months.
- **Custom Range**: Lets you determine the start and end of the time period.

### Users

This offers a drop-down menu from which you can choose the user. When you select a user, you will only see the activity for this user.

### Search

A text box that lets you filter by the content of some specific fields.

# Device level activity log

The activity log at device level lets you view the actions taken on a specific device regardless of the user or administrator responsible for the action.

There are two ways of accessing this log:

- Go to general menu **Sites**, click the site where the device is located, and then click the device whose activity log you want to view.
- Click **Audit** from the tab menu and then click the **Activity Log** selection control.

In both cases a list of actions is displayed, an entry for each activity, with the following information:

- **Type**: This uses an icon to show the type of activity on the device.
  - Remote desktop via RDP.
  - Remote screenshot.
  - Launch job.
  - Command Shell.
  - Remote desktop via VNC.
  - File transfer.
- **Name**: Name of the activity.
- **Started**: When the activity started.
- **Ended**: When the activity ended.
- **Policy**: Shows the name of the policy that triggered the action, if applicable.
- **Status**: Activity status.
- **Results**: Displays the result of the administrator's action by clicking the icon.
- **Progress**: If the activity is a task, a progress bar is included to show the status.
- **Stdout**: If the configured task displays data in the standard output as the result of its execution, this is displayed by clicking the icon.
- **Stderr**: If the configured task displays data in the standard output as the result of its execution, this is displayed by clicking the icon.

# Part 7

# Appendix

**Chapter 22:** Supported platforms and requirements

**Chapter 23:** Source code

Chapter 22

# Supported platforms and requirements

This chapter details the platforms supported by Panda Systems Management and the requirements that the devices on which you want to install and run the PCSM agent must meet for it to work properly. Nevertheless, for those devices that do not meet the specified requirements, please note that Panda Systems Management is compatible with any type of device through the SNMP protocol. For more information, refer to section "**Integrating network devices**" on page **55**.

CHAPTER CONTENT

## Supported platforms

For more detailed, up-to-date information, refer to the following link **https://www.pandasecurity.com/en/support/card?id=300102**

### Windows

- Windows Vista Enterprise (32-bit).
- Windows 7.
- Windows 8/8.1 with KB2999226 installed.
- Windows 10.

- Windows 2008 (does not support installation of .NET Core and cannot be used for SNMP monitoring).
- Windows 2008 SP1 (does not support Patch Management).
- Windows 2008 R2.
- Windows Server 2012 (64-bit) and Windows Server 2012 R2 (64-bit) with KB2999226 installed.
- Windows Server 2016 and Windows Core.
- Windows Server 2019.
- Windows Server Core 2008 R2, 2012 R2, and 2016.

## Apple Macintosh

Latest two versions of macOS.

## Linux

- **Fedora (64-bit)**: latest two versions.
- **CentOS (64-bit)**: latest two versions from version 7 with libicu package.
- **Debian (64-bit)**: latest two LTS versions with libicu-dev, libssl-dev, and libcurl4 packages.
- **Ubuntu (64-bit)**: current LTS version with libicu-dev and libssl-dev packages.

Red Hat Enterprise Linux (64-bit): version 7 and later using EPEL.

## For smartphones and tablets

⚠ *After September 1, 2021, the features associated with smartphones and tablets will reach EOM (End Of Maintenance), and Panda Security will stop supporting these devices. After March 1, 2021, new Panda Systems Management customers will not be able to enable the MDM module from the ComStore. Additionally, long-time customers who already have this module enabled will not be able to add new mobile devices to their IT network. After March 31, 2021, some features that require Push technology (Wipe, Remote Lock, etc.) will no longer work on iOS devices.*

- iOS 7 and later
- Android 2.3.3 and later

## Supported browsers

The web console is tested against the latest two versions of the following web browsers:

- **Google Chrome**: Google Chrome uses the Chromium engine. While we only test Chromium functionality using Google Chrome, other browsers using the same engine should behave similarly. Such browsers include:
  - Microsoft Edge

- Vivaldi
- Brave

- Mozilla Firefox
- Safari

# Detailed Windows requirements

The Panda Systems Management Agent requires the installation of certain components in order to be deployed to Windows devices. Should they not be installed, the setup process will download and install all necessary dependencies silently in the background. Should it be necessary to download the .NET Framework, the installation process may take a considerable amount of time depending on Internet bandwidth and device specification. In such case, since the PCSM agent installs silently on the background, no visual feedback will be present during this time.

> *The process to automatically download and install the necessary dependencies only takes place when installing new Agents for the first time. It doesn't take place in update processes. A device with a PCSM Agent version installed that does not meet the necessary requirements won't be updated.*

The necessary dependencies are:

- **.NET Full Framework version 4.0** (prerequisite for .NET Framework 4.0.3 (**https://www.microsoft.com/en-us/download/details.aspx?id=17718**)
- **.NET Full Framework version 4.0.3** (**https://www.microsoft.com/en-us/download/details.aspx?id=29053**)

> *The full version is required, not the Client Profile version of .NET Framework 4.0.3.*
>
> *Windows 8 (and later) and Windows Server 2012 (and later) operating systems automatically meet these requirements.*

- **Windows Imaging Component** (**https://www.microsoft.com/en-us/download/details.aspx?id=32**)

# Linux requirements

For the PCSM agent to work on Linux computers, the Mono libraries must be installed on the device. Panda Systems Management supports Mono versions 3 and later. Additionally, some platforms require that a series of requirements be met before installing the PCSM agent:

- Compatibility with .NET Core: while some ARM distributions are supported for the 32-bit architecture, generally a 64-bit version of Linux is required. Refer to this compatibility list: **ttps://github.com/dotnet/core/blob/master/release-notes/3.0/3.0-supported-os.md**.

- **Fedora and Debian:** require `yum-utils` to be manually installed prior to the agent.
- **Red Hat Enterprise Linux**: Mono can be installed from `EPEL`.

# VMware ESXi management requirements

VMware servers are managed via Windows devices with the Network Node role. It is not necessary that the Network Node device resides on the same subnet as the ESXi server.

## Network Node requirements for ESXi server monitoring

- The Network Node device must run on a Windows operating system.
- It must have Microsoft .NET Framework version 4.7 or higher.
- It must not be hosted on an ESXi server targeted for monitoring.

## VMWare ESXi requirements

Panda Systems Management supports ESXi versions 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, and 7.0.

In the case of VMware ESXi 6.5 and later versions, you need to establish an SSH connection in order to enable CIM access.

- Enable the SSH service on the ESXi server.
- Make an SSH connection to the ESXi server. Use PuTTY or a compatible program.
- Run the following commands:

```
esxcli system wbem set --enable true
```

```
/etc/init.d/sfcbd-watchdog start
```

# Chapter 23

# Source code

This section provides the Visual Basic Script source code for the components discussed in chapters "**Components and ComStore**" and "**Centralized software deployment and installation**".

## Quarantine monitor

```
Option Explicit
'***********************************************************************
'Quarantine_Monitor v1.0
'v.1.0: 4/12/2018
'v.099b: 06/03/2013
'By Oscar Lopez / Panda Security
'Target: this script monitors changes to EP quarantine folder
'Input:EP_PATH environment variable
'Output: stdout "Result=n new items detected in EP quarantine",
'***********************************************************************

dim WshShell,WshSysEnv
dim objFSO,objFolder,colFiles
dim iCountPast,iCountNow,iCount

Set WshShell=CreateObject("WScript.Shell")
Set objFSO=CreateObject("Scripting.FileSystemObject")

'access to environment variable and quarantine path
On error resume Next
    Set WshSysEnv=WshShell.Environment("PROCESS")
    Set objFolder=objFSO.GetFolder(WshSysEnv("EP_PATH"))

    if err.number<>0 then
        'PCSM didn't send the environment variable
        err.clear
        WScript.Echo"<-StartResult->"
        WScript.Echo"Result=PCOP_PATH variable not defined in PCSM console or path
not found"
        WScript.Echo"<-EndResult->"
        Set WshShell=nothing
        Set WshSysEnv=nothing
        Set objFolder=nothing
        WScript.Quit(1)
    end if
On error goto 0

'get the collection that contains the folder files
set colFiles=objFolder.files

'access to the registry for saving the count
On error resume Next
    'get previous file count
    iCountPast= cint(WshShell.RegRead("HKLM\Software\Panda Security\Monitor"))
    if Err.Number<>0 then
        'if error set to 0
        iCountPast=0
    end if
    iCountNow=colFiles.count
    'save the count
    WshShell.RegWrite "HKLM\Software\Panda Security\Monitor", iCountNow, "REG_SZ"

    Err.Clear
    Set colFiles = nothing
    set objFolder = nothing
    set WshShell = nothing
    set WshSysEnv = nothing
    set objFSO = nothing

    if iCountPast < iCountNow then
        iCount=iCountNow-iCountPast
    else
        iCount=0
    end if
    WScript.Echo "<-Start Result->"
    WScript.Echo "Result=" & iCount & " new items in EP quarantine"
    WScript.Echo "<-End Result->"
    WScript.Quit (0)

On error goto 0

WScript.Quit (0)
```

# File deployment

```
Option Explicit
'**********************************************************************
'Deploy_documents v1.0
'v.099b: 12/03/2013
'v.1.0: 4/12/2018
'By Oscar Lopez / Panda Security
'Target: It creates a folder in the user's desktop and saves to it the
'documents to deploy
'Input:
'-Files to copy
'-PCSM_PATH: script var with the folder on user's desktop where files will be
copied
'-USERDESKTOP: global var with the path to the user's.
'Output: code 0: OK
'Output: code 1: NOT OK. "Deploy unsuccessful"
'**********************************************************************

Dim CONST_PATH
Dim objFSO,objFolder,colFiles
dim WshShell,WshSysEnv

Set WshShell=WScript.CreateObject("WScript.Shell")

On Error Resume Next
    Set objFSO=CreateObject("Scripting.FileSystemObject")
    Set WshSysEnv=WshShell.Environment("PROCESS")
    Set objFolder=objFSO.GetFolder(WshSysEnv("PCSM_PATH"))

    If Err.Number=0 Then
```

```
        WScript.Echo "Deploy unsuccessful: The folder already exists"
        WScript.Quit (1)
    End If
    Err.Clear

    'The folder will be created on the user's desktop
     Set objFolder = objFSO.CreateFolder(WshSysEnv("USERDESKTOP") &
WshSysEnv("PCSM_PATH"))
    'the documents will be moved to the folder
    objFSO.MoveFile "doc1.docx", objFolder.Path & "\doc1.docx"
    If Err.Number<>0 Then
        WScript.Echo "Deploy unsuccessful: " & Err.Description
        WScript.Quit (1)
    Else
        WScript.Echo "Deploy OK: All files were copied"
        WScript.Quit (0)
    End If
On Error Goto 0
WScript.Quit (0)
```