Table of Contents

1. May 21st, 2019. 7.0 version (Systems Management Server v409, Agent v2074, Console v7.0.0.10) ................................................................. 6
   1.1. Added (summary): ........................................................................ 6
   1.2. Added (detail): ........................................................................... 6
       General......................................................................................... 6
       Monitoring.................................................................................. 7
       Management............................................................................... 7
       Reporting..................................................................................... 8
       Audit............................................................................................ 8
       Remote Support........................................................................... 9
       Jobs and components................................................................. 9
       Agent......................................................................................... 9
   1.3. Issues fixed.................................................................................. 10
2. November 21st, 2018. 6.1.0 version (Systems Management Server v398, Agent v2052, Console v6.1.0.1953) ...................................................... 11
   2.1. Added (summary): ...................................................................... 11
   2.2. Added (detail): .......................................................................... 11
       2.2.1. Reporting............................................................................. 11
       2.2.2. Antivirus management .......................................................... 13
       2.2.3. Patch Management............................................................... 15
       2.2.4. Device Summary and Device Audit redesign ......................... 16
       2.2.5. Jobs and components......................................................... 17
       2.2.6. Network control................................................................. 17
       2.2.7. Other enhancements and requirements.................................. 17
   2.3. Issues fixed.................................................................................. 17
3. February 13th, 2018. 5.5.0 version (Systems Management Server v4.6.351, Agent v2017, Console v5.5.0.1808) .................................................. 18
   3.1. Added (summary): ...................................................................... 18
   3.2. Added (detail): .......................................................................... 18
       3.2.1. Discovery............................................................................. 18
       3.2.2. Monitoring.......................................................................... 19
       3.2.3. Network Monitoring.......................................................... 21
       3.2.4. Network Control............................................................... 23
       3.2.5. COMSTORE...................................................................... 23
   3.3. Issues fixed.................................................................................. 23
   4.1. Added ........................................................................................ 24
   4.2. Issues fixed.................................................................................. 24
5.1. Added (summary): ........................................................................................................25
5.2. Added (detail): ...........................................................................................................25
  5.2.1. Patch Management .................................................................................................25
  5.2.2. Support ..................................................................................................................27
  5.2.3. Reporting ...............................................................................................................28
  5.2.4. Other enhancements and fixes ................................................................................28
5.3. Issues fixed ..................................................................................................................28
  6.1. Added (summary): ....................................................................................................29
  6.2. Added (detail): .........................................................................................................29
    6.2.1. Monitoring ............................................................................................................30
    6.2.2. Audit .......................................................................................................................31
    6.2.3. Support ..................................................................................................................32
    6.2.4. Reporting ..............................................................................................................33
    6.2.5. Other enhancements and fixes ..............................................................................34
  6.3. Issues fixed ................................................................................................................34
7. July 12nd, 2016-1 version (Systems Management Server v4.6.281, Agent v1887, Console v4.6.1438) ............................................................34
  7.1. Issues fixed ..................................................................................................................34
8. March 8th, 2016 version (Systems Management Server v4.6.265, Agent v1863, Console v4.6.1340) .................................................................35
  8.1. Added (summary): ....................................................................................................35
  8.2. Added (detail): .........................................................................................................35
  8.3. Issues fixed ................................................................................................................37
  8.4. Known issues ............................................................................................................37
  9.1. Added: .......................................................................................................................38
10. September 23th, 2015 version (Systems Management Agent v1839) ..........39
  10.1. Added (summary): ..................................................................................................39
  10.2. Added (detail): .......................................................................................................39
11. February 25th, 2015 version (Systems Management Agent v1826) ......45
  11.1. Issues fixed: ............................................................................................................45
12. February 21st, 2015 version (Systems Management Agent v1824) ......45
  12.1. Added: .....................................................................................................................45
13. April 8th, 2014 version (Systems Management Agent v1803) ..........47
  13.1. Added: .....................................................................................................................47
  13.2. Changed: .................................................................................................................49
  13.3. Issues fixed: .............................................................................................................49
14. October 6th, 2013 version .................................................................51
  14.1. Added: .....................................................................................................................51
  14.2. Changed: .................................................................................................................52

4 Release Notes
1. May 21st, 2019. 7.0 version (Systems Management Server v409, Agent v2074, Console v7.0.0.10)

1.1. 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.

1.2. 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.
1.3. Issues fixed

- 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.
- Fixed: 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 formatted.
- 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.
2. November 21st, 2018. 6.1.0 version (Systems Management Server v398, Agent v2052, Console v6.1.0.1953)

2.1. 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)

2.2. Added (detail):

2.2.1. 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.
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.
• 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.

<table>
<thead>
<tr>
<th>Services</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Management</td>
<td>97%</td>
</tr>
<tr>
<td>Monitoring</td>
<td>83%</td>
</tr>
<tr>
<td>Patch Management</td>
<td>4%</td>
</tr>
<tr>
<td>Antivirus</td>
<td>40%</td>
</tr>
<tr>
<td>Average Score</td>
<td>56%</td>
</tr>
</tbody>
</table>

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.

2.2.2. 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.

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:

<table>
<thead>
<tr>
<th>Existing Filter</th>
<th>Migrated Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Virus</td>
<td>Anti-Virus Status</td>
</tr>
<tr>
<td>Enabled</td>
<td>Running &amp; Up-to-Date</td>
</tr>
<tr>
<td>Disabled</td>
<td>Not Running</td>
</tr>
<tr>
<td>Security Management Status</td>
<td>Anti-Virus Status</td>
</tr>
<tr>
<td>Active Threats</td>
<td>Running &amp; Up To Date</td>
</tr>
<tr>
<td>Installed &amp; Active</td>
<td>Running &amp; Not Up to Date</td>
</tr>
<tr>
<td>Installed, not Active</td>
<td>Not Running</td>
</tr>
<tr>
<td>Needs Update</td>
<td>No valid license</td>
</tr>
<tr>
<td>reboot Required</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Users are advised to review existing antivirus-related filters to ensure the migration does not produce undesirable results upon release.
2.2.3. 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.

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

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Patches Not Approved</th>
<th>Patches Approved Pending</th>
<th>Patches Installed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3</td>
<td></td>
<td>182</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td></td>
<td>204</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td></td>
<td>168</td>
</tr>
<tr>
<td></td>
<td>54</td>
<td></td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td></td>
<td>154</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

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.

2.2.4. 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.
2.2.5. 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.

2.2.6. 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.

2.2.7. 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.

2.3. Issues fixed

- 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).
- 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.

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

3.1. 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.

3.2. Added (detail):

3.2.1. 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 onboard 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.

![Network Discovery Routine](image)

### 3.2.2. 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](image)
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.
Event Log Monitor
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%.

3.2.3. 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.
3.2.4. 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 use a Network Node to connect to the device and use the integrated version of PuTTY to create a seamless experience.

**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.

3.2.5. 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.

3.3. Issues fixed
- Servers online are shown as offline
- The manage tab takes more than 2 minutes to be loaded
- The manage tab takes 30 sec to load with just 15 devices

4.1. 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.

4.2. Issues fixed

- 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 the 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.

5.1. 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

5.2. Added (detail):

5.2.1. 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.

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.

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.

---

**5.2.2. 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.
5.2.3. 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.

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.

5.2.4. 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.

5.3. Issues fixed
- AV Health Report showing wrong av detection.
- Permissions to view the system policies, but in the moment you delete one system policy from the profile you delete it from system too.

6.1. 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

6.2. 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:

<table>
<thead>
<tr>
<th>Old term</th>
<th>New term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account (tab)</td>
<td>Setup</td>
</tr>
<tr>
<td>Account Admin, accountadmin</td>
<td>Administrator</td>
</tr>
<tr>
<td>CSM, CentraStage Server Manager</td>
<td>Web Portal</td>
</tr>
<tr>
<td>Custom Label, Custom Field</td>
<td>User-Defined Field</td>
</tr>
<tr>
<td>Default Filter</td>
<td>Device Filter</td>
</tr>
<tr>
<td>Details (Account &gt; Details tab)</td>
<td>My Info</td>
</tr>
<tr>
<td>Packages (tab)</td>
<td>Billing</td>
</tr>
<tr>
<td>Product Allocation Code</td>
<td>Material Code</td>
</tr>
<tr>
<td>Profile</td>
<td>Site</td>
</tr>
<tr>
<td>Profile Device Group</td>
<td>Site Device Group</td>
</tr>
<tr>
<td>Profile Filter</td>
<td>Site Device Filter</td>
</tr>
<tr>
<td>Role Security Level</td>
<td>Security Level</td>
</tr>
<tr>
<td>Severity</td>
<td>Component Level</td>
</tr>
<tr>
<td>System (tab)</td>
<td>Priority</td>
</tr>
<tr>
<td>System Device Group</td>
<td>Account</td>
</tr>
<tr>
<td>System Filter</td>
<td>Device Group</td>
</tr>
<tr>
<td>System Profile Group</td>
<td>Custom Device Filter</td>
</tr>
<tr>
<td>System Profile Group</td>
<td>Site Group</td>
</tr>
</tbody>
</table>
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!

6.2.1. 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.
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.

6.2.2. 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.
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.

6.2.3. 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.
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.

6.2.4. 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.
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.

6.2.5. 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

6.3. Issues fixed

- 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.

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

7.1. Issues fixed

- Dates are not sorted out when you press sort by date.
- System Filter Criteria not functioning correctly
8. March 8th, 2016 version (Systems Management Server v4.6.265, Agent v1863, Console v4.6.1340)

8.1. 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

8.2. 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>What to Enter</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Enter the IP address of your device</td>
</tr>
<tr>
<td>Name</td>
<td>Give your device a meaningful name</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a meaningful description</td>
</tr>
</tbody>
</table>
Enter the name of the manufacturer of your device

Enter the model of your device

Enter the ESXi credentials of your device. For more information, refer to the ESXi Credentials section in Account Settings and Profile Settings

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 credentials specified in Account Settings unless this option is disabled in Profile 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 device responds, it will be listed as an ESXi device in the discovered devices list.

Once your ESXi devices have been added as managed devices to your account, basic data can be seen at-a-glance in the Systems Management 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:

<table>
<thead>
<tr>
<th>Monitor Type</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi CPU Monitor</td>
<td>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.</td>
</tr>
<tr>
<td>ESXi Memory Monitor</td>
<td>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.</td>
</tr>
<tr>
<td>ESXi Data Store Monitor</td>
<td>Similarly to the “Disk Usage Monitor” 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.</td>
</tr>
<tr>
<td>ESXi Temperature Sensor Monitor</td>
<td>This monitor allows you to set up an alert if the temperature sensors on the ESXi host exceed a certain threshold.</td>
</tr>
</tbody>
</table>

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 synchronized. (called “round-trip” ticketing).

**8.3. Issues fixed**

- 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.

**8.4. 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.

9.1. Added:

**Support to the new OSX version called “El Capitan”**
The new OSX version (“El Capitan”) is now supported.

**New Patch Management Scheduler that**
It allows for more flexible patch deployment. See image below with the new options available

![Update patch policy](image)

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

10.1. 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

10.2. 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:
Managed devices view:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Hostname</th>
<th>Description</th>
<th>NIC Vendor</th>
<th>Model</th>
<th>SNMP Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.60</td>
<td></td>
<td>Hewlett-Packard Company</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.10.10.80</td>
<td>BRN001BM934EA84</td>
<td>BROTHER INDUSTRIES, LTD.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.10.10.113</td>
<td>DEVELOPMENT</td>
<td>GIGA-BYTE TECHNOLOGY CO., LTD.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.10.10.254</td>
<td></td>
<td>OSPCO SYSTEMS, INC.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.2.2.195</td>
<td></td>
<td>Hewlett-Packard Company</td>
<td>HP LaserJet Professional P1102w</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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:
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.

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
Steps: 2 customize and save
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.

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.

Net Assets 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).
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.

Search bar in scheduled job component window

Added a search facility to the job scheduler's component selection function.
11. February 25th, 2015 version (Systems Management Agent v1826)

11.1. 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.

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

12.1. 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)
New languages
Hungarian. The language is added in the console and in the agent

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

13.1. 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
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

Actions: Uncheck Mark

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 as `area:action`. For example, `component:create` or `agent:to`
5. **Parameters**: In-depth details of the action made. This will enhance the search functionality.

The following information is logged by the platform and can queried using the search bar.
Further details about 2FA, SNMP for printers and Linux in the Systems Management guide.

13.2. Changed:

**New license control:**

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

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.

13.3. 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
<table>
<thead>
<tr>
<th>Issue Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CagService.exe resource consumption</td>
</tr>
<tr>
<td>System filter isn’t showing devices it should show</td>
</tr>
<tr>
<td>Email is supposed to go to all account admins, which at present is not working.</td>
</tr>
<tr>
<td>Special characters not showing fine in console.</td>
</tr>
<tr>
<td>Energy Usage Report - Not Working</td>
</tr>
<tr>
<td>Not able to add an Additional recipient when the email address contains the &quot;-&quot; symbol</td>
</tr>
<tr>
<td>Grey icon tray. Number of machines higher that licenses.</td>
</tr>
<tr>
<td>Cagservice memory consupntion</td>
</tr>
<tr>
<td>Changes from ON &amp; OFF from system policy does not reflect to Profile Policy.</td>
</tr>
<tr>
<td>If you try to create a Software Package, the Window to define the software stays in the Background</td>
</tr>
<tr>
<td>Modifying Scheduled job shows an error</td>
</tr>
<tr>
<td>There is no option of modifying the auto resolution time for a status monitor</td>
</tr>
</tbody>
</table>
14. October 6th, 2013 version

14.1. 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.

![Profile Home: Hardware](image)

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

![Agent Update Settings](image)

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.
14.2. 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

14.3. Issues fixed:

Patch Management: It doesn’t work applying the update: KB976932 in the computers - Windows 7 Service Pack 1.
Error adding an additional email address to a Scheduled Job previously created.
Error when clicking on any application shown in ComStore, it only occurs if the console is in French.
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.
When sorting by column hostname, the devices appear messy if devices are offline.

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
15. December 10th, 2013 version

15.1. 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

15.2. Issues fixed:

- Systems Management Does Not Execute Remote Powershell Scripts Correctly. Path such as “Documents and settings” were not handled correctly
- Cannot create new Licensing Software packages
- Exporting Missing Patches to CSV Has Headers Only, No Data
- System filter isn’t showing devices it should show
- Error sending some specific errors