PANDA CLOUDSYSTEMSMANAGEMENT

Guide for Partners and IT Administrators

PANDA SECURITY | *The Cloud Security Company*

1. CONTENT

1. PROLOGUE

This guide contains basic information and procedures used to obtain the maximum benefit of the product **Panda Cloud Systems Management (PCSM, Systems Management).**

Audience

This documentation is written with users from two possible environments in mind:

- The IT Department which provides internal support to the rest of the organization.
- The Managed Service Provider (MSP) which currently provides services to their customer accounts onsite, remotely, reactively or proactively.

Icons

This guide will contain the following icons:

Additional information, for example, an alternate method for performing a particular task.

Suggestions and recommendations.

Important and/or useful tips for using **Panda Cloud Systems Management**.

2. INTRODUCTION

Panda Cloud Systems Management is a solution for cloud-based remote monitoring and management of devices for IT departments that want to offer a professional service while minimizing disruptions to the user. **Panda Cloud Systems Management** increases efficiency through centralized management of Devices, while promoting the automation of tasks. The overhead costs dedicated to serving each customer or account are reduced because PCSM includes:

- No additional infrastructure required on-site as the solution is hosted in the cloud.
- A very gentle learning curve for technical support, allowing you to deliver value from day one.
- Tools accessible from anywhere, anytime allowing you to administer support remotely and avoiding lost time and money by removing the need to travel to those sites.
- Automating tasks and responses triggered by configurable alerts that prevent failures before they occur.

Panda Cloud Systems Management is a product that promotes collaboration among Technicians responsible for providing support and minimizes or completely eliminates the time spent interacting with the user to determine the causes of the problems.

Principal Functions 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 supports NAT firewall and VPN device communications with the Management Console.
Automatic Detection of Devices	An 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 made to the device (hardware, software and system).
Software License Management	Keep track of all software installed
Alerts and Monitors	Monitor performance, services and Exchange Servers, with alerts... all in real time.
Scripting and Quick Tasks	Create your own scripts, download our preconfigured scripts from the ComStore online, and deploy them with one click, either on a scheduled basis or as an automatic response to an alert.
Patch Management	Automate the deployment of updates and patches for software installed.
Software Deployment	Centralized update and software deployment.
Policies	Establish a set of general settings to manage your IT environment in a flexible manner.
Remote Access	Task manager, file transfer, registry editor, command prompt, display the event log, etc. All of these integrated tools enable you to repair multiple devices without interrupting your users.
Remote Control	Shared or takeover access to the user's desktop that is compatible with firewall and NAT.
Secure Communication	All communications between the agents and the server are encrypted (SSL).
Detailed Information	Mail scheduled or special reports. Find out who does what, when, and find out who uses most of those resources.
Collaborative Environment	Manage the allocation, state and documentation of incidents with the ticket system. Facilitate the creation of historical documentation in 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.

Panda Cloud Systems Management User Profile

Most users of **Panda Cloud Systems Management** will share a technical medium – management and daily maintenance of computing devices subjected to a constant rate of use and change. However there are two specific, targeted user groups of **Systems Management**:

- **Enterprise Level IT Technicians**

High level techs are employed by a company to offer companywide a support service to the devices and end-users, no matter their location. These scenarios often include the existence of remote offices to which access is restricted so technicians must utilize monitoring tools and remote access for roaming users outside the office, which makes them susceptible to all types of problems with their devices.

- **Service Provider (MSP) Level Technicians**

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

Principal Components of Panda Cloud Systems Management

The following is a summary of the components that are within Systems Management:

- **Management Console / Console / PCSM Console**

This is a web portal accessible via compatible browsers, from anywhere, anytime with any web enabled device.

Most of the daily tasks of tracking and monitoring will be made from this console. This console is a resource available to technical support only.

- **Device Agent / Agent / PCSM Agent**

It is a small program less than 5 megabytes in size that is installed on each of the devices to be managed. After installing the agent on the device its information will become directly accessible through the Management Console.

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

– **User Mode**

In this mode the Agent is more or less unnoticed by the end-user. More access to some of the configuration of the Agent can be delegated by the Administrators.

– **Administration Mode**

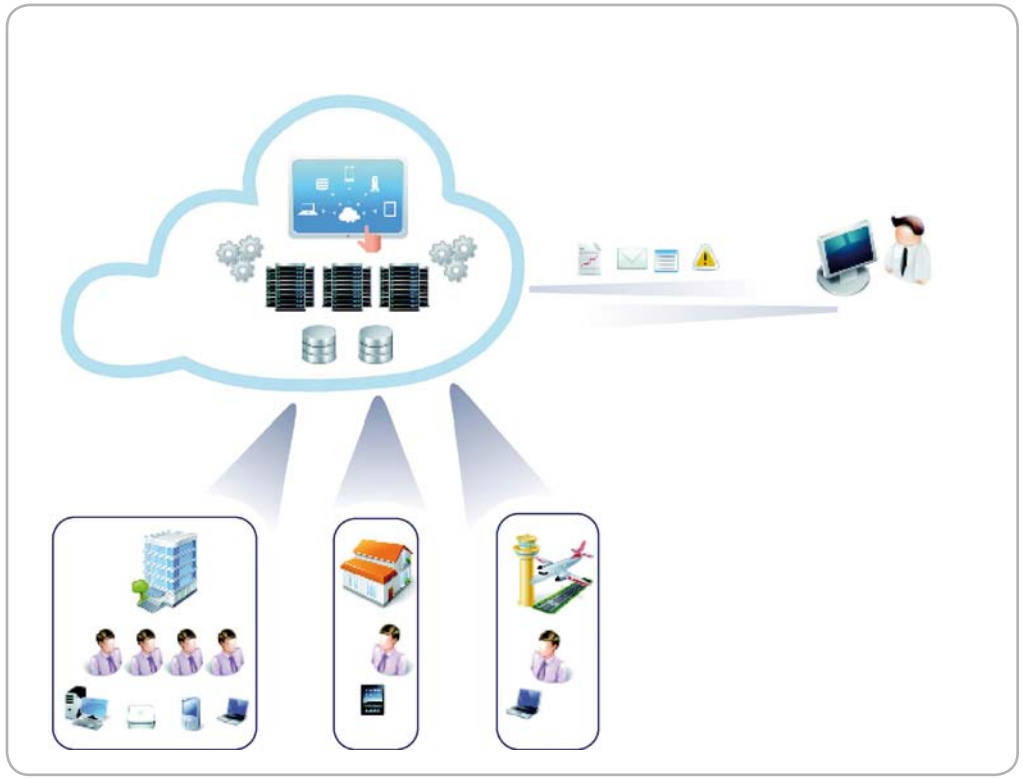
After using valid credentials, the technician may use the Agent in Administrator Mode to access devices remotely and administer support.

Install the Agent in both the client devices and those belonging to the technicians in order to have complete access to the entire solution.

- **Administration Server / Server / PCSM Server**

The **Management Console**, processes required to collect, synchronize and redirect messages, events, and information flows generated by the **Agents** and the databases that support them are all hosted in the **Cloud** and have 24 hour availability.

The status information that flows from each of the devices to the **Management Server** is highly optimized so that the impact on the customer's network is miniscule. In the Server this information is sorted and consolidated to be shown as a flow of events that will diagnose and even efficiently predict the problems of managed devices.



General communication architecture: Devices and technical team interacting with the PCSM Server.

Key Players of Panda Cloud Systems Management

The key players that are involved and will be referred to throughout the guide are listed below:

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

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

In any case, the responsibility of administering and monitoring the systems within the company lies with the technical staff of the IT department, or the MSP contracted to provide these services.

- **PCSM Administration Account / Administration Account**

Each client or company utilizing Panda Cloud Systems Management will have access to the Account Management tab. An account with the highest level of privileges can manage all product features.

Each Administration Account has a secure environment. Settings and Devices that run in other accounts will not be accessible by the administration team.

- **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. A client account generally means all the client devices are to be managed by the MSP. For companies that acquire Panda Cloud Systems Management for internal use the Client Account is a more organizational level: the different accounts will be created to organize the management of different departments of the company.

- **User**

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

- **Device**

A Device is a computer that has installed an agent and is operated by the user in their daily work.

3. HIERARCHY OF LEVELS WITHIN THE MANAGEMENT CONSOLE

In order to separate the management of devices from different customer accounts, reuse and limit procedures established by the Technical Staff in the Console, and to expedite and refine their management, Panda Cloud Systems Management provides three levels of organization:

1. ***System level***
2. ***Profile level***
3. ***Device level***

Administration hierarchy in 3 levels.

System Level

What is it?

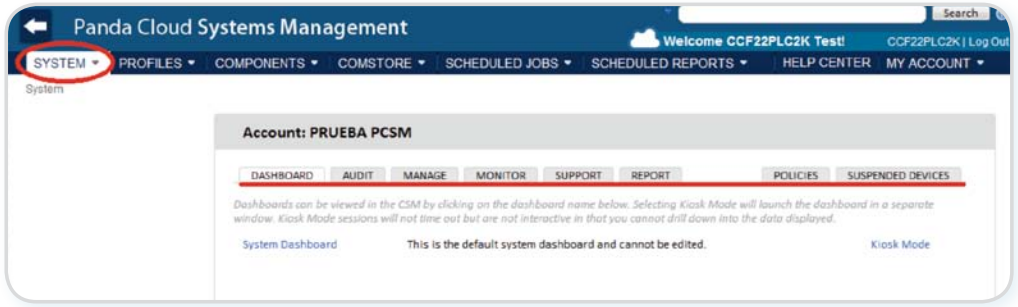
The System Level also referred to as Account or Account level entity cluster is the highest level, and is also unique for each MSP / IT Department. Under its roof fall all devices managed by the MSP / IT Department belonging to their customers and users, and have an Agent installed.

Scope

The actions taken at this level will affect all devices below the system level although they may be limited to a subset of devices using filters and groups, described below.

Access

Access to the resources of the System Level is reached from the System menu.



Functionality

The System Level has the ability to perform actions on a global basis, so you can get the status of all managed devices, consolidated reports from your environment and actions on all or part of the registered devices.

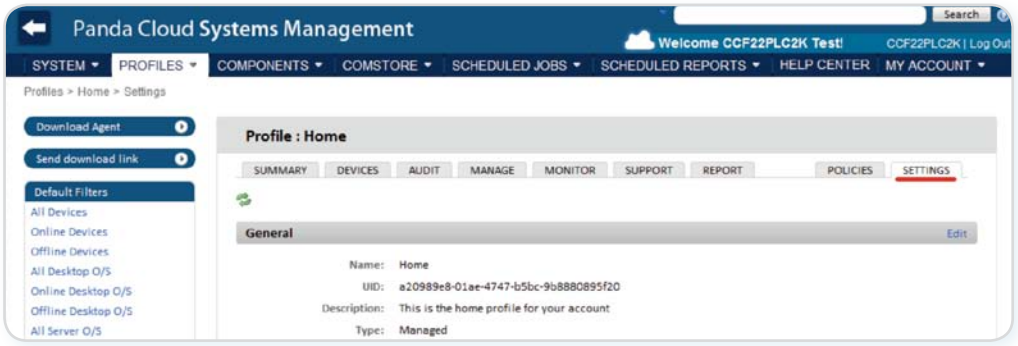
Profile Level

What is it?

The Profile Level is a grouping entity immediately below the System Level. It is a logical grouping that contains the devices that belong to the same customer account or set of profile configurations.

The list of Profiles and access to configuration at this level is under the Profiles tab.

Each Profile is associated with a number of configurations accessible from the Settings tab in the Management Console, which in turn are packaged with the Agent.



Configuration options can be divided into several groups.

- **Profile Identification**

This is used to identify a Profile from the rest of Profiles generated and used in filters or searches. Fields configurable are:

- **General:** Name of Profile and description
- **Variables:** Environmental variables so that the devices may be invoked from ascript for future use
- **Custom Labels:** Five fields with information defined by the Administrator

- **Contact Information**

The default email accounts which are used for sending reports and alerts.

– **Alert Mail Recipients**

– **Report Mail Recipients**

- **Local Cache**

This field will serve to identify the Profile's local cache to speed up client software, patches or scripts that are later distributed among the neighboring devices. This identifies a single system to handle these files, thus reducing bandwidth consumption by preventing them from having to download the aforementioned items individually.

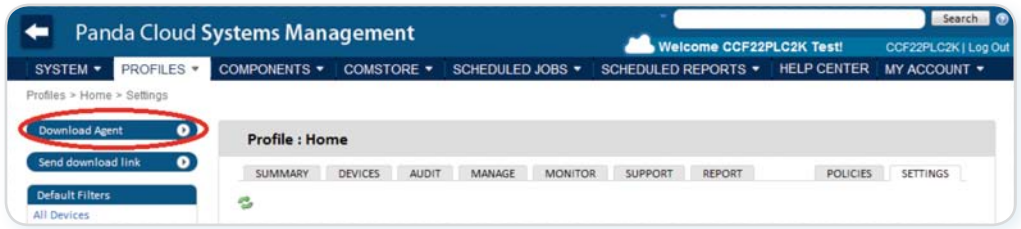
- **Login Information**

The execution of scripts in the user's device inherits the permissions associated with the local host account, but if the Profile needs to run scripts with the "Run As" command you can enter the login and password information here in the Web console for use.

- **Consumer Information**

We can associate power consumption information for each of the devices to show overall consumption as well as contrast it against variations in the power saving settings, through Policies which are explained below.

The above information has been embedded within the Agent as Profile membership, and as such is directly downloadable from the same screen as Profile Management.



When the **Agent** is installed on client devices they are automatically added to the correct **Profile** in the **Management Console**.

Scope

The configuration set at the Profile level can affect all devices belonging to that Profile, while some actions and configuration may be limited to a subset of devices using filters and groups, described below.

Unlike the System Level, the Administrator may create as many groups as needed within the Profile.

Membership

The membership of a given device to a Profile is determined by the Agent installation.

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

You can move devices from one **Profile** to another from the **Device Action** Bar after you install the **Agent**.

To minimize the tasks in the deployment phase it is recommended to first create a **Profile** and then download the **Agent** from it, so that ownership of the managed device is automatically assigned to the correct **Profile**.

Functionality

The **Profile Level** has the ability to perform actions on all of the devices that are contained within it. This makes it possible to create reports, alerts and tasks to run on the devices which make up the **Profile**.

Device Level

What is it?

This represents a single node, end-point, or **Device** which has an **Agent** installed and is reporting to the **PCSM Management Console**. **Devices** are automatically created within the **PCSM Console** when they have **Agents** installed on them.

Scope

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

Functionality

The **Device Level** has the ability to perform actions on a particular **Device**. This makes it possible to create reports, alerts and tasks to run on a single end-point.

4. BASIC ELEMENTS OF THE CONSOLE

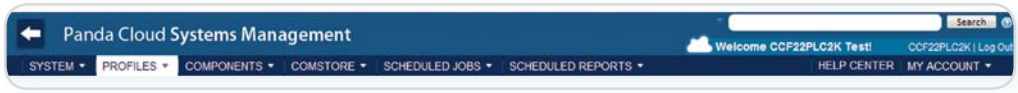
The **PCSM Management Console** is structured in an intuitive and visual manner, so that most management resources are a click away, avoiding the clutter of unnecessary checkboxes and configuration.

The goal is a Console which is clean, quick to use, and comfortable, while avoiding wherever possible the full page reloads and steep learning curve of other solutions, allowing you to deliver value to a client or department from the date of deployment.

The basic elements of the console to which we will refer to throughout this guide are:

General Menu

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



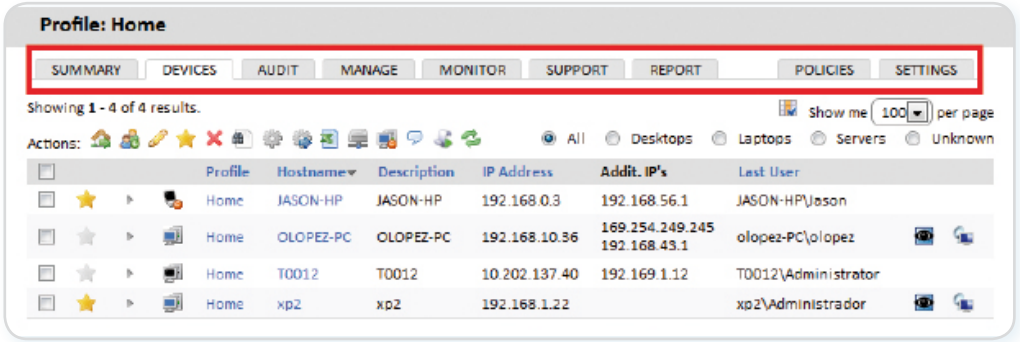
Elements:

Menu	Description
System	System Level Access
Profiles	Profile Level Access
Components	Applications, Tools, and Scripts accessible by 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

Tab Bar / Tab Bar Lists

The **Tab Bar** provides access to the various available actions and information in the console corresponding to the particular Devices and Levels at which it is accessed. It allows access to configuration changes, audit information, policy creation, etc., and is generally where most of the work is done at in the Management Console.

This bar is slightly different if it is accessed from **Profile, System**, or **Device Level**, and for each level the management scope is also different.



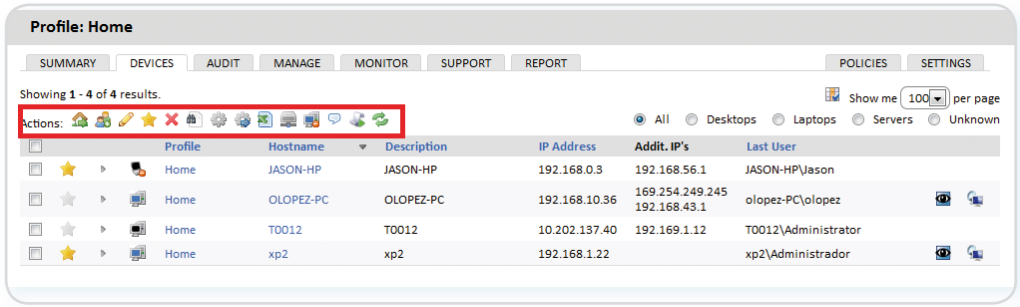
Elements:

Tab	Accessible From	Description
Summary	Profile, Device	**Information**
Dashboard	System	Master Information Control Panel
Devices	Profile	**Devices accessible** with associated information
Audit	System, Profile, Device	**Inventory** of hardware, software and licenses
Manage	System, Profile, Device	**Patch Management** with both pending and applied lists
Monitor	System, Profile, Device	**Alerts** created by monitors or finished jobs
Support	System, Profile, Device	Generated **Tickets**
Report	System, Profile, Device	Custom and predefined **Reports**
Policies	System, Profile, Device	Generated **Policies** (explained later)
Settings	Profile	**Profile** associated configuration
Suspended devices	System	Uninstalled **Devices**

The scope of the Tab Bar refers to the current level. Thus, if you access the Tab Bar at System Level it will show you the information for all Devices; if you look on Profile Level the data reflected will show only Device participants within that corresponding Profile. If you look at Device Level, it will only show information for that particular device.

Icon Bar / Action Bar

The Icon Bar or Action Bar allows access to actions aimed at changing the status or configuration of the devices. This bar does not exist in the System menu and varies slightly if accessed from the menu or from a Profile Device since the scope of management is different.



Icon	Accessible from	Description
Move Device to	Profile, Device	**Moves a Device** to another **Profile**
Agent Based	Profile, Device	**Adds Devices** to a selected Group
Edit	Profile	**Add notes and custom fields** for a selected Device that can be used by filters (discussed later)
Toggle	Profile, Device	Mark as favorite Devices for quick access from Summary / Dashboard
Delete	Profile, Device	**Deletes a Device from a Profile**. The option instructs the Agent to run an uninstall instruction and the Device is added to the **Suspended Devices Tab** under **System**
Request audit	Profile, Device	**Forces and Inventory** of the selected **Device**
Schedule Job	Profile, Device	**Create a Scheduled Job** for a later date
Run a Quick Job	Profile	**Create and Run a Job** using a selected component
Download CSV	Profile, Device	**Downloads a list of Profile Devices**
Add/Remove Cache	Profile, Device	**Mark the Device as local cache**
Turn Privacy On	Profile, Device	**Prevents Remote Access By The Administrator** of the devices unless approved by the User
Send a message	Profile, Device	**Sends a message** to the selected devices
Schedule reports	Profile	**Configure and Schedule Reports** for a later date
Refresh	Profile, Device	Refreshes the data on the screen
Initiate	Device	**Initiates a Deployment** from the selected device to other nodes connected to the same network as the device
QR Code	Device	QR code associated with the device for paper inventory

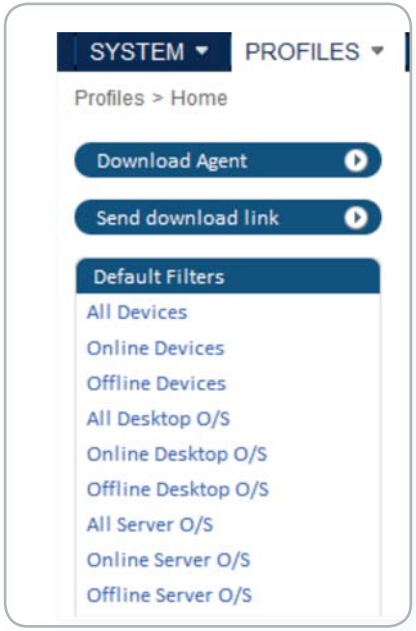
The scope of the **Icon Bar** will be formed by manual selection of Devices that have been marked in a Profile.

If you want to perform actions at the System Level you will need to create a filter or group (explained below) as the System Level does not display the toolbar by default.

Filters and Group Panel

The left side of the console will have three panels with different groups:

- **Default Filters:** Filters automatically generated by the system
- **Profile/Custom Filters:** Filters created by the Administrator in the Profile or System Level respectively
- **Profile/System Groups:** Groups created by the Administrator in the Profile or System level respectively.

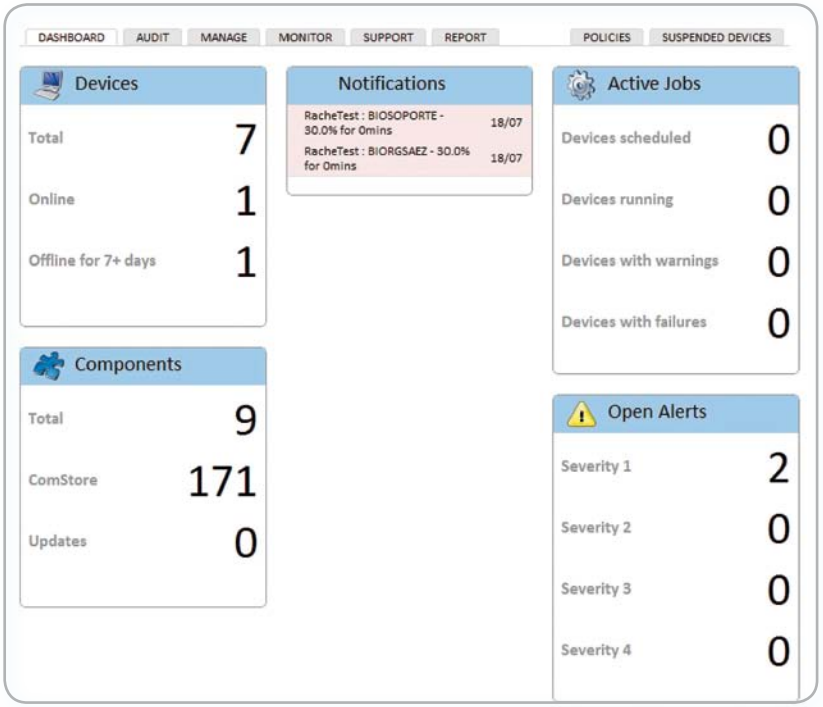


Control Levels

The Control Levels reflect the status of a set of devices. There are three types of Control Levels:

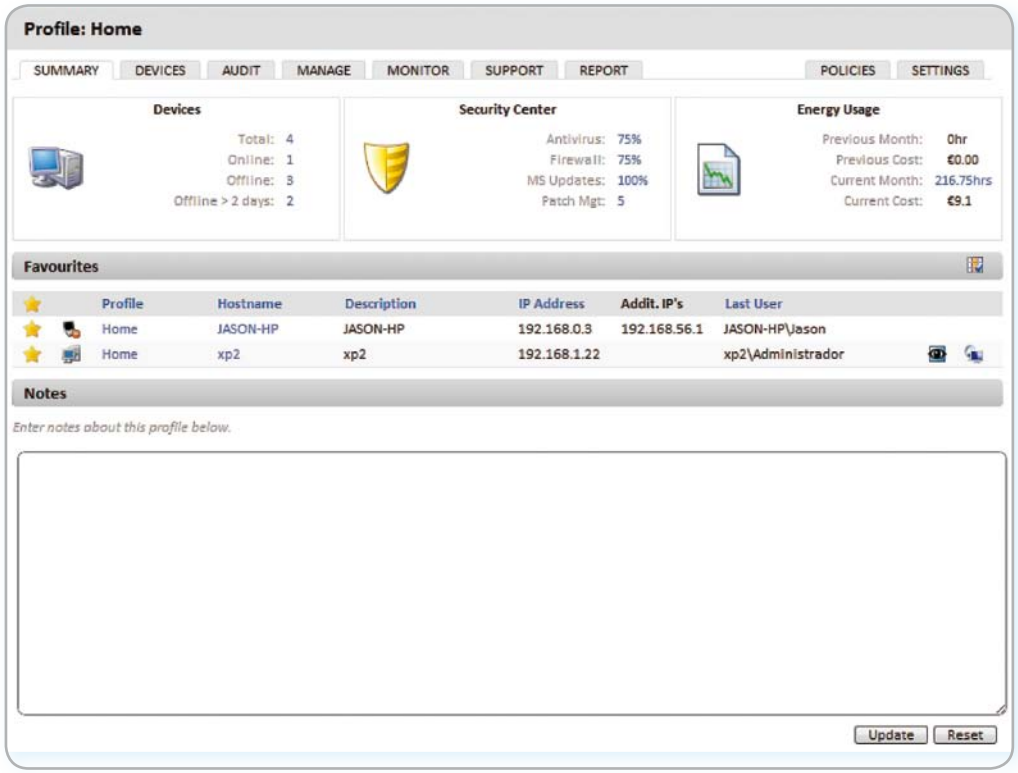
System (Account) Level

The System Level reflects the status of all Profiles and Devices contained that are managed by the MSP. This is the highest level and there is only one System (Account) Level Menu per account.



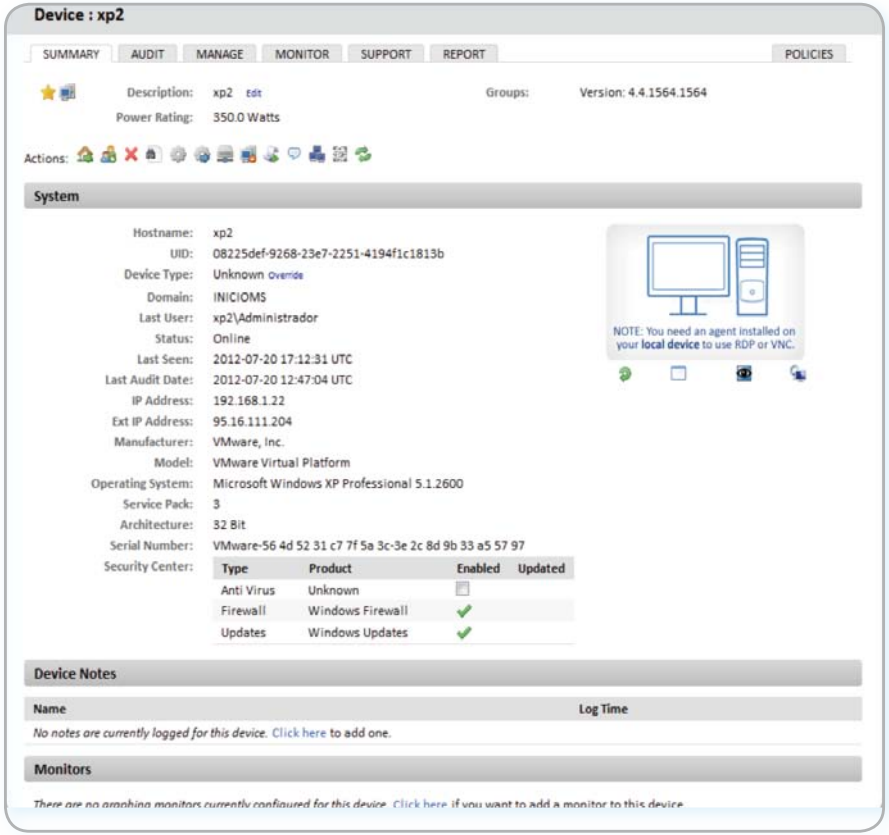
Profile Level

The Profile Level reflects the status of all Devices that belong to the selected Profile. There will be a Profile Menu for each Profile created.



Device Level

The Device Level reflects the status of a particular Device.



5. FILTERS AND GROUPS

What are the *Groups* and *Filters*?

Groups and Filters are resources designed to generate clusters of similar Devices within a Profile. So while creating a Profile is considered a static aspect of marking Devices as belonging to a specific container, Groups and Filters are designed to be modified with ease in response to temporary characteristics or criteria of those Devices.

Types of *Groups* and *Filters*

There are two types of Groups and Filters:

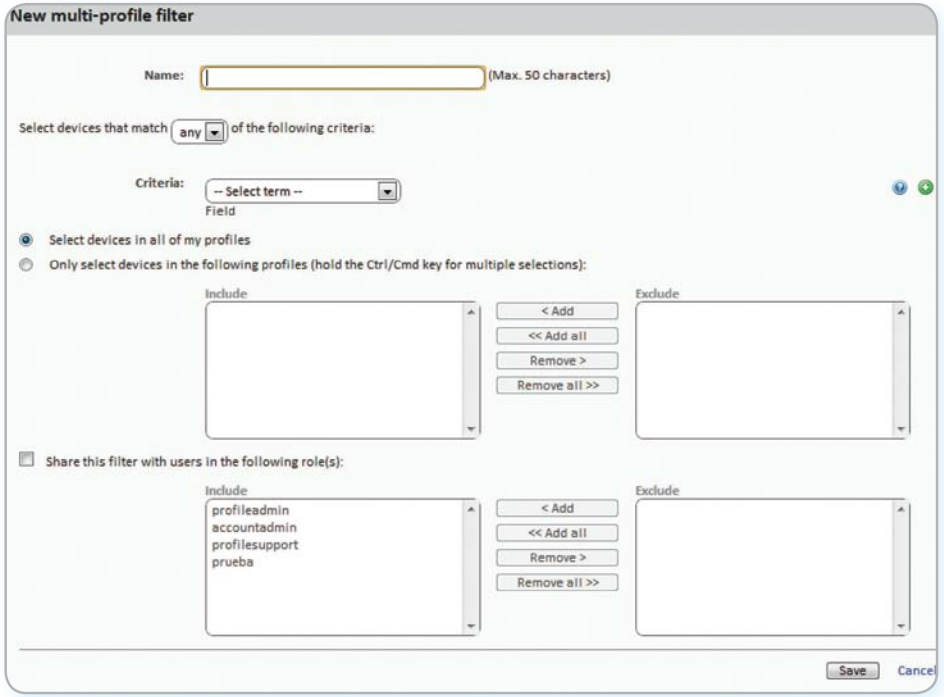
- **Profile Groups/Profile Filters:** Created within a selected Profile, they can only contain Devices within the corresponding Profile
- **Account (multi Profile) Groups / Custom Filters:** Created from the Profiles tab, without selecting a specific Profile, they can contain Devices that belong to one, several, or all Profiles

Groups

Groups are collections of static devices. Membership of a Device to a Group is manual by direct allocation.

Filters

Filters are dynamic groups of Devices. Membership of a device is automatic, as they set their conditions for membership. The conditions of membership of a filter can be one or more characteristics and are linked by logical operators (AND/OR).



The following are the steps to build a **Filter**

- **Name the Filter**. It is recommended 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 the logical operation that can be applied are:
  - 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 line consists of several terms that describe fields, by type:
  - **Field:** Field is the main feature of the device that it will include as part of the filter. The main areas are listed and classified below.
  - **Condition:** Sets the field for comparison which the Administrator can establish.
  - **Search Term:** Describes the content in the Field. Depending on the type of Field, the Search Term Condition will reflect changes made to date ranges, sections, etc.

Here are the different values for each 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	Strings may use % as a wildcard
Integer	Greater – Greater than or equal, Less – Less than or equal, Includes, Excludes	Numerical.
Binary	Profile	Interval of Dates

- Add several lines of type Criteria with "+" and "-" icons on the right
- **Select the area of the Filter:**
  - All Devices in all Profiles
  - Only Devices in the selected Profiles
- Select Users of the Console which have access to the Filter

The features described in the Field can be grouped as follows according to their function Device descriptor:

Device Status	Option	Definition
	Status – Online/Offline	Device on or off
	Status suspended	Suspended Device
	Antivirus On/Off	No AV Detected
	Firewall On/Off	No Firewall Detected
	Free disk capacity	Detects the device's free storage
	Windows updates On/OFF	Detects if the device has Windows Updates configured or not
Device Role	**Organization by OS, Client type, or Server type**	
	Device Type: Server, Workstation, Smartphone, Laptop	Specific type of installed Device
	Operating System	Allows system organization of server or client
Software Version	**Software Data**	
	Service Pack	Service pack version
	Software Package	Software installed
	Software version	Specific software versions
Hardware	**Information on model, version, device type, etc.**	
	CPU	Processor type
	BIOS Name/Release/version	Installed BIOS and version information
	Display Adapter	Type of display adapter installed
	Manufacturer	System manufacturer name
	Memory	Amount of included RAM
	Model	System model name
	Monitor	Type of monitor connected
	Motherboard	Type of motherboard model
	Network Adapter	Specific name and model number of Network Adapter

Function Device descriptor part 2:

Device ID	Information that identifies and describes the device	
	Description	Brief Device description
	Profile Description	User-created notes to describe the profile
	Profile name	Name of the profile the Device belongs to
	Domain	Network Domain the system is a part of
	IP Address	Individual system IP
	MAC Address	Available MAC address of hardware installed on Device
	Serial number	Device serial number
	Hostname	Name assigned by the OS
Other States		
	Favorite	For quick access from the Dashboard
	Last seen	Previous timestamp of connection information sent
	Last audit	Previous timestamp of full audit information sent to console
	Last user	Last user to have logged into the system

6. HOW TO MANAGE THE DEVICES EFFICIENTLY

The distribution in the console of the managed devices within an MSP or IT department with multiple client accounts and various levels of delegation drastically affects their efficiency since 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 of *Profiles*, *Groups* and *Filters*

The following describes the advantages and limitations of the three ways of grouping that are supported.

Profiles

- Benefits:
  - Associates the same outbound Internet settings to all devices: Device saves manual configuration to local cache
  - Linked contact information for sending reports, alerts, etc. via email
  - Access to the tabs bar and the icon bar that allow the execution of actions and display of Listings and Consolidated reports, which covers all of the Profile Devices for ease of use
- Limitations:
  - Any Device can only belong to one Profile
  - It is not possible to nest a Profile within a Profile

Filters and Groups

- Benefits:
  - The Groups / Filters let you create subsets of devices within one or more
- Limitations:
  - The Groups / Filters have limited functionality as they lose access to the tab bar so it is not possible to generate consolidated listings.
  - Reports generated via Groups / Filters will only contain information of those singular devices.

The Groups / Filters are cross functional between profiles and are unlimited (as many as you like) but have limited access to consolidated reporting and tab bar functionality

General Approach and Management Structure of Devices

The following general rules are applied:

- **Group Devices in Profiles to separate different customer accounts or configuration sets.**

The Profiles do not impose any inherent limitations on generating reports or consolidated listings and allow configuration to all of the Devices belonging to that Profile.

- **Create Profile Groups to group devices by similar features such as hardware, software, or configuration.**

For example, configure Profile Groups to separate Devices by departments within a client account with similar features (software utilized, general requirements, printer access, etc.) or by different roles (Servers/Workstations)

- **Create Profile Filters to find computers with common states within a Profile.**

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

It is not advisable to use filters for static character groups.

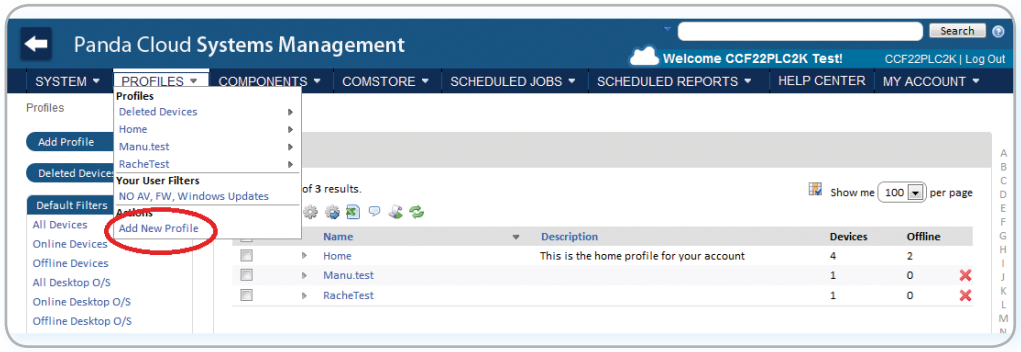
- **Associate Account Groups and Filters to Technical Profiles.**

If the size of an MSP or Company is very large there may be high level technicians on staff. In this case those Technicians may only support high level environments such as Citrix Farms or Exchange Servers. A Group or Account type Filter helps them locate and group these computers without having to go Profile by Profile in their search.

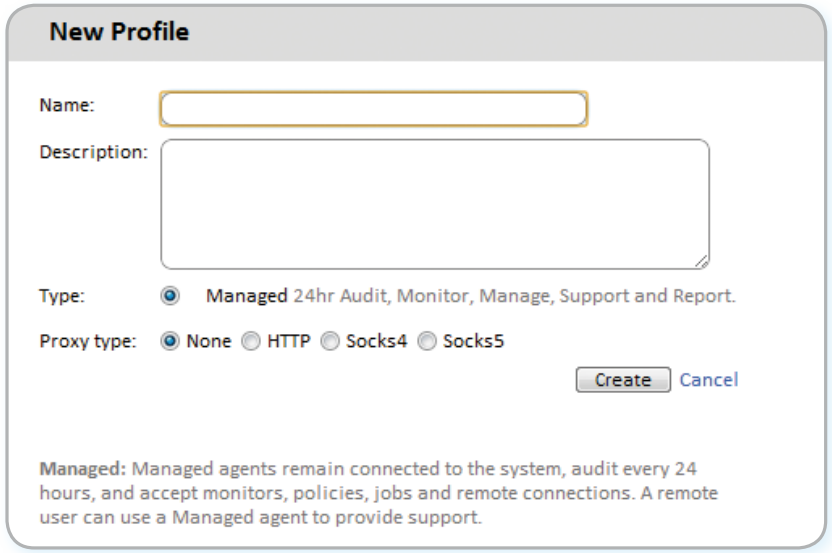
7. THE FIRST 8 STEPS TO BEGIN USING PCSM

Creation and configuration of the first *Profile*

First you must determine whether to create a new Profile or reuse one already in use, depending on the criteria you are using. Generally, a new Customer account or configuration set will correspond to a new Profile.



Fill in the information accordingly and keep in mind that the description field may be subsequently used by filters.



If the Profile Devices require additional HTTP proxy to access the Internet this information can be provided here or can be added at a later time.
Once the Profile is created, it is recommended that the Settings tab is configured. This configuration will be incorporated within the Agent installed on each managed device belonging to the Profile.

Deploy the Agent

The Agent installed on the Devices will require certain basic information in order for it to function:

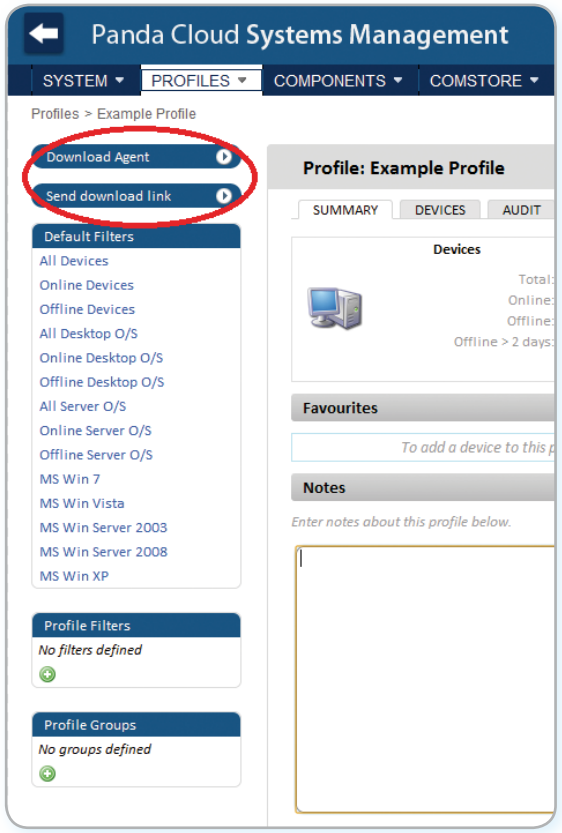
- The Profile which it will belong to.
- The minimum information required for it to reach the Internet and connect to the **PCSM Management Console.**

Profile membership is automatically established if the distribution of the Agent is started from within the Profile Agent.

The information set within the Profile Settings tab required to successfully connect to the Internet was indicated in the previous step so any subsequent installations of the Agent will automatically contain that information.

The Agent download can be done in two ways:

- Direct Agent downloads (mail, GPO package, etc.).
- Direct email link to the Agent .



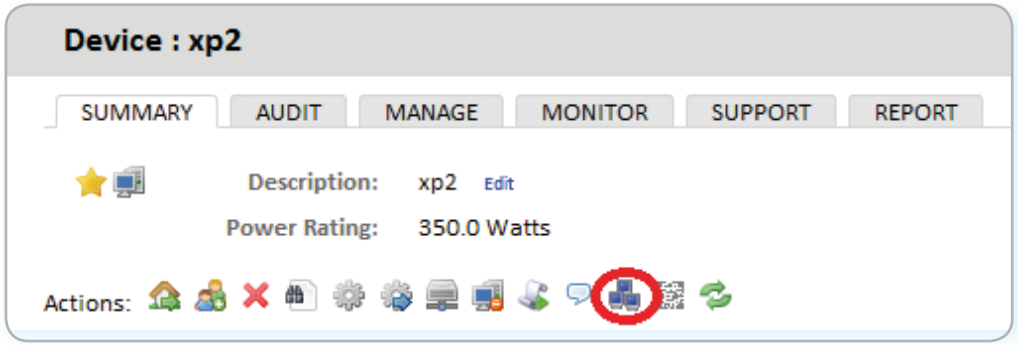
The installation and deployment of the Agent on large networks can be long and tedious if you have to send it to each device independently. It can be faster and easier if you perform a mass deployment:

- Send the Agent to the first Device on the Network.

Normally Agent installation only requires a double click on the downloaded package, and performs the install completely "silent" without confirmations. Once installed, the agent will connect to the PCSM Console and will appear in the list of managed devices in the selected Profile

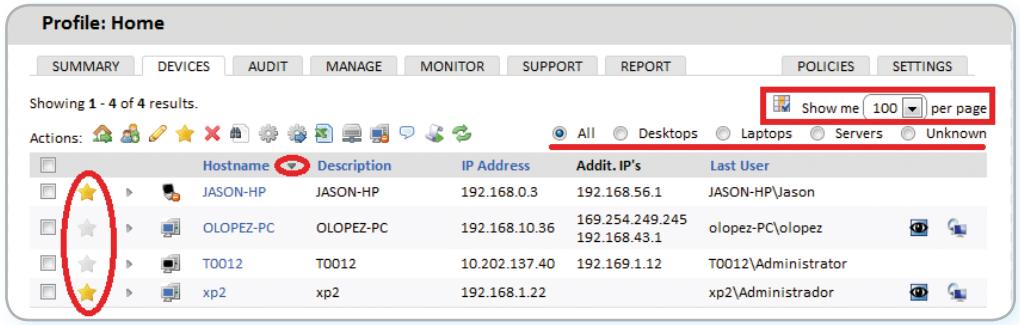
- Auto Deploy to other network devices.

Selecting the Device with the first Agent installation you can start a mass deployment within the rest of your network.



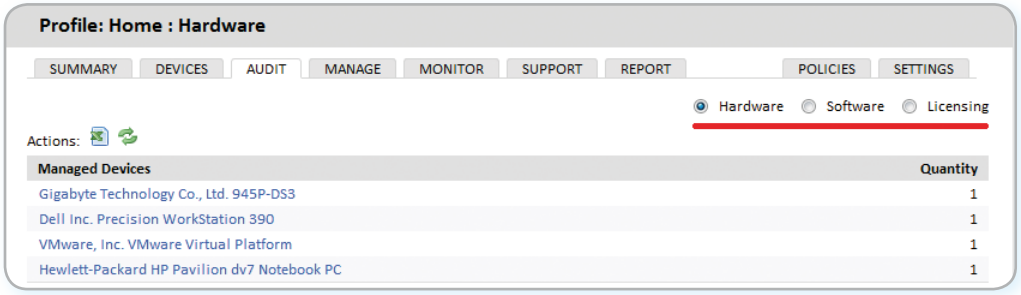
Check the List of Profile Devices and Basic Filtering

You can favorite the Devices, organize the lists, or quickly filter according to the role of the device and change the size of the list.



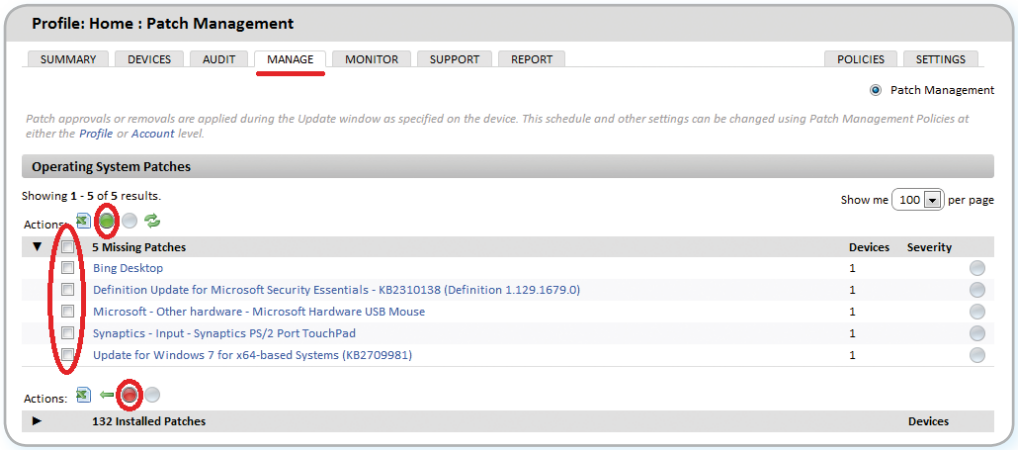
Software, License and Hardware Inventory

In the Audit tab you inventoried all the details of the devices belonging to the Profile or, if accessed from a device, it will show the information about the device in more detail.

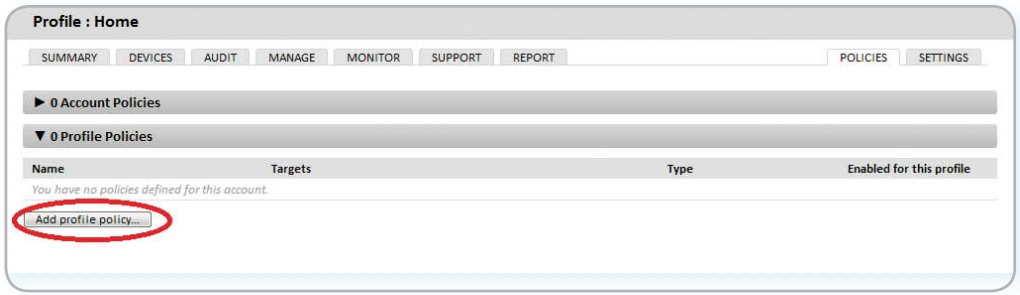


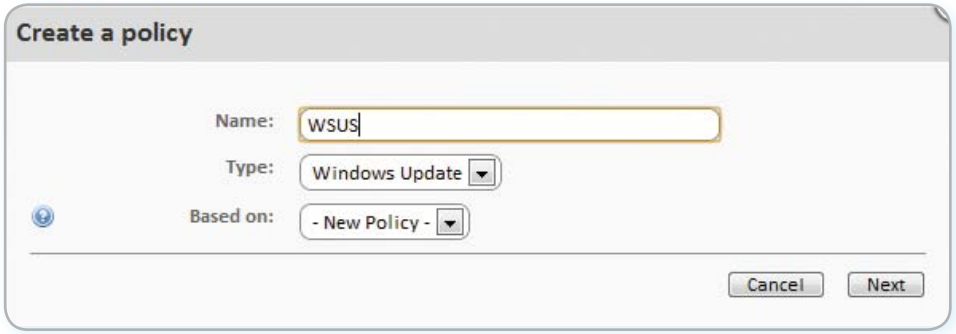
Patch Management

Approve patches that have not been installed on managed devices or run a rollback of those you want to uninstall in the **Manage Tab.**



Configure when to apply patches, steps to be taken after the application, and other parameters creating a Windows Update Policy from the Policies Tab in the Profile (explained later).

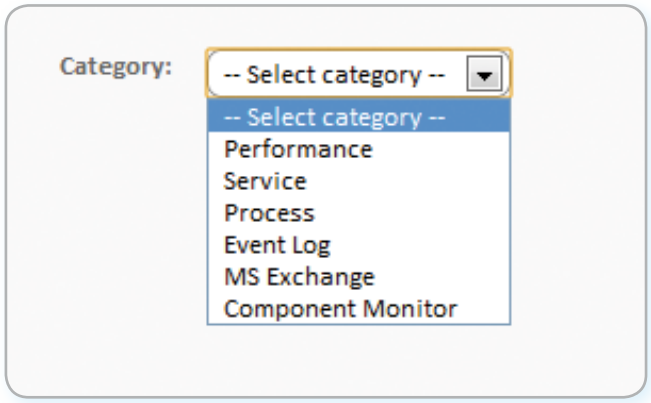




Monitor creation and configuration

Click a Device selected from those available in the Profile and use the Monitor tab to register a new Monitor, by selecting Monitors on the right.

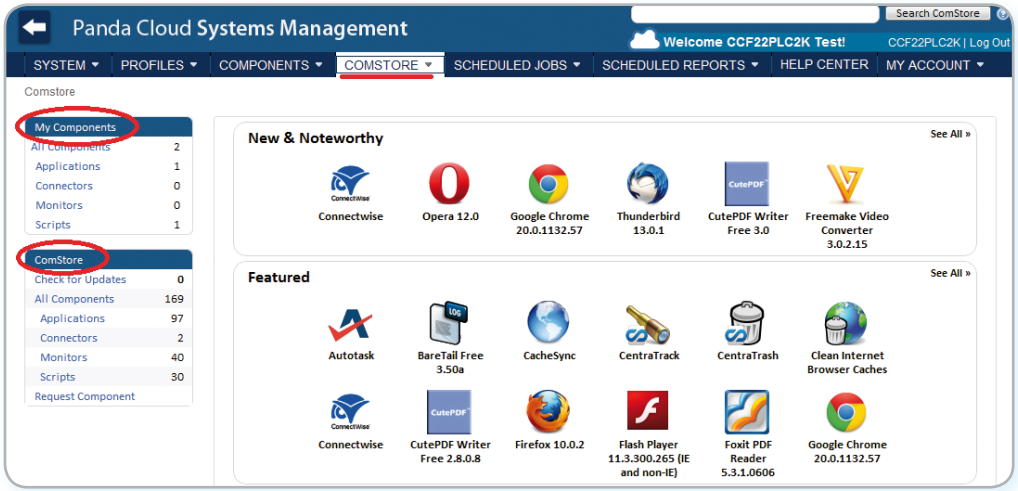
Choose the appropriate monitor type from those available.



Configure the parameters of the Monitor.

ComStore

Extends the functionality of **PCSM** and installs third-party software as published components, from this tab.



The components used directly by the Partner / IT Manager must be downloaded from the Comstore.

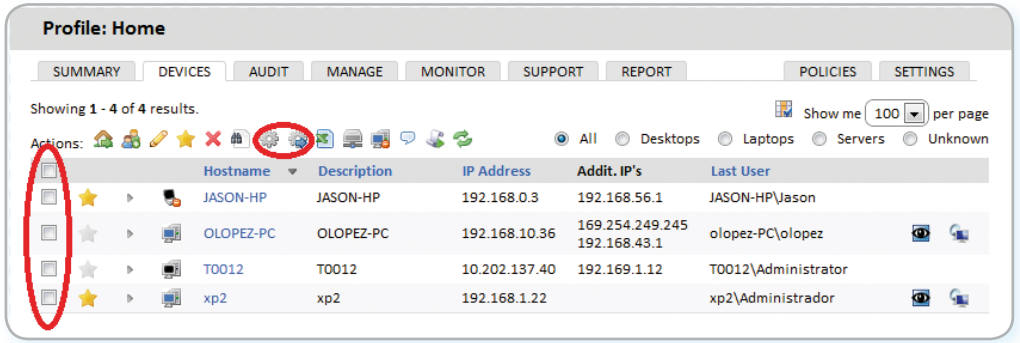
Under "My Components" shows the components already downloaded and available for use.

Under "ComStore" components are available for download.

In order to download a component, select one, and click "Buy". At that time it will populate under the **My Components** section. All components are free from the ComStore.

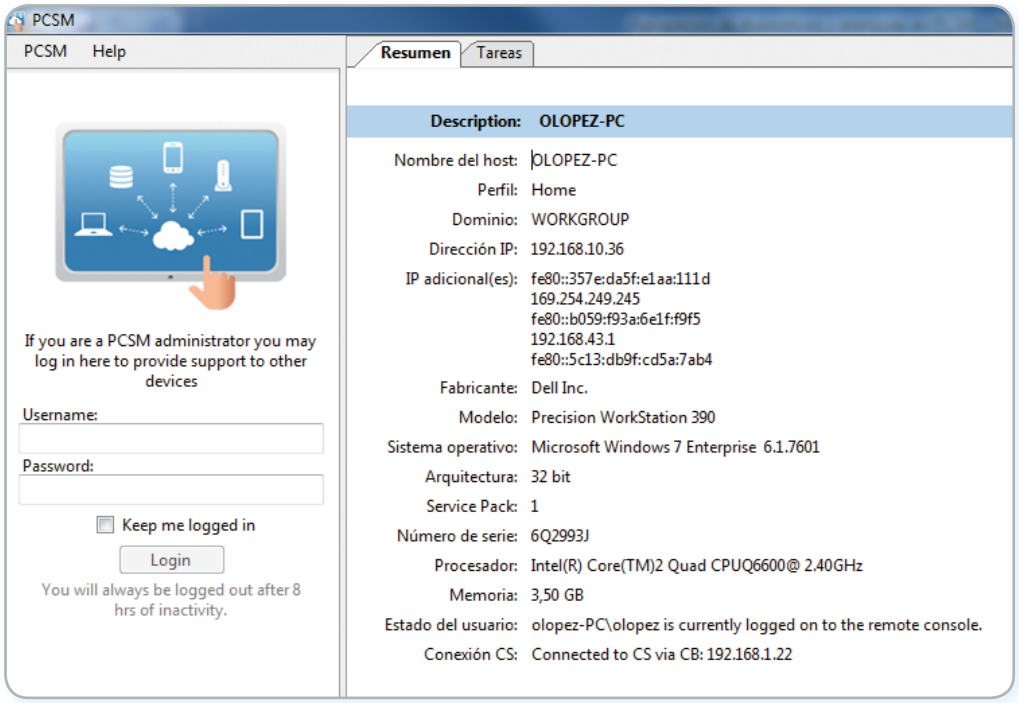
Depending on the type of component, it can be run as a task or in response to an alert generated by a monitor.

Under the Device tab within the Profile you can select the devices, apply a component and configure a schedule (Schedule a job) or run the component immediately (Run a quick Job).

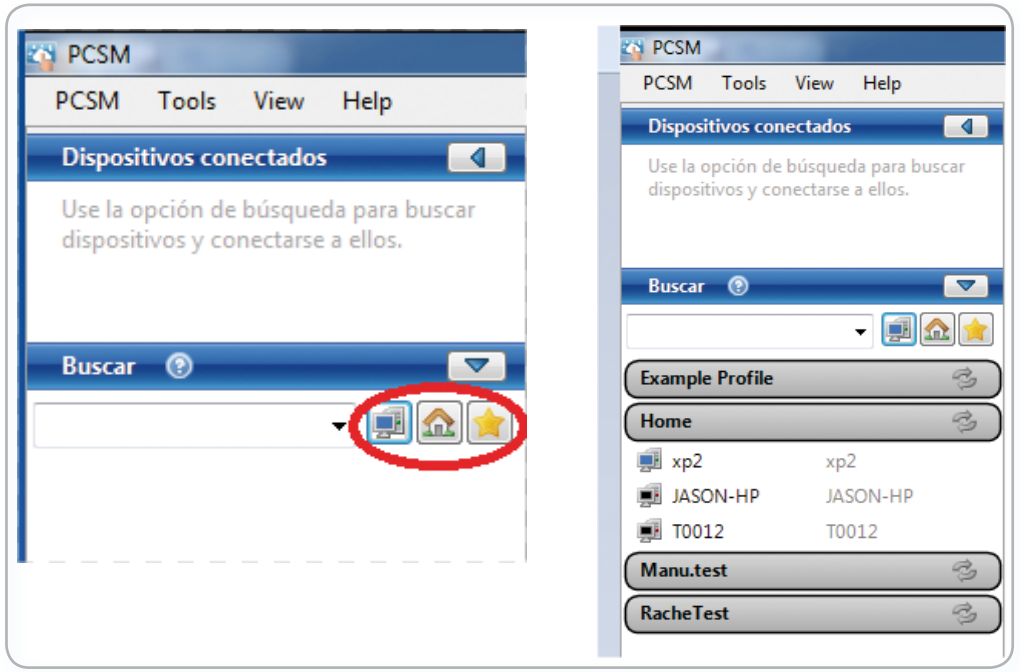


Remote Managed Devices and Resource Access

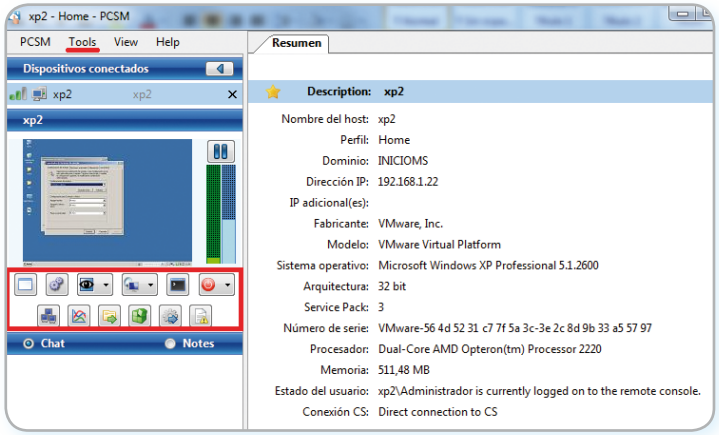
Although many daily operations can be performed directly from the console, it may be necessary to directly access the device using the Remote Support from the Agent. This requires the installation of the Agent on the Device so the Technician can perform remote support and login with their username and password.



Once logged in, locate the Device by name within the Profiles the Technician has access to, or through the Devices they have designated as favorites.



Once they have located and selected the Device, all of the options for remote access and control shall be accessible through both icons and menus.



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

- **Remote Screen Capture:** Takes a screen shot and displays it within the Agent.
- **Windows Services Tab:** Remote access to stop and resume services.
- **Screen Sharing Session:** Remote Desktop Sharing. The user sees what the technician is doing on their Device.
- **Command Shell:** Remote access to the DOS command line shell.
- **Agent Deployment:** Launch the deployment of the Agent.
- **Task Manager:** Remote access to Task Manager.
- **File Transfer:** Send and receive files.
- **Registry:** Remote access to Regedit tool.
- **Quick Jobs:** Launch jobs.
- **Event Viewer:** Remote access to the event viewer.

The options that will impede the user's ability to use their device are:

- **Windows RDP:** Remote Desktop Access which will close the user's session.
- **Shut Down / Reboot:** shut down or restart the target device.

8. POLICIES

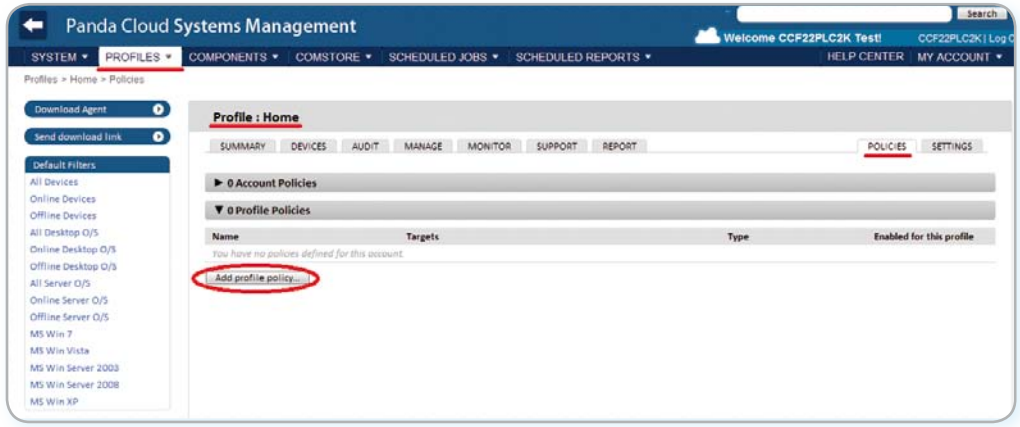
What are Policies

Policies are common configurations of System and Profile level groups or Custom Filters. In this case, a Policy created at the System Level (Account Policy) requests what Group / Filter applies from the System Level, whereas if the Policy was created at the Profile Level (Profile Policy) you would choose between the Groups / Filters available at the Profile Level.

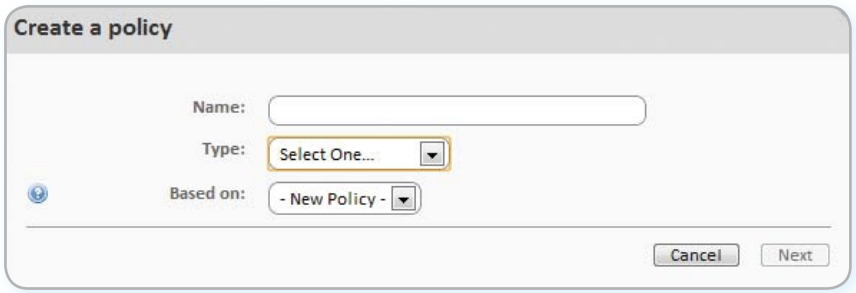
Creating Policies cannot be performed at the device level. At this level we can only see the legacy Policies defined at higher levels and affecting that device.

How to define a Profile Policy

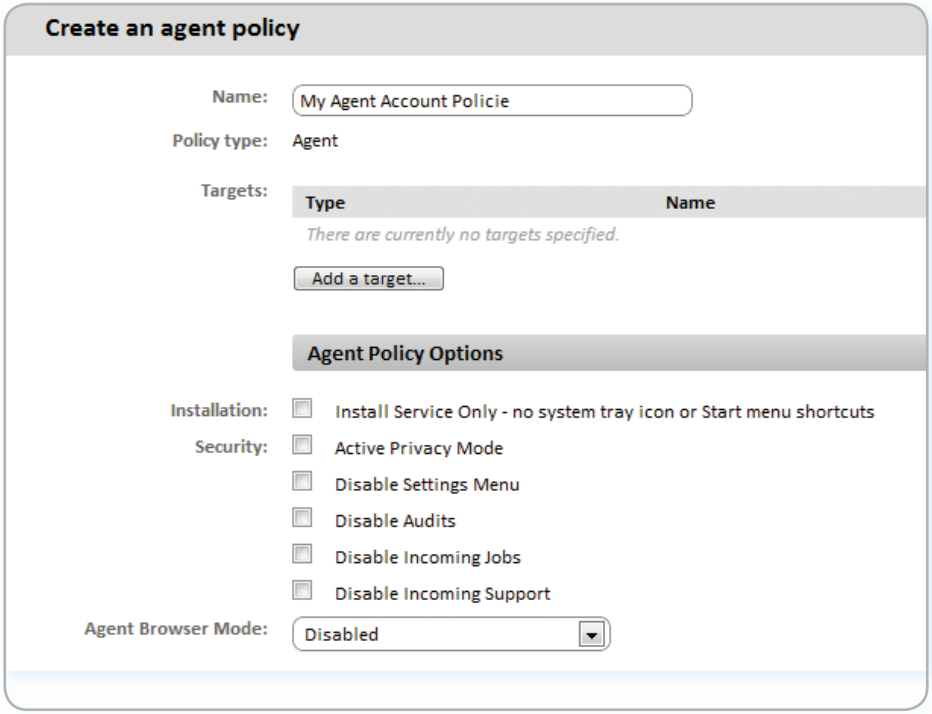
From the Profiles tab, select a specific profile then click on policies on the right followed by "Add profile policy" within the window.



It will show a window indicating the name of the Policy, and if the type is based on one created earlier to expedite the configuration.



The data requested in the next screen changes depending on the type of Policy you have chosen.

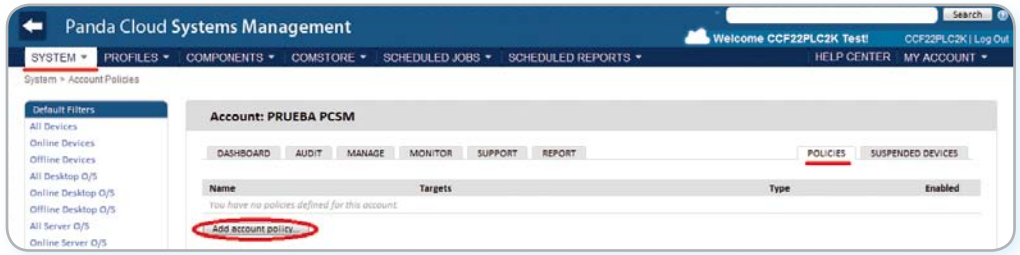


Here we have created an Agent Policy so "Agent Policy Options" will affect the configuration of the Agent on the devices.

All types of Policies will require configuration of the Target defined as a Group or Filter. As this is a Policy created at the Profile level it will only show the Groups or Filters previously created.

How to define an Account Policy

From the System Menu click on the tab labeled "Policies".



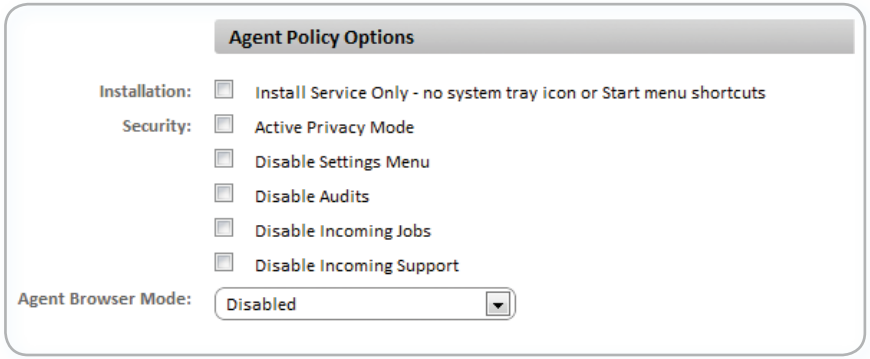
The remaining steps are identical to the creation of a Profile Policy.

Tips for Policies

The following are the 5 different types of Policies.

- **Agent**

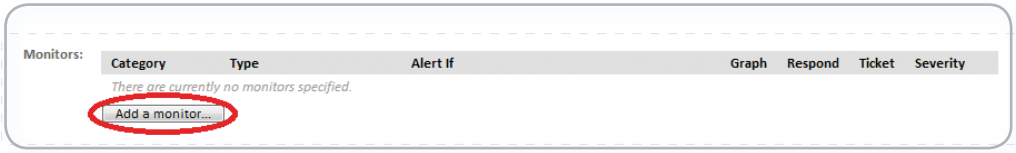
This type of Policy determines the appearance and interaction of the agent installed for both the user and the console.



- **Install Service Only:** This option hides the icon from the tray so the user cannot access the configuration windows.
- **Active Privacy Mode:** Remote connection to the desktop of the user device requires explicit acceptance by the user.
- **Disable Settings:** The user cannot access the context menu of the Agent.
- **Disable Audits:** The selected Devices will not send Audit, or hardware/soft ware data.
- **Disable Incoming Jobs:** Prevents sending jobs to the Agent.
- **Disable Incoming Support:** Disables access to the Agent by the Adminis trator.
- **Agent Browser Mode:** The Agent has three modes of operation.
  - **Disabled**
  - **User:** The Agent window will display but prevents access thout authentication.

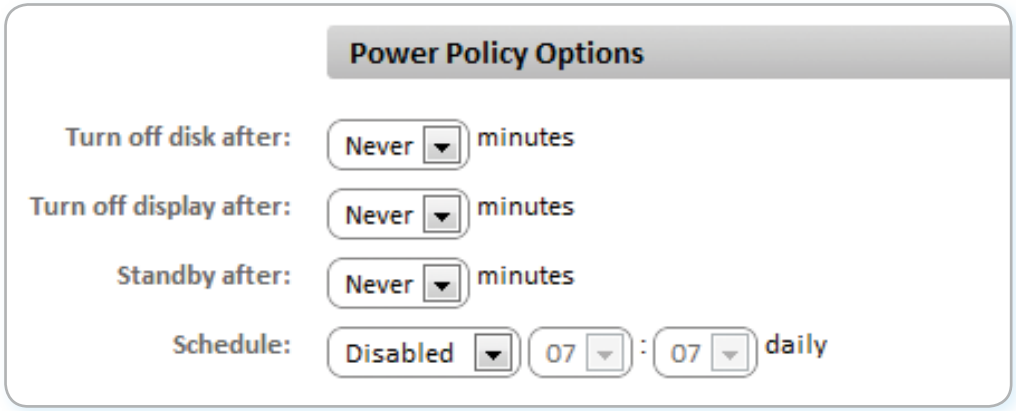
- **Administrator:** Complete access is given with the correct au thentication credentials.

- **Monitoring**



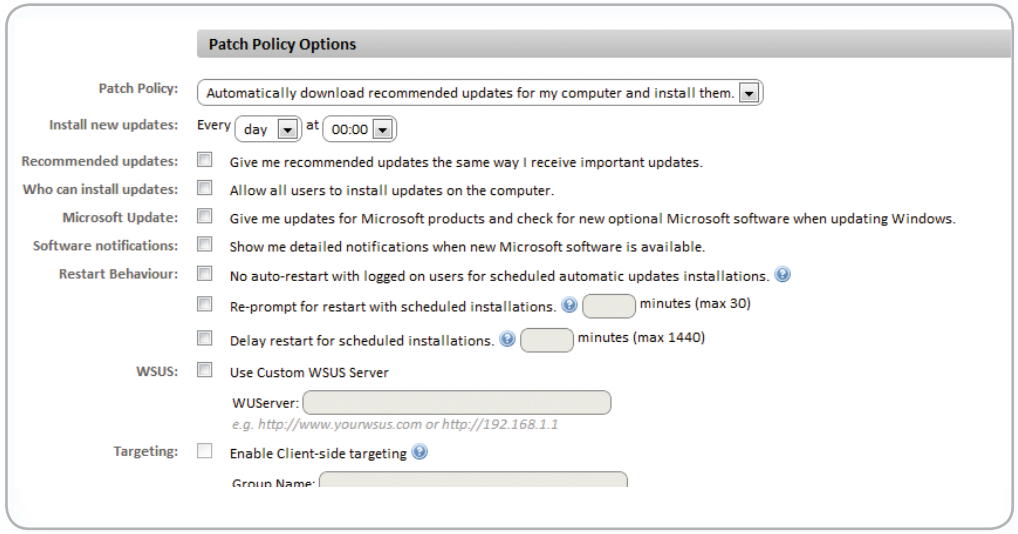
This allows you to add a Monitor Policy. Monitors will be explained in a later chapter

- **Power**



This Policy can configure the power saving settings of the devices that support them.

- **Windows Update**



This Policy is a transposition of the options available in a WSUS server and to configure the most common options for Patch Management for Microsoft systems.

PANDA SECURITY | *The Cloud Security Company*

www.pandasecurity.com