

Autotask® AEM Priorities 2017

v1.05 - Updated December 13, 2016



<i>Introduction</i>	3
<i>Disclaimer</i>	3
Monitoring	4
<i>Real-Time Monitor Status</i>	4
<i>Windows Performance Monitoring</i>	4
<i>Event Log Monitoring</i>	5
Network Monitoring	6
<i>Enhanced Network Discovery</i>	6
<i>Network Device Audit</i>	6
<i>SNMP Monitoring Policies</i>	7
<i>Ping Monitoring</i>	7
Network Device Control	8
Apple macOS Agent Browser	9
Reporting	10
<i>Improved Scheduler</i>	10
<i>Increased Flexibility of Existing Reports</i>	10
Autotask Integration	11
<i>Remote Control Activity to PSA Ticket</i>	11
<i>Admin Ticket Experience</i>	11
Public API	11

Introduction

This document outlines the development priorities for Autotask Endpoint Management in 2017.

2016 was an amazing year for Autotask Endpoint Management. This year we developed many great new features; to name a few:

- Unified platform experience with Autotask PSA with deep sync and single-sign-on
- Complete refactor of Patch Management and the addition of Local Caching for patches and greatly expanded Power Management controls
- Rebranding of the Agent and Platform to Autotask Endpoint Management
- Enhanced Audit, New Default Filters and Importable Monitoring Policies to make implementations easier
- New Privacy mode options and Monitoring Maintenance Windows
- New Webroot integration and upgraded Kaspersky and Splashtop integrations
- Many new Reports and ComStore Components

In 2017 we will continue to work on our vision of making Autotask Endpoint Management the RMM platform with the best user experience and feature set in the market.

We will **Refactor our Monitoring** capabilities, make many monitoring enhancements and add Real-Time Monitor Status visibility.

It will become much easier to **Discover, Monitor and Control Network Devices** like Routers, Switches and Storage Devices.

We will launch the **Apple macOS Agent Browser** that allows engineers to remote control any Agent from an Apple macOS platform.

Customers will benefit from having more ways to get data from AEM. We will make our **Reporting more flexible** and will release our **Public API**.

Besides investing in our product, we will also continue to invest in our Engineering and product Support teams. The AEM engineering team will grow by 20% and we will hire additional Sales and Implementation Engineers. There is a continued focus on customer reported defects and we will have more regular maintenance updates. Further investment in DevOps and Security tools will ensure we will continue to deliver 99.99% uptime.

Disclaimer

This document describes the development priorities for Autotask Endpoint Management in 2017. The information and mock-ups presented here are intentions, and demonstrative of our goals. As we get closer to releasing new functionality, we will publish more concrete information around the exact workings of these features and enhancements.

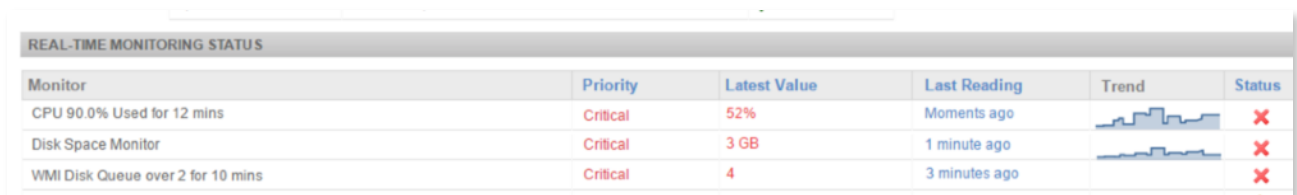
Monitoring

The Monitoring functionality of AEM will get a major upgrade. We will enhance many of the existing monitors, add new highly requested monitors and give much more visibility on the current state of applied monitors.

We will be introducing a new Monitoring Service. This will run in parallel with our Agent, handling the gathering and submission of monitoring data in a more efficient and flexible manner.

Real-Time Monitor Status

Applied Monitors will start reporting their latest values to the platform. We will display the current values and a history of these values on the Summary pages of both Agent and Network Devices. Engineers can use this data to quickly analyze if a device is functioning normally and if the monitoring is working properly even when no alert was generated.






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

Image 2: Monitor Status on the Device Summary

Windows Performance Monitoring

The Windows Performance Monitor 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 Windows Performance monitor integrates such functionality in a straightforward and effective manner, vastly simplifying tasks like monitoring SQL Servers or checking disk queue lengths.

Event Log Monitoring

The Event Log is one of the most important sources when monitoring Windows systems. The Event Log monitor will see some significant changes. 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 will also include 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-Resolve options.

The screenshot shows the 'Add a Monitor' dialog for 'Event Log Monitor (Windows Only)'. The dialog is titled 'Add a Monitor' and 'Event Log Monitor (Windows Only)'. It has a sidebar with 'Monitor Type', 'Monitor Details', 'Response Details', and 'Ticket Details'. The 'Monitor Details' section is active and contains: 'Trigger Details' with a text box for 'An Event In' and a dropdown for 'Raised by' set to 'Event source name'; 'Event Codes', 'Event Types' (with checkboxes for Error, Warning, Information, Success Audit, Failure Audit), and 'Event Descriptions'; a frequency selector '... is Raised' with a dropdown and time input; 'Alert Details' with a priority dropdown set to 'Moderate' and an 'Auto-Resolution' checkbox; and a 'Resolve the alert if an event matching the following is seen...' section with a matching text box. 'Back' and 'Next' buttons are at the bottom right.

Image 3: The new Event log monitor will have many new options

Network Monitoring

Expanding our Discovery, Monitoring and Management support to accommodate Switches, Routers, NAS and other Network Devices is a high priority for us.

Enhanced Network Discovery

The Agent scans the local subnet for new devices on a daily basis. Many companies are now using V-LANs to structure and secure their networks. This made it impossible for the Agent to see devices in these networks. We will be adding controls to add Additional IP ranges on a per Site basis to help customers in these situations.

We will also make it easier to on-board multiple, different types of devices at once. The improved Discovery Tab will make it easier to find, filter and add newly-found devices to AEM.

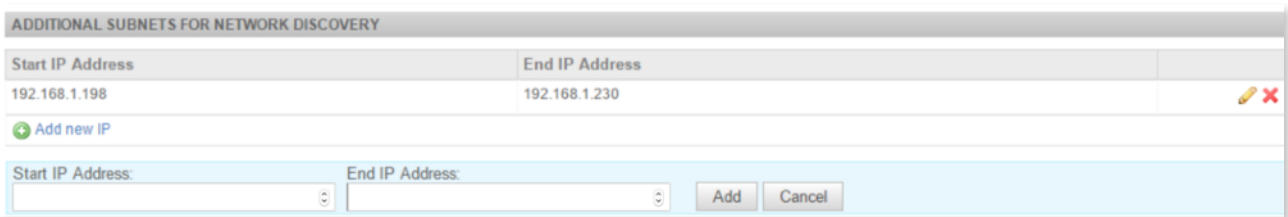


Image 4: Additional IP ranges to discover can be provided on the Site Settings tab

Network Device Audit

Network Devices (SNMP) and ESXi hosts will now 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. We will also establish a stronger relationship between the Network Node and the Network Device. This will make it possible to assign SNMP policies to these devices.

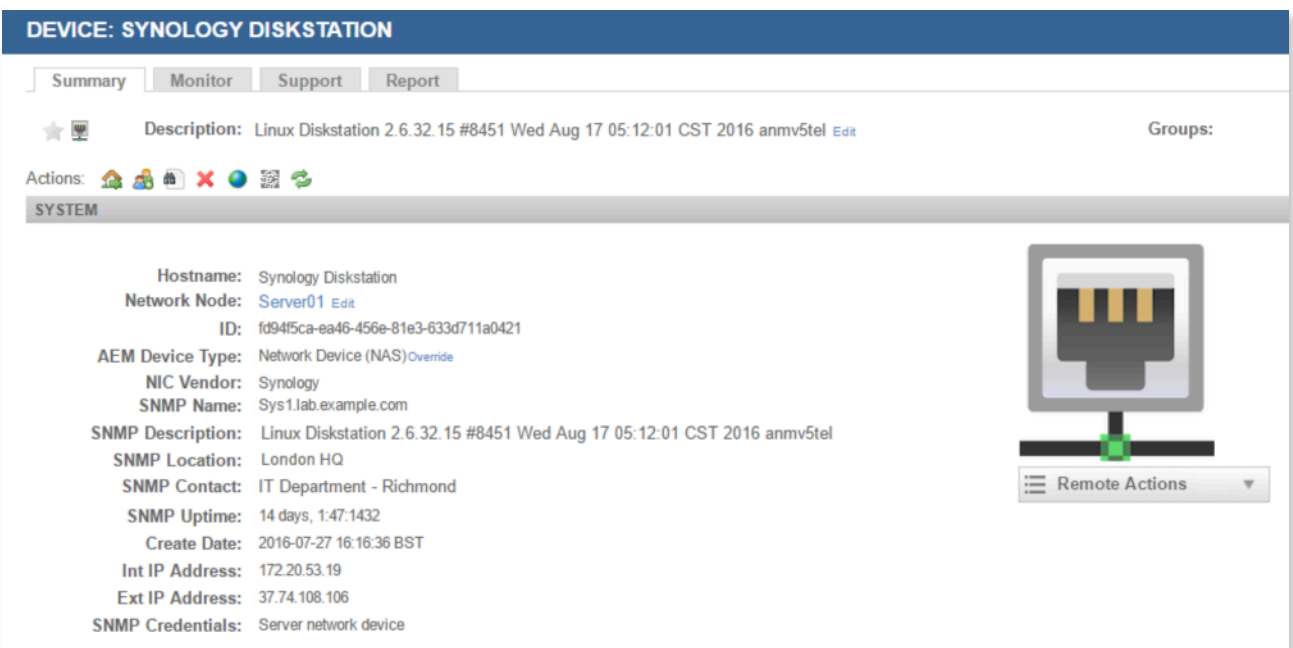


Image 5: More Audit information for all SNMP devices

SNMP Monitoring Policies

SNMP monitors will be assigned using a Monitoring Policy instead of Components. This will make it possible to automatically apply monitoring to these Network devices and allow for much faster device on-boarding. Engineers will find it easy to manage these SNMP Monitors since they can be managed and assigned much like any other policy. We will also share these new SNMP Monitoring policies in our ComStore so customers don't need to build their own SNMP monitors for commonly used devices.

To make it more convenient to do deeper Server Hardware and Linux monitoring, we will also make it possible to assign SNMP monitors to machines with an Agent installed.

The screenshot shows the 'Add a Monitor' configuration window for an SNMP Monitor. The window is titled 'Add a Monitor' and 'SNMP Monitor'. It has a sidebar with 'Monitor Type', 'Monitor Details', 'Response Details', and 'Ticket Details'. The 'Monitor Details' section is active and contains the following fields:

- Trigger Details:** SNMP OID to Query: 1.3.6.1.4.1.9.2.1.58, Index: [empty]
- Transform Result:** Result Calculation (Numeric Values): /1024, Result translation (Text Values): 0=Unknown, 1=OK, 2=Failed, 3=OK
- Display Name:** CPU, Data Type: %
- Alert Settings:** Alert when SNMP result: Greater Than, 90; Alert when OID is not responding: Moderate
- Check Interval:** 5 minutes, Store values on platform (for graphing and reporting): [checked]
- Auto-Resolution Details:** After 1 minute, resolve the alert if it is no longer applicable.

At the bottom right are 'Back' and 'Next' buttons.

Image 6: The new advanced SNMP monitor configuration

Ping Monitoring

ICMP, or more commonly called Ping, is a great tool to detect and analyze Network problems. We will add 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 will also alert if there is a lot of network latency or packet loss.

Network Device Control

There is an increasing need to provide support for Network devices, Printers and Storage devices. It's not possible to install Agents on these types of devices, so many engineers have to setup a VPN or remote control an Agent before they can manage these devices.

We will create a seamless and efficient experience for engineers to connect to Managed Network devices using common protocols like SSH, Telnet or HTTP.

These sessions can be quickly launched from the Web Console or Agent Browser. A Network Node in the network will seamlessly tunnel all the communication between the Admin and the Remote Device. The Agent Browser will immediately launch a Web Browser or Putty connection to the remote device. It will also be possible to use the Custom Connect to connect to any remote port with any local application.

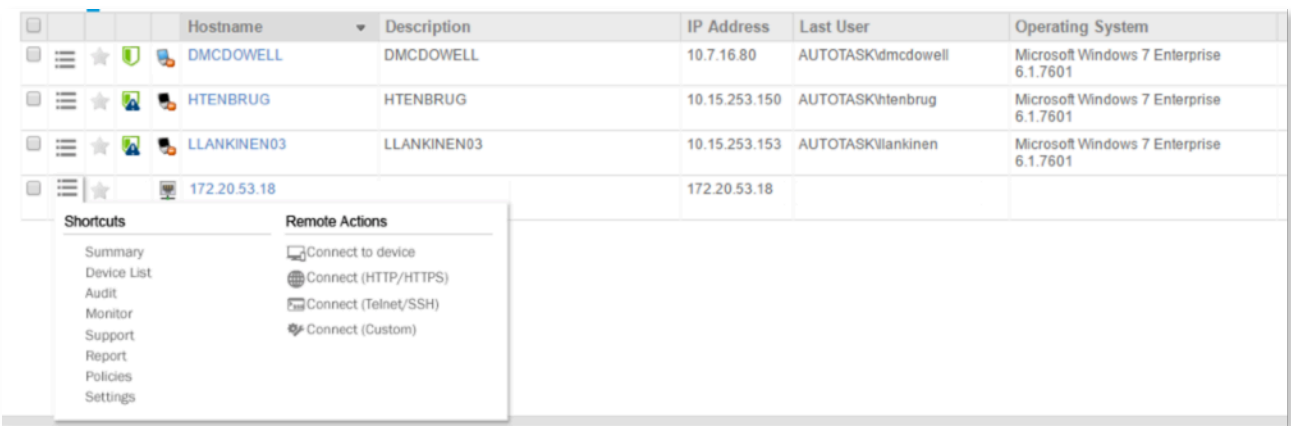


Image 7: Network devices can be quickly controlled from the Device List or Device Summary

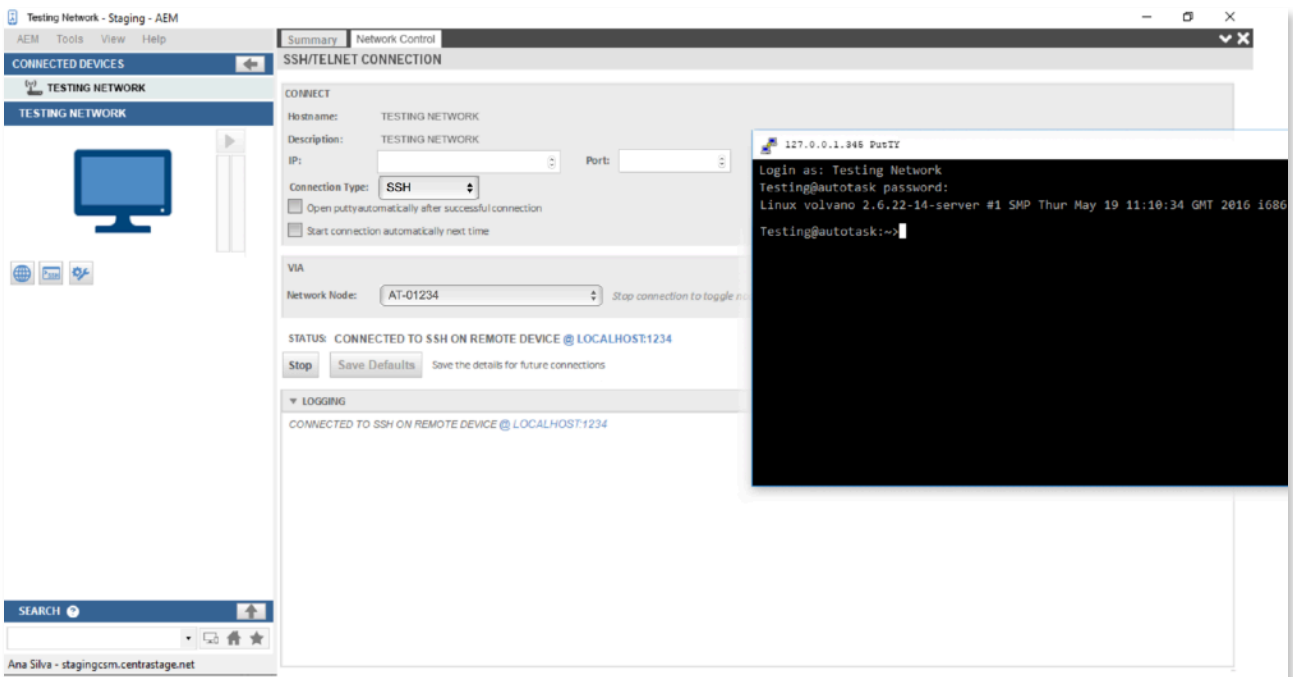


Image 8: The Agent Browser can open an SSH session directly to any Network Device

Apple macOS Agent Browser

Support engineers are increasingly working on Apple macOS systems. We will give these users a new Agent Browser that will run natively without the need of a Virtual Machine. Initially we will focus on delivering the most important features of the Windows version to the macOS Agent Browser. Our first version will include Remote Control, File Transfer and Remote Command Shell.

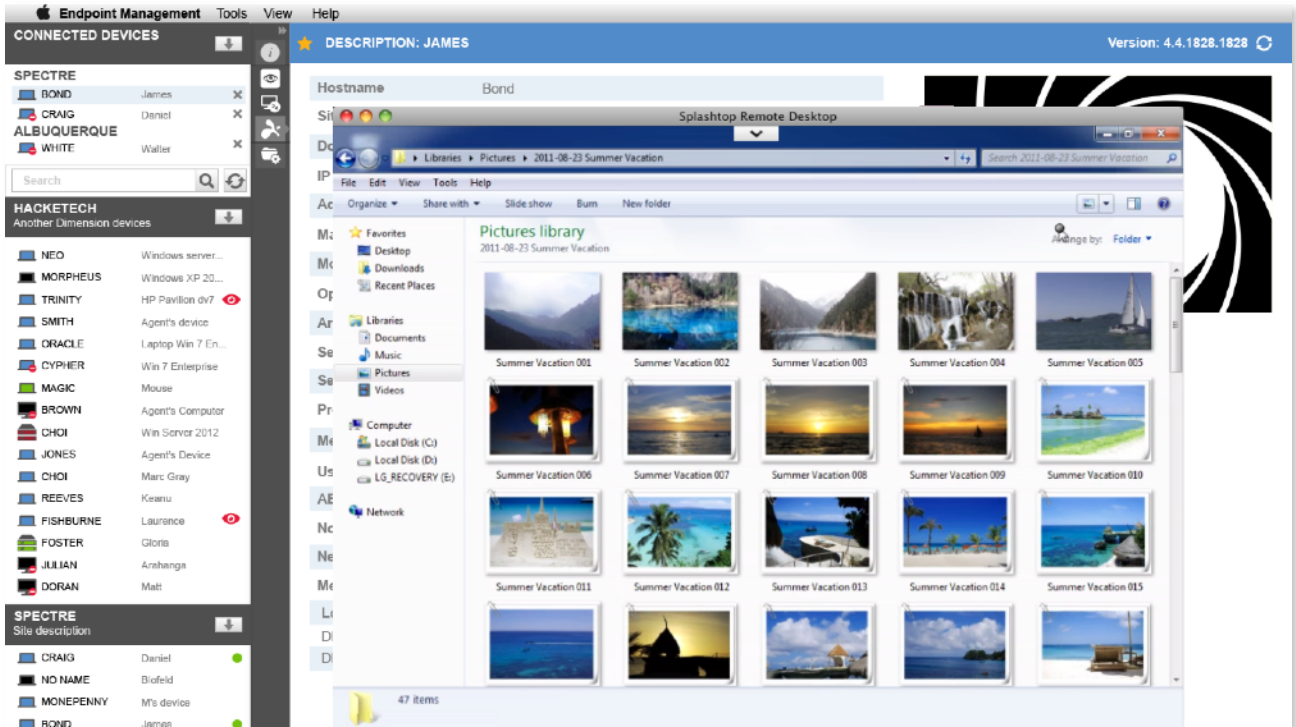


Image 9: The most important Agent Browser functions will be made available for Macs initially

Reporting

To help our customers to get more data out of AEM, we are looking to provide a lot more flexibility in the Reports Generation process.

Improved Scheduler

We are going to make significant improvements in the Reporting Scheduler. Reports will be able to be generated based on combinations of Filter Results, Sites and Individual Device Selections. For customers using languages other than English, we will be augmenting the scheduler to add a language selection option.

Increased Flexibility of Existing Reports

Existing Reports will be reviewed and enhanced. Depending on the Report, we will make certain aspects configurable by the user. We will introduce Date Range Selection, Report Part Selection and a Column Chooser.

The screenshot shows the 'NEW REPORT SCHEDULE' interface. It is divided into two main sections: 'GENERAL' and 'REPORTS'.

GENERAL

- Name:** [Text input field]
- Description:** [Text area]
- Schedule:**
- Enabled:** (To disable this report schedule without deleting, uncheck this option)
- Report Language:** (dropdown menu)
- Targets:**

Type	Name
Devices	CCOMER03, HGUY01, OLEMARIED, SHOLYOKE, WIN-2003R2-32, WIN-7-64, WIN-XP-32
Site Device Filter	All Server OIS

REPORTS

Choose the reports to be included in this scheduler

Report Name	Description	Date range	Type	Actions
Activity Summary	For the selected site, the report provides total activities and times by category of Jobs, Notes, Remote Shell and Remote Support for the previous 7 or 30 days. It also lists the top 5 devices associated with the site by number of activities. Then lists details for each activity, by device.	<input type="button" value="Date range"/> <input type="button" value="Choose the time of your report"/>		<input type="button" value="Print"/> <input type="button" value="Export"/> <input type="button" value="Delete"/>
Computer Summary	The report lists the computers associated with the selected site. It includes name, processor, operating system and service pack, memory, letter label, total drive space, amount and percentage of free space.	<input type="button" value="Date range"/> <input type="button" value="Last 7 days"/>		<input type="button" value="Print"/> <input type="button" value="Export"/> <input type="button" value="Delete"/>
Storage Report	The report displays fixed storage information for all devices in the selected site. It lists device by name, with drive letter, size, and amount and percentage of free space.	<input type="button" value="Date range"/> <input type="button" value="Last 30 days"/>		<input type="button" value="Print"/> <input type="button" value="Export"/> <input type="button" value="Delete"/>
Health Report	The report displays the number of devices in the selected site by operating system, including build number. It lists the number of devices without updated anti-virus, MS updates or firewall, with low free disk space or memory, and devices not online this month. It lists each device by name with last logged-in user, and their individual status for previous mentioned criteria.	Devices with <input type="text" value=""/> GB free space		<input type="button" value="Print"/> <input type="button" value="Export"/> <input type="button" value="Delete"/>
Performance Report	The report shows the CPU, Memory and Disk performance of the servers in a site over the last 30 days, including the average of the CPU and Memory, and the delta of the available disk space.	<input type="button" value="Date range"/> <input type="button" value="Last 30 days"/>	Desktops, Laptop, Servers, Network	<input type="button" value="Print"/> <input type="button" value="Export"/> <input type="button" value="Delete"/> Edit Report

Image 10: The new Report Scheduler will a lot of flexibility when generating Reports

Autotask Integration

After the original Unification Release, we've made several enhancements to make the experience even better. We will continue this effort, so that our customers get maximum value out of the Unified Platform.

Remote Control Activity to PSA Ticket

Engineers are constantly using the AEM Support tools to respond to alerts and solve incidents. The activity and time spent in these sessions are a valuable source of information. AEM will store the actions, notes and session details from these activities in Autotask and link them to the related support ticket.

Admin Ticket Experience

We will continue to enhance the Autotask ticketing experience. There will be more useful automatic notes when tickets are created, i.e. the recent machine changes will be added. Opening the support tickets in AEM will show tickets in Autotask directly instead of showing an AEM ticket form. With the release of the new Ticket UI in Autotask, we think this will result in a much better user experience.

Public API

For customers with more advanced needs, we will make our API publicly available. This will allow customers and partners to freely build their own integrations and reports. We will add methods to our API to return information like Historic Alerts, Performance Data and missing Patches. We will also provide detailed documentation and examples of how to integrate with our API.