MSP BUILDER
Tools for MSP Success

Release Notes

Release 3.0.22-175

Release Notes for RMM Suite V-3.0.22-175

June 24, 2022

The RMM Suite Version 3.0 is a major rewrite of the RMM Suite platform and is the result of five years of continuous development and improvements based on the feedback from our customers. One of the most important enhancements in V3 is *RMM Platform Independence*. While this means we can support other RMM platforms in addition to Kaseya VSA, it also means that many of the platform issues we faced in the past year will no longer impact the RMM Suite. We have eliminated all dependency on the RMM platform for configuration and file deployment (both configuration files and installation packages). There are lots of changes, so we'll break things into key groups.

Operational Enhancements

Component Configuration

The RMM Suite tools are highly configurable, based on data in configuration files. These have always given our customers the ability to customize settings down to a specific agent. This has come with some complexity, however, and we have made the simplification of configuration settings our top priority. As a result, we have eliminated the configuration files from the RMM platform and moved the data to a web-management portal. Each setting is available on-screen to view or adjust. Creating client, site, or even agent-specific configurations is as easy as selecting the correct values from a drop-down list. Once the configuration data is placed in our management platform, the data for a specific agent is assembled, ciphered, and delivered to our endpoint tool, where it is deciphered and passed to the applications. Copies are stored locally for testing and verification.

Migration of your current configuration data is automatic. We have pre-loaded the configuration management system with all of our client's current configuration settings, so when you switch to version 3.0, you won't need to do anything more than a quick review.

The Configuration Management system provides two levels of access - View and Manage. This allows all technicians to view the settings while limiting changes to be made by a select team.

Application and Component Deployments

Several of our tools depended on files uploaded to the RMM Shared Files folder. If the components were not uploaded, the tools would not function, and this resulted in quite a few support calls. These components are now *hosted* on the MSP Builder file distribution network, eliminating the need to upload and maintain these components. All files will be maintained by MSP Builder to support the tools, configuration commands, and application management tasks that are part of the RMM Suite.

We will still provide a template that uses RMM platform deployments for customized application deployment, which will also still support Managed Variables.

Cloud Script Variables

The Managed Variable feature in Kaseya VSA is powerful but somewhat awkward in operation. The RMM Suite 3.0 introduces Cloud Script Variables (CSV), allowing customer, site, and even agent-specific configuration data to be defined and delivered to scripts, procedures, and applications. All RMM Suite tools have been updated to utilize CSVs, and we have provided a tool to allow RMM platform tools to reference CSVs as well. As before, these variables can be used to inject license keys, credentials, and virtually any configuration parameter into an automation process, eliminating the need to write customer-specific scripts.

CSV Security

The Configuration Management system allows you to automatically cipher a designated password parameter. This has always been an RMM Suite capability through an external tool, but now all it takes is to check the "this is a password" option and the data value will be ciphered automatically using both the customer and org to seed the cipher key. As these values are transmitted, the entire data is ciphered, in effect double-ciphering the password values while in storage and during delivery. All* of our tools have the ability to dynamically decipher these values *just in time* to deliver them to the system calls that need them.

**The generic tool that extracts CSV data for use in RMM platform scripts will ignore requests to deliver any ciphered file to preserve the security of that data. Only core RMM Suite tools can access ciphered data.*

Telemetry Enhancements

We introduced telemetry data during 2021 to provide access to raw alarm data. This can be used to get a better perspective of what and how often alarms are being received, as well as to indicate how well ITP is handling these alarm events. New features released with Version 3.0 include:

- Links to the Configuration Management interface to view or modify settings.
- Detailed information on how to troubleshoot and even common methods to fix issues. This is an awesome reference page for L1 techs to help complete more tickets without assistance or escalation.
- Application health reporting - the RMM Suite applications themselves can report when they are not configured or operating properly or experiencing difficulties due to local security configurations. We can proactively notify our customers of conditions where the automation is impacted so action can be taken quickly and effectively.

Documentation

The RMM Suite Operation Guides have been completely rewritten. Twelve smaller and more focused guides have replaced the three comprehensive guides. This makes each Operations Guide smaller, more digestible, yet more comprehensive.

The How Do I library has been updated to reflect the new configuration methods and continues to be updated with common questions. These short, focused documents provide a quick step-by-step reference to many configuration and administrative tasks.

Platform Integration

The RMM Suite tools will no longer co-reside in the RMM Agent's folder. All RMM Suite tools are now located in and execute from the C:\PROGRAMDATA\MSPB folder. *This allows you to independently configure platform security for the RMM agent and the RMM Suite tools.*

The RMM Suite tools will automatically detect the RMM platform type where they are executing and self-adapt to function in that environment.

Platform Scripts / Procedures

The platform scripts have been greatly simplified, moving more of the process logic onto the endpoint system. This has resulted in the elimination of many complex scripts as well as script dependencies. Where version 2.5 had nearly 50 inter-connected procedures, version 3 has just one. We have replaced 14 scripts and over 400 lines of logic with one script containing just 8 lines of logic. What does this mean for you?

- Less complexity improves performance. Tasks now run and complete within seconds.
- Lower overhead on the RMM allows more endpoints to be supported.
- Reduced need to update the RMM Scripts. Virtually every platform script now executes an endpoint tool, eliminating the need to update the script. Endpoint tools update automatically each day, which means all of your platforms will *always* have the most up-to-date management tools available *without any administrative effort on your part*.

Since many of the complex scripts have been eliminated, the organizational structure has also been improved with fewer folders to navigate through.

Common Endpoint Automation

This process received some of the most aggressive updating - the single WIN-Daily Tasks procedure performs ALL endpoint management tasks.

- If it detects a new agent, it runs the Agent Init and Onboard Automation tasks automatically, then completes a full audit. All local configuration is performed automatically.
- The RMM Suite configuration and license data is loaded from the MSP Builder cloud network.
- The RMM Suite tools are downloaded or updated to ensure that the latest versions are installed.
- The configuration data is downloaded from the MSP Builder cloud network, deciphered, and written to the disk. Data is then passed to the appropriate applications as needed.
- Based on configuration options, the following Daily Tasks are performed:
    - Pre-Maintenance “Quick-Audit” to prepare for Zero-Day remediation tasks.
    - Proactive Daily Maintenance
    - Smart Monitor initiation
    - Full endpoint audit with RMM platform update

The same application can be used to perform sub-sets of tasks, such as updating the RMM Suite tools, re-running the New Agent Init process, or executing a Full Audit.

Configuration Tools

This is where you will now find the Policy Management scripts. These allow programmatic control over the automation by adding or removing control tags. This has been a staple of RMM Suite management since it’s initial release - only the location has changed.

Endpoint Tools

These are applications used to manage or configure the endpoint systems.

Agent Offboarding

These tools have been enhanced provide separate tasks for common needs when decommissioning or offboarding a client endpoint. Scripts are provided to fully uninstall the RMM Suite components; return Windows Updates to a default, Windows-managed configuration; and to uninstall the RMM platform agent. Any or all of the scripts can be used to prepare a customer agent for disposal or re-allocation.

Application Management

This introduces a completely new feature within the RMM Suite tool set. The scripts utilize a complex method of Ninite Pro, Choco, and Direct methods integrated into our RMUAMT application to install, update, or remove 35 distinct applications, with more on the way. These application management scripts are fully managed and maintained by the MSP Builder team to deliver the current application components without any need to download, upload, or otherwise configure files on your RMM platform. Cloud Script Variables are fully supported for license and other parameter injection.

This requires an additional subscription fee to license the Ninite, Choco, and SWD components used to deploy and maintain these applications. This subscription is less than Ninite or Choco alone yet includes all three application management tools!

Mac Maintenance Tools

These basic tools have been updated to provide essential maintenance for Mac-based platforms.

Reboot / Shutdown Tools

What may seem simple is actually a comprehensive solution that takes external configuration and operational concepts into account. The same Windows Reboot Tool will accept arguments to perform pre/post update reboots while honoring the patch configuration settings; reboot systems immediately without regard to external controls, but will communicate with other tasks to prevent alarms from both RMM platform and OOB monitors. Rebooting computers has never been smarter!

Suspend Alarms

A full selection of procedures that suspend the RMM Platform monitors. When run on server platforms, server OOB monitors are also suspended.

MSPB Diagnostic Tools

A set of tools that have been updated to verify the operation of the RMM Suite platform and collect diagnostic data.

System Utilities

This folder contains over 80 scripts/procedures, nearly every one rewritten to use our new dynamic content management system. These tools now download scripts and necessary applications on-demand, execute them, and then remove them to minimize the security footprint of the platform. This new method also allows MSP Builder to continuously maintain and enhance these tools without needing to access your RMM platform.

Two new RMM Suite applications are provided to support these utilities - RMUGES will get a script from our cloud infrastructure, along with any applications and configuration files and then execute the script. The results are logged and (where supported) uploaded to the RMM platform. The working folder is then removed. The second tool - RMUELC - will execute a local application that is already present on the endpoint.

Both applications support arguments passed from the RMM platform script, as well as both *required* and *optional* Cloud Script Variables. Commands are validated before execution, are delivered in a ciphered format to improve security, and the scripts, files, and logs are removed upon completion, where used.

Views and Automation Policies

Nearly every automation policy was reviews and updated or completely rewritten. The MSP-Customized folder contains several updated and new policies, and uses a new name to prevent interfering with your existing customizations during the upgrade process.

There is a new VSA policy for Remote Control for Require Permission/Deny, which has been requested by customers in the past. We have also broken the Baseline policy into separate policies that clearly identify the SAAS and On-Prem Only versions to avoid unwanted operations from occurring.

The RMM Suite policy collection has been trimmed to eliminate the duplicate but non-automated policies as these often cause confusion. All policies support automation via controls, so manually set policies have no need to exist. This simplifies maintenance and operation.

Views have been updated to ensure that operating systems are properly detected, and workstations / servers are identified without referencing version-specific parameters. This eliminates the need to maintain views as new platform versions are deployed. Certain views related to old/unsupported platforms and applications have been removed. Policy Control views now have just two prefix types - XAPC for an Automatic Policy Control view and XARC for an Automatic Remediation Control view. All views related to monitoring have been classified by name to be grouped together, similar to our other views.

Additional views and policies have been provided to handle new monitors for previously unsupported components such as My-SQL. Certain policies and views related to specialized LOB applications will be available on-demand as VSA and other platforms often can't import the settings until the components are detected by an audit or scan. This prevents the installation of non-working components that later require updating.

Patch Management

Several of the outdated Patch Policies have been removed from the RMM Suite, making administration appear less daunting. Only policies essential to operation, plus three special configurations, are now provided.

The RMM Suite components have taken control of more aspects of endpoint updating, including notifying users of updates, when updates are resuming after the computer was powered off, and even the hourly nag notice. The reboot nag is endpoint-based so it will not block RMM scripts, and the timing is controlled to be hourly *on-the-hour* to minimize interruption of meetings.

Software Management

We are still working with Kaseya engineering on the ability to support this. Unfortunately, the Software Management system still requires a minimum 1-hour distribution window, which we feel is unacceptable for precisely scheduling server updates. This would expand our 6-hour change window to at least 9 hours. There are also limitations within the configuration export/import process that are preventing us from deploying a full Software Management solution. We hope to have support for this once Kaseya resolves the scheduling issue or provides us with a specific work-around.

Third-Party Application Updating

The RMM Suite now offers a comprehensive third-party software updating solution for over 150 applications. This optional feature incorporates Ninite Pro and Chocolaty components, plus custom applications, all for a single competitive fee - far below direct licensing of these components.

External Alarm Processing

With the elimination of Kaseya's Ticketing module last July, we have implemented full support for Service Desk. This will allow email-based notifications to be received, analyzed by ITP and appropriately managed. The Service Desk components are part of all new installs and will be provided during the RMM Suite upgrade *unless Service Desk is already configured or the BMS PSA is used*. Kaseya does not support the VSA Service Desk when BMS integration is enabled, and the BMS service desk does not allow the level of event filtering that ITP can provide.

RMM Suite Applications

This has been one of the most extensive parts of the Version 3 upgrade process. Every single RMM Suite application has been reviewed for operational effectiveness, features, and then rewritten from the ground-up to be fast, efficient, feature-rich, and secure.

Many of the applications now reference Cloud Script Variables directly to create accounts, report on endpoint security, and perform configuration tasks. Security has been a prime driver for this update, so we have integrated complex cipher logic into many applications to secure data while in-transit and at-rest on the endpoint. Ciphers use a private/public keying method that includes both our customer's ID and their client's ID, making the keys very unique. Data remains ciphered up until the point it needs to be delivered to the system or application.

Many applications also communicate to our cloud infrastructure. We have implemented a 2-stage security process for these applications. They use a function-specific token to connect to the cloud, then must provide a second token to access the data from the back end. This second 64-byte token is client-specific and changes dynamically every 24-hours.

Applications now report operational status via telemetry, allowing MSP Builder to proactively address issues with configuration, environment, and other challenges to effective operation. These may result in MSP Builder opening a support ticket and assigning it to your team (with full guidance in the ticket!) to review and address.

Daily Tasks - RMURDT

This is a completely new application that has eliminated 14 RMM platform scripts, significantly reducing platform complexity while improving performance. This tool is initiated by the RMM platform, after which it takes full control of the process. It determines if the endpoint is configured and will automatically configure the RMM Suite tools, creating folders and registry values, and even initiate the process to perform the MSP-specific endpoint customization tasks.

All RMM Suite applications are verified and downloaded if missing or outdated. Unused tools are removed during the process to prevent outdated applications from becoming a potential security risk. The application configuration files are securely downloaded, and the daily task actions - Maintenance, Smart Monitors, and Audit - are executed where enabled.

Endpoint Audit - RMASDU

This new audit tool employs an updated configuration file that simplifies administration. It can search for Roles, Features, Services, and Applications and apply TAGs to identify when these components are found. Either the System Roles or System Data field can be updated with the tags to control RMM Suite automation as well as custom automation and reporting.

Additional data is collected and cached on a daily basis. Any of the collected values can be written to RMM platform data fields. A new capability allows plain text and multiple values to be written to a single field, allowing more effective and efficient use of these custom fields.

A new “Quick Audit” can collect specific service and application data *prior to* the Daily Maintenance process. This allows the results of the audit to directly control the actions of the maintenance process, turning the Audit + Maintenance into a very effective Zero-Day remediation tool. With the new cloud-based configuration files, MSP Builder can inject Zero-Day detection data into our customer’s audit file, allowing immediate detection without any administrative effort. Likewise, we can inject remediation tasks into the Maintenance configuration. Once you review our remediation process, you can simply enable the task to allow the Zero-Day Vulnerability remediation to operate, all with minimal administrative effort.

Post-Release Feature - Documentation Engine Integration

Version 3.0 lays the groundwork for an enhancement to the Daily Audit tool that will allow any data values that are collected to be written directly to a supported Documentation Engine via API integration. Initial support will be for Hudu and IT Glue. *Expected delivery by year-end 2022.*

Proactive Daily Maintenance - RMMSEQ

The Daily Maintenance tool has always been a powerful tool to maintain the endpoints. This completely new version adds several new capabilities while reducing the complexity of our original tool.

Simplified Configuration

The definitions for Task Schedule and Task Configuration have been combined. The Day/Night cycle has been eliminated to minimize conditions that report maintenance has not run because the computer was powered off before the Night cycle ran. Each task defined in the configuration file has a simple “Schedule” parameter that allows execution once, daily, weekly, or monthly.

If the task needs to run at a specific time or just “after hours”, a new Delay Until parameter provides that capability. Additional controls help define if the task should run at all, including the use of Role Tags, registry data, file data, and variables.

Variables - data can now be read from various sources and placed into any of 5 variables. These values can then be used in other task configurations as controls or arguments to commands.

New Functions

Several functions have been added, improved, or otherwise simplified.

- Download - Specify a download URL and path/filename to save the downloaded file to.
- UnZip - unzips a ZIP archive to a specified folder location.
- Registry READ - allows reading a registry value into a variable for later use
- INI File READ - allows reading a File/Section/Value into a variable for later use
- Registry WRITE - updated to perform a Delete if no data is provided
- INI File WRITE - writes a value (specific or from variable) to a File/Section/Value.
- Start a command in the USER context. Maintenance usually runs in the System context. This requires a logged-in user (active or idle, local or remote) and runs in that user’s environment.
- LocalAdminUser administration has moved to Maintenance, this improves the chances to create or update this account. The password is ciphered and stored locally, then deciphered when written to the custom field.
- Macros are available to be used in scripts, arguments, and certain other parameters. Available macros define the RMM Suite tools folder, local computer name, platform architecture, and up to 5 custom-defined variables. All environment variables are available for use in command and argument parameters.

Maintenance Interface - RMESTM

The maintenance interface has received a facelift, with unused fields being removed and deprecated functions eliminated. The “Run Now” option has been removed because there is no longer a Night cycle that could have been missed.

The MFA Code no longer requires defining and configuring a security key. The MFA Code tool used by technicians is automatically associated to the MSP’s organization to secure the operation to authorized agents.

The message processor has been upgraded to permit message queuing. This allows several applications to request messages to be displayed, and the messages will be displayed in sequence. The prior version allowed only one message at a time to be displayed. Other tools had to wait to request a message. This enhancement allows the other applications to exit more quickly, enhancing performance.

Smart Monitor: Operational Availability - RMSOAM

This Operational Availability monitor was originally released in V2.5 to provide an out of band mechanism to report on server availability. That version was susceptible to false alarms if the local computer time was off by more than a few minutes. The new version uses a cloud-based connection to check-in, eliminating any time-sync accuracy issues.

The monitor currently indicates that the server is operating and able to communicate with external resources. No configuration is required. An alarm is triggered when the server fails to check in over a 15-minute period.

The RMM agent service is also currently monitored. If the agent is stopped or removed, corresponding alarms are triggered. Being an OOB monitor, we can monitor the agent software without depending on the agent running.

Post-Release Features

Work is in-progress on two additional OOB monitoring capabilities:

- Performance Load - the system will monitor CPU and RAM load and report when a threshold is continuously exceeded for a specific period. This will prevent alarms that would occur from spikes or even short-duration high load events that often occur during backup or other intensive but otherwise normal operations.
- Service Health - instead of monitoring whether a service is *running*, the monitor will communicate with the service to determine if it is *functioning.* When such services are found via the audit, the corresponding tests will be performed unless disabled. Planned tests include DNS, DHCP, and IIS (root URL). Other custom tests, such as SQL queries, may also be supported but will require configuration.

These features will be available shortly after the initial release and no customer action will be needed to enable this additional functionality.