MSP BUILDER

Tools for MSP Success

The RMM Suite
Operations & Customization Guide

Platform Overview

MSP Builder, LLC
Version 3.0 / Release 22-175
Glenn Barnas

Last Updated: 2023/12/18

MSP Builder RMM Suite

The MSP Builder RMM Suite contains proprietary software, including unpublished source code. All software is (and remains) the property of MSP Builder LLC and no transfer of ownership is granted or implied.

The MSP Builder RMM Suite software is designed to audit, monitor and manage computers that use a number of RMM platforms. It is not designed or configured to collect personally identifiable information and should not be configured to do so without the consent of the individual or to be used in any unlawful manner, or in a manner that requires the consent of an individual.

MSP Builder LLC
385 Falmouth Ave
Elmwood Park, NJ 07407
201-300-8277

Contents

Introduction

The MSP Builder RMM Suite provides a comprehensive standards-based solution for operating and managing a Remote Monitoring and Management (RMM) Platform. The RMM Suite provides a set of endpoint applications that offload the RMM platform and standardize the operational processes, while delivering a solution that is easily customized to meet nearly any requirement. These tools are augmented with platform-specific components that leverage the RMM platform's built-in monitoring, scripting, patching, and other automation capabilities. The tools and operational practices are fully-documented, providing MSPs and IT departments with a time-tested method of operation.

The best way to understand the capabilities of the RMM Suite is by a "walk-through" of the components and automated operations.

Standard RMM Platform Components

The RMM Platform components leverage the core capabilities of the various commercial RMM platforms, including monitoring, patching, updating, and scripting. Each platform has unique capabilities and methods, so we will discuss this in a more general way.

Monitors

The RMM Suite provides collections of platform-specific monitor sets, delivering appropriate endpoint monitoring based on specific roles, services, and applications installed. Over 400 distinct monitoring objects are provided encompassing both Service and Event-Log monitors for Windows platforms. These monitor sets are designed to be independent of the actual platform or application version whenever possible for highest accuracy with minimal effort.

Patching

The RMM Suite utilizes the Windows Update API to directly patch endpoints. We utilize industry best-practices to configure and schedule updates and provide tools to manage the endpoint reboot to ensure that critical updates are applied consistently and correctly. Schedules are defined per-customer for workstations and per-endpoint for servers, offering 4 change windows with 4 or 8 schedules every day for maximum flexibility.

Scripting

The RMM Suite provides a large selection of scripts/procedures that help automate common tasks. Over 200 scripts are provided across all RMM platforms, using PowerShell whenever possible. Scripts are designed to leverage MSP Builder applications to allow automated updating whenever possible.

Ticket Processing

Intelligent Ticket Processing provides a highly configurable solution that evaluates every alarm received by the RMM platform and deciding if, when, and how to respond. Alarms can be filtered, deduplicated, mapped to automated processes, and based on priority, time of day, and other factors, notify your on-call team to respond to critical situations. Tickets are created or updated in your PSA with custom notes, fully classified, and properly assigned to queues. Multiple monitor platforms are supported to deliver a consistent PSA ticket experience, and events can be routed to queues or even different PSAs on a per-customer basis for seamless co-managed IT support.

Platform Automation

Platform automation will vary by RMM platform type, but its goal is to minimize the manual effort required to manage and maintain the RMM platform. Some automation will leverage the filters and policies available on the RMM platform to configure and deploy monitoring, schedule updating, and similar tasks that require manual effort. Other automation will help the RMM Admin to create customer

organizations or schedule server patching using a simple, MS-Excel spreadsheet and local management applications. This can eliminate many manual steps while ensuring a consistent configuration that the automation can leverage. Configuration of the RMM Suite tools is done via a web-based interface, directly on the mspbuilder.com website. This data is ciphered and delivered to endpoints, where it is deciphered before use. All transfers occur over encrypted channels.

Important Operational Concepts

The RMM Suite uses several operational concepts to standardize the configuration and operation of the platform. These standards are critical to the effective and efficient operation of automated technologies.

Managed and Unmanaged Endpoints

One of the most important concepts used by the RMM Suite is the distinction between a "managed" and an "unmanaged" endpoint. In the simplest form, a *managed* endpoint can have all automation applied to it, while an *unmanaged* endpoint will have most automation disabled.

The distinction between managed and unmanaged will vary based on the RMM platform in use, and different RMM platforms will have their own requirements that must be followed.

Kaseya VSA* 9 -** The "root" machine group is named "unm" to designate an unmanaged group. The agent ***must be placed into a group below the unm group for this to function properly. Changing the group name to "m" or anything other than "unm" changes the organization to fully managed.

Other RMMs - Employs a Group custom field "IsManaged" to define the customer status with a Boolean value of Y|N.

Note that the RMM platform may have its own designation for managed/unmanaged, but the RMM Suite specifically uses the IsManaged custom field to control our automation. You can consider the distinction as the RMM Platform defines which customers are managed while the RMM Suite custom field *enables* the automation.

Regardless of which RMM platform you use, all new customers should be initially configured as *unmanaged*. This will allow time to review the customer environment and prepare any configuration overrides that might be required before enabling the automation. Simply change the customer status from *unmanaged* to *managed* to allow the automation to take effect.

Certain automated tasks will be performed even when the customer is set to unmanaged. This includes performing non-invasive tasks such as patch scans and platform audits. The RMM Suite folder structure will be created and populated on all agents regardless of the managed/unmanaged status.

We do not recommend alternate onboarding methods, such as deploying to temporary accounts, as this may not be properly recognized as an unmanaged customer. Always create a proper customer account and machine group in an unmanaged state for onboarding and audit purposes to ensure proper suppression of all automated tasks.

Platform Classification

The RMM Suite can leverage the idea of platform classification to control automation. This allows you to group assets based on the role of the endpoint instead of the Operating System that it runs. For example, you might have a Windows 10 computer running Video Surveillance software, so the system should be treated more like a server. This is not a requirement for operating the RMM Suite, and not every RMM platform supports this, but those that do, our automation will enable this functionality automatically.

Kaseya VSA 9 - the first sub-group is defined as either "servers", "wkstns", or "special to define the operational role.

Other RMMs - An endpoint Custom Field called Host Class can be set as "server" or "workstation".

Location Groups

The RMM Suite can utilize location-specific groupings for customer assets to drive location-specific automation tasks. This could be used to deploy software, alternate licenses, credentials, and more. Not all RMM platforms support this functionality.

The United Nations LOCODE standard is used by default within the RMM Suite tool set. This is a world-wide standard that defines a code for every reasonably-sized city and town in the world. The RMM Suite customer is free to use any coding system they choose, but we strongly recommend the use of site-specific groupings, and our tools can automate the creation of these location groups based on the LOCODE data.

Note that this concept is not limited to use by physical locations. You can define groups of computers that have common configuration or operational requirements, such as grouping by department or computer purpose.

What Happens on Endpoints Every Day…

This is a summary of the automation that is performed on the RMM endpoints every day, and what resources you should review to customize them. Some tasks are specific to workstations or servers and will be identified with a "(w)" or "(s)" notation. The "(a)" notation indicates that the same task and configuration settings are run on all platforms, while the "(w)(s)" notation indicates that the runs on both platforms, but uses platform-specific configuration settings.

Quick-Audit

A quick check of Roles, Features, Services, and Applications is performed to allow dynamic adjustment of Daily Maintenance tasks based on the current endpoint configuration. This audit takes just 7-10 seconds and the user is generally unaware of this event. Pre-maintenance audits allow Daily Maintenance to be used to detect and remediate "Zero-Day" vulnerabilities.

Daily Maintenance

Daily Maintenance performs proactive tasks to keep the endpoint working efficiently and detect problems before they become serious. Tasks can be configured to run once, Daily, Weekly, or Monthly, and can be configured to run or not run based on certain conditions detected on the endpoint. It can also run based on information collected by the MSP Builder Daily Audit tool. The power and flexibility of the Daily Maintenance tool can reduce or even eliminate the need to create RMM platform scripts. Tasks can run both local commands/applications or (where supported by the RMM) execute RMM scripts.

Daily Maintenance Schedule

Maintenance is scheduled to run daily at a time that presents minimal impact on servers and when most workstations are powered-on and available. When the tasks are scheduled by the RMM platform, the distribution window is extended to minimize the RMM platform loading. Autonomous Operation mode places zero load on the RMM platform and targets the tasks for the lowest load times.

Platform	RMM-Initiated	Autonomous Operation Mode
Servers	06:00-08:00	06:00-07:00
Workstations	10:00-16:00	11:00-13:00

To minimize RMM platform and network load, the RMM will randomly schedule the maintenance task on endpoints during the defined schedule window when daily tasks are initiated by the RMM platform. The daily schedule must complete (with or without errors) to be considered as having run. If maintenance does not run on a workstation for 4 or more consecutive days, the end user will receive a message noting that maintenance has been missed and they will be given an opportunity to run all the tasks that have been missed during the past 7 days. Certain tasks - such as programmed reboots and reminder messages - are excluded from this catch-up operation.

NB: When Autonomous Operation Mode is used, the daily tasks will be run automatically upon power-up if the normal schedule was missed, improving maintenance operations.

NB: Daily Maintenance tasks support Class of Service (COS) operation, which allows tasks to be enabled when an endpoint is assigned to a specific Class of Service. COS allows systems to be configured based on arbitrary roles. Tasks can be associated with multiple COS roles.

Maintenance Tasks

The following tasks run on the platforms shown according to a default schedule.

Up-Time Check *Daily* *(w)(s)*

This process runs daily to identify platforms that exceed an uptime threshold. This task runs on both servers and workstations but operates slightly differently on each platform. For servers, only alarms are triggered when the defined thresholds are exceeded. On workstations, the user can be notified when the warning threshold is reached, recommending that they reboot at their convenience. This notice will repeat every 3 days. When the upper threshold is reached, an alert will be generated to notify the MSP of a machine with excessive uptime. *Excessive uptime is an indication that patches are not being applied.*

Patch Reminder *Every Wed* *(w)*

This displays a reminder message to the end-user that patching will be deployed to their computer that evening, explaining that they should log off, not shut down. If Patch + Reboot is enabled, the message will also remind them that their computer will be rebooted. The message - text or BMP image, can be customized by the MSP. This is the RMM Suite default patching schedule, but can be changed to accommodate MSP and customer requirements.

System Snapshot *Daily* *(a)*

The status of all system services, plus a "snapshot" of all running processes is written to a text file. This information is tracked and maintained in daily files for 1 week. The purpose is to potentially determine what is "normal" and what is "unusual" for a given platform

Disable Windows Updates *Every Tue* *(a)*

A task that will update the registry to disable Windows Update. W-U usually needs to be enabled to allow patch scans to run. The scan process does not always disable W-U, so this task ensures that W-U will do its job during the Monday Scans and then be turned off. This task is needed only when the RMM Platform patching enables Windows Update to perform scans but does not disable it when complete. *This should be disabled or removed when using MSP Builder's Flexible Patching.*

Disk Cleanup *Daily* *(a)*

All of the common TEMP file locations are checked for files that are not in use and more than 7 days old - these are removed. Additional folder locations can be specified by the MSP.

Local Backup *Daily* *(w)*

Key files from each user's personal profile folder, including Templates, Favorites, and Shortcuts, are copied to an alternate location on the computer. 7 days of backups are retained, allowing a file to be recovered if accidentally deleted. *This is a same-disk backup and the intent is to rapidly recover critical user files should the user profile become corrupt or a file is accidentally damaged or deleted. It is NOT an alternative to backup for full data recovery.*

Check Disk (CHKDSK) *Weekly* *(w)(s)*

Runs a S.M.A.R.T. check and generates alerts for error conditions. It then runs a CHKDSK command and either generates an alarm on servers or notifies the End-User on workstations if errors are found. If errors are found, the computer is rebooted at midnight, a CHKDSK /F attempts to repair the errors. If it fails to repair the disk, an alert is issued.

Platform Reboot *Every Sun* *(w-optional)*

When the Patch + Reboot configuration is not used, this reboots the workstation every Sunday during the maintenance cycle. If a user is logged in, they are warned of the reboot and given 10 minutes to defer the reboot for 30 minutes. Up to 8 deferrals can be done (4 hours) before the system will restart.

Custom Tasks

Daily Maintenance can be customized to run any script or command - these are simply the tasks and schedules provided in the default configuration. Maintenance can be used to deploy and maintain software, run complex operational tasks, and even perform zero-day remediations. Maintenance provides the ability to perform many tasks including URL file downloads, unzip files, read registry or config file values and use them in commands, create/maintain a local admin account, reboots, and user notifications.

Example Custom Maintenance Tasks:

- Install applications if missing, including the ability to re-install when removed.
- Application Log Management / Cleanup
- Perform user-based automation and configuration tasks for the logged-in user.

Resources for Daily Maintenance

The following resources are available to help you customize the Daily Maintenance components. All of these resources are available from our website. They are updated regularly, so be sure to check the website to ensure you are using the most current resources.

- **RMM Suite Operations Guide - 04 - Daily Audit**
  Details the operation, configuration, and administration of the Daily Audit.
- **RMM Suite Operations Guide - 05 - Daily Maintenance**
  Details the operation, configuration, and administration of the RMM Suite Daily Maintenance.
- **RMM Suite Operations Guide - 12 - Class of Service Operation**
  Details the use of Class of Service operation and configuration methods.
- **How Do I library**
  An ever-growing set of concise documents that explain most of the specific customization processes of the RMM Suite.
- **Self-Paced Training**
  Training guides for various RMM Suite components
    - RSCT-2-CDM - RMM Suite - Configuring Daily Maintenance
    - RSCT-3-TDM - RMM Suite - Troubleshooting Daily Maintenance

Smart Monitors

Smart Monitors are intelligent applications that replace several of the built-in monitoring capabilities as well as provide additional capabilities not offered through the RMM platform. These applications improve the accuracy of the monitoring, significantly reduce false alerts, and even self-remediate many conditions. Like the Daily Maintenance tasks, Smart Monitors can be custom configured to handle exceptions to the norm.

Smart Monitors are executed immediately after the Daily Maintenance cycle completes. Some monitors perform a single check while others run continuously for the next 24-hours, restarting the cycle again the next day. While some Smart Monitors run only on servers or workstations, they all run every day.

There are three key features of Smart Monitors:

1. **Automatically set reasonable thresholds based on the environment, where appropriate.**
2. **Suppress non-critical alarms to allow self-remediation to run (Transient Suppression).**
3. **Perform self-remediation to attempt to self-heal the condition. If self-healing is successful, a telemetry alarm is triggered, logging the event without creating a ticket.**

When a Smart Monitor detects a critical condition or the self-remediation task is unable to resolve the issue, an alarm is generated. Critical conditions do not delay the creation of an alarm!

The following Smart Monitors are part of the current RMM Suite. Since new monitor apps can be added in the future, always refer to the **RMM Suite Operations Guide - Smart Monitors** for the most current information.

Disk Capacity Check (a)

This monitor runs on all platforms to intelligently check the disk capacity and alert when too little free space is found, or when space is being consumed at a high rate.

Each disk volume is identified, classified, and those not meeting criteria for monitoring are eliminated. The remaining volumes are examined, a capacity threshold assigned based on their size, and the status assessed.

If the volume exceeds the calculated threshold by less than 60%, the condition is considered “non-critical”, the alarm is set but not triggered, and an auto-remediation is initiated to aggressively clean up data from temp locations. If - after 48 hours - the condition has not been resolved, the alarm is triggered. If the initial assessment showed that the threshold was exceeded by 60% or more, the alarm would be triggered immediately.

The Smart Monitor also tracks the rate of utilization of each volume and can trigger a warning alarm when the monitor determines that the low-space threshold will be triggered within 30 days at the current rate of consumption. This monitor also ignores the temporary volumes attached during system backup operations to further reduce false alarms from being triggered.

System Security Check (w)

The state of the workstation antivirus products is checked for the following conditions:

- Installed
- Running
- Enabled (protection not suspended/disabled)
- Definitions are current, update initiated if not (where file-based definitions are used)
- Preferred product is installed/running
- Multiple AV products are installed and running
- Duplicate Product registrations in Security Center

Alerts are generated for any condition that does not meet criteria, including when the Preferred Product is defined and not found to be active on the machine. This monitor will ensure that agents are protected with the product that you choose. The RMM Manager will need to define the default Preferred Product if this feature is desired.

This monitor integrates with Microsoft Security Center, which is not available on Server platforms.

Server Boot Monitor (s)

Servers are checked after each system restart to determine if the event occurred during business hours (8 AM to 8 PM, M-F by default). *The business hours and days can be customized*. This alert will trigger for locally initiated reboots, BSOD/system crash, and any other condition that results in a restart of the Server Operating System.

The monitor will also check for and alert when the server is configured to reboot into Safe or Directory Services Restore modes on the next reboot, which could render the system inaccessible. If the system boots into DSRM or Safe Mode with Networking, an alert will be generated if network connectivity is available.

This monitor can be configured to verify that critical services are in a running state 15 minutes after any reboot. This delay provides sufficient time for the server to boot and initialize before checking the service health. *The list of critical services must be customized on a per-machine basis.*

Local User/Group Security Check (a)

The local user accounts and groups are scanned for changes. Any user that is added or removed will generate an alert. Any user added to or removed from an administrator group will generate an alert. When this monitor runs on the domain controller holding the PDCe role, the checks will be performed against the Active Directory domain instead of the local account database. Two different alarms are triggered, one for normal account changes and one for admin accounts. Each can be independently enabled or disabled. A list of "allowed" accounts can be defined to prevent alarms from triggering when they are added to the monitored endpoint.

Network Time Check (a)

The time on the local computer is checked against the domain. When this monitor runs on the domain controller holding the PDCe role, the checks will compare Domain time with a public time source. Non-domain computers have no time reference and will not be checked.

If the time is determined to be out of sync, a sync with the appropriate time source will be initiated. If the difference exceeds 2.5 minutes (enough to affect domain security), an alarm will be triggered.

When run on a domain member Server or Domain Controller that is NOT holding the PDCe role, the Smart Monitor will verify that the time-sync method is using NT5DS. For the DC holding the PDCe role, the check will confirm that NTP is properly configured with a minimum of 3 public time servers, as per best-practice recommendations. *The list of public time servers can be customized, and this should be done for non-US locations.*

Server Operational Health Monitor (s)

Servers will report their operational health status regularly, providing insight on server-up/down more accurately than monitoring the RMM agent software. This monitor also checks the RMM agent service, monitors ongoing performance load issues, and can determine whether certain system services are responding properly - not just whether the service is running. All monitors are self-configuring and require no manual effort to use.

Note that Server Operational Health will eventually become part of the Monitor & Automation Service (MAS) and this monitor (RMSSAM) will be eliminated as a separate component.

Resources for Smart Monitors

The following resources are available to help you customize the Smart Monitor components. All of these resources are available from our website. They are updated regularly, so be sure to check the website to ensure you are using the most current resources.

- **RMM Suite Operations Guide - 06 - Smart Monitors**
  Details the operation, configuration, and administration of the Smart Monitor components.
- **How Do I library**
  An ever-growing set of concise documents that explain most of the specific customization processes of the RMM Suite.
- **Self-Paced Training**
  - RSCT-2-CSM - RMM Suite - Configuring Smart Monitors
  - RSCT-3-TSM - RMM Suite - Troubleshooting Smart Monitors

Daily Audit

The Daily Audit is a highly customizable application that collects data from every endpoint on a daily basis, including gathering results from Daily Maintenance and Smart Monitors. The results of this audit are core to the automation used by the RMM Suite to deploy monitors and even auto-configure Daily Maintenance.

The Daily Audit uses a configuration file to place selected pieces of data into Agent Custom Fields. These can be used to control additional automation, filter and classify agents, or provided data for advanced reporting.

Audit Tagging

When the audit runs, it collects data from many sources and writes it to an "audit cache" file on the endpoint. This file is uploaded (where supported) to the RMM platform when the audit completes. Once the data collection phase completes, the configuration data is examined and "tags" are associated with the various data values. A tag can identify a product or service ("SQL" for SQL Server) or a specific application version ("SQ16" for SQL Server 2016). Generic tags are used to apply monitor sets, while version specific tags can be used for reporting or to drive specific maintenance tasks.

Roles and Features

The endpoint's set of installed Windows Roles and Features is identified, and each is then mapped with a tag that can identify the component. These are generic tags, such as "SQL" or "DNS". These are identified using a standard system call and mapped to pre-defined tags that cannot be changed.

Services and Applications

This data collection can be highly customized to detect customer Line of Business applications and services. This collection pass can generate both generic as well as version-specific tags.

Non-Tagged Data

The remaining data collected is not assigned to tags as it can represent specific configuration items, such as local Firewall status, installed hotfixes, antivirus status, and TPM / Bitlocker status and recovery data.

System Data

This is a collection of information provided by the SystemInfo.exe tool that is part of the Windows platform. This data is extracted, formatted, and written to the audit cache file.

RMM Data

This is a collection of data provided by various RMM Suite tools, including Daily Maintenance and Smart Monitors. Key information such as Bitlocker status and recovery keys, Performance Indicator Data, Directory Service info, Geo-Location data, Battery Status, and more are collected automatically each day.

WMI Data

The Daily Audit allows the MSP to perform arbitrary WMI queries. The results of the queries are written to the audit cache file.

Application Data

All installed applications are reported in the SWINFO section of the SysInfo.ini file. An optional feature is available to compare the current and prior-day data and alarm on software being added, removed, or modified (version change).

This monitor is part of the EMM monitor set. Configuration options are available to generate a single alarm reporting all change or individual alarms per change. A second configuration option suppresses notification of version changes, limiting the alarms to Add or Remove. See the Daily Audit guide for configuration details.

Data Mapping

Data mapping is an extremely powerful ability of the Daily Audit tool. Once all data has been collected, the Data Mapping process will read values from the audit cache file and write them to a specific location. The Agent Custom Field on the RMM Platform is the primary target for this data, and the RMM Suite uses three custom fields to control its automation processes. Additional custom fields can be used to report on configuration or operational status or even drive custom automation. A future update will allow this data to be written directly to a Documentation Platform such as IT Glue or Hudu.

Resources for Daily Audits

The following resources are available to help you customize the Daily Audit components. All of these resources are available from our website. They are updated regularly, so be sure to check the website to ensure you are using the most current resources.

- **RMM Suite Operations Guide - 04 - Daily Audit**
  Details the operation, configuration, and administration of the Daily Audit.
- **How Do I library**
  An ever-growing set of concise documents that explain most of the specific customization processes of the RMM Suite.
- **Self-Paced Training**
  - RSCT-2-UDA - RMM Suite - Understanding Daily Audits
  - RSCT-3-CDA - RMM Suite - Customizing Daily Audits

Onboard Automation / Config-State Management

Onboard automation runs automatically the first time that the RMM Suite tools are deployed. When the RMM platform is configured to automatically install the RMM Suite tools after agent installation, a new computer can be fully configured with all client-specific software deployed without any manual intervention (beyond installing the RMM agent, of course).

Once the initial onboarding completes, the OBA/CSM tool runs daily to compare the actual configuration with the desired configuration, adding or removing software and updating configuration settings. Unlike using the RMM platform to schedule scripts and tracking which systems have or haven't run yet, the OBA/CSM tool runs automatically each day to check the status and make sure that deployment and configuration tasks have run. Since OBA/CSM are closely tied, new agents receive all OBA/CSM actions during the onboard phase.

The RMM Suite OBA/CSM tool employs a configuration file that defines the desired configuration state. There are 6 levels of configuration available, and each level can have zero or more tasks defined.

1. ALL COMPUTERS - generally used to globally deploy MSP software and configuration tasks.
2. ALL SERVERS - as level 1 but specifically targets Server Class or O/S systems.
3. ALL WORKSTATIONS - as level 1 but specifically targets workstation platforms.
4. ALL <CUST> COMPUTERS - performs customer-specific install and configuration tasks,
5. ALL <CUST> SERVERS - performs customer-specific install and config tasks on servers.
6. ALL <CUST> WORKSTATIONS - performs customer-specific install and config tasks on workstations.

Some RMM platforms support an additional level to deploy location/department-specific tasks on workstations. The RMM platform must support Org-level custom fields or Group custom fields.

The first three ALL levels also support Class of Service actioning on RMM platforms that support Org or Group custom fields. A "CCOS" custom field defines a Customer Class of Service (such as Bronze, Silver, or Gold) name. Any number of service classes can be defined, and these can be names or numbers. When a task is mapped to a CCOS ID that matches the customer CCOS value, the task is performed. Transitioning from one Service Class to another is supported, allowing applications to be removed and added based on the original and new class. All actions are automatic and occur when the daily tasks run, even if the computer has been in storage for months and is placed back into service.

Note that a task can be assigned to multiple COS role IDs. These IDs should be defined as a comma-delimited list, with no spaces after the comma. (ie: "bronze,silver") The task will be deployed when an endpoint's COS value matches one of the defined Role IDs.

What Happens Weekly or Monthly

Audits, Maintenance, and Smart Monitors all run daily, but select processes only operate weekly or monthly. Application updating and system patching are two common components that fit this schedule. Patching is available where supported by the RMM platform, and RMM Suite patching tools can be integrated with most RMM and third-party patch solutions.

Patching & Updating

While often considered "maintenance", the RMM Suite distinguishes patching and updating tasks as they are managed and/or tracked by separate components within the RMM platform. Patching has been carefully and precisely configured to ensure the most reliable solution possible.

Server Patching

Server patching is scheduled via an Agent Custom Field using a Patch Code. This code defines the day, week, and time that patching will be initiated. This allows precise control over scheduling, allowing related systems to be patches in a single change window but at different times. This ensures that these systems are restarted in the correct order to allow the application to function. Patching starts with a reboot. After a brief post-reboot delay, the updates are deployed. Once updates are complete, the server boots again to complete the patch process. Four separate Change Windows are available each day, with 8 schedules in each change window. When reboots are allowed, the server will be permitted to repeatedly download & install updates and then reboot until no more updates are available or the update schedule expires. The update schedule is 2.5 hours long.

It is important to understand that servers *require* a patch code to be defined for updates to be performed. Under no circumstance is a server patched or rebooted without the direct control of the RMM Platform Administrator willfully defining a patch code. In addition to the patch codes to schedule updates, there are two schedule codes that actually block automated updates. The code "Manual" indicates that the server should be updated but requires a manual update process. The code "None" indicates that patching is performed via some other method outside of the RMM platform, and most likely, not under the control of the MSP. This might be used when the MSP places an agent onto a server managed by another company, such as process-control machinery.

Workstation Patching & Updating

Workstations are patched once each week, with the schedule defined for each customer via the WS Patching custom field. Scans and pre-downloads occur 2-days prior to the scheduled updates, and the end-users are reminded of patching via Daily Maintenance pop-up notification the day prior to the updates.

The update process starts with an optional reboot at the start of the update schedule. The computer is rebooted if no user is logged in (console and Remote Desktop are checked), or if reboots are enabled in the configuration. If the Application Management feature is subscribed, all supported applications are updated at this time. Applications will be terminated if necessary to permit updating. Once application updates complete, operating system updates will be applied from the content pre-downloaded. If reboots are permitted, then the system will perform an additional scan, download, and update cycle to apply all available updates, rebooting as necessary until either all updates are applied or the update schedule (2-hours) expires.

All reboots are performed by RMM Suite applications, which will prevent automated reboots during business hours and clearly log when reboots are initiated by the tool. Reboot reminder messages (Nags) will be presented hourly when reboots are not automatically performed. These display on-the-hour and can be configured to force a reboot before the end of the business day.

Several options are available to configure workstation patching and rebooting.

Patch, No Reboot, No Continue

This is the default configuration, although *not* the configuration we recommend. This deploys updates *only if the computer is powered on*; reboots only if the user has logged off / nags the user hourly to reboot if they were logged on; and will not continue the patch process when the computer is turned back on. These schedule codes begin with a "P" (P0F1).

Patch, No Reboot, Continue

Similar to above, except that updates and patching will start once the computer is turned back on. This could impact the performance of the system while the user is active. Once updates are complete, the user will be nagged hourly to reboot their computer to complete the updates. These schedule codes begin with a "R" for Resume (R0F1).

Patch, Reboot, No Continue

This is the most effective configuration and the one that we strongly recommend. The process is very structured and provides a very high degree of patch compliance. The process is:

- Notify the end-user during the day prior to scheduled patching that their computer will be rebooted at midnight that night to allow patching to be completed.
- Computer reboots when the Update Schedule starts.
- Application Updates run 10 minutes after the reboot *if Application Management is licensed*.
- Windows Updates run after Application Updates complete.
- Computer reboots to complete installation of updates.

The computer is ready for use on Thursday morning, fully updated. The user is not nagged to restart their computer, and the MSP is not reliant on user compliance to ensure that deployed patches are activated. When this method is used, the weekly reboot configured by Daily Maintenance should be disabled.

Patch, Reboot, Continue

This method is the same as above except that updating and patching will resume the next time the computer is powered on. The user will be given a 10-minute warning for reboot when patching is complete, which could occur during business hours. The pre-patch reboot is not performed if the computer was powered off during the patch schedule.

WOL/VPro Options

Wake on Lan / Wake via VPro options are enabled to attempt to power on agents during the patch window. Results may vary as this configuration depends on the computers having WOL enabled and on a LAN with an active agent to initiate the Wake operation or being a VPro compliant platform. These features must also be supported by the RMM platform.

Available Schedules

The RMM Suite can support 4 schedules in each of the daily Change Windows. These schedules are 3 hours long, start randomly within the first hour so that they complete within 2 hours. The available schedules and change windows are fully documented in the Patching and Updating Operations Guide.

For VIPs or clients that have 24x7 operations, specific change windows can be accommodated by simply applying a Server Patch Code to the workstation's custom field. This will cause the workstation to be patched in the same manner as a server - once monthly in a reboot/update/reboot method at a specific time.

Disabling Windows Update

RMM Platform patch scans generally require that Windows Update be enabled. All RMM Suite patch operations will disable Windows Update once the scans complete to ensure that the RMM Suite maintains control over the patch schedule. Failure to control Windows Update's automatic scheduling could result in unexpected reboots. The RMM platform will employ patch scanning (only) to provide status reporting.

Custom Schedules

Custom patch schedules are not supported and generally are not necessary.

- There are four 6-hour change windows each day starting at Midnight, 6 AM, Noon, and 6 PM.
- Four workstation schedules are available on hourly intervals in each change window and each update schedule lasts for 3 hours. This provides 112 unique schedules each week (16 per day).
- Servers utilize 8 update schedules in each change window. These are on 30-minute intervals and start 30-minutes after the change window begins. Monitoring is automatically suppressed during server updates. This provides 224 unique schedules per week (32 per day).
- All schedules are configured so that updating will begin and end within the change window. This allows for alarm suppression and working with groups of related application servers to ensure that the patch and reboot in the correct order.

Resources for Patching & Updating

The following resources are available to help you customize the Patching and Updating components. All of these resources are available from our website. They are updated regularly, so be sure to check the website to ensure you are using the most current resources.

- **RMM Suite Operations Guide - 03 - Patching & Updating**
- **How Do I library**
  An ever-growing set of concise documents that explain most of the specific customization processes of the RMM Suite.
- **Self-Paced Training**
  - RSCT-2-APU - RMM Suite - Application & Patch Updating

Configuration Overview

Understanding the configuration options is key to leveraging the features of the RMM Suite platform. All of the RMM Suite tools can be customized by setting defaults, and then creating configurations to override the settings on a customer, location, or individual agent basis.

Configuration for all RMM Suite tools is managed via the MSP Builder website. Clients log in and will have access to the Configuration Management interface. Technician accounts will have READ access to this by default, but customers can grant MODIFY access to specific technicians. This will help to better control updates, particularly for larger organizations with many technicians. By default, the account owner has the ability to define technician access to READ or MODIFY. They can request (in writing) that this access be extended to a designated alternate staff member.

When the RMM Suite is installed, the customer will receive a default set of configuration parameters. These have been carefully selected to provide "safe and sane" default settings appropriate for most configurations. These defaults can be adjusted to meet the RMM Suite client's typical requirements.

When special situations arise, an override can be created at the proper level - customer, location, or agent. When the override page is selected, it will be populated with the defaults from the next higher level. For example, if you have a customer override and then create a site override for that customer, the new site settings will be inherited from the customer level data.

Daily Maintenance

There are several configuration collections for Daily Maintenance. The primary collection defines the maintenance tasks and their schedules. The secondary collections define the settings of specific maintenance tools that are in the RMM Suite.

Smart Monitors

Like Daily Maintenance, there are several configuration collections for Smart Monitors. All of these collections, however, are for settings used by specific Smart Monitor applications.

Daily Audit

There is just one configuration collection for Daily Audits. The collection defines all the parameters needed to define the tagging, optional data collection, and mapping of data values to custom fields and, in the future, documentation platforms such as Hudu and IT Glue.

Special Considerations

- New configuration options
  When new configuration options are defined at the root (defaults) level, they will not automatically propagate to lower-level overrides. There is an option in the configuration management portal to push out the changes to lower-level overrides.
- Removing an override
  When an override is no longer needed, it should be removed. The interface allows deleting the override data. By removing the unneeded overrides, you will be assured that any changes to the default or higher-level configurations will properly apply.

  NB: *When a significant change is made to a default or higher (broader) level that must be propagated to the lower (override) level, it may be easier to delete the override configuration and recreate it, which will add all of the default settings and values from the higher levels.*

This Page Intentionally Left Blank.

Monitoring

There are two general types of monitors provided by the RMM Suite - RMM Platform Monitors and Smart Monitors. Each type of monitor has its own specific benefits and advantages. Regardless of the type of monitor used, the RMM Suite automation automatically determines which monitors to apply, and all use a consistent naming format that allows our Intelligent Ticket Processing system to process the event, perform deduplication, automated remediation tasks, and deliver fully customized and classified tickets into the PSA. Monitors are placed into "sets", which is a collection of related monitors of different types (Service and Event Log) and priorities.

Endpoint Monitors

These monitors are most often used to process service faults or respond to Windows Event Log error messages. These monitors rarely have any "threshold" values beyond - possibly - event counts or durations. For example, a Windows Event Log alarm might not be triggered unless it happens several times in a specific time duration. In most cases, these platform monitors will trigger when the event happens and then suppress repeated alarms for a period of time. The RMM Suite provides Cloud-Based monitoring by default and - for select platforms - can provide RMM platform-based monitors. Both types provide identical capabilities, but cloud-based monitors are updated faster and more often than RMM platform based monitors and are the preferred method of monitoring.

Endpoint monitors are applied based on the results of the RMM Suite Daily Audit. The audit process detects system Roles, Features, Services, and Applications and applies a "TAG" to a **System Roles** custom field when one of these components are detected. This detection process is fully customizable to support Line of Business applications.

Controlling Endpoint Monitoring

Each monitor collection can be disabled by placing the TAG value that enabled it into the **Policy Control** custom field. For example, if Audit detects a DNS server is installed, the System Roles field will contain "DNS" and is a trigger to enable that monitor. However, placing "DNS" into the Policy Control field will override that trigger and prevent that monitor collection from being applied.

Smart Monitors

The RMM Suite Smart Monitors are applications that intelligently perform monitoring when specific environmental conditions should be considered, or when other complex combinations of events must be considered. For example, the Disk Capacity monitor automatically sets the low-space alarm threshold based on the actual size of the disk; and the Antivirus Status monitor can check for specific products, ignore secondary products, and automatically initiate updates for definition-based products.

Controlling Smart Monitors

There are two methods for controlling Smart Monitors - *configuration* and *enablement*. Most Smart Monitors have a corresponding configuration file in the RMM Suite Management Portal that defines specific operational parameters, such as adjusting thresholds or suppressing specific alerts. Smart Monitors also support enablement through the Policy Control custom field, specifically disabling the operation of the smart monitor via an "SM*xxx*" tag - where "*xxx*" is the three-letter identity of the Smart Monitor. ALL Smart Monitors can be disabled via deploying the "SMON" tag.

Monitor Set Naming

This information explains the format of the RMM Suite monitors and is essential for creating custom monitors or adapting existing RMM Platform monitors for use with ITP alarm processing.

Each monitor set, regardless of type, has a unique name that identifies the monitor, it's category, platform type (server or workstation), priority, and response action. This name is referred to as the Monitor Set ID (MONSETID). The Monitor Set ID is combined with a standard alarm subject that can provide additional data related to the event.

An RMM Suite alarm subject contains 6 parts delimited with vertical bars as shown here:

```
Name | Type | Data 1 | Data 2 | Data 3 | MonSetID
```

Spaces have been added for clarity but are not present in an actual alarm subject.

Name The unique name of the monitor.

Type The alarm type - usually Alarm or Warning.

Data 1-3 Up to 3 optional values to qualify/quantify the alarm condition.

MonSetID The Monitor Set ID, described below.

The Monitor Set ID consists of 5 parts, delimited with periods - shown below:

```
Name . Category . P-Type . Priority . Action
```

Again, spaces have been added for clarity.

Name The unique name of the Monitor Set ID. When used for Event Logs, it may also include a code to identify a specific event log being monitored.

Category A 3-4 character code to categorize similar alarms.

P-Type The Platform Type identifier, such as "W" for workstations, "S" for servers, or "X" for a generic monitor.

Priority The initial priority associated with the monitor set. This is the letter "P" followed by a digit in the range of 1-5. Our classifications are Critical (1), High (2), Medium (3), Low (4), Informational (5).

Action This is no longer used by ITP and previously helped to distinguish between Alarms, Actionable Alarms, and Requests. This is simply "alm" in all current RMM Suite alarms as the control is now performed within ITP based on the Category, Name, and Event ID (Data 1) values.

Automatic Processing

All RMM Suite monitors follow this alarm subject format to be able to map an event to specific process actions. The Intelligent Ticket Processing system can use this data to replace the subject with content that is meaningful to your technicians. It can assign up to 3 classification values (Issue/Sub-Issue:Item or Type/Subtype/Item) that can improve reporting or drive PSA workflow automation. The subject and classification data are fully customizable to easily integrate into existing PSA operations. Most PSA platforms allow routing of tickets to specific service boards/queues based on customer, alert type, and agent type.

For PSA platforms supported by an email-only integration, the subject and body include a unique event code that can be used to easily identify each of the hundreds of RMM Suite monitors. The code is included in subject and body to support all forms of PSA event parsing.

Co-Managed IT Support

ITP can easily handle co-managed IT situations by routing alerts to a unique queue or even a completely different PSA on a customer-by-customer basis. There is no additional fee to support multiple PSA platforms, although there may be a small service charge to assist in the install and configuration where complex integrations are requested.

Non-Standard / Custom Monitor Processing

Many RMM platforms can accept incoming email-based alerts from non-compute devices such as routers, switches, and power devices. ITP can examine these text-based subject lines and map key words or phrases into a proper RMM Suite subject format, allowing the full power of ITP to be leveraged. ITP can also initiate advanced parsing modules to extract data from the email body or decide to completely suppress informational messages. This mapping is the responsibility of the RMM Suite customer.

To make sure this mapping takes place, ITP considers any alarm that it cannot process as a "process failure". It passes the alert data directly to the PSA without any modification and sends an email to the RMM admin team to notify them that an unprocessed alarm was handled. The admin team should review these emails regularly and either configure ITP to handle the event or request an advanced processing module from MSP Builder. This provides a great deal of power and flexibility in handling non-agent alarm events.

Multi-RMM Platform Support

ITP can process alarm events from multiple RMM/monitoring platforms to provide a consistent integration between monitoring and ticketing. In a base configuration, ITP receives alarm data from the MSP Builder cloud servers and the MSP's primary RMM platform. If other monitoring platforms are used to provide dedicated network or Apple Macintosh monitoring, these can be queried with additional plug-in modules. Secondary monitoring modules are expected to released as demand warrants.

PSA Integration

The Intelligent Ticket Processing system can communicate with several popular PSA platforms via an advanced API integration. ITP currently supports an API integration for ConnectWise Manage, Datto Autotask, Kaseya BMS, and Halo PSA. Any other PSA can be supported with an email-based integration that provides unique parsing keys for each alarm event. The API integration provides 2-way communication, allowing ITP to determine if it should open a new ticket or update an existing, open ticket.

All API integrations will fall back to email-based communication to ensure that alarm tickets are never lost due to communication failures or temporary PSA outages. MSP Builder provides a Secure Mail Relay service to route email that can be subscribed if internal mail relay services are not available.

Smart Paging Support

ITP can notify an on-call team when priority alarms occur when the MSP/IT help desk is not staffed. Notifications are limited to server and network devices, alarms at High or Critical priority, and by defined customer operating hours. When alarms occur overnight and outside of client operating hours, the notification is deferred to an early-morning time. By intelligently combining priority with customer operating hours, the overnight calls are minimized. Many third-party paging services are supported, including On-Page, PagerDuty, and others. This requires a separate subscription to the pager service. Integration to Teams, Slack, and similar services is possible through this mechanism without additional cost, although integration with these services is the responsibility of the customer.

NOC Services Notification

ITP can integrate with third-party NOC services, allowing them to be notified of priority events. This notification runs in addition to creating a ticket in your PSA. This can also be used to provide customer notifications for alarm events. Supports client-specific configuration.

ITP Hosting

The ITP server service is generally installed on a customer provided host, which should be operated and maintained like any other server. It is essential that it function 24/7 with specific, scheduled monthly change windows for patching the O/S. ITP software is self-maintaining and checks for updates nightly at midnight. Updates are automatic and do not require service restarts. Changes to ITP service configuration settings are detected within 5 minutes and applied to the running configuration. Changes to process configuration apply immediately.

The ITP host requires a minimum of 1 CPU, 4GB RAM, and 750 MB of disk space running on any current Windows O/S - server or workstation.

MSP Builder can provide hosting of the ITP server for customers that prefer not to self-host. Contact sales for a quote, which will vary based on agent count and custom configuration needs.

Quick Reference

The Quick Reference section provides a mapping between "I need to" and the corresponding RMM Suite tool or configuration method. This will also reference the appropriate operations guide where additional details can be obtained, where appropriate.

Configuration & Control

- Disable a Monitor
  Use the Policy Control scripts to apply a TAG that corresponds to the TAG in the System Roles custom field that enabled the monitor.
- Disable a Smart Monitor
  Smart Monitors can be disabled using the Policy Control script. Pre-made scripts are present to disable ALL Smart Monitors. A specific Smart Monitor can be disabled by specifying "SM*xxx*", where "*xxx*" is the 3-letter code that identifies the Smart Monitor.
- Configure a Smart Monitor
  Most Smart Monitors can be customized and configured via the RMM Suite Management Portal on the mspbuilder.com website.
- Suppress running OBA and CSM tasks by applying a Policy Control TAG. XOBA suppresses both OBA and CSM actions, while XCSM allows OBA and suppresses daily CSM actions.

Automation Resources

- Automatically deploy an application
  Both Daily Maintenance and Onboard Automation can be used to deploy an application.
  - Daily Maintenance should be used with a Role or Control so it triggers only when necessary.
  - Onboard Automation will run either an RMM script or a CET package *one time*, tracking the execution and preventing additional attempts without additional configuration effort.
- Automatically deploy a missing application, re-deploy if/when necessary
  Both Daily Maintenance and Onboard Automation can be used to deploy missing applications. Configuring the Daily Audit to detect the application and apply a TAG is necessary.
  - Daily Maintenance should be used with a Role so it triggers only when necessary. Define the Role parameter with a dash prefixing the tag to indicate "not present".
  - Onboard Automation can switch from "one time only" to "when missing" by configuring a Class of Service. Define the COS code and a "-TAG" to cause the application install to be executed when Audit detects that the application is missing.
-