Panda Systems Management

Release Notes

Table of Contents

1. February 12nd, 2023. 11.3 version (Systems Management Agent v2169, Console v11.3.0.40)

1.1. Added (summary):

The 11.3 release is a new version including important improvements in the remote web, many new components for the most common tasks added in the COMSTORE, updates, fixes and much more.

The main changes added in the release are:

- **New filters added** for the new Windows Operating systems
- The **winvnc.exe binary** located in the Agent installation directory was **updated** to the latest and most secure version of 1.3.8.1.
- **Improvements on macOS agent notifications**, providing a more seamless end-user experience when conducting remote takeover or Web Remote chat sessions. End users on macOS endpoints will now receive prompts for Web Remote chat sessions to have better awareness about incoming chat requests
- **Web Remote chat**.
    - **Web Remote chat** is built from the ground up to provide a seamless experience for technicians to provide effective support.
    - **Support to multiple technicians** joining a chat session at the same time. This improves collaboration when troubleshooting complex issues.
- **Web Remote clipboard sync management**. When working across one or multiple machines, it helps to avoid accidentally copy and paste information to your clients' machines via the clipboard adding more control over how information is shared between clipboards.
- **Web Remote PowerShell.** When launching Web Remote, you can choose to begin a PowerShell session allowing to work without disturbing end users. Issues can be solved from the command line without requiring a screen share session.
- **Tens of new monitors for the most common applications, pre-prepared scripts and other utilities included in the COMSTORE** to make easy the automation of the most common tasks.
- **Fixes** in all the product areas.

Also, in this version, there is a **discontinuation of support for Windows Vista and Windows Server 2008:**

- Systems Management agents will stop functioning on endpoints that cannot run .NET6 (previously known as .NET Core). As such, Windows Vista and Windows Server 2008 will no longer be supported. (Windows Server 2008 R2 will be supported.)

And **TLS 1.0 and TLS 1.1 are deprecated** to improve security. The Systems Management platform will stop allowing communication using the deprecated TLS 1.0 and TLS 1.1 protocols. This change will prevent agents that still rely on .NET 4.0 from communicating with the platform.

1.2. Added (detail):

Agent

The Agent will now attempt to repair the Windows WMI repository and re-run an audit if it detects a failure during a full audit or delta audit.

Discontinuation of support for Windows Vista and Windows Server 2008:

- Systems Management agents will stop functioning on endpoints that cannot run .NET6 (previously known as .NET Core). As such, Windows Vista and Windows Server 2008 will no longer be supported. (Windows Server 2008 R2 will be supported.)
- Agents with unsupported requirements (Windows Vista and Windows Server 2008) might still function but won’t be able to receive feature and security updates.
- Other Windows operating systems might need to get the correct update installed to ensure continued operation.

TLS 1.0 and TLS 1.1 deprecation

To improve security, the Systems Management platform will stop allowing communication using the deprecated TLS 1.0 and TLS 1.1 protocols. This change will prevent agents that still rely on .NET 4.0 from communicating with the platform. Impact:

- Devices supporting TLS 1.2, such as Windows 6.1 and newer Windows environments that have .NET Framework 4.0 installed, will continue to be supported. This includes Windows 7, Server 2008 R2, and newer.
- Devices that are configured to communicate using versions of TLS below 1.2, such as those operating on Windows NT 6.0 or older, are no longer supported. This encompasses the Windows Vista and Server 2008 family of operating systems.
- Other devices such as those running Linux or macOS may require configuration changes, updates, or upgrades in order to communicate using TLS 1.2 if they are no longer connecting to the Systems Management platform.

How can I identify the devices not supported?

Windows devices that are no longer supported can be identified using the following filter: Operating system contains 5.0 OR 5.1 OR 5.2 OR 6.0.

Also, the local component cache has been deprecated:

- As part of our continued commitment to security, we are constantly reviewing the technologies leveraged by Systems Management to determine their suitability for the modern cyber security landscape.
- An analysis of agent methods used to peer share components across a local network for bandwidth efficiency reasons found them to be suboptimal in this regard. For this reason, we made the decision to remove the local cache functionality from the Systems Management Agent with this release.

Web Console

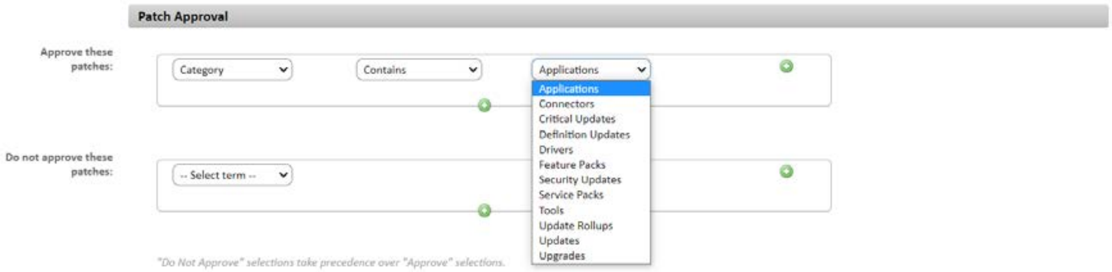
New filters added for the new Windows Operating systems:

- Filter for Windows 11. You can now access a Default Device Filter for devices running the Windows 11 operating system.
- Filter for Windows Server 2022. You can now access a Default Device Filter for devices running the Windows Server 2022 operating system.

We removed the Performance graphs from Device Summary page. These graphs will be replaced by the Long-Term Metrics in the next version with the New UI.

Patch Management

Patch Management policy support for Upgrades category. Patch Management policies can now target annual Windows Feature Updates specifically for inclusion or exclusion using the Upgrades category criteria under Approval.



Patch Approval

Approve these patches: Category | Contains | Applications

Do not approve these patches: -- Select term --

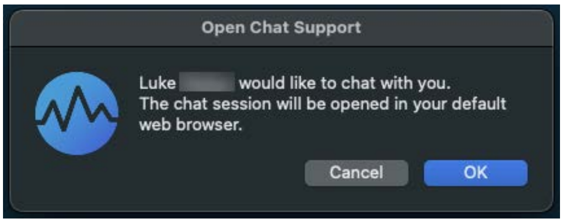
"Do Not Approve" selections take precedence over "Approve" selections.

Remote support

The winvnc.exe binary located in the Agent installation directory was updated to the latest and most secure version of 1.3.8.1.

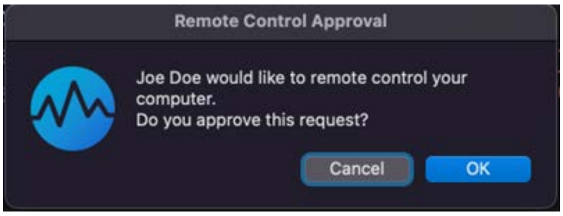
We have made improvements on macOS Agent notifications, providing a more seamless end-user experience when conducting remote takeover or Web Remote chat sessions. The improvements include the following:

- End users on macOS endpoints will now receive prompts for Web Remote chat sessions to have better awareness about incoming chat requests.
- Both the chat session prompt and privacy prompts now respect Agent branding on macOS.



Open Chat Support

Luke [redacted] would like to chat with you.
The chat session will be opened in your default web browser.



Remote Control Approval

Joe Doe would like to remote control your computer.
Do you approve this request?

Remote web chat

We're excited to announce the first iteration of **Web Remote chat**. Web Remote chat is built from the ground up to provide a seamless experience for technicians to provide effective support. Web Remote chat features include the following:

- A fast and responsive chat experience, right in your browser. As with the Web Remote control screen experience, you can initiate Web Remote chat from any modern web browser.
- Built-in flexibility to suit your workflows. Not every incident requires a full remote takeover session right away, so we've ensured you can initiate chat standalone, with an option to control the screen during the session. Chat is also available for use when using standard control screen functionality within Web Remote.

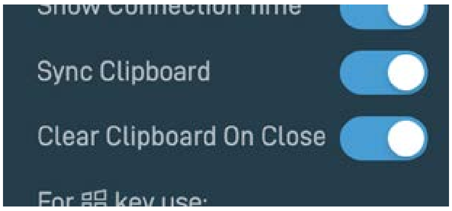
Web Remote chat now supports multiple technicians joining a chat session at the same time. This provides a number of benefits including the following:

- Improved collaboration when troubleshooting complex issues. For those more complex issues to troubleshoot, being able to have multiple technicians join the same chat with the same end user - as with the standard Web Remote Control Screen experience - helps improve collaboration and resolve incidents more effectively.
- Seamless handover between technicians. Multi-tech support also provides a seamless user experience for the end user when another technician takes over working with them on a support incident; for example, when escalating an issue to be worked on by a more experienced member of the team.

Web Remote clipboard sync management

When working across one or multiple machines, it can often be all too easy to accidentally copy and paste information to your clients' machines via the clipboard. As a result, some partners may desire more control over how information is shared between clipboards. To support this, we have made a number of improvements and changes to how clipboard synchronization works in Web Remote.

- **Sync Clipboard**. Enabled by default, this new option allows technicians to control whether the keyboard should automatically synchronize or not between the host and guest devices of a Web Remote session. This option allows technicians to decide whether to synchronize potentially sensitive data when connecting to client devices.
- **Clear Clipboard On Close**. Enabled by default, this new option allows technicians to ensure that the clipboard is cleared after disconnecting from a device.
- Web Remote now prevents propagation to both Microsoft's Cloud Clipboard and the local Clipboard History. Any material synchronized to a target endpoint's clipboard will not be replicated to other devices the target user owns, bypassing Microsoft's Cloud Clipboard feature. The clipboard is also not preserved by the target's local Clipboard History. This change to prevent propagation into clipboard history cannot be disabled by technicians nor Administrators.

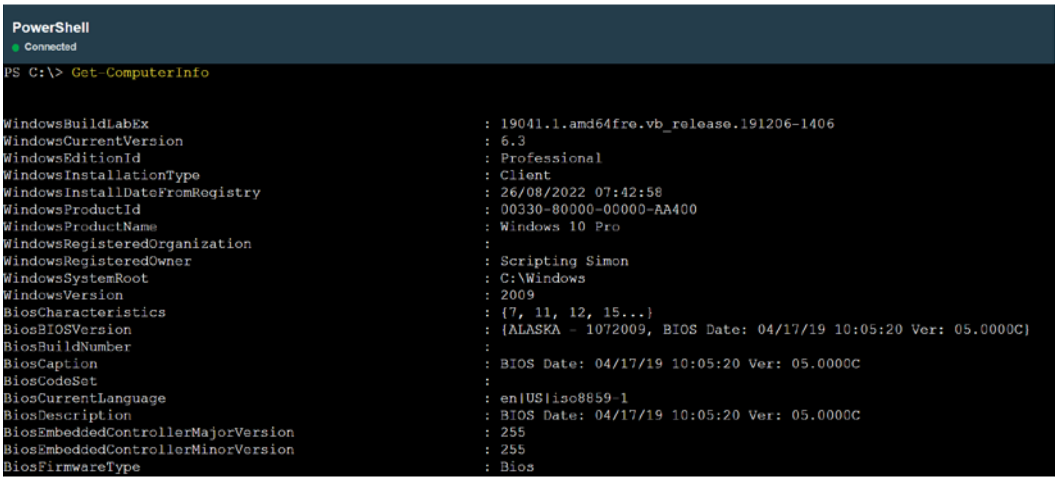


Show Connection Time ●
Sync Clipboard ●
Clear Clipboard On Close ●
For ⌘ key use:

Web Remote PowerShell

When launching Web Remote, you can now choose to begin a PowerShell session alongside the existing Chat and Control Screen options. The following features are available:

- Work without disturbing end users. Issues can be solved from the command line without requiring a screen share session.
- Run commands in private. Sensitive commands can be executed without end users viewing and potentially attempting to copy later.
- View real-time command output. Tail logs or view progress bars on long-running commands.



```
PS C:\> Get-ComputerInfo


WindowsBuildLabEx                                       : 19041.1.amd64fre.vb_release.191206-1406
WindowsCurrentVersion                                   : 6.3
WindowsEditionId                                        : Professional
WindowsInstallationType                                 : Client
WindowsInstallDateFromRegistry                          : 26/08/2022 07:42:58
WindowsProductId                                        : 00330-80000-00000-AA400
WindowsProductName                                      : Windows 10 Pro
WindowsRegisteredOrganization                           :
WindowsRegisteredOwner                                  : Scripting Simon
WindowsSystemRoot                                       : C:\Windows
WindowsVersion                                          : 2009
BiosCharacteristics                                     : {7, 11, 12, 15...}
BiosBIOSVersion                                         : {ALASKA - 1072009, BIOS Date: 04/17/19 10:05:20 Ver: 05.0000C}
BiosBuildNumber                                         :
BiosCaption                                             : BIOS Date: 04/17/19 10:05:20 Ver: 05.0000C
BiosCodeSet                                             :
BiosCurrentLanguage                                     : en|US|iso8859-1
BiosDescription                                         : BIOS Date: 04/17/19 10:05:20 Ver: 05.0000C
BiosEmbeddedControllerMajorVersion                      : 255
BiosEmbeddedControllerMinorVersion                      : 255
BiosFirmwareType                                        : Bios
```

Web Remote **PowerShell session requirements**:

- You must have PowerShell permissions enabled within Security Level Details - Remote Control Tools.
- The PowerShell session will run the version of PowerShell installed via C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe. Even if installed, pwsh will not be run.
- To retrieve the PowerShell version information, run the command get-host.

We now better support devices with Hybrid Graphic Systems, improved our chances of initial connection success if a pre-existing Web Remote module is already available, and use the Windows Toast Notifier to display Privacy Mode notifications on Windows 10/Server 2016 and newer.

COMSTORE

Tens of new monitors, pre-prepared scripts and other utilities included in the COMSTORE to make easy the automation of the most common tasks:

- **Clear all UDFs.** A handy tool for your Swiss Army Knife.
- **CPU Temperature Monitor v3.** Updated to use the latest build of LibreHardwareMonitor for improved CPU support.
- **Remote Wipe Windows**
- **Domain Controller Monitor v2**
- **Create URL Shortcut on Desktop**
- **Create New Administrative User**
- **Monitor OneDrive Sync Status**
- **Software monitoring for Windows**

- **Software monitoring for macOS**
- **Monitor Conditional Disk space**
- **Monitor and Generate WLAN Reports**
- **Monitor SSH Devices**
- **Windows 10: Upgrade via ISO**. The ISO for Windows 10 version 21H2 is now hosted on Systems Management servers. To push 22H2, use the Update/Upgrade to Latest Windows 10 Version component instead.
- **Windows 11 Upgrade via ISO.** Upgrade a system running Windows 10 build 2004 or higher to Windows 11 or update an existing Windows 11 installation.
- **SIP Monitor [MAC]:** Alert on the enablement of System Integrity Protection for your macOS devices.
- **FileVault 2 [MAC]:** Use to enable FileVault 2 on supported Macs and systems where the component has already been run once. Document the recovery key in a UDF.
- Monitor Battery Cell Health
- **ESXi VM Snapshot Monitor.** Uses a Windows-based device to alert if any VMs on an ESXi device have more than X snapshots. ESXi account credentials must be supplied via variables (read-only is sufficient).
- **Crash Monitor (macOS).** This component alerts if a new app crash (in either CRASH or IPS format) or a kernel panic (in PANIC format) is logged for macOS.
- **Microsoft Edge Update Monitor (Windows).** Windows keeps Edge up to date. This monitor allows users to see at a glance whether the update process is working properly.
- **Clear DNS Cache.** Clears the DNS cache and restarts mDNSResponder. Tested on macOS 11 and 12.
- **Reindex Spotlight.** Rebuilds Spotlight's indices for all drives. Tested on macOS 11 and 12.
- **HOSTS Integrity Monitor.** Alerts if the HOSTS file has been changed.
- **Remove Internet Explorer 11.** Removes Internet Explorer 11 from a Windows device in line with Microsoft's end-of-life advisory.
- **Logfile Monitors.** These new scripts for Windows and macOS will keep track of log files on local systems and alert when new lines appear containing phrases of note.
- **Install & Configure WinLogBeat**
- **Install & Configure NXLog**
- **Install & Configure SysMon**
- **Log4Shell Enumeration,** Mitigation and Attack Detection Tool. This component scans Windows devices for software containing Log4J and alerts if it or signs of an attempted attack leveraging it are discovered. Linux users can use the Fenrir Scan component.
- **Microsoft Office RCE (Follina) Workaround.** Use this CyberDrain Component to apply (or remove) a patch for the newly discovered Follina vulnerability in Microsoft Office. More information.
- **Potentially Unwanted Remote Support Software Scanner.** This monitor replaces dedicated monitors for Atera and Kaseya agents and adds support for TeamViewer and ConnectWise Control. Use it to ensure your devices have not had unauthorised RMM/RTO programs installed on them.
- **Microsoft Remote Desktop Client**
- **Uptime Monitor (Windows).** Post your devices' uptime counters in a UDF and optionally alert if devices have been online for too long a stretch. You can even configure a response component to reboot the device automatically.
- **Get/Set Default Browser (Windows).** Audit and select the default browser for the logged-in user.

- **Silent Knight (macOS).** Uses the command-line version of Silent Knight to perform a series of security checks on a macOS device.
- **PowerShell Version Audit (Windows)**. Discover at a glance what versions of Windows PowerShell your devices are running and which components they are compatible with.
- Azure Active Directory Audit
- **Install Updates with SUPER (macOS)**. A new solution using Kevin White's excellent SUPER has taken the place of the old Install Updates component. The ComStore component is a basic implementation, but the script can easily be copied and edited to add various setting options.

1.3. Issues fixed

Description
Some computers showing patch management policy result as "No data", and in those devices it is seen a patch audit error "HTTP error broken pipe"
Network node settings in italian shows a js error
Serial Number link you can click on in PCSM for Dell machines are redirecting to the wrong site and are therefore not showing the correct information about the machine
The agent is not detecting Panda as the local protection and shows windows defender instead
In "Hardware Lifecycle" report, It reports Windows 11 as unsupported
Customer is trying to get the temperatures of the hard drives on his Synology NAS using an SNMP monitor, but the monitor does not provide any data
Try to add an email address as "Additional Recipients" in the reports module. Include in the "local-part" of the address one of the characters "+", "%" or "&"
Avast Antivirus status showing as not running although the Antivirus is on and running
When using the same component more than once on the same job, the stdout comes from only one of the run times

Note: For further details, please contact support.

2. December 11st, 2021. 9.8 version (Systems Management Agent v2151, Console v9.8.0.36)

2.1. Added (summary):

The 9.8 release is a maintenance version including important fixes and some improvements as well. The main changes added in the release are:

- Interesting improvements added in the **remote Web:**
  - You can now access an option under **Preferences** to prevent mouse or keyboard input by the end user on the remote device
  - We have added an option to the **image quality selector** to dynamically adjust the display to offer best performance for the available bandwidth.

- **Microsoft Teams** for Windows, **Citrix Workspace** for Windows and macOS, and **Mozilla**

Thunderbird for Windows and macOS typically used in the remote work have been added in the **Software management** so it is software that it may be installed and updated automatically

- Due to a local privilege escalation issue reported with **VNC** we made the decision to not package VNC with PCSM by default. We offer our users the choice between RDP and Web Remote for users that prefer not to rely on VNC for remote takeover
- The **remote support** is now working in **macOS Monterey**
- A lof of additional fixes added

2.2. Added (detail):

Agent

The Agent Browser PowerShell tool now requires the launching device to have **PowerShell 5.1** or above installed. This is to leverage functionality not present in older versions to improve connection security.

We fixed an issue where incorrect process details such as the Service Name could be displayed.

We fixed an issue where filters could provide incorrect results when using the Additional IP address criterion.

Software management

We have added the following applications to Software Management:

- **Microsoft Teams** for Windows
- **Citrix Workspace** for Windows and macOS
- **Mozilla Thunderbird** for Windows and macOS

Patch Management

In this release we are deprecating two areas of functionality from the Patch Management policy: **patch cache** and **randomizing start time for patch installations**.

Remote support

Due to a local privilege escalation issue reported with VNC we made the decision to not package VNC with PCSM by default. We offer our users the choice between RDP and Web Remote for users that prefer not to rely on VNC for remote takeover.

There is a toggle in account settings which controls the downloading of VNC. Furthermore, there is a flag that can disable (or enable if required) VNC - at the account/site level.

For a device that does not have UltraVNC installed - If a user tries to force UltraVNC via WebRemote or click on VNC in the Agent Browser, we show a message to highlight that UltraVNC is disabled for that account.

Disabling UltraVNC will potentially have an impact in the remote web as Windows 7 and Server 2008 systems rely on UltraVNC to work and therefore will fail to invoke a Web Remote session. In these systems the alternative RDP/take over options is the Agent Browser - RDP

Remote web

You can now access an option under **Preferences** to prevent mouse or keyboard input by the end user on the remote device. This setting persists until the technician manually reverts it or the session ends.

Auto image quality selection. We have added an option to the image quality selector to dynamically adjust the display to offer best performance for the available bandwidth.

Reports

We fixed an issue where monitor alert messages were truncated in CSV reports.

3. April 11st, 2021. 9.2 version (Systems Management Server v461, Agent v2128, Console v9.2.0.32)

3.1. Added (summary):

The 9.2 release is the next major milestone in making Panda Systems Management the most powerful, scalable, and easiest to use RMM product in the market. The main improvements added in the release are:

- **Remote Web** so IT admins and partners will be able to open a remote session from any device with a web browser installed regardless the PCSM agent is installed or not FROM the device where you do the remote. The Web Remote will be multi-session aware, allowing technicians to support users on Windows Virtual Desktops and servers running Remote Desktop Services.
- **Zoom** and **Microsoft Office 365** typically used in the remote work have been added in the **Software management** so it is software that it may be installed and updated automatically
- **Improvements in the monitoring area (**VMware ESXi, SNMP monitors, etc)
- Full support to **macOS Big Sur,** including **ARM-based** devices **(M1 chip)**
- **New components** have been added to the **COMSTORE**
- **Fixes.** You can contact support if you need further details about the issues solved

3.2. Added (detail):

General

Account, site, and component variables now support up to 65534 characters.

Agent

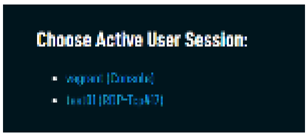
Full support to **macOS Big Sur,** including **ARM-based** devices **(M1 chip)**

Remote Support

New remote Web available so IT Admins and partners will be able to open a remote web session from any device with a web browser installed regardless the PCSM agent is installed or not FROM the device where you do the remote.

- The remote web will support **WebRTC** for fast peer-to-peer connections using Chrome and Firefox browsers.
- You will be able to **access Web Remote directly alongside the other tools available in the Agent Browser**
- Web Remote will be **multi-session aware**, allowing technicians to support users on Windows Virtual Desktops and servers running Remote Desktop Services. After initiating a Web Remote session on one of these devices, technicians can view a list of users who are logged into the device and then choose a user session from the Choose Active User Session page.

- Once a user session is selected, the Web Remote session with that user will be initiated. Only the selected user will see the pop-up notification that a session is being established.



Choose Active User Session:

- vagrant (Console)
- test01 (RDP-Tcp#7)

IMPORTANT :

- A Web Remote session can be initiated from any device (Windows, macOS, Linux, iOS, or Android) using the latest version of a Chrome, Firefox, Edge, or Safari browser.
- An Agent is not required.
- Only Windows and macOS devices with an agent installed can be controlled via a Web Remote session.
- In order for Web Remote to function properly on macOS devices running Mojave or later, these applications must be listed and checked under System Preferences > Security & Privacy > Privacy in the following sections:
  - Accessibility: PCSM Agent, Vine Server
  - Full Disk Access PCSM Agent, Vine Server

Further details about the Remote Web click here

We have made a number of enhancements to Web Remote to provide a superior technician experience. These include the following:

- Lock screen on disconnect. You can now select an option in the Preferences menu to lock the screen after disconnecting from the remote session.
- View-only mode. You can now select a view-only mode option in the Preferences menu to prevent keystrokes or mouse clicks passing through to the remote session.
- Blank desktop background. Web Remote now automatically blanks the desktop background during a session on Windows for improved performance, and it restores it on session disconnect.
- Branded connection popup. The notification displayed to inform an end user that a technician has connected now displays the custom branding desktop shortcut icon.
- Hybrid connection. Both WebRTC and WebSockets are now used in parallel with automatic failover to improve session reliability.

COMSTORE

New components have been added to the COMSTORE:

- A new component was added to the ComStore to **help with lost devices**. More information in this FAQ: Best practices for Lost Device security with Systems Management.
- We now **support installation of Windows 10 Enterprise Feature Updates** using the new Windows 10: Upgrade or update to latest Feature Release [WIN] ComStore component.
- We have released a new ComStore component, **Configure Windows Delivery Optimisation Settings**, which works with versions Windows 2004+.
- Also, the following components have been added to the ComStore:
  - Microsoft Teams
  - Zoom

Management

New Software typically used in the remote work has been added in the Software management so it is software that it may be installed and updated automatically

- **Zoom** has been added to Software Management to automate installation and updates on Windows devices.
- **Microsoft Office 365** has been added to Software Management to automate installation and updates on Windows devices.

Monitoring

Improvements in the monitoring area:

- VMware ESXi monitoring is now done by a different portion of the Agent and real-time monitoring metrics are now shown on the platform.
- SNMP monitors now have tabular OID support to raise independent alerts against multiple discovered SNMP table instances from a single monitor definition.
- SNMP monitors now support fetching live values during configuration when set at the device level for validation purposes.

Changes to monitor muting:

- IMPORTANT **The Mute Monitors for Devices action in the current UI will now disable the corresponding monitor at the device level.** All references to muting a monitor have been removed and muted alerts will no longer be available to view.
- Over 50% of alerts created in PCSM are muted and never viewed. This more than doubles the amount of resources required to process and store alerts, while offering no benefit to users. Due to this, we will be replacing monitor muting actions with disabling the monitor instead. Disabling a monitor can be performed from all places where muting a monitor was previously available, but the result is similar to disabling a monitor at the device level. The user requirement to stop receiving alerts from a monitor is still fulfilled.
- We have also introduced the automatic disabling of a monitor at the device level that raises over 10,000 alerts in a 24-hour period in both the current UI and the New UI.

System requirements for agents acting as network nodes. There is an important pre-requisite to support .Net Core on older systems. More details about requirements for the Systems Management agent here.

3.3. Issues fixed

Description
Error generated when trying to edit an active job after deleting the filter used to target devices
Special characters in audits (e.g. software names in software audit) may break audit xml generation
Update our Patch Audit to support Microsoft Windows 10 v20H1
Can not use option "ALL" for a large number of patches. - 504 error
Error received when selecting Account or Site policy from the drop down box - Account/Site > Manage > Account policy
MDM Policy Deploy can fail generating a LazyInitializationException
MacOS catalina devices shows free disk space as 0 bytes for all drives.
Custom device filter last reboot only shows years up to 2020. 2021 is not shown
When trying to get the available list of patches in a large numer of devices a 504 error message is shown
Error droping down the patch management policies menu in manage tab

Note: For further details, please contact support.

4. April 19th, 2020. 7.9 version (Systems Management Server v427, Agent v2100, Console v7.9.0.15)

4.1. Added (summary):

The 7.9 release is the next major milestone in making Panda Systems Management the most powerful, scalable, and easiest to use RMM product in the market. The main improvements added in the release are:

- **Improvements in the platform performance**. The scheduled jobs are giving a 503 error intermittently (some days in some specific hours). The new version includes architectural changes improving radically the platform performance.
- **Full support to macOS Catalina**. The new version works in Catalina without the need of any workaround.
- Significant performance enhancements to **offline device alerting**. Offline alerts are now seen almost immediately when a device goes offline.
- **Fixes**. Contact support if you have any doubt about some specific issue.

4.2. Added (detail):

General

Devices now support up to **30 User-Defined Fields (UDFs).**

Improvements in the platform performance. The new version includes architectural changes improving radically the platform performance.

Improved performance of the site listing page for a better log on experience for accounts with large numbers of devices.

Agent

Full support to macOS Catalina. The new version works when new installations are done in Catalina without the need of any workaround.

Deprecation of Connection Brokers. Part of streamlining Agent-to-platform communication for this release requires the deprecation of Connection Brokers. As functionality becomes increasingly reliant on the Agent Process rather than the Agent Service, Connection Brokers add a level of complexity that is no longer necessary.

Removed connection broker setup options from the Web Portal to deprecate this functionality.

PuTTY has been updated to 0.71.

Vine **VNC** has been updated to 5.2.1.

Remote Support

The request permission notification shown when attempting to connect to a device with privacy mode enabled **is now shown for three minutes** to allow more time for a user response.

Audit

Increased support for **antivirus vendors** as part of the default audit.

Antivirus Product	Windows	macOS
Avast Antivirus (from Windows 7 onward)	✓	
Avast Business Antivirus (from Windows Server 2012 onward)	✓	
Bitdefender Endpoint Security	✓	
ESET Endpoint Antivirus	✓	
Kaspersky Endpoint Security	✓	✓
Kaspersky Security for Windows Server (from Windows Server 2012 onward)	✓	
McAfee Endpoint Security	✓	
McAfee VirusScan Enterprise	✓	

Antivirus Product	Windows	macOS
Panda Endpoint Protection	✓	
Sophos Antivirus	✓	
Symantec Endpoint Protection	✓	
System Center Endpoint Protection (On Windows 7 and Windows Server 2012. On Windows Server 2016, it is detected as Windows Defender Antivirus.)	✓	
Trend Micro Worry-Free Business Security	✓	
Webroot SecureAnywhere	✓	✓
Windows Defender Antivirus (from Windows 8 onward)	✓	

Management

Improvements to patch scans better handle temporary issues and provide more useful troubleshooting information.

A patch scan is carried out on a device following an audit, however, **a patch scan is only triggered by the following events**:

- Patch management policy has run
- Initial full audit (right after Agent installation)
- Regular audit every 24 hours
- Manual audit (when a single device or multiple devices are selected)

Note that the following events do not trigger a patch scan:

- Quick jobs
- Scheduled jobs
- Alert response jobs
- User tasks

Updates to default **filter results for Hewlett Packard devices**. To return more complete results, a change was made to all related criteria to target manufacturers beginning with Hewlett OR HP, instead of the previous contains Hewlett OR Packard. Please be aware this change could impact existing jobs, policies, or reports using this filter for targeting purposes.

Reporting

Removed the Old Report Schedules export from the Reports > New Report > Export page.

Reports for deleted users are no longer scheduled.

A **new export** called **Site Device Count** has been created to show the total number of devices per site, grouped by device type.

Monitoring

We have changed how the Offline status for devices is determined, which results in **much faster offline alerting**.

Users can now change the IP address of a network device or an ESXi host from the Device Summary page.

4.3. Issues fixed

Description
Offline monitor alerts going off even when those devices are online
Machines send antivirus status alert when they power off
Inside the completed tasks tab the check to select them is not shown so they are not able to delete them or do anything with them
Android devices show offline even after auditing them
Linux /root/tmp fills up with tmp******** folders

Note: For further details, please contact support.

5. May 21st, 2019. 7.0 version (Systems Management Server v409, Agent v2074, Console v7.0.0.10)

5.1. Added (summary):

The 7.0 release is the next major milestone in making Panda Systems Management the most powerful, scalable, and easiest to use RMM product in the market. Among many other things, the release includes:

- **Software management**. This feature allows administrators to easily keep their endpoints updated with the latest versions of frameworks and applications, such as Adobe Flash or Oracle Java.
- **Powershell** is an extremely powerful command-line used by support engineers and system administrators to troubleshoot and configure Windows devices. With the new release, users can now connect to a full PowerShell interface on remote devices.
- **Reports** that are scheduled to run immediately can be downloaded from the platform so a user doesn’t have to wait for the email to arrive.
- Emails that would contain a **report** too large to process now have a link to the Web Portal so that you can download the report.
- **Notes** created in a **remote control** session now show up in the Device Activity report.
- The Antivirus audit now detects if the **Aether-based products** are updated or not.
- **Summary widgets** now link to corresponding devices for quick troubleshooting.

5.2. Added (detail):

General

A new Export to CSV option is available on the Users page to export a list of all users and their attributes in a single CSV file.

Administrators can now reset a user's 2FA status under Setup > Users to help them if they have lost their phones.

New customer accounts will now be loaded with a default Software Management policy so that devices will automatically report a status for managed applications.

A user is now automatically redirected to the login page after a session expires in the Web Portal.

The Site-level Antivirus Status and Patch Status widgets now link to the corresponding devices so users can better troubleshoot those devices.

When deleting users, Administrators now have the option to move the user's configuration data to another user in the system.

Much more user activity is being logged in the User Activity Log.

New accounts will get a default Audit-only Patch Management policy.

New accounts will get two default Monitoring policies.

The options "Mute Monitors for Account" and "Mute Monitors for Sites" have been removed from alerts.

When moving devices to a different site, you can now use a Search field to search for sites.

For new accounts, the Use Connection Brokers setting within the Setup > Account Settings > Custom Agent Settings section is now set to OFF by default.

Filters improvements:

- User are now able to view the criteria of all filters shared with them. Administrators are able to manage and delete any filter shared with them.
- Filters can now use “Equals” and “Does not equal” for all text fields.
- A new filter criterion for device Create Date has been created so that users can find devices that were recently added.
- A new filter criterion for Privacy Mode has been created.

Monitoring

The Event Log Monitor has been updated to better handle the event log level 0 messages on newer Microsoft operating systems so that they are correctly shown as Informational and not Critical.

When a user nominates an Agent as a Network Node, it no longer gets a Device-level Online Status Monitor assigned automatically.

Patch Monitor alerts now contain more detailed information about the patching issue.

Alert emails now use the Web Portal logo for their branding.

Installation of Windows patches not applicable to a device are now marked as a success rather than as a failure to prevent unnecessary alerts.

The alert notification email now has access to the AlertUID variable.

Alert emails no longer contain a section with social media icons.

Management

The Windows Update policy now has options to control Windows Active Hours, Update Channel, and Fast Startup.

"Next Run" has been renamed to "Schedule" on the Device-level Patch Management page.

Software Management

Software Management feature allows administrators to easily keep their endpoints updated with the latest security fixes. It has the following capabilities:

- Automatic, policy-based approach to 3rd-party software update management which keeps Windows and macOS endpoints updated with the latest versions of frameworks and applications, such as Adobe Flash or Oracle Java.
- Application update approval can be configured and applications can be installed on an endpoint if they are not already present.
- Built-in compliance reporting shows whether endpoints have the latest versions of critical applications and frameworks.

Application updates can be configured using a Software Management policy. There are two scheduling options to specify when updates should be installed:

Immediately on detection - An application update is installed as soon as the Agent detects that an update is ready.

On schedule - The Agent only checks for and installs software updates on a scheduled basis.

A new Software Management dashboard has been added to the Site and Account Manage tabs. The dashboard shows compliance across all managed devices. Software updates can also be approved from here.

At the Device level, the new Software Status field shows compliance directly from the Device Summary page. Refer to Status. From there, a link directs the user to the Software Management option under the Device Manage tab. Software updates can be approved here for that particular device.

Software Status is available in the column chooser on device list pages and as a filter criterion.

Software compliance reporting can be done using two altered reports:

- The Device Health Summary report has a new Software Status column showing if a device is considered compliant with Software Management.
- The Executive Summary report has a new section showing software compliance status for servers and workstations in the included sites. The Software Status impacts the overall health score in the report.

Software Management actions are also recorded in the device activity log.

PowerShell

PowerShell is an extremely powerful command-line used by support engineers and system administrators to troubleshoot and configure Windows devices.

With the Datto RMM 6.5.0 release, users can now connect to a full PowerShell interface on remote devices. A connection can be opened directly from the Web Portal or the Agent Browser (through the Command Shell icon). Multiple connections can be opened to the same endpoint, and multiple different PowerShell connections can be open at the same time.

The Powershell connection requires authentication much like an RDP connection. If the remote device has saved RDP credentials, those will be used for the PowerShell connection as well.

Reporting

Users are now able to target reports against Site Device Filters.

Notes created in a remote control session now show up in the Device Activity report.

Reports scheduled to run immediately can now again be downloaded directly from the Web Portal so that you don't have to wait for the email to arrive.

Emails that would contain a report too large to process now have a link to the Web Portal so that you can download the report.

The Device Storage report is now sorted in a more intuitive order.

The background image has been removed from all report cover pages.

A new Device Storage export has been added.

Audit

The Universal Antivirus audit now detects if the Aether-based products are updated or not.

Remote Support

RDP now works in configurations where a Windows GPO setting enforced that RDP should always prompt for a password upon connection. Users are now prompted for an additional password as per the policy.

A change was made so that on macOS Mojave, VNC is no longer in view-only mode and support techs can fully control macOS Mojave again. Vine Server (installed during the Agent install) now runs as user instead of root.

- ➔ This change results in support techs being disconnected from the session after user switching in the VNC session.

When using VNC to control a device, it is now possible to send CTRL-ALT-DEL, even when the Windows policy restricts this.

Jobs and components

PowerShell scripts run from scheduled or user-level jobs no longer require a Powershell execution policy override to work correctly.

A new type of job schedule is available: “On Audit”. This allows users to run jobs on new devices meeting a certain filter criteria as soon they come online so that initial system prep tasks can be run.

Device-level UDFs are now available in components as variables.

Users with sufficient rights are now able to change the Component Level of any component directly from the Components List, including those that were downloaded from the ComStore.

Agent

The Use Account Level Agent Deployment Credentials option under Sites > [site name] > Settings > Agent Deployment Credentials is now enabled by default so that newly created sites use the most common option and do not require additional configuration.

Support engineers can now use chat when supporting users that are on macOS. The support engineers can run the Agent Browser as normal.

The macOS Agent now has default Panda branding and will change based on macOS dark mode (this will not impact custom branding).

Implemented logic to validate the Agent GUID on the Agent to prevent issues for customers when they overwrite the Agent ID in the registry.

We now trigger messages in the log files when devices disconnect or go idle.

5.3. Issues fixed

Description
Notes for remote reports will be added again
Auto resolution of tickets doesn’t work (checkbox for function disable autoresolution of tickets not activated)
It is not possible to open windows event logs when connecting to a windows 10 device
Scheduled reports would go to completed as there was a problem in recalculating next run time
Reports that contain attachments bigger than 10mb are rejected by Amazon email service
Thailand language chat window is not correctly formated
PCSM antivirus audit does not detect if the aether-based products are signature "updated"
Right click menu for PCSM agent in macOS shows “Not found message”
Emails that should be sent by the PCSM ticketing system (ticket creation/modification) are not sent.
Network audit does not discover all devices in a /16 network. Fixed an issue where network discovery may not retrieve all devices in the network segment due to ARP cache limitations.

Note: For further details, please contact support.

6. November 21st, 2018. 6.1.0 version (Systems Management Server v398, Agent v2052, Console v6.1.0.1953)

6.1. Added (summary):

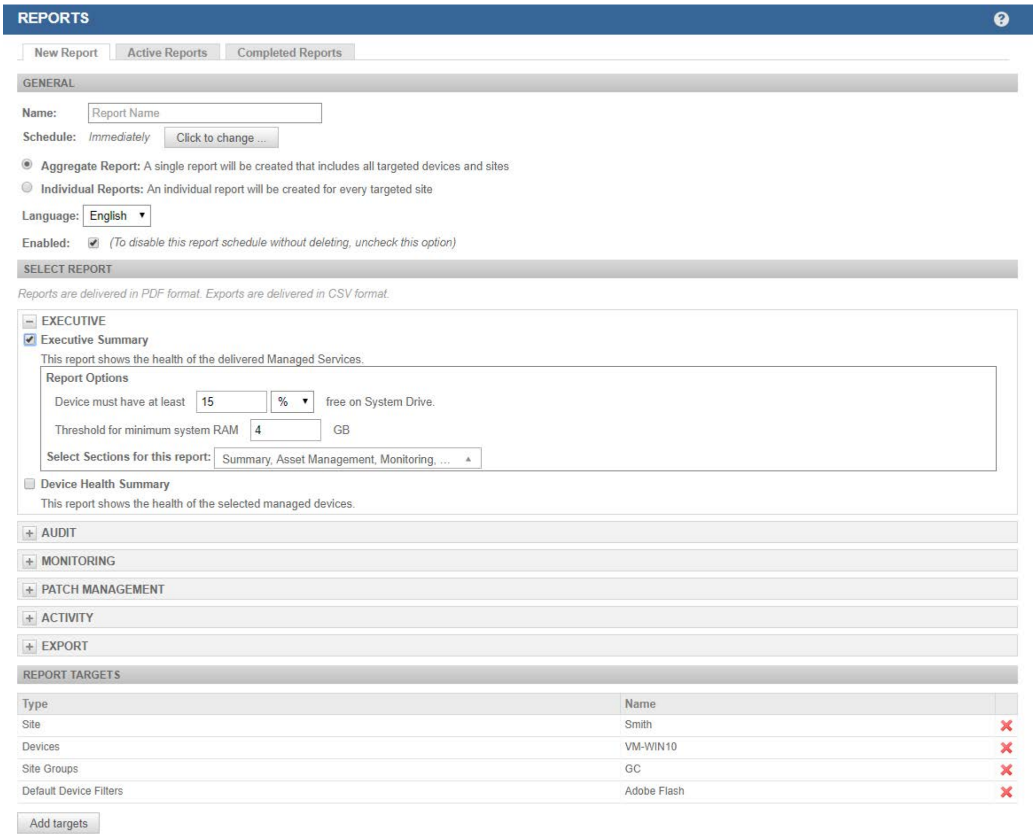
The 6.1.0 release is the next major milestone in making Panda Systems Management the most powerful, scalable, and easiest to use RMM product in the market. Among many other things, the release includes:

- A new, **flexible report scheduler and new reports** to help our customers show value and get accurate information from the system.
- A new **device patch status** system and improved **patch management dashboards** to be able to manage problematic devices with great efficiency.
- A **universal antivirus audit** feature so that customers can easily see if devices are protected, regardless of the antivirus product and operating system.
- An improved **Device Summary** and **Device Audit** page, and a flexible **job scheduler**.
- Support to **Mojave** (macOS)

6.2. Added (detail):

6.2.1. Reporting

The 6.1.0 release significantly improves reporting capabilities in **Panda Systems Management**. Major changes have been made in how reports are generated and how they look. A new, flexible report scheduler is introduced to help you get accurate information from the system, and the reports allow you to present data more elegantly than ever before.



Name: Report Name

Schedule: *Immediately*

● **Aggregate Report:** A single report will be created that includes all targeted devices and sites

○ **Individual Reports:** An individual report will be created for every targeted site

Language: English

Enabled: ☑ *(To disable this report schedule without deleting, uncheck this option)*

Reports are delivered in PDF format. Exports are delivered in CSV format.

☑ **Executive Summary**

This report shows the health of the delivered Managed Services.

Report Options

Device must have at least 15 % free on System Drive.

Threshold for minimum system RAM 4 GB

Select Sections for this report: Summary, Asset Management, Monitoring, ...

☐ **Device Health Summary**

This report shows the health of the selected managed devices.

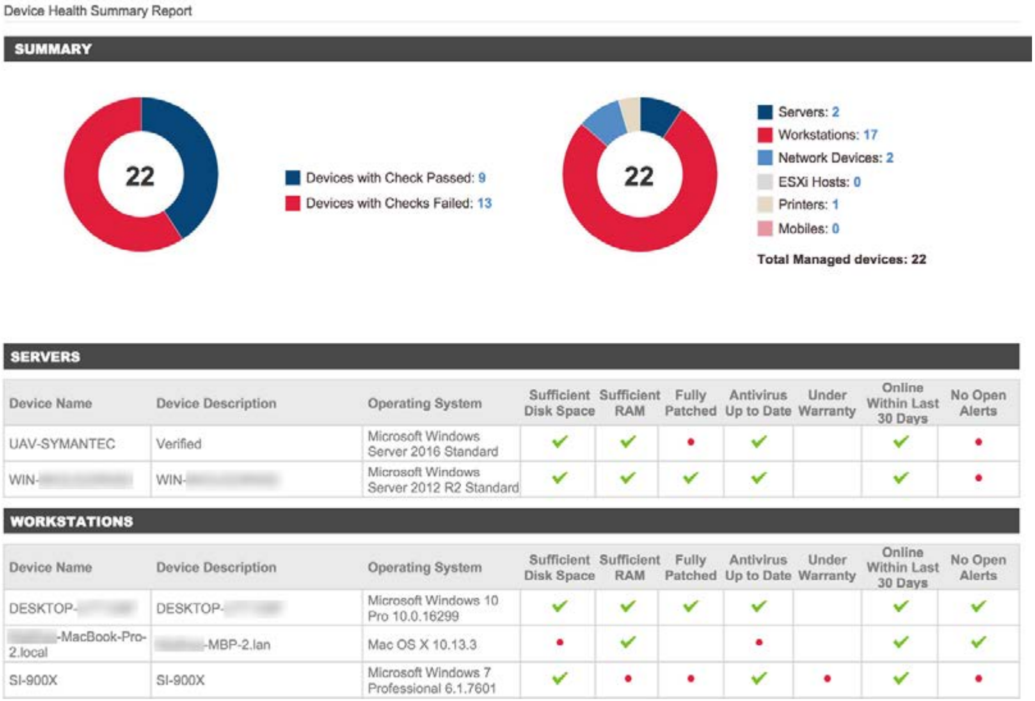
Type	Name	
Site	Smith	✖
Devices	VM-WIN10	✖
Site Groups	GC	✖
Default Device Filters	Adobe Flash	✖

The new report scheduler replaces all previous functionality.

- It is now possible to **schedule all reports and exports from one central hub, the Reports tab**. The report scheduler can also be accessed from device and site lists, and the Device Summary page.
- **Flexible target selection** is available. Any report can be run against a combination of devices, sites, filters, and groups.
- **Reports are multilingual**. You can set the language of the reports to English or German. Other languages will be available in the future.
- **Every report has its own set of criteria** that allow you to control what data is displayed in the report. Depending on the report, you can specify criteria, such as date range, columns, filters, and thresholds.
- **Exports are available in raw .CSV format** that you can use with third-party tools and applications.
- When multiple sites are included in the targets, you can use the **Aggregate Report** option to create a single report.

The 6.0.0 release completely overhauls and redesigns all PCSM reports, ensuring that each conforms to a specific design guideline. See two examples of the reports below.

- The **Device Health Summary Report** allows you to communicate the overall health of a device or network in a clear and simple way. It’s designed to help you articulate problem areas to your customers.



Device Health Summary Report

SUMMARY

■ Devices with Check Passed:	9
■ Devices with Checks Failed:	13

■ Servers:	2
■ Workstations:	17
■ Network Devices:	2
■ ESXi Hosts:	0
■ Printers:	1
■ Mobiles:	0

Total Managed devices: 22

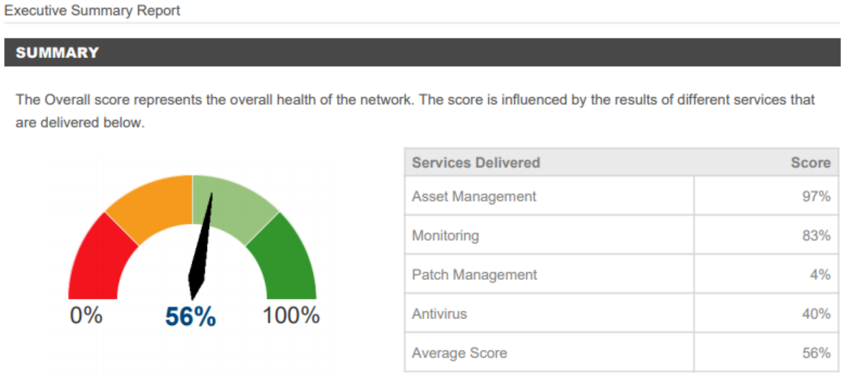
SERVERS

Device Name	Device Description	Operating System	Sufficient Disk Space	Sufficient RAM	Fully Patched	Antivirus Up to Date	Under Warranty	Online Within Last 30 Days	No Open Alerts
UAV-SYMANTEC	Verified	Microsoft Windows Server 2016 Standard	✓	✓	●	✓		✓	●
WIN-[redacted]	WIN-[redacted]	Microsoft Windows Server 2012 R2 Standard	✓	✓	✓	✓		✓	●

WORKSTATIONS

Device Name	Device Description	Operating System	Sufficient Disk Space	Sufficient RAM	Fully Patched	Antivirus Up to Date	Under Warranty	Online Within Last 30 Days	No Open Alerts
DESKTOP-[redacted]	DESKTOP-[redacted]	Microsoft Windows 10 Pro 10.0.16299	✓	✓	✓	✓		✓	✓
[redacted]-MacBook-Pro-2.local	[redacted]-MBP-2.lan	Mac OS X 10.13.3	●	✓		●		✓	✓
SI-900X	SI-900X	Microsoft Windows 7 Professional 6.1.7601	✓	●	●	✓	●	✓	●

- The **Executive Summary Report** provides information about the overall quality of your delivered managed services.



Executive Summary Report

SUMMARY

The Overall score represents the overall health of the network. The score is influenced by the results of different services that are delivered below.

Services Delivered	Score
Asset Management	97%
Monitoring	83%
Patch Management	4%
Antivirus	40%
Average Score	56%

Report schedule migration

The reporting changes impact all customers who have scheduled reports:

- All existing reports (at the Account, Site, and Device level) have been replaced by new reports. Therefore, all existing report schedules must be rescheduled when PCSM 6.0.0 is deployed.
- The Report History section of active and completed reports has been removed.
- Custom reports will no longer be available after PCSM 6.0.0.

A few notes on the report schedule migration process:

- When a schedule containing a legacy report is due to fire, the process will fail. Users will be notified via email at that time.
- A new export has been created detailing all legacy report schedules to ease the transition process.

6.2.2. Antivirus management

Universal antivirus audit

It’s vital for our customers that PCSM provides accurate information about their managed endpoints' antivirus status. The new universal antivirus audit creates a single source of truth allowing an endpoint to report the name and status of its antivirus product. The antivirus information is presented on the Device Summary page under the Status section. The data is also used on the Site Summary page, in reports, filters, and monitors.

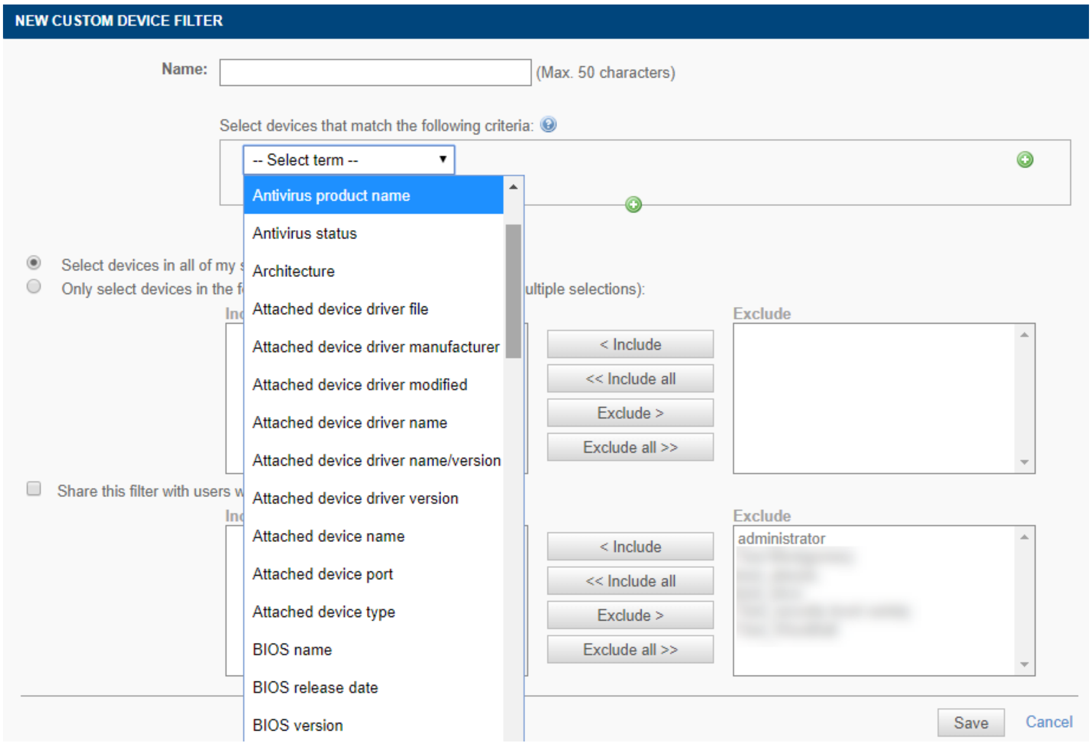
On Windows devices, the antivirus detection works out of the box for the most commonly used antivirus engines: Panda Security, Bitdefender, ESET, Kaspersky, McAfee, Sophos, Symantec, Trend Micro, and Webroot. When no antivirus engine is recognized on Windows Vista and above, the Agent will use the Windows Security Center information.

Antivirus Status Monitor

A new monitor called Antivirus Status Monitor has been added to replace the Security Center Monitor. This new monitor can alert when no antivirus product has been detected or it's not up to date or not running.

Antivirus filters and columns

You can choose the antivirus product and status columns from the column chooser in any device list. Additionally, new antivirus filters have been created to replace the filters based on Security Center information.



NEW CUSTOM DEVICE FILTER

Name: (Max. 50 characters)

Select devices that match the following criteria:

-- Select term --

Antivirus product name
Antivirus status
Architecture
Attached device driver file
Attached device driver manufacturer
Attached device driver modified
Attached device driver name
Attached device driver name/version
Attached device driver version
Attached device name
Attached device port
Attached device type
BIOS name
BIOS release date
BIOS version

● Select devices in all of my s

○ Only select devices in the f ultiple selections):

Inc Exclude

< Include
<< Include all
Exclude >
Exclude all >>

□ Share this filter with users w

Inc Exclude

< Include
<< Include all
Exclude >
Exclude all >>

administrator
[redacted]

Save Cancel

Removed functionality and migration

To make sure that all the data we present is accurate and the user experience is as straightforward as possible, we've removed or migrated certain parts that rely on data that we don't capture anymore.

- On the Site Summary page, the Security Status section, that relied on Kaspersky, Webroot, and Security Center Status information, has been removed. Refer to Site Summary.
- The Account Summary now redirects to the Account Dashboard. Refer to Account Dashboard.
- The Security Management Status filters and device icons (Kaspersky, Webroot) have been removed. Users can now use the new antivirus status filter. To minimize operational impact, existing filter definitions have been migrated using the following logic:

Existing Filter		Migrated Filter	
Anti-Virus		Antivirus Status	
Enabled	=	Running & Up-to-Date	
Disabled	=	Not Running	
Security Management Status		Antivirus Status	Reboot Required
Active Threats	=	Not Detected	
Installed & Active	=	Running & Up to Date	
Installed, not Active	=	Not Running	
Needs Update	=	Running & Not up to Date	
No valid license	=	Not Running	
Reboot Required	=		Yes

Users are advised to review existing antivirus-related filters to ensure the migration does not produce undesirable results upon release.

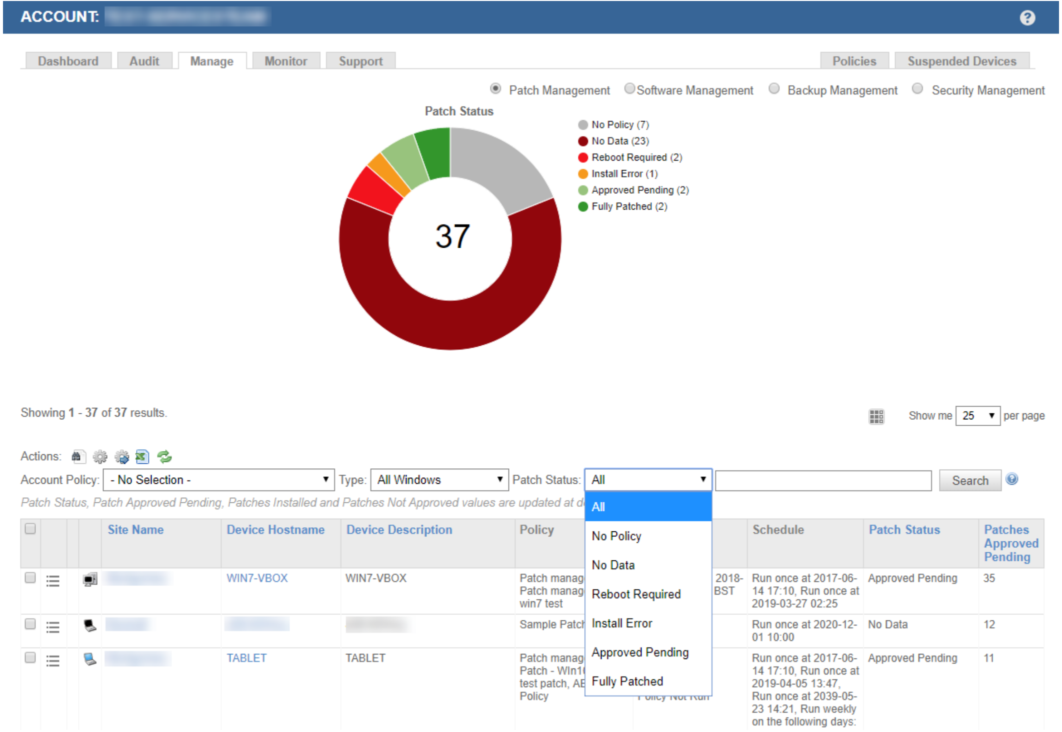
6.2.3. Patch Management

Device patch status

We are introducing new patch statuses for devices to improve the overall visibility and control of the patch process. Among others, a device's patch status will show if a device is fully patched, has approved pending patches, is waiting for a reboot, or if no patch policy has been applied.

Patch Management tab

The Account- and Site-level Patch Management tabs have been greatly improved. Using the new device patch statuses and other filters, users will find patching multiple devices to be much more straightforward.



ACCOUNT: [redacted]

● Patch Management ○ Software Management ○ Backup Management ○ Security Management

Patch Status

- No Policy (7)
- No Data (23)
- Reboot Required (2)
- Install Error (1)
- Approved Pending (2)
- Fully Patched (2)

Showing 1 - 37 of 37 results.

Show me 25 per page

Actions:

Account Policy: - No Selection - Type: All Windows Patch Status: All

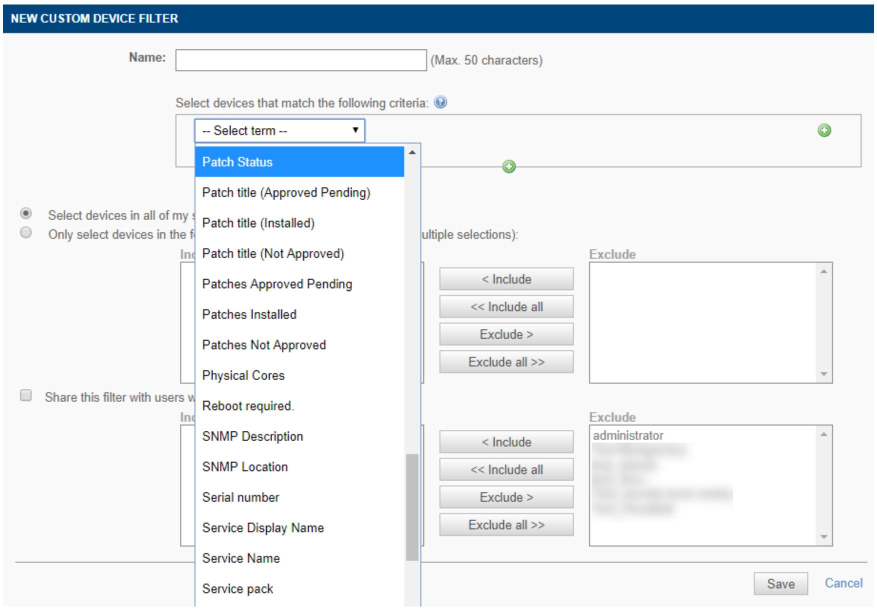
Patch Status, Patch Approved Pending, Patches Installed and Patches Not Approved values are updated at d

Site Name	Device Hostname	Device Description	Policy		Schedule	Patch Status	Patches Approved Pending
[redacted]	WIN7-VBOX	WIN7-VBOX	Patch manag Patch manag win7 test	2018- BST	Run once at 2017-06-14 17:10, Run once at 2019-03-27 02:25	Approved Pending	35
[redacted]	[redacted]	[redacted]	Sample Patch		Run once at 2020-12-01 10:00	No Data	12
[redacted]	TABLET	TABLET	Patch manag Patch - Win1 test patch, AE Policy	Policy Not Run	Run once at 2017-06-14 17:10, Run once at 2019-04-05 13:47, Run once at 2039-05-23 14:21, Run weekly on the following days:	Approved Pending	11

New filters and columns

The new patch statuses are available in device filters, device lists, reports, and CSV exports to allow users to quickly find devices that have issues or are not fully patched.

New filters have been added to find devices that are missing a specific patch or have many pending patches.



NEW CUSTOM DEVICE FILTER

Name: (Max. 50 characters)

Select devices that match the following criteria:

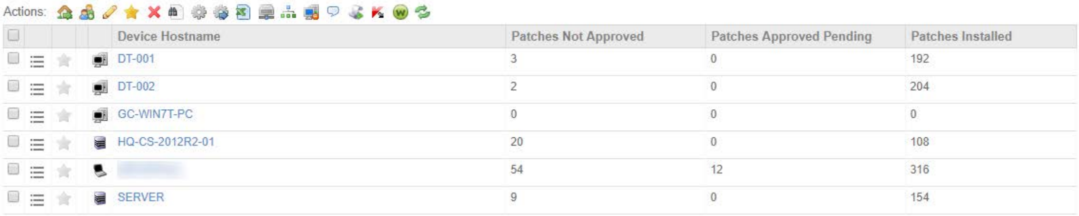
-- Select term --

● Select devices in all of my s

○ Only select devices in the f ultiple selections):

□ Share this filter with users w

New columns have been added to device lists to show how many patches are Not Approved, Approved Pending, and Installed.



Actions:

				Device Hostname	Patches Not Approved	Patches Approved Pending	Patches Installed
□	☰	☆		DT-001	3	0	192
□	☰	☆		DT-002	2	0	204
□	☰	☆		GC-WIN7T-PC	0	0	0
□	☰	☆		HQ-CS-2012R2-01	20	0	108
□	☰	☆		[redacted]	54	12	316
□	☰	☆		SERVER	9	0	154

Other patch management improvements

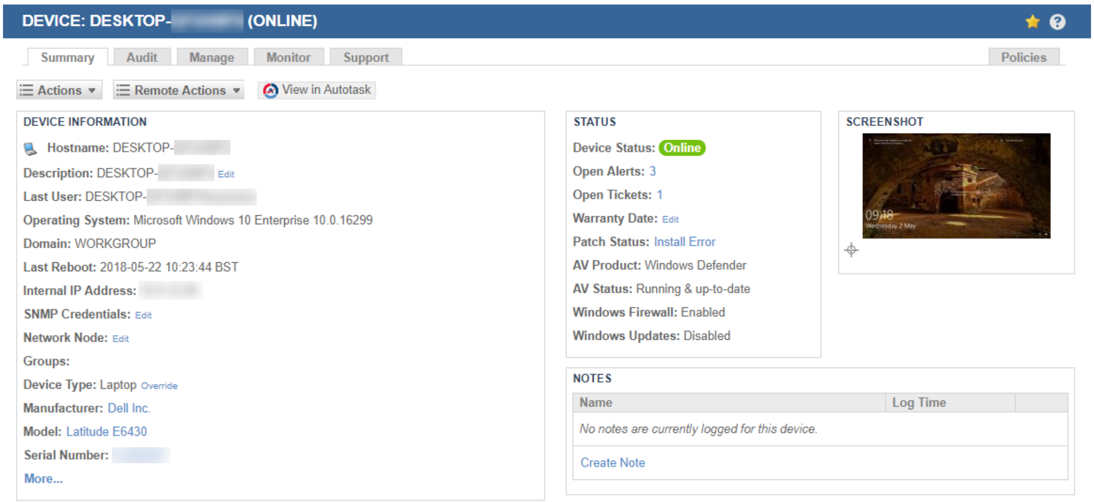
- Patches are installed in the best possible order. Security updates take preference and are installed before any other patch.
- When a device reports that a patch cannot be installed because it's been superseded or is not applicable to that device, it is no longer reported as a failure.
- Using a patch policy, you can now automatically approve or deny patches that are older than 7 or 14 days. Refer to Filter patches.
- The Device Activity shows when a patch policy started and ended. Refer to Device activity.
- When you click Run Now on a patch policy, offline devices will run it when they next come online.

6.2.4. Device Summary and Device Audit redesign

To help users find essential information about a device faster, we have redesigned both the Device Summary and the Device Audit page. Some data has been moved from the Summary page to the Audit page because it was rarely needed for troubleshooting purposes.

The new Status section on the Device Summary page quickly shows you if the device is online, has open alerts and tickets, and whether it's fully patched and properly protected. The Warranty Date field can be updated manually.

The Actions icons have been replaced by a new Actions menu on both the Device Summary and the Device Audit page.



DEVICE: DESKTOP-[redacted] (ONLINE)

DEVICE INFORMATION

Hostname: DESKTOP-[redacted]

Description: DESKTOP-[redacted] Edit

Last User: DESKTOP-[redacted]

Operating System: Microsoft Windows 10 Enterprise 10.0.16299

Domain: WORKGROUP

Last Reboot: 2018-05-22 10:23:44 BST

Internal IP Address: [redacted]

SNMP Credentials: Edit

Network Node: Edit

Groups:

Device Type: Laptop Override

Manufacturer: Dell Inc.

Model: Latitude E6430

Serial Number: [redacted]

More...

STATUS

Device Status: Online

Open Alerts: 3

Open Tickets: 1

Warranty Date: Edit

Patch Status: Install Error

AV Product: Windows Defender

AV Status: Running & up-to-date

Windows Firewall: Enabled

Windows Updates: Disabled

SCREENSHOT

NOTES

Name	Log Time
No notes are currently logged for this device.	
Create Note	

6.2.5. Jobs and components

Job scheduler

Just like the new report scheduler, the job scheduler allows for flexible target selection so that devices, sites, filters, and groups can quickly be added to a job. You can edit a job to add new targets without the need to create a new job from scratch.

You can also schedule jobs from your components list so that you don't have to navigate back to a device or site list after downloading a component from the ComStore.

If you use many components, you can now filter by component groups or use the search field when selecting components for a quick job or a scheduled job.

The Active and Completed Jobs pages have filters and a search field so that you can find a job by name or by a specific user who scheduled it.

New component variable: Selection

A new variable type has been introduced to be used in any component. The Selection variable type allows users to define a list with options and values that can be used within a component. As a result, power users will be able to write components that are easy to use by regular PCSM users because they only allow pre-defined answers rather than free text input.

6.2.6. Network control

The network control feature has been revamped. Network control allows users to remote control the web interface of any device, including devices without an Agent installed. This new version is based on a new proxy, making the connections much faster and more robust. It now also offers the much desired ability to remote control devices with an HTTPS interface.

6.2.7. Other enhancements and requirements

- Support to **Mojave** (macOS)
- Users can now open device pages directly from the Agent Browser.
- Users are able to search for alerts on the Monitor tabs.
- Users can search and filter for activities in the Device Activity log.
- Users can directly run and schedule jobs from the Site- and Account-level monitor tabs.
- As of PCSM 6.1.0, the network node device performing ESXi monitoring is required to have Microsoft .NET Framework version 4.5 or higher.

6.3. Issues fixed

Description
No server alert raised. Server down but no alert raised from monitor.
30 day health report shows 122% in uptime and too many minutes in downtime (non possible data)david
User software install report is empty
A user with a restricted security level is able to see an account level report
Change log report empty
Same report sent duplicated
Scheduled report not sent on 1st of each month
Report change log does not work

Note: For further details, please contact support.

7. February 13th, 2018. 5.5.0 version (Systems Management Server v4.6.351, Agent v2017, Console v5.5.0.1808)

7.1. Added (summary):

Main improvements added:

- Significant **improvements in the Discovery** to help customers better understand what devices are still unmanaged
- **Improvements in the monitoring capabilities**. We have a new foundation, added powerful new monitors, enhanced our existing monitors and added real-time monitoring graphs.
- **Many new capabilities for managing Network Devices**. We have improved our Discovery, we can now monitor the Network Devices using policies and we can even remote control these devices.
- **Best Practices Monitoring Policies** are now available in the COMSTORE (Monitoring Policies). These Policies include best practices for monitoring the most common platforms, common server roles like Exchange/DNS, hardware vendors like Dell/HP and Network Devices by vendors such as Cisco and SonicWall.
- Some **issues fixed**. See the Issues fixed section for further information

.NET 4.0 Framework required

The new Windows agent for PCSM is built upon the **.NET 4.0 Framework** and this means that all existing devices will have to have this version of .NET installed to be able to use the new agent, otherwise the agent won't be updated so the new features added in future releases won't work in devices without this version of .NET installed.

There is a filter available in order to identify the version of .Net in the customers' devices. Also there is a component available in the COMSTORE to update identified devices to the required version of the .NET Framework.

7.2. Added (detail):

7.2.1. Discovery

Network Discovery

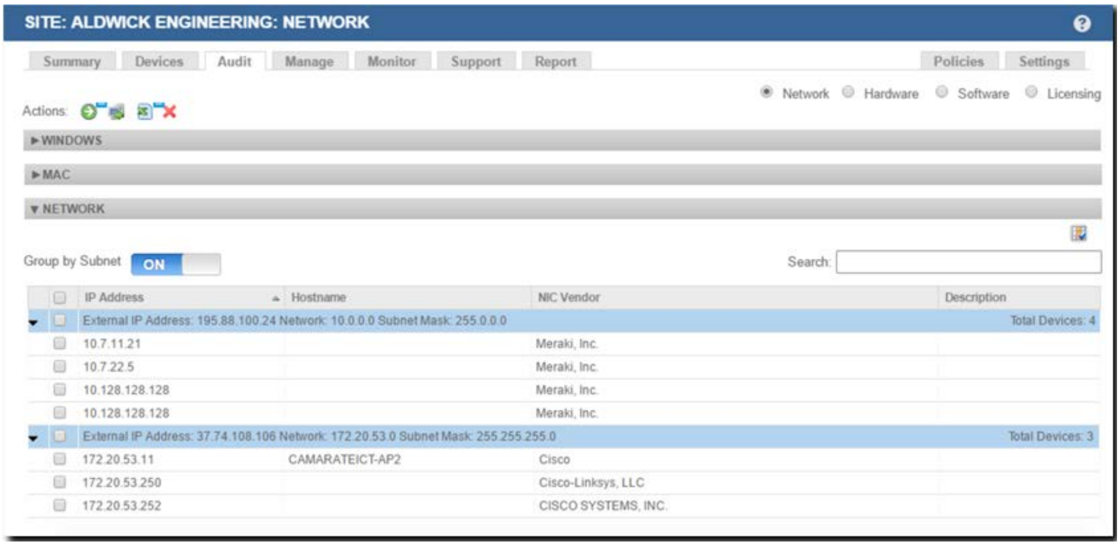
We have made significant improvements in our Network Discovery to help customers better understand what devices are still unmanaged.

Our new discovery layout gives a much better overview of what discovered devices are available in the network. Devices are now grouped by type, and from this view we've made it possible to on- board multiple, different types of devices at once. We have moved the Network Discovery results to a new section under Site Audit.

A new Network Audit view is also available on the Account level. This provides an at-a-glance view of newly-discovered and unmanaged devices across all managed sites.

Additional Subnets

The Network Discovery routine has been augmented to include support for additional subnets. Users whose networks consist of multiple V-LANs will now be able to add multiple subnets at the individual Site level to be scanned as part of the daily audit process.



SITE: ALDWICK ENGINEERING: NETWORK

	IP Address	Hostname	NIC Vendor	Description
▼ □	External IP Address: 195.88.100.24 Network: 10.0.0.0 Subnet Mask: 255.0.0.0			Total Devices: 4
□	10.7.11.21		Meraki, Inc.	
□	10.7.22.5		Meraki, Inc.	
□	10.128.128.128		Meraki, Inc.	
□	10.128.128.128		Meraki, Inc.	
▼ □	External IP Address: 37.74.108.106 Network: 172.20.53.0 Subnet Mask: 255.255.255.0			Total Devices: 3
□	172.20.53.11	CAMARATEICT-AP2	Cisco	
□	172.20.53.250		Cisco-Linksys, LLC	
□	172.20.53.252		CISCO SYSTEMS, INC.	

7.2.2. Monitoring

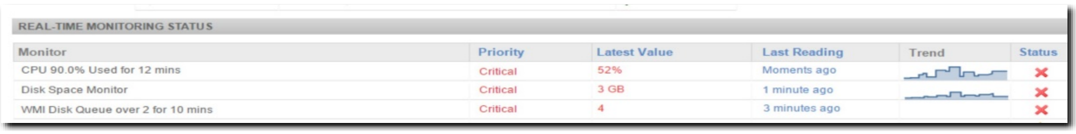
New Monitoring Core

We have refactored the core of our Monitoring engine. This results in a more reliable, efficient and powerful experience for our customers, while also giving us a foundation for future monitoring capabilities. Our Agents now run two independent services to separate communications and monitoring to divide workload and increase reliability.

We have also made significant changes to monitoring on our platform. We now have real-time communication between the Agents and the platform. This allows for more immediate application of configured monitors, and for customers to directly see what’s happening on managed devices.

Real-Time Monitoring Status

In addition to being ensured of a device’s proper function, engineers need to know if their monitors are working properly without having to wait (or fabricate alert conditions) for confirmation. To make this possible, applied monitors will now report their latest values to the platform. We will display the current values and a graphical history of these values on the Summary pages of both Agent and Network Devices. Monitoring performance data will be stored for a limited period and in a future release we will use this data for long-term trending.



REAL-TIME MONITORING STATUS

Monitor	Priority	Latest Value	Last Reading	Trend	Status
CPU 90.0% Used for 12 mins	Critical	52%	Moments ago		✗
Disk Space Monitor	Critical	3 GB	1 minute ago		✗
WMI Disk Queue over 2 for 10 mins	Critical	4	3 minutes ago		✗

WMI Monitor

The WMI provides access to a lot of great information on any Windows System. Currently, customers rely on component-based monitors to check systems for specific WMI information. Our new WMI monitor integrates this functionality in a straightforward and effective manner, vastly simplifying complicated monitoring tasks when monitoring Hyper-V environments for example.

Windows Performance Monitor

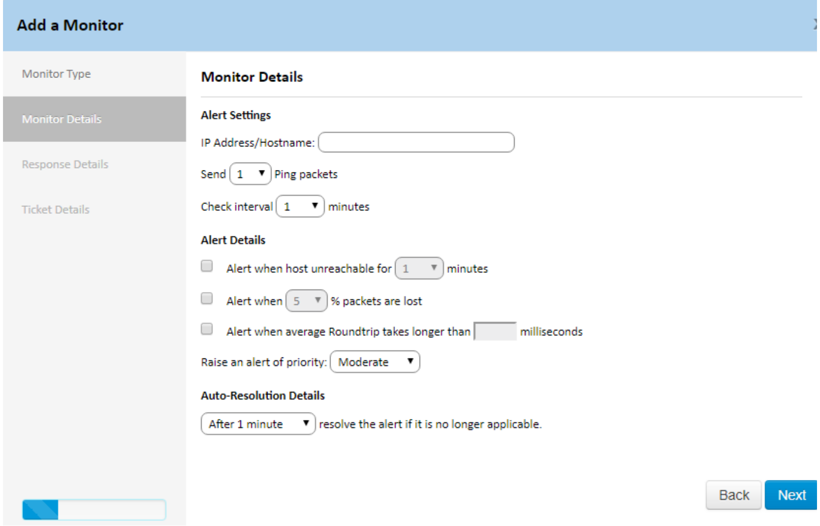
Many customers want to see real-time statistics and generate alerts for important performance indicators like SQL Server Cache hit ratio, Exchange E-mail Queues or a system's Disk Queue length. The new Windows Performance Monitor allows customers to set thresholds and monitor any Windows Performance Counter on a device.

Patch Failure Monitor

Our recent Patch Management release gave customers much more control and visibility over the patch process. The new Patch Monitor will make it possible for customers to only manage the patch exceptions in their estate. The monitor will create an alert when one or all patches fail to install, and can resolve the alert when patches are installed successfully in a subsequent run.

Ping Monitoring

ICMP, or more commonly called Ping, is a great tool to detect and analyze network problems. We've added a native Ping monitor that will help detect network issues earlier. The new monitor can simply detect if a device is still online, but it can also alert if there is a lot of network latency or packet loss.



Monitor Details

Alert Settings

IP Address/Hostname:

Send 1 ▼ Ping packets

Check interval 1 ▼ minutes

Alert Details

□ Alert when host unreachable for 1 ▼ minutes

□ Alert when 5 ▼ % packets are lost

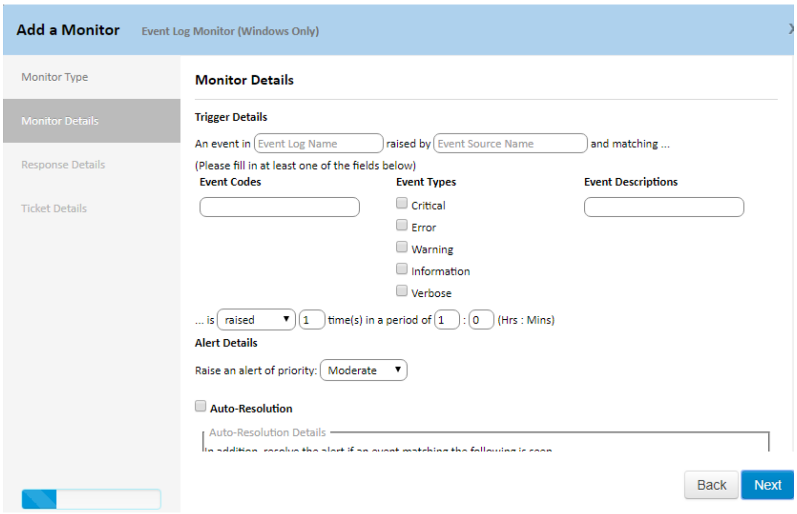
□ Alert when average Roundtrip takes longer than milliseconds

Raise an alert of priority: Moderate ▼

Auto-Resolution Details

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

Event Log Monitor



Monitor Details

Trigger Details

An event in Event Log Name raised by Event Source Name and matching ...

(Please fill in at least one of the fields below)

Event Codes

Event Types

□ Critical

□ Error

□ Warning

□ Information

□ Verbose

Event Descriptions

... is raised ▼ 1 time(s) in a period of 1 : 0 (Hrs : Mins)

Alert Details

Raise an alert of priority: Moderate ▼

□ Auto-Resolution

Auto-Resolution Details

In addition, resolve the alert if an event matching the following is seen

The Event Log is one of the most important sources when monitoring Windows systems. The Event Log monitor has been significantly improved. First of all, the Agent will be able to access the Event Logs that used to be inaccessible previously and filtering on Events will be enhanced. New functionality also includes the option to alert on the absence of events or alert when multiple events are generated in a specific time frame. Alerts from the Event Log monitor will also get Auto-Resolution options.

Disk Usage Monitor

We have made changes to our Disk Usage Monitor to make it easier for customers to apply Disk usage monitoring without having to worry about false positive alerts. In the monitor a new option is available to exclude disks below a certain size and to not apply the monitor to non-fixed drives.

Security Center Monitor

We have expanded the options of the Security Center Monitor so customers can better control when they want to generate alerts. The monitor now offers controls for category and type of exception. This allows a configuration where, for example, an alert is generated when the Antivirus is not running, but no alert is generate when the local Firewall is not running.

Component Monitor

Some subtle changes have been made that will please PCSM power users. Just like regular components, component monitors can now have files attached. This enables more powerful custom monitors on the endpoint without having to deploy required files beforehand. In addition, any component monitor can now report detailed output to the Alert diagnostic pane.

User Interface Enhancements

We've made many smaller useful enhancements to the User Interface. We've implemented a Search in various places to help customers quickly find alerts and policies. The device monitor configuration page is now grouped by policy to give customers a better view of where settings originate from. The CPU and Memory Monitors now allow any threshold so that alerts can be triggered at just 99% and above instead of 95%.

7.2.3. Network Monitoring

Network Monitoring Redesign

We have made many changes to help customers better manage Network Devices. A big change is the ability to manage Network Devices using a monitoring policy. To make this possible, every Network Device is now directly linked to a Network Node. The assigned Network Node will run the desired checks against the associated device. The Network Node will be assigned when adding a device to PCSM and can be changed from the device listing and device summary.

Other devices like Windows Servers and VMWare ESXi hosts will also use the assigned network node when getting monitoring settings assigned. This allows customers to control what node is monitoring the VMWare hosts. In the case of devices with an Agent, like Windows Servers, this change allows PCSM to apply SNMP monitors to the device to enable hardware monitoring.

SNMP Monitoring

This release introduces a new type of monitor, the SNMP monitor. This new monitor is consistent with the behaviour of other monitors, and any user familiar with PCSM monitoring will find it easy to deploy SNMP monitoring in their networks.

This new SNMP monitor can freely be assigned to any device or groups of devices using a policy. SNMP values can be calculated or translated so it's easier to understand the values. The new real-time monitoring capability of PCSM will show the SNMP results on the platform in real time and a graphical history of the values will be available.

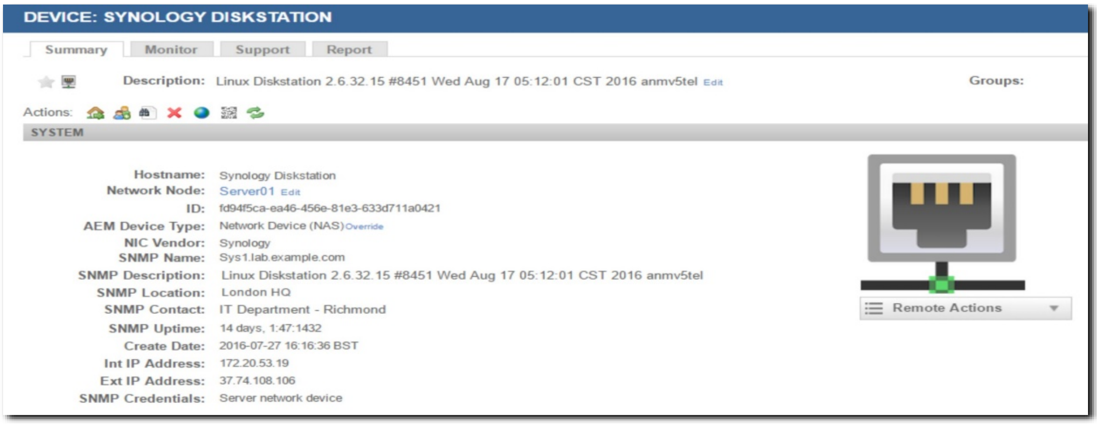
In addition to the new SNMP monitor, we will also be adding a new SNMP Throughput monitor. This monitor allows customers to monitor the bandwidth consumption for the internal or external interfaces of routers or switches.

Offline Monitoring

The offline monitoring can also be applied to Network Devices using a policy. Similar to the SNMP monitoring, the Network Node will check if the device is available. The Device status column on the platform will also show what the status is of the Network Device.

Network Device Audit

Network Devices will be audited on a regular basis, bringing functionality in line with that offered to devices running the PCSM agent. We will present many of the default SNMP fields in the system and make them available in our filters. New default filters will be available so monitoring policies can be used out of the box.



DEVICE: SYNOLOGY DISKSTATION

Description: Linux Diskstation 2.6.32.15 #8451 Wed Aug 17 05:12:01 CST 2016 anmv5tel Edit

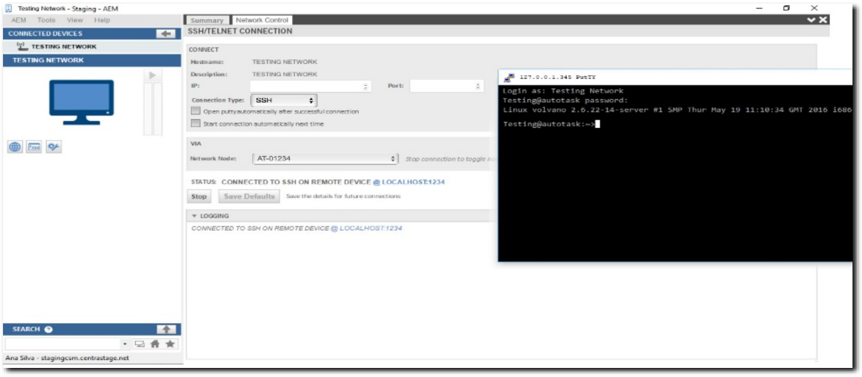
Groups:

Hostname: Synology Diskstation
Network Node: Server01 Edit
ID: fd94f5ca-ea46-456e-81e3-633d711a0421
AEM Device Type: Network Device (NAS) Override
NIC Vendor: Synology
SNMP Name: Sys1.lab.example.com
SNMP Description: Linux Diskstation 2.6.32.15 #8451 Wed Aug 17 05:12:01 CST 2016 anmv5tel
SNMP Location: London HQ
SNMP Contact: IT Department - Richmond
SNMP Uptime: 14 days, 1:47:1432
Create Date: 2016-07-27 16:16:36 BST
Int IP Address: 172.20.53.19
Ext IP Address: 37.74.108.106
SNMP Credentials: Server network device

7.2.4. Network Control

SSH/Telnet

Network devices need to be managed by engineers, but connecting to these can be cumbersome. Without the need of a VPN or any other tool, PCSM users can now directly connect to the terminal interface of any managed device. Sessions can quickly be started from the Device Summary, Device Listing and Agent Browser. The Agent Browser will us a Network Node to connect to the device and use the integrated version of PuTTY to create a seamless experience.



Testing Network - Staging - AEM

SSH/TELNET CONNECTION

CONNECT
Hostname: TESTING NETWORK
Description: TESTING NETWORK
IP:
Port:
Connection Type: SSH
□ Open putty automatically after successful connection
□ Start connection automatically next time

VIA
Network Node: AT-01234
Stop connection to toggle no

STATUS: CONNECTED TO SSH ON REMOTE DEVICE @ LOCALHOST:1234

Stop | Save Defaults | Save the details for future connections

LOGGING
CONNECTED TO SSH ON REMOTE DEVICE @ LOCALHOST:1234

127.0.0.1.345 PuTTY

```
Login as: Testing Network
Testing@autotask password:
Linux volvano 2.6.22-14-server #1 SMP Thur May 19 11:10:34 GMT 2016 i686

Testing@autotask:~>
```

HTTP/HTTPS

Similar to how the SSH/Telnet connections function, a PCSM user can set up a browser connection to any managed device in PCSM. The Network Node will act as a Proxy to connect to the device without the need of a VPN or additional tool. Connection settings can be changed, saved and the connections are logged in the PCSM activity log.

Custom Connections

The new Network Control feature can also be used to set up a custom tunnel to any device. This allows for the use of any application directly to any device. Common use cases are management of VMWare hosts using vSphere, or using a third-party management console on a Windows Device.

7.2.5. COMSTORE

Monitoring Policies

A new category is available in the COMSTORE for Monitoring Policies. We will provide "best-practice" policies for monitoring devices using PCSM. This will include policies for common server roles like Exchange/DNS, hardware vendors like Dell/HP and Network Devices by vendors such as Cisco and SonicWall. Monitoring Policies downloaded from the COMSTORE will appear in the user's own policies, where they can be altered before being applied to devices via filters or groups.

7.3. Issues fixed

Description
Servers online are shown as ofline
The manage tab takes more than 2 minutes to be loaded
The manage tab takes 30 sec to load with just 15 devices
The SNMP alerts are not raised from a printer, even though from SNMP test tool they work Ok.
Duplicated report
Small font size in chat windows

For further details, please contact support.

8. September 19th, 2017. 2017-0-3 maintenance version (Server v4.6.329, Agent v1995, Console v4.6.1639)

8.1. Added

For future releases, the new Windows agent for PCSM is built upon the **.NET 4.0 Framework** and this will mean that all existing devices will have to have this version of .NET installed to be able to use the new agent, otherwise the agent won't be updated so the new features added in future releases won't work in devices without this version of .NET installed.

In order to identify the version of .Net in the customers' devices, this maintenance version will incorporate a new filter. Also there is a new component available in the COMSTORE to update identified devices to the required version of the .NET Framework for future releases.

8.2. Issues fixed

Description
Agent browser does not remember login and password when closed
When going to any site, and then to settings, and trying to modify any of the emails already existing there, it shows up an error message.
Order in the filter criteria changes the filter result
Autotask branding issue
When monitoring warnings are converted into tickets, umlauts and special characters are not displayed correctly.
No server alert raised
On computer administration section, computer is shown as not having any patch installed (0 patch installed) even though it has patches correctly audited through th auditsnapshot.xml
30 day health report shows 122% in “Up time over last 30 days”
Different info provided on web console and reports
Customer has problem that he can't push the policy "AutoUpdate Windows Client RS"
A powershell component script isn't able to parse/obtain the values from the variables set up in the variables section
Thai chat is scrolled out and makes it unreadable

For further details, please contact support.

9. February 13th, 2017 version (Systems Management Server v4.6.317, Agent v1955, Console v4.6.1600)

9.1. Added (summary):

Main

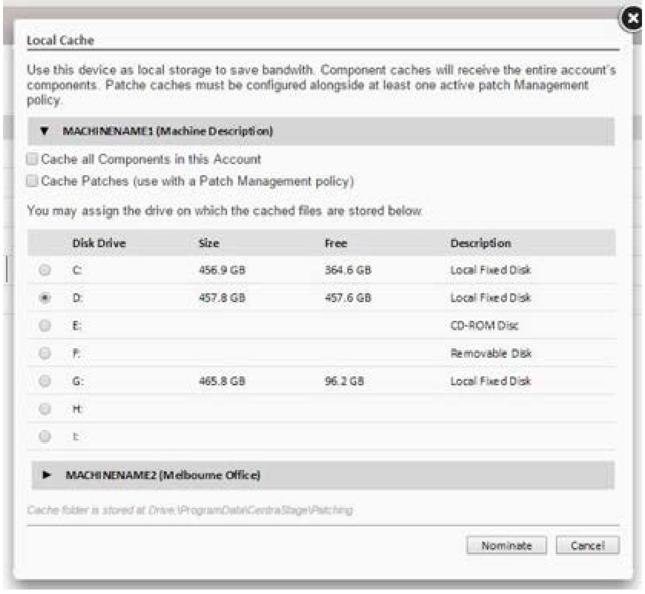
- We will improve our **Patch Management** to offer customers much more control and better visibility of the Patch process.
- We’ve enhanced our **File Manager** and added a Drive Information Tool to allow you to provide more efficient support to end users.
- New **Software Reports** and **COMSTORE update notifications** will allow you to pro-actively manage the 3rd party software running on endpoints.
- A lot of **issues fixed**. See the Issues fixed section for further information

9.2. Added (detail):

9.2.1. Patch Management

Local Caching for Patches

To reduce network load and speed up the patch process, customers can now use Agents as distribution points for Patches. An endpoint can be used as a Local Cache for Patches, Components or both. The Patch Policy can now be selected to use this cache when running.



Local Cache

Use this device as local storage to save bandwith. Component caches will receive the entire account's components. Patche caches must be configured alongside at least one active patch Management policy.

▼ MACHINENAME1 (Machine Description)

□ Cache all Components in this Account

□ Cache Patches (use with a Patch Management policy)

You may assign the drive on which the cached files are stored below.

	Disk Drive	Size	Free	Description
○	C:	456.9 GB	364.6 GB	Local Fixed Disk
●	D:	457.8 GB	457.6 GB	Local Fixed Disk
○	E:			CD-ROM Disc
○	F:			Removable Disk
○	G:	465.8 GB	96.2 GB	Local Fixed Disk
○	H:			
○	I:			

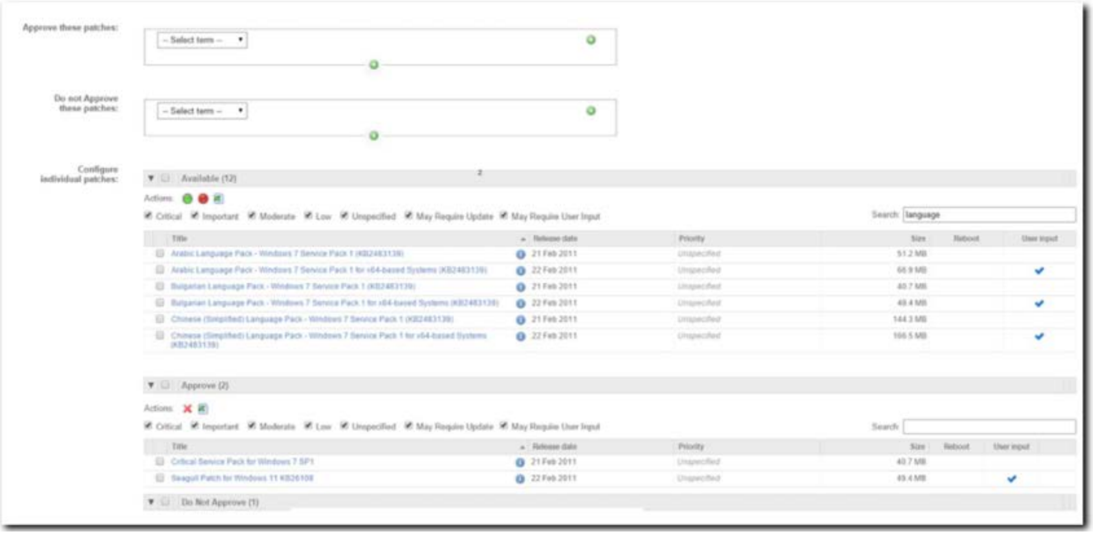
► MACHINENAME2 (Melbourne Office)

Cache folder is stored at Drive:\ProgramData\CentraStage\Patching

Enhanced Patch Approvals

Customers can now better control what patches they want to install on endpoints. Patches have three statuses: Available, Approved, Not Approved.

In addition, we have enhanced the Patch Approval UI. A combination of filters and individual patch selections can now be used to efficiently manage patch approvals for groups of devices.



Approve these patches: -- Select term --

Do not Approve these patches: -- Select term --

Configure individual patches:

▼ □ Available (12)

Actions:

☑ Critical ☑ Important ☑ Moderate ☑ Low ☑ Unspecified ☑ May Require Update ☑ May Require User Input

Search: language

	Title	Release date	Priority	Size	Reboot	User input
□	Arabic Language Pack - Windows 7 Service Pack 1 (KB2483139)	21 Feb 2011	Unspecified	51.2 MB		
□	Arabic Language Pack - Windows 7 Service Pack 1 for x64-based Systems (KB2483139)	22 Feb 2011	Unspecified	66.9 MB		✓
□	Bulgarian Language Pack - Windows 7 Service Pack 1 (KB2483139)	21 Feb 2011	Unspecified	40.7 MB		
□	Bulgarian Language Pack - Windows 7 Service Pack 1 for x64-based Systems (KB2483139)	22 Feb 2011	Unspecified	49.4 MB		✓
□	Chinese (Simplified) Language Pack - Windows 7 Service Pack 1 (KB2483139)	21 Feb 2011	Unspecified	144.3 MB		
□	Chinese (Simplified) Language Pack - Windows 7 Service Pack 1 for x64-based Systems (KB2483139)	22 Feb 2011	Unspecified	166.5 MB		✓

▼ □ Approve (2)

Actions:

☑ Critical ☑ Important ☑ Moderate ☑ Low ☑ Unspecified ☑ May Require Update ☑ May Require User Input

Search:

	Title	Release date	Priority	Size	Reboot	User input
□	Critical Service Pack for Windows 7 SP1	21 Feb 2011	Unspecified	40.7 MB		
□	Seagull Patch for Windows 11 KB26108	22 Feb 2011	Unspecified	49.4 MB		✓

▼ □ Do Not Approve (1)

Site level Patch Policy overrides

To allow our customers to better manage exceptions to policies for individual sites, we now have a way to override only specific parts of the patch policy for a site. The result is an elegant solution for cases where customers need to only change the time/day of the patch schedule or perhaps block a patch from installing at a certain site.

Wake-on-LAN in Patch Policy

Customers who want to make sure all endpoints are online when the Patch Policy starts to run can now use the integrated Wake-On -LAN feature in the Patch Policy. When selected, a network node will send the wake-up packet to devices ten minutes before it starts with the patch process.

Enhanced Visibility of current Patch Status

It is now much easier to understand the current Patch Status for any site or device. The manage tabs on Account, Site and Device have been revamped to show information like Missing Approved Patches. The most vulnerable devices and graphs can be shown only for selected policies and it's possible to drill into individual policies so it's possible to see what patches will get installed in the next patch run.

Visibility of Patch Activity

Customers can now exactly see what has happened during a Patch process. The Manage tab will now give clear insights into what patches have been installed in the last patch run for every site or device. The activity page of a single device now shows individual patch installations, which can be used to quickly analyze patch activity details and results.

Patch Reporting

A new Patch Activity report has been created to give customers a convenient way to see or demonstrate what exactly has happened during a patch run. This will detail what Patches were installed, when this happened and when Microsoft released the patch.

Existing Patch reports have been altered to support the new Approved Patch status.

Removal of Quick Patch and Patch Hiding on Manage tabs

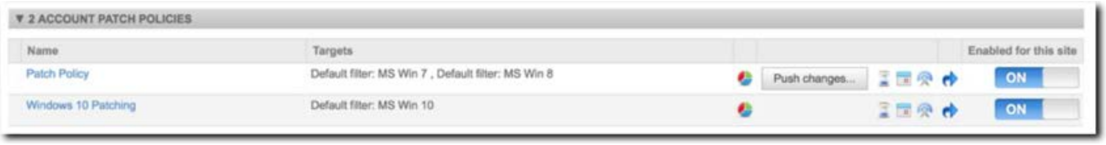
To make the Patch Management solution more predictable in behavior and easy to understand for users we've removed certain functions from the system.

Quick Patching, the process where an individual patch can be deployed to a device or site, worked completely separate from the Patch Policies in the past. This could result in unintended patch installations or have other consequences.

We've replaced this feature with the function to "Run Patch Policy now". This will immediately start to deploy approved patches to the device or site, but won't impact the Patch Schedule. Individual devices also have a permit patch option when customers only want to allow a single patch for an endpoint.

Patch Hiding and Approving has been removed from the Manage tabs. This process worked completely separate from the Patch Policy, and customers had difficulties managing Patch approvals and Patch settings as a result.

Customers using the manage tabs for patch management are recommended to use the new enhanced Patch Policies for much better control and visibility of the patch process.



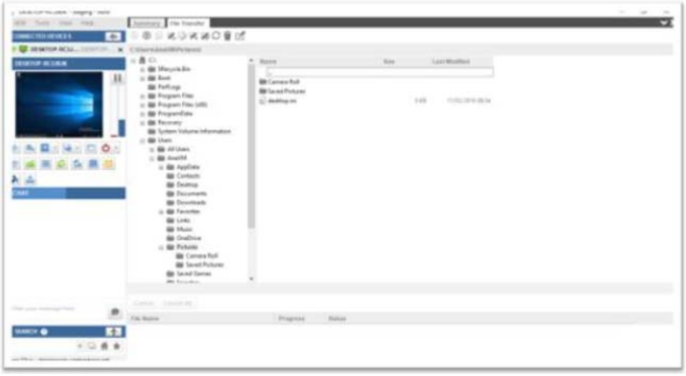
▼ 2 ACCOUNT PATCH POLICIES

Name	Targets			Enabled for this site
Patch Policy	Default filter: MS Win 7 , Default filter: MS Win 8		Push changes...	ON
Windows 10 Patching	Default filter: MS Win 10			ON

9.2.2. Support

File Manager

To provide more efficient enduser support, we've upgraded the File Transfer tool in the Agent browser to a full File Manager. Users can now Cut/Copy and Paste, Create Folders and Rename Files.



Drive Information Tool

Support engineers that need to understand what drives are currently present on a Device can now use the new Drive Information Tool in the Agent browser. This will list the current local and network drives, as well as offer a way to create new drive mappings for the device.

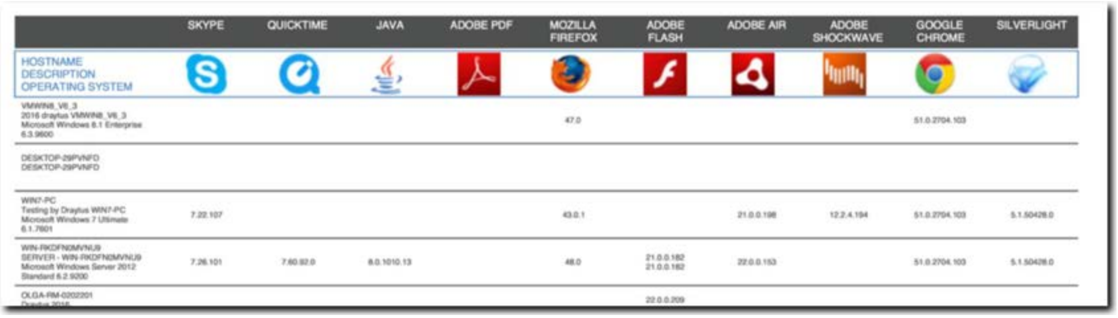
9.2.3. Reporting

COMSTORE Activity Notification email

Users can get notification e- mails from the system when new components are added or updated in the COMSTORE. Users can opt-in to these weekly notifications from the Account Settings tab. One of the major benefits that this will bring, is that Customers can now better rely on Components for 3rd party software management since they will know when a new version is ready to deploy.

New 3rd party critical software report

To help our customers to better show the value of the 3rd party software management service they provide, and make it much easier to verify if a device is up-to-date, a new report has been created called “Critical 3rd party software report”. This report will nicely show the most commonly used applications like runtimes and browsers and display their current versions on endpoints.



	SKYPE	QUICKTIME	JAVA	ADOBE PDF	MOZILLA FIREFOX	ADOBE FLASH	ADOBE AIR	ADOBE SHOCKWAVE	GOOGLE CHROME	SILVERLIGHT
HOSTNAME DESCRIPTION OPERATING SYSTEM										
VMWIN8_V6_3 2016 draytus VMWIN8_V6_3 Microsoft Windows 8.1 Enterprise 6.3.9600					47.0				51.0.2704.103	
DESKTOP-29PVNFD DESKTOP-29PVNFD										
WIN7-PC Testing by Draytus WIN7-PC Microsoft Windows 7 Ultimate 6.1.7601	7.22.107				43.0.1		21.0.0.198	12.2.4.194	51.0.2704.103	5.1.50428.0
WIN-RKDFN0MVNU9 SERVER - WIN-RKDFN0MVNU9 Microsoft Windows Server 2012 Standard 6.2.9200	7.26.101	7.60.92.0	8.0.1010.13		48.0	21.0.0.182 21.0.0.182	22.0.0.153		51.0.2704.103	5.1.50428.0
OLGA-RM-0202201 Draytus 2016						22.0.0.209				

New Software Audit report

Customers that need get a list of all applications installed on a site and have it grouped by device, can now do so. A new Software Audit report has been added to the Site level report section that simply lists all the devices of the site and shows the installed software and version for these devices.

This report will help our clients if they are audited by Microsoft.

9.2.4. Other enhancements and fixes

- Get user-defined field information from the Agent for Mac and Linux.
- Display amount of physical cores on Device Audit tab.
- ESXi hosts will now show the applied monitors in the Monitor tab.

9.3. Issues fixed

Description
AV Health Report showing wrong av detection
Permisssions to view the system policies, but in the moment you delete one system policy from the profile you delete it from system too
Panda MDM Agent won't scan QR Code
Order in the filter criteria changes the filter result
2 profiles not accessible from the agent browser
Mac 10.10+ not displaying free disc space in PCSM under audit
Different info provided on web console and reports
MDM bad integration with devices that have been previously in the platform
When i click on any serial number it sends me to the dell uk website and i am not in the uk and none of these dells are from uk.
Wrong time records in the activiry report
Delete profile device group
Android phone DOES not show phone number in console.
Transfering a *.lnk file via agent browser triggers the binary associated to lnk file
When downloading a CSV file åäö is replaced with pirate letters

W10 not showing the os version. Daily full audit not being done
Place holder sitename will not be translated
CPU/Memory graphic leaks during a certain period of time
Software policies not pushed to ios devices
App SEIKO Digital Multitool is not listed when searched in the commstore
if you create a filter with german umlauts (ä,ö,ü) the filter doesn't implement it and shown the „fÃ¼r“.
Licensing alerts are not working
Restrictions for components to be run in certain profiles is not working
Error on creating licensing audit
Win fw is disabled in the network, but most of the devices are shown as enabled.
CentraTrack Component does not achieve what it says it does
Not able to find an app on the appstore not even with the apple id
Default filter "offline for longer then a week" doesn't work
Account software audit without version and non common characters does not work when you ckick on them
Filter: Last Seen > 30d shows online machines aswell
System server summary mails sent every 30 seconds.
Security event monitor does not alert
Installing a Linux agent on CENTOS from a Profile with Proxy set, instead of setting HTTP, UnixService.exe.config shows SOCKS4.

! For further details, please contact support.

10. September 20th, 2016 version (Systems Management Server v4.6.293, Agent v1918, Console v4.6.1486)

10.1. Added (summary):

Main

- Alerts can now be muted on a schedule using **Monitoring Maintenance Windows**
- Systems Management is now much easier to setup using our **new filters** and our new **Best Practice Monitoring** policies that can be imported
- Integration with **Microsoft Hyper-V** and added new hardware monitors for VMWare ESXi
- More control over the **Privacy Mode** configuration
- Added a **new Server Performance report** showing the CPU, Memory and Disk performance over the last 30 days including the averages
- **Updated VNC** on both Windows as Mac OSX supporting non-English characters and Retina screens

10.2. Added (detail):

Agent Browser and Web Console Unification

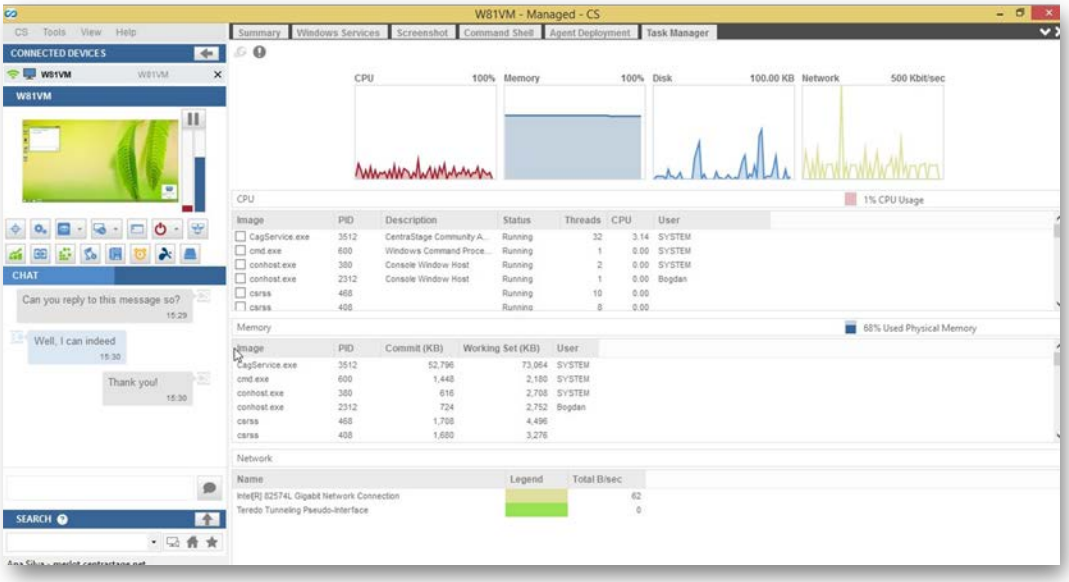
Terminology Changes

We've updated many terms in our system to make the system easier to use. The following major changes have been made to our terminology:

Old term	New term
Account (tab)	Setup
Account Admin, accountadmin	Administrator
CSM, CentraStage Server Manager	Web Portal
Custom Label, Custom Field	User-Defined Field
Default Filter	Device Filter
Details (Account > Details tab)	My Info
Packages (tab)	Billing
Product Allocation Code	Material Code
Profile	Site
Profile Device Group	Site Device Group
Profile Filter	Site Device Filter
Role	Security Level
Security Level	Component Level
Severity	Priority
System (tab)	Account
System Device Group	Device Group
System Filter	Custom Device Filter
System Profile Group	Site Group

Agent Browser and Web Portal Reskin

The Web Portal and the Agent Browser have both received a significant UI update. The results are amazing, the product feels new, fresher and more beautiful than ever!



Can you reply to this message so? 15:29

Well, I can indeed 15:30

Thank you! 15:30

Ana Silva - merlot.centrastage.net

CPU — 🟥 1% CPU Usage

Image	PID	Description	Status	Threads	CPU	User
□ CagService.exe	3512	CentraStage Community A...	Running	32	3.14	SYSTEM
□ cmd.exe	600	Windows Command Proce...	Running	1	0.00	SYSTEM
□ conhost.exe	380	Console Window Host	Running	2	0.00	SYSTEM
□ conhost.exe	2312	Console Window Host	Running	1	0.00	Bogdan
□ csrss	468		Running	10	0.00	
□ csrss	408		Running	8	0.00	

Memory — 🟦 68% Used Physical Memory

Image	PID	Commit (KB)	Working Set (KB)	User
CagService.exe	3512	52,796	73,064	SYSTEM
cmd.exe	600	1,448	2,180	SYSTEM
conhost.exe	380	616	2,708	SYSTEM
conhost.exe	2312	724	2,752	Bogdan
csrss	468	1,708	4,496	
csrss	408	1,680	3,276	

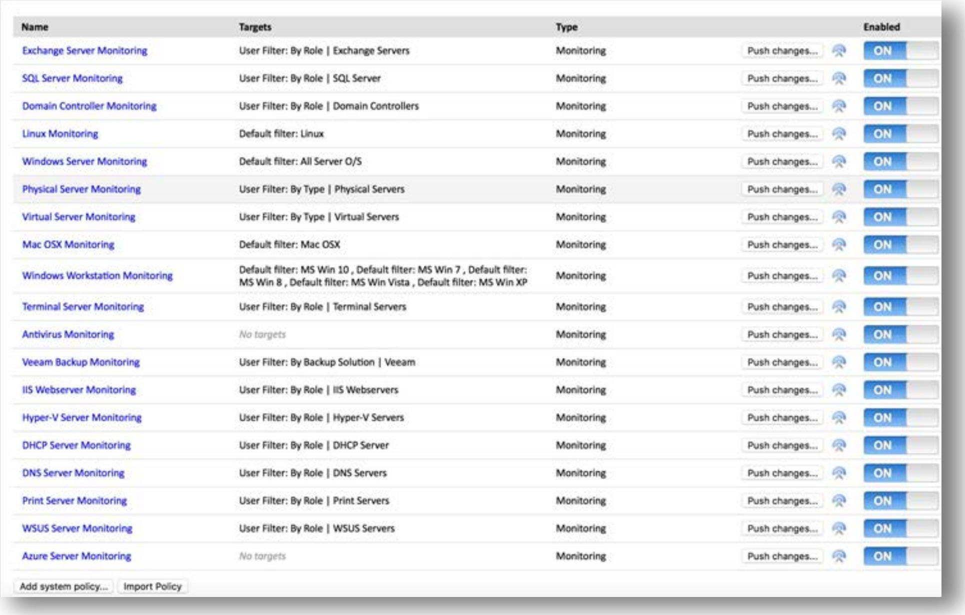
Network

Name	Legend	Total B/sec
Intel(R) 82574L Gigabit Network Connection	🟨	62
Teredo Tunneling Pseudo-Interface	🟩	0

10.2.1. Monitoring

Best Practices Monitoring Policies

Best Practices Monitoring Policies are available that can be imported into Systems Management. These Policies will include best practices for monitoring the most common platforms and applications like Exchange, SQL and IIS.



Name	Targets	Type		Enabled
Exchange Server Monitoring	User Filter: By Role | Exchange Servers	Monitoring	Push changes...	ON
SQL Server Monitoring	User Filter: By Role | SQL Server	Monitoring	Push changes...	ON
Domain Controller Monitoring	User Filter: By Role | Domain Controllers	Monitoring	Push changes...	ON
Linux Monitoring	Default filter: Linux	Monitoring	Push changes...	ON
Windows Server Monitoring	Default filter: All Server O/S	Monitoring	Push changes...	ON
Physical Server Monitoring	User Filter: By Type | Physical Servers	Monitoring	Push changes...	ON
Virtual Server Monitoring	User Filter: By Type | Virtual Servers	Monitoring	Push changes...	ON
Mac OSX Monitoring	Default filter: Mac OSX	Monitoring	Push changes...	ON
Windows Workstation Monitoring	Default filter: MS Win 10 , Default filter: MS Win 7 , Default filter: MS Win 8 , Default filter: MS Win Vista , Default filter: MS Win XP	Monitoring	Push changes...	ON
Terminal Server Monitoring	User Filter: By Role | Terminal Servers	Monitoring	Push changes...	ON
Antivirus Monitoring	*No targets*	Monitoring	Push changes...	ON
Veeam Backup Monitoring	User Filter: By Backup Solution | Veeam	Monitoring	Push changes...	ON
IIS Webserver Monitoring	User Filter: By Role | IIS Webservers	Monitoring	Push changes...	ON
Hyper-V Server Monitoring	User Filter: By Role | Hyper-V Servers	Monitoring	Push changes...	ON
DHCP Server Monitoring	User Filter: By Role | DHCP Server	Monitoring	Push changes...	ON
DNS Server Monitoring	User Filter: By Role | DNS Servers	Monitoring	Push changes...	ON
Print Server Monitoring	User Filter: By Role | Print Servers	Monitoring	Push changes...	ON
WSUS Server Monitoring	User Filter: By Role | WSUS Servers	Monitoring	Push changes...	ON
Azure Server Monitoring	*No targets*	Monitoring	Push changes...	ON

Monitoring Maintenance Windows

It is now possible to schedule a Monitoring maintenance window, during which alerting will be muted. The Monitoring Maintenance Windows can be scheduled as a policy for a dynamic set of devices. When alerts are generated for devices that are in maintenance no tickets are created and no automatic actions will be taken.

Importable/Exportable Monitoring Policies

Monitoring Policies can now be imported and exported directly from the Policies view. The export will include the configured monitors, thresholds and severity settings. This will dramatically reduce the time it takes to setup the system with industry best practices.

New VMWare ESXi Hardware Monitors

We've added three new monitors to monitor the hardware state of ESXi Hosts. Using these new monitors the Power Supply, RAID Status and Fan Status of ESXi hosts can be monitored and serious issues can be prevented.

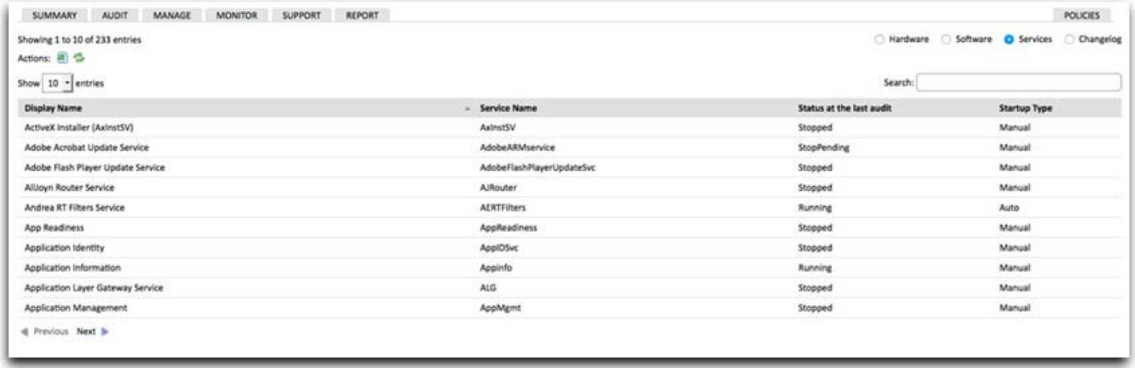
10.2.2. Audit

New Default Filters

Many new default filters have been added to Systems Management. The filters are now grouped by category and have an instant search so that users can get to machines much quicker than ever before. The new filters are a significant improvement for navigating the system and also makes it much easier to apply monitoring best-practices to managed devices.

Windows Services Audit

The daily audit process will now also capture all the installed services on a Windows device. The data is presented in the Audit section of the device, and can be quickly searched and used in our Filters. This will make it much easier to find machines that have a specific role or server application installed.



Showing 1 to 10 of 233 entries

Display Name	Service Name	Status at the last audit	Startup Type
ActiveX Installer (AxInstSV)	AxInstSV	Stopped	Manual
Adobe Acrobat Update Service	AdobeARMservice	StopPending	Manual
Adobe Flash Player Update Service	AdobeFlashPlayerUpdateSvc	Stopped	Manual
AllJoyn Router Service	AJRouter	Stopped	Manual
Andrea RT Filters Service	AERTFilters	Running	Auto
App Readiness	AppReadiness	Stopped	Manual
Application Identity	AppIDSvc	Stopped	Manual
Application Information	Appinfo	Running	Manual
Application Layer Gateway Service	ALG	Stopped	Manual
Application Management	AppMgmt	Stopped	Manual

Microsoft Hyper-V Guest Audit

When a Windows machine has the Hyper-V role enabled, the audit process will now capture all the Guest machines on that Hyper-V host. The machines will be displayed in the Summary section of the device. Users can now quickly get to any of the guests running on the Hyper-V host and troubleshoot issues faster.

Last Reboot and Reboot Pending Audit

Our device audits will now also capture the Last Reboot date and Reboot Pending Status from any Windows machine. The data is displayed in the Summary section of the device, and can be used in Filters. This will help users quickly find machines that still have a reboot pending or when a machine has not been rebooted for months.

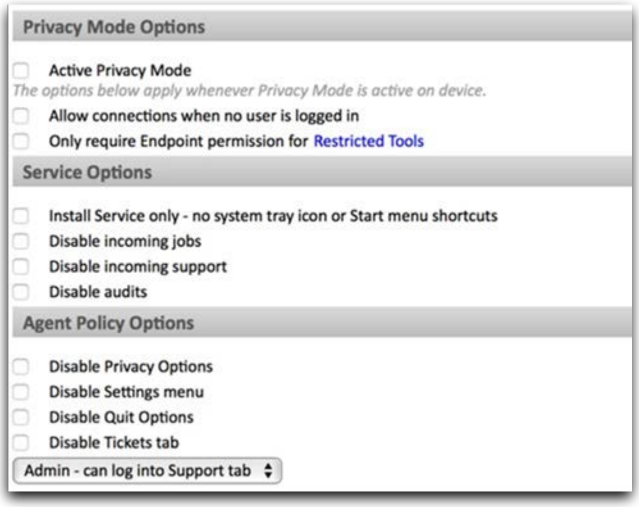
Deep Memory Audit

The Audit will now also capture the memory configuration of any Windows device. We will display the memory slots that are used/available including relevant details like the speed and type of memory. This information will be shown in the Hardware section of the device.

10.2.3. Support

Privacy Mode Enhancements

The agent policy now offers more control over the Privacy Mode configuration. It is now possible to allow connections to machines when Privacy Mode is enabled, but no user is logged into the system. It’s also possible to only require permission for the screen sharing tools VNC, RDP and Screenshot but allow the other tools in the agent browser without asking for user- permission when the Privacy mode is enabled.



Privacy Mode Options

☐ Active Privacy Mode

The options below apply whenever Privacy Mode is active on device.

☐ Allow connections when no user is logged in

☐ Only require Endpoint permission for Restricted Tools

Service Options

☐ Install Service only - no system tray icon or Start menu shortcuts

☐ Disable incoming jobs

☐ Disable incoming support

☐ Disable audits

Agent Policy Options

☐ Disable Privacy Options

☐ Disable Settings menu

☐ Disable Quit Options

☐ Disable Tickets tab

Admin - can log into Support tab

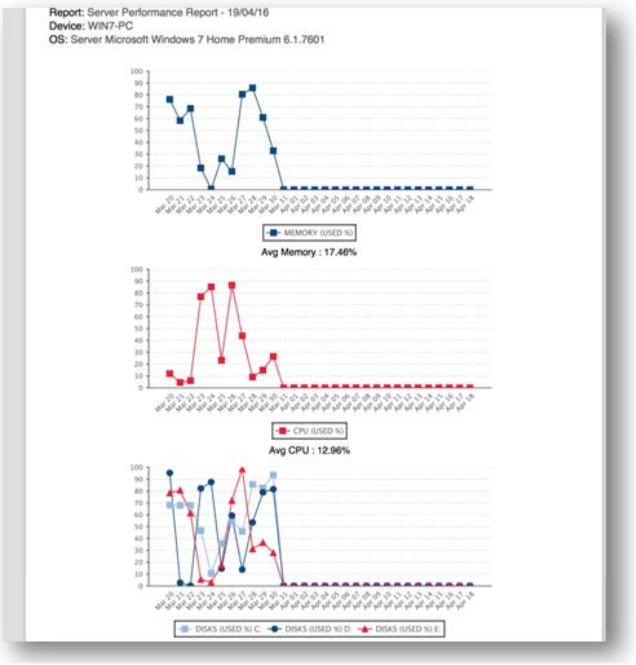
Updated VNC version

We've updated VNC on both Windows as Mac OSX. This will improve the remote control experience on Windows when using non-English characters in the session. The new VNC version for Mac adds support for Retina screens.

10.2.4. Reporting

New Server Performance Report

To allow users to better report customers on the performance of their servers we've added a new Server Performance report to Systems Management. This report will show the CPU, Memory and Disk performance over the last 30 days including the average of the CPU and Memory and the Disk Delta over this period.



Report: Server Performance Report - 19/04/16
Device: WIN7-PC
OS: Server Microsoft Windows 7 Home Premium 6.1.7601

Avg Memory : 17.46%

Avg CPU : 12.96%

New Site Remote Takeover Report

We’ve added a new report that details all the remote control sessions to a single site in the last 30 days.

10.2.5. Other enhancements and fixes

- The Role permissions have changed so that it now becomes possible for a user to only see devices that belong to a group.
- Logs are not deleted when the Agent is removed from a system
- Our new Linux agent works with systemd to support latest the latest Linux distributions
    - Fedora 19, 20, 21, 22, 23
    - Debian 7, 8
    - CentOS 6, 7
    - Ubuntu 12, 13, 14, 15, 16
- Powershell Component Monitors are now bypassing the Powershell executing policy
- New options under Help to quickly go to our Release Notes, Advanced Guide, etc
- German, Spanish, French, Hungarian, Italian, Portugues and Swedish translation updates

10.3. Issues fixed

Description
Remote control not working with Retina display in MAC
Remote control not working with special characters in Windows
Search and refresh of the web console
Issue in debian 7.5

For further details, please contact support.

11. July 12nd, 2016-1 version (Systems Management Server v4.6.281, Agent v1887, Console v4.6.1438)

11.1. Issues fixed

Description
Dates are not sorted out when you press sort by date.
System Filter Criterias not functioning correctly

Inventory age report duplicates hostnames
Ticket comment rows are shown in html format
job targets that results in the page not displaying
Searching and refreshing a device results in an error
Error message when MDM software policy is created
Editing Component monitors removes Data from the fields.
Cagservice sometimes fails to start when computer turns on / reboots
Download all the devices csv results in blanck
Audit only collecting some patch information
Iphone gps alocation service not working
Java 8 devices shows as vulnerable software
Onenote will not install via MDM software policy
Monitor component input variables are lost after if the monitor is edited after creation

For further details, please contact support.

12. March 8th, 2016 version (Systems Management Server v4.6.265, Agent v1863, Console v4.6.1340)

12.1. Added (summary)

The new version new features , numerous improvements and fixes. Of the finer points included within this release, the following stand out:

- Ability to enroll ESXi servers as network devices and both monitor and view crucial audit information pertaining to both the server unit and the virtual guests therein
- Numerous improvements to the manner in which network devices are handled, including dedicated support for SNMP v1-only devices
- Dedicated Agent support for the .NET 4.0 Framework, facilitating easier Agent silent-deployment on fresh Windows installations
- Improved ticketing engine

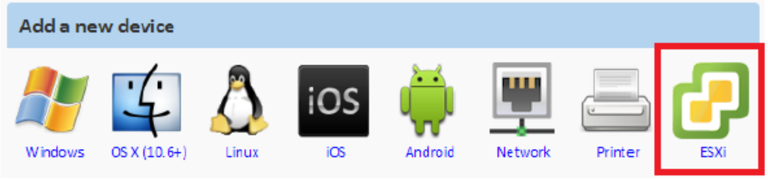
12.2. Added (detail)

VMware ESXi

VMware ESXi (also known as VMware vSphere Hypervisor) is a purpose-built bare-metal hypervisor, that is, a platform that allows multiple operating systems to run on a host computer (server) at the same time. ESXi installs directly onto a physical server enabling it to be partitioned into multiple servers referred to as virtual machines. Each virtual machine shares the same physical resources as the other virtual machines and they can all run at the same time.

Systems Management now supports the enrollment and monitoring of servers running the VMware ESXi bare-metal operating system. Enrollment is managed not by installing an Agent on the server but through management of the machine as a network device through the vSphere and CIM communications channels. Data is served via network nodes.

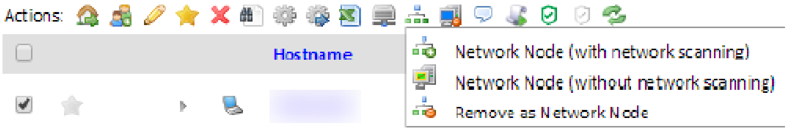
You will be able to add the ESXi devices to your account manually



The data required when an ESXi is added is shown in the next table

Field	What to Enter
IP Address	Enter the IP address of your device
Name	Give your device a meaningful name
Description	Enter a meaningful description
Manufacturer	Enter the name of the manufacturer of your device
Model	Enter the model of your device
New ESXi Credentials	Enter the ESXi credentials of your device. For more information, refer to the ESXi Credentials section in Account Settings and Profile Settings
Use System/Profile ESXi Cre-dentials	Choose this option if you have ESXi credentials stored at system or profile level. The profile ESXi credentials will be used in addition to the ESXi cre-dentials specified in Account Settings unless this option is disabled in Pro-file Settings. For information on how to store the ESXi credentials for the entire account or at profile level, refer to the ESXi Credentials section in Account Settings and Profile Settings

Or you can also nominate a fully managed network node device to discover and manage them for you. It will check for devices listening on port 902 and if a devices responds, it will be listed as an ESXi device in the discovered devices list.


Actions:
Hostname
Network Node (with network scanning)
Network Node (without network scanning)
Remove as Network Node

Once your ESXi devices have been added as managed devices to your account, basic data can be seen at-a-glance in the Systems Managementm console immediately such as asset tags and server model names.

Once audit data has been submitted, users will see in-depth data regarding individual virtual machine guests, installed RAM slots and Network Interface Cards.

Furthermore, virtual machines with Agents installed on them will be linked through in the interface, allowing users to keep close tabs on their inventory.

The ESXi devices managed, can be monitored through your network node device.

ESXi servers' temperatures, CPU and RAM usage, data store storage space and whether the ESXi host is offline can all be monitored through the existing monitoring interface. ESXi monitors can only be applied at system and profile level as part of an ESXi policy

The next table shows the four ESXi monitor types available:

Monitor Type	Function

ESXi CPU Monitor	Similarly to the "CPU Monitor" available for Windows, Mac and Linux devices, the ESXi CPU Monitor can alert you if your ESXi host has high CPU usage
ESXi Memory Mon-itor	Similarly to the "Memory Monitor" available for Windows, Mac and Linux devices, the ESXI Memory Monitor can alert you if your ESXi host has high memory usage.
ESXi Data Store Monitor	Similarly to the "Disk Usage Monitor" 7 available for Windows devices, the ESXi Data Store Monitor can alert you if the available space in any of the datastores on an ESXi host drops below a certain threshold.
ESXi Temperature Sensor Monitor	This monitor allows you to set up an alert if the temperature sensors on the ESXi host exceed a certain threshold.

The following ESXi builds are supported: 4.1, 5.0, 5.5 and 6.0.

SNMP

Numerous improvements to the existing SNMP functionality have been added in this release.

New with this release is dedicated support for devices only capable of broadcasting via the SNMP v1 protocol, instead of the previous backwards-compatibility support included in legacy releases.

When new network devices are added via the Web Portal, a scan will be performed to ascertain the type of network device that has been added. Audit data submission will begin immediately following device enrollment; once the data has been submitted, the Web Portal will attempt to identify the device. The Web Portal is currently able to identify network devices as printers, switches, routers and uninterruptable power supplies from the brand APC.

Agent support for .NET 4.0 Framework

Windows 8, 8.1 and 10 do not come with the .NET 2.0 Framework, making silent installation of the Agent on fresh installations of these operating systems difficult. The Agent now natively supports both the .NET 4.0 and 2.0 Framework, meaning that new installs of these three most recent consumer-level Windows operating systems will be able to run the Agent without needing any additional dependencies being installed.

Ticketing engine

The ticketing engine has been improved and now the changes introduced through the web console or through the agent are syncronized. (called “round-trip” ticketing).

12.3. Issues fixed

Description
Page will not load when device view is disabled for a default role
Cannot login if username contains an accent
Add 'Network Device' to system filter criteria list
Existing policies are not applied to new devices where changes to a policy are NOT pushed
Error when adding comments to a support ticket
Audit only collecting some patch information

Can't edit component icons

For further details, please contact support.

12.4. Known issues

VMware ESXi

The agent (device) nominated as a network node that discovers the ESXi device(s) needs the .NET Framework 3.5 installed to perform full audit of the ESXi devices.

13. December 17th, 2015 version (Systems Management Server v4.6.243, Agent v1854, Console v4.6.1181)

13.1. Added:

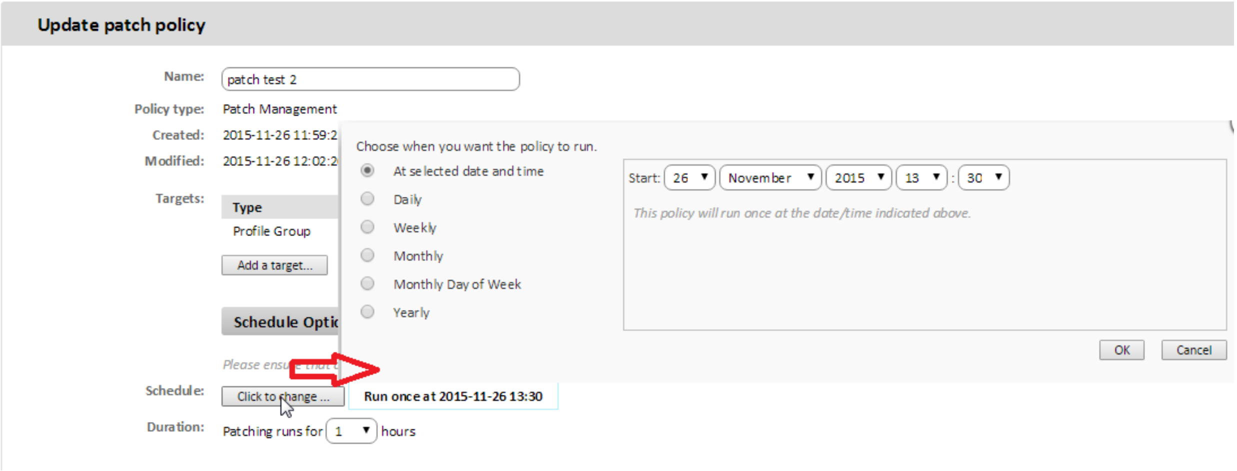
Support to the new OSX version called “El Capitan”

The new OSX version (“El Capitan”) is now supported.

For further details about the Systems Management features available by platform see the document Features by platform in the extranet

New Patch Management Scheduler that

It allows for more flexible patch deployment. See image below with the new options available



Update patch policy

Name: patch test 2

Policy type: Patch Management

Created: 2015-11-26 11:59:2

Modified: 2015-11-26 12:02:2

Targets:

Type
Profile Group

Add a target...

Schedule Optic

Please ensu[illegible]

Schedule: Click to change ... Run once at 2015-11-26 13:30

Duration: Patching runs for 1 ▼ hours

Choose when you want the policy to run.

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

Start: 26 ▼ November ▼ 2015 ▼ 13 ▼ : 30 ▼

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

10 Custom Fields.

10 Custom Fields are now available instead of 5 in previous versions. Users now have ten custom fields to work with, and the agent and reporting system has been upgraded to accommodate this.

13.2. Issues fixed:

All cases solved with the new version are marked In Salesforce as “Solved in next release” and return accordingly after the deployment. For further details, please contact support.

14. September 23th, 2015 version (Systems Management Agent v1839)

14.1. Added (summary):

Main

- SNMP management from Systems Management console
- SNMP v3 support
- Network Monitoring Components
- Editable ComStore components
- Alerts CSV export additions
- Deleted devices user Access
- Net Assests scanning control
- Search bar in scheduled job component window

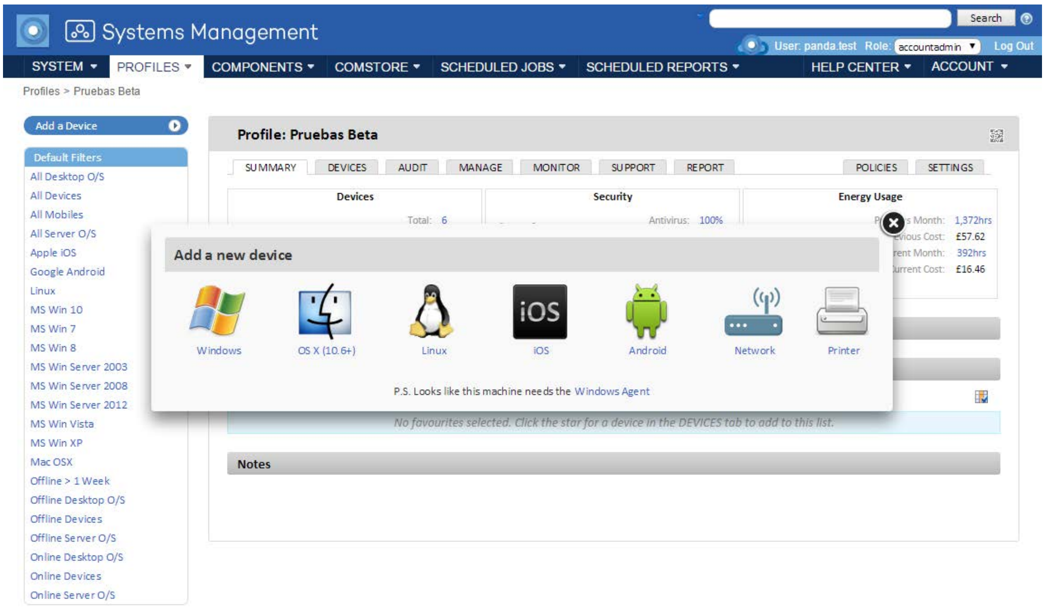
Minor

- Remove redundant RDP enable from Agent Installer
- Customer Health Summary Report to Include Java Update 40 & 45
- Add CPU types to Pass/Fail criteria for Customer Health Summary report

14.2. Added (detail):

SNMP management from Systems Management console

- ✓ Automatic discovery and identification network assets with ready-to-go SNMP monitoring templates.
- ✓ Easier to gain full visibility of customer's network and pro-actively monitor every device.
- ✓ Complete SNMP management from the console.
- ✓ Add new device screenshots including printer and network device:



Total: 6

Antivirus: 100%

Month: 1,372hrs

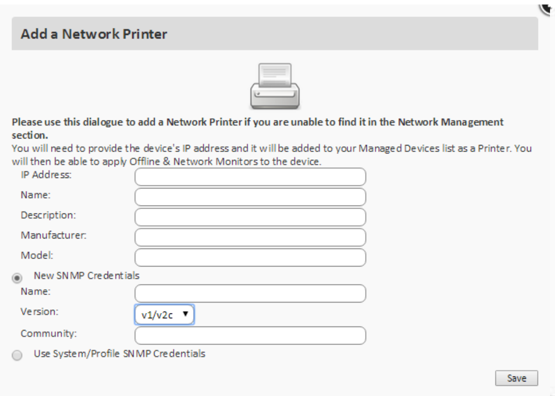
Previous Cost: £57.62

Current Month: 392hrs

Current Cost: £16.46

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

No favourites selected. Click the star for a device in the DEVICES tab to add to this list.



Add a Network Printer

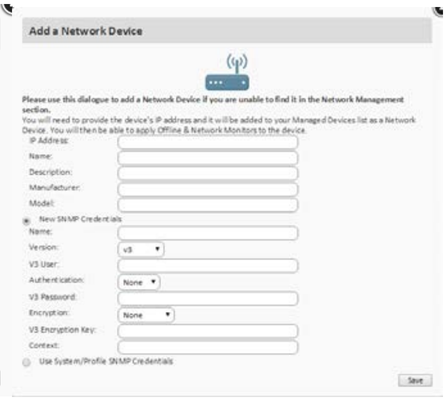
Please use this dialogue to add a Network Printer if you are unable to find it in the Network Management section.
You will need to provide the device's IP address and it will be added to your Managed Devices list as a Printer. You will then be able to apply Offline & Network Monitors to the device.

IP Address:	
Name:	
Description:	
Manufacturer:	
Model:	

● New SNMP Credentials

Name:	
Version:	v1/v2c ▾
Community:	

○ Use System/Profile SNMP Credentials



Add a Network Device

Please use this dialogue to add a Network Device if you are unable to find it in the Network Management section.
You will need to provide the device's IP address and it will be added to your Managed Devices list as a Network Device. You will then be able to apply Offline & Network Monitors to the device.

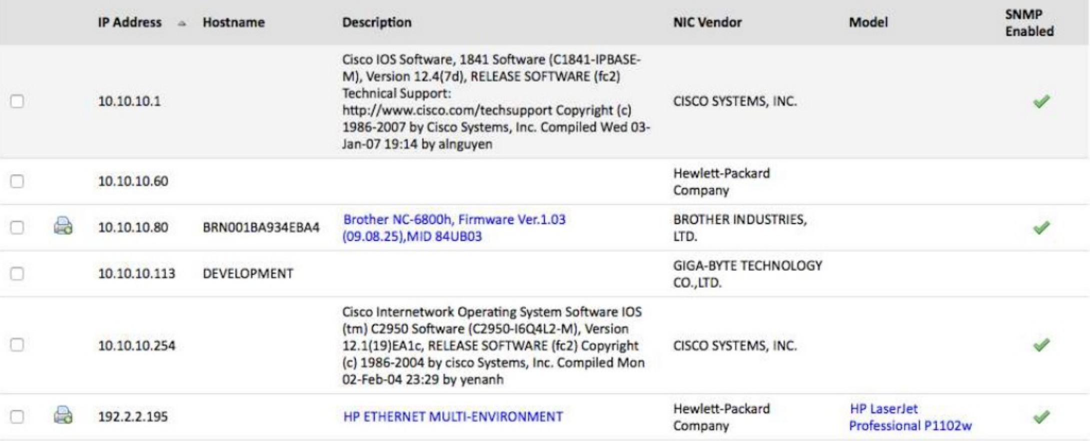
IP Address:	
Name:	
Description:	
Manufacturer:	
Model:	

● New SNMP Credentials

Name:	
Version:	v3 ▾
V3 User:	
Authentication:	None ▾
V3 Password:	
Encryption:	None ▾
V3 Encryption Key:	
Context:	

○ Use System/Profile SNMP Credentials

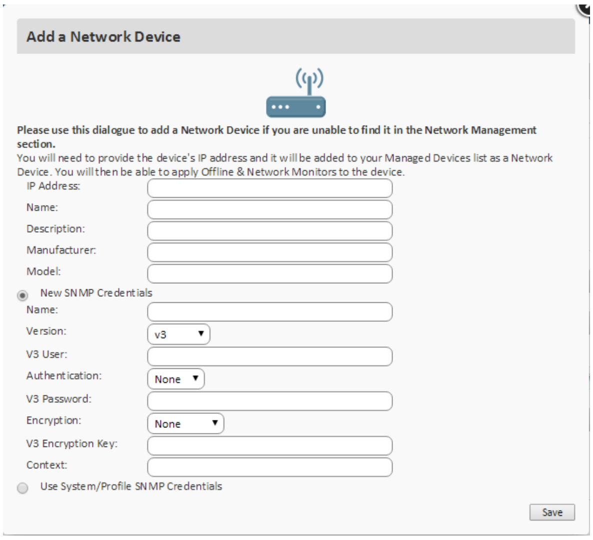
- ✓ Managed devices view :



		IP Address	Hostname	Description	NIC Vendor	Model	SNMP Enabled
□		10.10.10.1		Cisco IOS Software, 1841 Software (C1841-IPBASE-M), Version 12.4(7d), RELEASE SOFTWARE (fc2) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2007 by Cisco Systems, Inc. Compiled Wed 03-Jan-07 19:14 by alnguyen	CISCO SYSTEMS, INC.		✓
□		10.10.10.60			Hewlett-Packard Company		
□	🖨	10.10.10.80	BRN001BA934EBA4	Brother NC-6800h, Firmware Ver.1.03 (09.08.25),MID 84UB03	BROTHER INDUSTRIES, LTD.		✓
□		10.10.10.113	DEVELOPMENT		GIGA-BYTE TECHNOLOGY CO.,LTD.		
□		10.10.10.254		Cisco Internetwork Operating System Software IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(19)EA1c, RELEASE SOFTWARE (fc2) Copyright (c) 1986-2004 by cisco Systems, Inc. Compiled Mon 02-Feb-04 23:29 by yenanh	CISCO SYSTEMS, INC.		✓
□	🖨	192.2.2.195		HP ETHERNET MULTI-ENVIRONMENT	Hewlett-Packard Company	HP LaserJet Professional P1102w	✓

SNMP v3 support

- ✓ Management from Systems Management console.
- ✓ Strengthens the security features including authentication, privacy and access control; and management protocol, with greater modularity and the possibility of remote configuration.
- ✓ Add new network device window with v3 parameters to configure:



Add a Network Device

Please use this dialogue to add a Network Device if you are unable to find it in the Network Management section.
You will need to provide the device's IP address and it will be added to your Managed Devices list as a Network Device. You will then be able to apply Offline & Network Monitors to the device.

IP Address:	
Name:	
Description:	
Manufacturer:	
Model:	

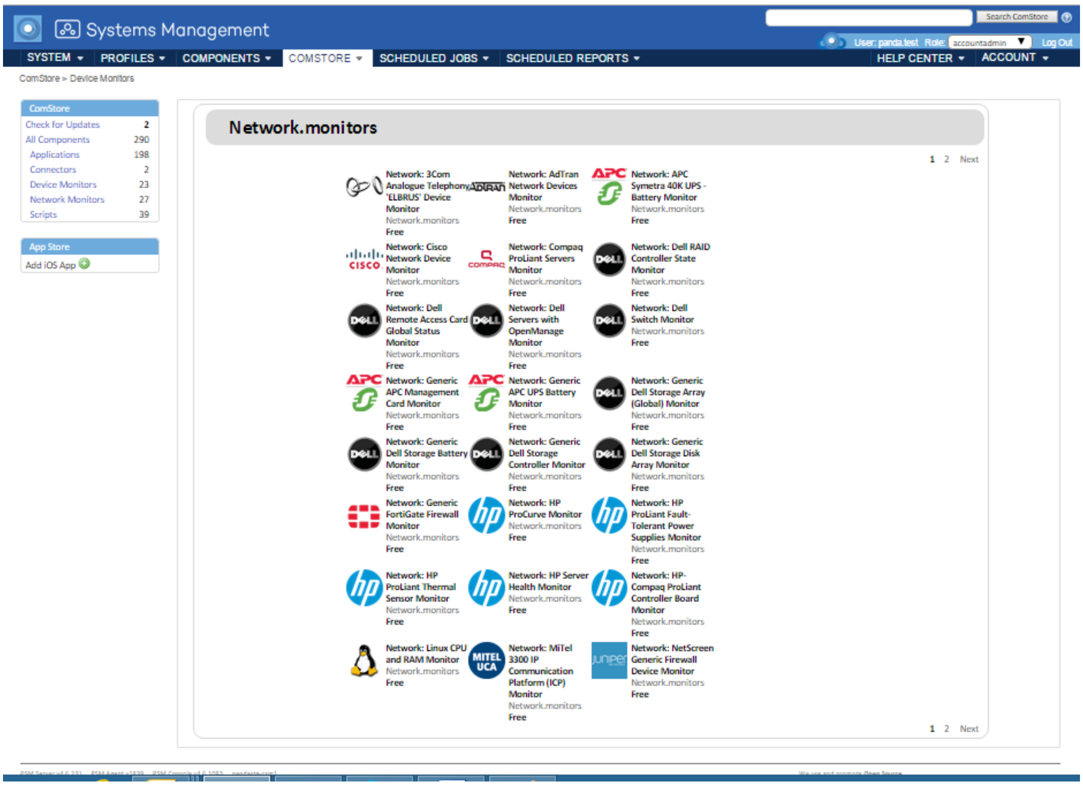
● New SNMP Credentials

Name:	
Version:	v3 ▾
V3 User:	
Authentication:	None ▾
V3 Password:	
Encryption:	None ▾
V3 Encryption Key:	
Context:	

○ Use System/Profile SNMP Credentials

Network Monitoring Components

- ✓ As number of new Network Monitor components have been released to the ComStore.
- ✓ These components are produced to get you up and running with Network Monitoring, and to demonstrate the ease of use and capabilities of this functionality.
- ✓ Users can download and use these components to monitor their network hardware if the two are compatible



ComStore	
Check for Updates	2
All Components	290
Applications	198
Connectors	2
Device Monitors	23
Network Monitors	27
Scripts	39

Network.monitors

Network: 3Com Analogue Telephony 'ELBRUS' Device Monitor
Network.monitors
Free

Network: AdTran Network Devices Monitor
Network.monitors
Free

Network: APC Symetra 40K UPS - Battery Monitor
Network.monitors
Free

Network: Cisco Network Device Monitor
Network.monitors
Free

Network: Compaq ProLiant Servers Monitor
Network.monitors
Free

Network: Dell RAID Controller State Monitor
Network.monitors
Free

Network: Dell Remote Access Card Global Status Monitor
Network.monitors
Free

Network: Dell Servers with OpenManage Monitor
Network.monitors
Free

Network: Dell Switch Monitor
Network.monitors
Free

Network: Generic APC Management Card Monitor
Network.monitors
Free

Network: Generic APC UPS Battery Monitor
Network.monitors
Free

Network: Generic Dell Storage Array (Global) Monitor
Network.monitors
Free

Network: Generic Dell Storage Battery Monitor
Network.monitors
Free

Network: Generic Dell Storage Controller Monitor
Network.monitors
Free

Network: Generic Dell Storage Disk Array Monitor
Network.monitors
Free

Network: Generic FortiGate Firewall Monitor
Network.monitors
Free

Network: HP ProCurve Monitor
Network.monitors
Free

Network: HP ProLiant Fault-Tolerant Power Supplies Monitor
Network.monitors
Free

Network: HP ProLiant Thermal Sensor Monitor
Network.monitors
Free

Network: HP Server Health Monitor
Network.monitors
Free

Network: HP-Compaq ProLiant Controller Board Monitor
Network.monitors
Free

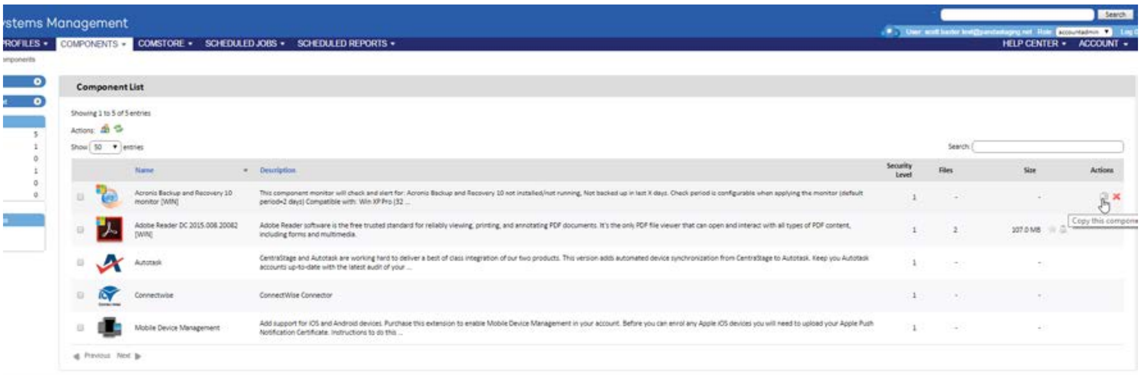
Network: Linux CPU and RAM Monitor
Network.monitors
Free

Network: MiTel 3300 IP Communication Platform (ICP) Monitor
Network.monitors
Free

Network: NetScreen Generic Firewall Device Monitor
Network.monitors
Free

Editable ComStore components

- ✓ Systems Management allows to download Components from the ComStore and edit them.
- ✓ User can use this new feature adapt and modify components in order to better suit their requirements
- ✓ Steps: 1 copy component



Component List

Showing 1 to 5 of 5 entries

Actions:

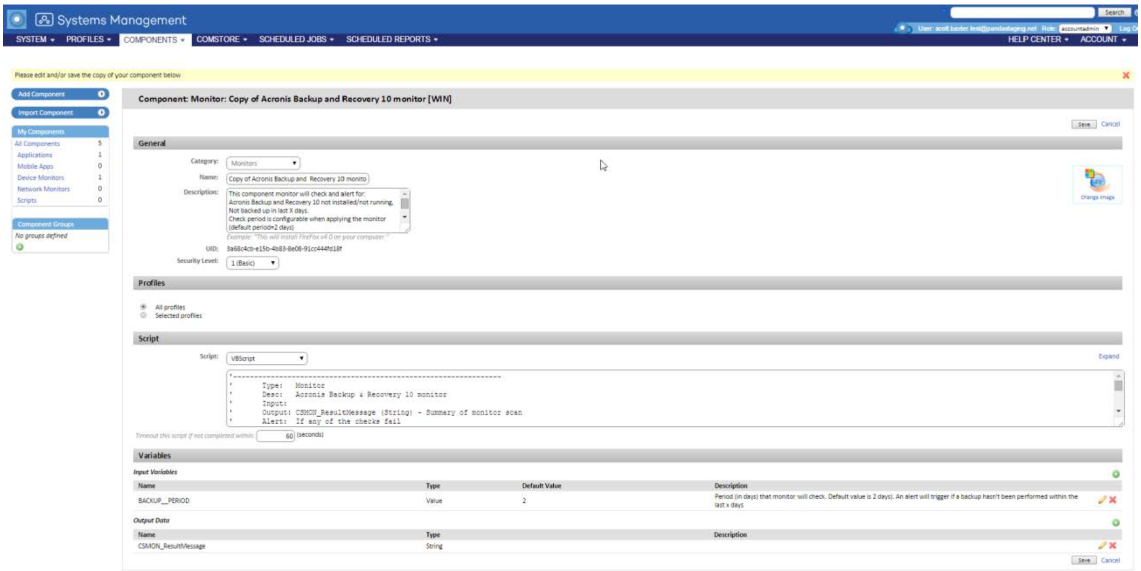
Show 50 entries

Search:

		Name	Description	Security Level	Files	Size	Actions
□		Acronis Backup and Recovery 10 monitor [WIN]	This component monitor will check and alert for: Acronis Backup and Recovery 10 not installed/not running, Not backed up in last X days. Check period is configurable when applying the monitor (default period=2 days) Compatible with: Win XP Pro (32 ...	1	-	-	
□		Adobe Reader DC 2015.008.20082 [WIN]	Adobe Reader software is the free trusted standard for reliably viewing, printing, and annotating PDF documents. It's the only PDF file viewer that can open and interact with all types of PDF content, including forms and multimedia.	1	2	107.0 MB	
□		Autotask	CentraStage and Autotask are working hard to deliver a best of class integration of our two products. This version adds automated device synchronization from CentraStage to Autotask. Keep you Autotask accounts up-to-date with the latest audit of your ...	1	-	-	
□		Connectwise	ConnectWise Connector	1	-	-	
□		Mobile Device Management	Add support for iOS and Android devices. Purchase this extension to enable Mobile Device Management in your account. Before you can enrol any Apple iOS devices you will need to upload your Apple Push Notification Certificate. Instructions to do this ...	1	-	-	

◀ Previous Next ▶

- ✓ Steps: 2 customize and save



Please edit and/or save the copy of your component below

My Components	
All Components	5
Applications	1
Mobile Apps	0
Device Monitors	1
Network Monitors	0
Scripts	0

Component Groups

No groups defined

Component: Monitor: Copy of Acronis Backup and Recovery 10 monitor [WIN]

General

Category: Monitors

Name: Copy of Acronis Backup and Recovery 10 monito

Description: This component monitor will check and alert for: Acronis Backup and Recovery 10 not installed/not running, Not backed up in last X days. Check period is configurable when applying the monitor (default period=2 days)

Example: "This will install FireFox v4.0 on your computer."

UID: 3a68c4cb-e15b-4b83-8e08-91cc444fd18f

Security Level: 1 (Basic)

Profiles

● All profiles
○ Selected profiles

Script

Script: VBScript

```
'-----------------------------------------------------------------
'       Type:   Monitor
'       Desc:   Acronis Backup & Recovery 10 monitor
'       Input:
'       Output: CSMON_ResultMessage (String) - Summary of monitor scan
'       Alert:  If any of the checks fail
```

Timeout this script if not completed within: 60 (seconds)

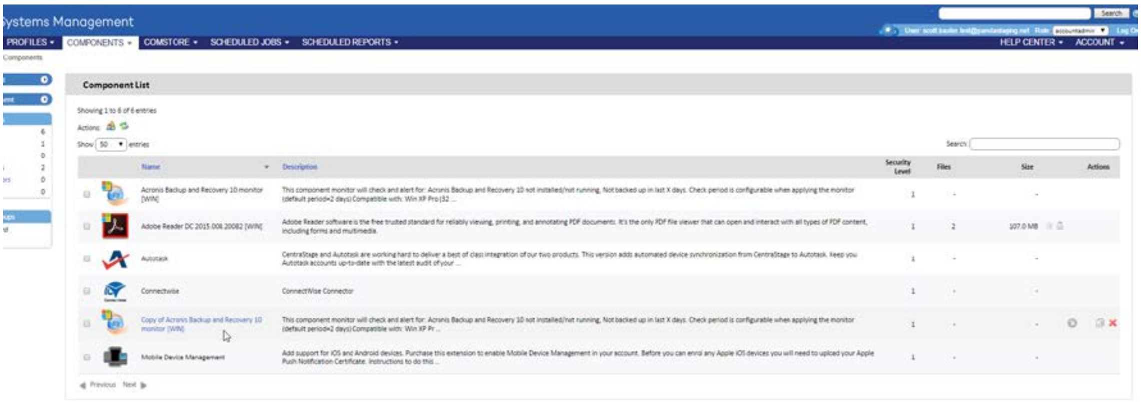
Variables

Input Variables

Name	Type	Default Value	Description
BACKUP__PERIOD	Value	2	Period (in days) that monitor will check. Default value is 2 days). An alert will trigger if a backup hasn't been performed within the last x days

Output Data

Name	Type	Description
CSMON_ResultMessage	String	



Component List

Showing 1 to 6 of 6 entries

Actions:

Show 50 entries

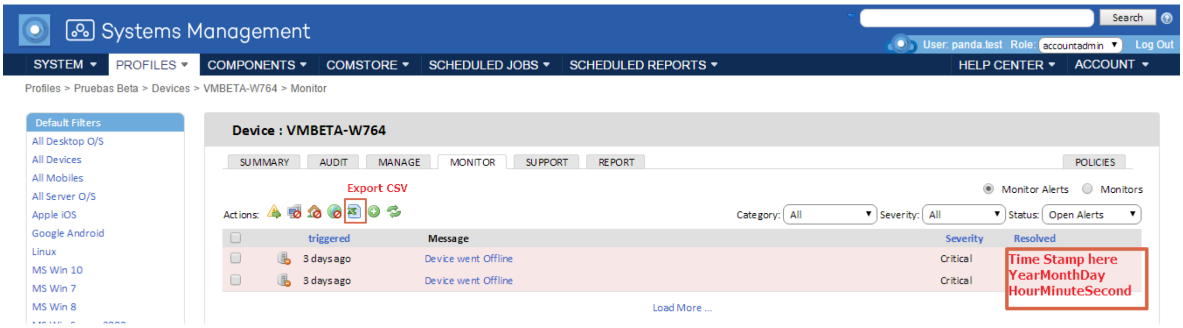
Search:

		Name	Description	Security Level	Files	Size	Actions
□		Acronis Backup and Recovery 10 monitor [WIN]	This component monitor will check and alert for: Acronis Backup and Recovery 10 not installed/not running, Not backed up in last X days. Check period is configurable when applying the monitor (default period=2 days) Compatible with: Win XP Pro (32 ...	1	-	-	
□		Adobe Reader DC 2015.008.20082 [WIN]	Adobe Reader software is the free trusted standard for reliably viewing, printing, and annotating PDF documents. It's the only PDF file viewer that can open and interact with all types of PDF content, including forms and multimedia.	1	2	107.0 MB	
□		Autotask	CentraStage and Autotask are working hard to deliver a best of class integration of our two products. This version adds automated device synchronization from CentraStage to Autotask. Keep you Autotask accounts up-to-date with the latest audit of your ...	1	-	-	
□		Connectwise	ConnectWise Connector	1	-	-	
□		Copy of Acronis Backup and Recovery 10 monitor [WIN]	This component monitor will check and alert for: Acronis Backup and Recovery 10 not installed/not running, Not backed up in last X days. Check period is configurable when applying the monitor (default period=2 days) Compatible with: Win XP Pr ...	1	-	-	
□		Mobile Device Management	Add support for iOS and Android devices. Purchase this extension to enable Mobile Device Management in your account. Before you can enrol any Apple iOS devices you will need to upload your Apple Push Notification Certificate. Instructions to do this ...	1	-	-	

◀ Previous Next ▶

Alerts CSV export additions

✓ The *“Alert Resolved time/date stamp”* is now available in the Alerts CSV export as well as displayed in the CSM Alerts list page.



Profiles > Pruebas Beta > Devices > VMBETA-W764 > Monitor

Device : VMBETA-W764

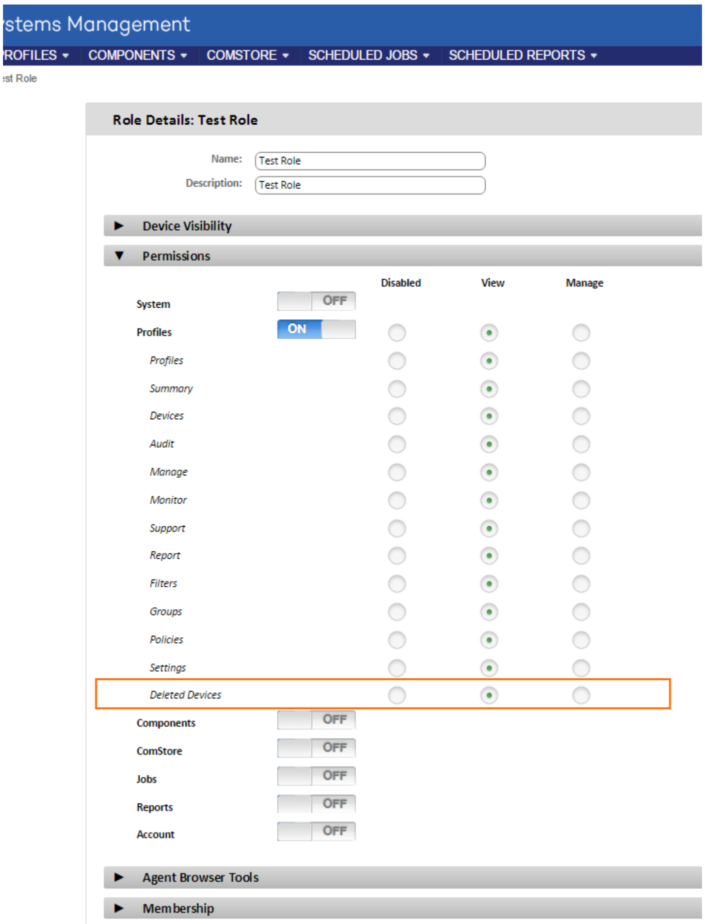
● Monitor Alerts ○ Monitors

Category: All Severity: All Status: Open Alerts

□	triggered	Message	Severity	Resolved
□	3 days ago	Device went Offline	Critical	Time Stamp here YearMonthDay HourMinuteSecond
□	3 days ago	Device went Offline	Critical	

Deleted devices user Access

Previously, only users with the Accountadmin role could view and manage the Deleted Devices page. Now a new permission option (see below) is added that covers View or manage rights for non-accountadmin users



Role Details: Test Role

Name: Test Role

Description: Test Role

		Disabled	View	Manage
System	OFF			
Profiles	ON	○	●	○
Profiles		○	●	○
Summary		○	●	○
Devices		○	●	○
Audit		○	●	○
Manage		○	●	○
Monitor		○	●	○
Support		○	●	○
Report		○	●	○
Filters		○	●	○
Groups		○	●	○
Policies		○	●	○
Settings		○	●	○
Deleted Devices		○	●	○
Components	OFF			
ComStore	OFF			
Jobs	OFF			
Reports	OFF			
Account	OFF			

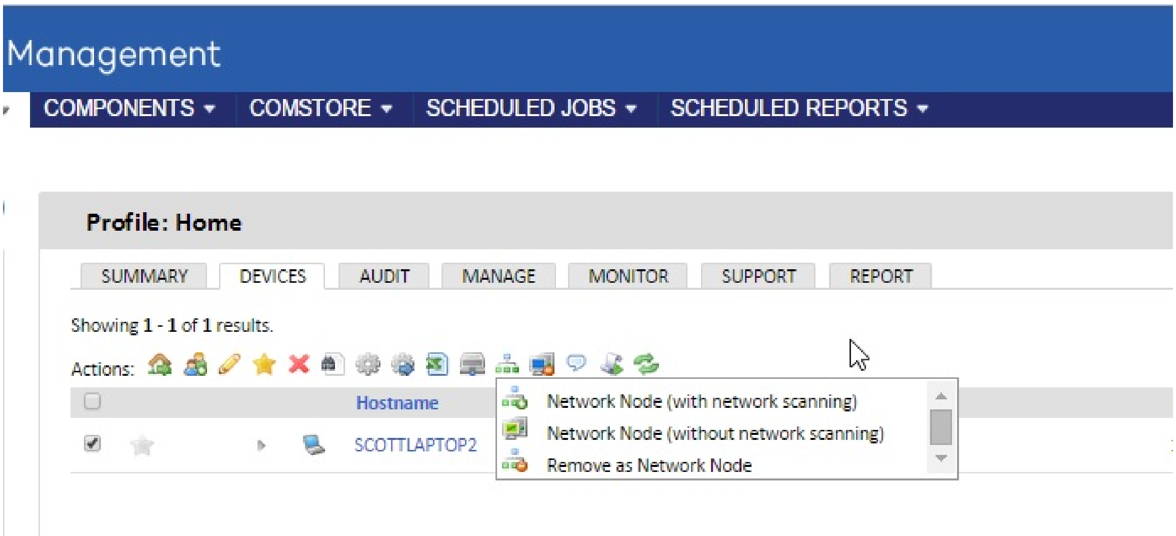
Net Assests scanning control

“Net Asset scanning control” refers to the change in behaviour of the Network Discovery function.

Previously, Network Nodes once nominated would perform a Network Scan automatically. We have now updated the options to be:

1. Network Node (with network scanning).
2. Network Node (without network scanning).
3. Remove as Network Node

Therefore, user can now elect to use a device as a Network Node for Network Device monitoring but without it performing a network scan each time it gets audited.



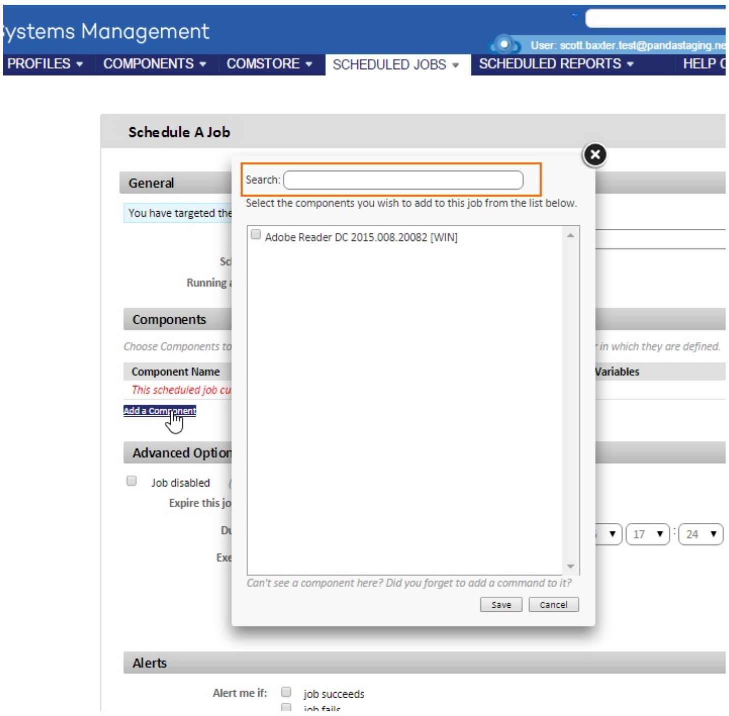
Showing 1 - 1 of 1 results.

☑ SCOTTLAPTOP2

- Network Node (with network scanning)
- Network Node (without network scanning)
- Remove as Network Node

Search bar in scheduled job component window

Added a search facility to the job scheduler's component selection function.



User: scott.baxter.test@pandastaging.ne

You have targeted the

Choose Components to ... in which they are defined.

This scheduled job cu

□ Job disabled

Alert me if: □ job succeeds □ job fails

Search:

Select the components you wish to add to this job from the list below.

□ Adobe Reader DC 2015.008.20082 [WIN]

Can't see a component here? Did you forget to add a command to it?

14.3. Issues fixed:

Summary
Fix non-transparent Mac agent icon
Fix formatting of incorrect email message
Fix missing printer model number
Fix policy columns rendering
Fix moved device error message
Fix device selection by filter issue
Fix software filter device results
Fix patch policy time schedule issue
Fix agent SNMP tool visibility
Fix missing patches filter logic
Fix SNMP not equal error message
Fix agent S3 proxy 403 and 404 errors
Fix filter results containing device with no operating system data
Fix patch title does not contain logic
Fix 2FA password reset issue
Fix security status filter results column sorting
Fix incorrect quick job window size
Fix search box paste behaviour issue
Fix agent branding user interaction icon
Fix agent download error code 1
Fix inconsistent alerts resulting from manually resolution
Fix patch policy severity logic
Fix alert re-raising issue
Fix subsequent agent OTP login issue
Fix date deleted field in deleted devices page
Fix monitoring policy email address deletion logic
Fix incorrect printer uptime
Fix agent event viewer field formatting
Fix incorrect agent custom field information
Drive information' tool is only partially hidden from customers with feature disabled
Fixed autotask setup issue which doesn't complete
Fixed Autotask wizard not working correctly if PSM language is German
Fixed Bad Request Internal Server Error
Fix for Patch Policy day of the week schedule

Remove redundant RDP enable from Agent Installer
Fixed commas in Accounts and Profiles names truncate in AT Integration mappings
Fixed incorrect message displayed when hiding or un-hiding Discovered Devices
Fixed mismatch in iOS download agent window
Fixed limited user roles / scheduled jobs visibility issue
Customer Health Summary Report to Include Java Update 40 & 45
Add CPU types to Pass/Fail criteria for Customer Health Summary report

15. February 25th, 2015 version (Systems Management Agent v1826)

15.1. Issues fixed:

2FA (Two-factor-authentication)

Bug fix to address an issue causing increased load on the platform by certain devices.

Added the new resources, including the resources for the Hungarian, the new language added.

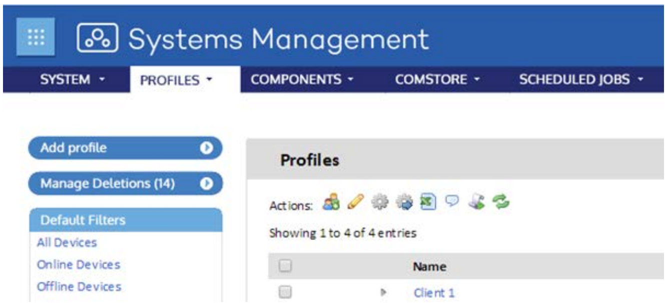
16. February 21st, 2015 version (Systems Management Agent v1824)

16.1. Added:

New Brand

New product name “Systems Management”

New look & feel. The new look & feel is associated to the new brand project we are addressing during this year.



New Policies for iOS

Restrictions: Over 50 configurations to control the usage of tablets and iOS mobiles managed by users so IT administrators will have a tight control about the apps the users can install and execute. Some examples of configurations the IT Admins will be able to control are

- **General:** Allow camera, Facetime, screenshots...

- **Application access:** Allow iTunes, Safari..
- **iCloud Services:** Allow iCloud back up, sync, photo stream…
- **Security and privacy**: Force encrypted backup
- **Content rating**: Allow movies, Apps, TV
- **Allow Airdrop**, App removal!

VPN / WIFI: Configuring connections iOS mobile devices: Being able to set the Wifi and VPN configuration automatically and in centralized way.

MDM: Passwords

- ✓ Password strength Set the minimum strength of passwords chosen by the user
- ✓ Maximum Password Age: Necessary for ISO standards etc
- ✓ Minimum Number of Characters
- ✓ Maximum Number of Failed Attempts: Wipe phone

SNMP monitoring of all kind of devices

- ✓ You will be able to manage new kind of SNMP devices (routers, switches, scanners etc)
- ✓ Managed through a Systems Management Designated Agent web console as SNMP Monitor
- ✓ No licenses required for the extra devices monitored through this feature

New remote installation

You will be able to select from the list of discovered devices in the Systems Management web console those who you want to install the agent automatically.

Greater control in Patch management

Ability to add individual patches to the policy created.

Device Approval

Before devices can use Systems Management policies, monitors etc they need to be approved by Administrator

Disabled by default

Static Broker

The broker communicates between the Server and agents in the network segments for certain tasks (keep-alive messages and certain communications used in the remote access)

If there is a specific high performance machine on the network segment that is always up you can define it as a static broker

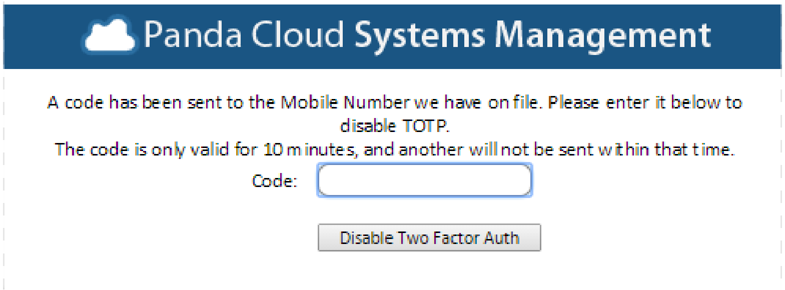
Additional device information

Disk usage over time (24 hours, 1 week and 1 month)

List of external USB devices connected to the device

Two Factor Authentication

In the case of emergency the new version you can disable two factor authentication using an SMS message (phone number on system)



A code has been sent to the Mobile Number we have on file. Please enter it below to disable TOTP.
The code is only valid for 10 minutes, and another will not be sent within that time.

New languages

Hungarian. The language is added in the console and in the agent

16.2. Issues fixed:

Issues fixed

Subject
Mac agent installs to Centrastage.app + CS icon
The option to "hide Start menu shortcuts" does not work
Branding on PCSM for MAC
Fehlermeldung Rolle/Profil PCSM
Agent Hide Policy does not hide start menu shortcuts
DD: PCSM - Accounts
Reports
PCSM MDM Application high battery usage on HTC One (Android)
PCSM MDM "Show Devices on MAP" missing in IE
Agent Hide Policy does not hide start menu shortcuts

Hardware audit not showing information
Download CVS file with information about Energy Usage shows no information
Software monitor with wildcarts doesn't work
Main account active despite being inactivated in the PCSM console.
PCSM - Fragen zum Produkt
Remote take-over icons lost
It's not possible to search machines through the serial number option within search.
Inventory Age XL and PDF Report Returns Subquery Error
Components in PCSM Console Will Not Delete
kan geen verbinding met telefoon maken
PCSM - Fragen zum Produkt
La búsqueda de ComStore falla
Cannot connect to PCSM client on mac
Maximum charachter size exceeded when trying to add a printer
The following componet can't be updated
Inventory Age report has bugs
Display problem PCSM in IE9
PCSM Probleme mit SNMP
PCSM Probleme mit Reports (Health & Profile Health)
Cannot delete 1 user of demo account to can create it in the final account

Mail report secduled job
Customer Health Summary does not show correct information regarding Antivirus
PCSM indicates there are still updates to install, yet Windows says everything is up to date
Pcsm agent installation problem
Error creating detailed computer audit report
OS X agent will not start
"Connect to" toolbox dissapears from profile device view when mobile device is present.

17. April 8th, 2014 version (Systems Management Agent v1803)

17.1. Added:

2FA (Two-factor-authentication)

2 steps for accessing to Panda Cloud Systems Management web console.

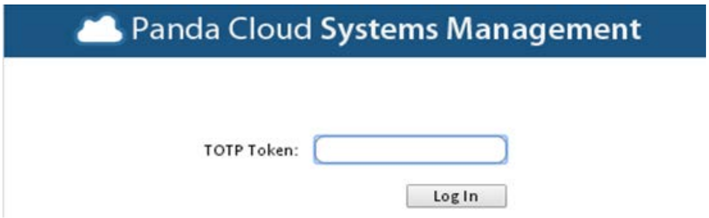
Deactivated by default

It is activated by user, NOT by account

Authentication is made using Mobiles/Tablets with apps such as Google Authenticator

Once 2FA is activated

1. Logging in Panda Cloud Login Page
2. Introduce the TOTP (Time-based One-time Password Algorithm) code



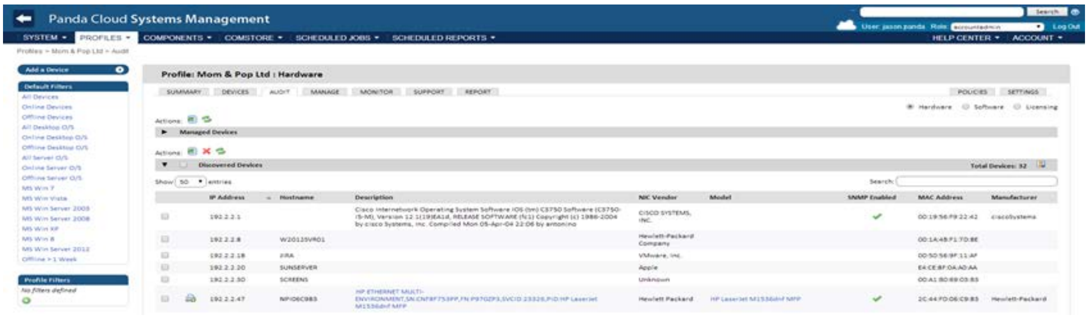
SNMP for printers

Printers discovered can now be managed within the Systems Management

Printers added to the account charged as a managed device

Gives customers additional control over their environment

Monitor Supply levels



Profile: Mom & Pop Ltd : Hardware

		IP Address	Hostname	Description	NIC Vendor	Model	SNMP Enabled	MAC Address	Manufacturer
□		192.2.2.1		Cisco Internetwork Operating System Software IOS (tm) C3750 Software (C3750-I5-M), Version 12.1(19)EA1d, RELEASE SOFTWARE (fc1) Copyright (c) 1986-2004 by cisco Systems, Inc. Compiled Mon 05-Apr-04 22:06 by antonino	CISCO SYSTEMS, INC.		✓	00:19:56:F9:22:42	ciscoSystems
□		192.2.2.8	W2012SVR01		Hewlett-Packard Company			00:1A:4B:F1:7D:8E	
□		192.2.2.18	JIRA		VMware, Inc.			00:50:56:9F:11:AF	
□		192.2.2.20	SUNSERVER		Apple			E4:CE:8F:0A:AD:AA	
□		192.2.2.30	SCREENS		Unknown			00:A1:B0:69:03:B3	
□	🖶	192.2.2.47	NPI06C9B3	HP ETHERNET MULTI-ENVIRONMENT,SN:CNF8F753PP,FN:P970ZP3,SVCID:23326,PID:HP LaserJet M1536dnf MFP	Hewlett Packard	HP LaserJet M1536dnf MFP	✓	2C:44:FD:06:C9:B3	Hewlett-Packard

Linux

Further visibility of estate with the introduction of the Linux agent

Red Hat and Ubuntu supported. Further details in the datasheet

MAC

Deployment, scripting and application installations now supported

User activity logging

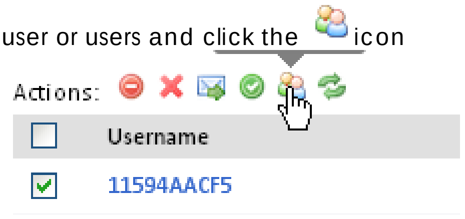
It will be recorded all actions made (both in the Systems Management and the agent) of all users in the account. This information is then made available to search, filter on and export as required.

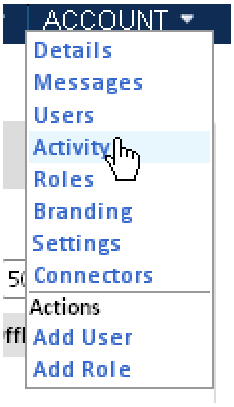
To access user activity logging your account must be Account Admin.

Valuable tool for Account Admins for tracking user actions

It is accessed from the Account Menu, selecting Activity

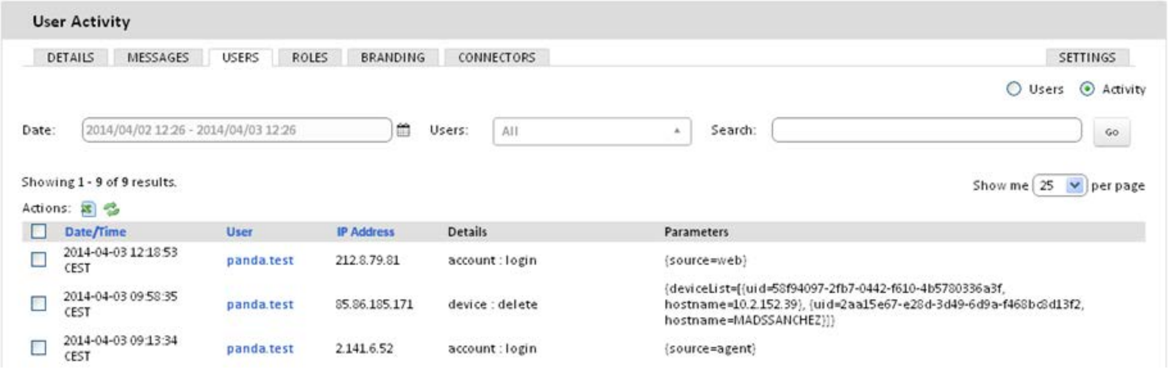
It is also accessed from the Account menu select Users and then select the desired user or users and click the icon





The following information is logged by the platform and can queried using the search bar.

1. **Date/Time**: Time stamp
2. **User**: The user performing the activity. Clicking on the user hyperlink will take you to the user configuration window.
3. **IP Address**: Public IP address of the users site.
4. **Details**: An overview of the area accessed. This is formatted - **area:action**. For example, **component:create** or **agent:rto**
5. **Parameters**: In-depth details of the action made. This will enhance the search functionality.



○ Users ● Activity

Date: 2014/04/02 12:26 - 2014/04/03 12:26 Users: All Search:

Showing 1 - 9 of 9 results.

Show me 25 per page

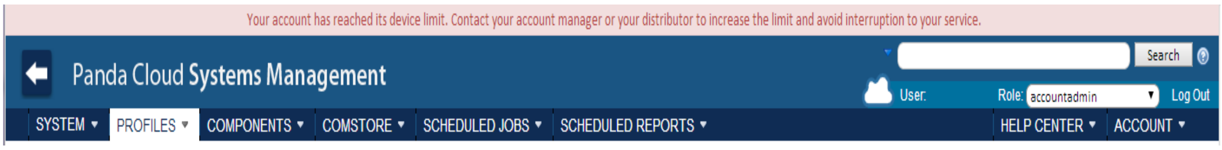
□	Date/Time	User	IP Address	Details	Parameters
□	2014-04-03 12:18:53 CEST	panda.test	212.8.79.81	account : login	{source=web}
□	2014-04-03 09:58:35 CEST	panda.test	85.86.185.171	device : delete	{deviceList=[{uid=58f94097-2fb7-0442-f610-4b5780336a3f, hostname=10.2.152.39}, {uid=2aa15e67-e28d-3d49-6d9a-f468bc8d13f2, hostname=MADSSANCHEZ}]}
□	2014-04-03 09:13:34 CEST	panda.test	2.141.6.52	account : login	{source=agent}

Further details about 2FA, SNMP for printers and Linux in the Systems Management guide.

17.2. Changed:

New license control:

Customers will now be warned in the Web Console when their device limit is reached.


Your account has reached its device limit. Contact your account manager or your distributor to increase the limit and avoid interruption to your service.

A 10% buffer has been added to ensure connectivity not lost. A client with 100 licenses will be able to install the Systems Management agent in 110 devices.

New agents added above the limit (number of licenses acquired + 10%) will not connect and will not be shown in the Systems Management console until new licenses are acquired.

Agents already in account will not lose connection.

All the devices in an offline state due to the lack of licenses will move automatically to an online state once the client acquires the necessary licenses

17.3. Issues fixed:

Platform improvements

Potential issues running jobs and pushing policies on Systems Management are fixed. These should not happen with the new version.

Issues fixed with the new version

DESCRIPTION OF THE ISSUES FIXED WITH THE NEW VERSION
Wake-On-LAN doesn't work

CagService.exe resource consumption
System filter isn't showing devices it should show
Email is supposed to go to all account admins, which at present is not working.
Special characters not showing fine in console.
Energy Usage Report - Not Working
Not able to add an Additional recipient when the email address contains the "-" symbol
Grey icon tray. Number of machines higher that licenses.
Cagservice memory consuption
Changes from ON & OFF from system policy does not reflect to Profile Policy.
If you try to create a Software Package, the Window to define the software stays in the Background
Modifying Scheduled job shows an error
There is no option of modifying the auto resolution time for a status monitor

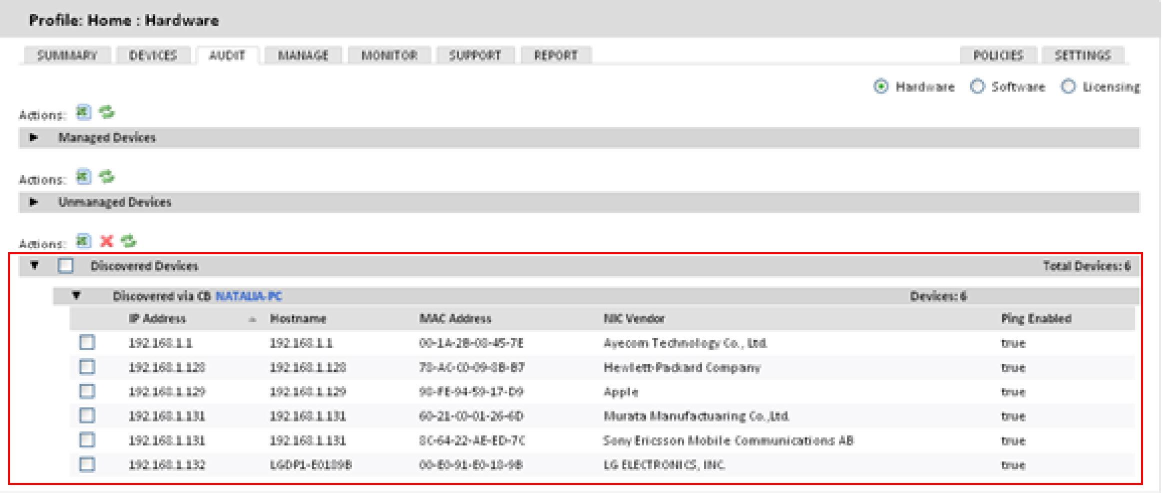
All cases solved with the new version are marked In Salesforce. For further details, please contact support..

18. October 6th, 2013 version

18.1. Added:

Network Device Discovery. Further information about your supported Network environment is now available through the Systems Management Network Device Discovery feature. All network devices on your LAN will now be found and recorded in each Profile. This information is then available as a CSV export report.

The list of all other network devices discovered on it's local area network will be listed under Discovered Devices in the Systems Management console.

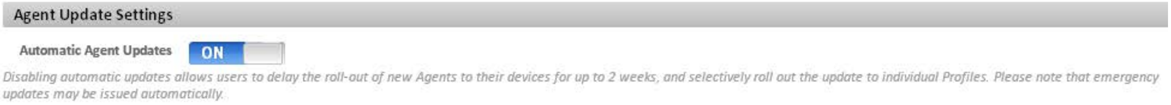


	IP Address	Hostname	MAC Address	NIC Vendor	Ping Enabled
□	192.168.1.1	192.168.1.1	00-1A-2B-08-45-7E	Ayecom Technology Co., Ltd.	true
□	192.168.1.128	192.168.1.128	78-AC-C0-09-8B-B7	Hewlett-Packard Company	true
□	192.168.1.129	192.168.1.129	90-FE-94-59-17-D9	Apple	true
□	192.168.1.131	192.168.1.131	60-21-C0-01-26-6D	Murata Manufacturing Co.,Ltd.	true
□	192.168.1.131	192.168.1.131	8C-64-22-AE-ED-7C	Sony Ericsson Mobile Communications AB	true
□	192.168.1.132	LGDP1-E0189B	00-E0-91-E0-18-9B	LG ELECTRONICS, INC.	true

We will automatically discover devices with an IP address on the LAN and are not presently being managed so we can deploy the Systems Management agent on them.

Agent Updates. You can now control the release of the Systems Management Agent updates to your devices via the Systems Management console. Individual Profiles can be set to receive the update before you release the agent to all Profiles.

The agent updates can be configured in Account / Settings



Automatic Agent Updates: ON

Disabling automatic updates allows users to delay the roll-out of new Agents to their devices for up to 2 weeks, and selectively roll out the update to individual Profiles. Please note that emergency updates may be issued automatically.

Disabling automatic updates allows users to delay the roll-out of new Agents to their devices for up to 2 weeks, and selectively roll out the update to individual Profiles.

NLA support. New supported feature for Agent Browser RDP connections

Network Level Authentication (NLA) is a technology used in Remote Desktop Services (RDP Server) or Remote Desktop Connection (RDP Client) that requires the connecting user to authenticate themselves before a session is established with the server.

18.2. Changed:

When we delete an account, all the agents of the account will be uninstalled automatically losing all settings:

1. Commercial accounts are deleted 90 days after expiring all the licenses
2. Trial accounts are deleted 30 days after the trial expiration date

18.3. Issues fixed:

CEN-239 – Patch Management: It doesn’t work applying the update: KB976932 in the computers - Windows 7 Service Pack 1.
CEN-261 –Error adding an additional email address to a Scheduled Job previously created.
CEN-370 –Error when clicking on any application shown in ComStore, it only occurs if the console is in French.
CEN-399 – When listing devices using the links on the Summary tab, it displays an error indicating that no devices have been selected to launch Scheduled Jobs or audits on the list of devices displayed.
CEN-410 - When sorting by column hostname, the devices appear messy if devices are offline.

CEN-111. Issues with the Patch management information in a wrong language

This feature is now dependant on the language selected in the Systems Management. It also depends heavily on device audits to harvest the patch information for the languages. Therefore, if you only have an English and Spanish PC’s you will only see English and Spanish patch info. When audits come in from other language device these will be added to the DB and shown in the Systems Management to the selected language.

If there is no patch available for a certain language it will default to English.

The languages supported are the one supported by the Systems Management:

- English
- Spanish
- French
- Italian
- Dutch
- Portuguese
- Swedish

19. December 10th, 2013 version

19.1. Added:

MDM. Further information download the Guide for Partners and IT Administrators that can be downloaded from here

Our URL for the MDM push server will be here: Systems Management-mdm.pandasecurity.com

19.2. Issues fixed:

CEN- 164 - Systems Management Does Not Execute Remote Powershell Scripts Correctly. Path such as "Documents and settings" were not handled correctly (SalesForce 03673033 ; 03646453)
CEN- 242 -- Cannot create new Licensing Software packages (SF 03746389; 03716868)
CEN- 440 -- Exporting Missing Patches to CSV Has Headers Only, No Data (SF 03730775)
CEN- 349 -- System filter isn't showing devices it should show (SF 03738864; 03733038)
CEN- 137 – Error sending some specific errors (SF 03758707)