



PANDA
CLOUDSYSTEMS
MANAGEMENT

PANDA CLOUD SYSTEMS MANAGEMENT

Partners and Network Managers Guide



www.pandasecurity.com

PROLOGUE

Audience. Icons.

03

INTRODUCTION

Main features of Panda Cloud Systems Management. Panda Cloud Systems Management user profile. Key players of Panda Cloud Systems Management.

04

HIERARCHY OF LEVELS WITHIN THE PCSM MANAGEMENT CONSOLE

System Level. Profile Level. Device Level.

08

BASIC COMPONENTS OF THE PCSM CONSOLE

General Menu. Tab Bar / List Bar. Icon Bar / Action Bar. Filters and groups panel. Dashboards.

11

FILTERS AND GROUPS

What are groups and filters? Types of groups and filters. Groups. Filters.

16

HOW TO ARRANGE MANAGED DEVICES EFFICIENTLY

Differences between profiles, groups and filters. General approach and device management structure.

20

THE FIRST 8 STEPS TO START USING PCSM

Create and configure the first Profile. Deploy the PCSM Agent. Check the device list in the Profile and basic filtering...

22

POLICIES

What are Policies? How to define a System Policy. How to define a Profile Policy. How to define a Device Policy. Policy types. How to deploy a policy.

28

MONITORING

What is it? Composition of a monitor. Create monitors.

31

COMPONENT EXECUTION

Why develop components? What are the requirements for developing components? General architecture of PCSM components. Create a monitor component. Create a Script type component.

35

CENTRALIZED SOFTWARE DEPLOYMENT AND INSTALLATION

Objective of centralized software installation. Centralized software installation requirements. Package deployment and installation procedure...

43

TICKETING

What is the ticketing system? Description of a ticket. Create a ticket. Ticket Management.

52

PATCH MANAGEMENT

What is Patch Management? What patches can I deploy / apply? Patch deployment and installation. Audits.

55

USER ACCOUNTS AND ROLES

What is a user account? What is a role? Why are roles necessary? The accountadmin role. Access user account and role configuration. Create and configure user accounts...

61

MOBILE DEVICE MANAGEMENT

Which platforms are supported? Integrating mobile devices in PCSM. Tools for remotely managing mobile devices.

67

APPENDIX A

Source code of the component in chapter 10.

72

APPENDIX B

Source code of the component in chapter 11.

74

01. PROLOGUE

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




AUDIENCE

This documentation is written for technical staff that offer support services to users without IT knowledge and in two possible environments:

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

ICONS

This guide contains the following icons:

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



02. INTRODUCTION

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


- ✓ 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 Cloud 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.

MAIN FEATURES OF PANDA CLOUD SYSTEMS MANAGEMENT

The following are the most important features of the product:

Feature	Description
Cloud-based solution	No additional infrastructure at the client or the MSP / IT Department site. Manage all your devices anytime, anywhere.
Agent based	A very light Agent supporting NAT firewall and VPN connects each device to the PCSM Server .
Automatic detection of devices	A PCSM Agent installed on a single device can detect other devices connected to the same network and initiate automatic installation.
Scheduled and custom audits	Track all changes to the device (hardware, software and system).
Software license management	Keep track of all software installed.
Alerts and monitoring	Monitor CPU usage, memory and disk space, services and Exchange Servers, performance graphs, panel alerts... all in real time.
Create scripts and quick jobs	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	Automate deployment of updates and patches of the software installed.
Software deployment	Centralized update and software deployment.

Continue 

Feature	Description
Policies	Define a set of general settings to manage your IT environment in a flexible manner.
Remote access	Task manager, file transfer, registry editor, command prompt, event log viewer, etc. All of these integrated tools enable you to repair multiple devices without interrupting the users.
Remote control	Shared access to the user's desktop or total control. Supports firewalls and NAT.
Secure communications	All communications between the Agents and the PCSM Server are encrypted (SSL).
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 IM Messaging service.
ComStore	Extend the capabilities of the platform. Select and download the components you need.
Mobile Device Management (MDM)	Compatible with iOS and Android, enables you to monitor Smartphone's and tablets, locate them and avoid data loss in the casa of stolen or lost devices.

PANDA CLOUD SYSTEMS MANAGEMENT USER PROFILE

Most **Panda Cloud Systems Management** users will have a medium – high technical profile, as this tool provides daily maintenance of computing devices subject to constant use and change. However there are two specific, targeted user groups of **Panda Cloud Systems Management**:

✓ Enterprise level IT technicians

Technicians subcontracted or belonging to a company to offer a company-wide support service for devices and end-users. These scenarios often include the remote offices to which access is restricted so technicians must use monitoring tools and remote access for 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 client accounts that have decided to outsource or subcontract the IT Department for maintenance of their devices.

Main components of Panda Cloud Systems Management

✓ PCSM Console

A web portal accessible via compatible browsers, from anywhere, anytime with any web enabled device. Most of the daily tracking and monitoring tasks will be performed from this console via a browser. This resource is available to technical support only

✓ PCSM Agent

A small program, less than 5 megabytes, that is installed on each device to be managed. After installing the **PCSM Agent** on the device, its information will become directly accessible through the **PCSM Console**.

The **PCSM Agent** supports two execution modes:

User Mode and 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 by the administrator.

Administration Mode

After entering valid credentials, the network administrator can use the **PCSM Agent** in to access remote devices.

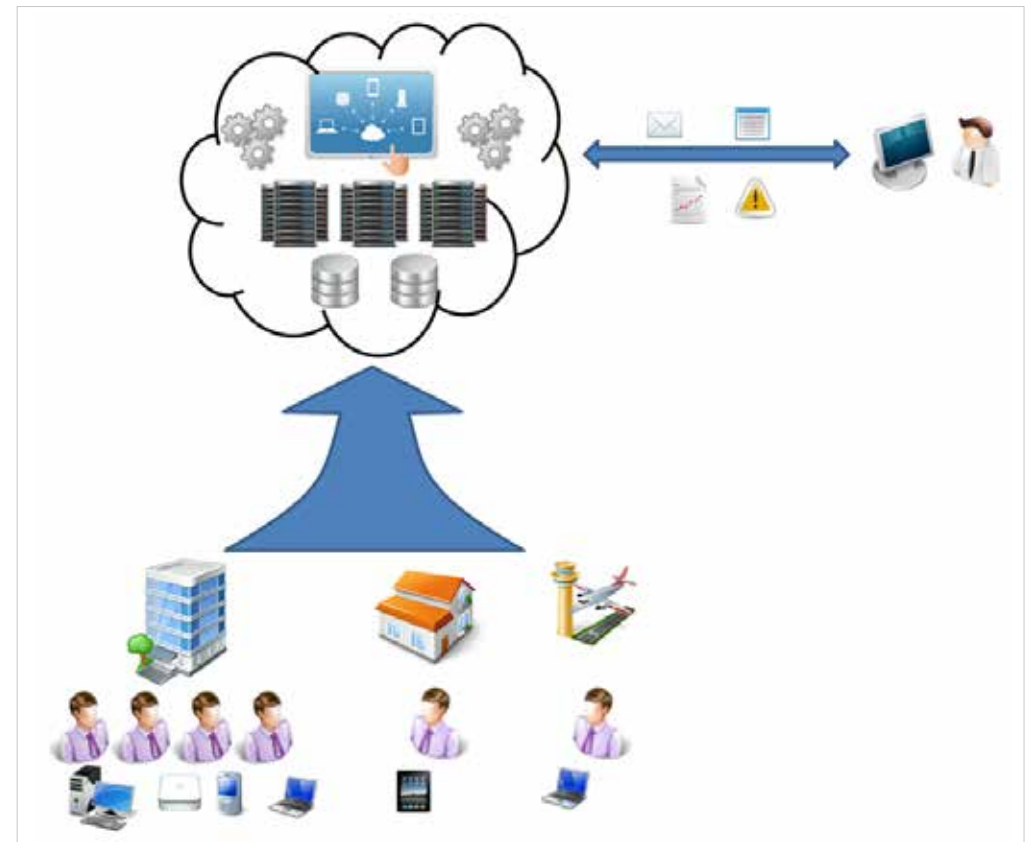


Install the **PCSM Agent** on both client devices and those belonging to the technicians for remote management.

✓ PCSM Server

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

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



KEY PLAYERS OF PANDA CLOUD 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 **PCSM 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 Cloud Systems Management** to manage and monitor its systems or the MSP staff who access the client's devices to manage and monitor them.

✓ **PCSM administration account / Principal administration account**

Each client or company using **Panda Cloud Systems Management** will be given a principal administration account. An account with the highest level of privileges that can manage all the resources of the product.



Chapter 14 describes how to create new users and roles in order to restrict the access of systems technicians' to key **Panda Cloud Systems Management** resources.

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

✓ **Client account / Client**

A client 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 14, describing how to create users and roles, 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 client network that will require maintenance.

✓ **User**

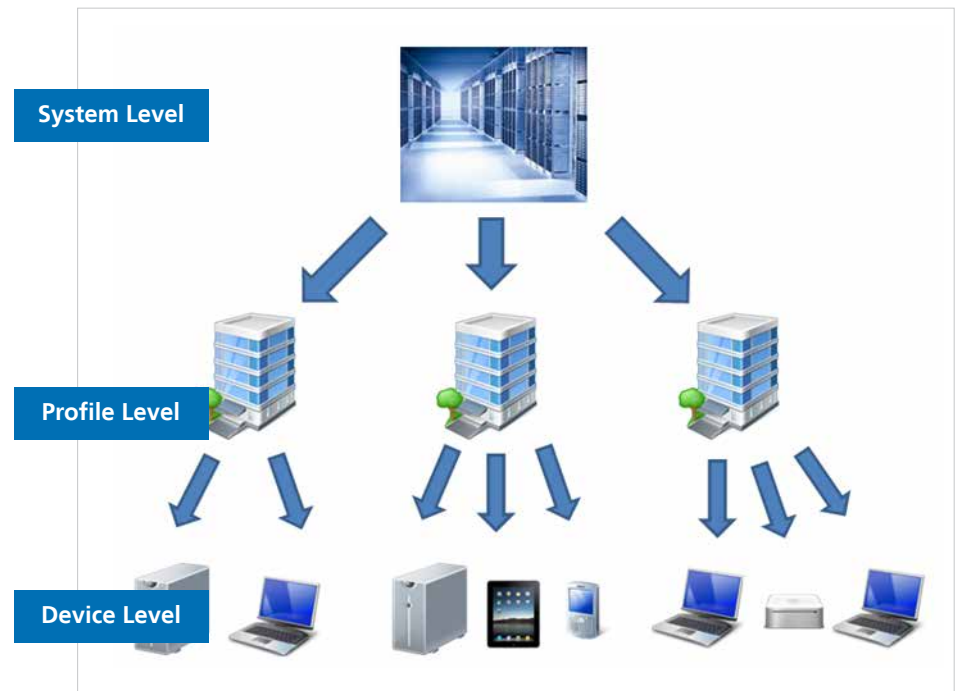
The user is the person using the device that requires direct support from the MSP or IT department.

✓ **Device**

A device is a computer with a **PCSM Agent** installed and which is used by the user in their daily work.

03. HIERARCHY OF LEVELS WITHIN THE PCSM MANAGEMENT CONSOLE

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



SYSTEM LEVEL

What is it?

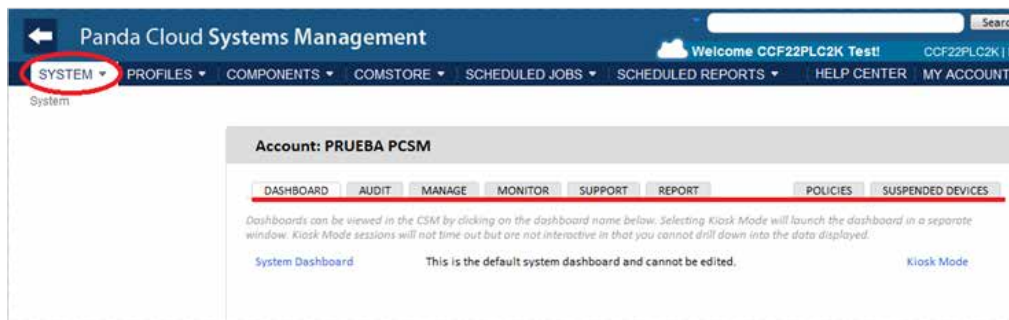
System Level also referred to as Account or Account level entity cluster is the most general and highest level, and is also unique for each MSP / IT Department. It automatically groups all devices managed by the MSP / IT Department belonging to their clients and users with a **PCSM Agent** installed.

Scope

The actions performed on this level will affect all devices registered on the system, although they can be limited to a subset of devices using filters and groups, described in chapter 5.

Access

The System Level resources are accessed from General Menu, System.



Functionality

System 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.

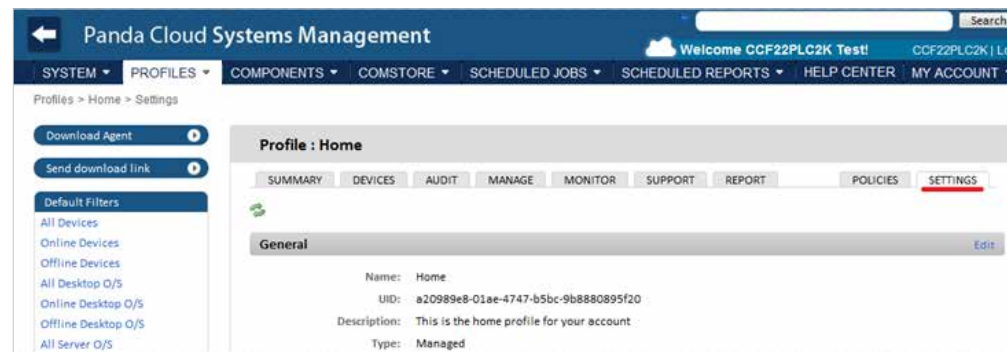
PROFILE LEVEL

What is it?

Profile Level is a grouping entity immediately below System. It is a logical grouping that contains the devices that belong to the same client account or office.

The Profiles list can be accessed from General Menu, Profiles.

Each Profile is associated with a number of configurations accessible from Tab Bar, Settings in the **PCSM Console**, which in turn, are bundled with the **PCSM Agent**.



Configuration options can be divided into several groups.

✓ Profile Identification

Information used to identify a Profile within the rest of the Profiles generated and which can be used in filters or searches. The configurable fields are:

- ✓ **General:** Profile name and description.
- ✓ **Variables:** environment variables that the devices belonging to the profile inherit and which can be invoked later from scripts or components developed by the administrator. Chapter 10 describes how to create and deploy components.
- ✓ **Custom Labels:** five fields with information defined by the administrator.

✓ Contact Information

These are the email accounts used by **Panda Cloud Systems Management** to contact the service administrators. They are generally used to send reports or alerts.

✓ Mail Recipients

✓ Local Cache

This field is used to identify the cache on the client's LAN to speed up software, patch or script downloads, which will then be deployed to neighboring devices. This method reduces bandwidth consumption by preventing devices belonging to the same network from having to access the internet in order to download these individually

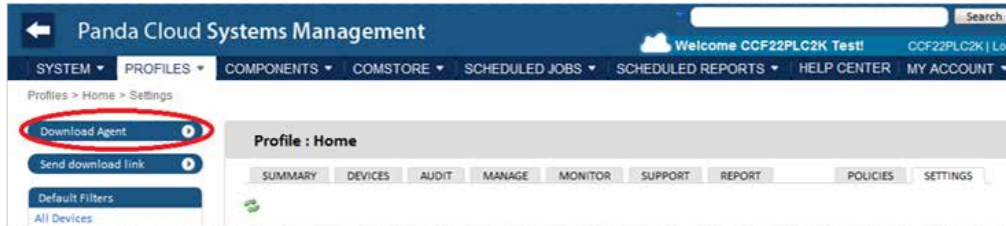
✓ Login Information

Execution of scripts on the user's device inherits the permissions associated to the Localhost account, but if the Profile needs to execute scripts with the Run As command, you can enter the login and password details here.

✔ Consumption Information

Power consumption information can be associated to each device so that the **PCSM Server** can calculate overall consumption and contrast it against variations in the power saving settings, through System Policies or Profile Policies, which are explained later on.

In addition to the information above, the information corresponding to the Profile generated is incrustrated in the **PCSM Agent**, as it is can be directly downloaded from the Profile management screen.



After the **PCSM Agent** has been installed on client devices, they are automatically added to the correct Profile in the **PCSM Console**.

Scope

The procedures triggered at Profile Level can affect all devices belonging to that Profile, while some actions can be restricted to a subset of devices using filters and groups, described in chapter 5.

Unlike System Level, which is unique, the administrator can create as many Profile groups as needed.

Membership

Membership of a given device to a Profile is determined when installing the **PCSM Agent**.



Download the **PCSM Agent** from the chosen Profile page so that when installed on the user's device, it will be automatically added to the Profile in question in the **PCSM Console**.



You can move devices from one Profile to another from the **PCSM Console** after you have installed the **PCSM Agent** on the user's device.



To minimize the tasks in the deployment phase, it is recommendable to create a Profile first and then download the **PCSM Agent** from it, so that the managed devices automatically belong to the Profile created.

Functionality

Profile Level can perform actions on all of the devices it contains. In this way, you can obtain the status of devices, consolidated reports and tasks to perform on all or some of the devices which make up the Profile.

DEVICE LEVEL

What is it?

This represents a single node, end-point, or device with a **PCSM Agent** installed and reporting to the **PCSM Server**. Devices are automatically created in the **PCSM Console**, as they are added as the **Agents** are installed on the client's devices.

Scope

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

Functionality

Device Level can perform actions on a particular device. This allows lists with the most details as possible on the device and reports and actions to be obtained.

04. BASIC COMPONENTS OF THE PCSM CONSOLE

The **PCSM Console** is structured in an intuitive and visual manner, so that most management resources are just a click away, avoiding the clutter of unnecessary checkboxes and settings.

The goal is a **PCSM Console** which is clean, quick and convenient to use, while avoiding, wherever possible, full page reloads and offering a gentle and short learning curve so that the IT department can deliver value to a client from the outset.

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

GENERAL MENU

This menu is accessible from anywhere in the **PCSM Console**. It consists of 6 entries:



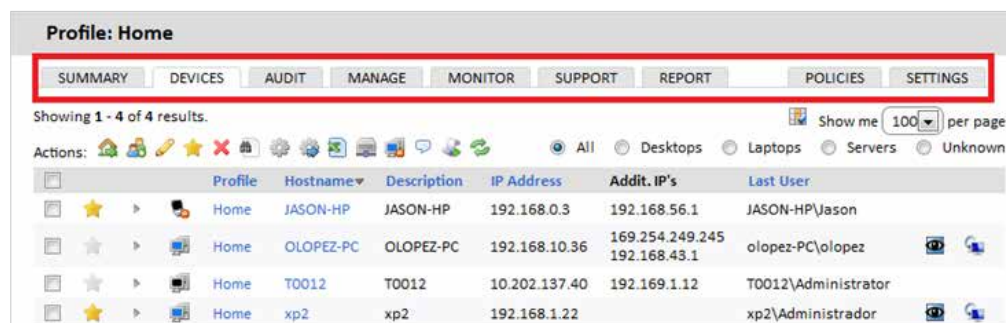
Menu	Description
System	Access to System Level.
Profiles	Access to Profile Level.
Components	Access to components downloaded by and accessible to the administrator.
ComStore	Repository of components created by Panda Security that extend the functionality of PCSM .
Scheduled Jobs	List of active and finished jobs.
Scheduled reports	List of configured and default reports.
Help Center	Help center with links to Panda Security resources.
Account	Access to the details of the principal administration account and to resources for creating new roles and users. For more information, see chapter 14.

Tab	Accessible from	Description
Summary	Profile, Device	Status Information.
Dashboard	System	General control panel.
Devices	Profile	List of devices accessible with associated information.
Audit	System, Profile, Device	Hardware, software and license audit list .
Manage	System, Profile, Device	List of patches pending and applied.
Monitor	System, Profile, Device	List of alerts created by monitors or finished jobs
Support	System, Profile, Device	List of tickets generated.
Report	System, Profile, Device	List and generation of on-demand reports.
Policies	System, Profile, Device	List and generation of policies, described later.
Settings	Profile	Configuration associated to the Profile.
Suspended devices	System	List of uninstalled Devices.

TAB BAR / LIST BAR

The Tab Bar and also the List Bar provides access to the tools available in the **PCSM 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 Profile Level, System Level or Device Level for a specific device, as each management scope is also different.

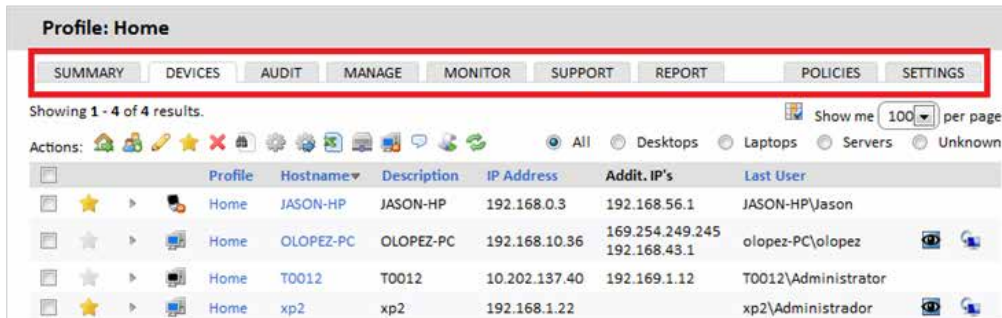


The scope of the Tab Bar refers to the current level. Therefore, if you access the Tab Bar at System Level, it will show information for all devices. If you access at Profile Level, it will show consolidated information on the devices in the Profile. If you access at Device Level, it will only show information for that particular device.

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 General Menu, System and varies slightly if accessed from General Menu, Profile 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 Profile.



Icon	Accessible from	Description
Move Device to	Profile, Device	Move a or the devices selected to another Profile.
Add Device to	Profile, Device	Move a or the devices selected to a group.
Edit	Profile	Add notes and custom fields to the selected devices that can be used by filters.
Toggle	Profile	Mark devices as favorite for quick access from Summary / Dashboard.
Delete	Profile, Device	Delete a Device from a Profile. The device will no longer be managed, the PCSM Agent will be uninstalled and the device will be added to the Suspended Devices Tab under General Menu, System.

Continue 

Icon	Accessible from	Description
Request audit	Profile, Device	Forces an audit to be launched (the audit is an automatic job performed every 24 hours).
Schedule Job	Profile, Device	Create a scheduled job for a later date.
Run Job	Profile, Device	Create and run a job already created.
Download	Profile	Download the list of devices in the Profile.
Add/Remove Cache	Profile, Device	Mark the device as network cache.
Turn Privacy	Profile, Device	Prevent remote access to the devices by the administrator unless approved by the user.
Send a message	Profile, Device	Send a message to the selected devices.
Schedule reports	Profile	Schedule Reports for a later date.
Refresh	Profile, Device	Refresh the data on the screen.
Initiate	Device	Initiate Agent deployment from the selected device to other devices in the same network.
QR Code	Device	QR code associated to the device for paper auditing.

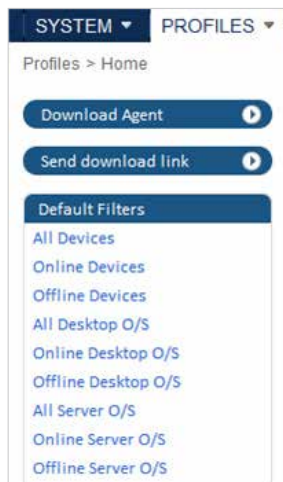


If you want to perform actions at System Level, you will need to create a filter or group, as System Level does not display the Icon Bar by default.

FILTERS AND GROUPS PANEL

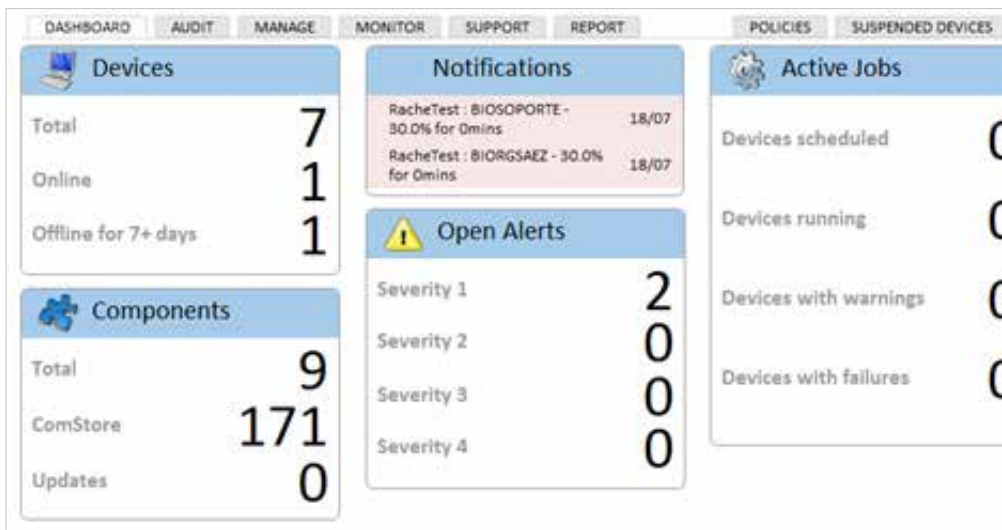
The left of the **PCSM Console** contains three panels with different groups:

- ✔ **Default Filters:** filters automatically generated by the system.
- ✔ **Profile Filters / System Filters:** device filters created by the administrator at Profile Level or System Level, respectively.
- ✔ **Profile Device Groups / System Device Groups:** device groups created by the administrator at Profile Level or System Level, respectively.
- ✔ **System Profile Groups:** only available at System Level, these are groups of various Profiles.



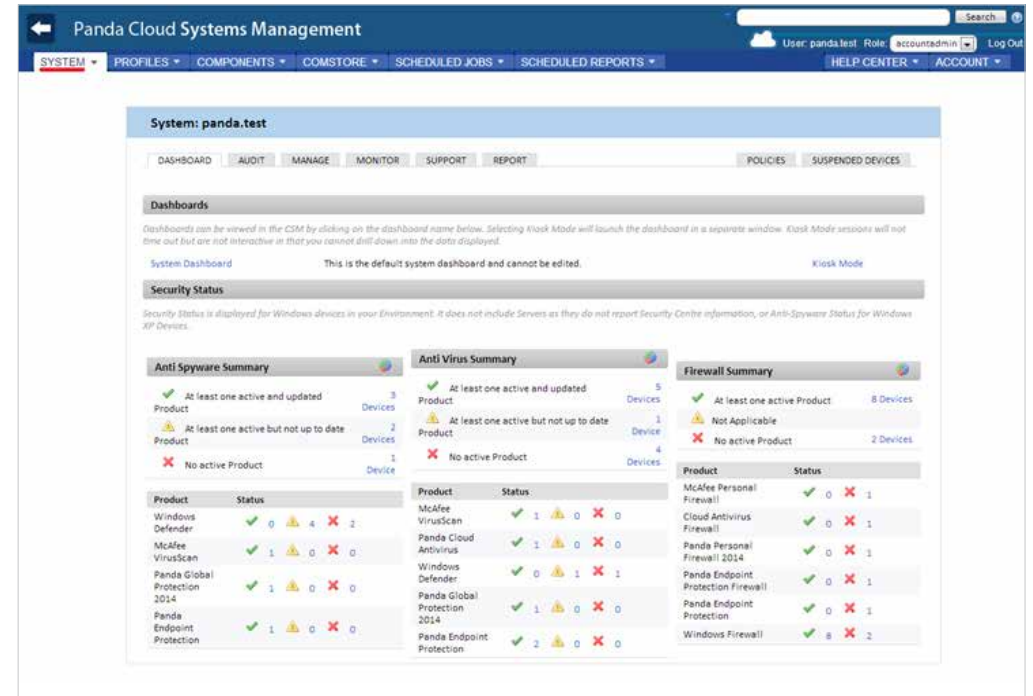
DASHBOARDS

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



Security Status

Accessible from General Menu, System, it reflects the security status of all managed devices.



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

Summary (Profile)

Accessible from General Menu, Profile. It reflects the status of all the devices that belong to the selected Profile. There will be a Summary Dashboard for each Profile created.

Profile: Bilbao Office

SUMMARY DEVICES AUDIT MANAGE MONITOR SUPPORT REPORT POLICIES SETTINGS

Devices

Total: 10
Online: 2
Offline: 8
Offline > 2 days: 7

Security Center

Antivirus: 60%
Firewall: 80%
MS Updates: 100%
Patch Mgt: 247

Energy Usage

Previous Month: 0hr
Previous Cost: £0.00
Current Month: 75hrs
Current Cost: £3.15

Security Status

Security Status is displayed for Windows devices in your Environment. It does not include Servers as they do not report Security Centre information, or Anti-Spyware Status for Windows XP Devices.

Anti Spyware Summary

At least one active and updated Product: 3 Devices
At least one active but not up to date Product: 2 Devices
No active Product: No Devices

Product	Status
Windows Defender	0 4 1
McAfee VirusScan	1 0 0
Panda Global Protection 2014	1 0 0
Panda Endpoint Protection	1 0 0

Anti Virus Summary

At least one active and updated Product: 5 Devices
At least one active but not up to date Product: 1 Device
No active Product: 3 Devices

Product	Status
McAfee VirusScan	1 0 0
Panda Cloud Antivirus	1 0 0
Windows Defender	0 1 0
Panda Global Protection 2014	1 0 0
Panda Endpoint Protection	2 0 0

Firewall Summary

At least one active Product: 7 Devices
Not Applicable: 1 Device
No active Product: 2 Devices

Product	Status
McAfee Personal Firewall	0 1
Cloud Antivirus Firewall	0 1
Panda Personal Firewall 2014	0 1
Panda Endpoint Protection Firewall	0 1
Panda Endpoint Protection	0 1
Windows Firewall	7 2

Summary (Device)

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

Device : xp2

SUMMARY AUDIT MANAGE MONITOR SUPPORT REPORT POLICIES

Description: xp2 [edit](#) Groups: Version: 4.4.1564.1564
Power Rating: 350.0 Watts

Actions:

System

Hostname: xp2
 UID: 08225def-9268-23e7-2251-4194f1c1813b
 Device Type: Unknown [Override](#)
 Domain: INICIOIMS
 Last User: xp2\Administrador
 Status: Online
 Last Seen: 2012-07-20 17:12:31 UTC
 Last Audit Date: 2012-07-20 12:47:04 UTC
 IP Address: 192.168.1.22
 Ext IP Address: 95.16.111.204
 Manufacturer: VMware, Inc.
 Model: VMware Virtual Platform
 Operating System: Microsoft Windows XP Professional 5.1.2600
 Service Pack: 3
 Architecture: 32 Bit
 Serial Number: VMware-56 4d 52 31 c7 7f 5a 3c-3e 2c 8d 9b 33 a5 57 97

Security Center:

Type	Product	Enabled	Updated
Anti Virus	Unknown	<input type="checkbox"/>	
Firewall	Windows Firewall	<input checked="" type="checkbox"/>	
Updates	Windows Updates	<input checked="" type="checkbox"/>	

Device Notes

Name: Log Time

No notes are currently logged for this device. [Click here](#) to add one.

Monitors

There are no graphing monitors currently configured for this device. [Click here](#) if you want to add a monitor to this device.

05. FILTERS AND GROUPS

WHAT ARE GROUPS AND FILTERS?

Groups and filters are resources for generating clusters of devices in a similar way to the Profile but more easily and dynamically. So, while creating a Profile is considered a static aspect of marking devices as belonging to a specific client account, groups and filters are designed to be easily modified in response to temporary characteristics or criteria of the devices.

TYPES OF GROUPS AND FILTERS

There are various types of groups / filters:

- ✓ **Profile Device Groups / Profile Filters:** created within a specific Profile, they can only contain devices that belong to the selected Profile.
- ✓ **System Device Groups / System Filters:** created at System Level, they can contain devices that belong to one, various or all Profiles.
- ✓ **System Profile Groups:** created at System Level, they are groups of Profiles.



Filters and groups can be inter-profile device groups; depending on where they are generated, they can include devices from one or various Profiles.

GROUPS

Groups are groups of static devices. A device is manually assigned to a group by direct allocation.

FILTERS

Filters are dynamic groups of devices. A device is automatically and indirectly assigned to a filter, depending on the conditions for membership settings. There can be one or various conditions of membership to a filter and they are linked by logical operators (AND /OR).

Below are the steps for building a filter.

- ✓ **Name the filter.** It is recommendable that the name be descriptive, indicating the common characteristics of the devices grouped (i.e. “Microsoft Exchange Servers”, “Workstations with little free space”).

- ✓ If there are multiple conditions, specify the **logical operation** to apply:
 - ✓ **Any:** any device that meets at least one condition will be included in the filter.
 - ✓ **All:** only devices that meet all the conditions will be included in the filter.
- ✓ **Criteria:** each condition line consists of several fields that describe it, according to the type:
 - ✓ **Field:** the main field that specifies which feature of the device will be used to include it in the filter. The main Criteria fields are listed and classified below.
 - ✓ **Condition:** sets the Field comparison mode with that set by the administrator.
 - ✓ **Search Term:** describes the content of the Field. Depending on the type of Condition, the Search Term field will reflect changes made to date ranges, sections, etc.

Below are the values available for each Criteria condition line.

Field	Condition	Search Term
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.
Integer	Greater – Greater than or equal to, Less – Less than or equal to, Includes, Excludes	Numeric.
Binary	True / False	
Date	Before – After, Older than 30/60/90 days	Date Interval.

✔ **Add** several Criteria type lines with the “+” and “-” icons on the right

✔ **Select the scope of the filter:**

- ✔ All Devices in all Profiles
- ✔ Only Devices in the selected Profiles

✔ Select the **PCSM Console** users who can access the filter.

The characteristics described in Field can be grouped as follows, according to the device function descriptor:

Device Status	Status – Online/Offline	Device on or off.
	Status suspended	Devices suspended.
	Antivirus On/Off	
	Firewall On/Off	
	Free disk capacity	Detects devices with little free space.
	Windows updates On/OFF	Devices suspended.
Device Role	Distinguishes devices by their main function.	
	Device Type: Server, Workstation, Smartphone, LapTop	
	Operating System	Distinguishes between server or client operating systems.
	Arquitecture	32-bit or 64-bit.

Continue ▶

Software Version		
	Service Pack	Service pack version
	Software Package	Software installed
	Software versión	
Hardware	Information on manufacturer, model, version, etc.	
	CPU	
	BIOS Name/Release/versión	
	Display Adapter	
	Manufacturer	
	Memory	
	Model	
	Monitor	
	Motherboard	
	Network Adapter	
Device ID	Information that identifies and describes the device.	
	Description	Brief description.
	Profile Description	

Continue ▶

Device ID	Información que identifica y describe al dispositivo.	
	Profile name	
	Domain	
	IP Address	
	MAC Address	
	Serial number	The serial number of the device.
	Hostname	Name assigned by the OS.
Other status		
	Favourite	Shortcut from the dashboard.
	Last seend date	
	Last audit	
	Last user	



06. HOW TO ARRANGE MANAGED DEVICES EFFICIENTLY

The distribution in the **PCSM Console** of the managed devices in an MSP with multiple client accounts or in an IT department with various offices, drastically affects efficiency, as many procedures and actions can be configured to run on many devices. This can be alleviated through the right combination of Profiles, groups, and filters.

DIFFERENCES BETWEEN PROFILES, GROUPS AND FILTERS

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

Profiles

✓ Benefits:

- ✓ They associate the same internet connection settings to all devices: avoid having to manually configure 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 Profile conveniently and rapidly.

✔ **Limitations:**

- ✔ A Device can only belong to one Profile.
- ✔ It is not possible to nest a Profile within a Profile.


Filters and Groups

✔ **Benefits:**

- ✔ Groups / filters let you create subsets of devices within one or more Profiles.
- ✔ 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 consolidated lists..
- ✔ Access to reports is limited; the reports generated will only contain information about one device.

 Groups / filters are Profiles within Profiles (as many as you like) but have limited access to consolidated reports and the Tab Bar.

GENERAL APPROACH AND DEVICE MANAGEMENT STRUCTURE

The following general rules are applied:

✔ **Group Devices in Profiles to separate the devices of different client accounts.**

Profiles 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 Profile.

✔ **Create Profile Device Groups to group devices by hardware / software / configuration / use**

For example, configure Profile Device Groups to separate devices by department within a client account with similar features (software used, general requirements, printer access, etc.) or by role (Servers/Workstations).

✔ **Create Profile Filters to find computers with a common status within a Profile.**

Use filters to quickly and automatically search abnormal conditions that do not fall within predetermined thresholds proactively (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 character groups.

✔ **Create System Profile Groups to group Profiles.**

If there are client accounts or offices with very similar characteristics and a variety of devices, you can group them in the same System Profile Group to ease management.

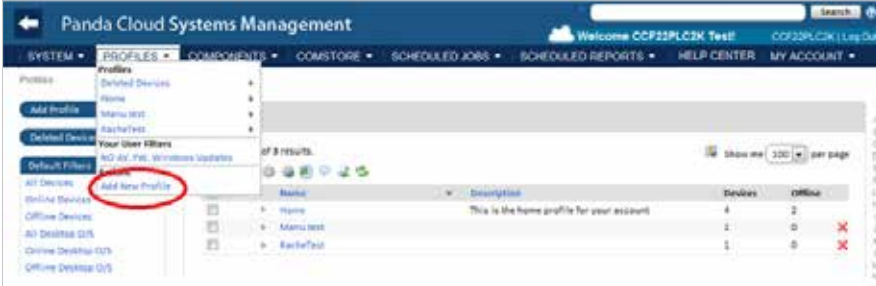
✔ **Associate Account Groups and Filters to technical profiles.**

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. A System group or filter helps locate and group these devices without having to go Profile by Profile to find them. To complete the scenario, it is recommendable to create and configure roles and new user accounts, as described in chapter 14.

07. THE FIRST 8 STEPS TO START USING PCSM

CREATE AND CONFIGURE THE FIRST PROFILE

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



The screenshot shows the Panda Cloud Systems Management (PCSM) web interface. The top navigation bar includes 'SYSTEM', 'PROFILES', 'COMPONENTS', 'COMSTORE', 'SCHEDULED JOBS', 'SCHEDULED REPORTS', 'HELP CENTER', and 'MY ACCOUNT'. The 'PROFILES' menu is open, showing options like 'Deleted Devices', 'Add Profile', 'Default Device', 'Default Filters', and 'Add New Profile' (which is circled in red). Below the menu, there is a table with columns for 'Name', 'Description', 'Devices', and 'Offline'. The table contains one row with the name 'Home' and a description 'This is the home profile for your account'. The 'Devices' column shows '4' and the 'Offline' column shows '2'.

Name	Description	Devices	Offline
Home	This is the home profile for your account	4	2

Fill in the information accordingly and keep in mind that the description field may be used by the filters you add and that refer to the content of this field.

If the device in the Profile requires additional information about the HTTP proxy to access the internet, this information can be provided here or can be added later.



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

DEPLOY THE PCSM AGENT

The PCSM Agent installed on the client's devices will require certain basic information in order to function:

- ✓ The Profile to which it will belong.
- ✓ The minimum information it requires to access the internet and connect to the PCSM Server.

The Profile to which the **PCSM Agent** belongs is automatically defined when you start downloading or sending from the Profile.

The internet connection data was specified in the previous step when creating the Profile or in Tab Bar, Settings, so that the PCSM Agent downloaded will already contain this information.



The PCSM Agent can be downloaded in two ways:

- ✓ Send the downloaded **PCSM Agent** (email, deploy with Active Directory, etc.)
- ✓ Email direct link to the Agent.

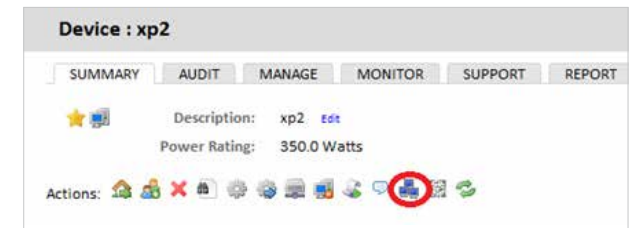
Installing and deploying the **PCSM Agent** across large networks can be long and tedious if you have to send it to each device separately. The simplest way to perform mass deployment is:

- ✓ Send the **PCSM Agent** to the first device on the network.

Normally, to install the **PCSM Agent**, you simply need to double click the downloaded package, and installation is completed "silently" without confirmations. Once installed, the **PCSM Agent** will connect to the **PCSM Server** and appear in the list of managed devices in the selected Profile.

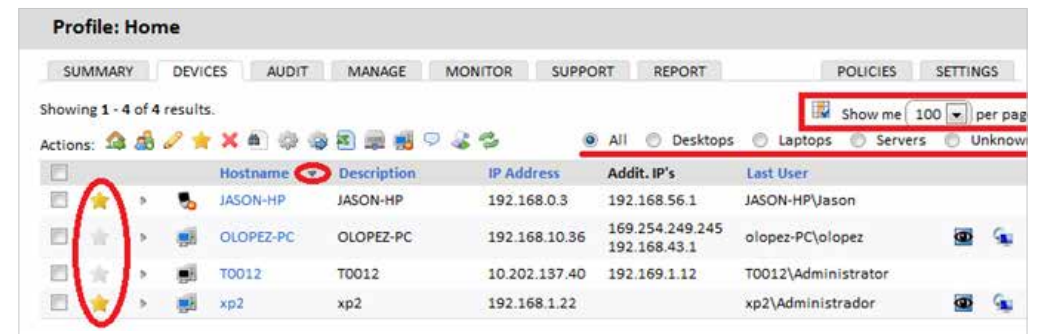
- ✓ Auto Deploy to other network devices.

By selecting the Device with the first PCSM Agent installed, you can start mass deployment to the rest of the network segment.



CHECK THE DEVICE LIST IN THE PROFILE AND BASIC FILTERING

You can favorite the devices to access them more quickly later, 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.



Actions	Hostname	Description	IP Address	Addit. IP's	Last User
[Star]	JASON-HP	JASON-HP	192.168.0.3	192.168.56.1	JASON-HP\Jason
[Star]	OLOPEZ-PC	OLOPEZ-PC	192.168.10.36	169.254.249.245 192.168.43.1	olopez-PC\olopez
[Star]	T0012	T0012	10.202.137.40	192.169.1.12	T0012\Administrador
[Star]	xp2	xp2	192.168.1.22		xp2\Administrador

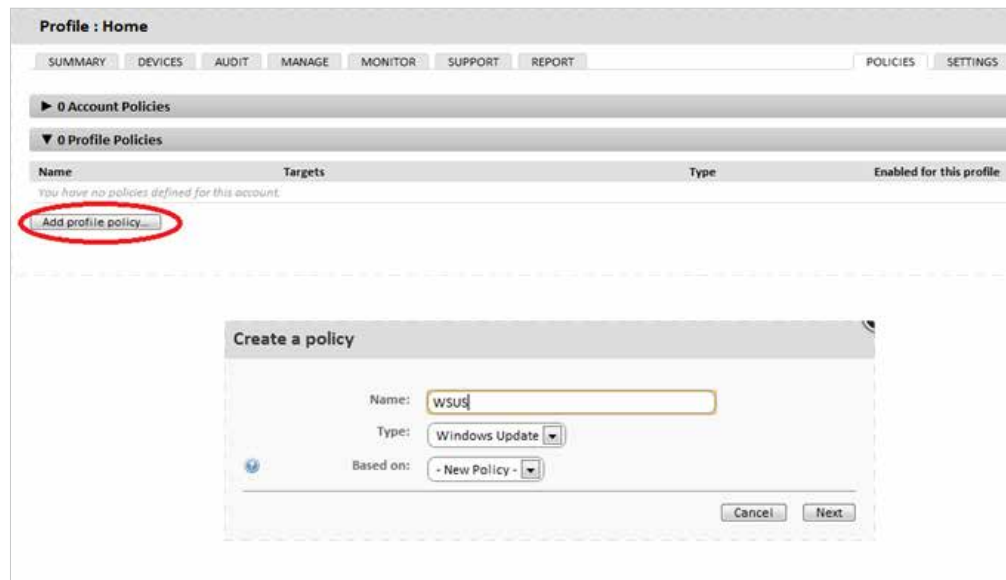
HARDWARE, SOFTWARE AND LICENSE AUDIT

Tab Bar, Audit contains all of the audit details of the devices belonging to the Profile or if accessed at Device Level, it will display detailed information about the device.



PATCH MANAGEMENT

Approve patches that have not been installed on managed devices or rollback those you want to uninstall in Tab Bar, Manage.

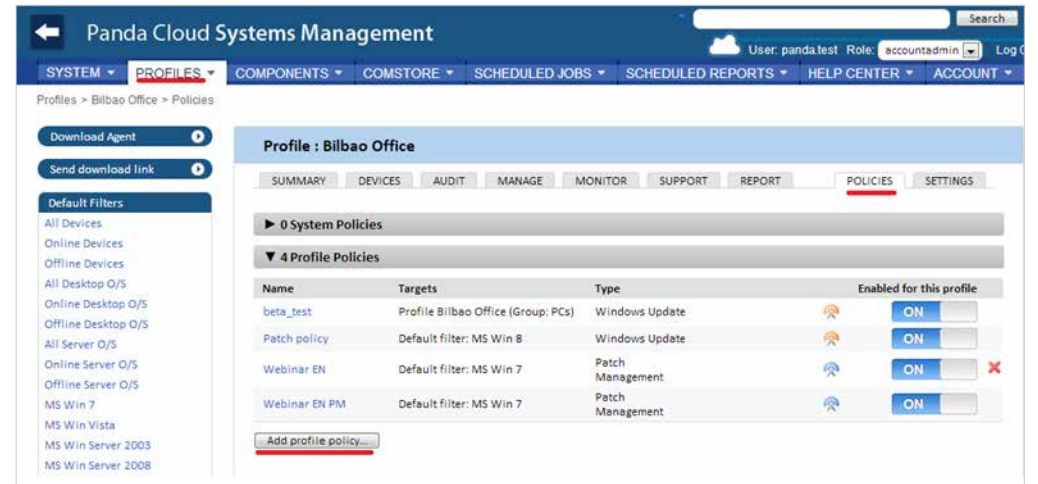


Configure when to apply patches to the device in the Profile, the steps to be taken once applied and other parameters by creating a Windows Update or Patch Management Policy from Tab Bar, Policies in the Profile. For more information about Patch Management, see chapter 13. For more information about creating Policies, see chapter 8.

CREATE MONITORS

Deploy monitoring mechanisms to network devices.

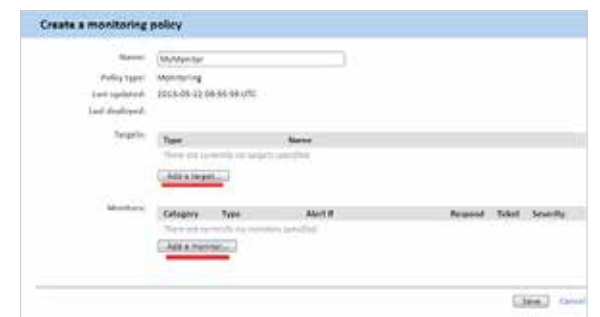
From General Menu, System or from a specific Profile in Tab Bar, Policies, click Add System/Profile Policy.



In type select monitoring.



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.



More information about monitors in chapter 9

COMSTORE

Extend the functionality of PCSM and centrally install third-party software with the components published in the ComStore.



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

“My Components” shows the components already downloaded and available for use.

“ComStore” shows the components available for download from the ComStore.

In order to download a component, select one 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 Profile, select the devices to which to apply the component and choose between Schedule a job and Run a quick Job.

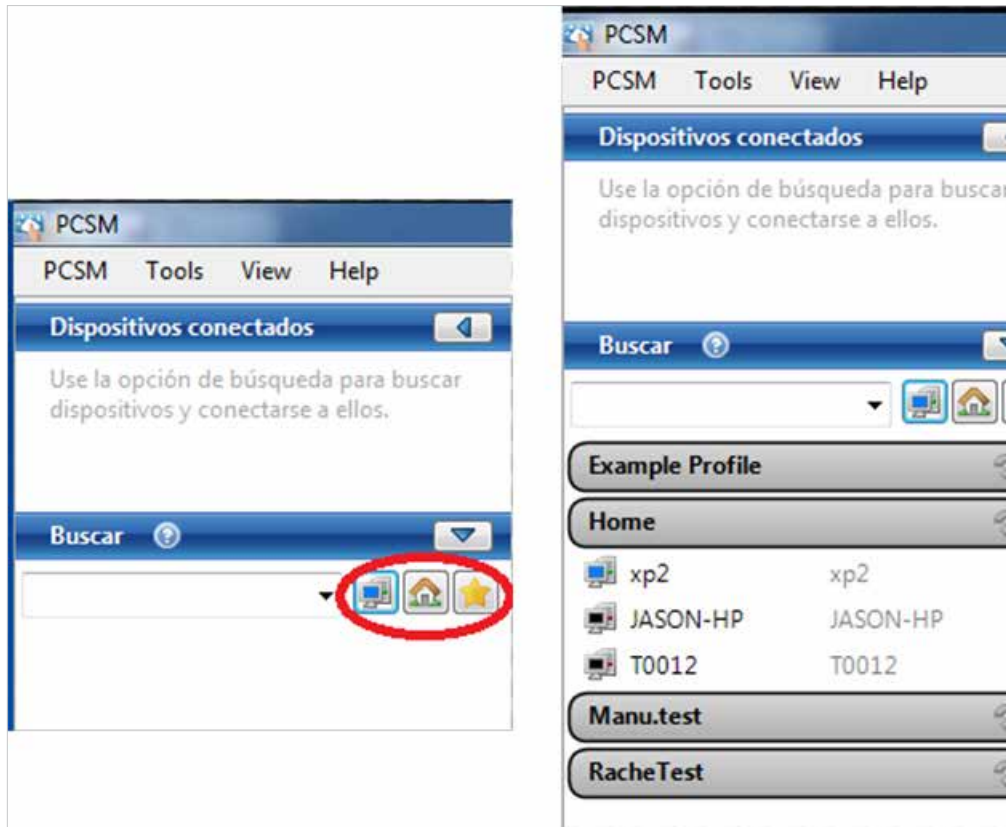


ACCESS REMOTE MANAGED DEVICE RESOURCES

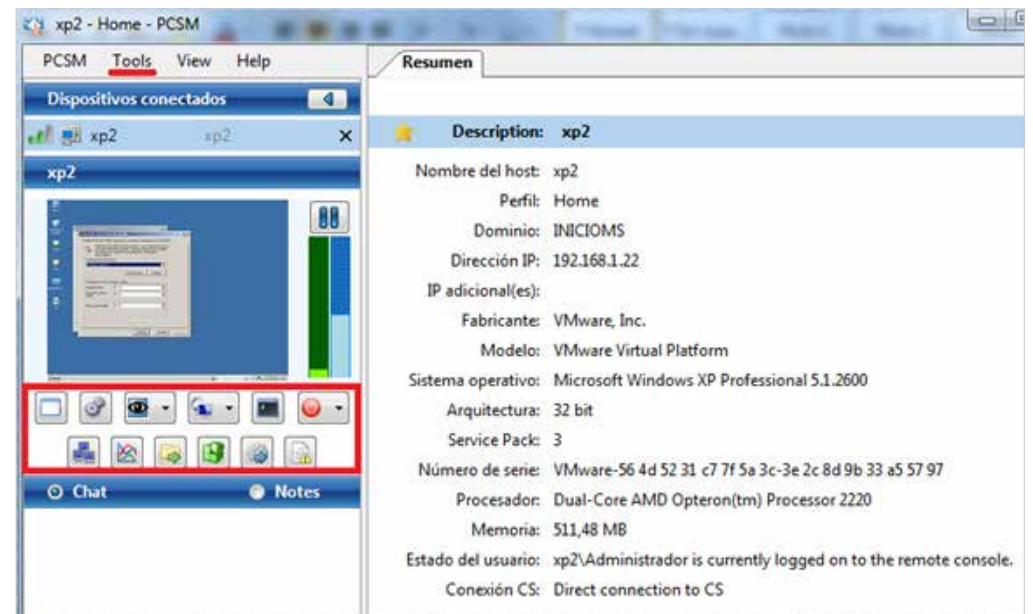
Although many daily operations can be performed directly from the **PCSM Console**, it may be necessary to directly access the device through the **PCSM Agent**. This requires installing the agent on technicians' devices so that they can provide remote support and login with their username and password.



Once logged in, locate the device to manage using its name by expanding the Profiles the technician can access with the credentials supplied or by listing the devices marked as favorites.



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 PCSM Agent across the LAN.
- ✓ **Task manager:** remote access to the task manager without needing to access the remote desktop.
- ✓ **File transfer:** send and receive files.
- ✓ **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 switch 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.
- ✔ **ShutDown / Reboot:** shut down or restart the target device.



08. POLICIES

WHAT ARE POLICIES?

Any specific configuration or action that is repeated at regular intervals over time, on one or various devices managed through **PCSM**. It is applied by pushing out a policy to every **PCSM Agent** installed. Policies are configuration containers made up of:

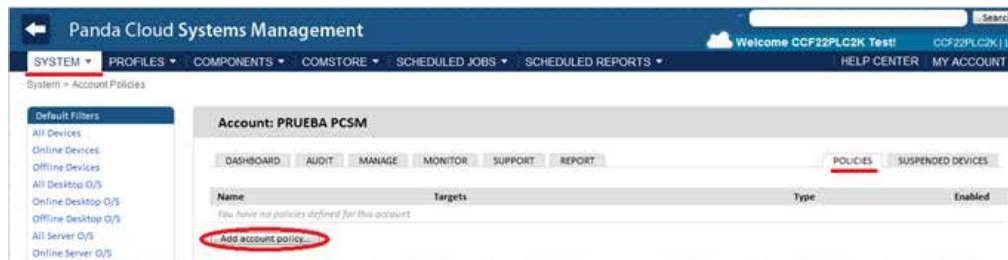
- ✓ Targets: groups of devices to which the policy will be applied.
- ✓ Services: depending on the Policy Type, the **PCSM Agent** will perform a specific series of actions on each device.

Policies can be created at the three levels available, depending on the number of devices and whether they belong to the same client or various:

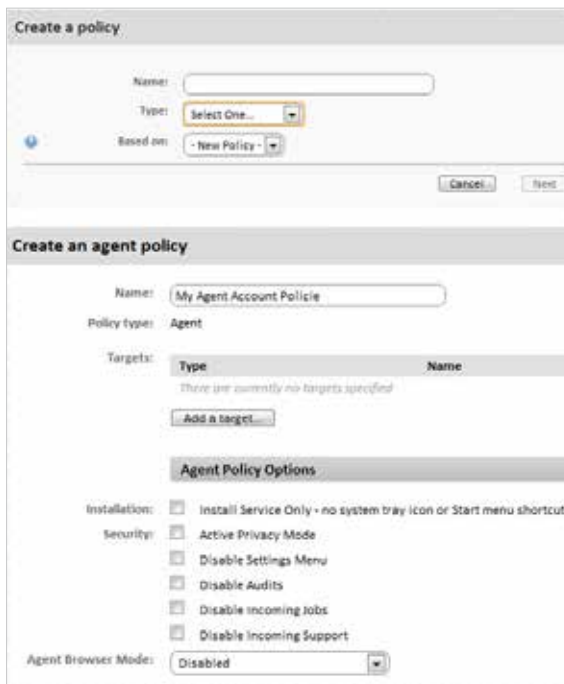
- ✓ System Policy: define an action to apply to System Profile Groups, System Filters or System Device Groups.
- ✓ Profile Policy: define an action to apply to Profile Groups or Profile Filters.
- ✓ Device Policy: define an action to apply to a specific device.

HOW TO DEFINE A SYSTEM POLICY

From General Menu, System by clicking Tab Bar, Policies.



A window appears where you can enter the name of the Policy and if the Type is based on another policy created earlier to ease generation.



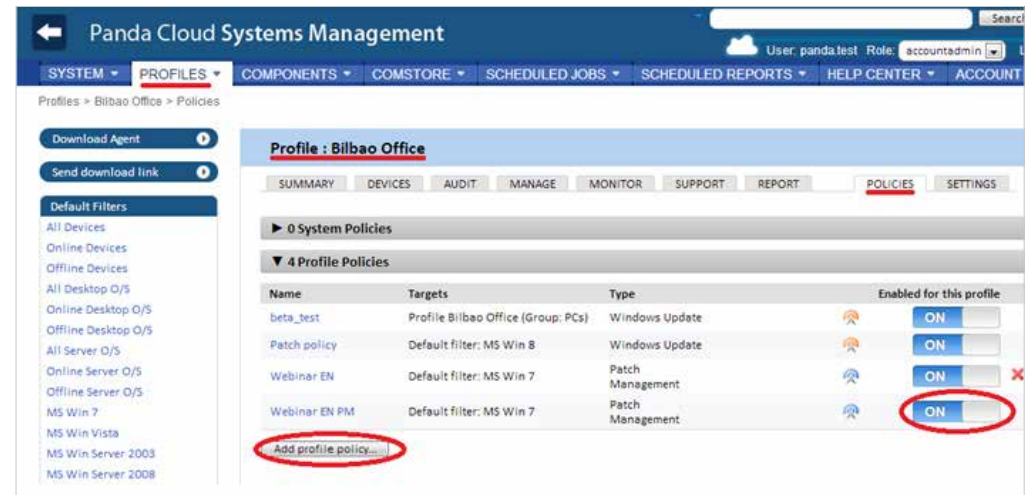
The next window requests the data needed to configure the policy. Depending on the policy type selected in this window, it will request one type of data or other.

In this case, we have created an Agent policy and therefore, the "Agent Policy Options" section will request the configuration details that will affect how the **PCSM Server** and the user will interact with the **PCSM Agent** installed on network devices.

All types of policies will require configuration of the Target, which will be a group or filter already defined. As this is a policy created at System Level, only previously created System Device Groups, System Filters and System Profile Groups will be displayed.

HOW TO DEFINE A PROFILE POLICY

From General Menu, Profiles, select a specific profile then click Tab Bar, Policies.



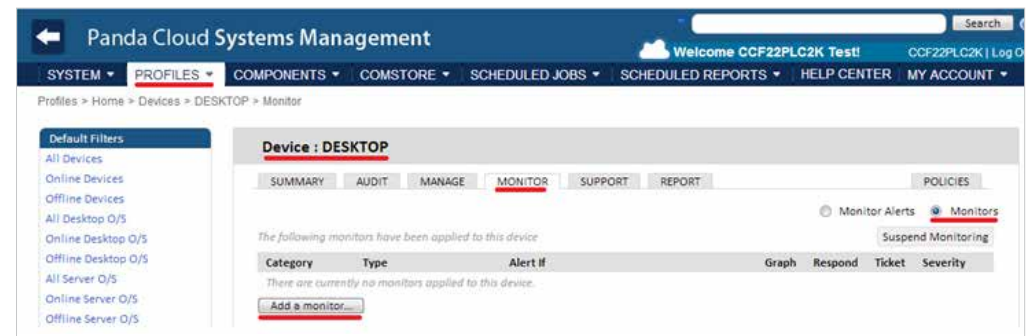
The remaining steps are the same as those for creating a System Policy.

As this is a policy created at Profile Level, only previously created Profile Device Groups and Profile Filters will be displayed.

To disable a Policy in the Profile to which it applies, click On / Off under "Enabled for this profile".

HOW TO DEFINE A DEVICE POLICY


From the Profiles Menu, select a specific Profile and then select a Device, in Tab Bar, Monitor and select Monitors.

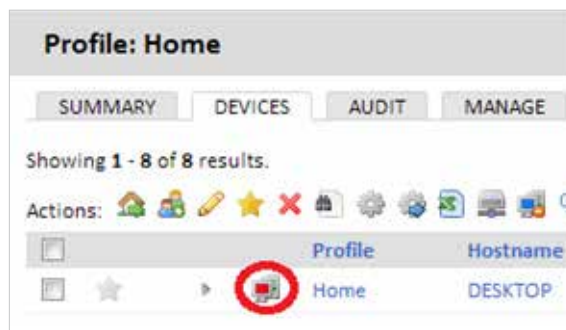


The remaining steps are the same as those for creating a System Policy or Profile Policy.

As it is a Device Policy, the option to choose the Target does not appear: the Policy will only apply to the selected device.

The Suspend Monitoring button disables all active monitors on this device; the device will appear in the **PCSM Console** as Suspended.

 System Policies and Profile Policies are defined in Tab Bar, Policies but Device Policies are defined in Tab Bar, Monitor.



POLICY TYPES

There are 5 types of policy:

- ✓ **Agent**
This policy type specifies the appearance of the **PCSM Agent** and the functionality shown to the user and to the **PCSM Server**.
- ✓ **Install Service Only**: hide the tray icon so that the user cannot access the configuration windows.
- ✓ **Active Privacy Mode**: remote connection to the desktop of the user's device requires explicit acceptance by the user.
- ✓ **Disable Settings**: the user cannot access the **PCSM Agent** context menu.
- ✓ **Disable Audits**: the selected devices will not send hardware/software audit data.
- ✓ **Disable Incoming Jobs**: prevents jobs being sent to the **PCSM Agent**.
- ✓ **Disable Incoming Support**: disables administrator access to the **PCSM Agent**.

✓ **Agent Browser Mode**: allows the **PCSM Agent** execution mode to be defined.

- **Disabled**.
- **User**: the PCSM Agent will not display the Support window and therefore, prevents access in Administrator Mode.
- **Administrator**: complete execution of the **PCSM Agent**.

✓ **Monitoring**

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

✓ **Patch Management**

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

✓ **Power**

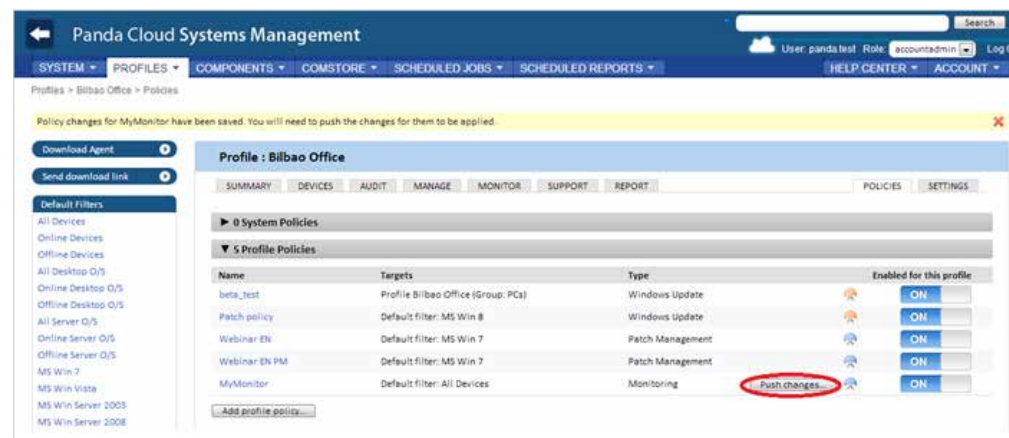
This policy allows configuration of the power saving settings on the devices that support them.

✓ **Windows Update**

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

HOW TO DEPLOY A POLICY

After a policy has been created, a line will be added to the policies screen.



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

09. MONITORING

WHAT IS IT?

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.

COMPOSITION OF A MONITOR

A monitor consists of three configuration groups:

- ✓ **Monitor type:** specifies its function.
- ✓ **Conditions:** monitor parameters that describe the conditions under which a response will be triggered.
- ✓ **Response:** automatic actions that the monitor can trigger. There are three types of response:
 - Execute components
 - Send emails
 - Generate tickets (chapter 12)

CREATE MONITORS

From General Menu, System or from a specific Profile in Tab Bar, Policies, click Add System/Profile Policy.

In type select Monitoring.

Add a target and a monitor.



A policy can have more than one associated monitor.

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

Step 1: 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	Function	Available in
Online Status Monitor	Check whether the device is online.	Windows, Mac
CPU Monitor	Control CPU usage.	Windows, Mac
Memory Monitor	Control memory usage.	Windows, Mac
Component Monitor	Launch a monitor component from the ComStore or designed by the administrator.	Windows, Mac
Process Monitor	Control the status of a specific process.	Windows, Mac

Continue

Monitor	Function	Available in
Service Monitor	Control the status of a specific service.	Windows
Event Log Monitor	Supervise the event viewer.	Windows
Software Monitor	Supervise the software installed on or uninstalled from the device.	Windows
Security Center Monitor	Control the operating system Security Center status.	Windows
Disk Usage Monitor	Control hard disk usage.	Windows
File/Folder Size Monitor	Control the size of files and folders.	Windows

Step 2: Monitor Details

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.

Step 3: Response Details

In this step, you can select the response that will be triggered when the limits defined in step 2 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 Profile to which the monitor created belongs and those defined at global level in General Menu, Account, Settings.

Step 4: Ticket Details

In this step, you can enable automatic generation of tickets as the response generated by the monitor on reaching the limits defined in step 2.

The screenshot shows a web interface for configuring a monitor. The window title is "Add a Monitor" and the monitor type is "CPU Monitor". On the left, there is a sidebar with navigation options: "Monitor Type", "Monitor Details", "Response Details", and "Ticket Details" (which is currently selected). The main content area is titled "Ticket Details" and contains the following configuration options:

- Create Support Ticket:** A checkbox that is checked, with a red circle around it.
- Ticket owner:** A text input field.
- Assignee:** A dropdown menu with "Panda Test" selected. A red horizontal line is drawn underneath this dropdown.
- Ticket Email Notification:** A checkbox that is checked, with a red circle around it.

At the bottom right of the configuration area, there are two buttons: "Back" and "Submit".

- ✓ **Assignee:** assign the tickets generated by the monitor to a technician.
- ✓ **Ticket Email Notification:** send an email with the data generated by the monitor to the technician's address.

10. COMPONENT EXECUTION

WHY DEVELOP COMPONENTS?

Developing components allows the administrator to create new processes to run on users' devices and which add extra functionality to the **PCSM Platform**.

Although **Panda Cloud Systems Management** offers a default component repository (ComStore) which extends its basic function, it might be necessary to develop specific components to perform very specific tasks on users' devices.

Panda Cloud Systems Management is therefore, presented as an expandable remote management and monitoring platform, which very easily adapts to the specific needs of each client.

WHAT ARE THE REQUIREMENTS FOR DEVELOPING COMPONENTS?

Firstly, basic programming knowledge of one of the scripting languages supported:

WHAT ARE THE REQUIREMENTS FOR DEVELOPING COMPONENTS?

Firstly, basic programming knowledge of one of the scripting languages supported:

Language	Included as standard in	Provider
Batch	All versions of Windows.	Microsoft
Visual Basic Script Monitor	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

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 and 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 support directly by the user's device, it is recommendable to run an automatic job to distribute the parser. Software distribution is described in chapter 11.

GENERAL ARCHITECTURE OF PCSM COMPONENTS

The components developed for **Panda Cloud Systems Management** are divided into three types, according to their purpose, behavior and execution method.

✓ Applications:

These components ease software deployment across the client's network. These will be described in chapter 11.

They are script are that are generally run just once and are associated to at least one external file, which will be the software to install.

✓ Monitors:

The Monitor Profile Policies or System Policies are associated to a component that performs the monitoring task. In general, there are three types of monitor:

- ✓ **Internal:** accessible directly from the PCSM Console on creating a policy.
- ✓ **External:** components published by Panda Security in the ComStore.
- ✓ **Custom:** components developed by the IT administrator.

External and Custom components are executed on the device every 60 seconds.



The run interval of an External or Custom component cannot be changed. To lengthen the run time of an External or Custom component, this must be done within the component, for example by storing timestamps with the last run date and checking this value whenever execution of the component is triggered.

✓ Scripts:

These are small programs developed in script language which run on the client's device.

They can be run once through a job or periodically according to the calendar specified in the Scheduler.

In all cases, once the components are loaded on the PCSM Server platform, they will be copied to and run on all devices necessary.

Summary table

Component type	Run from	Run every	Purpose
Applications	Quick Job or Scheduled job.	On demand or when specified in the calendar.	Centralized software deployment and installation. Software deployment is described in chapter 11.
Monitors	Profile Policy or System Policy.	60 seconds (fixed).	Device monitoring.
Scripts	Quick Job or Scheduled Job.	On demand or when specified in the calendar.	Run applications developed by the administrator.



Monitors, Applications and Scripts have almost the same internal structure. The component type only specifies how it connects to the PCSM Console. Therefore, when creating a job, only Script or Application components will be listed and when creating a monitor, only Monitor components created or imported from the ComStore will appear.

CREATE A MONITOR COMPONENT

Component presentation and purpose

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

The purpose of the component is to easily and simply manage the quarantine of the security product **Panda Cloud Office 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 Profile.
Script language	Visual Basic Script.
Frequency of sending information	Every 10 minute notification is sent of whether the number of items in quarantine has increased.
PCSM actions	An email is sent to the administrator with the monitoring results Automatic alert generation.

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

Necessary components

To follow this example, a **Panda Cloud Office Protection** license is required and the **PCSM Agent** must be installed on the device. However, as the items added to quarantine by **Panda Cloud Office Protection** are files in a specific folder on the device, this example can be used with any other folder on the system.

Panda Cloud Office 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.

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.

Communications protocol between the component and the PCSM Server

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

These environment values are automatically created by the **PCSM Agent** when a component is launched. However, it is normal for the script to create environment variables manually to send responses to the **PCSM Server**, which it will gather and add to the **PCSM Console**.

In this case, three environment variables are required.

Variable name	Address	Purpose
PCOP_PATH	Read.	The script recovers the path where Panda Cloud Office Protection stores the quarantine on each user's device from the PCSM Server.
Result	Write.	Send data to the PCSM Server every 10 minutes through the standard output.
Errorlevel	Write.	Script error code. If it is 0, the PCSM Server concludes that monitoring is correct and does not collect the standard output data. If it is 1, the PCSM Server concludes that monitoring is incorrect, collects the standard output data (Result variable) and processes it.

The settings needed to execute the component on the client'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 PCSM console will be used in order to add more flexibility to the component.

The Errorlevel will inform the PCSM 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 PCSM 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->
```

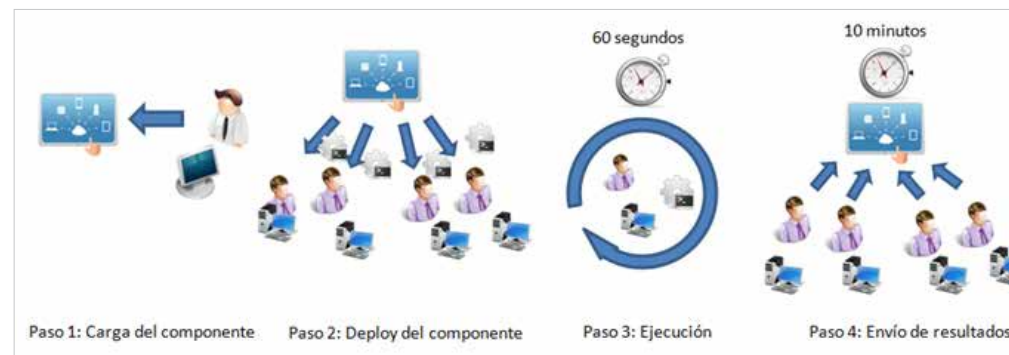


If the script language chosen is Batch, the symbol ^ must be inserted in front of each "<" o ">" character. For example ^<-Start Result-^>

Result will be the variable from which the **PCSM Server** will extract the data to terminate execution of the component. The string on the right of "=" is the content that the **PCSM Server** will store and process.

General functioning schema

- ✔ Step 1: load the monitor component on the **PCSM Platform**.
- ✔ Step 2: deploy the monitor through System Policies or Profile Policies.
- ✔ Step 3: execute the component every 60 seconds.
- ✔ Step 4: send information every 10 minutes and processing in the **PCSM Platform**.

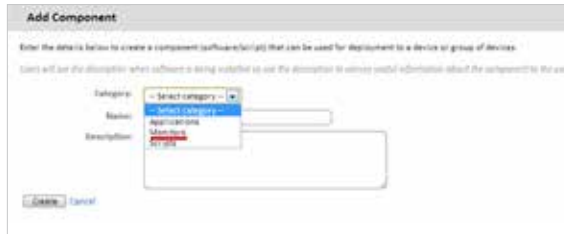


Step 1: load the monitor component on the PCSM Platform

In General Menu, Components, Add Component.



Select the script type Monitors.



Select the scripting language to use, in this example VBScript.

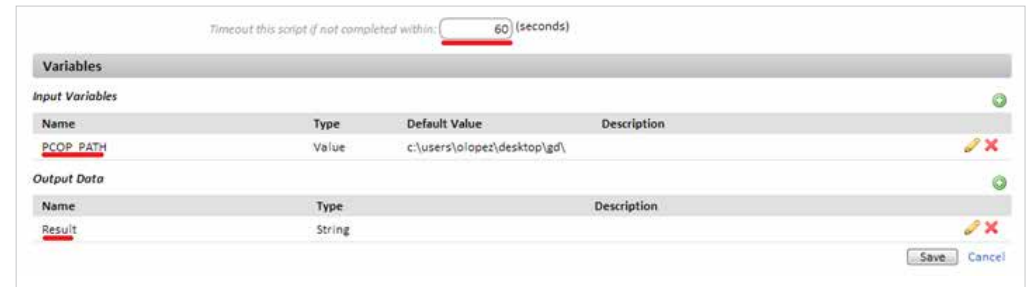


Set the maximum execution time of the component. After this time has elapsed, the **PCSM Agent** will interrupt execution.



It is recommendable 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 Cloud Office Protection** quarantine folder. Result will contain the script output.

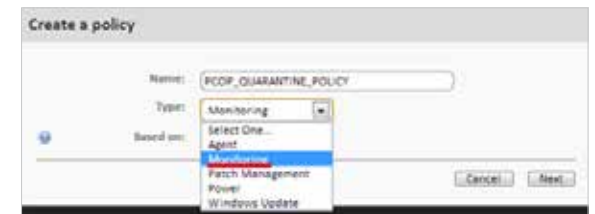


By clicking Save, the component will be added to the account repository.



Step 2: deploy the monitor through System Policies or Profile Policies

If you are developing a monitor, a Monitoring Profile Policy or System Policy must be created.



Add the target Windows 7 and a Component Monitor.

Select the recently created component and save.

You can specify the severity of the alert that **PCSM** 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 **PCSM Server** to generate an email when new items are detected in quarantine, define an email response (Respond) with the recipient's address. The content of the Result response variable will be copied to the email that will be sent to the administrator.

After a monitor has been created, a line will be added to the Policies screen.

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.

Step 3: create environment variables and execute 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 a FileSystemObject type object 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 **PCSM 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 four
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 recommendable 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

```

Step 4: send standard output every 10 minutes and processing in the PCSM platform

If the script ends execution with Errorlevel 0, the response is not considered by the **PCSM Server**. If it ends with Errorlevel 1, the **PCSM Server** will read the standard input 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.

How to use global variables

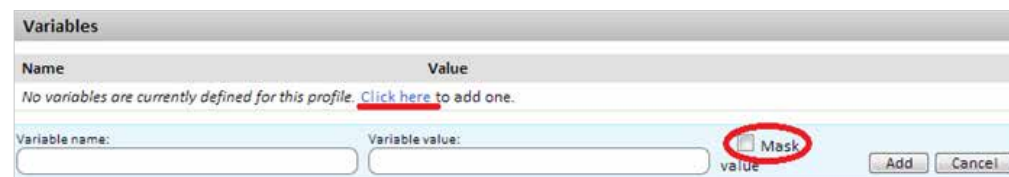
If new scripts are developed frequently, it is highly probably that you will want common data in all of them, such as paths to specific folders on the user's hard disk, the letters of shared drives on servers or even common credentials to execute certain tasks.

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 Profile or System level that can be used directly by the scripts.

In General Menu, System, Settings or Profile Menu, 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 usernames and passwords, you can select the "mask" checkbox to replace the content of the variable with asterisks in the **PCSM Console**.



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

How to display the status of a device in the PCSM Console

Step 2 in the example specified which tasks the **PCSM 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 **PCSM Console** every so often. However, it might be necessary to simply view the status of device without considering the error conditions. To do this, the data of interest must be published in the **PCSM Console**.

For this scenario, the component will use the Custom Fields of the **PCSM Console** that appear in Tab Bar, Summary at Device Level on each device.



The "Custom Field 1" tag and subsequent (up to 5) can be renamed globally for all devices managed by the partner, regardless of the Profile to which they belong or it can be defined at a specific Profile level:

- ✓ In System Level in General Menu, Account, Settings
- ✓ At Profile Level in Tab Bar, Settings.

Custom Field	System Label	Account Override
1	Custom field 1	try
2	Custom field 2	Custom field 2
3	Custom field 3	Custom field 3
4	Custom field 4	Custom field 4
5	Custom field 5	Custom field 5

The content of the Custom Fields take on the branches of the registry of each device, 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

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

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

CREATE A SCRIPT TYPE COMPONENT

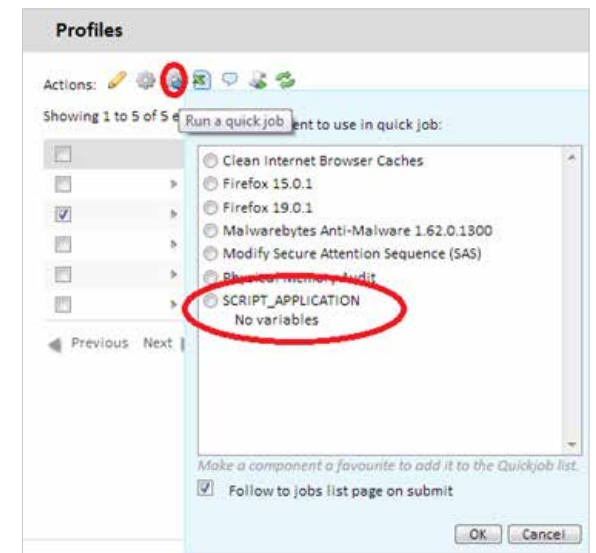
A Script component is created in exactly the same way as a monitor component. First of all, select Scripts on creating the component.

The configuration screen is only different from the one in Monitors as regards the information collection area: you cannot define output variables but instead, you can search for strings in the Standard output (stdout) or Error output (stderr) to enable Warning conditions in the **PCSM Console**.



Con esto aparecerá en los listados de Quick Jobs y jobs.

Haciendo click en Ok el componente se ejecutará de forma inmediata.



11. CENTRALIZED SOFTWARE DEPLOYMENT AND INSTALLATION

OBJECTIVE OF CENTRALIZED SOFTWARE INSTALLATION

The PCSM Server can automatically deploy software files and packages to all the managed devices across the network. This allows the administrator to guarantee that all of the devices managed have the software or documents users need to work without having to go to each device individually or connect via remote access.

Automatic software deployment will help the administrator to keep software vulnerability-free (Java, Adobe, etc.), thereby, significantly reducing the risk of infection and loss of confidential data.

CENTRALIZED SOFTWARE INSTALLATION REQUIREMENTS

Software deployment and installation is a process that is executed through Application components.

Like the Monitor and Script components, described in chapter 10, 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 device.



PACKAGE DEPLOYMENT AND INSTALLATION PROCEDURE

The general procedure consists of 4 steps:

1. Identify the devices on which to install the software.

The procedure for finding the devices that do not have the files or programs installed will vary depending on whether the **PCSM 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 **PCSM** software audits and 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 **PCSM Server** cannot filter 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 10 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 **PCSM 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 **PCSM Console**.
- ✔ 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 **PCSM Console**.

DEPLOYMENT EXAMPLES

To illustrate software distribution, below are four examples:

1. Deploy documents through script language
2. Deploy documents without script language
3. Deploy self-install software
4. Deploy software without an installer



The procedures described here and the third-party tools and script languages used are examples and could vary. **Panda Cloud Systems Management** is designed to be flexible and adapt to the tools with which the administrator feels most comfortable.

Deploy documents through 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 **PCSM 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 Profile 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
```

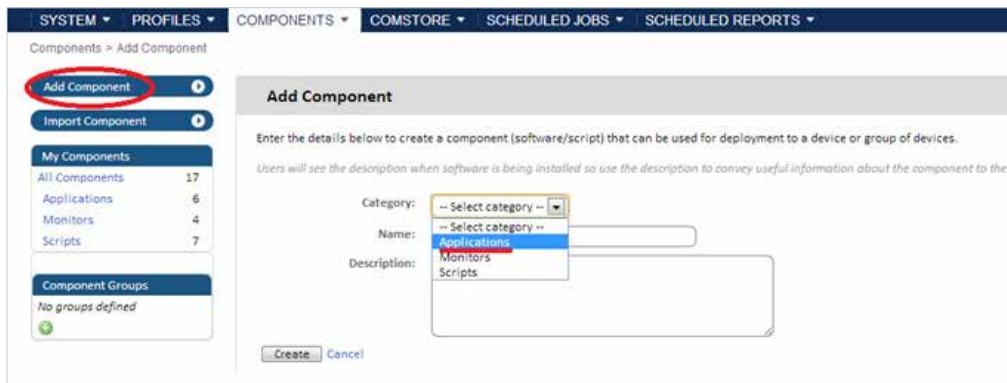
If the folder does not exist, it is created (line 28), the documents are moved to it (lines 30-32) and a message is sent through the Standard Output (line 37).

```

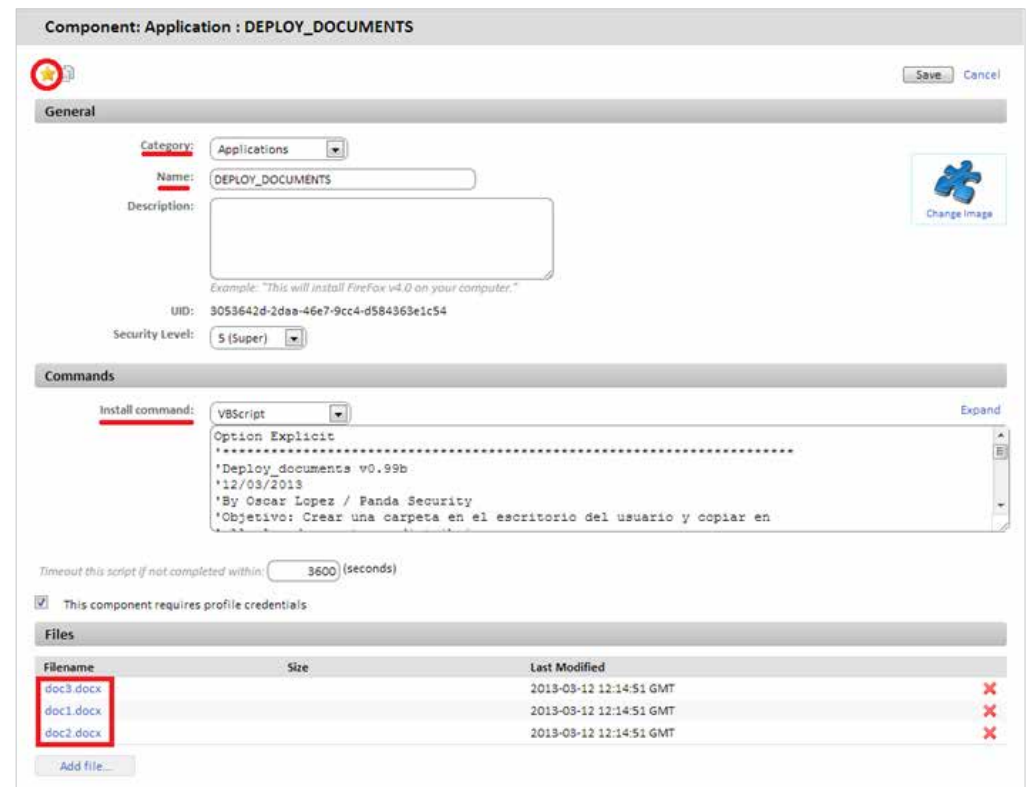
28 Set objFolder = objFSO.CreateFolder(CONST_PATH)
29 'the documents will be moved to the folder
30 objFSO.MoveFile "doc1.docx", objFolder.Path & "\doc1.docx"
31 objFSO.MoveFile "doc2.docx", objFolder.Path & "\doc2.docx"
32 objFSO.MoveFile "doc3.docx", objFolder.Path & "\doc3.docx"
33 If Err.Number<>0 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 PCSCM Console will interpret as Warnings.

Post-Conditions		
Warning Text	Qualifier	Resource
Deploy unsuccessful	is found in	stdout
Add		

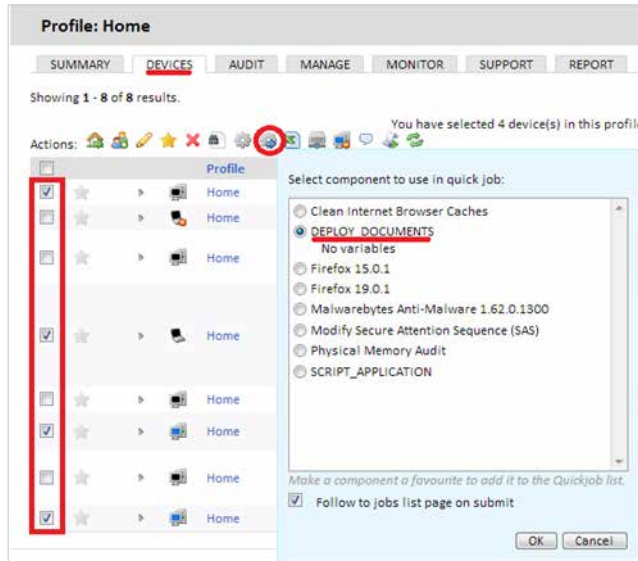
The example specifies that if the Standard Output (Resource:stdout) contains (Qualifier:is found in) the string "Deploy unsuccessful", the result of executing the script will be considered Warning.

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

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



At System Level, you can select complete Profiles to which to apply software deployment.



4. Collect the deployment result in order to identify possible errors.

The output conditions defined in the script in example 3 are:

- ✓ 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 **PCSM Server** will interpret as Warning, as configured in the Post-Conditions area 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 were Successful.



The Stdout and Stderr icons show a copy of the Standard Output and Standard Error generated by the script.

Furthermore, 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.

Deploy documents without 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 **PCSM 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:

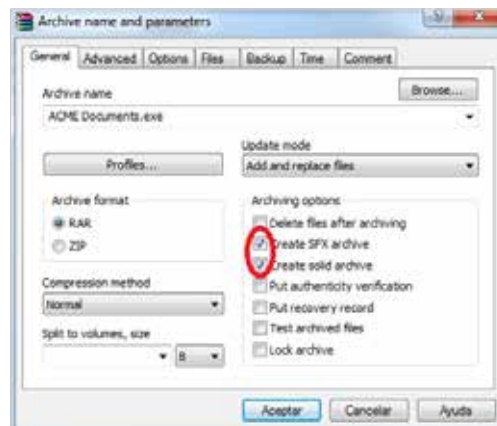
- ✓ Functioning in Silent mode.
- ✓ The folder with the content will be automatically created in C:\.
- ✓ If the folder already exists, its content will be over overwritten without warning.



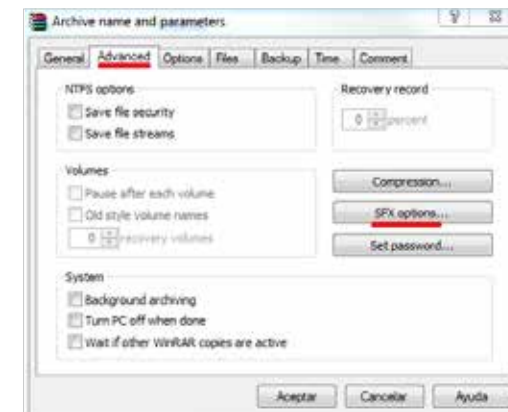
It is essential to generate a self-extracting file that functions in Silent mode, i.e., it does not display dialog boxes or windows and does not require user intervention.

Steps for generating a silent self-extracting installation file:

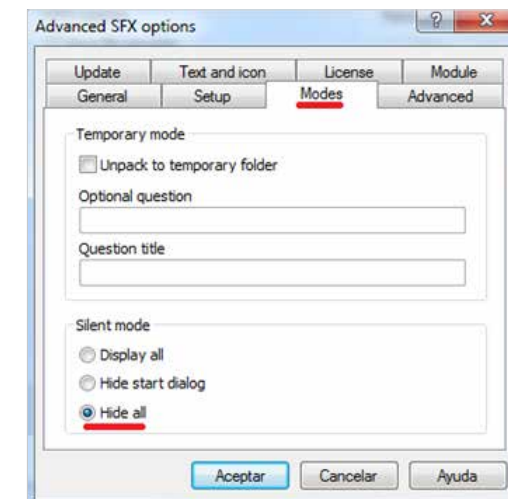
- ✓ **Step 1:** prepare the folder with the documents to deploy. Create the root folder “ACME Documents” in the example and place all of the files, folders and sub-folder to be deployed inside.
- ✓ **Step 2:** generate the executable file. With the WinRAR program open, drag the recently created folder “ACME Documents” and select the option “Create SFX archive” and “Create solid archive”.



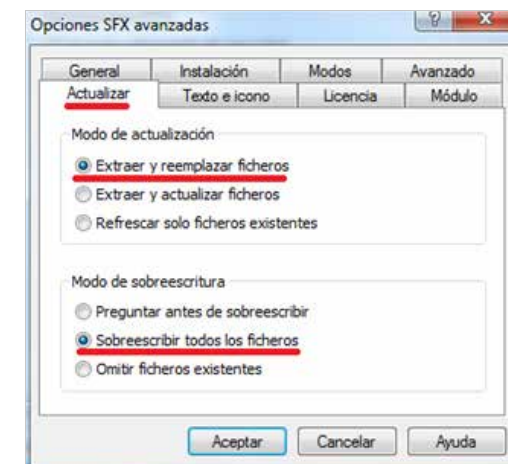
- ✓ **Step 3:** configure the executable file as “Silent”. To do this, enable Hide All in Advanced -> SFX Options -> Modes -> Silent Mode.



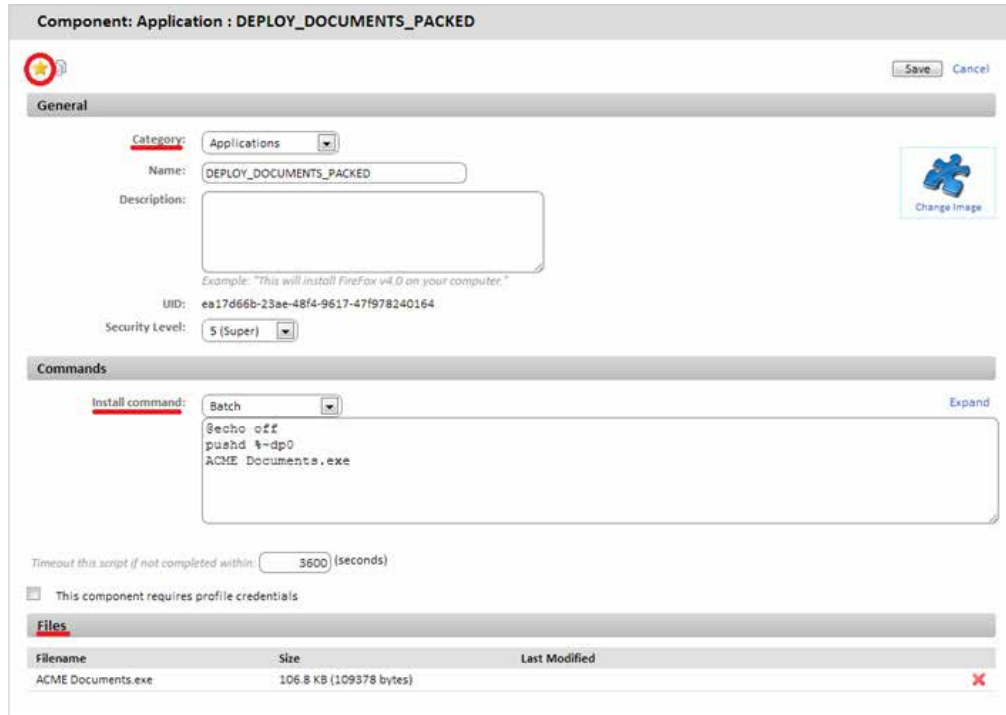
- ✓ **Step 4:** in the General tab, specify the path to extract, where the folder will be created.



- ✓ **Step 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”.

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.

Self-install software deployment

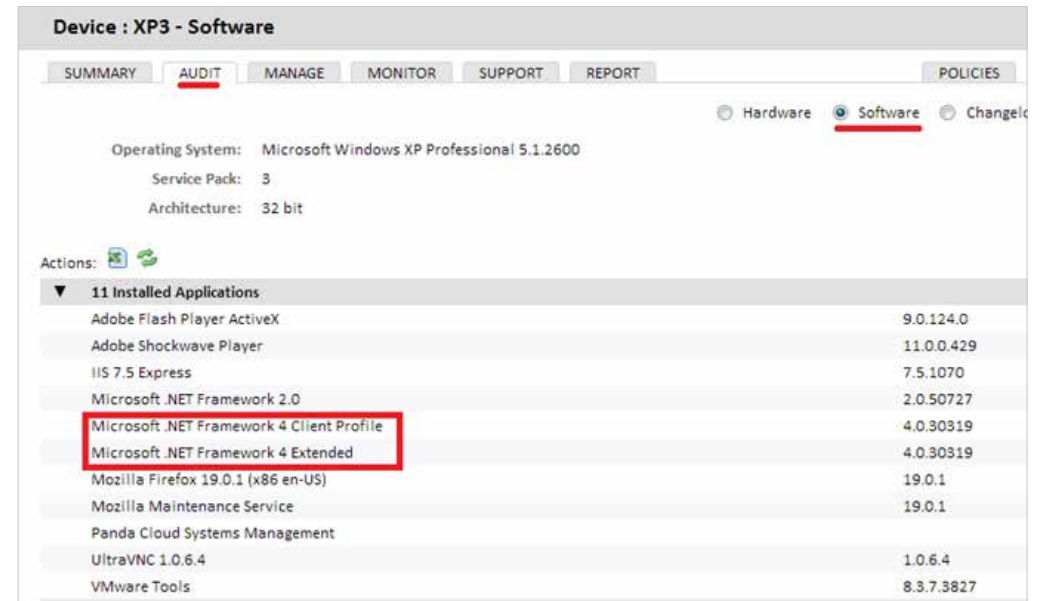
In this example, the Microsoft Framework .NET 4.0 dotNetFx40_Full_x86_x64.exe package will be deployed to the devices on which it is not already installed.

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.

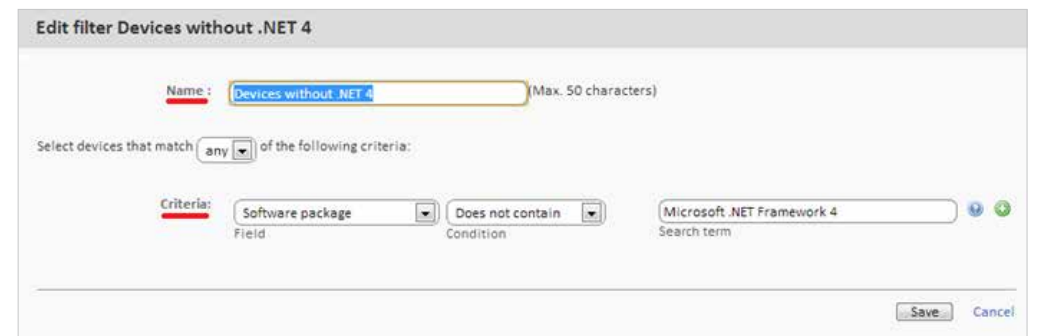
The installation package is a self-extracting .EXE that admits the parameters /q /norestart to execute in silent mode and prevent the device from restarting, so no additional special preparation is required.

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 Profile Filter or a System 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.

2. Generate a software installation component.

It is extremely easy to create an installation component.

Component: Application : DEPLOY .NET

General

Category: Applications

Name: DEPLOY .NET

Description:

UID: 65617c46-5b0f-4e62-bdb0-ffc90164688d

Security Level: 5 (Super)

Commands

Install command: Batch

```
@echo off
pushd %~dp0

dotNetFx40_Full_x86_x64.exe / q /norestart
```

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

This component requires profile credentials

Files

Filename	Size	Last Modified
dotNetFx40_Full_x86_x64.exe	48.1 MB (50449456 bytes)	

Add file...

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 "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 **PCSM Server** by the **PCSM 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.

Deploy 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 **PCSM Server** from generating a reliable audit of 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.



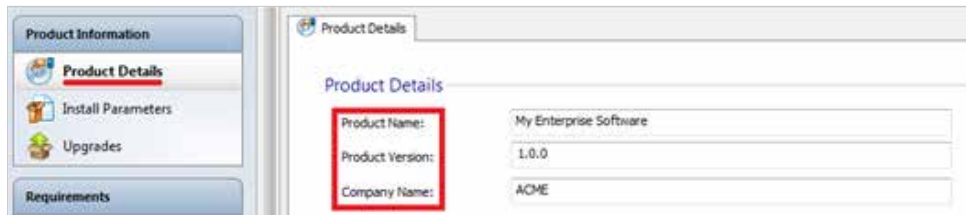
To download the free version of Advanced Installer, go to <http://www.advancedinstaller.com/download.html>

Follow these steps to generate the installer:

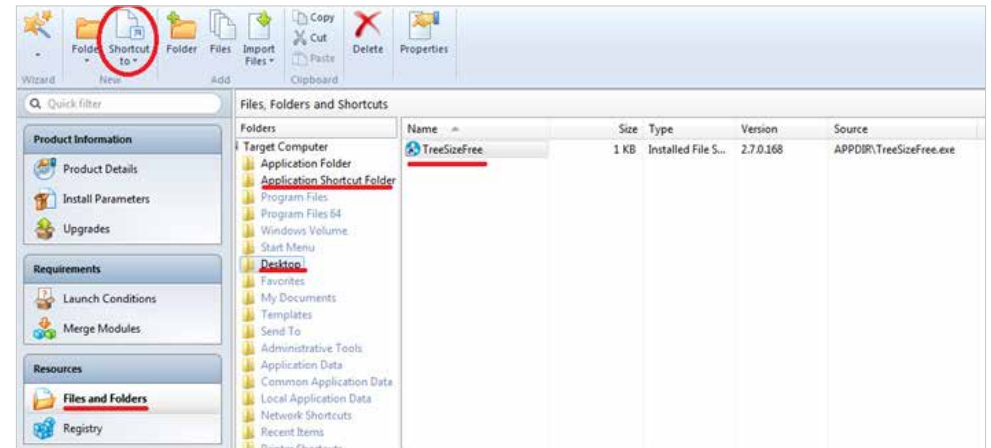
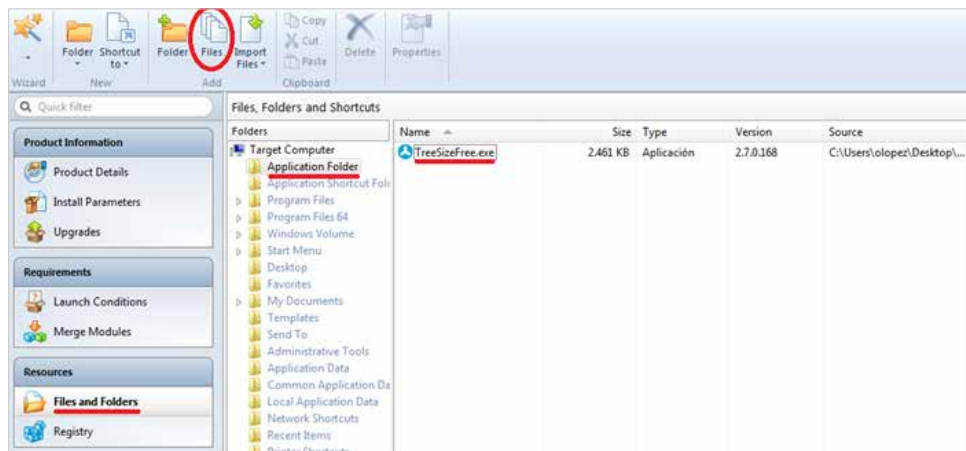
- ✔ Select the Simple template (free).



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

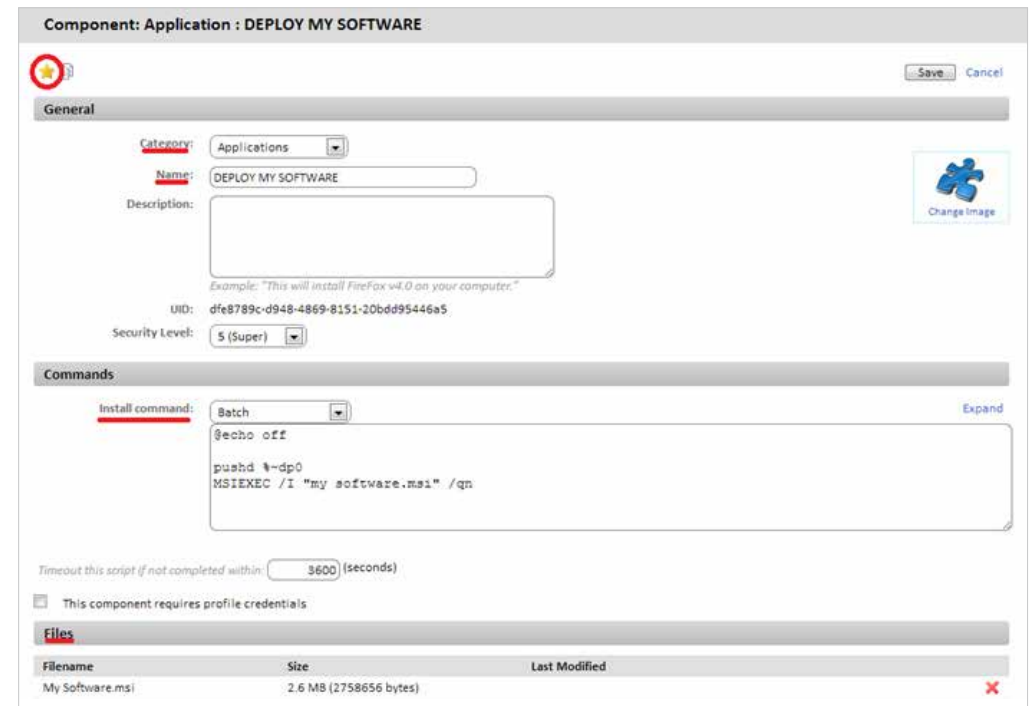


- ✔ Add the files and programs to install and the shortcuts to create. This is done in the Files and Folders tab.



- ✔ 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 script in Batch, whose installation command will vary slightly.



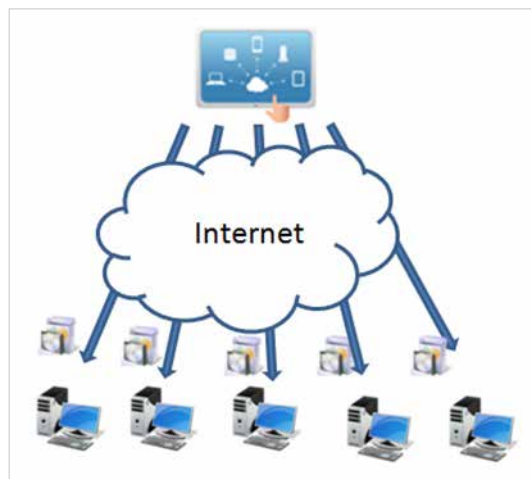
The MSIEXEC utility is invoked using the /qn parameter to launch a silent installation.

- ✔ 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".

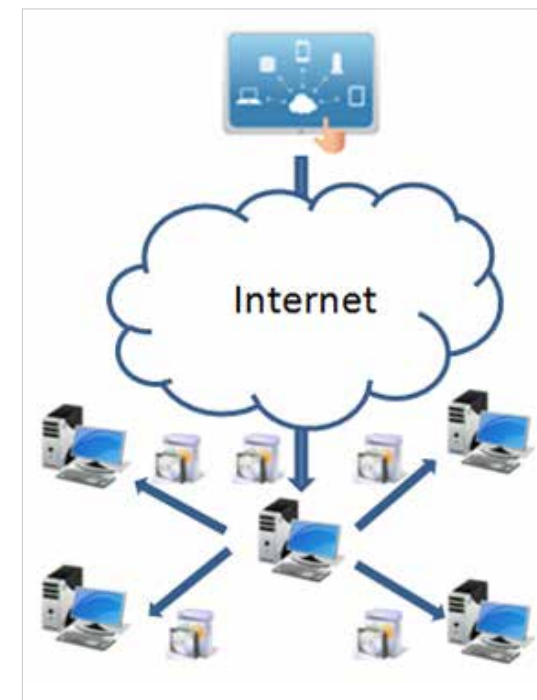
Save bandwidth in software deployment

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

To 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 from the **PCSM Server** and then deploy the package to all of the affected network devices.



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



Device : XP3

SUMMARY AUDIT MANAGE MONITOR SUPPORT REPORT

★ Description: XP3 [Edit](#)

Power Rating: 350.0 Watts

Actions:

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.

A photograph of two IT support staff members, a man and a woman, wearing headsets and working at a computer. The man is on the left, wearing a light blue shirt and tie, smiling. The woman is on the right, wearing a light blue patterned shirt, also smiling. They are in a bright, modern office environment. A large blue graphic overlay is on the right side of the image, containing the section title.

12. TICKETING

WHAT IS THE TICKETING SYSTEM?

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 intermediate 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.

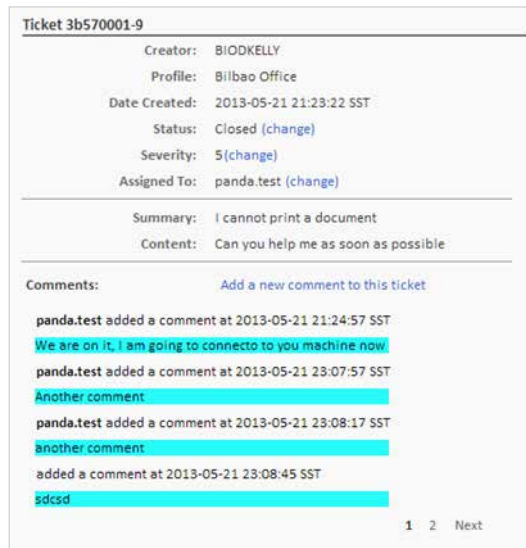
Secondly, forcing documentation of incidents allows the procedure to be reused in the future and fine-tuned, minimizing the response time for open cases.

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.

DESCRIPTION OF A TICKET

Each ticket contains a series of fields that describe it:

- ✔ **Creator:** ticket creator. It can be a device, if the ticket were created from the **PCSM Agent** by a user or system account, if it were created by a monitor and assigned to a technician.
- ✔ **Profile:** 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 job has been done yet.
 - ✔ **In progress:** the technician assigned from the IT department is managing the incident.
 - ✔ **Waiting:** resolution of the incident has been identified by external causes (lack of information, confirm changes by the users or others)
 - ✔ **Closed:** the incident has been resolved and closed.
- ✔ **Severity:** severity of the ticket. If it were 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.



Ticket 3b570001-9

Creator: BIODKELLY
Profile: Bilbao Office
Date Created: 2013-05-21 21:23:22 SST
Status: Closed (change)
Severity: 5(change)
Assigned To: panda.test (change)

Summary: I cannot print a document
Content: Can you help me as soon as possible

Comments: Add a new comment to this ticket

panda.test added a comment at 2013-05-21 21:24:57 SST
We are on it. I am going to connect to your machine now

panda.test added a comment at 2013-05-21 23:07:57 SST
Another comment

panda.test added a comment at 2013-05-21 23:08:17 SST
another comment

added a comment at 2013-05-21 23:08:45 SST
sdcsd

1 2 Next



It is recommendable 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 simplify similar incidents in the future.

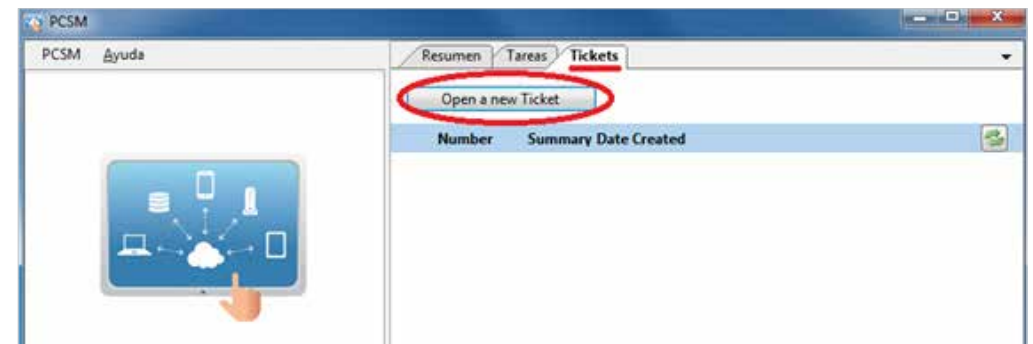
CREATE A TICKET

Tickets are created in three ways:

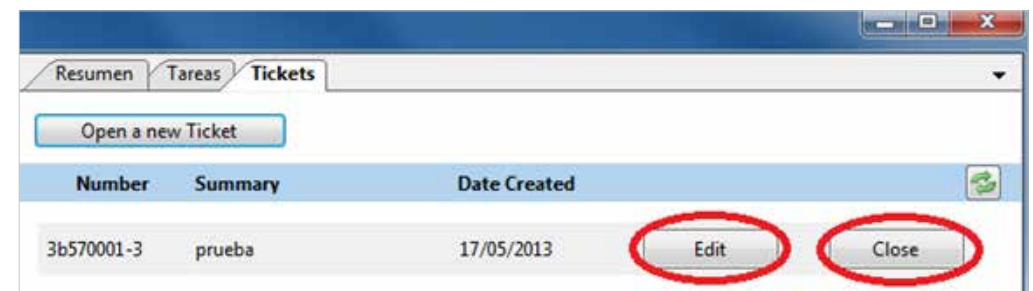
Manually by the user from the PCSM Agent

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 **PCSM Agent** by right-clicking its icon, select Open and click Tickets, Open a New Ticket tab.



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



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

When defining a Monitor policy, in the Ticket Details tab.



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

Manually by the IT department from the PCSM console: these are usually reminders or task that officially join the department's queue.

From Profile Level or System Level in Tab Bar, Support, by clicking Create Support Ticket.

! Tickets created at System Level do not have a Profile assigned and are not displayed in any Profile created in the **PCSM** account.



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.

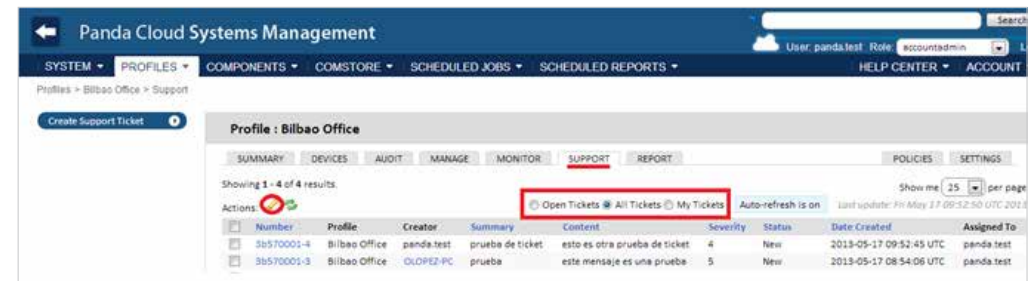


TICKET MANAGEMENT

Tickets that have already been created are managed from Tab Bar, Support at Profile, System 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 Profile Level to which this device belongs.

With the icons in the Action Bar, you can 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.



13. PATCH MANAGEMENT

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, guaranteeing that all devices are updated with the latest patches published.



Patch Management uses the Windows Update API on all Microsoft Windows devices supported by **Panda Cloud Systems Management**.



Patch Management supports Microsoft Windows systems.

WHAT PATCHES CAN I DEPLOY / APPLY?

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

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

Microsoft Office	Visual Studio	Microsoft Lync
Exchange 2003	Zune Software	Silverlight
SQL Server	Virtual PC	Windows Media Player
Windows Live	Virtual Server	Otros...
Windows Defender	CAPICOM	

PATCH DEPLOYMENT AND INSTALLATION

Panda Cloud Systems Management includes three complementary patch management methods. Each of them has different functions to adapt to all possible needs and/or scenarios.



Although three methods are complementary, some of the functions are shared by all of them. If you are going to use various patch management methods at the same time, be particularly careful not to define processes that overlap, as the end result could vary depending on the order defined, thereby achieving unpredictable results.



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 recommendable to disable the policies of third-party manufacturers that interfere with those defined in **Panda Cloud Systems Management**.

Method 1: Manual patch management

General description

Manual patch publication allows you to select the patches to install one by one, according to the criteria applied by the administrator.

This method allows maximum granularity, as all of the patches installed on each device and the patches pending installation are displayed at all times.

The grouping levels supported by this method are the three existing levels: System Level, Profile Level and Device Level. Therefore, you can select patches for a specific device (Device Level), for a specific group (Profile Level) or for all devices registered on **PCSM** (System Level).

Access the manual patch management method.

It is accessed through Tab Bar, Manage in the three levels available.

The actions available are:

Approve patch: by selecting the patches and clicking the green circle icon.

After approving a series of patches they will be pending installation. Approved patches are installed manually at the time specified in Tab Bar, Manage at System Level.



Only the time that approved patches will be manually installed can be defined at System Level. All of the devices managed through **PCSM** will update the approved patches pending at the configured time.

- ✔ **Hide patch:** by selecting the patches and clicking the blue circle icon to hide the patches available lists.
- ✔ **Quick patch:** by selecting the patches and clicking the green circle icon with an arrow, the patches will be installed immediately, without waiting for the time defined in the Manage (System Level) settings.
- ✔ **Reset patch:** by clicking the white circle icon, the patches selected will be cleared.

View patches

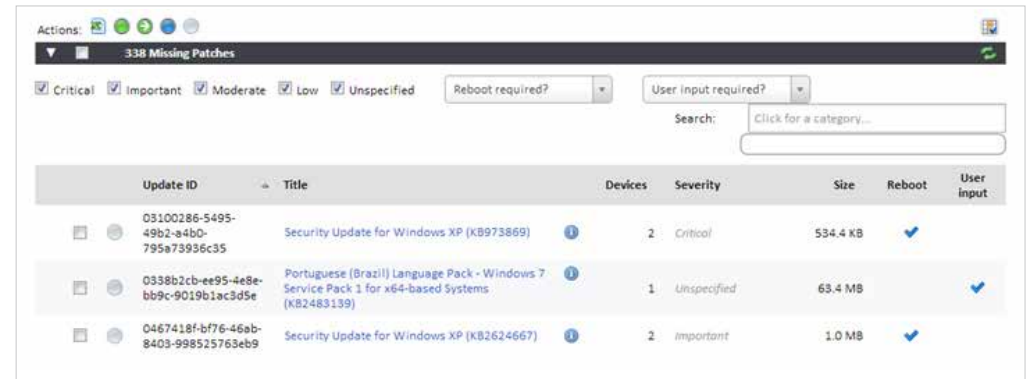
All of the patches published by Microsoft over time are grouped in three drop-down lists, depending on their status with respect to the managed device.



The three statuses are:

- ✔ **Missing patches:** patches that have not yet been installed on the devices belonging to the selected level. At levels above Device, the number of devices on which each specific patch is not installed is also shown.
- ✔ **Installed Patches:** patches that have already been installed at the selected level. At levels above Device, the number of devices on which each specific patch is installed is also shown.
- ✔ **Hidden Patches:** patches that the administrator has decided to hide because they do not need to be applied and a reminder is not needed.

In order to simplify searches, detailed information is available on expanding each category and an Icon Bar is available to filter the patch lists.



The Search Bar allows you to choose the patches displayed according to the following criteria:

- ✔ **Severity:** the severity defined by Microsoft: Critical, Important, Moderate, Low, Unspecified.



Microsoft only specifies the severity of security patches (Security Updates). The rest of the patches generally have Unspecified severity.

- ✔ **Reboot required?** If the device must be rebooted after applying the patch.
- ✔ **User input required?** If user input is required to apply the patch.
- ✔ **Category:** allows you to search for the patches that apply to a specific software program.

PCSM provides the following information for each entry:

Title	Severity	Size	Reboot	User Input
Cumulative Security Update for ActiveX Killbits for Windows XP (KB2618451)	Critical	489.4 KB	✔	

- ✔ **Check:** to select the patch.
- ✔ **Action icon:** patches with actions pending will appear with the circle icon in green.
- ✔ **Title:** full name of the patch provided by Windows Update.
- ✔ **Severity:** importance of the patch provided by Windows Update (only for Security Updates).

- ✔ **Size:** size of the patch to download, provided by Windows Update.
- ✔ **Reboot:** if rebooting is required after installing the patch.
- ✔ **User input:** if user input is required to install the patch or not (dialog boxes to accept EULAs and others).

Manual patch management method usage scenarios.

When the administrator requires very accurate supervision of the patches applied on the devices managed.

Method 2: Windows Update Policy

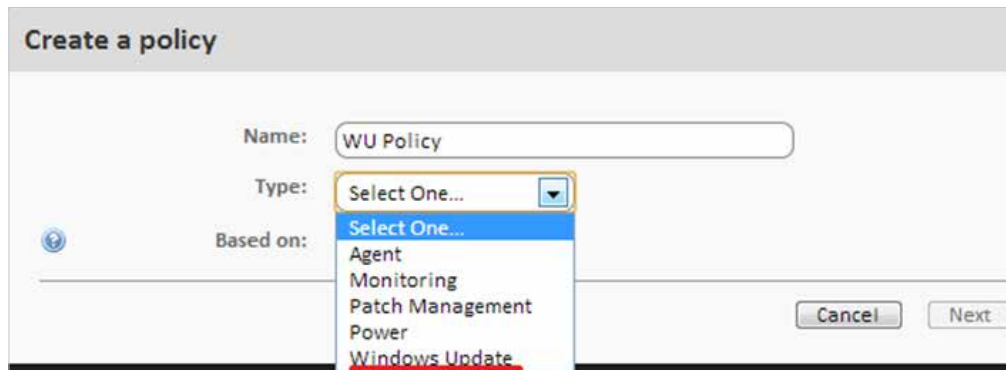
General description

Windows Update policies permit centralized configuration of the Windows Update features integrated in the Windows devices on the network.

As it is a policy, the grouping levels supported by this method are System Level and Profile Level.

Access Windows Update Policy method

To access this method, create a Windows Update policy at Profile Level or System 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
- ✔ Opcional

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 **PCSM** using other Patch Management methods.

i All of the settings in this policy are a transposition of the features of Windows Update on Windows devices. All of the actions specified therefore, refer to the devices and not the **PCSM Agent** or the **PCSM console**.

! Although the policy settings are the same for all devices, the behavior of Windows Update on each device can vary slightly between the different operating system versions.

Below are some of the policy options:

- ✔ **Add target:** lets you add filters or groups that delimit 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
- ✔ **Install new Updates:** specifies when the patches will be installed.
- ✔ **Give me recommended Updates the same way I receive important Updates:** apply the policy selected in Patch Policy for both Important and Recommended patches.
- ✔ **Allow all users to install updates on the computer:** allow the user to manually install the patches.

- ✔ **Give me updates for Microsoft products and check for new optional Microsoft software when updating Windows:** check 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:** define the time before Windows Update prompts the user to restart the device if patches are installed that require this.
- ✔ **Delay restart for scheduled installations:** define 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:** allow an alternative local or remote Windows Server Update Services server to be used in order to minimize downloading of individual patches by each network devices.
- ✔ **Enable Client-side targeting:** if a WSUS server is used with Client-side targeting enabled, the groups and devices they contain will be manually defined in the WSUS server. In this parameter of the policy, you can 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 Policy method usage scenarios.

- ✔ When the administrator needs a guarantee that all important patches are automatically installed on all network devices, without the user obstructing the process.
- ✔ When the administrator does not require control of each patch installed and can delegate the installation decision to Microsoft according to its classification of patches as Important or Recommended.
- ✔ When patches classified as optional do not need to be installed automatically.

Method 3: Patch Management Policy

General description

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 grouped. Whereas the Manual method allows you to choose each patch to apply and the Windows Update Policy allows you to apply patches by level (Important, Recommended or Optional), the Patch Management Policy allows you to select the patches to be applied by grouping them in a more flexible manner: by name, description, size, type and other.

As it is a policy, the grouping levels supported by this method are System Level and Profile Level.

Access Patch Management Policy method

To access this method, create a Patch Management Policy at Profile Level or System Level.

A screen appears where you can centrally configure the behavior of Patch Management for all of the devices affected by the policy created.

Below are some of the less obvious policy options:

- ✔ **Add target:** lets you add filters or groups that delimit the scope of application of the policy.
- ✔ **Window:** allows you to define a patch installation window. During the installation window, the patch downloads can be deployed so as not to collapse the client's data line by selecting the "**Randomize the start time to smooth network load**" checkbox.
- ✔ **Install criteria:** allows you to install all patches published that affect the device without discrimination (**Install all patches**) or define a filter that meets one or various criteria. To define a criteria:
 - ✔ Choose a field in the information published associated to each patch to filter (Field).
 - ✔ Choose the condition (Condition). It will vary according to the data type of the selected Field.
 - ✔ Choose the search term (Search term). It will vary according to the data type of the selected Field.

Install criteria: Install all patches

Filter patches by the following criteria:

<input type="text" value="Description"/> Field	<input type="text" value="Begins with"/> Condition	<input type="text" value=""/> Search term
<input type="text" value="Title"/> Field	<input type="text" value="Contains"/> Condition	<input type="text" value=""/> Search term
<input type="text" value="Severity"/> Field	<input type="text" value="Less than"/> Condition	<input type="text" value="Recommended (1) and Critical (0)"/> Search term

Patch Management Policy method usage scenarios.

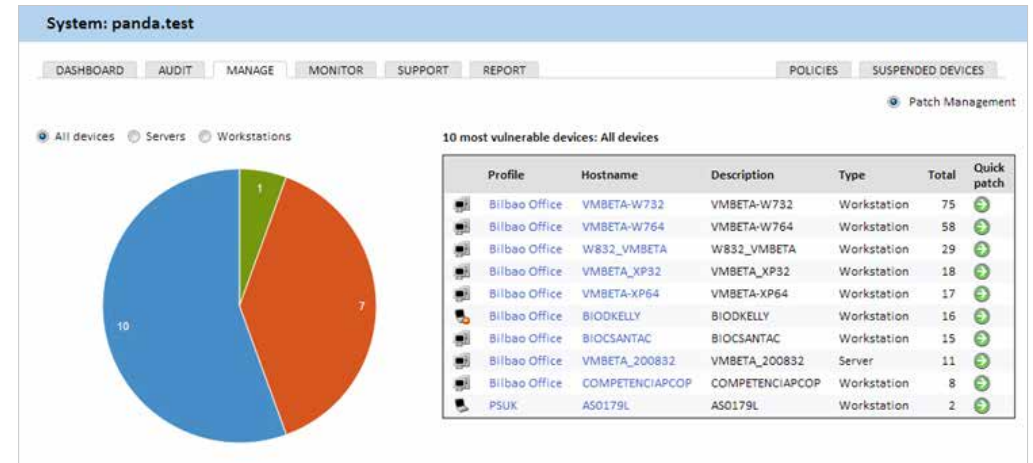
- ✓ When the administrator needs higher granularity than that provided by the Windows Update Policy method.
- ✓ When the administrator needs to install all patches without exception, automatically and centrally.

Method comparative table

Method	Patch selection granularity	Automation	Configuration time
Manual management	High Select patch by patch.	Low Requiere de la aprobación manual y continua de parches.	High Manual revision of all patches published and selection.
Windows Update Policy	Low Patch selection according to "Important" and "Recommended"	High Se configura una vez los grupos de parches a instalar.	Low Choose whether "important" and optional" patches are installed.
Patch Management	Moderate Patch selection via configurable multiple criteria.	High Una vez creados los filtros los parches se instalan automáticamente según Microsoft los libere.	Moderate Define the filters to select the patches to install.

AUDITS

The Manage tab at Profile Level or System Level shows at a glance, the status of the entire network managed as regards patch application.



Selection criteria

The selection criteria (All devices, Servers, Workstations) define a filter for all of the devices in the profile (Manage at Profile Level) or all of the devices managed (Manage at System Level).

Pie chart

After defining the filter criteria, the pie chart will show:

- ✓ The number of devices with non-critical updates not installed (blue).
- ✓ The number of devices with critical updates not installed (orange).
- ✓ The number of devices completely updated (green).

List of vulnerable devices

Clicking any of the two sections of the pie chart updates the vulnerable devices list.

The vulnerable devices list shows information about the most vulnerable devices (critical updates or non-critical updates not applied). It also offers several shortcuts to resolve this situation:

- ✓ **Hostname:** enter Device Level for this specific device in order to see exactly which patches have not been applied and approve those necessary.
- ✓ **Quick Patch:** instantly apply the patches specified by the selected criteria: critical or non-critical, depending on whether you have clicked the blue or orange section of the pie chart.



14. USER ACCOUNTS AND ROLES

WHAT IS A USER ACCOUNT?

A user account is a collection of information, including credentials for accessing the **PCSM Console** and the **PCSM Agent**, needed to manage network devices.

User accounts are only used by IT administrators who want to use the services offered by **Panda Cloud Systems Management**.

In general, each IT administrator has a single user account.



The users of the devices do not need any type of user account as they do not access the **PCSM Console** and the **PCSM Agent** installed on their devices is configured in Monitor Mode by default.



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 Cloud Systems Management**, in this chapter, “user” can refer to a user account or access account for the **PCSM Console**.

WHAT IS A ROLE?

A role is a specific permission configuration for accessing the **PCSM Console**, which is applied to one or more user accounts. This authorizes a specific administrator to view or modify certain **PCSM Console** resources, depending on the role to which the user account used to access **Panda Cloud Systems Management** belongs.

One or more user accounts can belong to one or more roles.



Roles only affect the access level of IT administrators to **PCSM Console** resources to manage network devices. They do not affect other device users.

WHY ARE ROLES NECESSARY?

In a small IT department, all technicians access the **PCSM Console** as administrators with no restrictions. However, in a medium or large IT department or in partners with many clients, 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 clients 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 managed the devices of other offices.

There could also be restricted access to the sensitive data of specific clients, 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 clients 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 role in the IT department, they might only need access to monitoring / validation (read-only) or more advanced access, such as modification of device configurations.

The three criteria can overlap, creating a very powerful configuration matrix that is easy to define and maintain, which allows you to perfectly restrict the **PCSM Console** functions accessible to each technician according to their profile and responsibilities.

THE ACCOUNTADMIN ROLE

A **Panda Cloud Office Protection** user license comes with a default control role, called **accountadmin**. The default administration account belongs to this role and it allows absolutely every action available on the **PCSM Console** to be performed. **Accountadmin** is also the only role that can create new roles and users and modify existing roles.

The **accountadmin** role cannot be deleted from the **PCSM Server** and any user account can belong to this role after it has been assigned through the **PCSM Console**.



All of the procedures described in this chapter require an account that belongs to the **accountadmin** role.

ACCESS USER ACCOUNT AND ROLE CONFIGURATION

In General Menu, Account, there are two entries associated to managing roles and user accounts:

- ✓ **Users:** create new user accounts and define whether they belong to one or various roles.
- ✓ **Roles:** create and modify new settings for accessing **Panda Cloud Systems Management** resources.

Username	Name	Roles	Security Level	Account Admin
<input type="checkbox"/> panda.test	Panda Test	[accountadmin]	5	
<input type="checkbox"/> panda.test@panda345.com	panda.test@panda345.com	[Custom_panda.test@panda345.com]	2	<input type="checkbox"/> OFF
<input type="checkbox"/> panda1234@panda.com	[Custom_panda1234@panda.com]	[Custom_panda1234@panda.com]	2	<input type="checkbox"/> OFF
<input type="checkbox"/> panda@example.com	[Custom_panda@example.com]	[Custom_panda@example.com]	2	<input type="checkbox"/> OFF



The users and roles tabs are only accessible if the user belongs to the special accountadmin role.

CREATE AND CONFIGURE USER ACCOUNTS

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

1) Add new user account: click Add user to add a new user, set a password, specify the role or roles to which it belongs and define the associated security level (from 1 to 5).



The security 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:

- Default
- accountadmin
- Custom_panda.test@panda345.com Migrated custom role for panda.test@pand...
- Custom_panda1234@panda.com Migrated custom role for panda1234@panda...
- Custom_panda@example.com Migrated custom role for panda@example.c...

2) Edit a user account: clicking the username displays a form with all of the account details.

3) Delete or disable user accounts: select the users by selecting the associated checkboxes and click the prohibited and cross icons on the Action Bar.

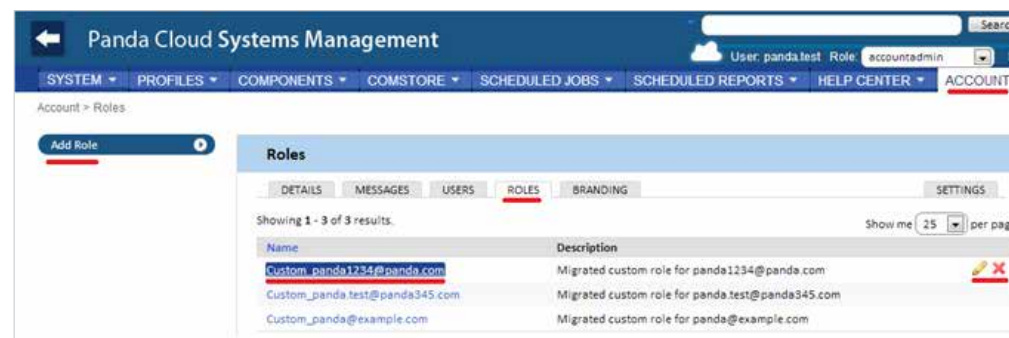
4) Assign total control permissions: click On/OFF in Account Admin.

A user account can belong to one role or more. In the case of the latter, the **PCSM Console** will display a drop-down list through which you can choose the role with which the user account will operate.



CREATE AND CONFIGURE ROLES

In General Menu Account, Users, you can perform all of the necessary actions related to creating and modifying roles.



5) Add new role: click Add Role to add a new role. 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 role will be based on a previous role.

6) Edit a role: clicking the role name or the pencil icon displays a form with all of its settings.

7) Delete role: the X icon deletes the selected role.



If user accounts are assigned to a role when it is deleted, you will be prompted to assign a new role to these accounts.

CONFIGURE ROLES

The configuration of a role is divided into 4 sections:

- ✔ **Device visibility:** enables or restricts access to device groups.
- ✔ **Permissions:** enable or restrict access to the **PCSM Console** features.
- ✔ **Agent Browser Tools:** enable or restrict access to the **PCSM Agent** features.
- ✔ **Membership:** specify the user accounts that belong to the role configured.

Device Visibility

With this configuration group, you can specify the network devices that will be visible to the PCSM Console users who belong to a certain role.

You can allow access to the four static groups available in PCSM:

- ✔ Profiles
- ✔ System Device Groups
- ✔ Profile Device Groups
- ✔ System Profile Groups



You can allow access to dynamic groups such as filters.

Each of them allows you to define whether the device groups of the specified type and created previously by an administrator will be accessible in a certain role or not.

Clicking ON displays a configuration panel.



A group listed in the Include textbox will be visible to all of the user accounts that belong to this role. Similarly, if the group is listed in the Exclude textbox, this device group will not be visible in the **PCSM Console**.

Permissions

Permissions defines the access level for each of the main tabs in the **PCSM Console**:

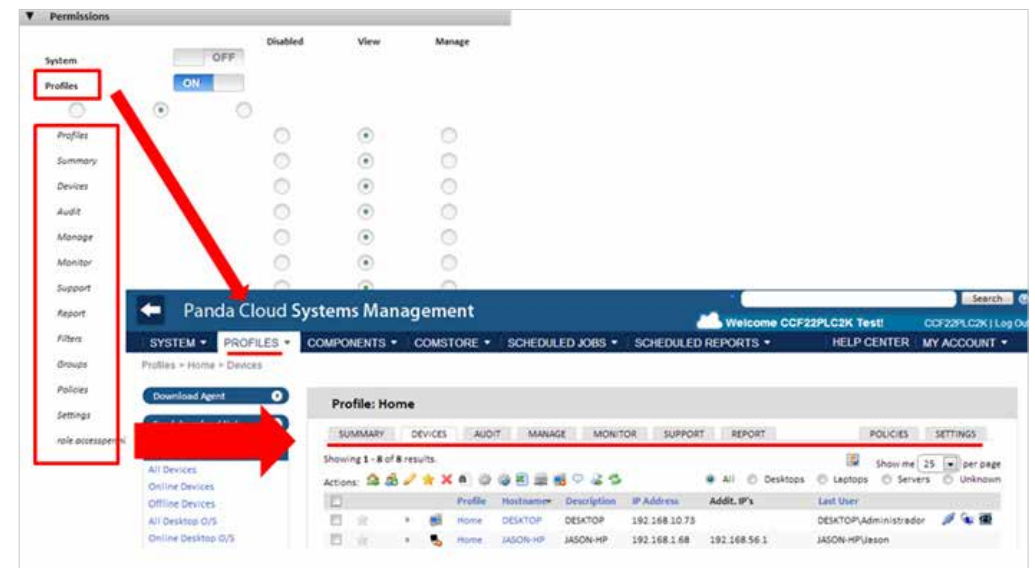
- ✔ System
- ✔ Profiles
- ✔ Components
- ✔ ComStore
- ✔ Jobs
- ✔ Reports
- ✔ Account

There are three access levels:

- ✔ Disabled
- ✔ View
- ✔ Manage

Clicking ON allows you to define each category separately. The content of each category in the Permissions section is a transposition of the options displayed in the **PCSM Console** plus the access level, which can be set for each option.

By clicking General Menu, Profiles for example, you can check the equivalent tabs in the **PCSM Console**.



Agent Browser Tools

This configuration group allows you to specify access to the remote administration tools in the **PCSM 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



Any change made in Agent Browser Tools requires the **PCSM Agent** to be restarted.



These restrictions apply to the local **PCSM Console** of the **PCSM Agent**, on logging on to manage remote devices (Administrator Mode).

Membership

Allows you to configure the user accounts that belong to the role configured.

HOW MANY DIFFERENT ROLES ARE NEEDED?

You can generate as many roles as necessary, bearing in mind that the objective of a role is to restrict administrator access to the devices or **PCSM 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 clients or tasks, so that the exact number of roles on a system will be the result of the weighting of two variables: flexibility vs. security.

Horizontal roles

In general, a company with several offices and an independent IT team in each one will want a total control role 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 office, the following configuration will be needed in each office:

- ✓ 1 Profile o System Group que agrupe a los dispositivos de la delegación.
- ✓ 1 rol que permita el acceso a los dispositivos del Profile y deniegue el resto.
- ✓ Una cuenta por cada técnico, asignada al rol que cubra la delegación designada.

The same schema can be used by a partner who wants to segregate clients and assign specific technicians to them.

Vertical roles

For devices largely aimed at specific tasks, such as print, database, mail servers, etc., you can create roles that restrict access to this type of device.

This will allow a company or partner with many offices or clients 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:

- ✓ Un System Group que agrupe a todos los servidores de correo independientemente del Profile / cliente/ delegación al que pertenezcan.
- ✓ Un rol A que permita el acceso a los dispositivos contenidos en el System Group y deniegue el acceso al resto de dispositivos.
- ✓ Un rol B que deniegue el acceso a los dispositivos contenidos en el System Group y permita el acceso al resto de dispositivos.
- ✓ Tantas cuentas de usuario del rol A como técnicos lleven el mantenimiento de los servidores de correo de la empresa o partner.
- ✓ Tantas cuentas de usuario del rol B como técnicos lleven el mantenimiento de los dispositivos de usuario de la empresa o partner.

Resource access roles

In accordance with the profile or level of experience of each technician, 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 **PCSM 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 **PCSM 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 security levels than those set in the user account.



15. MOBILE DEVICE MANAGEMENT

Panda Cloud 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 **PCSM** 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.

WHICH PLATFORMS ARE SUPPORTED?

Panda Cloud Systems Management supports iOS and Android tablets and smartphones.

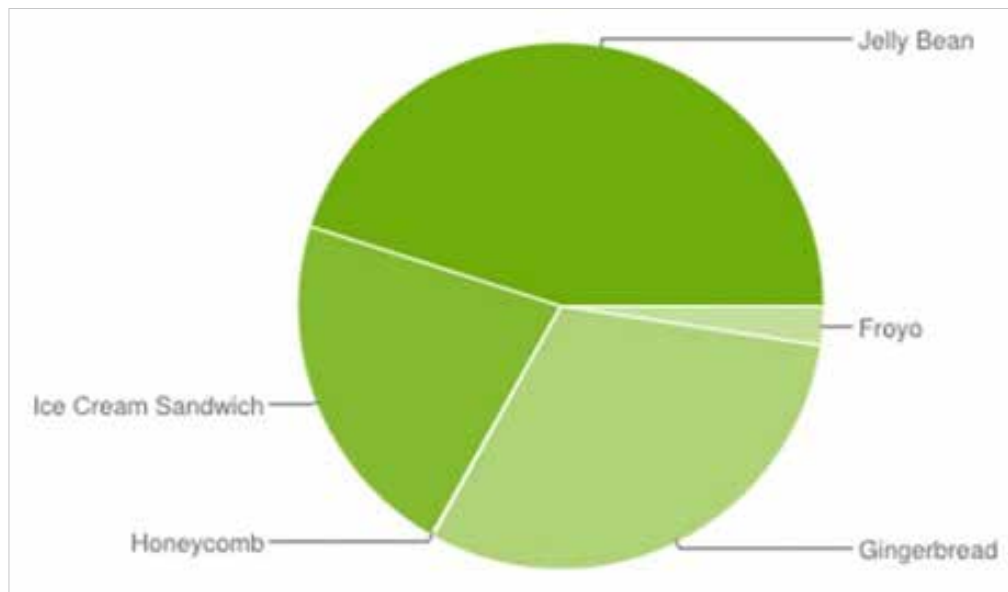
More specifically, the solution supports iPhone and iPad tablets using iOS 6 or later. Here is a list of the supported models:

Model

iPhone 3G (*)	iPhone 4 (*)	iPhone 4S (*)
iPhone 5	iPhone 5C	iPhone 5S
iPad 2 (*)	iPad (3 ^o generation) (*)	iPad (4 ^o generation)
iPad Mini		

(*) Requires upgrade to iOS 6 or later to be compatible with PCSM.

PCSM supports Android devices running version 2.3.3 (Gingerbread) and later. This is the vast majority of Android devices currently in use, except for a negligible percentage of terminals that still use Froyo (2.2.x).



INTEGRATING MOBILE DEVICES IN PCSM

Follow the steps below to manage your mobile devices from the central admin console.

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.

New & Noteworthy

- Firefox 24.0
- Mobile Device Management** (highlighted)

Featured

- Adobe Reader 11.0.05
- Autotask
- CCleaner Slim 4.06.4324
- Clean Internet Browser Caches
- Compatibility Pack for the 2007 Office System
- Connectwise
- Flash Player 11.9.900.117 (IE and non-IE)
- Foxit PDF Reader 5.5.6.218
- Google Chrome 30.0.1599.101
- Hard Drive predicted failure Monitor
- Install uVNC Mirror Driver - NOT XP or Server 2003

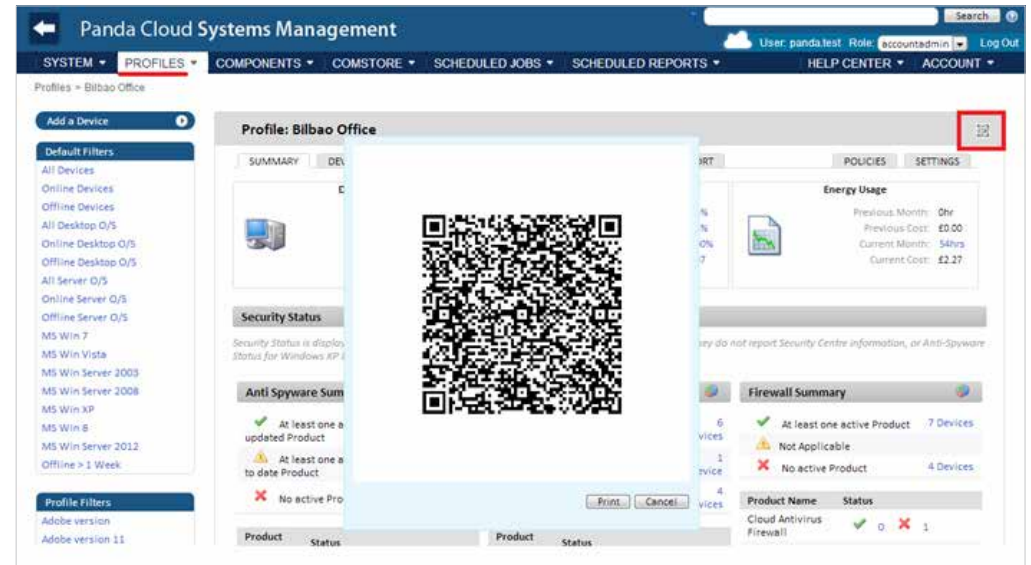


Even though the "Mobile Device Management" component is free, every mobile device with a **PCSM Agent** installed will count as a regular license for the purpose of counting the total number of purchased licenses.

Install the agent

As with other types of devices, to manage a supported smartphone or tablet you need to install a **PCSM Agent** on the device to establish secure communication with the **PCSM server**.

To deploy the **PCSM Agent** to the user's device, **Panda Cloud Systems Management** will generate an email with all the necessary information. To do that, select the Profile to which the mobile device will belong, choose Android or iOS and enter the user's email address.



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

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

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

On mobile phones without camera it is possible to open the .MDM file from the email message by simply touching the file.

After loading the .MDM file, the PCSM Agent will display the message "Connected" on the user's device, and appear on the **PCSM Console**.



The client will receive an email with a download link from the Apple Store or Google Play, and an .MDM file with information about the Profile that the device will be associated with.

Associate the device with a Profile

After the iOS or Android **PCSM Agent** has been installed on the client's device, the user must take the following steps to associate it with the selected Profile. There are two ways to associate a device with a Profile:

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

On a PC with the Web console displaying the Profile to be associated with the user's mobile device, click the QR code to enlarge it.



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

Import the certificate into the PCSM Console (for iOS-based devices)

In addition to the previous steps, it will also be necessary to incorporate -into the **PCSM Console**- the certificate generated by Apple for iOS devices to be able to connect to the **PCSM Server**.



Importing the Apple certificate is a mandatory, one-time process for each client/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 PCSM Server and the user's device.

To do so, follow the steps below:

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

The screenshot shows the PCSM Console interface. At the top, there is a navigation bar with 'ACCOUNT' selected. Below it, the system name 'panda.test' is displayed. A series of tabs includes 'SETTINGS', which is currently active. Under the 'Apple Push Certificate' section, there are instructions for downloading and uploading a CSR and a push certificate. A file selection button 'Seleccionar archivo' is visible, along with a 'Cargar' button. An 'Important Notes' section at the bottom provides details about certificate renewal.

- ✓ 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 instructions on-screen.

Go to <https://identity.apple.com/pushcert> and sign in with your Apple credentials. Click "Create Certificate" and follow the instructions on-screen. Load the CSR file you downloaded in the previous step.

The screenshot shows the 'Certificates for Third-Party Servers' page in the Apple Push Certificate Portal. A table lists the current certificate for 'Mobile Device Management' from 'CentraStage Limited', with an expiration date of 'Oct 17, 2014' and a status of 'Active'. The 'Actions' column includes 'Renew', 'Download', and 'Revoke' buttons. A 'Create a Certificate' button is circled in red at the top right of the page.

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

This screenshot is similar to the previous one, but the 'Download' button in the 'Actions' column of the certificate table is circled in red, indicating the next step in the process.

Go back to the **PCSM 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:

The screenshot shows the 'Apple Push Certificate' section in the PCSM Console. A red-bordered box highlights a confirmation message: 'You have already uploaded the Apple push certificate, which expires on 2014-10-17 15:56:51 UTC Apple Push Topic: com.apple.mgmt.External.9f1992a1-56c5-4431-8ec2-96b56a5ba883'. Below this, there are instructions for renewing the certificate and a list of steps for downloading and uploading a new CSR and push certificate. An 'Upload' button is visible at the bottom right.

TOOLS FOR REMOTELY MANAGING MOBILE DEVICES

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

The **PCSM Console** functions regarding mobile devices are only available at Device Level for the relevant device.

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



Device Wipe

Performs a remote factory reset of the device. This feature prevents data theft in the event of device 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.

Geolocation

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 (Wifi Position System)
- ✔ GeoIP



GeoIP may report a location completely different from where the device actually is.

Lock Device

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.

Unlock Device

Unlocks a locked device (resets the security PIN should the user forget it).

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 launches a remote request to the user to set the PIN, it doesn't allow the administrator to set it from the console.

Audits

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

The **PCSM Agent** collects all hardware and software information from the device on which it is installed, and notifies any changes to the **PCSM 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 (usually 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.

Reports

The reports adapt to the type of device. The Reports tab behaves in the same way as for Windows and Mac devices.

16. APPENDIX A

Source code of the component in 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
    `PCSM didn't send the environment variable
    err.clear
    WScript.Echo "<-Start Result->"
    WScript.Echo "Result=PCOP_
PATH variable not defined on PCSM 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 text
    `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 is 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

```

17. APPENDIX B

Source code of the component in chapter 11

```
Option Explicit
*****
`Deploy_documents v0.99b
`12/03/2013
`By Oscar Lopez / Panda Security
`Target: It creates a folder int the user's desktop and copy on it the
`documents to deploy
`Entrada: files to copy
`Salida: 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 in 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)
```

