385 Falmouth Ave
Elmwood Park, NJ 07040
201-300-8277
www.mspbuilder.com

June 28, 2022

Status of Support for Software Management on Kaseya VSA

MSP Builder's engineering team has been working with Kaseya to improve Software Management since it's pre-release in 2019. We review the product status after each VSA release to determine if the components necessary for integration into the RMM Suite are present and functional at a level that we can support.

There are several key requirements for us to support any component on any RMM platform:

- Proper operation. It has to function as advertised at a reasonable level across most common configuration requirements.
- Reasonable performance. The product needs to function within our design parameters, such as change windows and other related/integrated functions.
- Commercial support. The product needs to be able to be developed, configured, and then distributed to our customers via standard software distribution and installation or import methods. On a secondary level, the product must permit our automated support tools to install and configure updates.

Engineering Report as of 6/24/2022

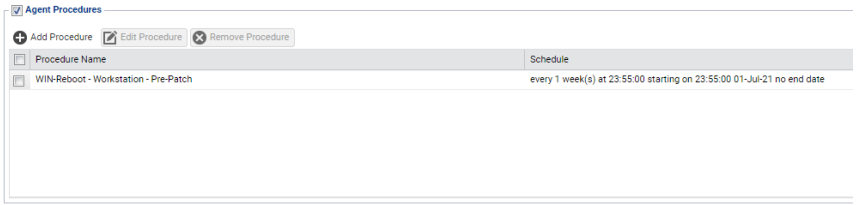
The latest Software Management components were reviewed on 6/24/2020. The following Software Management configurations were created on the Development server:

- Alarm for Patch Install Fail to meet MSPB alarm standards
- Scan Schedule Policy for Workstations - Mondays between 10 AM and 4 PM to match current Patch Management settings.
- Scan Schedule Policy for Servers - Mondays between 1 and 5 AM to match our current Patch Management settings.
- Patch Deployment schedule policy for workstations - Thursdays between 02:30 and 04:30 to match our NITE HOLD and NITE RESUME P-M configs.
- Patch Deployment schedule policy for servers. Only one of the 77 standard schedules was created for testing.
  It was determined that a 1-minute distribution window could be created, which will satisfy our need for patching servers with Software Management.

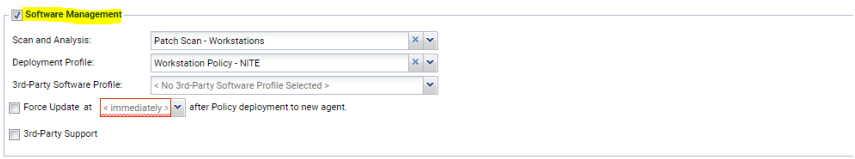
The above Software Management policies were exported and reviewed. The XML files are quite simple compared to the complexity of other export file content. It should be trivial to synthetically create an XML import file for all the schedules we'll need for server (77) and workstation (4) systems. There are only 2 scan schedules and one alarm policy, so no additional effort is needed there.

A System Policy to test workstation patching for Software Management was created. The View for this policy is triggered by placing "-SM-" into the Server Patch Code. This disables Patch Management and enables Software Management for a specific agent and is done only for testing in this environment. In production, either the Patch Management or Software Management policies would be used as a "mix and match" configuration is not supported.

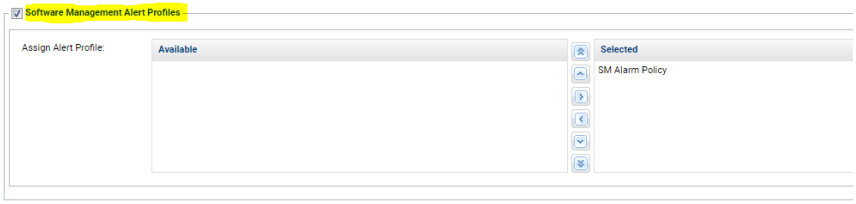
This is the policy content:



Pre-Update Reboot task



Patch Scan Schedule
Update Schedule



Alarm Policy

This looked quite promising and generally aligns with our current capabilities with Patch Management. The above System Policy was then exported and the contents examined.

```
<?xml version="1.0" encoding="utf-8"?>
<Policies>
  <Policy id="246321659137644" ref="Patching: (Auto)
    <agentMenu />
    <agentProcedures>
      <agentProcedure id="795630693759596" partitionI
    </agentProcedures>
    <alerts />
    <checkin />
    <credential />
    <distributeFiles />
    <logging />
    <machProfile />
    <monitorSets />
    <patchSettings />
    <protectionPolicy />
    <workingDir />
    <remoteControl />
    <patchFileSource />
    <patchProcedureSchedule />
    <patchRebootAction />
    <auditSchedule />
    <eventlogsettings />
    <updatelistbyscan />
    <windowsUpdate />
  </Policy>
</Policies>
```

This is the Policy declaration

This is the schedule to run the Pre-Update Reboot procedure at 23:55 Wed

There are no Software Management settings defined anywhere in the export. No export/import functionality exists.

Without the ability to export the System Policy definitions that control Software Management, it is impossible to provide the necessary automation to support an enterprise style server patching solution. We use 81 separate System Policies to schedule patching, plus another 5-6 that handle overrides and special conditions.

Patch Management allows you to define the update schedule in the System Policy, so 81 policies to define the Patch Configuration Policies and the schedule are sufficient. The same scheduling configuration in these policies can apply to servers or workstations, allowing precise scheduling of "servers" that run a workstation O/S. Software Management instead places the Patch Configuration and Deployment Schedule into the Software Management policy. The System Policy selects a Software Management policy to both define and schedule updates. This would require duplicating the 77 server schedules to reference workstation settings, doubling the System Policy footprint, as well as adding 77 new views to control the "workstation as server" configuration. This introduces additional complexity but will not prevent the use or support of Software Management.

The lack of any ability to import (or export) System Policies that define Software Management settings is a major issue. This would require that we manually create close to 90 System Policies to support the current server and workstation schedules and would need to add 77 more if we wanted to support "Server as Workstation" scheduling the way we currently do. This is an impossible task, as any manual effort introduces significant potential for error. Considering that this would schedule updates and reboots, there is no margin for error in this configuration.

At this time, the inability for Kaseya VSA to export or import Software Management configuration settings in System Policies precludes our ability to support this component. We will continue to test and evaluate as new updates are released.