Introduction 3
Availability 3
System Requirements Updated (.NET 4 Framework) 3
Discovery 4
Network Discovery 4
Additional Subnets 4
Monitoring 5
New Monitoring Core 5
Real-Time Monitoring Status 5
WMI Monitor 5
Windows Performance Monitor 5
Patch Failure Monitor 5
Ping Monitoring 5
Event Log Monitor 6
Disk Usage Monitor 6
Security Center Monitor 6
Component Monitor 6
UI Enhancements 6
Network Monitoring 7
Network Monitoring Redesign 7
SNMP Monitoring 7
Offline Monitoring 7
Network Device Audit 8
Migration of Old Network Monitoring Configurations 8
Network Control 9
SSH/Telnet 9
HTTP/HTTPS 9
Custom Connections 9
Autotask Integration 10
Remote Control Activity to PSA Ticket 10
Tickets 10
Configuration Items 10
ComStore 11
Monitoring Policies 11
Auto-Update of Components 11
Other Enhancements 11
Introduction
Our 2017-1 release is the next major milestone in making AEM the most powerful, scalable and easiest to use RMM product in the market. Among other things, this release will significantly improve our Monitoring and Network Management capabilities.

The release includes:

- **Refactor of 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, can now assign monitoring using policies and can even remote control these devices.
- **Much improved experience working with Autotask PSA tickets.** We now also capture Remote Control activity in PSA tickets and sync more asset data.

Availability
We will release 2017-1 in the first half of 2017. Release announcements will be made at status.autotask.net and our AEM community.

System Requirements Updated (.NET 4 Framework)
As of 2017-1, the AEM Agent will be built on version 4 of the .NET Framework as opposed to version 2 for previous builds.

This change has massive benefits for our customers. Our new Monitoring Framework, Network Control functionality and Agent Logging Framework are all made possible by having the Agents run on version 4 of the .NET framework.

This will require Windows endpoints to have version 4.0.3 or higher of the .NET Framework installed in order to update to this new Agent or permit its fresh installation. Version 4 of the .NET Framework is supported from Windows XP SP3 and Windows 2003 SP2; customers can filter devices using the new .NET Framework Version field in the web portal to find devices that will need the .NET Framework component run on them. Devices still running version 2 of the .NET Framework after the update to 2017-1 will retain a degree of functionality, but support for such devices will not be provided.

April 2017 marks the 3-year anniversary of Microsoft’s end-of-life of Windows XP and Windows 2003 Server has been end-of-life since July 2015. Updates are no longer issued for these platforms; running them in a business environment is considered a high risk to security. We strongly encourage any customer still running these platforms to migrate away from them.
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.

Image 1: New Network Audit will work across multiple subnets
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.

*Image 2: Monitor Status on the Device Summary page*

**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.

Image 3: The new Event log monitor will have many new 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 AEM 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.

UI Enhancements
We’ve made many smaller useful enhancements to the UI. 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%.
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 AEM and can be changed from the device listing and device summary.

Other Managed 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 AEM 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 AEM 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 AEM 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 AEM 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](image)

*Image 4: Audit information for all SNMP devices*

Migration of Old Network Monitoring Configurations
Network Monitor Components will be removed from the ComStore and the Components listings. Existing Network Monitor Components and Network Offline Monitors that have been applied to devices will persist as SNMP Monitors. We will use existing monitoring data to retroactively assign pre-existing devices to Network Nodes located in the same site (provided any exist).

We encourage our customers to convert these monitors to policies at a later stage since managing a single policy is much easier than managing many individual monitors.
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, AEM 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, an AEM user can set up a browser connection to any managed device in AEM. 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 AEM 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.

Image 5: The Agent Browser can open an SSH session directly to any Network Device
Autotask Integration

Remote Control Activity to PSA Ticket
The activity data from a typical Remote Control session contains a wealth of immensely useful business information. AEM will now store this activity in Autotask PSA after completing a Remote Control session. Directly after closing a connection with a remote device, engineers can decide to store all the Remote Control activity in one or more PSA tickets. The engineer can choose what activity will be stored in the Hidden Notes of the ticket. The activity can also be used to quickly create a new PSA ticket directly from the Agent Browser.

![Remote Control activity can be stored in PSA tickets](image)

Tickets
We have made it much easier for engineers to work with PSA tickets directly from AEM. In multiple places a “New Ticket” button has been added to AEM. Creating a new ticket from AEM will now directly open a ticket for the right entity (Account/Configuration Item) in PSA.

AEM will also open tickets directly in PSA instead of using its own ticket forms. This will create a more seamless experience for engineers since all the fields, workflows and security settings that are configured in the PSA will now also be in effect when working from AEM.

Configuration Items
More AEM device data in Autotask allows for better reports, widgets and decisions. AEM will now sync the Last User and Approved Pending Patches to PSA.

In addition AEM users can quickly jump from an AEM device to the PSA Configuration Item. A new button will be present from any device that links directly to the Configuration Item. We will also show the current sync status for that device.
ComStore

Monitoring Policies
A new category will be made available in the ComStore for Monitoring Policies. We will provide “best-practice” policies for monitoring devices using AEM. 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.

Auto-Update of Components
Components downloaded from the ComStore can now be set to auto-update. This will significantly improve the workflow when providing third-party party patch management based on AEM components.

Other Enhancements

• Users can be set to expire automatically for improved security and better management of temporary users
• AEM will clearly show when policies are disabled on a device at a higher level (Site or Account) and can’t be overwritten on the Device Level.
• The Last Reboot value will now be audited at Agent check-in instead of daily audit to increase the accuracy.
• The Agent has a new logging framework that will make troubleshooting much easier and much more detail about the exceptions will be present at the endpoint. Exceptions will now also be sent to our platform so our team can proactively see and solve Agent issues.