



Panda Systems Management

Guide for network Administrators

1

Version: 5.1.0

Author: Panda Security

Date: 6/02/2018

Contents

1. PREFACE	11
1.1. Introduction	12
1.2. Target audience	12
1.3. Icons	12
2. INTRODUCTION	13
2.1. Introduction	14
2.2. Main features of Panda Systems Management	14
2.3. Panda Systems Management user profile	16
2.4. Main components of Panda Systems Management	16
2.5. Key players of Panda Systems Management	17
3. HIERARCHY OF LEVELS WITHIN THE MANAGEMENT CONSOLE.....	20
3.1. Hierarchy of levels within the Management Console	21
3.2. Account Level	21
3.3. Site Level	23
3.4. Device Level	26
4. BASIC COMPONENTS OF THE CONSOLE	27
4.1. Introduction	28
4.2. General menu	28
4.3. Tab bar / List bar	29
4.3.1 Components	29
4.4. Icon bar / Action bar	30
4.4.1 Components	30
4.5. Filters and groups panel	32
4.6. Dashboards	32
4.6.1 Security Status	33
4.6.2 Account Dashboard	33
4.6.3 Summary (Site)	33
4.6.4 Summary (Device)	34
5. DEPLOYING AND MANAGING DEVICES	35
5.1. Introduction	36
5.2. Prerequisite steps prior to adding devices to Panda Systems Management	36

5.3. Sending the Agent via email	37
5.4. Direct download of the PCSM Agent	38
5.5. Remote installation	39
5.5.1 Designate the installed Agent as a Network Node (with network scanning)	39
5.5.2 Run a computer discovery task from the console	39
5.5.3 Install the Agents remotely from the console	40
5.5.4 Run a computer discovery task from the installed Agent (alternative method)	41
5.6. Installing the Agent on Android and iOS	41
5.7. Administration of devices not supported by the Agent	45
5.7.1 Adding Network Devices	46
5.7.2 Assigning a Network Node computer to a device	46
5.8. Managing ESXi servers	47
5.8.1 Adding ESXi servers individually	47
5.8.2 Adding multiple ESXi servers at the same time	48
5.8.3 Assigning a Network Node computer to an ESXi server	48
5.9. Managing Hyper-V servers	49
5.10. Approving devices	49
5.11. Configuring a Connection Broker	50
5.11.1 Assigning the Connection Broker role to a device	50
5.11.2 Disabling the use of Connection Brokers	51
5.12. Other Agent Connection parameters	51
5.13. Configuring a Network Node	52
5.13.1 Requirements for configuring a Network Node	53
5.13.2 Designating a Network Node	53
5.13.3 Types of Network Nodes	53
5.14. Managing devices	53
5.14.1 Devices compatible with the PCSM Agent	54
5.14.2 Devices not compatible with the PCSM Agent	55
5.15. Viewing device information	58
5.16. Managing device resource consumption	63
5.16.1 Specifying the type of device	63
5.16.2 Specifying the power rating for each type of device	63
5.16.3 General power rating view	64
6. FILTERS AND GROUPS	65
6.1. What are groups and filters?	66
6.2. Types of groups and filters	66

6.3. Groups.....	66
6.4. Filters.....	66
6.4.1 Predefined filters	66
6.4.2 Filter composition.....	71
7. MANAGING DEVICES EFFICIENTLY	76
7.1. Introduction	77
7.2. Differences between sites, groups and filters.....	77
7.2.1 Sites.....	77
7.2.2 Filters and groups.....	77
7.3. General approach and device management structure	78
7.4. Quick view of device information.....	79
8. THE FIRST 8 STEPS TO START USING PANDA SYSTEMS MANAGEMENT	81
8.1. Introduction	82
8.1.1 Current startup status of Panda Systems Management.....	82
8.2. Creating and configuring the first site.....	82
8.3. Deploying the Systems Management Agent	83
8.4. Checking the site's device list and basic filtering	83
8.5. Hardware, software and license audit.....	84
8.6. Patch management.....	84
8.7. Creating monitors	84
8.8. ComStore	86
8.9. Accessing resources on the remote managed devices	87
9. POLICIES	89
9.1. What are policies?	90
9.2. Creating policies.....	90
9.3. Managing policies.....	91
9.3.1 Managing policies at Account Level.....	91
9.3.2 Viewing the devices affected by a policy	91
9.4. How to deploy a policy.....	92
9.5. Policy types	92
9.5.1 Agent	92
9.5.2 ESXi.....	93
9.5.3 Monitoring Maintenance Window	93
9.5.4 Monitoring	93

9.5.5	Patch management	94
9.5.6	Power	94
9.5.7	Windows update.....	94
9.5.8	Mobile Device Management.....	94
10	MONITORING	95
10.1	Introduction	96
10.2	Monitor composition.....	96
10.3	Creating monitors manually	96
10.3.1	Steps to create a monitor	96
10.4	Importing ComStore monitors.....	99
10.5	Importing and exporting a monitoring policy.....	99
10.5.1	Importing monitoring policies	99
10.5.2	Exporting monitoring policies.....	99
10.6	Monitoring printers	99
10.7	Creating SNMP monitors.....	100
10.7.1	Parameters to monitor	100
10.7.2	Steps to create an SNMP monitor.....	100
10.8	Creating ESXi monitors	102
10.8.1	How to create an ESXi monitor.....	102
11	COMPONENTS AND COMSTORE	105
11.1	What is a component?	106
11.1.1	Components developed by the administrator	106
11.1.2	Components developed by Panda Security	107
11.2	Using components in the platform	107
11.2.1	Integrating components into the platform	107
11.2.2	Using components from a Quick Job	111
11.2.3	Using components from a Scheduled Job	112
11.3	Developing components	113
11.3.1	What are the requirements for developing components?.....	113
11.4	Creating a monitor component	114
11.4.1	Component presentation and purpose.....	114
11.4.2	Necessary elements.....	114
11.4.3	Communications protocol between the component and the Server.....	115
11.4.4	How to work with a monitor component	116
11.4.5	How to use global variables	120
11.4.6	Labels and user-defined fields.....	121
11.5	Creating a script component	122

11.6. Editing components.....	123
12.ASSETS AUDIT.....	124
12.1. Introduction	125
12.2. Hardware audit	126
12.2.1 Account level.....	126
12.2.2 Site level.....	126
12.2.3 Device level.....	127
12.3. Software audit.....	129
12.3.1 Account level.....	129
12.3.2 Site level.....	129
12.3.3 Device level.....	129
12.4. License audits.....	129
12.4.1 Account level.....	129
12.4.2 Site level.....	130
12.5. Services audit.....	131
12.5.1 Device level.....	131
12.6. Changes audit.....	131
12.6.1 Device level.....	131
13.CENTRALIZED SOFTWARE DEPLOYMENT AND INSTALLATION	133
13.1. Objective of centralized software installation.....	134
13.2. Requirements.....	134
13.3. Package deployment and installation procedure.....	134
13.4. Deployment examples.....	135
13.4.1 Deploying documents using a script language.....	136
13.4.2 Deploying documents without a script language.....	138
13.4.3 Deploying self-installing software.....	141
13.4.4 Deploying software without an installer	143
13.5. Bandwidth optimization.....	145
13.5.1 Designating a device as a local cache.....	146
13.5.2 Configuring the behavior of devices designated as a local cache	147
13.6. Installing software on iOS devices.....	147
13.6.1 Requirements for installing apps on iOS devices	147
13.6.2 Installing the iOS apps included in the Application List	148
14.TICKETING	150
14.1. Introduction	151
14.2. Description of a ticket.....	151

14.3. Creating a ticket	152
14.3.1 Manually by the user from the Agent	152
14.3.2 Automatically from a monitor that detects a condition defined as an anomaly on a user's device.....	153
14.3.3 Manually by the IT Department from the Console	154
14.4. Ticket management	154
15.PATCH MANAGEMENT	156
15.1. What is patch management?	157
15.2. What patches can I deploy/apply?.....	157
15.3. Patch deployment and installation	158
15.4. Method 1: Windows Update policy	158
15.4.1 Access to the Windows Update Policy method	158
15.5. Method 2: Patch Management policy	160
15.5.1 General workflow and Patch Management policy override.....	160
15.5.2 Creating a Patch Management policy.....	162
15.5.3 Creating a patch filter	165
15.5.4 Overriding the policies defined at Account Level	166
15.5.5 Modifying Patch Management policies per device	166
15.5.6 Patch Management method: Usage scenarios	169
15.6. Device patch status	169
15.7. Patch Management policy method: Usage scenarios	171
16.USER ACCOUNTS AND SECURITY LEVELS	173
16.1. User accounts.....	174
16.2. Main user	174
16.3. Security levels.....	174
16.4. Security levels: Purpose	175
16.5. The administrator security level	176
16.6. Accessing user account and security level configuration settings	176
16.7. Creating and configuring user accounts	176
16.8. Creating and configuring security levels	177
16.9. Configuring security levels.....	178
16.9.1 Device visibility	178
16.9.2 Permissions.....	179
16.9.3 Agent Browser Tools.....	179
16.9.4 Membership.....	180
16.10. Strategies for generating security levels.....	180

16.10.1	Horizontal security levels.....	180
16.10.2	Vertical security levels.....	181
16.10.3	Resource access security levels.....	181
17.MOBILE DEVICE MANAGEMENT		182
17.1.	Introduction	183
17.2.	Supported platforms	183
17.3.	Mobile Device Management policies	183
17.3.1	Mandatory and optional policies.....	184
17.3.2	Types of Mobile Device Management policies	184
17.4.	Tools for remotely managing mobile devices	188
17.4.1	Device Wipe	188
17.4.2	Geolocation	188
17.4.3	Device Lock.....	189
17.4.4	Device Unlock	189
17.4.5	Password Policy.....	189
17.4.6	Audits	189
17.4.7	Reports.....	190
18.ACTIVITY LOG		191
18.1.	Introduction	192
18.2.	Account level activity log	192
18.3.	General activity log	192
18.3.1	List of activities.....	193
18.3.2	Activity filter and searches.....	193
18.4.	Device level activity log.....	193
19.REPORTS.....		195
19.1.	Introduction	196
19.2.	Accessing the reports system	196
19.3.	Generating reports.....	196
19.3.1	Generating reports on demand	196
19.3.2	Scheduled generation of reports.....	197
19.4.	Reports features and type of information	198
19.4.1	Level.....	198
19.4.2	Time period	198
19.4.3	Type of report	198
19.5.	Executive reports.....	200
19.5.1	30/7 Day Account Executive Summary (Account)	200

19.5.2	30 Day - Executive Summary Report (Site Level)	200
19.5.3	30/7 Day Site Executive Summary (Site)	201
19.5.4	30 Day - Executive Summary Report - Only Servers and Workstations (Site Level)	201
19.6.	Activity reports	202
19.6.1	30/7 Day Site Activity Summary.....	202
19.6.2	30 Day/7 Account Activity Summary	202
19.6.3	Site Activity.....	202
19.6.4	30/7 Day Account User Summary.....	202
19.6.5	Remote Activity.....	203
19.6.6	Site Remote Takeover Report.....	203
19.6.7	30/7 Day Device Activity Summary	203
19.7.	Alert reports	203
19.7.1	30/7 Day Site Alert Summary.....	203
19.7.2	30/7 Day Account Alert Summary	204
19.7.3	30/7 Day Device Alert Summary	204
19.7.4	Monitor Alerts Report (Device Level)	204
19.7.5	Monitor Alerts Report (Site Level)	204
19.7.6	Monitor Alerts Report (Account Level)	205
19.8.	Inventory reports	205
19.8.1	Computer Summary.....	205
19.8.2	Critical 3 rd -Party Software Summary Report.....	205
19.8.3	Site Serial Numbers	206
19.8.4	Account Server IP Information.....	206
19.8.5	Account Server Storage	206
19.8.6	Site Server Storage.....	206
19.8.7	Site Software	207
19.8.8	Site Software and Hotfixes.....	207
19.8.9	Software Audit Report.....	207
19.8.10	User Software Install	207
19.8.11	Site Storage.....	208
19.8.12	Site IP Information	208
19.8.13	Detailed Computer Audit	208
19.8.14	Device Summary.....	209
19.8.15	Device Change Log.....	209
19.8.16	Site Device	209
19.8.17	Inventory Age.....	210
19.8.18	Microsoft License	210
19.9.	Health reports	210
19.9.1	Customer Health Summary	210
19.9.2	Exception Report	210

19.9.3	Site Health	211
19.9.4	Health Report	211
19.10.	Patch management reports.....	212
19.10.1	Patch Management Activity Report.....	212
19.10.2	Patch Management Detailed Report.....	212
19.10.3	Patch Management Summary Report	212
19.11.	Other reports.....	213
19.11.1	Site User-Defined Fields.....	213
19.11.2	Server Performance Report (Site Level).....	213
19.11.3	Server Performance Report (Account Level)	213
20.	<u>SERVICE ACCESS SECURITY AND CONTROL</u>	<u>215</u>
20.1.	Introduction	216
20.2.	Two-factor authentication.....	216
20.2.1	Essential requirements.....	216
20.2.2	Settings.....	216
20.2.3	Installing Google Authenticator.....	217
20.2.4	Enabling Two Factor Authentication for all accounts.....	218
20.2.5	Disabling Two-Factor Authentication from the login screen	219
20.3.	Password policy	219
20.4.	IP address restrictions to grant or deny access to the Console	220
20.5.	IP address restrictions to grant or deny access from the Agent to the Server.....	220
21.	<u>APPENDIX A: SOURCE CODE</u>	<u>221</u>
21.1.	Chapter 10.....	222
21.2.	Chapter 11	224
22.	<u>APPENDIX B: SUPPORTED PLATFORMS</u>	<u>225</u>
22.1.	Supported platforms	226
22.2.	Detailed Windows requirements.....	227
22.3.	VMware ESXi management requirements	227

1. Preface

Target audience

Icons

1.1. Introduction

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

1.2. 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.

1.3. 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.

2. Introduction

Main features

User profile

Main components

Key players

2.1. Introduction

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 customer or account are reduced as **Panda Systems Management**:

- Requires no additional infrastructure on-site as the solution is hosted in the cloud.
- 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.

2.2. 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. Management of VMware ESXi servers (VMware vSphere Hypervisor 4.1, 5.0, 5.5 and 6.0) and Microsoft Hyper-V servers in 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).

Feature	Description
Software license management	Keep track of all software licenses installed.
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 of the software installed.
Software deployment	Centralized software deployment to Windows, Linux, Mac and iOS computers.
Policies	Define a set of common configurations to manage your IT environment faster and more effectively.
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.
Remote control	Shared access to the user's desktop or total control. 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	Send scheduled or special reports via email. Find out who does what, when, and who uses most of those resources.
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 1: Panda Systems Management feature list

2.3. Panda Systems Management user profile

Panda Systems Management is designed for users with a medium to high level of technical knowledge, as this tool provides daily support of computing devices subject to constant use and configuration changes. However, there are two specific user groups of **Panda Systems Management**:

- **Enterprise level 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.

2.4. Main components of 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.

- **Agent**

This is a small program (6.5 MB) of size in the 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.

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.

- **Server**

The Console, the processes required to collect, synchronize and redirect the messages, events, and information flows generated by the Agents, and the databases that support them are all hosted on a cloud-based server farm available 24 hours a day.

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.

2.5. 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.

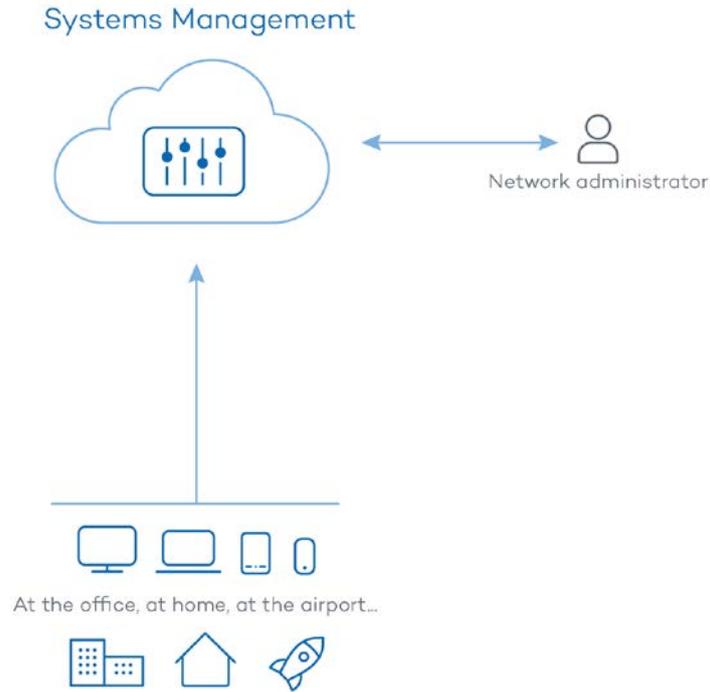


Figure 1: Panda Systems Managements basic operation diagram

- **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.



Chapter 16: User account and security levels describes how to create new users and security levels in order to restrict the access of system technicians to key Panda Systems Management resources.

In Chapter 20: Security and control over access to the service, you can see how to configure two-factor authentication to access the Console.

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 User is the person using the device that requires direct support from the MSP or IT department.

- **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.

3. Hierarchy of levels within the Management Console

Hierarchy of levels

Account Level

Site Level

Device Level

3.1. Hierarchy of levels within the Management Console

In order to separate management of the devices of different customer accounts and reuse and restrict procedures defined by technical staff in the Console, and to expedite and refine management, **Panda Systems Management** provides three entities/group levels/operation levels. From the most general to the most specific, these are the following:

- Account level
- Site level
- Device level

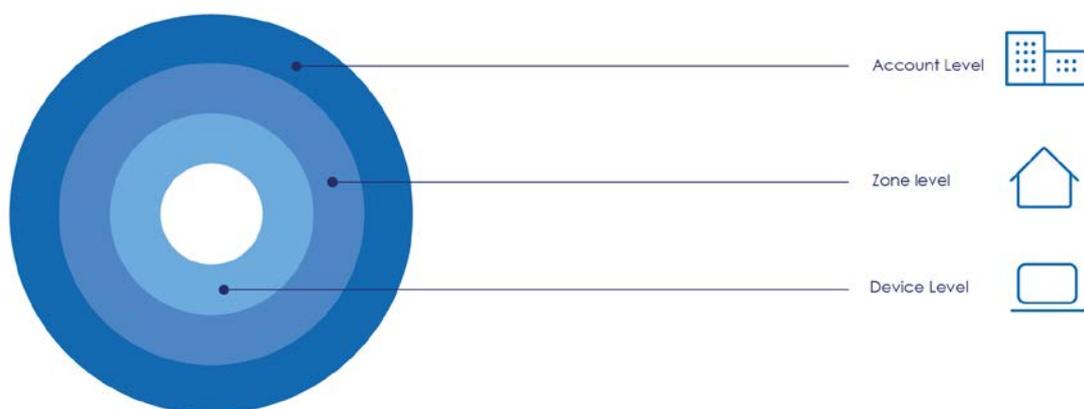


Figure 2: level hierarchy

3.2. 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 6: Filters and Groups.

Access

The Account Level resources are accessed from General Menu, **Account**.



Figure 3: accessing general menu Account

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.

Parameter	Description
Password Policy	This lets you set password policies. See Chapter 20: Security and control over access to the Panda Systems Management service for more details.
Access Control	Lets you set advanced access controls for the Console and the service. See Chapter 20: Security and control over access to the Panda Systems Management service for more details.
Power Rating	Lets you set power consumption parameters (in Watts) for each type of device in order to calculate monthly consumption. See Chapter 5: Devices for more details.
Agent Deployment Credentials	Lets you set the credentials required for remotely installing the Agent. See Chapter 5: Devices for more details.
End-User Ticket Assignee	Indicates the account to which users send the tickets that are opened directly from the Agent. See Chapter 14: Ticketing for more details.
Variables	Variables passed to the scripts run on the devices. See Chapter 11: Components and the ComStore for more details.
User-defined fields	Lets you define the names of the labels used to collect the results of the scripts run on the devices. See Chapter 11: Components and the ComStore for more details.
Custom Agent Settings	Lets you define how the Agents will perform as the Connection Broker. See Chapter 5: Devices for more details.
SNMP Credentials	Lets you define the default connection settings for the SNMP protocol, applicable to the network devices to manage and which are not compatible with the Systems Management Agent.
ESXi Credentials	Lets you define the default connection settings to manage ESXi servers.
Agent Update Settings	Prevents or allows the automatic updates of the Agents installed.

Parameter	Description
Mail Settings	Lets you configure the source account and the reply for the emails sent by the Systems Management Server to service administrators.
Mail Recipients	Lets you configure the email accounts that will receive alerts, reports and summaries of the new components added to the ComStore, as well as updates and notifications of new devices added to the account managed by Panda Systems Management .
Update site variables	Variables passed to the scripts run on the devices.
Apple push certificate	Lets you configure the certificate required to manage Apple mobile devices. See Chapter 17: Mobile device management for more details.
Reset Columns Display	Lets you restore the default settings to display basic information about the devices managed. See Chapter 5: Devices for more details.

Table 2: settings available at Account Level

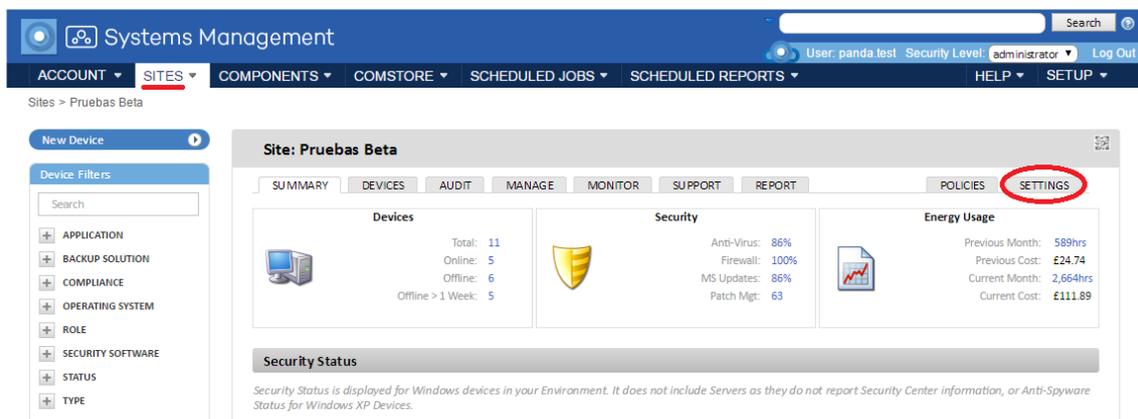
3.3. Site Level

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. These settings can be accessed from tab bar, **Settings** in the Console. 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.



The screenshot shows the Panda Systems Management interface. The top navigation bar includes 'ACCOUNT', 'SITES', 'COMPONENTS', 'COMSTORE', 'SCHEDULED JOBS', 'SCHEDULED REPORTS', 'HELP', and 'SETUP'. The 'SITES' menu is selected, showing a breadcrumb 'Sites > Pruebas Beta'. On the left, there is a 'Device Filters' sidebar with categories like APPLICATION, BACKUP SOLUTION, COMPLIANCE, OPERATING SYSTEM, ROLE, SECURITY SOFTWARE, STATUS, and TYPE. The main content area is titled 'Site: Pruebas Beta' and has a tab bar with 'SUMMARY', 'DEVICES', 'AUDIT', 'MANAGE', 'MONITOR', 'SUPPORT', 'REPORT', 'POLICIES', and 'SETTINGS'. The 'SETTINGS' tab is highlighted with a red circle. Below the tabs, there are three summary cards: 'Devices' (Total: 11, Online: 5, Offline: 6, Offline > 1 Week: 5), 'Security' (Anti-Virus: 86%, Firewall: 100%, MS Updates: 86%, Patch Mgt: 63), and 'Energy Usage' (Previous Month: 589hrs, Current Month: 2,664hrs, Current Cost: £111.89). A 'Security Status' section at the bottom provides a disclaimer: 'Security Status is displayed for Windows devices in your Environment. It does not include Servers as they do not report Security Center information, or Anti-Spyware Status for Windows XP Devices.'

Figure 4: 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 6: Filters and groups.

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 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.



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 Chapter 5: Devices



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, select the relevant profile in the **general menu Sites** and click the **Settings** tab.

Below is a complete list of all options, noting the chapters in which they are described if applicable.

Parameter	Description
General	General site information: Name , internal identifier (UID), Description and Types of devices hosted in the site.
Power Rating	Lets you set power consumption parameters (in Watts) for each type of device in order to calculate monthly consumption. See Chapter 5: Devices for more details
Proxy	Lets you set the proxy details for network users without a direct Internet connection. See Chapter 5: Devices for more details.
Custom Agent Settings	Lets you define how the Agents will perform as the Connection Broker. See Chapter 5: Devices for more details.
Additional Subnets for Network Discovery	Agents nominated as a Network Node will scan their local subnet in order to find unmanaged devices. This setting enables a Network Node to scan additional subnets.
Agent Deployment Credentials	Lets you set the credentials required for remotely installing the Agent. See Chapter 5: Devices for more details.
SNMP Credentials	Lets you define the default connection settings for the SNMP protocol, applicable to the network devices to manage and which are not compatible with the Systems Management Agent.
ESXi Credentials	Lets you define the default connection settings to manage ESXi servers.
Local Caches	Lets you assign the role of cache to one of the network devices. This saves bandwidth during software deployment. See Chapter 13: Centralized software deployment and installation for more details.
Mail Recipients	Lets you configure the email accounts that will receive alerts, reports and notifications of new devices in the site managed by Panda Systems Management .
End-User Ticket Assignee	Indicates the account to which users send the tickets that are opened directly from the Agent. See Chapter 14: Ticketing for more details.
Variables	Variables passed to the scripts run on the devices. See Chapter 11: Components and the ComStore for more details.
Credentials	This is for setting the credentials for software deployment. See Chapter 13: Centralized software deployment and installation for more details.
User-defined fields	Lets you define the names of the labels used to collect the results of the scripts run on the devices. See Chapter 11: Components and the ComStore for more details.

Table 3: Settings available at Account Level

3.4. 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.

4. Basic components of the Console

General menu

Tab bar / List bar

Icon bar / Action bar

Filters and groups panel

Dashboards

4.1. Introduction

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 partners and administrators will be able to deliver value to their customers from the outset.

The basic components of the Console to which we will refer throughout this guide are:

4.2. General menu

This menu is accessible from anywhere in the **Systems Management** Console. It consists of eight entries:



Figure 5: general menú

Components:

Menu	Description
Account	Access to Account Level.
Sites	Access to Site Level.
Components	Access to components downloaded by and accessible to the administrator.
ComStore	Repository of components created by Panda Security that extend the capabilities of Panda Systems Management .
Scheduled Jobs	List of active and finished jobs.
Scheduled Reports	List of configured and default reports.
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 16: User account and security levels.

Table 4: general menu items

4.3. Tab bar / List bar

The Tab bar (also called **List bar**) provides access to the tools available in the Console for generating and presenting consolidated lists on-screen, with details of the status of the devices belonging to the level accessed. It also allows configurations to be defined and viewed.

This bar is slightly different if it is accessed from Site Level, Account Level or Device Level for a specific device, as each management scope is also different.

Figure 6: tab/List bar

4.3.1 Components

Tab	Accessible from	Description
Summary	Site, Device	Status Information
Dashboard	Account	General control panel
Devices	Site	List of devices accessible with associated information
Audit	Account, Site, Device	Hardware, software and license audit list
Manage	Account, Site, Device	Lists of the patches applied and pending patches, software installed on devices, as well as devices discovered on the network and managed by Accounts Management
Monitor	Account, Site, Device	List of alerts created by monitors or finished jobs
Support	Account, Site, Device	List of tickets generated
Report	Account, Site, Device	List and generation of on-demand reports
Policies	Account, Site, Device	List and generation of policies, described later.
Settings	Site	Configuration associated to the Site.

Tab	Accessible from	Description
Suspended devices	Account	List of uninstalled devices

Table 5: Tab/List bar items



The scope of the Tab bar refers to the current level. Therefore, If you go to the Tab bar at Account Level, you'll see consolidated information on all devices. If you access it at Site Level, it will show consolidated information on the devices in the site. If you access it at device Level, it will only show information for that particular device

4.4. Icon bar / Action bar

The Icon bar or Action bar accesses actions to change the status of the devices. This bar does not exist in the general menu **Account** and varies slightly if accessed from the general menu **Sites** or a specific device, as the management scope is different.

The scope of the Icon bar will be formed by manually selecting the devices that have been selected in a site.

The screenshot shows the 'Site: Pruebas Beta' interface. At the top, there are navigation tabs: SUMMARY, DEVICES, AUDIT, MANAGE, MONITOR, SUPPORT, REPORT, POLICIES, and SETTINGS. Below the tabs, it says 'Showing 1 - 11 of 11 results.' and 'Show me 25 per page'. There are several filter checkboxes: All, Desktops, Laptops, Servers, Network, ESXi Host, Unknown, and Unapproved. An 'Actions' bar contains various icons for device management. Below this is a table with columns: Hostname, Description, IP Address, Last Updated, Agent Version, Status, and AEM Device Type. The table lists four devices: BetaESXi (ESXi de Beta), BETA_ (BETA_AUTO_TEST), BIOOS (BIOOSLOPEZ), and pandas-Pro.local (pandas-MacBook-Pro.local).

Figure 7: icon bar

4.4.1 Components

Icon	Accessible from	Description
Move Device to	Site, Device	Move the selected devices to another site.
Add Device to	Site, Device	Move the selected devices to a group.
Edit	Site	Add notes and custom fields to the selected devices that can be used by filters.

Icon	Accessible from	Description
Toggle	Site	Mark devices as favorite for quick access from Summary / Dashboard .
Delete	Site, Device	Delete a device from a site. The device will no longer be managed, the Agent will be uninstalled, and the device will be added to the Suspended devices tab under the general menu Account .
Request audit	Site, Device	Force the launch of an audit. For more details see Chapter 12: Assets audit
Schedule Job	Site, Device	Create a scheduled job for a later date. For more information, see Chapter 11: Components and the ComStore.
Run a Quick Job	Site, Device	Create and run a job already created. For more information, see Chapter 11: Components and the ComStore.
Download	Site	Download the list of devices in the site.
Add/Remove Cache	Site, Device	Mark the device as network cache to speed up component download and installation, as well as software deployment to network devices
Network node settings	Site, Device	Nominate a device as a Network Node and use it to deploy Panda Systems Management and communicate with the server more easily
Turn Privacy On	Site, Device	Prevent remote access to the devices by the administrator unless approved by the user
Send a message	Site, Device	Send a message to the selected devices
Schedule Reports	Site	Schedule reports for a later date
Refresh	Site, Device	Refresh the data on the screen
Show device(s) on Google Map	Device	Geolocation of devices on a map.
QR Code	Device	QR code associated to the device for paper auditing

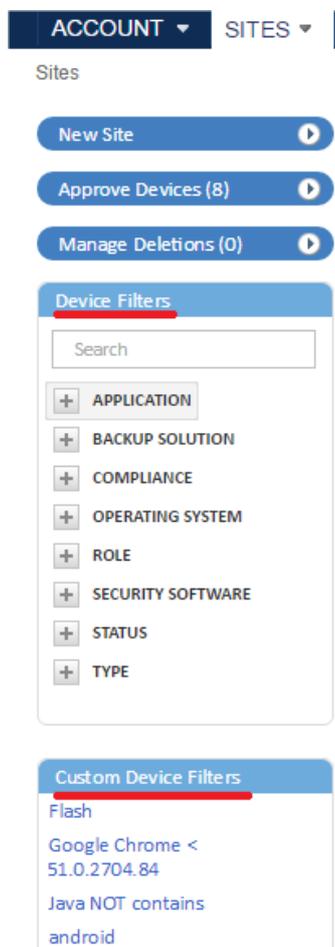
Table 6: Icon bar items



To perform actions on devices at Account Level, you need to create an Account filter or Site group with the selected devices. The Account Level will not display the Icon bar unless you select devices using a filter or group..

4.5. Filters and groups panel

The left of the Console contains three panels with different groups:



- **Device filters:** Preconfigured filters to help locate devices.
- **Site Device Filters / Custom Device Filters:** Device filters created by the administrator at Site Level or Account Level, respectively.
- **Site device groups/Custom device groups:** Device groups created by the administrator at Site Level or Account Level, respectively.
- **Site groups:** Only available at Account Level, these are groups of various sites.

Figure 8: side panel with the grouping and filtering tools

4.6. Dashboards

The dashboards reflect the status of a set of devices. There are four types of dashboard:

- Security Status
- Account Dashboard
- Summary (Site)
- Summary (Device)

4.6.1 Security Status

Accessible from the general menu **Account**, it reflects the security status of all managed devices.



Figure 9: security dashboard

4.6.2 Account Dashboard

Accessible from the general menu **Account** by clicking **Account, Dashboard**.

It collects general information on the status of all devices: notifications, jobs, alerts, etc.

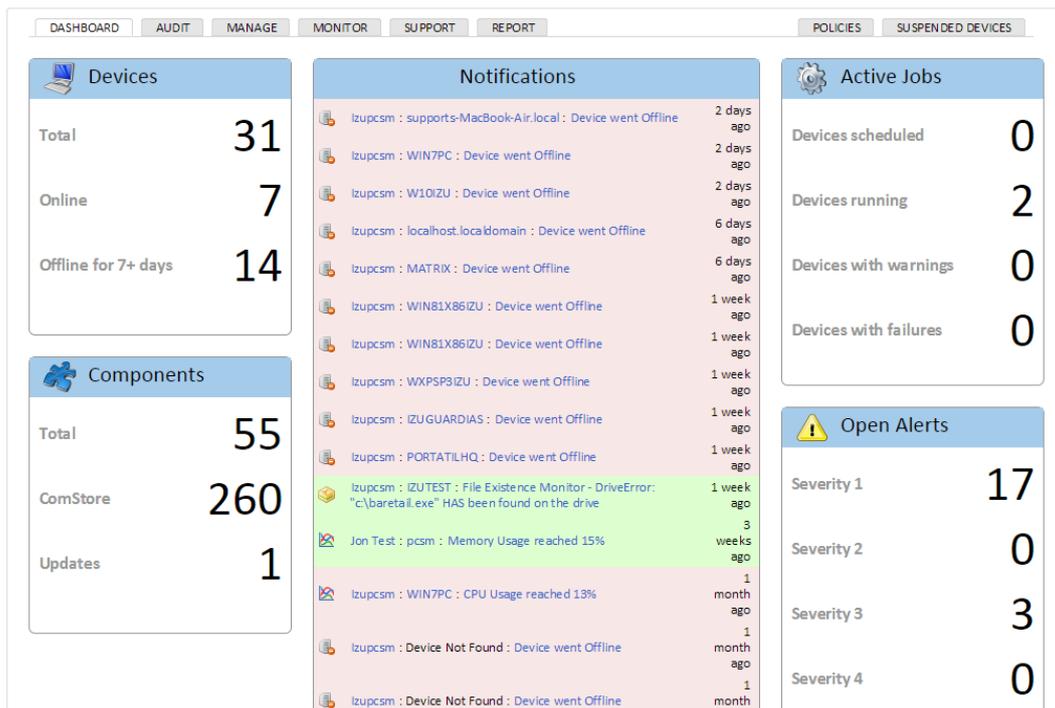


Figure 10: account dashboard

4.6.3 Summary (Site)

Accessible from the general menu **Sites**, and by selecting a specific site. It reflects the status of all the devices that belong to the selected site. There will be a summary dashboard for each site created.

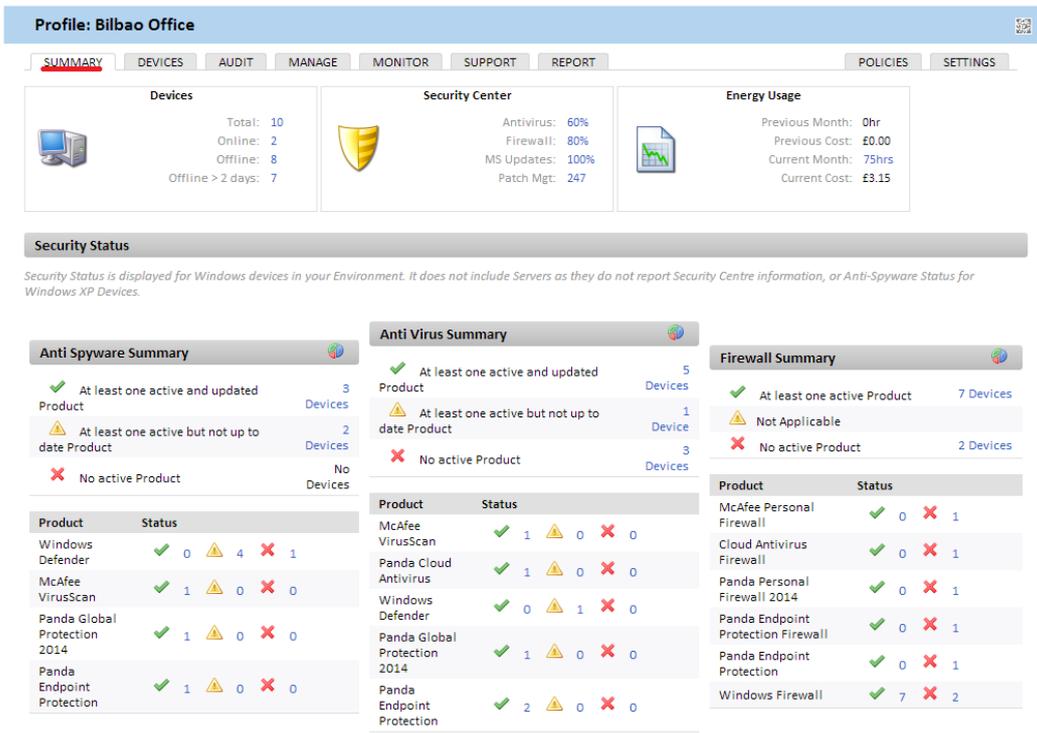


Figure 11: site dashboard

4.6.4 Summary (Device)

Accessible from a device. It reflects the status of a specific device. There is one for each managed device.

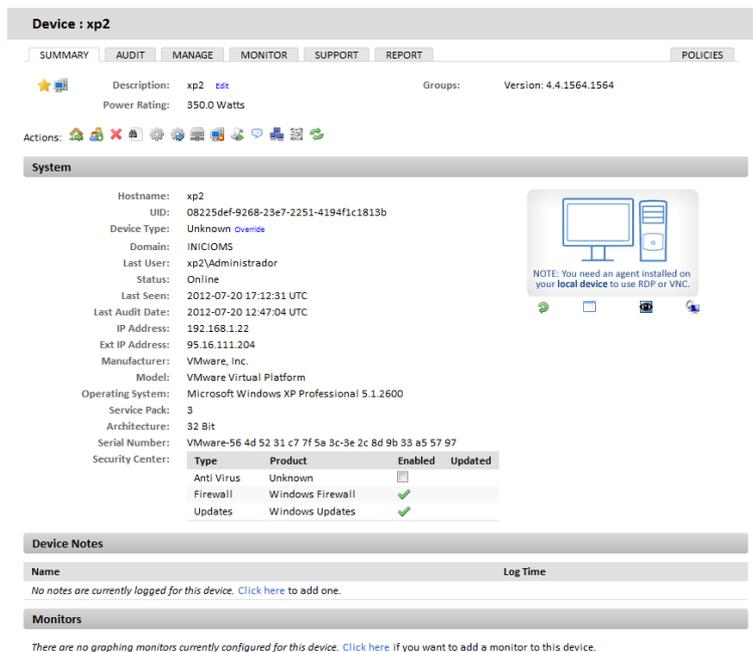


Figure 12: device dashboard

5. Deploying and managing devices

Prerequisites steps

Sending via email

Direct download

Remote installation

Installing on Android and iOS

Administration of devices not directly supported

Managing ESXi servers

Managing Hyper-V servers

Approving devices

Configuring a Connection Broker

Other connection parameters

Configuring a network node

Managing devices

Viewing device information

Managing device resource consumption

5.1. Introduction



See Appendix B to see the platforms that support installation of the Agent

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

All devices managed by **Panda Systems Management** send and receive information that the Server collects, catalogs and displays in real time in the Console.

There are three possible forms of communication between the Server and any given device:

- Directly by installing the 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 without a direct Internet connection. We describe how to configure a proxy later in this chapter.
- Indirectly via SNMP or other proprietary protocols (ESXi).

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 Server.

5.2. Prerequisite steps prior to adding devices to Panda Systems Management

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

- The site to which the Agent will belong.
- Connection information.

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 Mac OS X), 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 in 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 the section **Installing the agent on Android and iOS platforms** later in this chapter.

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 in two ways:

- **Manually in each installed Agent:** Right-click the Systems Management icon in your desktop's Notification area. 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 general menu Sites, 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.

5.3. Sending the Agent via email

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

- Go to the general menu **Sites**, and select the site to which the devices to manage will belong.
- Click **Devices** on the tab bar and then **Add a device**. 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).

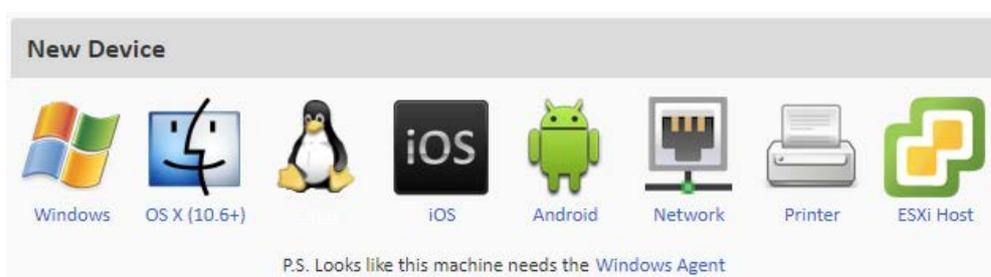


Figure 13: platforms supported by Panda Systems Management

- Once you've selected the platform, you'll be asked to 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, Mac OS

X and Linux), or with a link to download it from Google Play or Apple 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**:

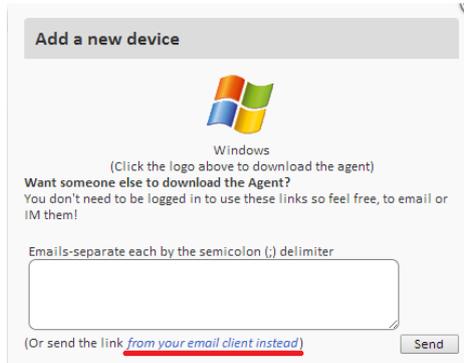


Figure 14: link for sending the PCSM Agent from the email client installed on your computer

5.4. Direct download of the PCSM Agent

Administrators can download the Agent from the Console, then distribute it manually or using distribution tools such as Active Directory. To do this, use the same procedure but click the platform icon.



Figure 15: direct download of the PCSM Agent



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.

5.5. Remote installation

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 Mac OS X 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 Mac OS X)
 - From the installed Agent (Windows only)
- Install the agents remotely
 - From the Console (Windows and Mac OS X)
 - From the installed Agent (Windows only)

5.5.1 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. See later in this chapter for more information about how to assign the Network Node role to a device.

5.5.2 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.

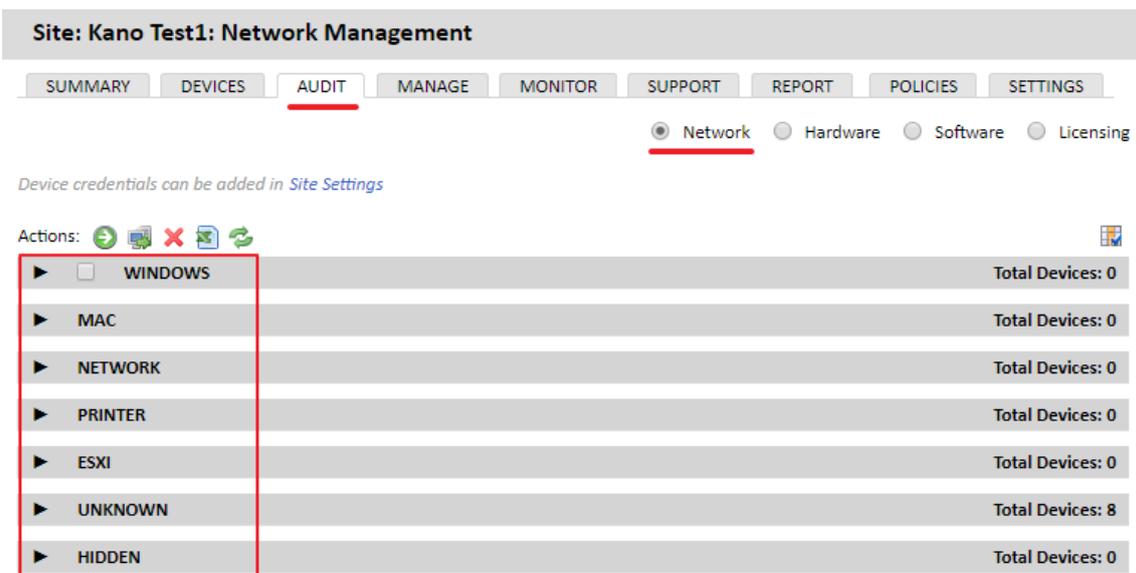
Device discovery requirements

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: SSH port 22, HTTP port 80, HTTP port 8080, HTTPS port 443.

5.5.3 Install the Agents remotely from the console

- Within 15 minutes after the launch of the discovery task, go to general menu Sites, Audit tab, and select the Network radio button to display all discovered computers grouped by type.



Site: Kano Test1: Network Management

SUMMARY DEVICES **AUDIT** MANAGE MONITOR SUPPORT REPORT POLICIES SETTINGS

Network Hardware Software Licensing

Device credentials can be added in Site Settings

Actions:     

▶ <input type="checkbox"/> WINDOWS	Total Devices: 0
▶ MAC	Total Devices: 0
▶ NETWORK	Total Devices: 0
▶ PRINTER	Total Devices: 0
▶ ESXI	Total Devices: 0
▶ UNKNOWN	Total Devices: 8
▶ HIDDEN	Total Devices: 0

Figure 16: computer discovery

- 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. The domain account used for the installation is configured in the **Settings** tab of the site corresponding to the devices. Enter the user name and password of the domain administrator in the **Agent Deployment Credentials** section.



An installed 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 Mac OS X Agent will deploy agents to Apple devices.

5.5.4 Run a computer discovery task from the installed Agent (alternative method)

To deploy the PCSM Agent directly from a Windows computer already integrated in **Panda Systems Management**, click the discovery icon and launch a device discovery task.

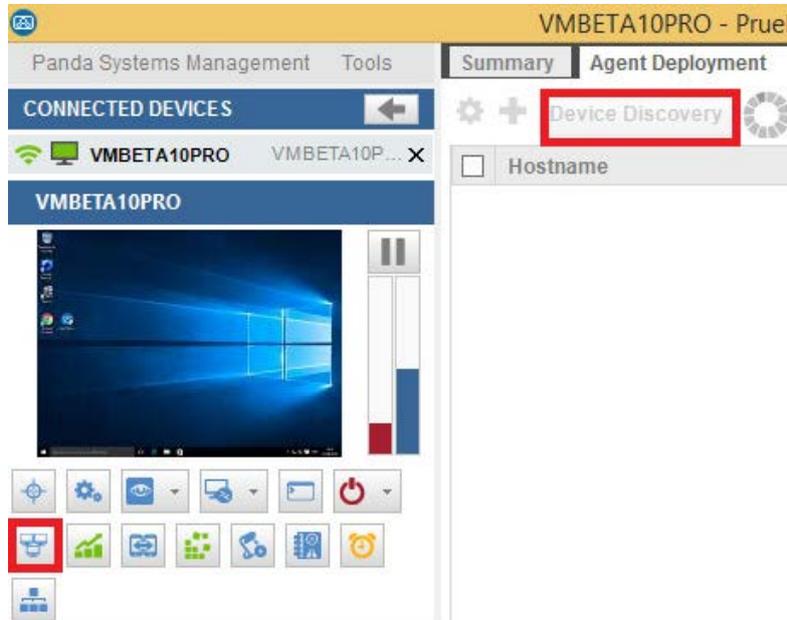


Figure 17: device discovery from the PCSM Agent

The Agent will display all of the computers that are connected to its subnet, and will also indicate if they already have a **Systems Management** Agent installed as well as its version. When the process is completed, select the computers that will receive the Agent and click **Deploy**.

Before the deployment process actually starts, a window will be displayed to enter the necessary user credentials to install the agent and create the necessary services on the target computers.

5.6. Installing the Agent on Android and iOS

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.

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 18: mobile Device Management component

 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**.

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)



Figure 19: 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.



Figure 20: creating a new certificate in the Apple Push Certificates Portal

Download the new Apple signed certificate (.PEM) to your computer



Figure 21: downloading the certificate from the Apple Push Certificates Portal

Go back to the Console. Browse to the Apple signed certificate (.PEM) downloaded from the *Apple Push Certificate Portal*, and upload it. Once uploaded, the following message will appear in the Console.



Figure 22: certificate uploaded to the PCSCM Console

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.

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**

On a PC with the Web console displaying the site that the user’s mobile device will belong to, click the QR Code icon to enlarge it (you’ll find it in the top right corner of the window).

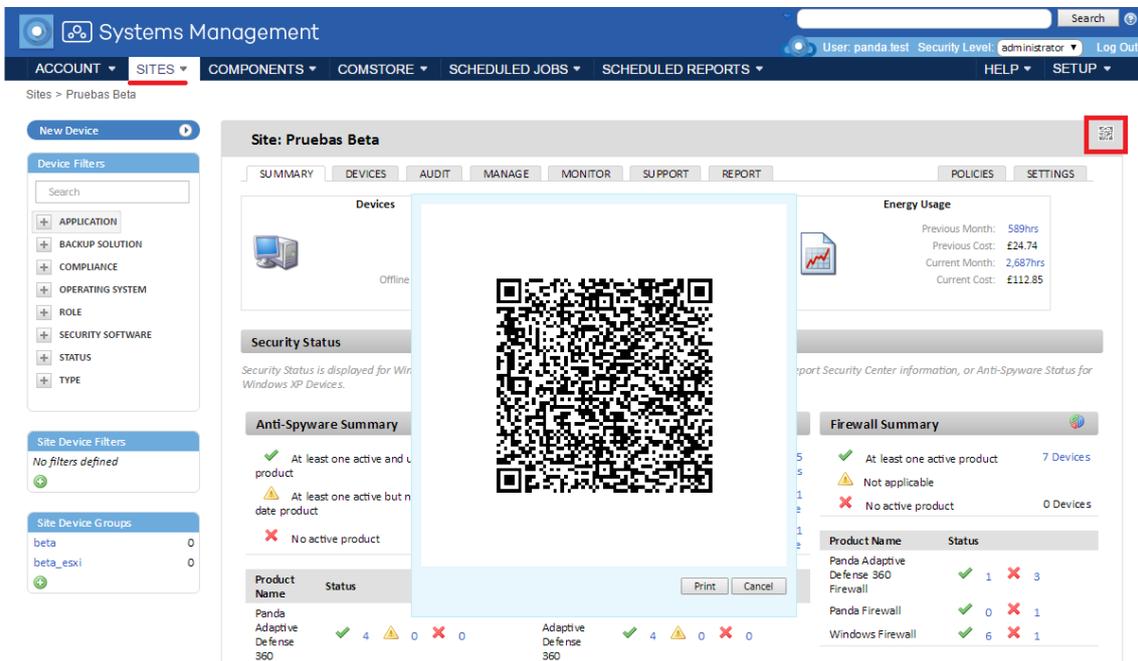


Figure 23: generating the QR Code

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



Figure 24: PCSM Agent on the mobile device

After reading the code, the Agent will display the message **Connected** on the user's device, and appear on 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 on the Console



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

5.7. Administration of devices not supported by the Agent



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. Mibble is a MIB browser available for free from the Mibble website.

Panda Systems Management allows you to use the SNMP protocol to manage devices that don't support software installation, such as printers, routers, switches, 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

5.7.1 Adding 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

- On the **Audit** tab, select **Network**. This will display all discovered computers, grouped by type. **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.

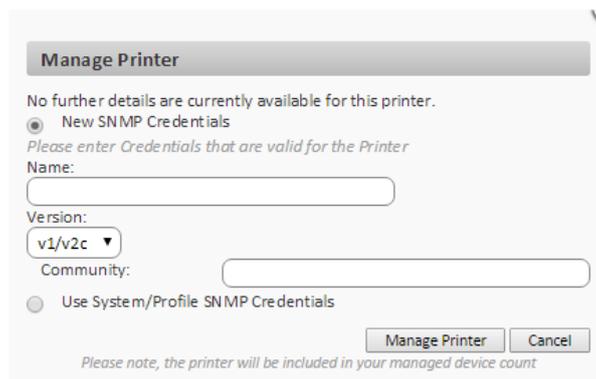


Figure 25: entering the SNMP credentials for managing a device via SNMP



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

5.7.2 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.

Assigning a Network Node to a single device not compatible with the PCSM Agent:

- Click the general menu **Sites**, select the site that the device to manage belongs to and click the **Summary** tab.

- 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.

Assigning a Network Node computer to multiple devices

- Click the general menu **Sites** and select the site that the devices belong to.
- Select the target devices and click the  icon on the actions bar.
- Select **Assign Network Node** from the drop-down menu. A window will be displayed for you to select a Network Node from all available nodes.

5.8. 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.

5.8.1 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.

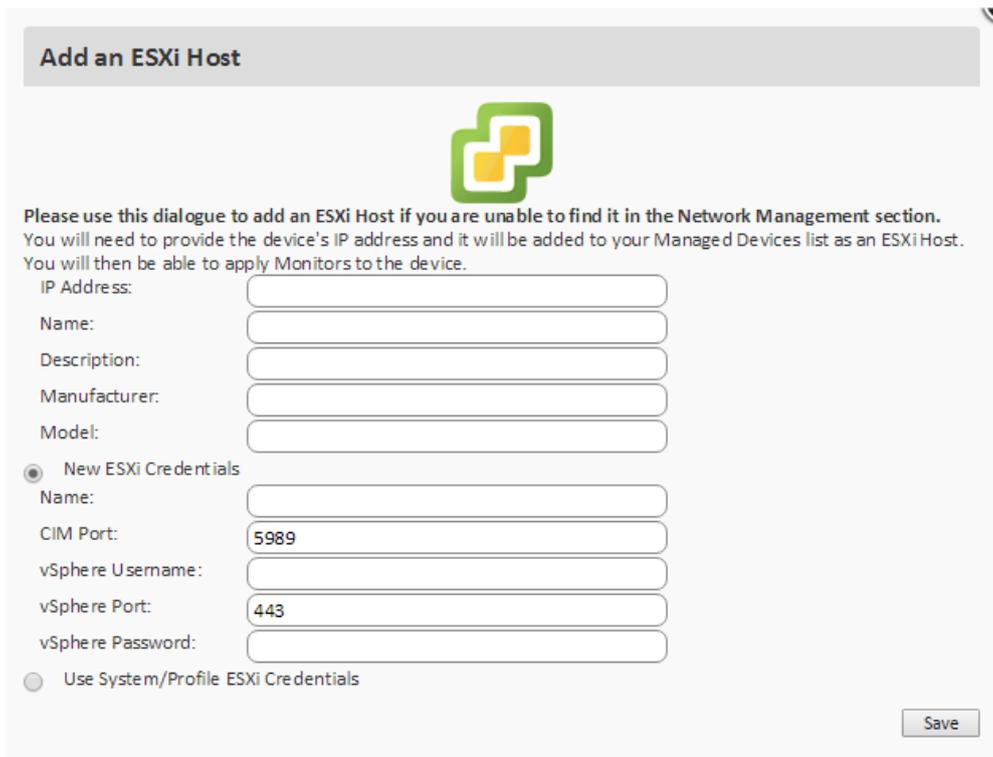


Figure 26: ESXi server connection window

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**.

The ESXi server credentials can be defined individually for the ESXi server to be added, or you can inherit the general configuration established at global level in the **general menu Account, Setup**, or at site level by selecting the relevant level and clicking **Settings** in the tab bar.



For more information, refer to [Chapter 3: Hierarchy of levels within the Management Console](#).

5.8.2 Adding multiple ESXi servers at the same time

Go to Tab bar, **Manage** to view all of the devices discovered on the network. Use the **Other** filtering option or **Search** field to find the ESXi server to add.

Once located, click the **Manage device**  icon and the ESXi icon to select the type of device. A form will be displayed for you to enter the necessary credentials for a PCSM agent on the network to connect to the ESXi server and extract the monitoring and status information.

5.8.3 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 5.7.2.

5.9. 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 **Adding Agent-compatible devices** 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.

5.10. 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).

To configure manual approval of devices, go to the general menu **Setup, Account Settings**.

Once manual approval of devices is enabled, they will appear under the **Approve Devices** option as the Agents are installed on the computers. The administrator will then be able to approve the devices to be included in the service.

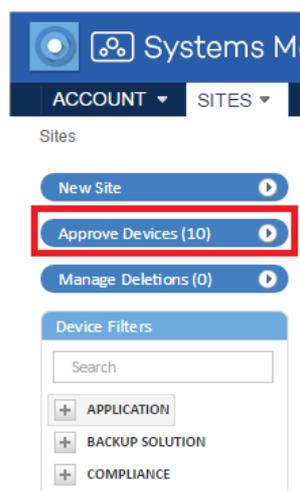


Figure 27: approve Devices button

Even if devices are not approved, they will still be included in the inventory processes and it will be possible to access them via remote desktop.



Non-approved devices will still use up licenses but will not receive jobs nor deployed components.

When a device is waiting approval, a message will appear in the corresponding site's list of devices.

Site: Pruebas Beta

SUMMARY **DEVICES** AUDIT MANAGE MONITOR SUPPORT REPORT

Showing 1 - 11 of 11 results.

Actions:             All Desktops Laptops Servers Network

<input type="checkbox"/>	Hostname	Description	IP Address	Last Updated	Agent Version
You currently have 2 device(s) awaiting your approval in this site.					

Figure 28: message indicating there are devices that require approval

5.11. Configuring a Connection Broker

A Connection Broker is a Windows device with an Agent installed and which is responsible for performing a series of additional tasks aimed at minimizing traffic on customers' networks, as well as supporting connectivity of the remote desktop on neighboring devices.

By default, on each network segment there will be an Agent that automatically takes the role of Connection Broker. It will be responsible for maintaining centralized communication with the Server and the managed devices in order to minimize bandwidth consumption. The Connection Broker also discovers devices on the same network segment, even if they are devices without an Agent installed, printers, routers or others.



If you have problems starting a remote desktop session on a network segment, restart the computer acting as the Connection Broker and try again

5.11.1 Assigning the Connection Broker role to a device

Even though promoting a device to Connection Broker is an automatic process performed on the basis of the characteristics of each device (the time it is switched on, available bandwidth, CPU power, etc.), in some cases it may be advisable to promote a specific network device manually.



Make sure you assign the Connection Broker role to a server-type device on each network segment, to ensure it has sufficient resources and it is always in service.

To do this, go to the settings of the Agent that you want to act as Connection Broker, right-click and select **Settings, Preferences**.

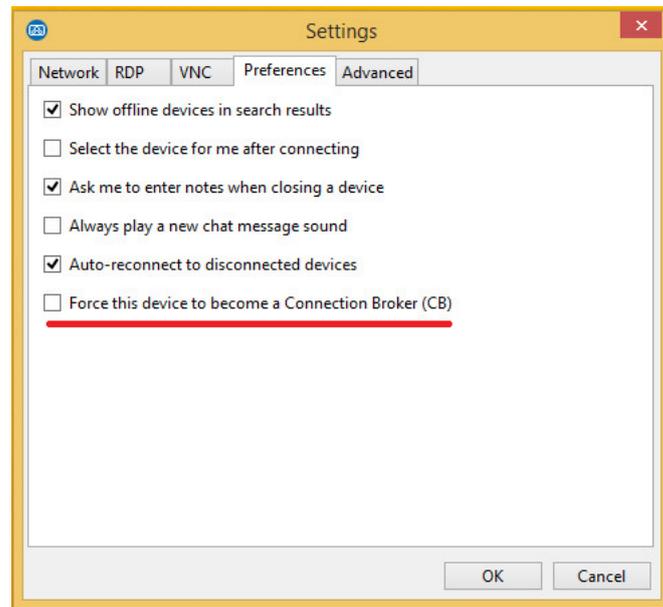


Figure 29: PCSM Agent window for designating a Connection Broker

5.11.2 Disabling the use of Connection Brokers

Given that when an Agent is promoted to a Connection Broker it requires resources on the device CPU and on the customer's local network which may not be available, it is possible to completely disable this feature from the general menu **Setup, Account Settings** in **Custom Agent Settings**, or from **Site, Settings** if you only want to disable this feature for a specific site.

5.12. 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 settings, go to the general menu **Setup, Account Settings** and edit the connection parameters:

Use Connection Brokers: ON

When switched off, this prevents any Agent in your account from becoming a Connection Broker (default setting is "On")
Note: This setting will override any selection made at Site level

Use alternative settings for Agent

Control Channel Address:

Control Channel Port:

Web Service Address:

Tunnel Server Address:
(You must specify an IP/domain and a port e.g. 123.45.6.789:443)

Network Subnet Limit:
Default: 65,534, Maximum: 65,534, Minimum: 0 (Off)

Network Scan Limit:
Default: 254, Maximum: 1024, Minimum: 0

Figure 30: window for configuring the connections used by the PCSM Agent

Field	Description
Control Channel Address	Use restricted to the Panda Security Support Dept.
Control Channel Port1	Use restricted to the Panda Security Support Dept.
Control Channel Port2	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 7: configuration parameters for the connections used by the PCSM Agent

5.13. 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.

5.13.1 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.

5.13.2 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  .

5.13.3 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 can send and receive SNMP commands, but cannot perform network searches.

5.14. Managing devices

Panda Systems Management provides different tools to access the devices managed by the product, depending on whether they are compatible with the PCSM Agent or not.

5.14.1 Devices compatible with the PCSM Agent

Follow the steps below to manage computers compatible with the PCSM Agent:

- Click the general menu Sites, select the site the device belongs to, and click the device to manage.
- The Summary tab will display different icons through which you can access the device.

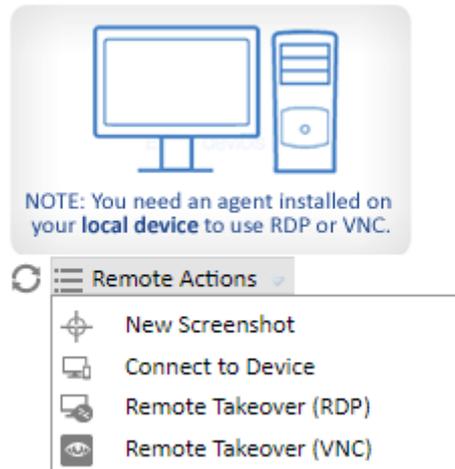


Figure 31: access to the remote access tools

Refresh 	Takes a new screenshot of the device desktop and displays it on screen
New Screenshot 	Lets you download a screenshot of the device desktop
Connect to device 	Connects the local agent to the selected device
Remote takeover (RDP) 	Connects to the device's remote desktop via RDP
Remote takeover (VNC) 	Connects to the device's remote desktop via VNC

Table 8: tools for accessing devices remotely

Accessing resources on the remote managed devices

Follow the steps below to run commands on a specific computer:

- Click the **Connect to Device** option on the device's **Summary** tab. This will open the installed PCSM Agent with the relevant administrator credentials.
- Once you have connected to the remote device, use the available icons and menus to perform the necessary access and control actions on it.

The options that do not prevent the user from continuing to work on the system are:

- **Remote screen capture:** Rapid viewing of error messages.
- **Windows Services Tab:** Remote access to stop, start and restart services without needing to access the remote desktop,
- **Screen Sharing Session:** Shared remote desktop. The user sees what the technician is doing on the device
- **Command shell:** Remote DOS command line.
- **Agent deployment:** Deploy the Agent across the LAN.
- **Task manager:** Remote access to the task manager without needing to access the remote desktop.
- **File transfer:** Provides full access to the target device's file system, allowing the administrator to transfer files between their computer and the user's computer, as well as move files, create and delete folders and rename items.
- **Drive information:** Lists the current local and network drives connected to the device, allowing the administrator to add or delete network paths.
- **Registry editor:** Remote access to the regedit tool without needing to access the remote desktop.
- **Quick Jobs:** Launch Jobs.
- **Event viewer:** Remote access to the event viewer without needing to access the remote desktop.
- **Wake Up:** Allows a device that is switched on to send the rest of the devices in the same LAN segment a "magic packet" to switch them on remotely.

The options that will prevent the user from using the device are:

- **Windows RDP:** Remote desktop access via RDP, which will close the user's session.
- **Shut Down / Reboot:** Shut down or restart the target device.

5.14.2 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 HTTP, 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.

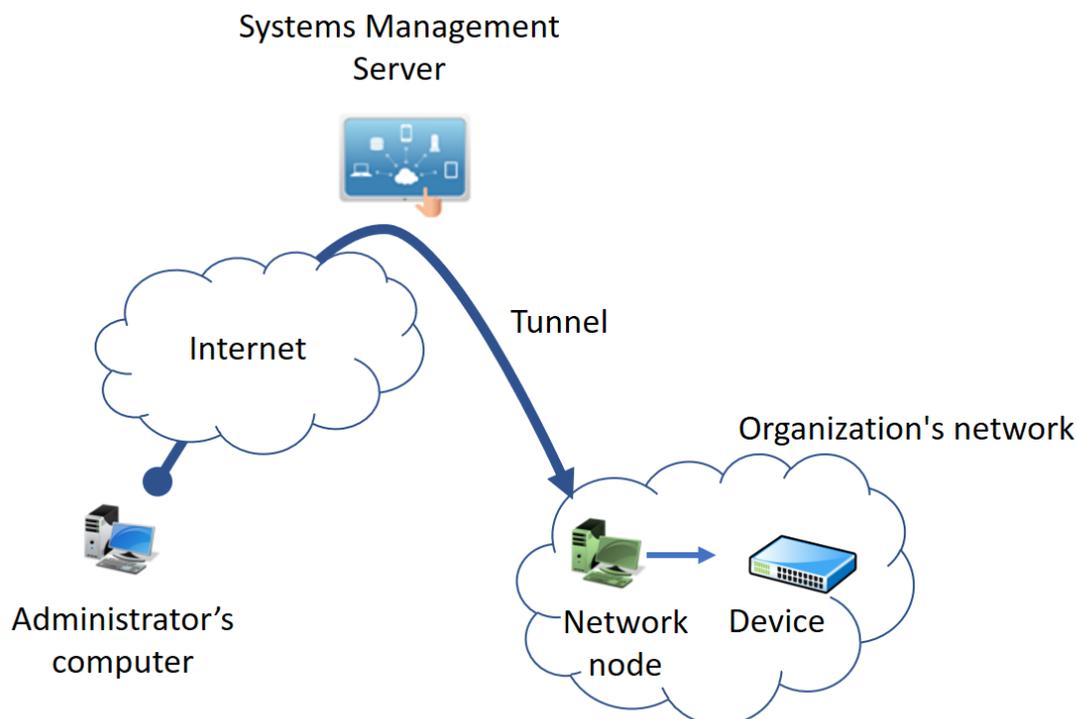


Figure 32: connection established between the administrator's computer and the Network Node through the tunnel

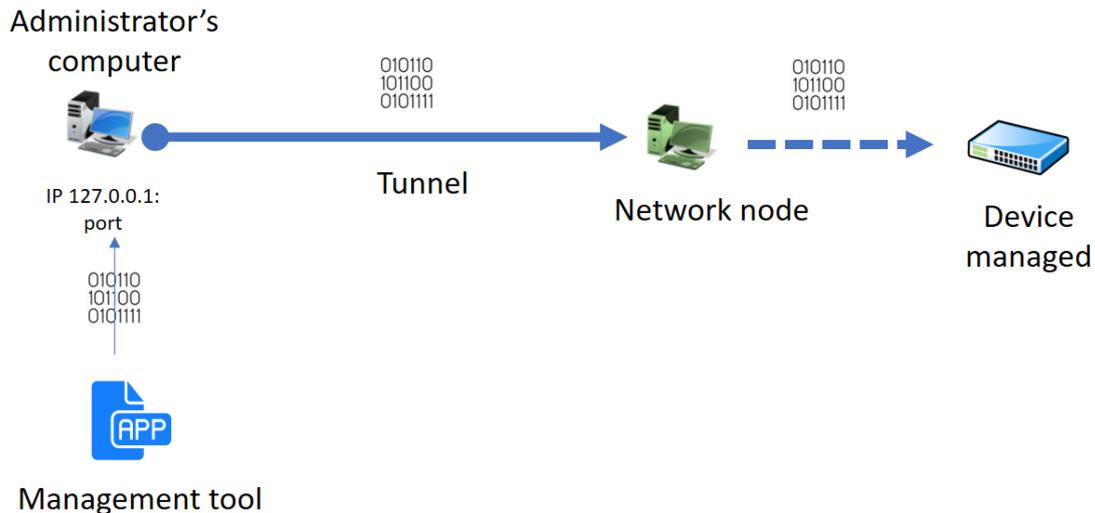


Figure 33: access from the management tool to the managed device

Follow the steps below to access a network device via HTTP:

- 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 (HTTP)** 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 via SSH

- The device to manage must incorporate a remote commandline 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

5.15. Viewing device information

The information gathered from each device is available at the Device Level associated with the relevant device. To access it, go to the general menu Sites, select the site the device belongs to, click the Devices tab and then the device to view. The following general information is displayed.

The Site Level displays the following general information.



Depending on the type of device (server, workstation, smartphone/tablet, ESXi server or network device), some entries may vary or not be available

The information displayed is divided into five categories:

- General device information
- System information
- Administrator notes
- Activity information
- Performance information

General device information

Field	Description	Available for
Description	An editable text description of the device. Initially it contains the device name.	All devices
Groups	Groups to which the device belongs.	All devices
Version	Version of the agent installed.	Windows, Linux, Mac OS X, Android, iOS
Power Rating	A default consumption rating will be assigned depending on the type of device. See later in the chapter for details about how to manage the power consumption of managed devices.	Windows, Linux, Mac OS X, ESXi
Custom field	This field lets you define descriptive labels for the devices. The difference between this and the Description field is that the Custom field is accessible from the scripts run on the devices, as it is a visual way of integrating the result of executing a script in the Console. See Chapter 11: Components and the ComStore for more details.	All devices

Table 9: general device information

System information

Field	Description	Available for
Hostname	Device name	Windows, Linux, Mac OS X, ESXi, Network Devices
Network node	Name of the Network Node computer. Computers with a PCSM Agent installed will display the text localhost, as they don't need a Network Node in order to be monitored and managed.	Windows, Linux, macOS, ESXi, Network Device
UID	Internal device identifier	Windows, Linux, Mac OS X, ESXi, Network Devices
Device Type	Type of device (Unknown, Automatic, Desktop, Laptop, Server, Smartphone, Tablet, Network Device, ESXi Host)	All devices
Domain	Windows domain to which the device belongs	Windows, Linux, Mac OS X
Hyper-V version	Windows Server internal version	Windows Server with the Hyper-V role enabled
Last User	Last user to log in to the device	Windows, Linux, Mac OS X
Status	Status (Online, Offline)	Windows, Linux, Mac OS X, ESXi
Last Reboot	Last time the device was restarted	Windows, Linux, MAC OS X

Field	Description	Available for
Last Seen	Date that the Server last accessed the device	Windows, Linux, Mac OS X, ESXi, Android, iOS
Last Audit Date	Last time a software and hardware audit was performed. See Chapter 12: Assets Audit for more details	Windows, Linux, Mac OS X, ESXi, Android, iOS
Date Created	Date the device was created on the system	Windows, Linux, Mac OS X, ESXi, Android, iOS, Network Devices
Int IP Address	Local IP address of the device	Windows, Linux, Mac OS X, ESXi, Android, iOS, Network Devices
Ext IP Address	IP adress of the router or device that connects the device to the Internet	Windows, Linux, Mac OS X, ESXi, Android, iOS, Network Devices
Additional IP(s)	IP Alias	Windows, Linux, Mac OS X, ESXi, Android, iOS
ESXi Credentials	Access credentials to ESXi servers, defined in the site's Settings tab. Refer to chapter 4 for more information about the settings available for the Account and Site levels	ESXi
Manufacturer		Windows, Linux, Mac OS X, ESXi, Android, iOS
Model		Windows, Linux, Mac OS X, ESXi, Android, iOS
Operating System		Windows, Linux, Mac OS X, ESXi, Android, iOS
Service Pack		Windows, Linux, Mac OS X
Service / Asset Tag	Text string to identify the server	ESXi
IMEI	Mobile device ID	Android, iOS
ICCID	SIM card ID	Android, iOS
Operator	Company that provides the telephone service	Android, iOS
Number	Phone number	Android, iOS
GPS info	GPS coordinates	Android, iOS
Snapshots	Number of snapshots taken from the virtual machines hosted on the ESXi server	ESXi
Guest info	Information about each virtual machine hosted on the ESXi server (Hostname, Guest Name, Operating System, Status). This information is only available if a PCSM Agent is installed on each virtual machine	ESXi
Architecture	32-bit or 64-bit	Windows, Linux, Mac OS X

Field	Description	Available for
Serial Number		Windows, Linux, Mac OS X
Security Center	Status of the protection resources installed on the device	Windows, Linux, Mac OS X
SNMP Credentials	SNMP settings for the device, defined in the site's Settings tab. Refer to chapter 4 for more information about the settings available for the Account and Site Levels.	Network Devices

Table 10: system information



Some fields have a Google search field to provide information about the manufacturer, make or model of the device.

Administrator notes

Here administrators can add reminders and comments as well as procedures for resolving recurring problems with the device to enable collaboration with other administrators.

Activity log

Displays the actions taken on the device. This is a summary of the information displayed in the **Reports** tab, selecting the **Activity** box. You can reach this screen directly by clicking the **more...** link at the bottom of the list.

Type	Name	Started	Ended	Status
	VNC Remote Takeover by panda.test	2014-10-28 16:22:53 CET	2014-10-28 16:23:13 CET	
	VNC Remote Takeover by panda.test	2014-10-28 16:21:38 CET	2014-10-28 16:22:34 CET	
	Screenshot by panda.test	2014-04-03 09:08:55 CEST	2014-04-03 09:08:55 CEST	
	Screenshot by panda.test	2014-04-03 09:06:43 CEST	2014-04-03 09:06:43 CEST	
more...				

Figure 34: Activity log

Performance

The Console displays three line graphs showing usage of the CPU, the memory and the hard disk. It also indicates the time the device has been operating.

- Disk usage (a line for each disk on the device)

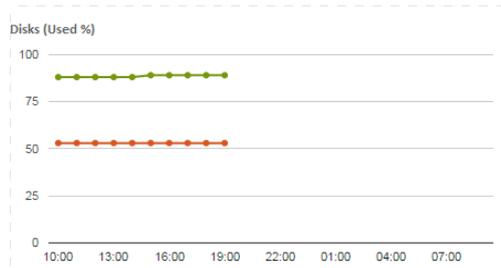


Figure 35: Disk usage chart

- Memory usage

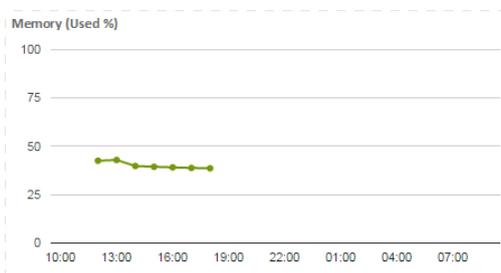


Figure 36: Memory usage chart

- CPU usage

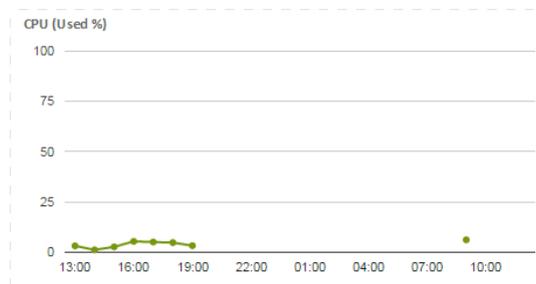


Figure 37: CPU usage chart

- Total time that the device has been powered on (on the current day)



Figure 38: device uptime

- **Scale**

Lets you define the time period displayed in the charts:

- 24 hours
- 1 week
- 1 month

5.16. Managing device resource consumption

Panda Systems Management lets you automate the monitoring of managed devices' resource consumption. This requires an initial configuration, which although largely established in the default settings, may require an adjustment. It is therefore advisable to adjust the real resource consumption values to reflect the reality in each country/company infrastructure.

The complete cycle of resource consumption management is divided into three sections:

- Specification of the type of device.
- Specification of resource consumption by type of device.
- General consumption view.

Each section is described below.

5.16.1 Specifying the type of device

Panda Systems Management distinguishes among four major groups of devices with regard to consumption.

- Desktop
- Laptop
- Server
- Others

The system automatically assigns the type of device that best describes each managed device, though if this is not accurate, the value can be changed in the corresponding Device Level in the **Summary** tab.

5.16.2 Specifying the power rating for each type of device

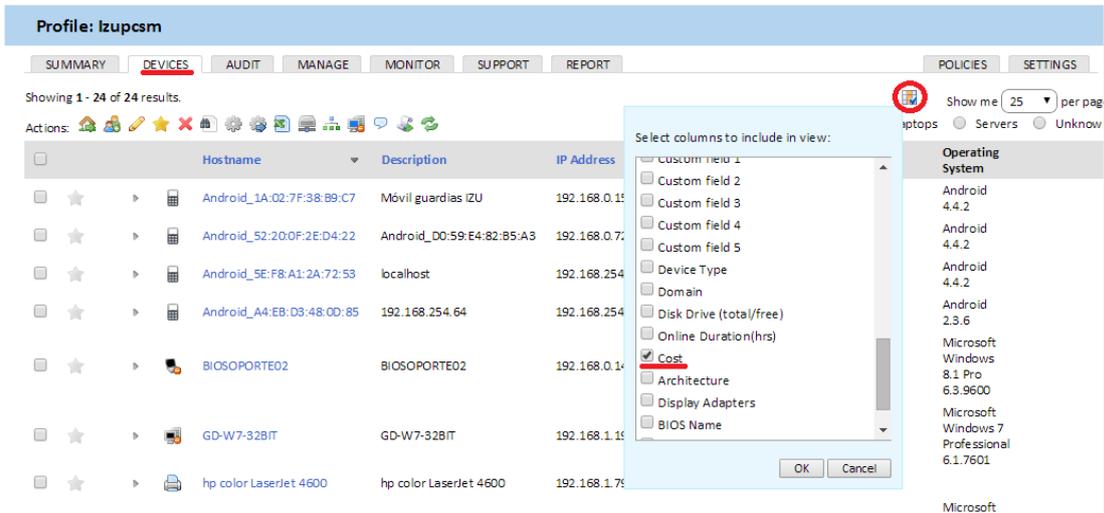
By default, the system assigns specific power ratings for laptops, smartphones and servers. These are average values calculated according to typical hardware configurations.

- How to change these values for all managed sites: Go to general menu **Setup, Account Settings** tab, **Power Rating** section. Enter the watts consumed for each type of device.
- How to change these values for a specific site: Click the **Settings** tab of the selected site.

As electricity prices vary enormously from country to country, and even across regions, it is also possible to specify the cost per Kwh.

5.16.3 General power rating view

To view the consumption for each device, select **Cost** in the list of site devices.



The screenshot shows the 'DEVICES' tab for profile 'Izupcsm'. A modal dialog is open over the device list, titled 'Select columns to include in view:'. The 'Cost' option is checked in the list of columns. The device list shows columns for Hostname, Description, and IP Address. The 'Operating System' column on the right shows various OS versions like Android 4.4.2 and Microsoft Windows 8.1 Pro.

Hostname	Description	IP Address
Android_1A:02:7F:38:B9:C7	Móvil guardias IZU	192.168.0.11
Android_52:20:0F:2E:D4:22	Android_DO:59:E4:82:B5:A3	192.168.0.71
Android_5E:F8:A1:2A:72:53	localhost	192.168.254
Android_A4:E8:D3:48:0D:85	192.168.254.64	192.168.254
BIOSOPORTE02	BIOSOPORTE02	192.168.0.11
GD-W7-32BIT	GD-W7-32BIT	192.168.1.11
hp color LaserJet 4600	hp color LaserJet 4600	192.168.1.71

Figure 39: Screen for selecting the data displayed on the device list

6. Filters and groups

What are groups and filters?

Types of groups and filters

Groups

Filters

6.1. What are groups and filters?

Groups and filters are resources for generating clusters of devices in a similar way to sites but more easily and dynamically. So, while sites consider static aspects of devices such as membership to a specific customer account or office, groups and filters are designed to be easily modified in response to temporary characteristics or criteria of the devices.

6.2. Types of groups and filters

There are various types of groups / filters:

- **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.



Filters and groups can be inter-site device groups; depending on the level where they are generated, they can include devices from one or various sites.

6.3. Groups

Groups are groups of static devices. A device is manually assigned to a group by direct allocation by an administrator. A single device can belong to more than one group.

6.4. 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.

6.4.1 Predefined 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 filters are organized into seven groups:

- **Application:** This group contains filters for applications such as Adobe Flash, Java, Microsoft Office, etc.
- **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.
- **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.)

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.
	Mozilla Firefox	Shows devices with the Mozilla Firefox browser installed.
	SQL Express	Shows devices with the Microsoft SQL Express personal database installed.
Backup Solution	Acronis TruImage	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	< 2 GB Free Space	Shows devices with less than 2 Gigabytes of free space on any of their hard disks.

Category	Filter	Use
	< 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.
Operating System	All Desktop O/S	Shows all desktop devices.
	All Server O/S	Shows all server devices.
	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.
	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 XP	Shows all devices with Microsoft Windows XP.
Mac OSX	Shows all devices with Mac OS X.	
Role	DHCP Server	Shows all devices that operate as a DHCP server on the network.

Category	Filter	Use
	DNS Servers	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 Servers	Shows all devices on the network that act as hosts for virtual machines, based on Microsoft Hyper-V technology.
	SQL Servers	Shows all servers with SQL Server or Microsoft SQL Server Express on the network.
	IIS Webservers	Shows all devices on the network that act as Web servers running Internet Information Server.
	Print Servers	Shows all devices on the network that act as print servers.
	SQL Server	Shows all devices on the network that act as database servers.
	Sharepoint Servers	Shows all devices on the network that act as Sharepoint servers.
	WSUS Servers	Shows all devices on the network that act as WSUS update servers.
Security Software	AVG	
	Avira	
	ESET	
	McAfee	
	Panda	
	Sophos	

Category	Filter	Use
	Symantec	
	Trend Micro	
	Webroot	
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. See Chapter 5 for more details on this role.
	Offline > 1 Week	Shows switched off devices or devices that have been offline for more than one week
	Offline Desktop O/S	Shows 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.
Type	Reboot > 30 Days	Shows all devices that haven't been rebooted in over 30 days.
	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 Network Devices	Shows all network devices managed by PCSM. See Chapter 5 for more details on network devices.
	All Network Printers	Shows all printers installed on the network and managed by PCSM.
	ESXi	Shows the ESXi hosts (ESXi servers) managed by PCSM.
	Physical Servers	Shows all physical servers (not virtual).

Category	Filter	Use
	Virtual Machines	Shows all virtual servers managed by PCSM.

Table 11: List of predefined filters



The predefined filters are not editable.

6.4.2 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	Empty – Not empty, Contains – Does Not contain, Starts with – Does not start with, Finishes with – Does not finish with	String. Use % as a wildcard.

Field	Condition	Value
Integer	Greater – Greater than or equal to, Less – Less than or equal to, Includes, Excludes	Numeric.
Binary	Enabled / Disabled	
Date	Before – After, Older than 30/60/90 days	Date interval
Selection	Is a member of, is not a member of	Available groups

Table 12 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.



Figure 40 Logical OR operator between two attributes

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 (Yes/No)	Lets you filter devices with the Windows Update engine enabled or disabled
Display adapter	Lets you filter by the name, make and model of the graphics card installed on the device.
Network adapter	Lets you filter by the make and model of the network adapter installed on the device.
Antivirus (Yes/No)	Lets you filter devices by the status of the antivirus installed (enabled/disabled)

Attribute	Description
Attached device driver file	Lets you filter by the driver file field of the external USB drives connected to the device. Refer to Chapter 12: Assets Audit for more details.
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
Disk size	Lets you filter devices by the size of the hard disk
Disk free space	Lets you filter devices by the free space on the hard disk
Attached device driver modified	Lets you filter by the Driver modified field of the external USB drives connected to the device. Refer to Chapter 12: Assets Audit for more details.
Description	Lets you filter devices by the value of the Description field Refer to Chapter 5: Devices for more information
Site description	Lets you filter devices by the Description field of the site to which the device belongs
Disk description	Lets you filter devices by the value of the Description field of the internal storage devices connected to the computer.
IP address	
Additional IP address	Lets you filter devices by the IP alias
External IP address	Lets you filter devices by the IP address used to connect to the Server
MAC address	
Managed devices	Not used.
OnDemand devices	Not used.
Domain	Lets you filter devices by the domain the device belongs to on Microsoft networks
OnDemand sites	Not used.
Status - Online/Offline	
Status - Web port OK	Not used.
Status - Suspended	
Manufacturer	Company that assembled the device.
Attached device driver manufacturer	Lets you filter devices by the Driver manufacturer field of the external USB devices connected to the computer. Refer to Chapter 12: Assets Audit for more details.
Favorite	Lets you filter devices marked as favorite
BIOS release date	
Last seen date	Date when the device was last seen by the Server
Firewall (Yes/No)	Lets you filter devices by the firewall status (enabled/disabled)
Site device group	Lets you filter devices by the name of the site group the device belongs to
Device group	Lets you filter devices by the name of the system group the device belongs to

Attribute	Description
Memory	Lets you filter devices by the amount of memory installed on the device
Model	
SNMP monitor	Lets you filter those devices with the Connection Broker role
Monitor / screen	
BIOS name	
Attached device driver name	Lets you filter devices by the value of the Driver name field of the external USB devices connected to the computer Refer to Chapter 12: Assets Audit for more details.
Attached device name	Lets you filter devices by the value of the Device field of the external USB devices connected to the computer. Refer to Chapter 12: Assets Audit for more details.
Host name	
Site name	Lets you filter devices by the name of the site to which the device belongs
Attached device driver name/version	Lets you filter devices by the value of the Name/Version field of the external USB devices connected to the computer Refer to Chapter 12: Assets Audit for more details.
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
Patch Title (installed)	Lets you filter devices by the name of a patch installed on the device
Custom field 1-10	Lets you filter by the content of the specified custom field (1 to 10). Refer to Chapter 5: Devices for more information
Motherboard	Lets you filter by the manufacturer, make and model of the device's motherboard
Attached device driver port	Lets you filter devices by the content of the Driver port value of the external USB devices connected to the computer. Refer to Chapter 12: Assets Audit for more details.
Service Pack	
Operating system	
Device type	
Attached device driver type	
BIOS name	
Software version	Lets you filter devices by a specific software package version installed on the computer.
Agent version	
Attached device driver port	Lets you filter devices by the content of the Driver port value of the external USB devices connected to the computer. Refer to Chapter 12: Assets Audit for more details.
Reboot required	Lets you filter the devices that require a reboot in order to complete an action, such as the installation of security patches, etc.

Attribute	Description
Last audit	Date of the most recent hardware/software audit on the device. Refer to Chapter 12: Assets Audit for more details.
Last user	Lets you filter devices by the last user to log on to the device.

Table 13: Attribute list

7. Managing devices efficiently

Differences between sites, groups and filters

General approach and device management structure

Quick view of device information

7.1. Introduction

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.

7.2. Differences between sites, groups and filters

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

7.2.1 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.

7.2.2 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.

7.3. General approach and device management structure

The following general rules are applied:

- **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 Chapter 16: User account and security levels.

7.4. Quick view of device information

Once the devices are organized correctly, it is important to be able to access the information rapidly at a glance. The management Console displays lists of devices with information fields that can be configured by the administrator.

To configure the information displayed in any list of devices, you have to click the  icon:

This icon is accessible from any list of devices (sites, groups or filters). The options available are as follows:

Field	Description
UID	The device's internal ID
Site	Name of the site to which the device belongs
Host name	Name of the device
Description	
IP Address	Local IP address of the device
Addit. IP's	IP Alias
Ext IP Addr	IP address of the router or device that connects the device to the Internet
Last User	Last user to log in to the device.
Group	
Date Created	Date the device was created in the system.
Last Updated	The last date the Server accessed the device.
Last Audited	Date of the last software and hardware audit. Refer to Chapter 12: Assets Audit for more details.
Session Name	Not in use
Favorite	Bookmarks the device for quick access from the system dashboards.
Privacy Mode	Privacy mode on the device.
Agent Version	Minor agent version
Display Version	Full agent version
Web Port OK	The device can connect to the Web service for downloading branding items, components, updates, etc.
SNMP monitor	The Agent has the Connection Broker role enabled

Field	Description
Status	Status (Online, Offline). Online indicates that the Agent can connect to the Control Channel to send 'keep alives'.
Model	
Operating System	
Service Pack	
Serial Number	
Motherboard	
CPU	Make, model, and CPU speed.
Memory	Amount of memory installed.
MAC Address(es)	
Custom field 1-10	Content of the Custom Fields defined. Refer to Chapter 11: Components and the ComStore.
Device Type	Type of device (workstation, laptop, tablet, smartphone, printer, network device, ESXi host).
Domain	Windows domain that the device belongs to.
Disk Drive (total/Free)	Total space and free space of all drives installed on the device.
Online Duration (hrs)	
Cost	Cost corresponding to the device based on its consumption. Refer to Chapter 5: Devices.
Architecture	32-bit or 64-bit
Display Adapters	Make and model of the graphics card installed on the device.
BIOS Name	Make and model of the BIOS.
BIOS Release Date	
BIOS Version	
Last Reboot	Last time the device was restarted.
Reboot required	Indicates whether a device requires a restart to complete the installation process.

Table 14 Data fields available on the Devices tab

Once the view has been configured, click on the column names to establish the most convenient criteria to organize the fields.

8. The first 8 steps to start using Panda Systems Management

- Creating and configuring the first site
 - Deploying the agent
- Checking the site's device list and basic filtering
- Hardware, software and license audit
 - Patch management
 - Creating monitors
 - ComStore
- Accessing resources on the remote managed devices

8.1. Introduction

This chapter provides a summary of the steps to take to start using **Panda Systems Management** with a managed Windows device.

8.1.1 Current startup status of Panda Systems Management

You can see whether the service startup process has been completed through a section of the administration console which graphically displays the deployment status of the service on the customer's network.

To see this, click the general menu **Sites**. At the bottom of the screen there is a wizard with three steps, which also indicates the progress of each step:

- Step 1: Deployment of the agent on the devices
- Step 2: Monitor creation
- Step 3: Audit execution, patch management, policy configuration

These three steps are described in detail later in this chapter.

8.2. Creating and configuring the first site

First you must determine whether to create a new site or reuse one already in use, depending on the management criteria you are using. A new customer account will generally correspond to a new site.

In general menu **Sites**, click **New site** and fill in the necessary information. Keep in mind that the **Description** field may be used by the filters you add and that refer to the content of this field.

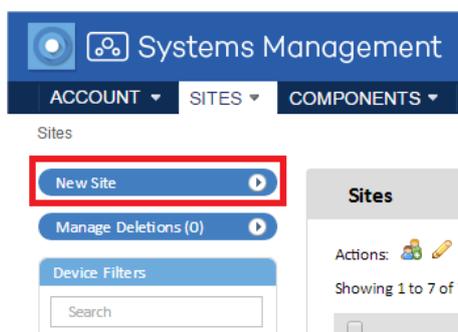


Figure 41: create site button

If the devices in the site require additional information about the HTTP proxy used to access the Internet, this information can be provided here or can be added later.

After creating the site, it is advisable to configure it through the **Settings** tab. This configuration will be incorporated in the Agent installed on each managed device.

8.3. Deploying the Systems Management Agent

The Agent installed on the customer's devices requires certain basic information in order to operate:

- The site to which it will belong.
- Minimum information required to connect to the Internet and connect to the Server.

The site to which the Agent belongs is set automatically if the downloading or sending of the download link is done through the site.

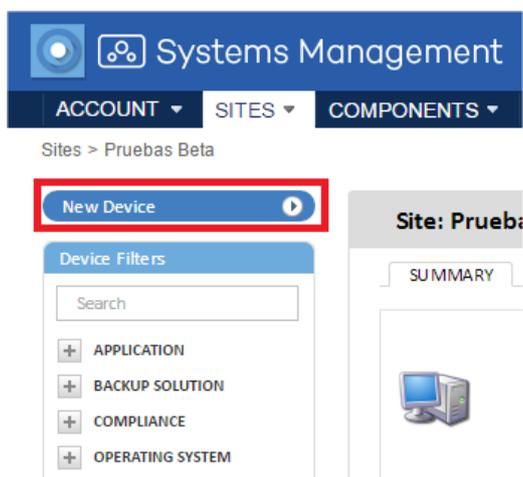


Figure 42: add device button

The Internet connection data was specified in the previous step when creating the site or in tab bar, **Settings**, so that the Agent downloaded will already contain this information.

The Agent can be downloaded in three ways:

- Sending the Agent via email
- Sending the download URL via email
- Direct download

8.4. Checking the site's device list and basic filtering

You can mark devices as favorite to access them more quickly, arrange lists, quickly filter them according to the role of the device, and change the size of the list to display more or fewer items.

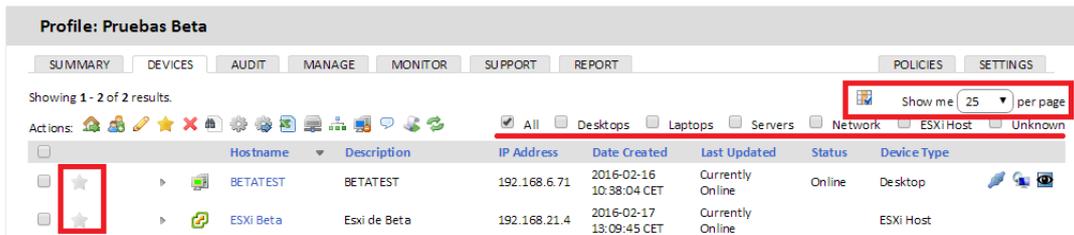


Figure 43: computer list filters

8.5. Hardware, software and license audit

Tab bar, **Audit** contains all of the audit details of the devices belonging to the site or if accessed at Device Level, it will display detailed information about the device. For more information about inventories, see Chapter 12: Assets audit

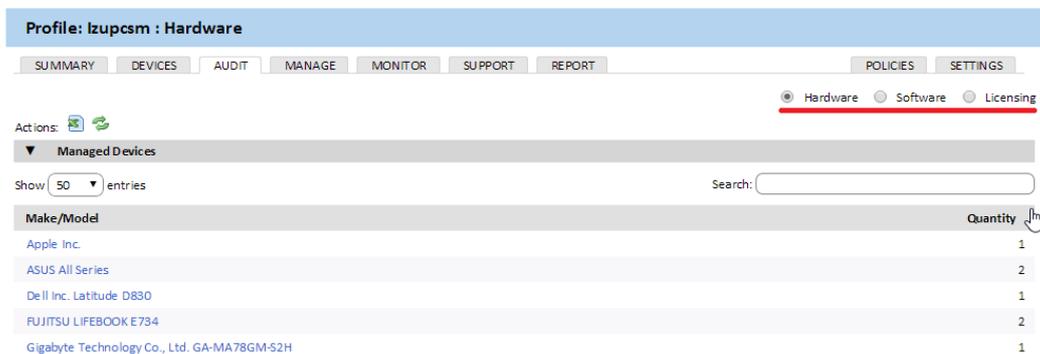


Figure 44: hardware inventory window

8.6. Patch management

Approve the patches that have not been installed on your managed devices or rollback those you want to uninstall from **tab bar, Manage**.

Configure when to apply patches to the devices in the site, the steps to be taken once applied, and other parameters by creating a **Windows Update** or **Patch Management** policy from **tab bar, Policies** in the site. For more information about Patch Management, refer to Chapter 15: Patch management and Chapter 9: Policies.

8.7. Creating monitors

To implement monitoring of network devices, monitors have to be installed and set up. These monitors then notify the **Server** when any devices do not meet the criteria established in a given period of time.

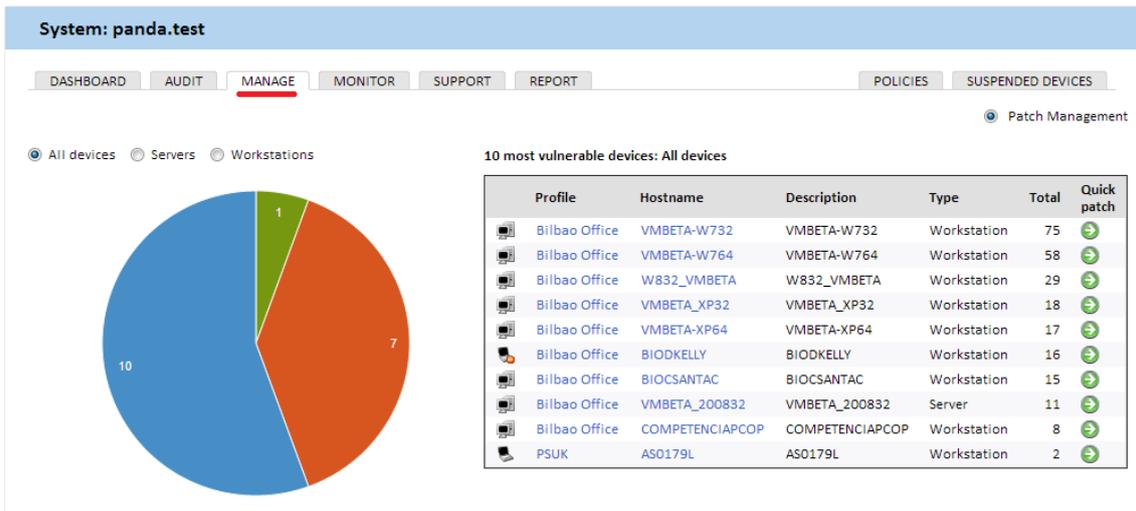


Figure 45: patch management window

Panda Systems Management automatically configures certain monitors depending on the type of device that has been added to the administration console. This way, administrators don't need to spend time setting up a basic set of monitors to display the status of their devices.

There are also monitors that can be imported in order to get the most from the service right from the outset.

You can add additional monitors from the **general menu Account** or from a specific site in **tab bar, Policies**, by clicking **Add Site Policy**.

In Type, select Monitoring.

The 'Create a policy' window shows the following fields:

- Name:** MyMonitor
- Type:** Monitoring (selected from a dropdown menu)
- Based on:** - New Policy - (selected from a dropdown menu)

Buttons for 'Cancel' and 'Next' are visible at the bottom right.

Figure 46: create policy window

Add a target (one or various groups or filters) and a monitor. On adding a monitor, a 4-step wizard appears where you can configure the necessary settings.

For more information about monitoring, refer to Chapter 10: Monitoring.

Create a monitoring policy

Name:

Policy type: Monitoring

Last updated: 2013-05-22 09:55:39 UTC

Last deployed:

Targets:

Type	Name
There are currently no targets specified.	

[Add a target...](#)

Monitors:

Category	Type	Alert If	Respond	Ticket	Severity
There are currently no monitors specified.					

[Add a monitor...](#)

Figure 47: policy settings window

8.8. ComStore

ComStore is a repository of predefined components that enhances the **Panda Systems Management** service and enables the centralized installation of third-party software.

Figure 48: comstore section

The components used directly by the partner/IT Manager must be downloaded from the **ComStore**.

To download a component, select it and click **Buy**. It will be immediately added to **My Components**.



All components in the ComStore are free

Depending on the component type, it can be run as a job or in response to an alert generated by a monitor.

In **tab bar, Devices**, within the site, select the devices to which to apply the component and choose between **Schedule a Job**  and **Run a quick Job**. 



For more information about how to develop and deploy components, refer to Chapter 11: Components and ComStore. For more information about how to install applications on Windows, Mac and Linux computers, as well as on iOS tablets and smartphones, refer to Chapter 13: Centralized software deployment and installation. For a list of components published by Panda Security in the ComStore along with descriptions and instructions, refer to Appendix C.

8.9. Accessing resources on the remote managed devices

Although many daily operations can be performed directly from the Console, it may be necessary to directly access the device through the Agent. This requires installing the agent on technicians' devices so that they can provide remote support and log in with their user name and password.

Follow the steps below to access a device via the PCSM Agent:

- Install the Agent on the device of the technician that will provide remote support.
- Select the site the device belongs to.
- Click the  icon to expand the device's context menu. Alternatively, click the device's name and then click the  icon of the **Summary** tab.
- Select **Connect to Device**. The PCSM Agent will open and connect automatically to the device.
- After locating the device, all of the remote access and remote control options will be accessible through both the icons and menus.

The options that do not prevent the user from continuing to work on the system are:

- **Remote screen capture:** Rapid viewing of error messages.
- **Windows Services Tab:** Remote access to stop, start and restart services without needing to access the remote desktop,
- **Screen Sharing Session:** Shared remote desktop. The user sees what the technician is doing on the device
- **Command shell:** Remote DOS command line.
- **Agent deployment:** Deploy the Agent across the LAN.
- **Task manager:** Remote access to the task manager without needing to access the remote desktop.

- **File transfer:** Provides full access to the target device's file system, allowing the administrator to transfer files between their computer and the user's computer, as well as move files, create and delete folders and rename items.
- **Drive information:** Lists the current local and network drives connected to the device, allowing the administrator to add or delete network paths.
- **Registry editor:** Remote access to the regedit tool without needing to access the remote desktop.
- **Quick Jobs:** Launch Jobs.
- **Event viewer:** Remote access to the event viewer without needing to access the remote desktop.
- **Wake Up:** Allows a device that is switched on to send the rest of the devices in the same LAN segment a "magic packet" to switch them on remotely.

The options that will prevent the user from using the device are:

- **Windows RDP:** Remote desktop access via RDP, which will close the user's session.
- **Shut Down / Reboot:** Shut down or restart the target device.

9. Policies

What are policies?

Creating policies

Managing policies

How to deploy a policy

Importing and exporting policies

Policy types

9.1. What are policies?

Policies are used to implement specific management or remediation actions scheduled to be repeated at regular intervals over a specific period of time, or triggered when certain conditions are met on one or various managed devices.

Policies are configuration containers 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 levels available, depending on the number of devices and whether they belong to the same customer or various:

- **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 or Site Device Groups.
- **Device policy:** Defines an action to apply to a specific device.

9.2. 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 one of the sites previously created, 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**, select one of the sites previously created, and click the device that the policy will be assigned to. Then, click the **Monitor** tab, and the **Add a monitor** button at the bottom of the window.



At Device Level you can only add monitor-type policies. Refer to chapter 10 for more information about 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).

9.3. Managing 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.

9.3.1 Managing policies at Account Level

Go to general menu Account, **Policies** tab. A window will be displayed showing all policies created at Account Level, along with their associated information:

- **Name:** The name of the policy.
- **Targets:** Groups of devices to which the policy will be applied.
- **Type:** The type of policy. More information about the policy types supported by **Panda Systems Management** is provided later in this chapter.
- **Enabled (ON/OFF):** Enables/disables the policy.

Also, the following five additional controls are available:

- **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 15 for more information about policy inheritance.
- **Push changes:** Deploys the policy to all devices selected as a target.
-  : Lets you view the 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.

9.3.2 Viewing the devices affected by a policy

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

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

9.4. 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, click **Push changes**. This will apply the policy to all of the affected devices, triggering its execution.

9.5. Policy types

There are eight types of policies, summarized below:

9.5.1 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:** Hides the icon displayed in the notification area next to the Windows clock . This prevents 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.**
- **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 in administrator mode.
 - **Admin:** The Agent is run will full permissions.

9.5.2 ESXi

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



Refer to Chapter 10: Monitoring for more information.

9.5.3 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.

9.5.4 Monitoring

This policy allows you to add device resource monitoring processes.



Refer to Chapter 10: Monitoring for more information.

9.5.5 Patch management

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



Refer to Chapter 15: Patch Management for more information.

9.5.6 Power

This policy allows configuration of the power saving settings on the devices that support them.

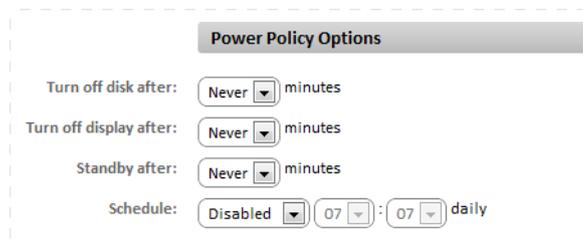


Figure 49: power policy settings

9.5.7 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 15: Patch Management for more information.

9.5.8 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.



Refer to Chapter 17: Mobile Device Management for more information.

10. Monitoring

Monitor composition

Creating monitors manually

Importing Comstore monitors

Importing and exporting

Monitoring printers

Creating SNMP monitors

Creating ESXi monitors

10.1. Introduction

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.

10.2. Monitor composition

A monitor consists of four groups of settings:

- **Monitor type:** Specifies its function.
- **Monitor 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 14: Ticketing).

10.3. Creating monitors manually

Just as with policies, you can create monitors manually at the three available levels, depending on the devices to be monitored:

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

10.3.1 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.

Monitor name	Function	Available for
Online Status Monitor	Checks whether the device is online	Windows, Mac, Linux, ESXi, Network Device
CPU Monitor	Monitors CPU usage	Windows, Mac, Linux
Memory Monitor	Monitors memory usage	Windows, Mac, Linux
Component Monitor	Launches a Monitor component from the ComStore or designed by the administrator	Windows, Mac, Linux
Process Monitor	Monitors the status of a specific process	Windows, Mac, Linux
Service Monitor	Monitors the status of a specific service	Windows
Event Log Monitor	Monitors the event viewer	Windows
Software Monitor	Monitors the software installed on or uninstalled from the device	Windows
Security Center Monitor	Monitors the status of the operating system Security Center	Windows
Disk Usage Monitor	Monitors hard disk usage	Windows
File/Folder Size Monitor	Monitors the size of files and folders	Windows
Patch Monitor	Monitors the installation of the patches scheduled using Panda Systems Management's Patch Management module.	Windows
Ping monitor	Monitors device connectivity via the ICMP protocol, checking the proper operation of the network.	Windows
SNMP Monitor	Monitors network devices compatible with the SNMP protocol.	Windows, Mac, Linux, Network Device
SNMP Throughput Monitor	Monitors the bandwidth consumption of the network devices, detecting overload conditions and device failure.	Network Device
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

Monitor name	Function	Available for
Windows Performance Monitor	Monitors certain operating system metrics associated with running processes, triggering alerts if certain values fall under the established thresholds.	Windows
Printer Monitor	Monitors your printers, displaying the current status of printer consumables and triggering alerts if certain values fall under the established thresholds.	Network printer

Table 15 List of available monitors

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:** You can specify the time required for an alert to be considered automatically resolved.

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.

10.4. Importing ComStore monitors

Panda Systems Management helps speed up the process of configuring monitors for the devices that make up an organization's IT infrastructure by providing 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**.

10.5. Importing and exporting a monitoring policy

10.5.1 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.

10.5.2 Exporting monitoring policies

In Install command, enter the installation command line that will run the package comparativa de politicas de aplicación:

- 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.

10.6. Monitoring printers

Panda Systems Management adds preconfigured monitors automatically as soon as new devices are incorporated into the management platform. Therefore, as soon as you add a printer to the console, the **Policies** tab of the relevant site will display a new monitor.

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

10.7. Creating SNMP monitors



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.

10.7.1 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.

10.7.2 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 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 **Systems Management Agent** 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 or similar.

2 Designate a device with a Systems Management Agent installed as the Network Node

Refer to Chapter 5 Devices for more information about how to assign an Agent the role of Network Node.



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

Refer to Chapter 5 Devices for more information about how to add to the management Console those devices that do not support installation of the Systems Management Agent.

4 Create 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.

Follow the steps below to create an SNMP monitoring policy:

- Establish the level of the policy to create (Account, Site, Device).
- Click the **Policies** tab of the relevant Level (Account or Site). To create a monitor at Device Level, click the **Monitor** tab and select the **Monitors** radio button in the top right corner of the window.
- Click the **New account policy** button (Account Level), **New site policy** (Site Level), or **Add a monitor** (Device Level).
- Enter a name for the policy and select **Monitoring** from the drop-down menu.

- If you are creating a site or account policy, click the **Add a target** button to define the policy scope.
- Click the **Add a monitor** button and select **SNMP Monitor**. A configuration wizard will be displayed.
- In the **SNMP OID to Query** field, specify the **SNMP Object Identifier** that you want to monitor.
- In **Alert Settings**, enter the conditions that must be met to consider that a device is malfunctioning. To monitor situations where the device is not responding to the SNMP requests, select the **Alert when OID is not responding** checkbox.
- 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.
- In **Alert Details**, select the severity of the alerts.
- In **Auto-Resolution Details**, specify if the alert will be resolved automatically after a certain period of time.

5 Import an SNMP monitoring policy (optional).

The **ComStore** provides policies for monitoring the most common network devices. Follow the steps below to use one of these components:

- Go to general menu **ComStore, Monitoring Policies**.
- Click the **Add to Account Policies** button associated with the policy you want to use.
- A window will open for you to configure the policy (policy target and other monitor parameters).



Panda Systems Management's SNMP components give visibility into the internal status of managed devices not compatible with the Agent. Writing to the devices' MIB or receiving SNMP traps is not supported.

10.8. Creating ESXi monitors

ESXi servers require a specific type of monitor, different from the one used to monitor devices compatible with the PCSM Agent.

10.8.1 How to create an ESXi monitor

1 Choose the policy type

As this is an ESXi monitor, select **ESXi**.



You can create ESXi policies at Account and Site Level. It is not possible to create an ESXi policy at Device Level.

2 Add a target

Select the devices or device groups to be monitored, and the type of monitor to add to the policy.

Click the **Add a monitor** option to display a four-step wizard for you to enter the necessary settings.

3 Choose the monitor type

Specify the type of monitor to add to the policy based on the resources to be monitored on the ESXi server.

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.
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 server's status

Table 16: list of monitors compatible with ESXi servers

4 Configure the monitor

To configure an ESXi monitor, follow the same steps as with a device compatible with the PCSM Agent. The procedure to follow was explained earlier in this chapter.

5 Set the monitor response

To configure the ESXi monitor response, follow the same steps as with a device compatible with the PCSM Agent. The procedure to follow was explained earlier in this chapter.



It is not possible to run a ComStore component in response to an event generated by an ESXi monitor.

6 Create the tickets

To generate the tickets, follow the same steps as with a device compatible with the PCSM Agent. The procedure to follow was explained earlier in this chapter.

11. Components and ComStore

What is a component?

Using components in Panda Systems Management

Developing components

Creating a monitor component

Creating a script component

Editing components

11.1. What is a component?

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

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**.

11.1.1 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 Chapter 13: Centralized software deployment and installation.

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).

- **Monitor**

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 monitor component to the policy.

- **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 scheduled job	or 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	Site or account policy	60 seconds (fixed interval).	Monitor devices.
Scripts	Quick job scheduled job	or At the time or creating the component or when scheduled.	Run applications developed by the administrator.
Network Monitors	Device policy	60 seconds (fixed interval).	Monitor devices not compatible with a Systems Management Agent .

Table 17: 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 monitor-type components created by the administrator.

11.1.2 Components developed by Panda Security

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.

11.2. Using components in the platform

11.2.1 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 the **general menu, ComStore** to access the library of components developed and certified by **Panda Security** and made available to the **Panda Systems Management** customers.

To add a component from the **ComStore** to the **Component List**, simply 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 **Buy** to add the component to the **Component List**.

Searching for components in the ComStore

To search for components, go to **ComStore** and use the panel on the left. This panel classifies the components that **Panda Security** adds to the **ComStore** in the same way as the **My Components** panel of the **Components** section. You can also use the search tool on the upper right side of the screen to search for components by their name.

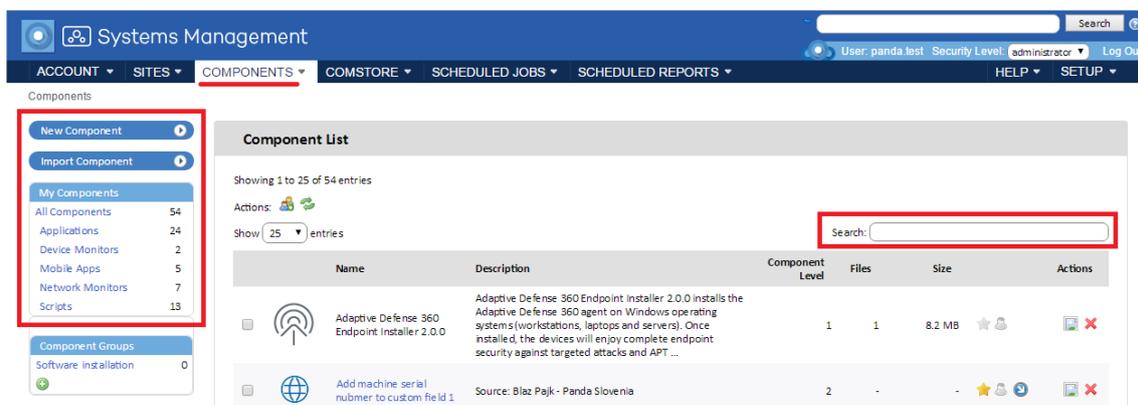


Figure 50: component search tools

Importing components

To import a component directly from the PCSM Console, go to the general menu, **Components**, and click **Import Component**

You can only import components previously exported from the PCSM Console. To export a component to disk, click the arrow icon in the component list.

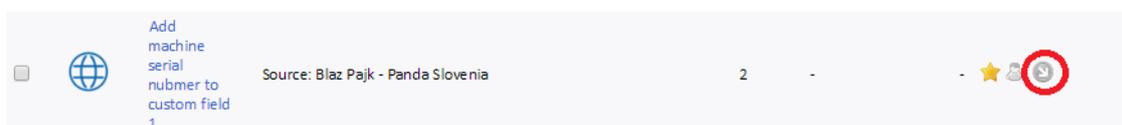


Figure 51: icono para exportar una componente

Sorting and classifying the integrated components

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

The **My Components** section on the left hand side of the screen classifies all integrated components automatically based on their functionality. Six categories are available:

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

Also, administrators can create new component groups by using the component grouping tool located under the Component List.



Figure 52: creating new component groups

Follow the steps below to create a component group:

- Go to general menu **Components**.
- Click the  icon. A window will open for you to enter the name of the new component group.
- Enter a name and click **Save**.
- Select the components to group and click the  icon.
- A window will be displayed listing all available component groups. Select the group to add the selected components to.

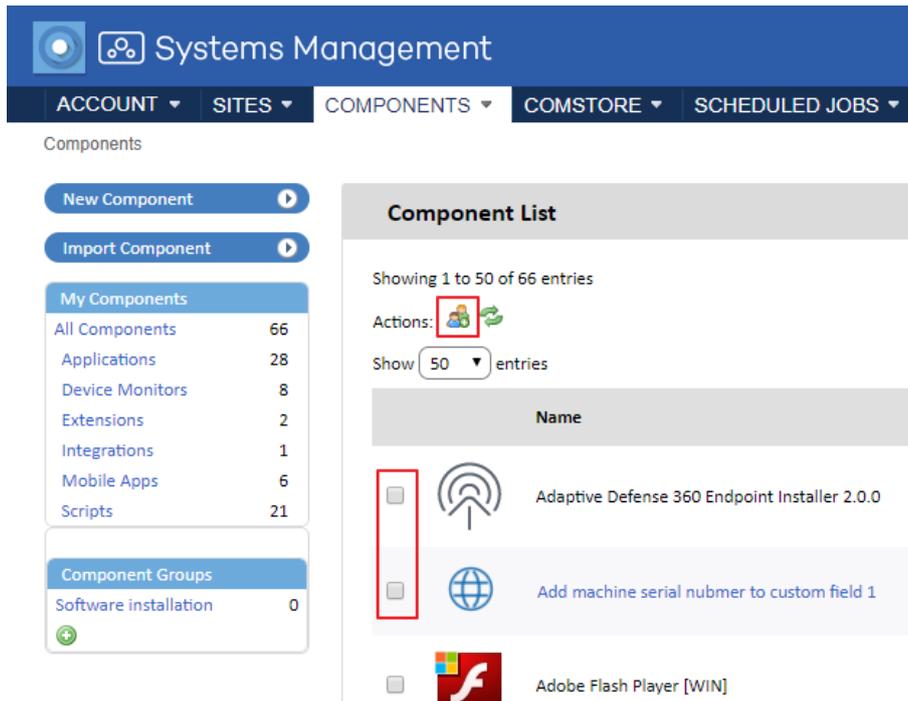


Figure 53: adding components to a group

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 update** of the **ComStore**.

ComStore	
<u>Check for Updates</u>	5
All Components	268
Applications	149
Integrations	1
Device Monitors	33
Network Monitors	30
Scripts	54

Figure 54: component update (global)

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**.



Figure 55: component update (individual)



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.

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**.

11.2.2 Using components from a Quick Job

Scheduled Jobs tab

After a Quick Job has been launched, you can view the results in the **Scheduled Jobs** tab, which shows both Active Jobs and Completed Jobs.

Follow the steps below to run a component integrated into Panda Systems Management through a quick job:

- Go to general menu **Components**.
- From the component list, click the  icon of the component you want to run.

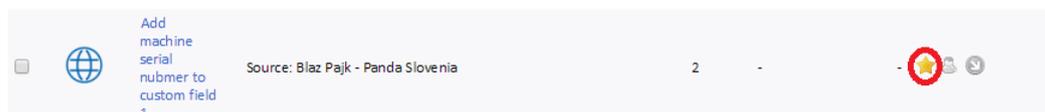


Figure 56: selecting a component to be used in a quick job

You can add as many components as you want to your workspace and select those you want to

Follow these steps to configure a quick job:

- Select the computers that the job will be applied to, and click the  icon you'll find on the icon bar.
- The quick job icon can be found on the icon bar at Account Level, Site Level and Device Level. That is, you can launch a quick job on all the devices included in one or multiple sites, on several computers in the same site, and on one single device, respectively.
- Select the component to run from the drop-down menu displayed. Only those components that have been previously added to the quick job list using the  icon will be displayed.

Active Jobs

This tab shows queued jobs awaiting execution. You can use the available toolbar to filter the results.

Completed Jobs

This tab shows every completed job, along with an error code indicating the job result.

11.2.3 Using components from a Scheduled Job

Scheduled Jobs are just like Quick Jobs, the only difference being that they are scheduled to be run later. Scheduled Jobs require entering more information to create them, for example, the time at which the job will be run, its frequency, how many times the job must be run before it is considered finished, etc.

To configure a Quick Job, go to the **Icon bar** at Account, Site or Device Level and click the Scheduled Job icon . A window will open for you to enter the relevant settings.

Execution cycle

To set the execution cycle, click **Click to change** in the **Schedule** section. Depending on the frequency that you choose (daily, weekly, etc.), the panel on the right will display different options for you to specify the execution dates.

Component selection

Click the **Add Component** link to open a window for you to select the component to run.

Job end date

This section lets you enter the date when the job stops repeating and is considered finished.

Additionally, it lets you force the computers where the Scheduled Job is to be run to have an interactive session open.

Alerts

This section lets you generate alerts if any of the configured conditions is met. Use the **Job Recipients** section to enter email addresses to send the alerts to multiple recipients.

Mailing the Scheduled Job output

This option lets you copy the error code returned by a **Scheduled Job** to an email.



Refer to chapter 3 for more information about the account and site settings

11.3. 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 **Systems Management Agent**.

Panda Systems Management is therefore an extensible remote management and monitoring platform, which adapts very easily to the specific needs of each customer.

11.3.1 What are the 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	Mac OS X 10.3 (Panther)	Python Software Foundation
Ruby	None	Yukihiro Matsumoto
Groovy	None	Pivotal & Groovy Community
Unix (Linux, Mac OSX)	Linux, Mac OS X	Variable

Table 18: 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 13: Centralized software deployment and installation.

11.4. Creating a monitor component

11.4.1 Component presentation and purpose

Below are the details of the steps to create a monitor and distribute it to the devices in a specific site.

The purpose of the component is to easily and simply manage the quarantine of the security product **Panda Endpoint Protection**. Quarantine stores suspicious files that could contain malware and also files detected as a virus. For this reason, the administrator needs to know how many items are in quarantine at all times.

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
Systems Management actions	An email is sent to the administrator with the monitoring results. An alert will be generated automatically

Table 19: features of the component to develop

One of the problems to tackle is that the Agent will automatically execute the script every 60 seconds but only reports information every 10 minutes.

11.4.2 Necessary elements

To follow this example, a **Panda Endpoint Protection** license is required and the Agent must be installed on the device. 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.

Panda Endpoint Protection is a complete cloud-based security solution, which is easy to use and leverages the power of Collective Intelligence to provide maximum protection against spam and known threats in real-time for desktops, servers, laptops and Exchange Server.



Panda Endpoint Protection is a complete, easy-to-use cloud security solution that leverages the power of Collective Intelligence to deliver maximum real-time protection against spam and other known threats for PCs, servers, laptops and Exchange servers.

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.

11.4.3 Communications protocol between the component and the 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 Server and the component will be performed through environment variables created on the device.

These environment variables are automatically created by the 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
<code>PCOP_PATH</code>	Read	The script recovers from the Server the path where Panda Endpoint Protection stores the quarantine on each user's device.
<code>Result</code>	Write	Send data to the Server every 10 minutes through the standard output.
<code>Errorlevel</code>	Write	Script error code. If it is 0, the Server concludes that monitoring is correct and does not collect the standard output data. If it is 1, Panda Systems Management concludes that monitoring is incorrect, collects the standard output data (<code>Result</code> variable) and processes it.

Table 20: 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.

The `Errorlevel` will inform the Server whether it must process the script response (`Result` variable) or not: if the number of files in quarantine is the same or lower (emptying of quarantine), an `Errorlevel 0` will be sent. However, if the number of files has increased, then 1 will be sent and certain information will be written in the standard output (`Result` variable). 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:

```
Linea 1: <-Start Result->
Linea 2: Result=(datos a enviar)
Linea 3: <-End Result->
```



If the script language chosen is Batch, the symbol `^` must be inserted in front of each `"<"` or `">"` 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 on the right of `"="` is the content that the Server will store and process.

11.4.4 How to work with a monitor component

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

Go to the general menu, Components, Add Component.

- Select the script type **Monitors**.
- Select the scripting language to use, in this example VBScript.

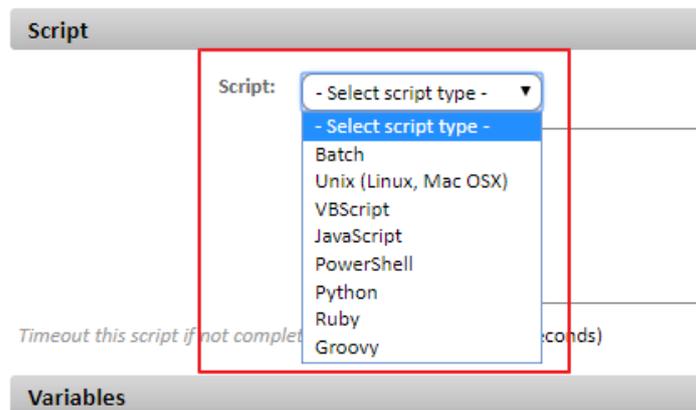


Figure 57: list of script engines compatible with Panda Systems Management

- 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.

- Set the input and output variables, in this example PCOP_PATH will contain the path to the **Panda Endpoint Protection** quarantine folder. Result will contain the script output.

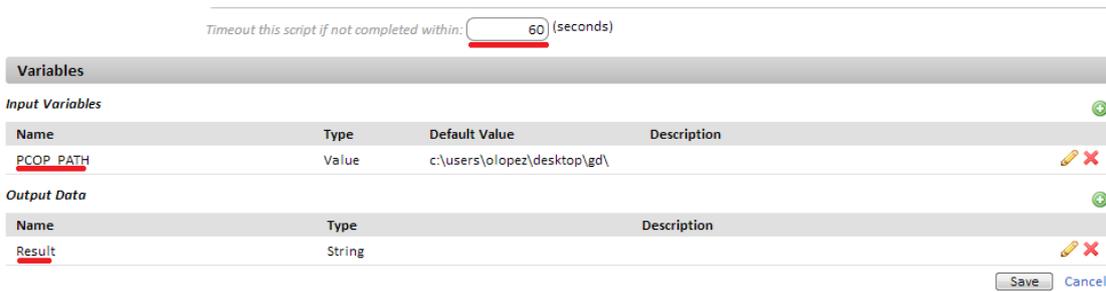


Figure 58: component input and output variables

- By clicking **Save**, the component will be added to the repository.

2 Deploying the monitor through Account Policies or Site Policies

- If you are developing a monitor, a **monitoring** site policy or account policy must be created.

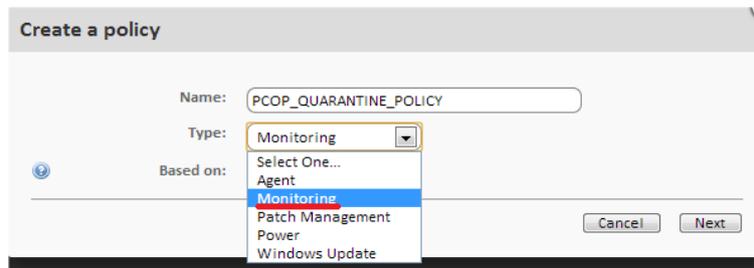


Figure 59: selecting a Monitoring-type policy

- Add the Target (Windows 7) and a **Component Monitor**.

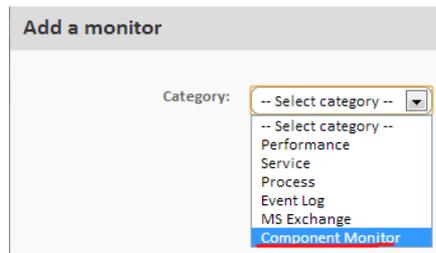


Figure 60: selecting a Monitoring-type policy

- Select the recently created component and save.



Figure 61: selecting the monitor category

- You can specify 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.

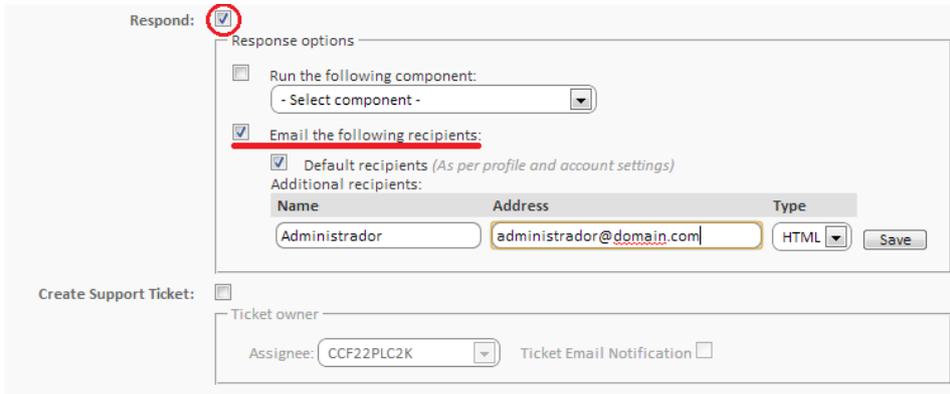
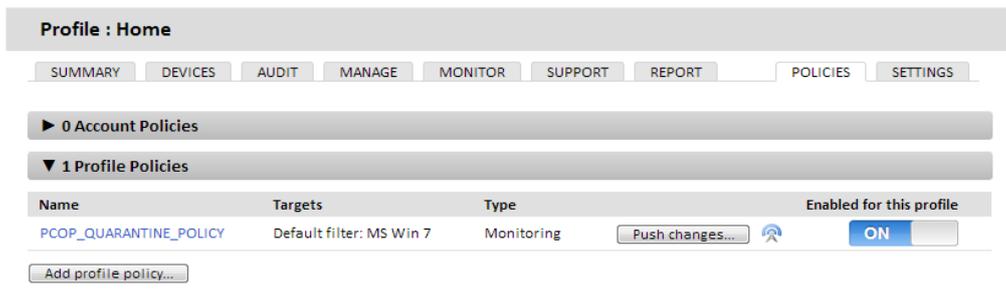


Figure 62: configuring the monitor response

- 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.



Name	Targets	Type	Enabled for this profile
PCOP_QUARANTINE_POLICY	Default filter: MS Win 7	Monitoring	ON

Figure 63: list of policies associated with a site

- 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 Creating environment variables and running the component every 60 seconds.

Once the monitor has been deployed to the devices, it will run every 60 seconds. To do this, it invokes the associated script parser, reads the necessary environment variables and writes the appropriate response.



The full source code of the script is included in Appendix A.

In line 24, it reads the PCOP_PATH environment variable and obtains an object of type FileSystemObject that points to the quarantine folder.

```

23 Set WshSysEnv = WshShell.Environment("PROCESS")
24 Set objFolder = objFSO.GetFolder(WshSysEnv("PCOP_PATH"))

```

Lines 25 to 30 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).

```

25 if err.number <> 0 then
26     'PCSM didn't send the environment variable
27     err.clear
28     WScript.Echo "<-Start Result->"
29     WScript.Echo "Result=PCOP_PATH variable not defined on PCSM console or path not found"
30     WScript.Echo "<-End Result->"
31     Set WshShell = nothing
32     Set WshSysEnv = nothing
33     Set objFolder = nothing
34     WScript.Quit(1)
--

```

In lines 44-51, the number of items in the monitored folder is written to the Registry of the device. As the script is run every 60 seconds and we want to make a comparison every 10 minutes, 10 entries are written in the registry with the value registered every 60 seconds.

```

44 While Err.Number=0 And n < 10
45     iCountPast= cint(WshShell.RegRead("HKLM\Software\Panda Security\Monitor" & n))
46     If err.number<>0 then
47         WshShell.RegWrite "HKLM\Software\Panda Security\Monitor" & n, colFiles.count, "REG_SZ"
48     Else
49         n=n+1
50     End If
51 Wend

```



The component is executed on the user's device "atomically": the status between two successive executions of the same script is not stored. If the same script must be executed several times in order to generate a valid result, the intermediary status must be saved on the device and read every time the component is executed.

It is recommended to use the registry to store the status between two or more executions of the component on a device, although temporary files can also be used.

When the counter is equal to 9 (10 entries in the Registry, 10 minutes) the initial value will be compared with the final (line 57). If it is higher in lines 59, 60 and 61, the difference will be sent and the script will terminate with `Errorlevel 1`.

When the final cycle has ended, all of the entries will be deleted from the Registry (lines 64-66) and the last entry will be copied as the first to continue the process.

```

54     If n=9 Then
55         iCountPast= cint(WshShell.RegRead("HKLM\Software\Panda Security\Monitor0"))
56         iCountNow= cint(WshShell.RegRead("HKLM\Software\Panda Security\Monitor9"))
57         if iCountPast < iCountNow then
58             'there is more items in the folder, it updates the registry and sends an alert
59             WScript.Echo "<-Start Result->"
60             WScript.Echo "Result=" & iCountNow - iCountPast & " new items in PCOP quarantine"
61             WScript.Echo "<-End Result->"
62             bHit=true
63         end if
64         For n=0 To 9
65             WshShell.RegDelete("HKLM\Software\Panda Security\Monitor" & n)
66         Next
67         WshShell.RegWrite "HKLM\Software\Panda Security\Monitor0", colFiles.count, "REG_SZ"
68
69     end if
    
```

4 Sending the standard output every 10 minutes and processing in the Panda Systems Management platform

If the script ends execution with `Errorlevel 0`, the response is not considered by the Server. If it ends with `Errorlevel 1`, the 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 definition will be performed.

11.4.5 How to use global variables

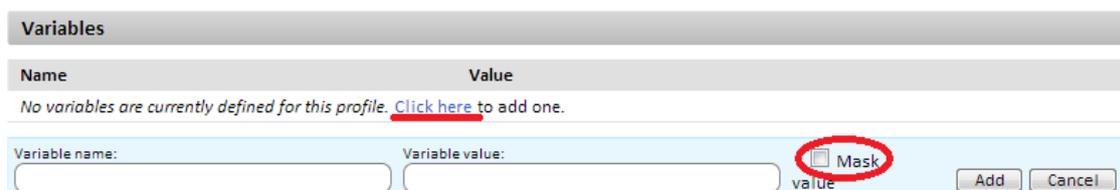
If new scripts are developed frequently, it is highly probably that you will want common data in all of them, such as paths to specific folders on the user's hard disk, the letters of shared drives on servers or even common credentials to execute certain tasks.

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.

In general menu, **Account, Settings** or **Sites, Settings**, you can define variables and their content, which will be directly accessible from the scripts that you design when they are executed on users' devices.

In the case of storing sensitive data, such as user names and passwords, you can select the **mask** checkbox to replace the content of the variable with asterisks in the **Console**.



Variables

Name	Value
No variables are currently defined for this profile. Click here to add one.	

Variable name: Variable value: Mask

Figure 64: checkbox for hiding sensitive data

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.

11.4.6 Labels and user-defined fields

Step 2 in the example specified which tasks the Server must trigger when the component result is "error"; in this case, an email reporting the change of status of the device was sent to the administrator.

This approach is correct in the case of a device that meets an error or exception condition and the administrator wants to be informed of this without needing to check the Console every so often. However, it might be necessary to simply view the status of the device without considering the error conditions. To do this, the relevant data must be published in the Console.

In that case, the component will use the user-defined fields that are in **tab bar, Summary** at Device Level for each device, as well as the device lists, and will add the necessary column as explained in Chapter 5: Devices.



Figure 65: user-defined fields on the Device Summary page

The **User-defined field 1** tag and subsequent (up to 10) can be renamed globally for all the devices managed by the partner regardless of the site to which they belong, or it can be defined for a specific site:

- At Account Level, in the general menu **Account, Settings**
- At Site Level, in tab bar, **Settings**

This way, the Console will display the tag name that you chose instead of **User-defined field X** at Device Level or in the site's device list.

The content of the user-defined fields is taken from the branches of each device's registry specified below:

```
HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom1
HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom2
HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom3
HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom4
HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom5
HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom6
```

HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom7
 HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom8
 HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom9
 HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom10

Custom Labels		
Custom Field	System Label	Profile Override
1	Custom field 1	Click here to override  
2	Custom field 2	Click here to override  
3	Custom field 3	Click here to override  
4	Custom field 4	Click here to override  
5	Custom field 5	Click here to override  
6	Custom field 6	Click here to override  
7	Custom field 7	Click here to override  
8	Custom field 8	Click here to override  
9	Custom field 9	Click here to override  
10	Custom field 10	Click here to override  

Figure 66: configuring labels for user-defined fields

Each branch specified can contain a string of up to 255 characters.

A component can freely write in 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.

11.5. Creating a script component

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

- Go to general menu **Components**, and click **New Component**.
- Select the script type.
- The settings screen for a script component only differs from the settings screen for a monitor component 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.

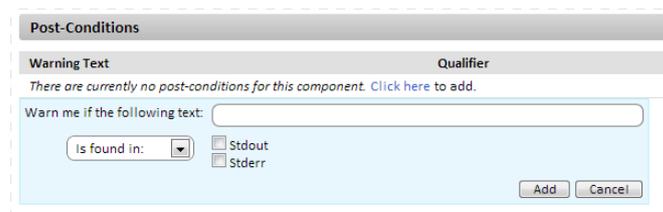


Figure 67: post-conditions warning text filter

- 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.

11.6. 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's because it has not been previously copied.

12. Assets Audit

Hardware audit

Software audit

License audit

Services audit

Changes audit

12.1. Introduction

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.

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 a site, select a 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 binoculars icon in the Actions Bar.*

Actions:             

The **Audit** tab is available at the three levels (Account, Site and Device) displaying more detailed or generic information depending on the level selected.

It also offers five types of audits:

- **Hardware:** Devices on the customer’s network, installed hardware, etc.
- **Software:** Software on the devices with the Agent installed.
- **Licenses:** Details of the software licenses used.
- **Services:** Shows the services installed on Windows computers and their status.
- **Changes:** Logs system, software and hardware changes.

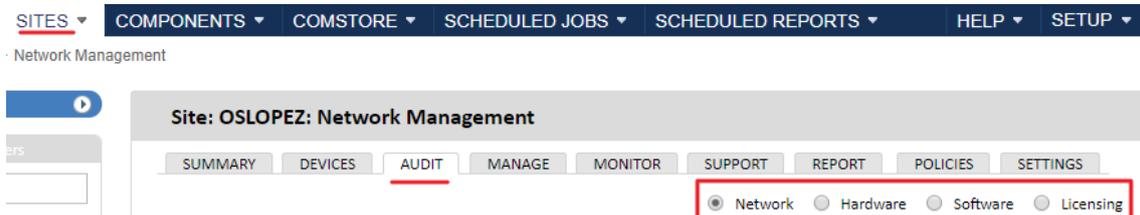


Figure 68: audit screen

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
Hardware	YES	YES	YES
Software	YES	YES	YES
Licenses	YES	YES	NO
Services	NO	NO	YES
Changes	NO	NO	YES

Table 21: auditing features based on the selected level

12.2. Hardware audit

12.2.1 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.

12.2.2 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 to display a form for the administrator to enter relevant information about the unmanaged device.



Figure 69: fields for entering unmanaged device hardware information

12.2.3 Device level

The Device Level audits are the most detailed, displaying all relevant information about the selected device.

The content of the **Audit** tab changes depending on the type of device. The information displayed will be as follows:

For Windows, Linux and OS X

Field	Description
Host name	Device name
UID	Internal ID of the device
Operating system	Operating system installed on the device and internal version
Motherboard	Motherboard make and model
BIOS Name	BIOS manufacturer
BIOS Version	
BIOS Release Date	
Processor	Processor make and model
Memory	Number of free and used memory slots, as well as the part number, serial number, capacity and speed
Display Adapter	Video card make and model
Storage	Information about the hard disks and local storage resources installed: Disk Drive, Size, Free and Description
Monitors	Make and model of the connected monitor
Network Adapters	Network card information: make and model, Mac address and interface speed

Table 22: hardware information for Windows, Linux and macOS computers at Device Level

Android and iOS systems

Field	Description
Host name	Device name
UID	Internal ID of the device
Operating system	
IMEI	Mobile device ID
Model	Smartphone or tablet model
ICCID	SIM card ID
Operator	Company that provides the telephone service
Number	Phone number
Network Adapter:	Network card information: logical identifier, Mac address and interface speed

Table 23: hardware information for Android and iOS devices at Device Level

ESXi systems

Field	Description
Host name	Device name
UID	Internal ID of the device
Operating system	
Processor	Processor make and model
Guest info	Information about the virtual machines created on the ESXi server: Hostname, Guest Name, Operating System, Data Store, CPU, RAM, Snapshots
Memory	Detailed information about the memory banks installed: Module, Type, Part Number, Serial Number, Capacity, Speed
Storage	Detailed information about the local and remote data stores configured on the server: Data Store Name, Manufacturer, File System, Capacity, Free, Subscription, Status

Field	Description
Network Adapters	Network card information: logical identifier, Mac address and interface speed

Table 24: hardware information for ESXi servers at Device Level

12.3. Software audit

12.3.1 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.

12.3.2 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.

12.3.3 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.

12.4. License audits

12.4.1 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.



In other words: all packages available at Account level will be available for use at lower levels.

Creating a software package

Click 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.

12.4.2 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.

12.5. Services audit

12.5.1 Device level

This displays the services installed on a device along with the current status and the startup type.

- **Display name:** The name of the service as seen by the user.
- **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**).

12.6. Changes audit

12.6.1 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.

13. Centralized software deployment and installation

Objective

Requirements

Procedure

Deployment examples

Bandwidth optimization

Installing software on iOS devices

13.1. Objective of centralized software 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.

13.2. Requirements

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 Chapter 11: Components and the ComStore, 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.

13.3. Package deployment and installation procedure

The general procedure consists of four steps:

1 Identify the devices on which to install the software.

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 Generate a software installation component.

The steps are the same as those described in Chapter 11: Components and the ComStore to create script or monitor components.

3 Launch a job to push the installation component to the Agents 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.

13.4. Deployment examples

To illustrate software distribution, below are four examples:

- 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

13.4.1 Deploying documents using a script language

The objective of this example is to deploy three Word documents to a folder in the root directory of the user's device. To do this, the following steps are followed:

1 Identify the devices on which to install the software.

As in this case, the Server does not have visibility of the status of the hard disk on the user's device at system file level, the installation script will be deployed to all of the devices in the site and the script (lines 19-24) will check if the folder containing the documents exists or not.

```

19 Set objFolder = objFSO.Getfolder(CONST_PATH)
20 If Err.Number=0 Then
21     'the folder already exists, the files won't be copied
22     WScript.Echo "Deploy unsuccessful: The folder already exists"
23     WScript.Quit (0)
24 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).

```

28 Set objFolder = objFSO.CreateFolder(CONST_PATH)
29 'the documents will be moved to the folder
30 objFSO.MoveFile "doc1.docx", objFolder.Path & "\doc1.docx"
31 objFSO.MoveFile "doc2.docx", objFolder.Path & "\doc2.docx"
32 objFSO.MoveFile "doc3.docx", objFolder.Path & "\doc3.docx"
33 If Err.Number<>0 Then
34     WScript.Echo "Deploy unsuccessful: " & Err.Description
35     WScript.Quit (1)
36 Else
37     WScript.Echo "Deploy successful: All files were copied"
38     WScript.Quit (0)
39 End If
  
```

2 Generate a software installation component.

An applications component will be added, to which the documents to deploy and the script that will create the folder and move the three documents on each device will be added.

In the **Component** screen: **Application** it is important to specify:

- The component is **Favorite** so that it appears on the component lists (star icon in the top left).
- The component category (**Applications**) and name.
- The script language used (**Install command**).
- Add the documents to deploy in the **Files** section.

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.

Component: Application : DEPLOY_DOCUMENTS

General

Category: Applications
 Name: DEPLOY_DOCUMENTS
 Description:
Example: "This will install FireFox v4.0 on your computer."
 UID: 3053642d-2daa-46e7-9cc4-d584363e1c54
 Security Level: 5 (Super)

Commands

Install command: VBScript
Expand

```

Option Explicit
'*****
'Deploy_documents v0.99b
'12/03/2013
'By Oscar Lopez / Panda Security
'Objetivo: Crear una carpeta en el escritorio del usuario y copiar en
    
```

Timeout this script if not completed within: 3600 (seconds)

This component requires profile credentials

Files

Filename	Size	Last Modified
doc3.docx		2013-03-12 12:14:51 GMT
doc1.docx		2013-03-12 12:14:51 GMT
doc2.docx		2013-03-12 12:14:51 GMT

Figure 70: configuring a component

3 Launch a job to push the software to the Agents on the affected devices.

Click **Quick job** or **Job** after selecting the devices from the site to which to deploy the documents.

Profile: Home

Showing 1 - 8 of 8 results.

You have selected 4 device(s) in this profile

Actions:

Profile	Home
<input checked="" type="checkbox"/>	Home
<input type="checkbox"/>	Home
<input type="checkbox"/>	Home
<input checked="" type="checkbox"/>	Home
<input type="checkbox"/>	Home
<input checked="" type="checkbox"/>	Home
<input type="checkbox"/>	Home
<input checked="" type="checkbox"/>	Home

Select component to use in quick job:

- Clean Internet Browser Caches
- DEPLOY_DOCUMENTS**
No variables
- Firefox 15.0.1
- Firefox 19.0.1
- Malwarebytes Anti-Malware 1.62.0.1300
- Modify Secure Attention Sequence (SAS)
- Physical Memory Audit
- SCRIPT_APPLICATION

Make a component a favourite to add it to the Quickjob list.

Follow to jobs list page on submit

Figure 71: running an installation component in a quick job



At Account Level, you can select complete sites to which to apply software deployment.

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).

```

28 Set objFolder = objFSO.CreateFolder(CONST_PATH)
29 'the documents will be moved to the folder
30 objFSO.MoveFile "doc1.docx", objFolder.Path & "\doc1.docx"
31 objFSO.MoveFile "doc2.docx", objFolder.Path & "\doc2.docx"
32 objFSO.MoveFile "doc3.docx", objFolder.Path & "\doc3.docx"
33 If Err.Number<>0 Then
34     WScript.Echo "Deploy unsuccessful: " & Err.Description
35     WScript.Quit (1)
36 Else
37     WScript.Echo "Deploy successful: All files were copied"
38     WScript.Quit (0)
39 End If
  
```

- **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.

```

19 Set objFolder = objFSO.Getfolder(CONST_PATH)
20 If Err.Number=0 Then
21     'the folder already exists, the files won't be copied
22     WScript.Echo "Deploy unsuccessful: The folder already exists"
23     WScript.Quit (0)
24 End If
  
```

After the job has been launched, it will appear in General menu, **Scheduled Jobs, Active Jobs**.

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.

Additionally, this tab contains an **Icon bar** that allows several actions to be triggered:

- The **Actions** area groups the icons that allow you to relaunch the job, reload the page to update the job status, or download the standard output and error to a file.
- The **Views** filter allows you to filter the jobs by status.

13.4.2 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:\.`
- 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.

Steps for generating a silent self-extracting installation file.

1 Prepare the folder with the documents to deploy.

Create the root folder `ACME Documents` and place all of the files, folders and sub-folder to be deployed inside.

2 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**.

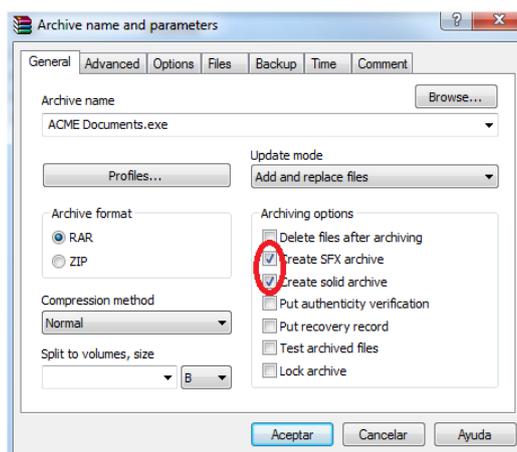


Figure 72: creating a self-extracting archive

3 Configure the executable file as Silent.

To do this, enable Hide All in Advanced, SFX Options, Modes, Silent Mode.

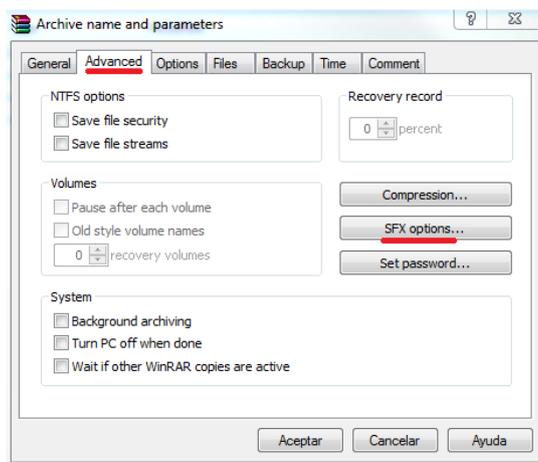


Figure 73: running the archive in silent mode

4 In the General tab, specify the path where the folder will be created.

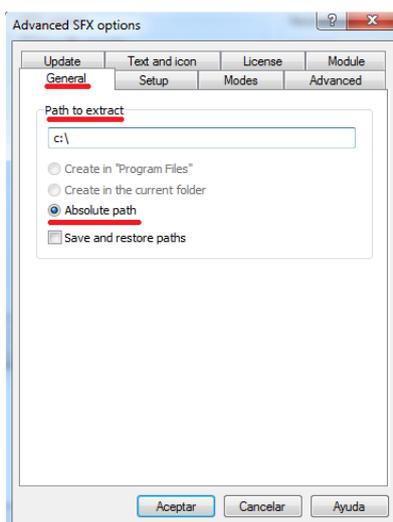


Figure 74: archive path

5 Specify that all files will be overwritten if they already exist without asking the user.

Once the ACME Documents.exe package has been generated, create the **application** component to deploy it.

In the **Component** screen: **Application** it is important to specify:

- The component is **Favorite** so that it appears on the component lists (star icon in the top left).
- The component category (**Applications**) and name.
- The script language used (**Install command**), in this case **Batch**.
- Add the package to install ACME Documents.exe.

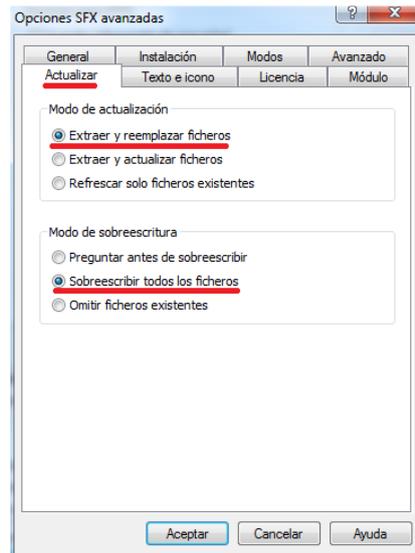


Figure 75: option to overwrite extracted files without any prompt

The script will simply execute the self-extracting package, which will create the folder in the c:\ drive along with the internal structure, overwriting any previous content.

13.4.3 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.

This data is used to create a site filter or an account filter with the following settings:

- **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.

Device : XP3 - Software

SUMMARY **AUDIT** MANAGE MONITOR SUPPORT REPORT POLICIES

Hardware Software Changelog

Operating System: Microsoft Windows XP Professional 5.1.2600
 Service Pack: 3
 Architecture: 32 bit

Actions:  

▼ **11 Installed Applications**

Adobe Flash Player ActiveX	9.0.124.0
Adobe Shockwave Player	11.0.0.429
IIS 7.5 Express	7.5.1070
Microsoft .NET Framework 2.0	2.0.50727
Microsoft .NET Framework 4 Client Profile	4.0.30319
Microsoft .NET Framework 4 Extended	4.0.30319
Mozilla Firefox 19.0.1 (x86 en-US)	19.0.1
Mozilla Maintenance Service	19.0.1
Panda Cloud Systems Management	
UltraVNC 1.0.6.4	1.0.6.4
VMware Tools	8.3.7.3827

Figure 76: obtaining the installed application ID string

2 Generate a software installation component.

It is extremely easy to create an installation component.

In the **Component** screen: **Application** it is important to specify:

- The component is **Favorite** so that it appears on the component lists (star icon in the top left).
- The component category (**Applications**) and name.
- The script language used (**Install command**), in this case Batch.
- **Install command** contiene la línea de comando que ejecuta el paquete:

```
@echo off
pushd %~dp0
dotNetFx40_Full_x86_x64.exe /q /norestart
```

- Add the package to install dotNetFx40_Full_x86_x64.exe.

The script only has one relevant line, which is the one that executes the installation package with the parameters necessary for a silent installation.

3 Launch a job to push the software to the Agents on the affected devices.

Firstly, select the previously prepared filter and then execute a job with the application created.

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 in the Action Bar.

SUMMARY DEVICES AUDIT MANAGE MONITOR SUPPORT REPORT

Showing 1 - 8 of 8 results.

Actions:          

13.4.4 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 the free version of `Advanced Installer`, go to <http://www.advancedinstaller.com/download.html>

Follow these steps to generate the installer:

- Select the **Simple** template (free).

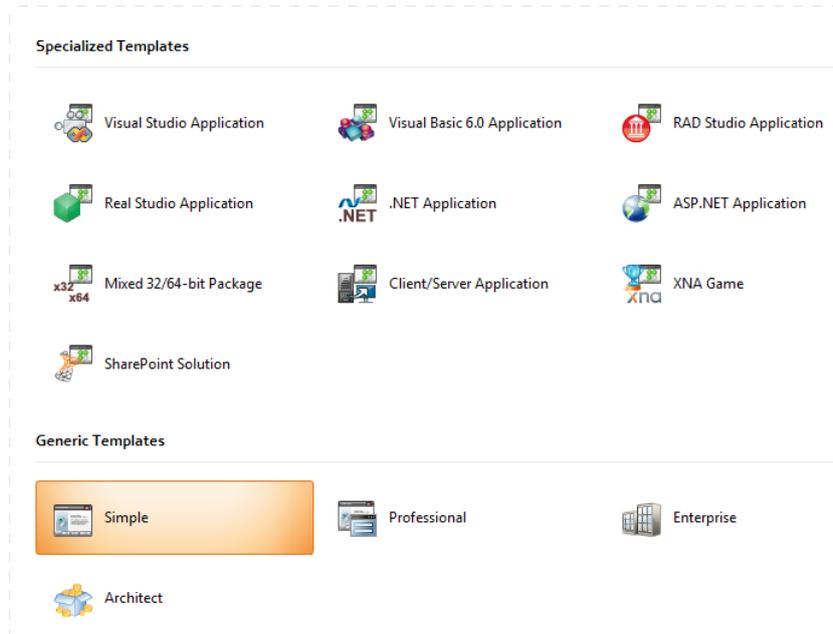


Figure 77: template selection

- In **Products Details**, enter the basic details of the installer: **Product Name**, **Product Version** and **Company Name**.

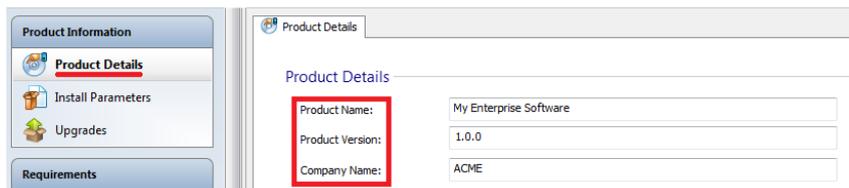
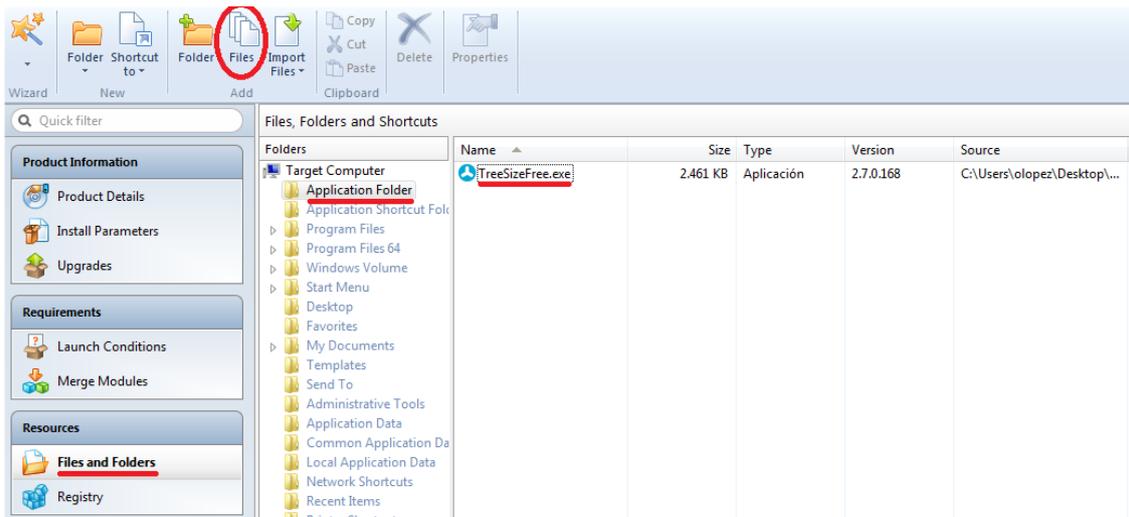


Figure 78: installer details

- Add the files and programs to install and the shortcuts to create. This is done in the **Files and Folders** tab.



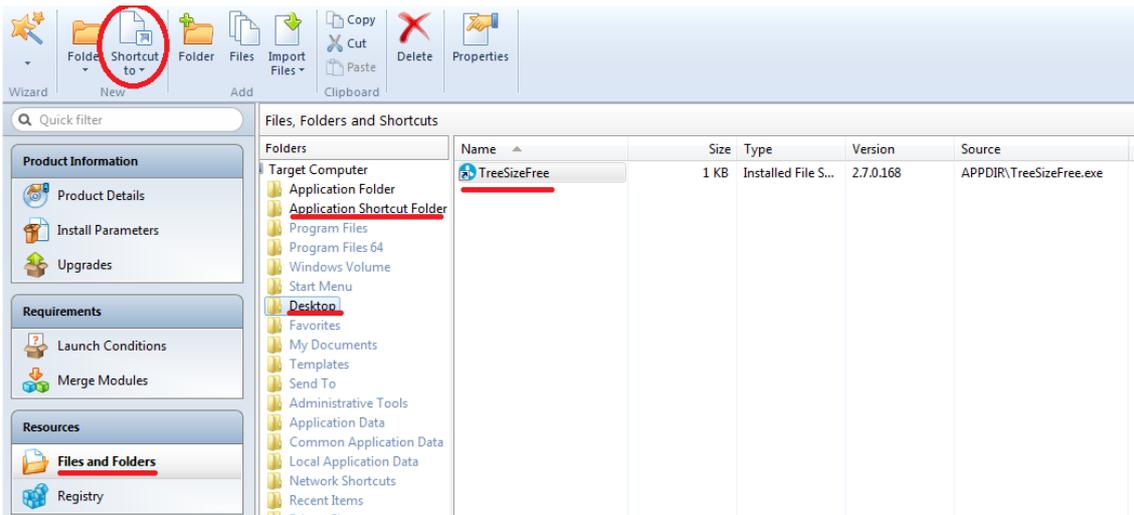


Figure 79: adding the files to deploy

- Finally, execute **Build** and the MSI package will be generated in the selected folder.

Once the installation package has been generated, the steps for creating an installation component and deploying it are the same as in previous examples, except for the Batch script, whose installation command will vary slightly.

```
@echo off
pushd %~dp0
MSIEXEC /I "my software.msi" /qn
```

The MSIEXEC utility is invoked using the /qn parameter to launch a silent installation.

In the **Component** screen: **Application** it is important to specify:

- The component is marked as **Favorite** so that it appears on the component lists (star icon in the top left).
- The component category (**Applications**) and name.
- The script language used (**Install command**), in this case **Batch**.
- Add the package to install `My Software.msi`.

13.5. Bandwidth optimization

The Agent installed on each device checks the 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.

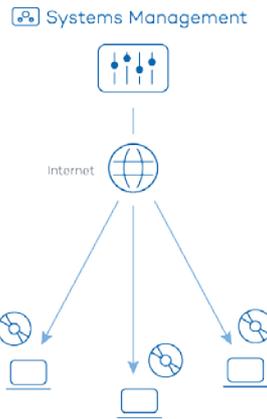


Figure 80 Deploying packages individually

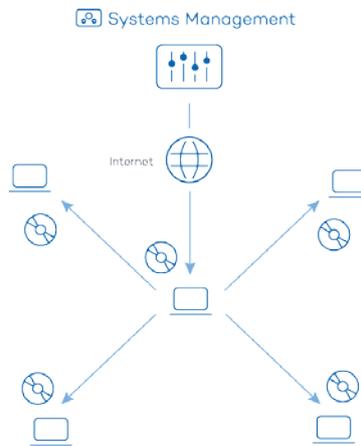


Figure 81: deploying packages centrally

To minimize the total download volume, one of the network devices can be promoted to the role of repository/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.

13.5.1 Designating a device as a local cache

To promote a device to the role of repository/cache, access the device at Device Level in the Console and click the **Add/Remove as local cache** icon in the Action bar.

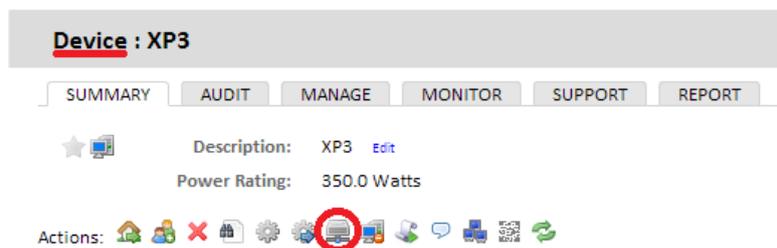


Figure 82: designating a device as a local cache

A window will be displayed to select the device on which the cached files are stored.

Furthermore, the local cache will also store the patches downloaded from Windows Update, as described in chapter Patch Management

The allocated device will then download and deploy the components and installation package to the devices in the local network, speeding up deployment and minimizing bandwidth usage.

13.5.2 Configuring the behavior of devices designated as a local cache

The Local Caches section in tab menu Settings lets you indicate the maximum number of days that cached patches and components will be stored in each device, as well as the order of precedence of the devices on the network.

13.6. Installing software 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.

13.6.1 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.

To be able to download apps to iOS devices, you must first download the Mobile Device Management component from the **ComStore**.



Figure 83: mobile Device Management component

- Add the apps that you want to deploy to the Application List. To do that, click the Add iOS App button to access the app selection window.



Figure 84: access to the iOS app 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**.

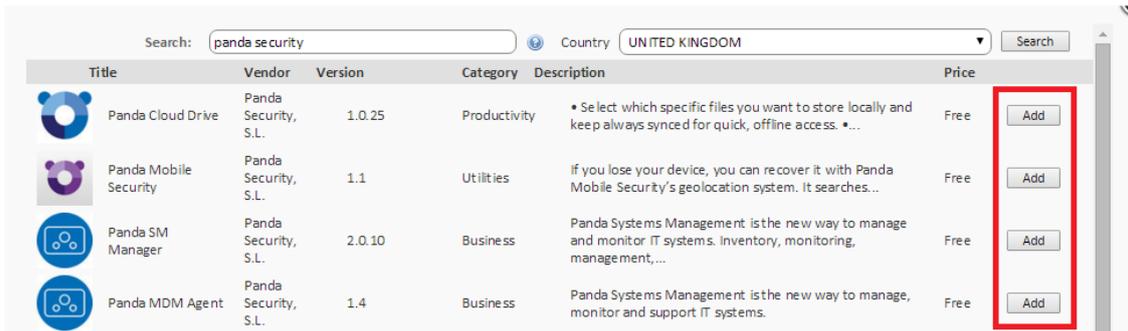


Figure 85: adding the iOS apps to deploy

13.6.2 Installing the iOS apps included in 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.  Get the changes to be automatically applied as soon as the device becomes available, click the  icon.

14. Ticketing

Description of a ticket

Creating a ticket

Ticket management

14.1. Introduction

The increase in the number of devices to manage and the growing number of technicians assigned to resolving problems will sooner or later require the implementation of a system that allows each case handled by the IT Department to be documented and coordinated.

Ticketing systems are used to track each incident from the moment it is created until it is closed, recording all of the intermediates statuses through which it evolves.

Therefore, it is possible to assign a case to a specific technician and reassign it to another one if the original technician is not available or the task requires very specific knowledge, storing all of the documentation and progress made up until then and minimizing interruptions to the end user with repeat requirements for information about the same problem.

Secondly, forcing documentation of incidents allows the procedure to be reused in the future and fine-tuned, minimizing the response time for open cases.

Finally, a ticketing system allows you to identify the workload of the IT Department, filtering the tickets open at a given time and assigning more resources if necessary.

14.2. Description of a ticket

Each ticket contains a series of fields that describe it:

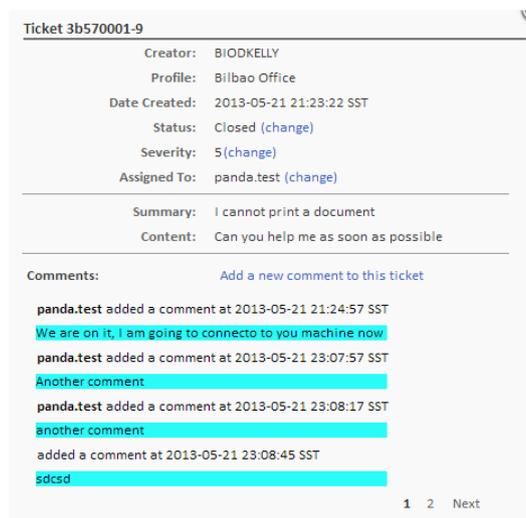


Figure 86: ticket overview

- **Creator:** Ticket creator. It can be a device (if the ticket was created from the Agent by a user), or system account (if it was created by a monitor and assigned to a technician).
- **Site:** Group of devices to which the ticket belongs.
- **Date Created:** Creation date of the ticket.
- **Status:** There are four statuses:

- **New:** Recently created ticket with the description of the problem and assigned to a technician. No task has been performed yet.
 - **In progress:** The technician assigned from the IT Department is managing the incident.
 - **Waiting:** Resolution of the incident has been stopped by external causes (lack of information, confirm changes by the users or others).
 - **Complete:** The incident has been resolved and closed.
- **Severity:** Severity of the ticket. If it was generated by a monitor, the severity assigned to it will be copied.
 - **Assigned to:** Technician assigned to resolve the incident.
 - **Summary:** Summary of the incident.
 - **Content:** Description of the incident.
 - **Comments:** In this field, both the technician and user can add entries that complete and update the incident.



It is recommended to use the Comments field frequently, documenting changes to the incident and the actions performed, by both the technicians from the IT Department and the user through the tests performed and other data of interest. The aim is to reuse this information to speed up resolution of similar incidents in the future.

14.3. Creating a ticket

Tickets are created in three ways:

- Manually by the user from the agent installed on their computer.
- Automatically from a monitor that detects a condition defined as an anomaly on a user's device.
- Manually by the IT department from the console.

14.3.1 Manually by the user from the Agent

If the user notices that the device is not working correctly and wants to leave a written record of the symptoms.

To register a ticket manually, the user must open the Agent by right-clicking its icon, select **Open** and click **Tickets, Open a New Ticket** tab.

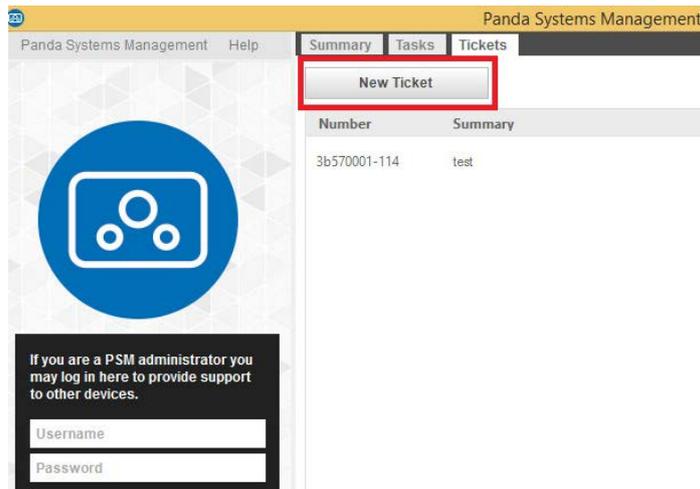


Figure 87: ticket creation tool in the PCSM Agent installed on users' devices

After creating the ticket, new comments can be added and it can be closed.



Figure 88: ticket editing tool in the PCSM Agent installed on users' devices

 Tickets created from the Agent are automatically assigned to the user account configured in General menu, Account, Settings, End-user Ticket Assignee, or from the Site in Setup.

14.3.2 Automatically from a monitor that detects a condition defined as an anomaly on a user's device

This can be configured when defining a monitor policy, on the Ticket Details tab.

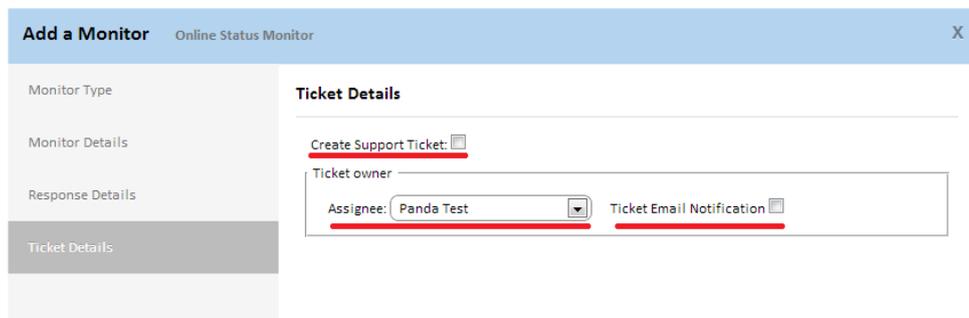


Figure 89: settings for automatically generating tickets

In this case, you can choose the technician assigned, and if an email notifying that the ticket has been created will be generated.

14.3.3 Manually by the IT Department from the Console

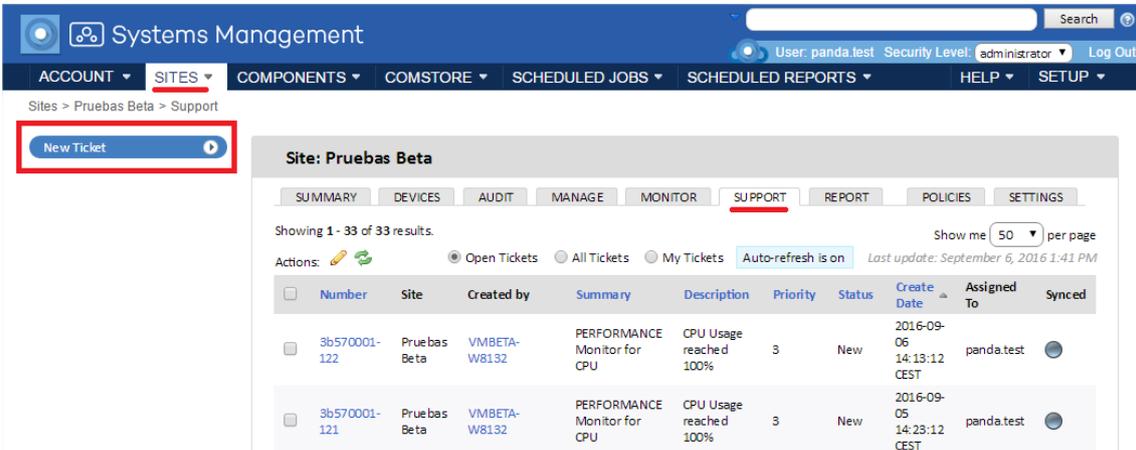
This feature allows IT staff to set reminders and add tasks to the Department's queue.

Follow these steps to create a ticket from the Console:

- Determine the Level that the ticket must be created at:
 - To create a ticket at Account Level, go to general menu Account, Support tab.
 - To create a ticket at Site Level, go to general menu Sites, select a site and click the Support tab.
- Click New ticket



Tickets created at Account Level do not have a site assigned and are not displayed in any site created.



The screenshot shows the 'Systems Management' interface. The navigation bar includes 'ACCOUNT', 'SITES', 'COMPONENTS', 'COMSTORE', 'SCHEDULED JOBS', 'SCHEDULED REPORTS', 'HELP', and 'SETUP'. The current view is 'Sites > Pruebas Beta > Support'. A 'New Ticket' button is highlighted with a red box. The main content area shows a table of tickets for 'Site: Pruebas Beta' under the 'SUPPORT' tab. The table has columns for Number, Site, Created by, Summary, Description, Priority, Status, Create Date, Assigned To, and Synced. Two tickets are listed:

Number	Site	Created by	Summary	Description	Priority	Status	Create Date	Assigned To	Synced
3b570001-122	Pruebas Beta	VMBETA-W8132	PERFORMANCE Monitor for CPU	CPU Usage reached 100%	3	New	2016-09-06 14:13:12 CEST	panda.test	<input type="checkbox"/>
3b570001-121	Pruebas Beta	VMBETA-W8132	PERFORMANCE Monitor for CPU	CPU Usage reached 100%	3	New	2016-09-05 14:23:12 CEST	panda.test	<input type="checkbox"/>

Figure 90: creating a ticket at Site Level

In this case, you can specify the severity of the ticket and its content and assign it to a technician to be resolved or reassigned.

14.4. Ticket management

Tickets that have already been created are managed from tab bar, **Support** at Site, Account or Device level.



Tickets created at lower levels will be displayed at higher levels. For example, if tickets are created at Device Level, they will appear at the Site Level to which this device belongs.

The icons in the Action bar let you filter the ticket list (**Open Tickets, My Tickets, All Tickets**) or edit their status with the pen icon  . To change the severity, status and the technician to whom it is assigned, click the Ticket number.

15. Patch Management

- What is patch management?
- What patches can I deploy / apply?
- Patch deployment and installation
 - Windows update policy
 - Patch Management policy
 - Device patch status
 - Usage scenarios

15.1. What is patch management?

Patch management is 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.

15.2. What patches can I deploy/apply?

All the patches and updates published by Microsoft through Windows Update can be centrally managed through **Panda Systems Management**.

Microsoft publishes updates for all the Windows operating systems currently supported and for the software it develops:

- Microsoft Office
- Microsoft Exchange
- SQL Server
- Windows Live
- Windows Defender
- Visual Studio
- Zune Software
- Virtual PC
- Virtual Server
- CAPICOM
- Microsoft Lync
- Silverlight
- Windows Media Player
- Other...

15.3. 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 Updates policy.
- Patch Management policy.



Windows updates policies and Patch management policies are mutually exclusive. It is advisable to disable Windows Updates when using Patch Management policies to update Windows operating Systems, otherwise there may be unpredictable consequences. See section Method I: Windows Update Policy below to disable Windows Update.

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.

15.4. Method I: Windows Update policy

Windows Update policies 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.

15.4.1 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.

Windows Update classifies the patches it receives into three categories:

- **Important**
- **Recommended**
- **Optional**

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:

- **Add Target:** Lets you add filters or groups that limit the scope of application of the policy.
- **Patch Policy:** Specifies the general behavior of Windows Update on each device with respect to the patches classified as "Important" by Microsoft:
 - Automatically download and install.
 - Manual download and selection by the user.
 - Notify without downloading.
 - Disable Windows Update.



To prevent policies from overlapping, if you are already using another method for updating patches within PCSM or with third-party products, it is advisable to create a Windows Update with the patch policy field "disable Windows Update".

- **Install new updates:** Specifies when the patches will be installed.
- **Give me recommended updates the same way I receive important updates:** Applies the policy selected in Patch policy for both **Important** and **Recommended** patches.
- **Allow all users to install updates on the computer:** Allows the user to manually install patches.
- **Give me updates for Microsoft products and check for new optional Microsoft software when updating Windows:** Checks for **Optional** patches, generally patches for other Microsoft products.
- **Show me detailed notifications when new Microsoft software is available:** Detailed notifications are shown to the user when new Microsoft software is available.
- **No auto-restart with logged on users for scheduled automatic updates installations:** If this option is selected, the patches are applied and the user is notified of the need to reboot. If it is not enabled, the patch will be installed and the user will be notified that the device will reboot in 5 minutes.

- **Re-prompt for restart with scheduled installations:** Defines the time before Windows Update prompts the user to restart the device if patches are installed that require this.
- **Delay restart for scheduled installations:** Defines the time that the system will wait to restart after installing patches. If nothing is specified, the default value will be used: 15 minutes.
- **WSUS:** Allows an alternative local or remote Windows Server Update Services server to be used in order to minimize downloading of individual patches by each network device.
 - **Do not allow any connections to Microsoft for Patching or Searching when using a WSUS Server:** In the event that the administrator has a WSUS server installed on the network, this option prevents searching for patches across the Microsoft network when the WSUS server is unavailable.
 - **Enable Client-Side Targeting:** If a WSUS server is used with **Client-Side Targeting** enabled, the groups and the devices they contain will be manually defined in the WSUS server. This parameter allows you to specify the groups to which the device to which the policy applies belongs (separated by a semi-colon).



If some or all of the devices affected by the Windows Update policy do not coincide with the devices defined in the WSUS groups, the policy will not be applied to these 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.

15.5. Method 2: 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.

15.5.1 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.

The figure below shows the workflow phases:

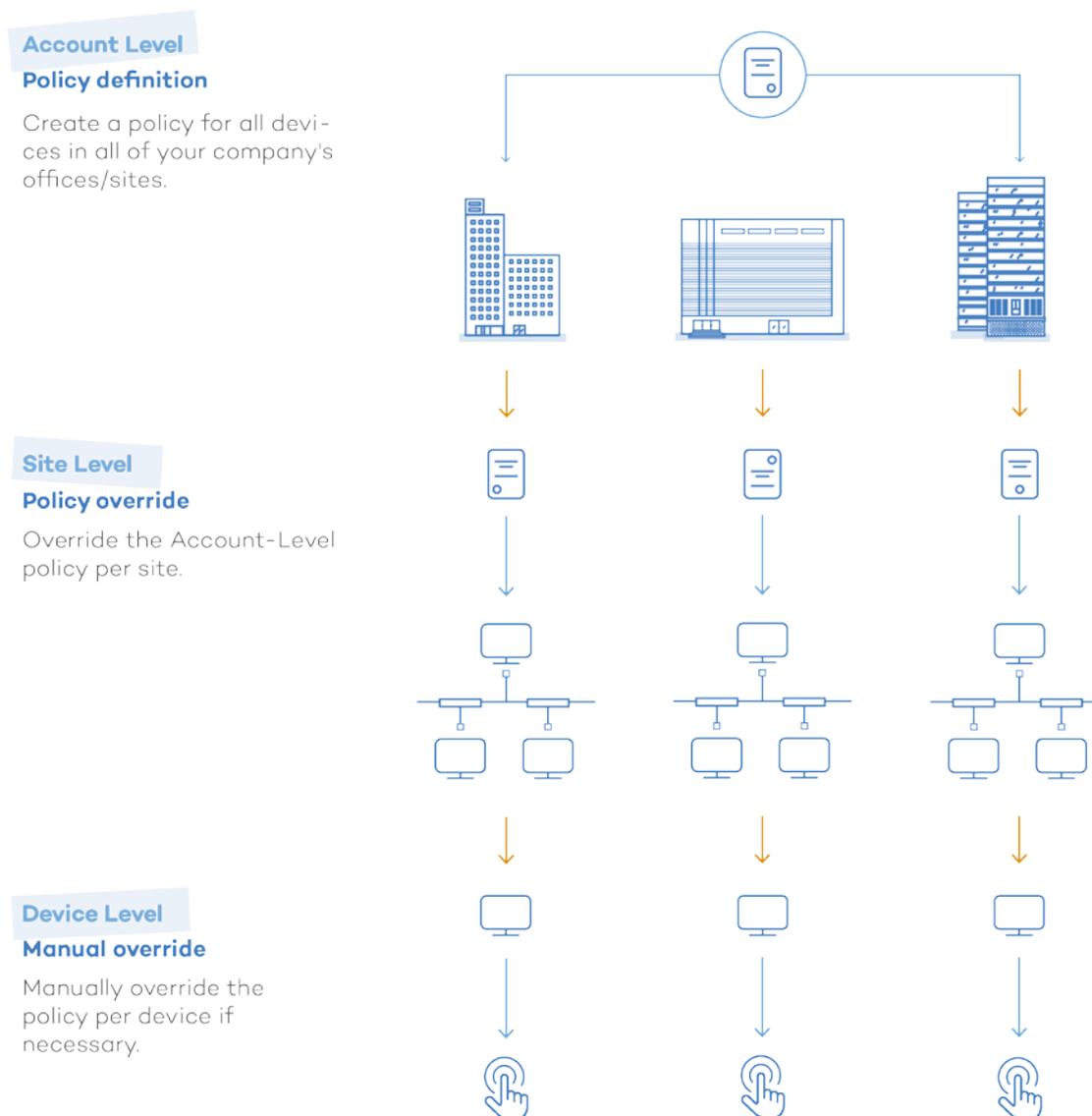


Figure 91: general strategy for defining Patch Management policies

The workflow can be divided into three 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** later in the guide for information about how to configure a Patch Management policy.

Overriding the 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.

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.

15.5.2 Creating a Patch Management policy

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** them. This is part of the **Patch Management** policy configuration process:

- **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:

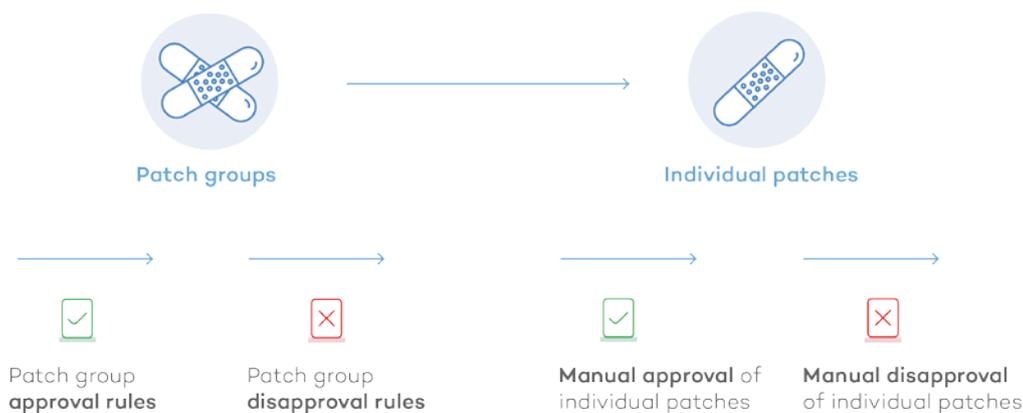


Figure 92: patch approval/disapproval flows

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.

- **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.
- **Timing options:** Lets you select when the patches will be applied and define the patch window duration.
 - **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.

Choose when you want the policy to run.

At selected date and time
 Daily
 Weekly
 Monthly
 Monthly Day of Week
 Yearly

Start: 24 February 2016 10:23

This policy will run once at the date/time indicated above.

OK Cancel

Figure 93: patch schedule settings

Select a frequency. The panel on the right will change to allow the network administrator to specify the precise times and dates when patches must be installed.

- **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:** Lets you select the repository from which you want the PCSM agents to collect the patches to install.
 - **Download patches from Windows Update:** The targeted devices will connect to the Windows Update server to download patches.
 - **Use a local cache:** Allows targeted devices to use the device designated as a local cache to download patches.



For more information about how to designate one or more network devices as a local cache, refer to section 13.5.1 in chapter 13

- **Permit devices to contact Windows Update:** If the devices designated as a local cache are not available, the targeted devices will connect to the Windows Update server to download the necessary patches.
- **Patch Approval:** Lets you set filters to select the patches to install. The available patches are divided into two categories: Approve and Do Not Approve.
 - **Approve these patches:** Lets you define filters based on the characteristics of the patches released by Microsoft in order to install them on the targeted devices.
 - **Do not approve these patches:** Lets you define filters based on the characteristics of the patches released by Microsoft to prevent their installation. 'Do Not Approve' selections take precedence over 'Approved' selections.

See later in this chapter for information about how to define a filter.

- **Configure individual patches:** Lets you manually approve or deny patches.
 - **Available:** Displays all available patches published in Microsoft's directory.
 - **Approve:** Patches selected for installation.
 - **Do Not Approve:** Patches that won't be installed.

The three options include search filters that let you filter the patches to display based on the following criteria:

- **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

After locating the patches, select them and click the  icon to approve them, or  to exclude them. You can also export the patch list by clicking the icon .

- **Power:** Lets you define how your devices must behave before and after the patch process:
 - **Boot:** When selected, wakes all targeted devices compatible with the Wake-On-LAN feature ten minutes before it starts with the patch process



To use this feature, Wake-On-LAN support must be enabled in the computers' BIOS. Also, you must have a Network Node device in the same site as your targeted devices

- **Reboot:** Lets you define how the targeted devices must behave after the patch process:
 - **Power down:** Shuts down the targeted devices after the patch schedule window
 - **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**.
 - **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

15.5.3 Creating a patch filter

The **Patch Approval** section contains a series of resources that allow administrators to define advanced filters to group patches based on the selected criteria.



Refer to section 6.4.2 for a description of how to create filters

The available fields to create a filter for patches are detailed below:

- **All:** Selects all published patches
- **Category:** Filters patches by category, such as **Critical Updates** or **Drivers**.
- **Description:** Allows you to filter by the description of the patch
- **Download size**
- **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
- **Reboot behavior:** Filters patches based on how they behave after installation: **Never reboots** (0), **Always requires reboot** (1), **Can request reboot** (2)
- **Release Date**
- **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

15.5.4 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. At the bottom of the screen, you will see a list of the **Patch Management** policies created at Account Level. These policies have a green icon to their left that differentiates them from regular policies, and display the button **Edit Override**.

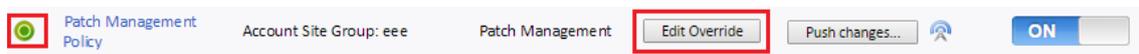


Figure 94: patch Management policy override

Clicking the **Edit Override** button will display a screen with controls to selectively modify the settings of the Account-Level policy. However, clicking the policy's name will take you to the policy's original settings.

Click the **Override** button to edit the policy settings, changing and overriding the original values.

15.5.5 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.

Update Patch Management Policy

Name: Patch Management Policy
 Policy type: Patch Management
 Created: 2017-01-16 10:18:20 UTC
 Modified: 2017-01-16 10:18:20 UTC (panda.test)

Targets:

Type	Name
Site Group	eee

Timing Options

Override: ON

Please ensure that all of your devices are on the latest Agent version.

Schedule:

Duration: Patching runs for hours

Patch Location

Override: OFF

Figure 95: patch Management policy override options

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: BIOOLOPEZ - Patch Management

SUMMARY
AUDIT
MANAGE
MONITOR
SUPPORT
REPORT
POLICIES

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	<input checked="" type="button" value="Run Now"/>

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 96: 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.
- **Next Run:** 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 re-installed 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

15.5.6 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.

15.6. Device patch status

Go to the **Manage** tab at Site or Account Level, and click **Patch Management** to view at a glance the patch status of your entire IT network.

Site: Pruebas Beta: Patch Management

SUMMARY DEVICES AUDIT **MANAGE** MONITOR SUPPORT REPORT POLICIES SETTINGS

Patch Management
 Network Management
 Software Management

The chart below shows device compliance with the approved patch list. Patches not approved are not reported as missing.

All Policies

All devices
 Workstations
 Servers

10 Most vulnerable devices in terms of Approved Pending Patches

Hostname (Description)	Policy	Last Run	Next Run	Last Audit Date	Approved Pending Patches
VMBETA-W764 (VMBETA-W764)	patch pruebas beta		Run once at 2017-01-17 18:00	2017-01-18 15:58:57 CET	98

▼ 1 Account Policies

Name	Targets	Last Run	Next Run	Actions	Enabled for this site
PMP	Account Site Group: North		Run once at 2017-01-20 10:26	Push changes...	<input checked="" type="checkbox"/> ON

▼ 1 Site Policies

Name	Targets	Last Run	Next Run	Actions	Enabled for this site
patch pruebas beta	Site Pruebas Beta (Group: beta)		Run once at 2017-01-17 18:00	Push changes...	<input checked="" type="checkbox"/> ON

Figure 97: network status regarding Patch Management

The **Manage** screen is divided into the following three areas:

- **Pie chart:** Shows the percentage of fully patched devices and devices with pending patches
- **10 Most vulnerable devices in terms of Approved Pending Patches:** Displays the ten computers that demand most attention from the administrator in terms of approved pending patches
- **List of assigned policies:** Helps you locate the Patch Management policies assigned to the Site

Pie chart

Shows the percentage of fully patched devices and devices with pending patches.

A computer is considered to be fully patched when all approved patches have been successfully installed. The chart will display in red those computers with approved patches that have not been installed yet or returned errors that prevented installation.

By default, the chart displays all devices in the Site/Account. However, you can click the  icon in the policy list to only display the devices assigned to a specific policy.

Furthermore, at the bottom of the chart you can find a selector to filter the data displayed by device type (**All devices**, **Workstation**, **Servers**).

10 Most vulnerable devices

This section displays a list of your ten most vulnerable devices in terms of approved pending patches. The device with the highest number of approved pending patches will be listed first, regardless of the severity of the patches. You will see the following details for each computer:

- **Hostname:** The name of your device. Clicking on the Hostname hyperlink will direct you to the **Manage** tab at the Device Level.
- **Site:** The site that the device is added to. This field is only visible at the Account Level.
- **Policy:** The name of the policy that targets the device.
- **Last Run:** The last run time of the policy.
- **Next Run:** The next run time of the policy. Policies with an overridden schedule show the overridden data, not the original data.
- **Last Audit Date:** The last time the device was audited.
- **Approved Pending Patches:** The total number of approved pending patches for each device.

List of assigned policies

This section displays the list of Patch Management policies created at the Account Level and Site Level.

You will see the following details for each policy:

- **Override active icon**  . This icon only appears if the Account-Level policy in question is overridden at the Site Level. To view/edit the override, click Policies at the Site Level. To view the policy's original settings, click its name.
- **Targets:** The targets of the policy
- **Last Run:** The last run time of the policy
- **Next run:** The next run time of the policy
-  : Clicking on this icon will toggle what is shown in the (big) pie chart above the list of policies. The icon toggles between an All Policies overview and the data for the policy in question, showing the policy name over the pie chart.
- **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. Clicking on the icon will open a pop-up window showing the last run time and the following patch information: **Patch Description, Size, Targeted Devices, Successes and Failures.**
 -  : Allows you to see what patches would be installed if the policy was run now. It lets you validate the created policy, making sure all approved patches are included in the list, and all disapproved patches are excluded from it.
 -  : Shows all sites targeted by the policy. It also displays overridden policies and lets you enable or disable policies for your sites.
 -  : Clicking this icon will display a dialog box where you can confirm whether you want to run the policy now, outside of its schedule.
- **Enabled for this site:** A toggle to turn the policy ON or OFF:

15.7. Patch Management policy method: Usage scenarios

Method	Patch selection granularity	Automation	Configuration time
Windows Update Policy	Low Patch selection according to "Important" and "Recommended" groups	High The groups of patches to install are configured once	Low Choose whether "important" and optional" patches are installed

Method	Patch selection granularity	Automation	Configuration time
Patch Management	Moderate Patch selection via multiple configurable criteria	High After creating the filters, the patches will be automatically installed as Microsoft releases them	Moderate Define the filters to select the patches to install

Table 25: comparison of the Patch Management policies available in Panda Systems Management

16. User accounts and security levels

User accounts

Main user

Security levels

Security levels: purpose

The administrator security level

Accessing user account and security level configuration settings

Creating and configuring user accounts

Creating and configuring security levels

Strategies

16.1. User accounts

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.

16.2. 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.

16.3. 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.

16.4. 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.

16.5. 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.

16.6. Accessing user account and security level configuration settings

In general menu, **Account**, there are two entries associated to managing security levels and user accounts:

- **Users**: Lets you create new user accounts and define whether they belong to one or various security levels.
- **Security levels**: Lets you create and modify new settings for accessing **Panda Systems Management** resources.



The Users and security levels tabs are only accessible if the user belongs to the special administrator security level.

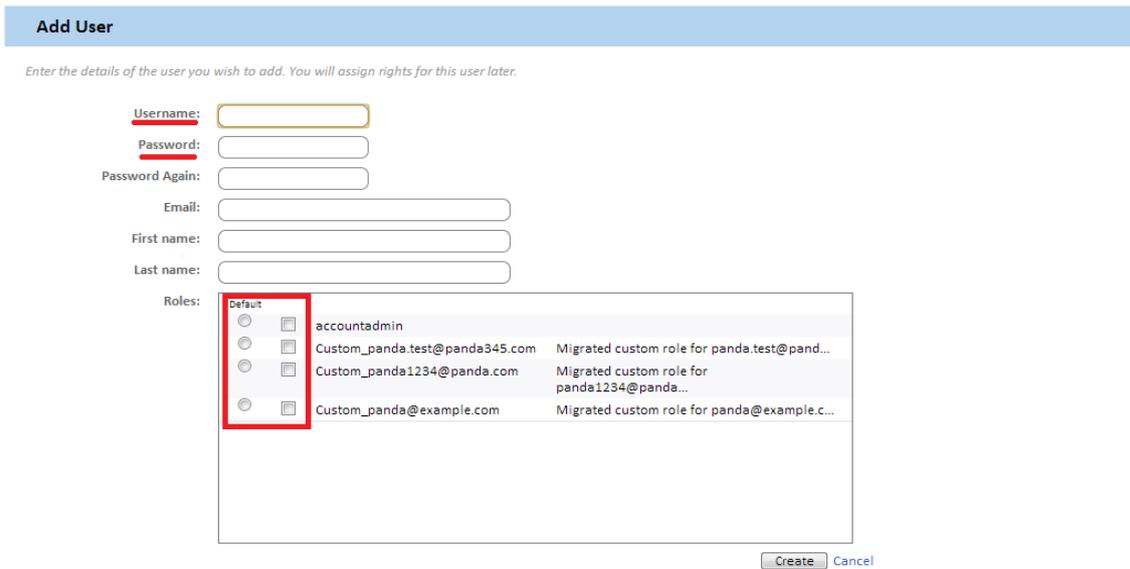
16.7. Creating and configuring user accounts

In **General menu, Account, Users**, you can perform all of the necessary actions related to creating and modifying user accounts.

- **Add new user account**: Click **Add User** to add a new user, set a password, specify the level or security levels to which it belongs and define the associated Component level (from 1 to 5).



The Component level associated to a user allows you to restrict access to the components developed or imported from the ComStore with a higher security level.



Add User

Enter the details of the user you wish to add. You will assign rights for this user later.

Username:

Password:

Password Again:

Email:

First name:

Last name:

Roles:

<input checked="" type="checkbox"/>	<input type="checkbox"/>	Default	
<input type="checkbox"/>	<input type="checkbox"/>	accountadmin	
<input type="checkbox"/>	<input type="checkbox"/>	Custom_panda.test@panda345.com	Migrated custom role for panda.test@pand...
<input type="checkbox"/>	<input type="checkbox"/>	Custom_panda1234@panda.com	Migrated custom role for panda1234@panda...
<input type="checkbox"/>	<input type="checkbox"/>	Custom_panda@example.com	Migrated custom role for panda@example.c...

Figure 98: assigning a user name, password and security level to a user account

- **Edit a user account:** Clicking a user name displays a form with all of the **account** details.
- **Delete or disable user accounts:** Select a user by selecting the associated checkbox and click the prohibited and cross icons on the **Action bar**.
- **Assign total control permissions:** Click On/OFF in **Account Admin**.

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.

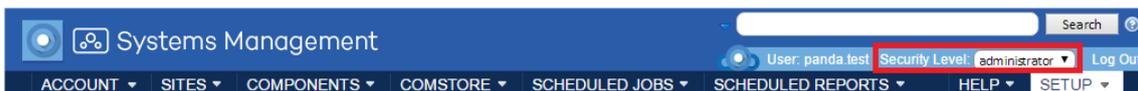


Figure 99: changing the security level of an existing user account

16.8. Creating and configuring security levels

In general menu, **Account**, security levels, you can perform all of the necessary actions related to creating and modifying security levels.

- **Add new Security level:** Click **Add Security level** to add a new security level. You will be prompted to enter the name and whether you want to use a blank configuration/template as a base or if the new security level will be based on a previous security level.
- **Edit a Security level:** Clicking a security level name or the pencil icon displays a form with all of its settings.
- **Delete Security level:** The X icon deletes the selected security level.



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.

16.9. 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.

16.9.1 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**



You cannot allow access to dynamic groups such as filters.

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.

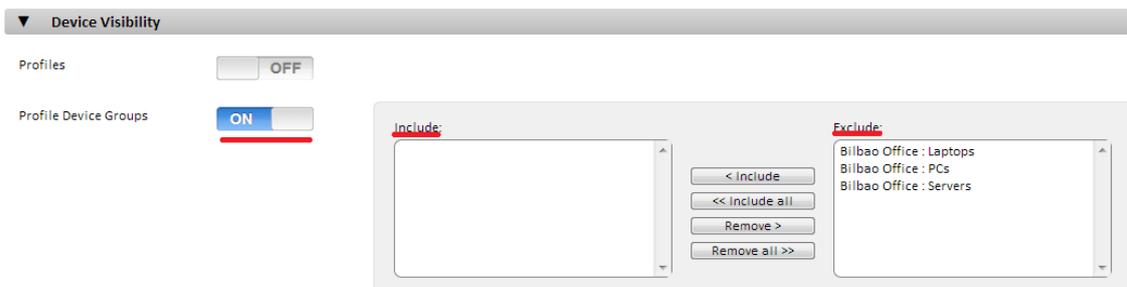


Figure 100: configuring the items accessible to a security level

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.

16.9.2 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:

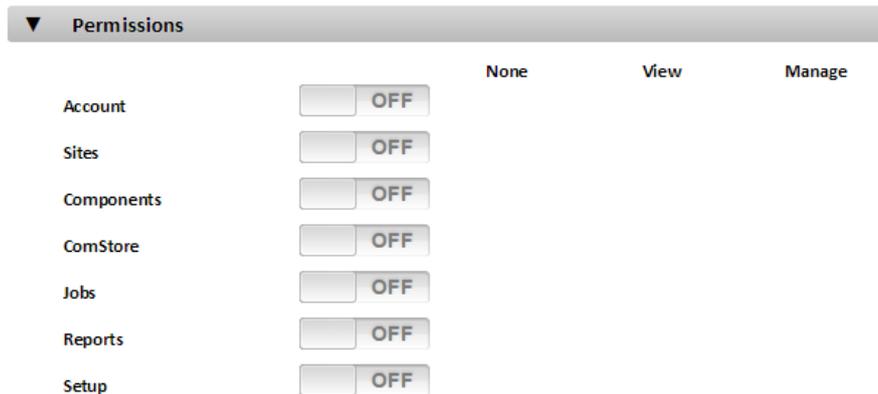


Figure 101: general menu items

To set the access level of each role 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. 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.

16.9.3 Agent Browser Tools

This setup group allows you to specify access to the remote administration tools available in the Agent.

Toggle all options:	<input type="checkbox"/> OFF		
ScreenShot	<input type="checkbox"/> OFF	LAN Deploy	<input type="checkbox"/> OFF
Services	<input type="checkbox"/> OFF	Task Manager	<input type="checkbox"/> OFF
VNC	<input type="checkbox"/> OFF	File Transfer	<input type="checkbox"/> OFF
RDP	<input type="checkbox"/> OFF	Registry Editor	<input type="checkbox"/> OFF
Command Shell	<input type="checkbox"/> OFF	Quick Jobs	<input type="checkbox"/> OFF
Restart/Shutdown	<input type="checkbox"/> OFF	Event Viewer	<input type="checkbox"/> OFF
Thumbnail Screen	<input type="checkbox"/> OFF	Notes	<input type="checkbox"/> OFF
Chat	<input type="checkbox"/> OFF	Wake-On-Lan	<input type="checkbox"/> OFF

Figure 102: configuring access to the PCSM Agent management tools



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).

16.9.4 Membership

Allows you to configure the user accounts that belong to the security level configured.

16.10. 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.

16.10.1 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:

- 1 site or device group that groups the office's devices.
- 1 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.

16.10.2 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, whilst 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.

16.10.3 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 tab bar, **Reports** and read-only access to the rest of the Console.
- Script development and software deployment technicians: With access to general menu, **Components** and **ComStore**
- Support technicians: With access to **Tab bar**, **Support** 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.

17. Mobile Device Management

Supporte platforms

Mobile Device Management policies

Tools for remotely managing devices

17.1. Introduction

Panda Systems Management includes MDM (Mobile Device Management) tools that enable you to manage the mobile devices on your company's IT network easily and centrally. With **Panda Systems Management**, you'll be able to respond to the challenges posed by the growing presence of mobile devices in the workplace from the same console that you use to manage the rest of your IT infrastructure.

17.2. Supported platforms

Panda Systems Management supports iOS and Android tablets and smartphones.

More specifically, the solution supports iPhone and iPad tablets using iOS 6 or later. Here is a list of the supported models:

Modelo
iPhone 4, 4S
iPhone 5, 5c, 5s, SE
iPhone 6, 6 Plus
iPhone 6s, 6 Plus
iPhone 7, 7 Plus
iPhone 8, 8 plus
iPhone X
Ipod Touch 5 ^o , 6 ^o generation
iPad 2, 3, 4, Air, Air 2, mini, mini 2, mini 3, mini 4, Pro (all sizes)

Table 26: list of iOS devices compatible with Panda Systems Management

Panda Systems Management supports Android devices running version 2.3.3 (Gingerbread) and later. This is the vast majority of Android devices currently in use.

17.3. 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.



Refer to Chapter 9: Policies for more details.



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

17.3.1 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.

17.3.2 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 users' passwords.
Minimum passcode length	
Minimum Number Of Complex Characters	Lets you set a minimum number of non-alphanumeric characters for valid passwords.
Maximum Passcode Age	Lets you set the maximum valid period for a password.
Auto Lock	

Field	Description
Passcode History	The device keeps a history of passwords used by users to prevent them from being re-used when choosing a new password.
Maximum Number Of Failed Attempts	

Table 27: passcode settings

Restriction

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.
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 or 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	Allows users to access Control Center when the device is locked.
Show Notification Center in lock screen	Displays Notifications Center when the device is locked.
Show Today view in lock screen	Displays the Today view in Notifications Center when the device is locked.

Field	Description
Allow documents from managed apps in unmanaged apps	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	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	Allows 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
Allow iCloud document sync	Allows document sync
Allow iCloud Keychain sync	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 TV Shows	Allows or blocks TV shows based on the specified ratings

Field	Description
Show iMessage	Allows users to use iMessage
Allow app removal	Allows uninstallation of apps
Allow Game Center	Permits the use of 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)
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 28: usage restrictions settings

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

Field	Description
Proxy Type	Proxy to be used with the VPN connection

Table 29: VPN settings

Wi-Fi

Field	Description
SSID	Sets the Service Set Identifier
Security	Type of Wi-Fi security
Password	Wi-Fi password
Proxy Type	Proxy to be used with the Wi-Fi connection

Table 30: WiFi connection settings

17.4. Tools for remotely managing mobile devices

This section describes the tools available from the Console, how they work and the benefits they provide.

The Console's mobile device management features are only available at Device Level for the relevant device.

After you select a mobile device in the console, the Action bar and the Tab bar will change automatically, displaying the new actions available.

17.4.1 Device Wipe

This feature performs a remote factory reset of the device, preventing data theft in the event of loss, theft or malfunction.



Please be aware that this will remove any user data (programs, specific configurations, modifications) stored on the device. The device is returned to its factory settings.

17.4.2 Geolocation

This feature shows 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.

17.4.3 Device Lock

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.

17.4.4 Device Unlock

This feature unlocks a locked device (it resets the security PIN should the user forget it).

17.4.5 Password Policy

This feature works in conjunction with the Device Lock feature as it forces the owner of the device to set a password (PIN). When enabled, 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.

17.4.6 Audits

Audits work in the same way as on Windows devices, and are fully integrated in the Console. This feature allows filters to be set on mobile devices based on the programs installed, for example.

The Agent collects all hardware and software information from the device on which it is installed, and notifies any changes to the Server, which displays them on the **Audit** tab.

The **Hardware** section displays the following information about mobile devices:

- Operating system and version.
- Model.
- ICCID (Integrated Circuit Card ID, a unique number that identifies SIM cards).
- SIM card operator.
- SIM card phone number.
- Storage (internal memory and SD card memory).
- Network adapters installed on the device (generally Wi-Fi).

The **Software** section shows all packages installed on the device.

The **Changelog** section reports all hardware and software changes made to the device.

17.4.7 Reports

The reports adapt to the type of device.

The **Reports** tab behaves in the same way as for Windows and Mac devices.

18. Activity log

[Account level activity log](#)

[General activity log](#)

[Device level activity log](#)

18.1. Introduction

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.

18.2. 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.

18.3. 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**.

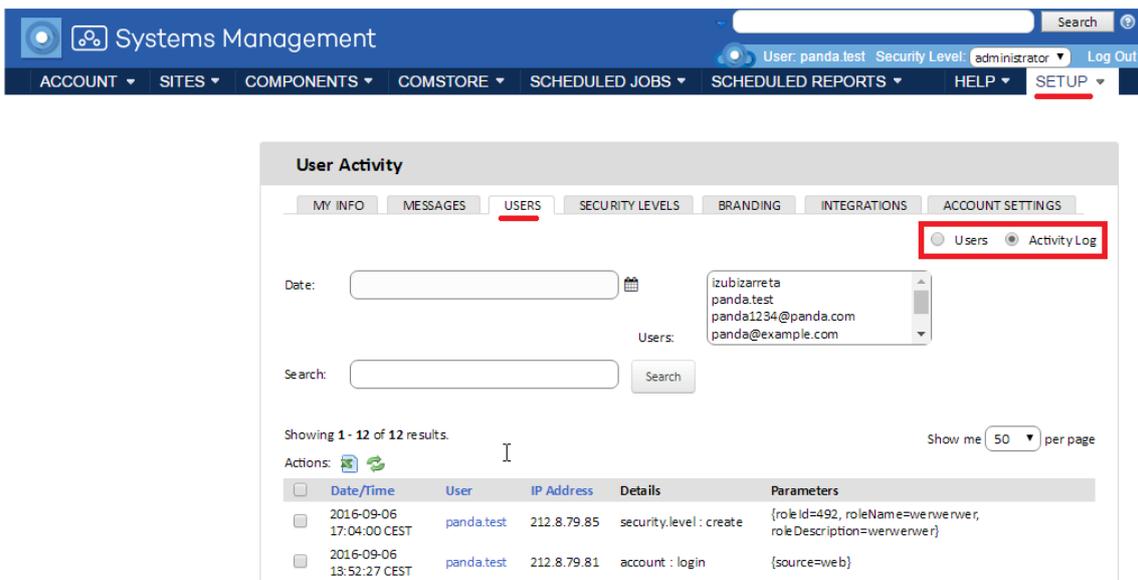


Figure 103: list of actions taken by the administrator

18.3.1 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.

18.3.2 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

18.4. 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: from the **Summary** tab at device level (general menu **Sites**, select the site that contains the device and click the specific device) and from the **Reports** tab, using the **Activity log** selector.

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.
- **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.

19. Reports

Accessing the reports system

Generating reports

Reports features and type of information

Executive reports

Activity reports

Alert reports

Inventory reports

Health reports

Patch management reports

Other reports

19.1. Introduction

Panda Systems Management offers numerous ways of viewing the information collected from the company's IT resources, and one of these is the reports system.

The reports system lets you export the data about the status of your devices to .PDF format, and configure the data to the needs of those to whom the reports are aimed. The data can also be exported to .XLS if you want to manage the information with external tools.

There are more than 50 types of reports covering all aspects managed by **Panda Systems Management**. This chapter explains how to select the report depending on who it is aimed at, and offers a general description of each report.

19.2. Accessing the reports system

The report system can be accessed through the three levels of **Systems Management**. The level of detail of the information will vary depending on the selected level, as well as the range of devices whose data will be included in the report.

Not all reports are available at all levels; many of them are only for specific devices (Device level) or would be more relevant for a specific site or for the entire managed account.

The three levels of reports are accessible from the **Reports** tab in the tab menu. When the tab menu is accessed from the general **Account** menu, you will see a window with the reports that are available for that level. Similarly, when selecting a specific site or device, the **Reports** tab displays the reports that are available for the Site or Device level.

19.3. Generating reports

Reports can be generated on demand or scheduled.

19.3.1 Generating reports on demand



Click the   icons in the list of reports in the **Reports** tab to launch a process to collect data in the background which will conclude with a download popup in the top-right corner of the screen.

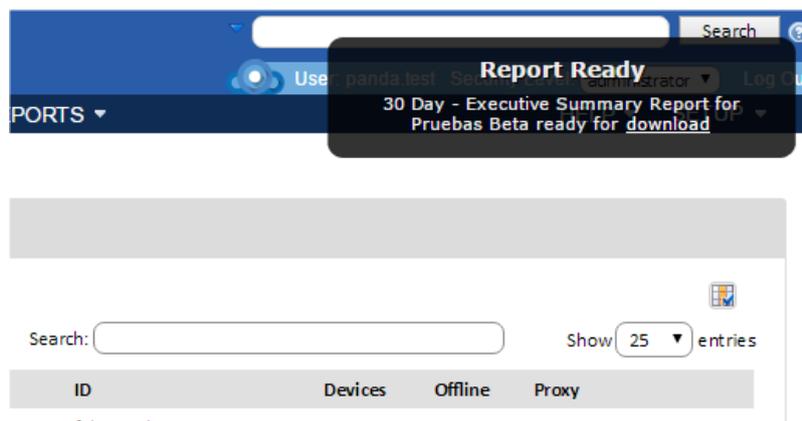


Figure 104: report download popup

You can generate as many reports as you need.

19.3.2 Scheduled generation of reports

You can schedule the generation of reports by clicking the relevant icon in the actions bar of the **Reports** tab.

A new window will be displayed with the information required to schedule the generation of one or more reports.

- **General**
 - **Name:** Name of the report generation job.
 - **Description:**
 - **Schedule:** You can determine when the report generation job will run.
 - **Enable:** This lets you enable or disable the report generation settings so that they can be ready to use but without creating unnecessary noise.
- **Reports:** Select the reports to generate in PDF and/or Excel.
 - **Email recipients**
 - **Subject**
 - **Text**
 - **Default account report recipients:** Sends the reports to the email accounts set for the site, which can be configured in Email Recipients in the Settings tab, in the selected site.
 - **Default site report recipients:** Sends the reports to the email accounts set for the entire Systems Management account, which can be configured in Email Recipients in the general Setup menu.
 - **Additional recipients:** This lets you add additional email addresses to those configured at Account or Site level.

19.4. Reports features and type of information

The reports are defined by preconfigured parameters and features which it is necessary to understand in order to generate the right report. The parameters are reflected in the name of the report and the level (Account, Site or Device) at which they were created.

The parameters that define a report are as follows:

- **Level**
- **Time period**
- **Type of report**

19.4.1 Level

The level (Account, Site or Device) is used to define the scope of the report.

- **Account:** Includes all devices in the account.
- **Site:** Includes all devices in the selected site.
- **Device:** Information for the selected device.

19.4.2 Time period

Establishes the time period that will be covered by the report. This period will be defined in the name of the report with the prefix "x day".

- **30 Day:** Contains information from the last 30 days. The report includes data up to the day before it is generated.
- **7 Day:** Contains information from the last seven days. The report includes data up to the day before it is generated.
- **No prefix:** Reports that only include data on the status of the device at the moment that the report is generated.



In some cases, the reports cover complete weeks or months in the past. This is indicated in the report description and they are used by partners (VAR or MSP) to demonstrate to end-customers the activities performed during the corresponding invoice period.

19.4.3 Type of report

The type of report is indicated in the name and reflects the aspects of the company's IT resources that are covered in the report. Below you can see the different types of reports and later in this chapter, the various reports have been grouped by type, with an explanation for each one.

Executive

Executive reports summarize in a single document several aspects of the managed network. They are useful to get a quick idea of the network status, without going into too much detail, and to show general trends and developments.

Activity

These display the activity of the network administrators responsible for managing the company's devices. Depending on the report, the activity can be broken down into the following groups:

- **Jobs**
- **Command Shell**
- **Remote Support**
- **Notes**

Alert

These show the alerts generated by monitors and other components, which in turn help ensure the IT resources are operating normally. They also show the productivity of employees whose downtime due to IT failures is reduced, as well as that of the IT staff, measured in the average time of incident resolution.

Inventory

These compile details of the assets managed by the IT department, both hardware and software, and can determine if there is obsolete or inadequate technology on the network which ought to be replaced.

Health

These reflect the propensity of devices to generate problems, depending on parameters such as if there is an antivirus, absence of critical patches, etc.

Performance

These include details on CPU and hard disk usage and other parameters that indicate the performance of a device.

Patch management

These reports reflect the extent to which systems on the network are up-to-date with patches: which patches are required, which are critical and the security level of network devices.

Other reports

This category includes those reports that don't fit into the other categories.

19.5. Executive reports

19.5.1 30/7 Day Account Executive Summary (Account)

Time period: Last 7 or 30 days.

Scope: Account.

Information:

- Top 5 sites by activities
- Top 5 sites by alerts
- For each site:
 - Totals for activities
 - Alerts by category
 - Individual user activity

19.5.2 30 Day - Executive Summary Report (Site Level)

Time period: Last 7 or 30 days.

Scope: Site.

Information:

- Overview of the current status of servers:
 - Inventory
 - Disk usage
 - Patch status
 - Missing critical patches
 - Uptime
- Overview of the current status of workstations:
 - Replacement recommendations
 - Operating systems in use
 - Inventory checks
- Details:
 - Workstations' hardware inventory
 - Disk usage
 - Patch status and missing critical patches
- Lists:
 - Managed network devices
 - Managed mobile devices
- Summarizes:

- Monitoring alerts (by totals per category)
- Activity on devices (by totals per category, total time and the number of activities of the top 5 devices)

19.5.3 30/7 Day Site Executive Summary (Site)

Time period: Last 7 or 30 days.

Scope: Site.

Information:

- Total activities and times by category
- Lists top 5 devices by number of activities
- Details for each activity, by device

19.5.4 30 Day - Executive Summary Report - Only Servers and Workstations (Site Level)

Time period: Last 30 days.

Scope: Site.

Information:

- Status of servers:
 - Inventory
 - Disk usage
 - Patch status
 - Missing critical patches
 - Uptime
- Status of workstations:
 - Replacement recommendations
 - Operating systems in use
 - Inventory checks
- Details workstation:
 - Hardware inventory
 - Disk usage
 - Patch status
 - Missing critical patches

19.6. Activity reports

19.6.1 30/7 Day Site Activity Summary

Time period: Last 7 or 30 days.

Scope: Site.

Information:

- Total activities and times by category
- Lists the top 5 devices by number of activities
- Details for each activity, by device

19.6.2 30 Day/7 Account Activity Summary

Time period: Last 7 or 30 days.

Scope: Account.

Information:

- Top 5 sites by number of activities
- For each site:
 - Lists activities by category with totals and detail amounts

19.6.3 Site Activity

Time period: Last 30 days.

Scope: Site.

Information:

- Lists Jobs, Notes and Remote Takeover sessions

19.6.4 30/7 Day Account User Summary

Time period: Last 7 or 30 days.

Scope: Account.

Information:

- Lists activities by category, with total quantity and details
- For each username:
 - Site activity, time started and ended and total time.

19.6.5 Remote Activity

Time period: Last complete month.

Scope: Account.

Information:

- Lists all the remote control sessions:
 - Username, site and hostname, start and end date and time, length, and the remote takeover tool that was used.

19.6.6 Site Remote Takeover Report

Time period: Last 30 days.

Scope: Site.

Information:

- Lists all the remote control sessions:
 - Username, site and hostname, start and end date and time, length, icon of the remote takeover tool used.

19.6.7 30/7 Day Device Activity Summary

Time period: Last 7 or 30 days.

Scope: Device.

Information:

- Total activities and times by category
- Lists details for each activity event:
 - Username
 - Date/time started and ended
 - Total time

19.7. Alert reports

19.7.1 30/7 Day Site Alert Summary

Time period: Last 7 or 30 days.

Scope: Site.

Information:

- Total number of alerts and average response time by category.
- For each alert:
 - Priority, alert date and time, end time and time of response.

19.7.2 30/7 Day Account Alert Summary

Time period: Last 7 or 30 days.

Scope: Account.

Information:

- Lists the top 5 sites by number of alerts.
- For each site:
 - Alerts by type with total number and total time.

19.7.3 30/7 Day Device Alert Summary

Time period: Last 7 or 30 days.

Scope: Device.

Information:

- Total number of alerts and average response time by category
- For each alert:
 - Priority, alert date and time, end time and time of response

19.7.4 Monitor Alerts Report (Device Level)

Time period: Current.

Scope: Device.

Information:

- For each alert by type:
 - Includes alert message, priority and time of alert

19.7.5 Monitor Alerts Report (Site Level)

Time period: Current.

Scope: Site.

Information:

- Lists device name, alert type, message and priority, and date/time of alert

19.7.6 Monitor Alerts Report (Account Level)

Time period: Current.

Scope: Account.

Information:

- Lists device name, site, total number of active alerts, and number of active alerts broken down by priority.

19.8. Inventory reports

19.8.1 Computer Summary

Time period: Current.

Scope: Site.

Information:

- For each computer:
 - Name, operating system and service pack
 - Memory, processor, letter label
 - Total drive space, amount and percentage of free space.

19.8.2 Critical 3rd-Party Software Summary Report

Time period: Current.

Scope: Site.

Information:

- Lists all Windows and Mac devices in the Site with a PCSM agent installed:
 - For each device, the reports shows the version of multiple critical third-party software applications:
 - Skype
 - QuickTime
 - Java
 - Adobe Acrobat Reader
 - Mozilla Firefox
 - Adobe Flash

- Adobe Air
- Adobe Shockwave
- Google Chrome
- Silverlight

19.8.3 Site Serial Numbers

Time period: Current.

Scope: Site.

Information:

- Lists each device with serial number

19.8.4 Account Server IP Information

Time period: Current.

Scope: Account.

Information:

- IP address for all servers

19.8.5 Account Server Storage

Time period: Current.

Scope: Account.

Information:

- Storage information for servers (graphically displayed):
 - Drive label, size
 - Amount and percentage of space

19.8.6 Site Server Storage

Time period: Current.

Scope: Site.

Information:

- For each server:
 - Drive letter
 - Size

- Amount and percentage of free space.

19.8.7 Site Software

Time period: Current.

Scope: Site.

Information:

- For each installed software:
 - Number of installations

19.8.8 Site Software and Hotfixes

Time period: Current.

Scope: Site.

Information:

- For each installed software:
 - Number of installations.

19.8.9 Software Audit Report

Time period: Current.

Scope: Site.

Information:

- The report shows the following information for each device in the Site:
 - Installed software
 - Software version

19.8.10 User Software Install

Time period: Last 30 days.

Scope: Site.

Information:

- For each installed software:
 - Software name
 - Version

- Changes (added or deleted)
- Date the action was taken

19.8.11 Site Storage

Time period: Current.

Scope: Site.

Information:

- For each device:
 - Name
 - Letter
 - Size
 - Amount and percentage of free space

19.8.12 Site IP Information

Time period: Current.

Scope: Site.

Information:

- For each device:
 - Adapter name
 - IP address

19.8.13 Detailed Computer Audit

Time period: Last 7 or 30 days.

Scope: Account.

Information:

- For each computer:
 - Hardware information: asset tag and date, Serial number, memory, motherboard, BIOS, processor, video
 - Domain and username
 - Virus scanner details
 - Date of last contact
 - OS, Windows update
 - IP and MAC addresses
 - Physical disk drive size and free space

19.8.14 Device Summary

Time period: Current.

Scope: Device.

Information:

- For each device:
 - Agent version and status
 - Domain, last user
 - Last audit date, last seen date
 - Hardware: manufacturer, model, ID, motherboard, processor, memory, storage, display and network adapters, and monitor information
 - Software: operating system, service pack, serial number, software installed with version number
 - Security: anti-virus, firewall and updates

19.8.15 Device Change Log

Time period: Since the last agent was installed.

Scope: Device.

Information:

- Changes to the system:
 - When software was changed, added or deleted.
 - Date and IP address.

19.8.16 Site Device

Time period: Current.

Scope: Site.

Information:

- For each device:
 - IP Address
 - Last updated date
 - Model, Serial number
 - Last logged-on user

19.8.17 Inventory Age

Time period: Current.

Scope: Site.

Information:

- Displays replacement recommendations for the next 12 months to two years
- Lists operating systems in use
- Lists individual devices by name, last user, serial number and build date
- Warnings for low memory, free disk space or not online this month

19.8.18 Microsoft License

Time period: Current.

Scope: Site.

Information:

- Lists software type, Microsoft product name, and quantity of devices with that product installed

19.9. Health reports

19.9.1 Customer Health Summary

Time period: Current.

Scope: Site.

Information:

- Hardware Summary
- Security Summary
- Maintenance software Summary
- Players and readers installed
- How many devices have failed or passed the test
- Devices with a warning

19.9.2 Exception Report

Time period: Current.

Scope: Site.

Information:

- Summary of all MS Windows devices:
 - Warnings for devices without updated anti-virus
 - MS updates
 - Firewall
 - Devices with low free disk space
 - Devices not online this month

19.9.3 Site Health

Time period: Current.

Scope: Site.

Information:

- Lists number of devices by operating system:
 - Build number
- lists the number of devices without:
 - Updated anti-virus,
 - MS updates or firewall
 - Low free disk space or memory
 - Not online this month
- For each device:
 - Name
 - Last logged-in user
 - Status

19.9.4 Health Report

Time period: Last 30 days.

Scope: Site.

Information:

- Summary by servers and workstations, with and without warnings
- Lists alerts, jobs run, and remote takeover minutes
- Alert turnaround time summary
- Lists individual devices by hostname, IP address, and last logged in user
- Shows warnings for devices without updated anti-virus, anti-spyware, MS updates or firewalls
- Shows warnings for devices with low disk space and not online this month.

19.10. Patch management reports

19.10.1 Patch Management Activity Report

Time period: Last 30 days.

Scope: Site.

Information:

- The report shows the following information for each device:
 - Number of patches released, patches installed and approved pending patches
 - Percent of approved pending patches, and number of alerts
- Devices requiring attention
- Summary and analysis of fully patched/not fully patched devices
- Detailed list of patches by device:
 - Name
 - Critical rating
 - Installation status

19.10.2 Patch Management Detailed Report

Time period: Current.

Scope: Site.

Information:

- For each device:
 - Number of patches released, installed and missing
 - Percent missing and number of alerts
- Lists devices missing patches
- Summary and analysis of devices requiring patches by number of patches needed
- Detailed list of patches by device:
 - Name
 - Critical rating
 - Installation status

19.10.3 Patch Management Summary Report

Time period: Current.

Scope: Site.

Information:

- Percentage of devices fully patched or missing specific number of patches
- Lists devices missing patches and number missing
- For each device:
 - Number of patches released, installed and missing

19.11. Other reports

19.11.1 Site User-Defined Fields

Time period: Current.

Scope: Site.

Information:

- Report on User-Defined Fields

19.11.2 Server Performance Report (Site Level)

Time period: Last 30 days.

Scope: Site.

Information:

- For each server shows performance on:
 - CPU
 - Memory
 - Disk
 - Average of the CPU and Memory
 - Delta of the available disk space

19.11.3 Server Performance Report (Account Level)

Time period: Current.

Scope: Account.

Information:

- For each server shows performance on:
 - CPU
 - Memory
 - Disk

- Average of the CPU and Memory
- Delta of the available disk space

20. Service access security and control

Two-factor authentication

Password policy

IP-based access control to the Console

IP-based access control from the Agent to
the Server

20.1. Introduction

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.

20.2. Two-factor authentication

Two-factor authentication 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

20.2.1 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.

20.2.2 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**.
- 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** later in this chapter).
- 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**.

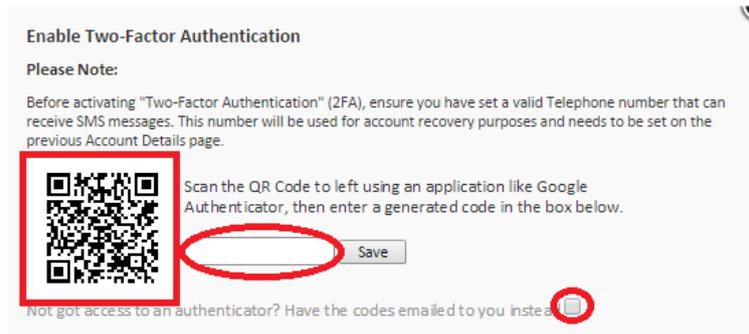


Figure 105: token generation and emailing screen

- 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.

20.2.3 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**.

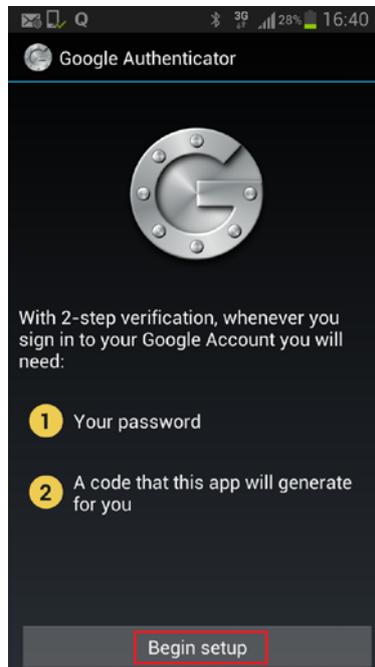


Figure 106: Google Authenticator settings screen

- Tap **Scan a barcode** to scan the QR code displayed in the Console.

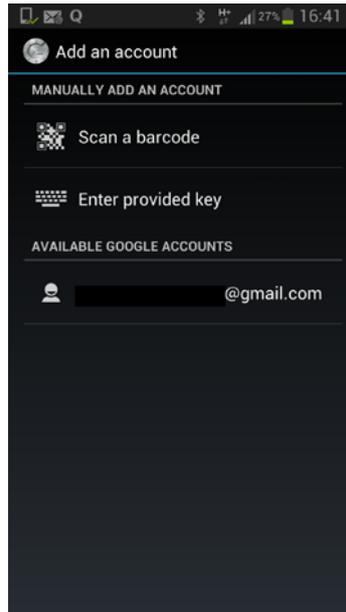


Figure 107: scanning the QR Code

- The app will start to generate tokens automatically. Each token is valid for 30 seconds.

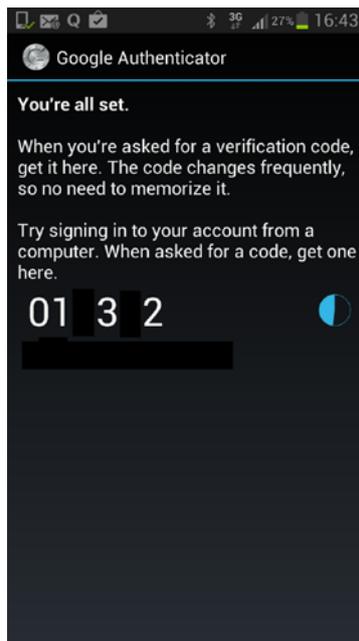


Figure 108: token generation screen

20.2.4 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 **Account, Setup, 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.

20.2.5 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.

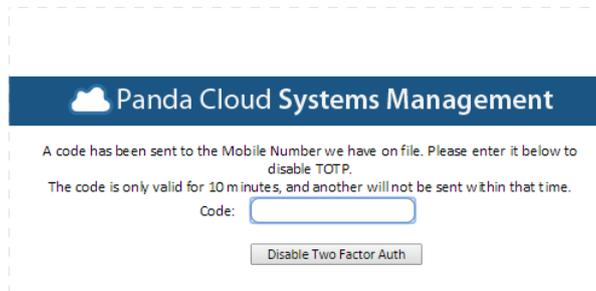


Figure 109: window for disabling Two-Factor Authentication

20.3. 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.

20.4. IP address restrictions to grant or deny access to 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.

20.5. IP address restrictions to grant or deny access from the Agent to the Server

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.

21. Appendix A: Source code

[Chapter 10](#)

[Chapter 11](#)

21.1. Chapter 10

Option Explicit

```

'*****
'Quarantine_Monitor v0.99b
'06/03/2013
'By Oscar Lopez / Panda Security
'Target: It monitors changes on PCOP quarantine folder
'Input: PCOP_PATH environment variable
'Output: stdout "Result=n new items detected in PCOP quarantine",
'n is the added file number in the monitored folder
'*****

dim WshShell,WshSysEnv
dim objFSO,objFolder,colFiles
dim iCountPast,iCountNow
dim bHit
Dim n

Set WshShell = WScript.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("PCOP_PATH"))
  if err.number <> 0 then
    'SM didn't send the environment variable
    err.clear
    WScript.Echo "<-Start Result->"
    WScript.Echo "Result=PCOP_PATH variable not defined on SM console or
path not found"
    WScript.Echo "<-End Result->"
    Set WshShell = nothing
    Set WshSysEnv = nothing
    Set objFolder = nothing
    WScript.Quit(1)
  end if
On error goto 0

'it gets the collection that contains the folder files
set colFiles = objFolder.files

On error resume Next
  'access to the registry. 10 incremental entries will be created, one per
minute.
  n=0
  While Err.Number=0 And n < 10
    iCountPast= cint(WshShell.RegRead("HKLM\Software\Panda
Security\Monitor" & n))
    If err.number<>0 then
      WshShell.RegWrite "HKLM\Software\Panda Security\Monitor" & n,
colFiles.count, "REG_SZ"
    Else
      n=n+1
    End If
  Wend
  Err.Clear

```

```
    If n=9 Then
        iCountPast= cint(WshShell.RegRead("HKLM\Software\Panda
Security\Monitor0"))
        iCountNow= cint(WshShell.RegRead("HKLM\Software\Panda
Security\Monitor9"))
        if iCountPast < iCountNow then
            'there are more items in the folder, it updates the registry and
sends an alert
            WScript.Echo "<-Start Result->"
            WScript.Echo "Result=" & iCountNow - iCountPast & " new items in
PCOP quarantine"
            WScript.Echo "<-End Result->"
            bHit=true
        end if
        For n=0 To 9
            WshShell.RegDelete("HKLM\Software\Panda Security\Monitor" & n)
        Next
        WshShell.RegWrite "HKLM\Software\Panda Security\Monitor0",
colFiles.count, "REG_SZ"

        end if
    On error goto 0

'finale
Set colFiles = nothing
set objFolder = nothing
set WshShell = nothing
set WshSysEnv = nothing
set objFSO = nothing

if bHit then
    WScript.Quit (1)
else
    WScript.Quit (0)
end if
```

21.2. Chapter 11

Option Explicit

```

'*****
'Deploy_documents v0.99b
'12/03/2013
'By Oscar Lopez / Panda Security
'Target: It creates a folder on the user's desktop and copies the
'documents to deploy to it
'Input: files to copy
'Output: error code or OK
'*****

```

```
Dim CONST_PATH
```

```
Dim objFSO,objFolder,colFiles
```

```
'Maybe you want to use a global variable for this constant?
```

```
CONST_PATH="C:\ACME Documents"
```

```
On Error Resume Next
```

```
Set objFSO=CreateObject("Scripting.FileSystemObject")
```

```
Set objFolder = objFSO.Getfolder(CONST_PATH)
```

```
If Err.Number=0 Then
```

```
    'the folder already exists, the files won't be copied
```

```
    WScript.Echo "Deploy unsuccessful: The folder already exists"
```

```
    WScript.Quit (0)
```

```
End If
```

```
'the folder will be created on the user's desktop
```

```
Err.Clear
```

```
Set objFolder = objFSO.CreateFolder(CONST_PATH)
```

```
'the documents will be moved to the folder
```

```
objFSO.MoveFile "doc1.docx", objFolder.Path & "\doc1.docx"
```

```
objFSO.MoveFile "doc2.docx", objFolder.Path & "\doc2.docx"
```

```
objFSO.MoveFile "doc3.docx", objFolder.Path & "\doc3.docx"
```

```
If Err.Number<>0 Then
```

```
    WScript.Echo "Deploy unsuccessful: " & Err.Description
```

```
    WScript.Quit (1)
```

```
Else
```

```
    WScript.Echo "Deploy successful: All files were copied"
```

```
    WScript.Quit (0)
```

```
End If
```

```
On Error Goto 0
```

```
WScript.Quit (0)
```

22. Appendix B: Supported platforms

[Supported platforms](#)

[Detailed Windows requirements](#)

[VMWare ESXi requirements](#)

22.1. Supported platforms

For Windows

- Windows XP SP3 (Home, Professional, Professional x64)
- Windows Vista 32/64-bit (Starter, Home Basic & Premium, Business, Enterprise, Ultimate editions)
- Windows Server 2003 & R2 SP2 32/64-bit (Web, Standard, Enterprise, Datacenter, Small Business, Home Server editions)
- Windows 7 (32/64-bit)
- Windows 8/8.1 (32/64-bit)
- Windows 10 (32/64-bit)
- Windows 2008 & R2 32/64-bit (Standard, Enterprise, Datacenter, Web, Small Business editions)
- Windows Server 2012 (64-bit) & Windows Server 2012 R2

For Apple Macintosh (1)

- macOS 10.12
- macOS 10.13

For Linux

- Fedora 19, 20, 21
- CentOS 7
- Debian 7, 8
- Ubuntu LTS
- Red Hat Enterprise Linux 7 and later (3)

For smartphones and tablets

- iOS 7 and later
- Android 2.3.3

Supported browsers: (4)

The PCSM Console supports the last two versions of the following browsers:

- Internet Explorer
- Google Chrome
- Mozilla Firefox
- Safari



(1) The PCSM Agent will work on macOS 10.7.x and later versions but support is provided and the Agent is tested only on the versions specified above.

(2) The PCSM Agent may work with any Debian-based distribution but support is only provided for the ones listed.

(3) For new installations of the PCSM Agent you must pre-install the Mono runtime.

(4) The PCSM Console may work with earlier versions of the aforementioned Internet browsers or browsers from other vendors, but support is only provided for the ones listed..

22.2. Detailed Windows requirements

The 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.



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 4.0** (Requirement for .NET Framework 4.0.3 (<https://www.microsoft.com/en-us/download/details.aspx?id=17718>))
- **Framework .NET Full 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 7 and later operating systems automatically meet these requirements.

- **Windows Imaging Component** (<https://www.microsoft.com/en-us/download/details.aspx?id=32>)

22.3. 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 reside on the same subnet as the ESXi server.

Panda Systems Management supports ESXi versions 4.1, 5.0, 5.1, 5.5, 6.0 and 6.5.

In the case of VMware ESXi 6.5, you need to establish an SSH connection in order to enable CIM access. Follow the steps below:

- 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
```



Panda Systems Management

Neither the documents nor the programs that you may access may be copied, reproduced, translated or transferred to any electronic or readable media without prior written permission from Panda Security, Santiago de Compostela, 12, 48003 Bilbao (Bizkaia) SPAIN.

Registered trademarks. Windows Vista and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. All other product names may be registered trademarks of their respective owners.

© Panda Security 2018. All rights reserved.