6.5.0 Software Management overview

Version: 1.0
Last Edit: 22-10-2018
By: Matthé Smit

Introduction

Keeping software applications updated is a major part of any Endpoint security strategy. Common third-party software applications like Adobe Reader and frameworks like Oracle Java, being internet-facing, often serve as attack vectors, both from new “zero-day” vulnerabilities and from existing, unpatched flaws; studies show that over 90% of cyber-attacks exploit security flaws for which a remediation has been made available. Maintaining and exercising application version control is, therefore, imperative to any modern operation and the Datto RMM Software Management feature was designed with this in mind.

Datto RMM’s new Software Management feature allows administrators to easily keep their Endpoints updated with the latest security fixes in a manner that is clear and transparent. It features the following capabilities:

- Automatic, policy-based approach to **3rd-party software update management** makes it effortless to keep **Windows** and **macOS** Endpoints updated with the latest versions of frameworks and applications like Adobe Flash and Oracle Java.
- Optionally, application **update approval** can be configured and applications can be **installed** when not already installed on an Endpoint.
- Built-in **compliance reporting** to show customers that Endpoints are outfitted with the latest versions of critical applications and frameworks.

Availability

Version 6.5.0 of Datto RMM is planned for release in November. Planned release dates might change for quality reasons. Official platform update announcements will be made at https://status.autotask.net and on our Community forums.

Supported Applications

The primary goal of Software Management is to ensure that critical software applications and frameworks are always up-to-date. To ascertain what should be deemed as ‘critical’, we

drew up an initial list of supported software products by analysing usage numbers and update frequencies from internal usage data. The feature will work with these products.

This support list should be expected to evolve over time. Customers can request new applications in the Ideas section of our Community.

At launch, the following Applications will be supported:

Name	Platforms supported	Comments
7-Zip	Windows	Program is not available for macOS platform.
Adobe AIR	Windows & macOS	
Adobe Flash	Windows & macOS	
Adobe Shockwave	Windows	No mainstream macOS web browser supports the Shockwave framework as of 2018.
Adobe Reader	Windows & macOS	macOS devices cannot update the software if it is in use. In such cases the installation will fail gracefully.
Autotask Endpoint Backup	Windows & macOS	When installing, AEB Team Keys can automatically be provisioned using the Site Variable: `teamKey`
Autotask Workplace	Windows & macOS	When installing, AWP Team Keys can automatically be provisioned using the Site Variable: `teamKey`
Google Chrome	Windows & macOS	
Oracle Java	Windows & macOS	Old versions of Java are disabled – not removed – as part of the installation process.
Mozilla Firefox	Windows & macOS	
Microsoft Skype	Windows & macOS	As Skype is set to run on boot, the macOS installer will kill Skype if it is running to update it. If it was killed, it will be restarted after.

Software Management Policy

Application updates can be configured using new Software Management policies.
By default, one policy will be present for each customer following provision; this policy is configured with every supported program set to “Manual Update” so as not to change Endpoint software configurations without administrative intervention.

Software Management policies have two different scheduling options to determine when updates get installed:

1. Immediately on detection: An application update will be installed as soon as the Agent detects that an update is ready.
2. On schedule: The Agent will only check for (and, if configured, install) software updates on a scheduled basis.

The following Policy actions are defined:

Policy action	Meaning	Compliance reporting
Unmanaged	The Agent will neither install nor update this program.	The program will always be considered Compliant.
Manual update	The user will need to specifically approve individual updates for this program as they become available. If the program is not installed it will not be installed.	The program will be considered Compliant either when absent or, if installed, when it is up-to-date.
Manual update + install if not present	The user will need to specifically approve individual updates for this program as they become available. If the program is not installed, the user will need to approve its installation.	The program will be considered Compliant only when it is both present and up-to-date.
Auto update	The Agent will automatically update the program without requiring approval. If the program is not installed, the user will need to approve its installation.	The program will be considered Compliant either when absent or, if installed, when it is up-to-date.
Auto update + install if not present	The Agent will automatically update the program without requiring approval. If the program is not installed, it will be installed automatically.	The program will be considered Compliant only when it is both present and up-to-date.

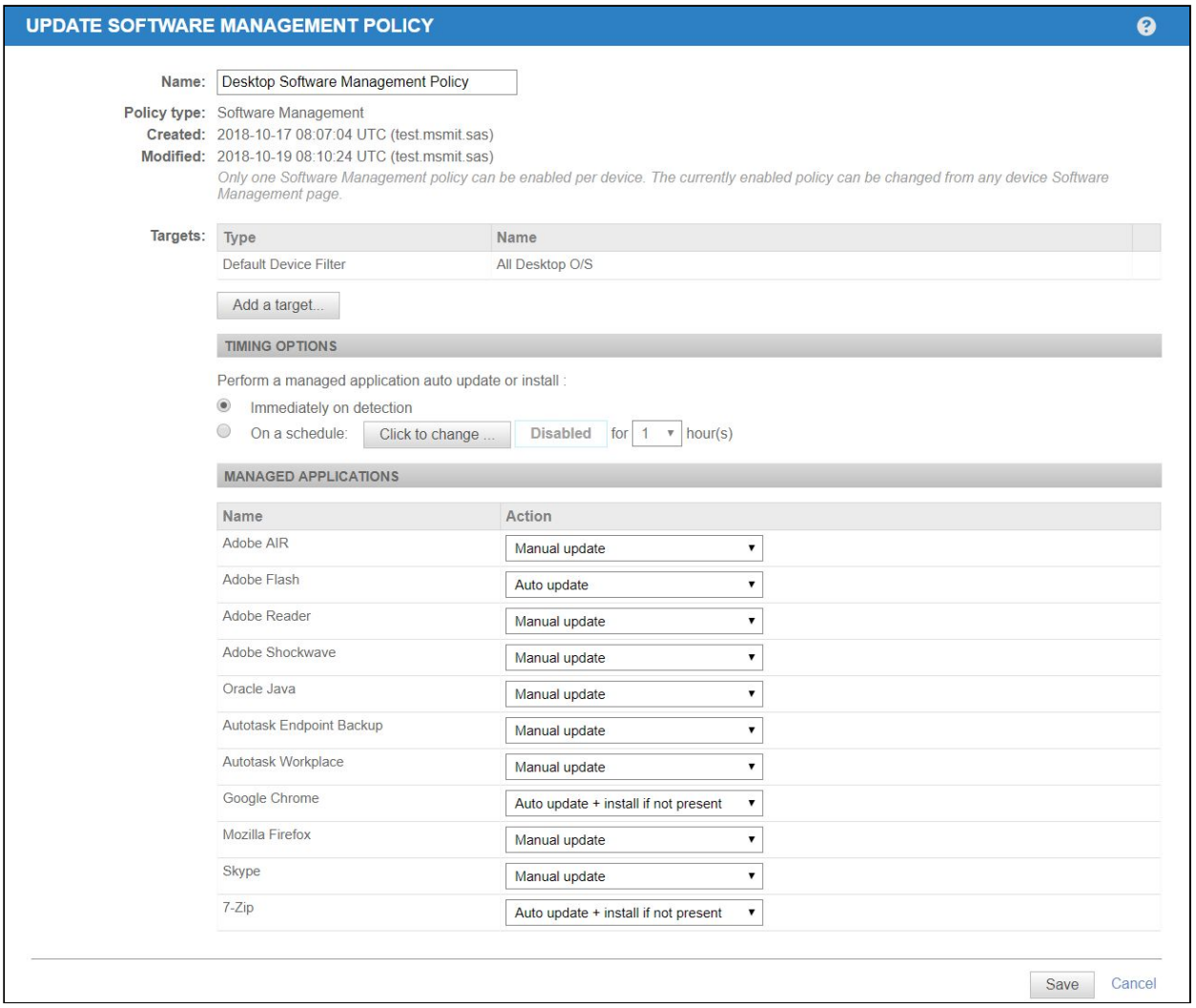

Image 1: The new Software Management Policy

Site and Account - Software Management

A new management dashboard will be added under the Site and Account Manage tabs. Like with Windows Patch Management, this dashboard will show compliance across all managed devices. Users can use this to quickly find devices that are Not Compliant and diagnose these devices.
Software Updates can also be approved from here. The Applications table on this dashboard will list all applications that have devices that still require an approval.
(In this instance, the Policy is set to Manual Update).

Approving an update for the Account level will approve the update for all the devices in the entire account that currently have that update missing.
Approving an update for the Site level will approve the update for all the devices in the selected site that currently have that update missing.
An "approval" action cannot be reversed.

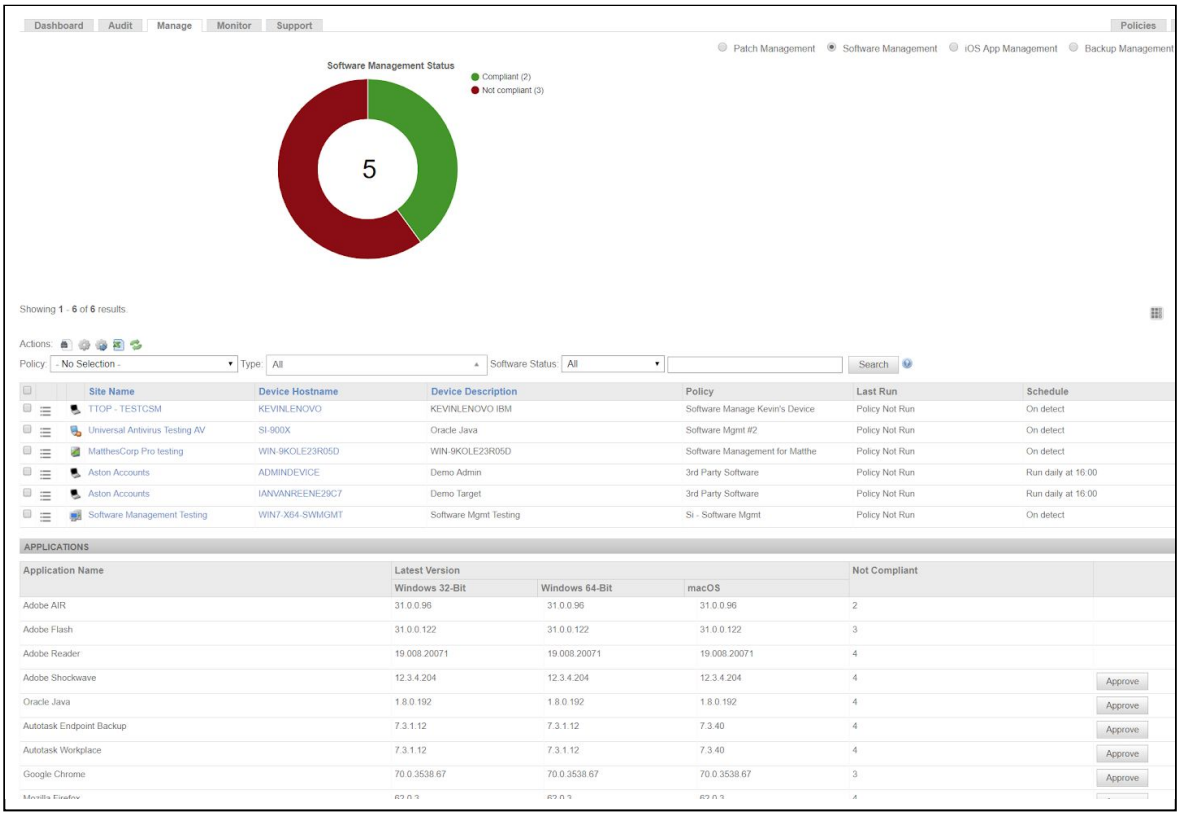

Image 2: The new Software Management Dashboard

Device - Software Management

The new Software Status page shows compliance directly from the Device Summary tab. Clicking the Software Status link will take the user directly to the new Software Management option under the Device Manage tab.

From the device level Software Manage tab a user can quickly see what applications and versions are currently installed and what the latest available version is for that application. Users can Approve an update from the Managed Applications list for this device only.

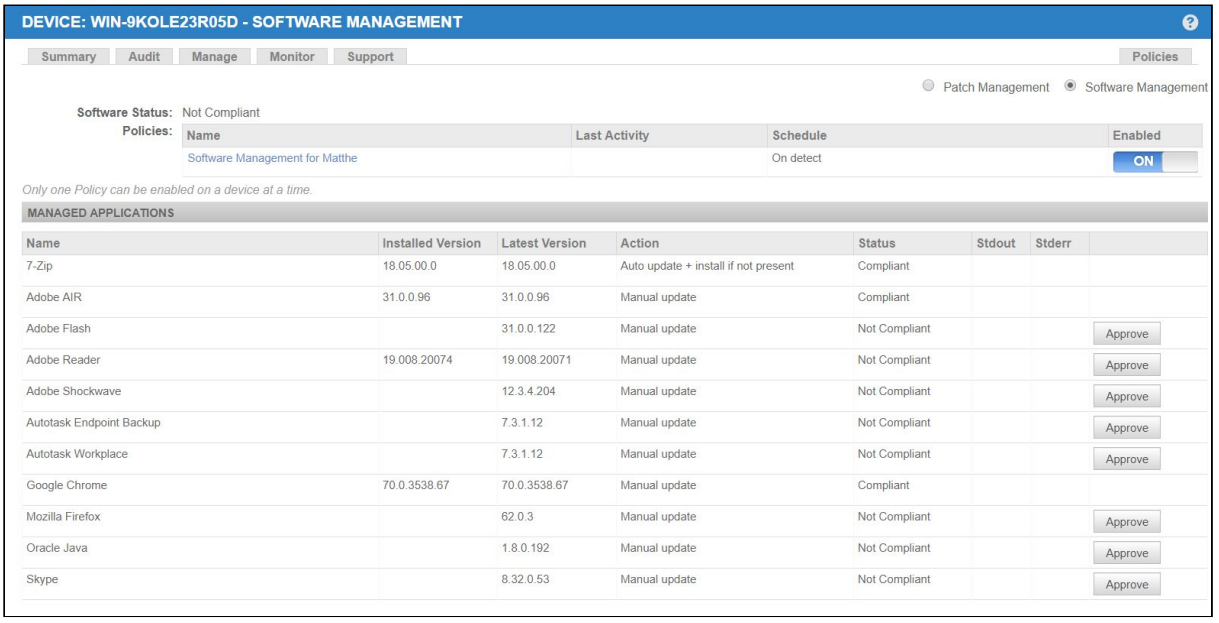

Image 3: The new Software Management page on Device level

Reporting

Software compliance reporting can be done using two altered reports:

1. The Device Health Summary has a new column called Software Status to show if a device is considered compliant with Software Management
2. The Executive Summary report has a new section to show the Software compliance status for the Servers and Workstations in the included sites. Like with Patch Management, the Software status will impact the overall health score in the report.

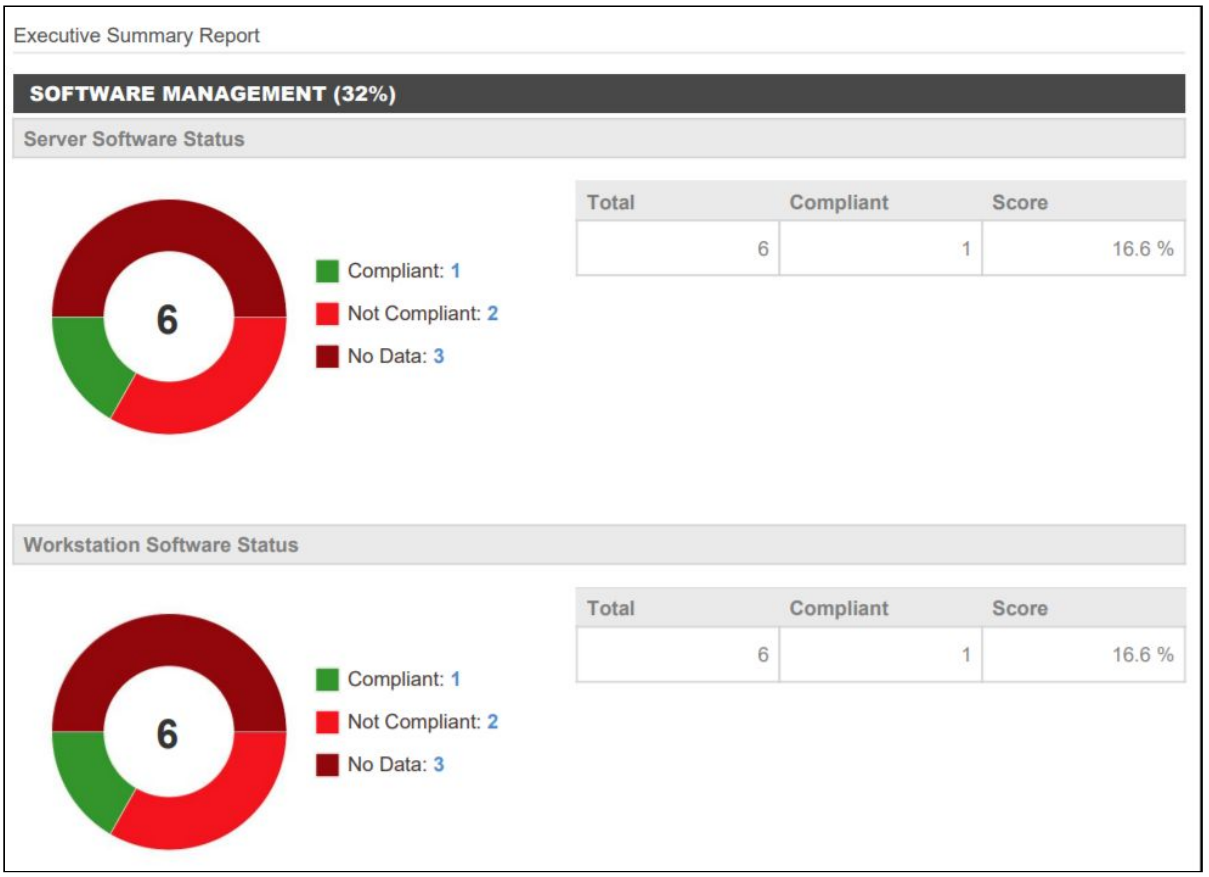

Image 4: The new Software section in the Executive Summary

Filters, Columns and API

To make it easier for users to find the devices that are out of compliance, a new column called Software Status has been added to the device lists. A new filter criteria for the same field is also available. Additionally, the Device API will be returning the field softwareStatus when queried.

Application update quality assurance

Our team will continuously monitor for the vendors of the managed applications to determine if new versions are available. Any new version will go through a quality assurance process to determine if the installer logic works and if the update is deployed successfully. Applications are tested to ensure they install properly; Datto RMM staff do not test to ensure programs have benefited substantially from the update process.

We aim to have new applications tested and available with Software Management within 48 hours after becoming available from the vendor.
Application updates will be in the same language as the previous version of the application. In case of new installations, the application installer logic will determine the best application language for the managed endpoint.

Customers can also find all application updates in the ComStore as regular Application components. Like with other components, customers can inspect the files and code used in any of these components by copying them from within their Component libraries.