The RMM Suite
Operations & Customization Guide

Smart Monitors

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

Last Updated: 2025/03/27

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The MSP Builder RMM Suite contains proprietary software, including unpublished source code.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 ("COMPANY") CONFIDENTIAL

NOTICE: All information contained herein is and remains the property of COMPANY. The intellectual and technical concepts contained herein are proprietary to COMPANY and may be covered by U.S. and Foreign Patents, patents in process, and are protected by trade secret or copyright law.

Dissemination of this information or reproduction of this material is strictly forbidden unless prior written permission is obtained from COMPANY. Access to the source code contained herein is hereby forbidden to anyone except current COMPANY employees, managers or contractors who have executed Confidentiality and Non-disclosure agreements explicitly covering such access.

The copyright notice above does not evidence any actual or intended publication or disclosure of this source code, which includes information that is confidential and/or proprietary, and is a trade secret, of COMPANY. ANY REPRODUCTION, MODIFICATION, DISTRIBUTION, PUBLIC PERFORMANCE, OR PUBLIC DISPLAY OF OR THROUGH USE OF THIS SOURCE CODE WITHOUT THE EXPRESS WRITTEN CONSENT OF COMPANY IS STRICTLY PROHIBITED, AND IN VIOLATION OF APPLICABLE LAWS AND INTERNATIONAL TREATIES. THE RECEIPT OR POSSESSION OF THIS SOURCE CODE AND/OR RELATED INFORMATION DOES NOT CONVEY OR IMPLY ANY RIGHTS TO REPRODUCE, DISCLOSE OR DISTRIBUTE ITS CONTENTS, OR TO MANUFACTURE, USE, OR SELL ANYTHING THAT IT MAY DESCRIBE, IN WHOLE OR IN PART.

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

Contents

Introduction

The MSP Builder RMM Suite utilizes Smart Monitor technology to provide intelligence at the endpoint for monitoring components that are traditionally difficult, inaccurate, or simply unavailable through standard RMM components. There are three key parts to MSP Builder's Smart Monitor technology.

Intelligent Automatic Thresholds

The ability to automatically set a custom alert threshold based on actual environmental conditions is one of the most important features of Smart Monitors. Unlike typical RMM monitors that have a fixed threshold, or require you to manually assess the environment an manually apply an appropriate monitor set, Smart Monitors evaluate the environment and calculate the most appropriate threshold to use.

Consider disk capacity monitors - RMM monitoring uses a single threshold value, typically between 10 and 20%. As disk sizes increase, these values result in a high number of false alarms. The Smart Monitor instead examines the disk configuration every hour and generates a threshold based on the size of the volume. Thus, smaller drives have higher thresholds - around 11-14% - while large, multi-terabyte drives have lower thresholds - closer to 2-4%. This increases the accuracy of monitoring, significantly reduces false alerts, and requires no additional effort by the technician to configure. Thresholds can be manually overridden where needed for unique situations.

Self-Remediation

Many Smart Monitors have the ability to correct common situations without generating a service ticket. A Disk Capacity alarm will trigger a cleanup of temp folders that's more aggressive than the daily cleanup task, while the Antivirus Status monitor can detect when definitions are outdated and initiate the update process. These remediation tasks run automatically when the event is detected.

Note that Self-Remediation is quite different from the Auto-Remediation capabilities of the RMM Suite. Self-Remediation occurs through the Smart Monitor logic and *happens before an alarm is triggered*. Auto-Remediation is a process that initiates an RMM platform script *in response to an alarm*. Self-Remediation will prevent both the alarm and the resulting PSA ticket, while Auto-Remediation can only change the status of the ticket it creates in the PSA. If Auto-Remediation is successful, a ticket is created in the PSA with a *Complete* status instead of a *New/Open* status.

Transient Event Suppression

When the Smart Monitor is capable of self-remediation, the severity of the condition is evaluated. If the severity is not considered critical, the alarm state is set, but creation of the alarm event is suppressed for up to 48 hours to allow the Self-Remediation tasks time to work. If the condition is at a critical level, the alarm will be triggered immediately. If, during the suppression period, the self-remediation reports that it was unable to resolve the condition, the alarm is submitted without further delay.

Command-Line Arguments

Many of these Smart Monitor applications can accept command-line arguments. These are not used (or needed) when invoked through Daily Automation. They are primarily used when executed manually, whether to obtain information, set machine-specific controls, or perform specific tasks for testing or addressing unusual conditions. All normal operation is controlled by the configuration file and settings defined in the MSPB Management Portal.

This Page Intentionally Left Blank.

General Operation

Operation of the Smart Monitors is highly automated - a Smart Monitor Sequencer runs as part of the RMM Suite Daily Tasks. The sequencer application consults a configuration file (managed by MSP Builder) to execute the individual Smart Monitors based on the platform type and class. If the type or class match, the specific Smart Monitor is executed.

Some Smart Monitors are designed for specific platforms - the AntiVirus Status, for example, only runs on workstations (due to Microsoft's decision to not support Security Center on servers), while other Smart Monitors are specific to servers (booting during business hours, for example). The RMM Suite default is to run the appropriate Smart Monitors on every managed machine, using reasonable defaults. This minimizes the amount of custom configuration necessary to effectively and appropriately provide monitoring within a client environment.

While the default settings used by Smart Monitors are appropriate (or auto-adjust) for most situations, there are times where something will need to be customized or a Smart Monitor disabled.

Disabling Smart Monitors

While uncommon, globally disabling a Smart Monitor can be done by defining a control in the root-level configuration file associated with a specific Smart Monitor. When disabled in this way, the Smart Monitor will launch and immediately exit without performing any work.

It is far more common to disable a specific Smart Monitor on a particular endpoint. This is done easily with an RMM script. Each Smart Monitor has a 5-character Control Code in the form "SMxxx". That code can be placed into the Policy Control field for a specific machine. When the Smart Monitor starts up, it will exit immediately without any action if the control code is found. Smart Monitors that run on a regular cycle - such as Server Operational Health and Disk Capacity - will not enable the schedule. The Smart Monitor will be suppressed for that day's cycle. This allows you to later remove the Control Code and permit the Smart Monitor to operate during the next scheduled daily cycle.

The Control Code for each Smart Monitor is "SM" plus the last 3 characters of the Smart Monitor name. The IDs are defined in **Appendix I – Smart Monitor Identification** later in this guide. You can also find configuration notes in our website's Telemetry pages by selecting Smart Monitors and one of the related alarm events. (ex. To disable the Server Boot Monitor – RMSSBM – apply the SMSBM tag in Policy Control. Suppression can also be applied manually to an entire customer organization by adding the blocker tag, with added dashes, to the PControl Org-level custom field.

Customizing Smart Monitors

In some cases, the default settings used by Smart Monitors must be adjusted. A common example is altering the Disk Capacity Smart Monitor settings to adjust for an exceptionally small disk, or when the applications running manage the disk space at a level below our default thresholds.

The Smart Monitors utilize a standard INI-file format. These data files are removed at the start of each day's cycle, securely downloaded from the MSP Builder cloud, decrypted, and written to the local disk. This prevents using any manually created local changes during automated operation. You can, however, edit the local file settings and invoke the individual Smart Monitor manually. This is useful when you want to test the new configuration before updating the settings in our cloud and deploying them on a wider scale.

Use of the MSP Builder Cloud Configuration System is documented in a specific Operations Guide. The individual Smart Monitor options are discussed in the next section of this guide.

Smart Monitor Operation

The operation and customization of each Smart Monitor will be detailed in this section. We recommend that you reference this guide/section when defining custom configuration settings in the MSP Builder cloud server environment.

Note that each Smart Monitor application employs a consistent naming format. Smart Monitor applications begin with "RMS" and are followed with 3 characters that identify the specific Smart Monitor. All RMM Suite applications use a ".BMS" file extension. The log files that are generated are written to the **`%PROGRAMDATA%\MSPB\Logs`** subfolder and employ a similar naming format. The Smart Monitor ID "RMSxxx" is followed by a format that includes the day number (0-6=Sun-Sat) followed by the 3-letter abbreviated day name. This groups all logs from a specific application together and displays them in day-sequence when sorting by name.

Current Smart Monitors

RMSSEQ — The Smart Monitor Sequencer
No customization or configuration is possible. Logs report the actions performed.

RMSSSC — System Security Checks
Performs checks for AV security operational status as well as identifying when multiple products are running or a preferred product is not found. Defining the "Preferred Product" is a required customization task if this check is to be used!

RMSSBM — Server Boot Monitor
This monitor reports when servers reboot during business hours and can be customized to report an additional alarm status when specific applications or services are not running within 15-minutes of the reboot.

RMSICC — Internet Connectivity Check
This manually applied monitor reports when a customer with redundant Internet connections has switched between primary and secondary connections.

RMSOAM — Server Operational Availability Monitor
A monitor that reports on the general health, connectivity, performance, and overall operational capability of the computer, independent of the RMM agent software.

RMSDCC — Disk Capacity Monitoring
Performs a detailed analysis of each disk volume, excluding those that don't meet the criteria for monitoring (flash, removable, temporary, etc.) and then generates a specific threshold for each volume based on its size. It also tracks "rate of use" to alarm proactively when volumes are filling rapidly.

RMSUSC — User Security Check
Reports when local or domain users are added or removed from an endpoint. Separate alarms are configurable for regular and administrative users.

RMSNTP — Network Time Protocol Check
This monitor performs two separate checks - one to verify that local time is in-sync with the domain, and a second check that ensures that the time sync service is properly configured as per Microsoft's standards. This monitor does not perform any monitoring on endpoints that are not domain-joined.

RMSSSC System Security Checks

Determines the state of the AV & security products, alerting if missing, outdated or not running.

Summary

This is a Workstation-only utility that uses Microsoft's Security Center API to determine the AV product(s), status, and related information. The API is not available on server platforms, so this monitor will exit silently when a server operating system is detected. The AV Status field will show "API Unsupported" on servers to indicate that the Smart Monitor has run and exited.

Alerting

The following alerts are generated by this Smart Monitor.

Class	Event	Source	Message
INFO	110	RMM-SMARTMON	RMSSSC: Security Checks Performed.
INFO	110	RMM-SMARTMON	RMSSSC: STATUS: <message>
ERROR	111	RMM-SMARTMON	RMSSSC: Antivirus - Product not detected!
ERROR	112	RMM-SMARTMON	RMSSSC: Antivirus - Outdated - <AV_NAME>
ERROR	113	RMM-SMARTMON	RMSSSC: Antivirus - Not running - <AV_NAME>
ERROR	114	RMM-SMARTMON	RMSSSC: Antivirus - Multiple products are running!
ERROR	115	RMM-SMARTMON	RMSSSC: Antivirus - Protection is suspended - <AV_NAME>
ERROR	116	RMM-SMARTMON	RMSSSC: Antivirus - Preferred Product not installed!
ERROR	117	RMM-SMARTMON	RMSSSC: Antivirus - Duplicate product registrations

The "Info" events do not generate alarms and are used to provide operational status only. Error 117 will not create an alarm event by default but will report the condition in the AV Status field.

Transient Suppression

Varies – most conditions alert immediately and then suppress additional alerts, limiting them to once every 3 days, while the Outdated alert (112) will not alert for 48 hours while self-remediation attempts to resolve the issue, then will alert every 3 days thereafter until resolved.

Self-Remediation

If the detected AV definitions are not current, the commands defined in the configuration file for the identified product are run to initiate a manual definition update. In many cases, the next check will find that the definitions are current, and no alert will be generated. When the update fails, an alert will be generated when the transient suppression period expires. This often indicates that the agent is incapable of accessing the definition update URL either due to an invalid setting or other security software blocking the update URL.

Arguments

--s run silently, suppress all screen output. This monitor normally displays status on the console window.

--d enables debug logging – additional status messages are displayed and logged. The MSP can run this utility locally in Debug mode to display the status data used to determine various conditions. *In particular, this option displays the product name defined in MSSC, which must be used exactly as shown when setting the Preferred Product*

--a display status (audit) – used with other automation to report whether the condition(s) that caused an alert still exist.

--p:name specify the preferred product. Run the RMSSSC.BMS script interactively in Debug mode to see the list of product names, or check the latest log file. This argument is typically used to override the Preferred Product defined in the configuration file to validate the name.

Configuration File & Parameters

The configuration file for this Smart Monitor named "**RMSSSC.ini**" and is *required* for operation. It has certain default settings like other Smart Monitors, but there are two required parameters that are defined in the configuration file. The first is the Preferred Product (which is usually MSP-specific) and then one or more Remediation definitions.

COMMON Section

This section controls the operation of the Smart Monitor.

Preferred The name of the preferred antivirus product. When not defined, error 116 is never triggered by the monitor.
When the AV product experiences a name change, you can specify the old and new names, separated by a comma. This should only be done when a single AV product reports multiple names to Microsoft Security Center.

MultipleAllowed A list of products that are allowed to run concurrently.

SkipAll If true, all alerts are suppressed.

SkipEventID_# If true, the alert ID specified is suppressed. Multiple individual alerts can be suppressed by specifying individual SkipEventID values. See the list of alert code numbers under the Alerting section above.

Product_AV

This section is named after the product and must include the "_AV" suffix. A section can exist for each of multiple AV products, and define the steps to take to identify and then run the process to manually update the definitions. It supports the following configuration values:

Type Either REG or CMD, determining whether to obtain the command from a PATH## or KEY## parameter.

Path## The disk path where the command is located. "##" is either 32 or 64 and represents the value for 32 or 64-bit platforms.

Reg## The registry path where the command path is defined. "##" is either 32 or 64 and represents the value for 32 or 64-bit platforms.

RVal The registry value to read to obtain the command folder path, or use "#ENUM#" to enumerate the values in the key.

Cmd The command to run after appending it to the path extracted from the Path or Key values above.

Arg The argument(s), if any, to pass to the command to initiate a definition update.

Response A key word or phrase to check for in the response to determine if the request was successful.

Note:
These definitions are required only for definition-based products to define the commands needed to initiate a definition update. The Product_AV definitions are provided and maintained by MSP Builder. If you use an AV / Security product that is not supported, contact MSP Builder support to request a definition be added.

RMSSBM – Server Boot Monitor

Alerts when a server boots during business hours or into DSRM or Safe Mode.

Summary

This Smart Monitor will alert after any reboot that occurs during normal business operating hours – 8am to 9pm local time by default. It will alert when the server is *configured* to boot into Safe Mode or Directory Services Restore Mode on the next system restart, and will alert if the server has booted into the Safe Mode with Networking state. The Smart Monitor creates an At Startup scheduled task to perform the post-reboot checks. This task is removed and recreated each day when the Smart Monitors initialize.

Alerting

The following alerts are generated by this Smart Monitor.

Class	Event	Source	Message
ERROR	121	RMM-SMARTMON	RMSSBM: The system has booted into Safe Mode.
ERROR	122	RMM-SMARTMON	RMSSBM: The system has booted into Directory Services Restore Mode
ERROR	123	RMM-SMARTMON	RMSSBM: The system has Safe Mode Boot enabled
ERROR	124	RMM-SMARTMON	RMSSBM: One or more monitored services have failed to start
ERROR	126	RMM-SMARTMON	RMSSBM: The system has booted during business hours.
ERROR	129	RMM-SMARTMON	RMSSBM: Unable to calculate uptime.

The “Info” events do not generate alarms and are used to provide operational status only.

Transient Suppression

None – all alerts are triggered upon detection. The Safe Mode alerts are suppressed for a defined period (default – 15 minutes) after system boot to allow time for an engineer to perform a controlled boot into Safe Mode, perform a remediation task, and then reboot normally. The intent is to alert on unintentional or uncontrolled booting into Safe Mode in response to a boot-detected issue. Event 123 will alert that the next reboot of the server will cause it to start in Safe Mode. This is a predictive alert and not indicative of the current system state.

Self-Remediation

None.

Arguments

--d	enables debug logging – additional status messages are displayed and logged.
--c	Enables the checks. Without this argument, it creates the “at startup” scheduled task.
--r	Removes the Startup Task and exits.

Configuration File & Parameters

The configuration file “**RMSSBM.INI**” is used to alter the Safe Mode detection timer, the business operational hours, and to include Weekends in the business hour time period.

COMMON Section

SMDetectTimer The time delay (in minutes) after booting into safe mode before an alert is generated. The default value is 15 minutes, which is also the minimum allowed value. When changing this value, it is not recommended to use values above 60 to ensure effective alerting.

BusinessHours A comma-delimited pair of HH:MM values that define the start and end of what should be considered “business hours”. The default range is 8am to 9pm (08:00,21:00), Monday through Friday.

Weekend A Boolean (T/F) value that, when True, includes Saturday and Sunday in the business hours reboot alerting process.

SERVICES Section

ServiceName A Boolean (T/F) value that, when True, generates an error if the named service is not running after the startup delay timer has expired.

RMSICC - Internet Connectivity Checks

Provides notification when Internet Connection transitions between Primary and Backup links.

Summary

This is a manually-applied Smart Monitor that will trigger an alarm each time the configured Internet connection transitions from or to the primary interface. The monitor tracks the public IP address and triggers when that address changes. This monitor is optional and does not necessarily indicate a problem, although it can be used to trigger actions or notifications that might be needed when the public IP address changes.

Alerting

WARN	- 131	RMM-SMARTMON	RMSICC: On Primary Connection
WARN	- 132	RMM-SMARTMON	RMSICC: On Backup Connection
ERROR	- 135	RMM-SMARTMON	RMSICC: Primary IP not set - NOT CONFIGURED!
ERROR	- 136	RMM-SMARTMON	RMSICC: Unsupported Platform!

Transient Suppression

None - the alarm triggers when the transition between primary and backup connection is detected.

Self-Remediation

None. The monitor can be configured for Auto-Remediation actions performed by ITP, where necessary.

Arguments

--d	enables debug logging – additional status messages are displayed and logged.
--SETA	Automatically sets the primary address to the current public IP Address. This is used when invoked via an RMM script.
--SET	Confirms that the current public IP Address should be set to the primary address. This should be run manually when the primary address is active. *Do not use this argument for any form of automation!*

Configuration File & Parameters

None - all configuration is performed automatically when the primary public IP Address is active.

Deployment

This tool should be deployed in an environment where both primary and backup Internet connections are available. It may be deployed to any server class system (any Windows O/S that is operational 24/7). The Smart Monitor configures itself to identify the primary IP Address and then run via Task Scheduler on a 5-minute interval. Care should be taken to perform the deployment when the primary IP Address is active, and to not deploy more than one such monitor per customer site.

The alarm will be associated with the computer where it was installed. Despite this, the alarm represents the state of the Internet connection for the entire site. This is due to the fact that most RMM platforms associate alerts with specific assets.

See Also

Consider leveraging the ITP Web/Connection Monitor to track the state of customer Internet Gateways to report on the loss of Internet connectivity for sites without redundant connections.

RMSOAM - Server Operational Availability Monitor

Reports on an assortment of conditions that could impact operational availability, including network & Internet connectivity, extreme load, RMM Agent failure, and core service issues.

Summary

This is an automatically deployed Out of Band (OOB) monitor that tracks operational status of an endpoint. This monitor requires that the server can reach the MSP Builder cloud server. If servers are unable to connect to the Internet, this monitor will not function, and an alarm may result.

Specific monitoring tasks include:

- Server is powered off unexpectedly for 12+ minutes.
- Communication - Alarms if the server may be unable to communicate on the network or to the Internet.
- Extended High Load - Alarms when CPU or RAM utilization exceed set thresholds for 30+ minutes OR the system resource levels prevent SAM from functioning.
- RMM Agent - Alarms when the RMM platform-specific service has stopped and can't be restarted, or if key services or components are missing.
- Service Operation - Alarms when select system services do not respond properly. Unlike typical RMM Service Monitors that report when a service has stopped, this monitor will attempt to communicate with the service and determine its operational status.

Each monitor is capable of triggering independent alarm notifications. When multiple conditions are reported, a single ticket is created with information related to each issue. No further tickets will be generated until the conditions have been cleared during a given day. A communication failure - inability to communicate to the MSP Builder cloud server - will take precedence over all other conditions when creating alarms.

NOTE:

As this monitor operates outside of the RMM platform and its primary purpose is to alert when key server services are unavailable, specific actions are required when decommissioning a server. Prior to shutting down a server for an extended period or permanently, perform any one of the following tasks:

- Use the MSPB RMUWRT application to shut the system down. This will clear the SAM monitors. **`RSRUN RMUWRT --SHUT --G:0`**
- Use the RMSSAM application to clear the monitoring status prior to invoking the local shutdown command. **`RSRUN RMSSAM --CLEAR`**
- Remove the RMM Suite software from the device. This is the preferred method for a permanent decommissioning of any device. **`RSRUN RMURMRS`** or the WIN-Offboard RMM Suite script on the RMM platform.

Alerting

Alerts are presented directly from ITP. No local event log alarms are recorded.

Transient Suppression

Yes - once an alarm is triggered, it will not be repeated until the condition has been cleared. Most events must exceed a time duration. Communication failures, including server offline, trigger after 14 minutes; excessive load alarms trigger after 30-minutes of continuous high-load state; Service Operation and RMM Agent Status will trigger after 14-minutes in continuous fault status. The condition of missing RMM components is not deferred and will trigger upon detection.

Self-Remediation

If the RMM Agent Software service is not running, an attempt to restart it will be made. An alarm will trigger if the restart was unsuccessful.

Arguments

--D	enables debug logging – additional status messages are displayed and logged.
--CW[:#]	Initiates a Change Window for # minutes (default is 720 or 6 hours). The monitor is disabled for this period of time and will not generate an OAM alarm for any condition.
--SHUTDOWN	Terminates operation of the OAM Smart Monitor and create a task to resume monitoring after the system reboots. This suppresses operation from the point the command is issued until it restarts after a system reboot. This can be initiated by RMM-initiated reboot scripts to minimize the time when monitoring is suppressed.
--STOP	Terminates operation of the OAM Smart Monitor. The Smart Monitor will not restart unless initiated by an external process, such as the daily Smart Monitor sequencer application.
--ST	Performs the initialization tasks, creating the scheduled task to run the monitor every 6 minutes. Prior scheduled tasks are removed before creating a new task. The task starts in 6 minutes, and the Smart Monitor performs an immediate check-in to the MSP Builder cloud server. *Note: this is NOT supported when running the RMM Suite in autonomous mode*.
--CLEAR	Clears the cloud status. This can be called *immediately* prior to initiating a shutdown that does not utilize the RMM Suite shutdown/reboot tool. The MSPB reboot tool properly clears the SAM cloud status.

Configuration File & Parameters

There are no configurable parameters available at this time. The monitor can be disabled by applying the policy control “SMSAM” or “SMOAM”. (The tag “SMSAM” is preferred in V3.0 and above.)

RMSDCC – Smart-Logic Disk Capacity Check

Performs hourly disk capacity checks and once-daily utilization trending analysis.

Summary

This smart monitor intelligently checks each detected volume on a system for available capacity. The check allows different threshold factors to be used to determine the optimal alerting threshold. With this design, as the disk size increases, the alarm threshold decreases proportionally. Volumes below a certain size or having specific volume names are excluded from monitoring. Workstations and Servers both have a unique set of calculations, generating the most appropriate thresholds for each platform type.

The monitor supports both volumes with assigned drive letters and mounted volumes, removing the limitation of monitoring by drive letter.

When the monitor starts each day, it updates the prior 30 days of utilization data for every monitored volume. The trending of space utilization is then projected 30 days into the future to determine if the threshold will be crossed at the current usage rate. If so, a warning event will be generated.

Temporary volumes used by many backup solutions are ignored to prevent false alarms. A volume must be assigned and active for 6 hours before it is enabled for monitoring.

Alerting

The following alerts are generated by this Smart Monitor.

Class	Event	Source	Message
INFO	160	RMM-SMARTMON	RMSDCC: Disk Capacity Check passed.
INFO	160	RMM-SMARTMON	RMSDCC: STATUS: <message>
ERROR	161	RMM-SMARTMON	RMSDCC: Disk Capacity Trend Alarm for <D:>. Anticipate full utilization in 28 days at current consumption rate.
WARNING	162	RMM-SMARTMON	RMSDCC: Disk Capacity Warning. Free space is near the minimum threshold on one or more drives.
ERROR	162	RMM-SMARTMON	RMSDCC: Disk Capacity Alarm. Free space is below minimum threshold on one or more drives.
ERROR	163	RMM-SMARTMON	RMSDCC: Disk Capacity CRITICAL Alarm. Free space is >85% below minimum threshold on one or more drives.
WARNING	165	RMM-SMARTMON	RMSDCC: Disk Monitors suspended on drives: <list> (alert only with --q argument)
ERROR	169	RMM-SMARTMON	RMSDCC: Invalid custom parameter specified

The “Info” events do not generate alarms and are used to provide operational status only. “Warning” level events are optional and must be enabled if they are desired.

Transient Suppression

Yes – Alerts are suppressed for 48 hours unless the utilization crosses the threshold by 65%, which will generate an immediate alert. Warnings for projected utilization are triggered once upon detection. If the combination of Transient Suppression and Self-Remediation resolves the alert condition, the successful remediation is logged with Event 160 and the event details in the <message> body.

A disk volume must be “seen” for more than 6 consecutive check cycles before it is considered “permanent” and monitoring will be permitted. This will prevent temporary volumes mounted during virtualization-aware backups from reporting a low-space condition. The “seen” count can be adjusted via the configuration file.

Self-Remediation

Yes – upon detection of disk capacity below the calculated threshold, the EMM Maintenance tool “RMMSCU.BMS” script will be invoked to initiate a cleanup of all temporary file locations, using an

argument that reduces the file age to 1 day. Note that any additional folders defined by a local configuration file will also be examined and processed for file cleanup.

Arguments

Many of the available arguments are intended for an engineer to use when running interactively, either to generate a report, diagnosing a configuration, or modify the operation. The procedure that executes this Smart Monitor can also be modified to include any appropriate argument.

--a	Audit - Report 0 if no issues detected, 1 if space alerts exist. This can be used by custom automation to determine if the problem detected has been resolved.
--d	Enable Debugging messages.
--w	Enable Warning messages to be logged (default is Alert only).
--r	Report on allowed drives.
--q	Generate alert if drive monitors are suspended.
--st	Create the Scheduled Task. This removes (if necessary) and re-creates the scheduled task to perform hourly checks. This is the argument used by the Smart Monitor sequence engine to start the process each day.
--su d: #	Suppress reporting for the specified volume. "#" represents the number of days to suppress reports.
--t	Turn off "Tiny Drive" exclusions - report on drives of all sizes.
--c:<d>	Clear disk trending data for the specified volume name. The trending data restarts with the next monitoring cycle.

Configuration File & Parameters

The configuration file "**RMSDCC.INI**" is used to provide general and volume-specific overrides for the container sizes, threshold factors, or both. As the common and volume-specific parameters are the same, they will be covered only once.

COMMON Section

The common section contains parameters that control the configuration of the Smart Monitor, including settings that apply to all volumes.

ExcludeTinyDrives A Boolean value that can enable checking of "tiny" drives. By default, any disk volume with a size below 18 GB is ignored. This prevents alerting on what are typically "recovery" volumes. Set this value to "Y" to enable checking all volumes regardless of their size.

TinyDriveSize Changes the "Tiny Drive" default value of 18 GB to a custom size, in GB.

NoWarn Turn off trending warnings.

LabelExclusionList Adds a comma-delimited list of volume labels to the default list of "NOMON", "recovery" and "HP Tools". Any volume label containing any of these terms will be excluded from capacity checks. See the end if this topic for a tip on easily excluding volumes!

TDSThreshold Defines an override for the Temporary Drive Sighting Threshold. The default is 6, so a volume will not generate an alert until the 7th hourly scan. This prevents temporary volumes mounted during backup operations from being alerted upon. This count also prevents the first 6 (or otherwise defined) monitoring cycles from generating an alert for any disk volume.

DiskFactor The comma-delimited list of values that sets the "container" size used to apply a threshold calculation factor. There are 9 values in this list, and all must be specified. The default values are 99, 299, 499, 999, 2499, 3999, 5999, 7999, and 99999 for

servers and 49,99,149,199,249,299,499,749,9999 for workstations. The actual volume size is compared to determine which size range (container) it belongs to. For example, a workstation volume of 160GB is greater than 149 but less than 199, so it is in "container 3". The matching SizeFactor value is then used to compute a free-space threshold against the actual volume size. This design allows container sizes to be adjusted for typical workstation and server systems. This value rarely needs to be customized, and customizing SizeFactor should be preferred.

SizeFactor The value that is used in the internal calculation to determine the free space threshold. It works in conjunction with the DiskFactor value. The default values are 9, 11, 14, 17, 20, 24, 26, 30, and 32. Using the prior example of a 160 GB volume, it would fit into Container 2. The corresponding size factor value is "11".

The SizeFactor value is the most often adjusted parameter and is usually customized when a system has a volume close to the threshold and no plan exists to increase the available space. The DiskCapCalc.xlsx spreadsheet, provided with the EMM Suite and is available for download from the mspbuilder.com website, will assist in determining the appropriate override value to use. The spreadsheet itself has detailed instructions for use.

Note that both the DiskFactor and SizeFactor parameters require a list of 9 values. An incorrectly formatted parameter will generate an Event 169 alert, and the default values will be applied.

DisableWS A Boolean value that, when True, disables processing of this Smart Monitor on workstation class systems.

VOLID Section

When a server has multiple volumes of a similar size, it may not be appropriate to modify the common parameters for DiskFactor and SizeFactor. In this case, a volume-specific section can be created and the SizeFactor value defined. In this case, it will apply only to the named volume. Disks are specified as "D:/" (including the slash), and mounted volumes are defined by their mount path (C:/mount/data). Note the use of *forward slash* in this parameter!

When defining the VOLID section, only the DiskFactor and/or SizeFactor parameters can be provided. Any other values will be ignored.

Refer to the `HKLM\SOFTWARE\RMM\Maintenance\DiskCapChk*` registry key to confirm the volume names that this Smart Monitor uses.

*On 64-bit systems, this registry path is "`HKLM\SOFTWARE\WOW6432Node\RMM\Maintenance\DiskCapChk`".

Volume ID Exclusions

Volumes can be excluded by defining an "EXCLUDE" section in the configuration file. This section will contain VolumeID values with a Boolean value that will cause the named volume to be excluded from processing when the value is "True". Any Boolean value that evaluates to True can be used, including "T", "Y", or "1".

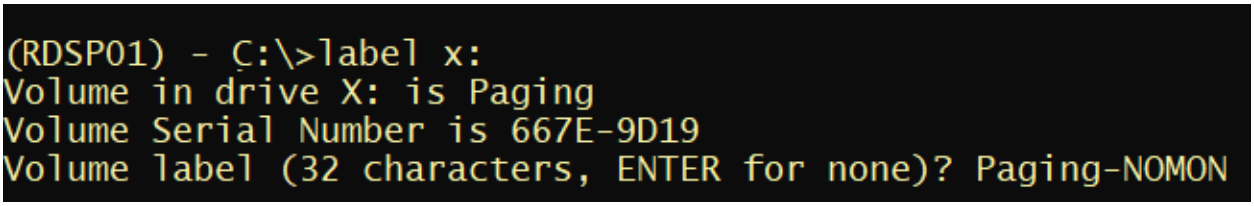
The Volume ID of any valid volume is reported in the logs, making the name easy to identify. This allows the exclusion of drives, mounted volumes, and unmounted volumes that are active. All three types are shown in the example below:

```
[EXCLUDE]
C:/=Y
C:/Mount/LocalData/=Y
Volume{57eae949-0000-0000-0000-606a25000000}=Y
```

Helpful Tip

The ability to exclude monitoring by volume label provides an easy way to suppress monitoring. When a volume needs to be excluded, instead of creating a host and volume-specific override, simply update the volume label to include “NOMON”.

From an admin command prompt on the endpoint, run “label”. This will display any current label and prompt you to enter a new one. If there is no label, just type “NOMON”. If there is currently a label, retype the current label and add “-NOMON”. That’s it - the drive will immediately be excluded from further monitoring!



RMSUSC – User & Group Security Check

Generates warning alarms when changes to user accounts and groups are detected, both local and in Active Directory.

Summary

This monitor will keep track of local and (on the PDCe) Active Directory groups and generate an alert when changes are detected. Changes include adding a group, removing a group, adding an object to a group, or removing an object from a group. The group, action, and all changes are reported in the alert. Only ONE alert is generated for any number of detected changes per pass of the Smart Monitor.

Alerting

The following alerts are generated by this Smart Monitor.

Class	Event	Source	Message
WARN	171	RMM-SMARTMON	RMSUSC: <messages> This is a change to a regular (non-admin) user account.
ERROR	172	RMM-SMARTMON	RMSUSC: <messages> This is a change to user account with admin rights.
WARN	173	RMM-SMARTMON	RMSUSC: <messages>

Changes to groups or user accounts will generate a 171 Warning event. Accounts added to the local Administrators group or any of the standard admin groups in AD (domain admins, schema admins, or enterprise admins) will generate a 172 Error event. ONE event is generated regardless of the number of changes detected; however all changes are logged in the event message body. A 173 Warning event is generated when an account lockout condition is first detected.

The AD users/groups are checked only on the PDCe host.

Messages

The following messages are written as part of the alert. One alert may have several messages.

GROUP ADDED: <name> - USERS: <list>
GROUP REMOVED: <name>
USER ADDED: <user> IN GROUP: <name>
USER REMOVED: <user> FROM GROUP: <name>

Transient Suppression

There is no suppression of events in this Smart Monitor. All changes are reported immediately.

Self Remediation

No self-remediation actions are performed.

Arguments

No arguments are used by the Smart Monitor.

Configuration File & Parameters

The configuration file for this Smart Monitor is optional and can be used to define exclusions for trusted accounts. A built-in exclusion is the LAUser account. It can also allow select customizations to operation.

COMMON Section

Exclude A comma-delimited list of account names to exclude from the detection process. The following wildcard formats are supported:
“name” - requires an exact match for UserID.
“*name” - requires a match on the end of the UserID.

	"Name*" - requires a match on the beginning of the UserID. Wildcards are not permitted on both ends of a name.
DelayInit	Allows immediate execution after first-time run if set to "N". Normally, the Smart Monitor will not run for the first 48-hours after onboarding or first execution.
SuppressNonAdmin	Suppresses Event 171 alarms for changes to non-admin accounts. SuppressNonAdmin=Y suppresses all 171 events on all platform types.
SuppressNonAdmin_W	Suppresses the alarm only on workstations.
SuppressNonAdmin_S	Suppresses the alarm only on servers. Suppressing alarms on servers is not recommended to maintain effective security awareness.

RMSNTP – Network Time Check

Verifies the local system time against the local domain, and against public NTP if running on a PDCe.

Non-US users are urged to custom define the ntp.org time services appropriate for their region. Time sync will be accurate regardless of the hosts chosen, but non-local hosts result in additional processing overhead by the time sync service.

Summary

This monitor will check the Windows Time Sync service and verify that it is configured according to Best Practices and within synchronization limits. When remediation is enabled the Smart Monitor will reset the time service parameters and/or initiate a resync.

There are two configuration settings considered "correct" by Microsoft. The PDCe should be configured to use NTP for synchronization, and all other member devices should use NT5DS. When the Smart Monitor detects a PDCe configured for NT5DS, it reconfigures it to use NTP, and assigns three separate time hosts. The default time hosts are 0, 1, and 2.us.pool.ntp.org. In regions outside of the US, or organizations with a specific internal time hierarchy, the Smart Monitor deployment procedure should be updated so that the --t:*list* argument provides the desired time server hosts. For non-PDCe systems running NTP, the configuration is reset to use NT5DS.

Alerting

The following alerts are generated by this Smart Monitor.

Class	Event	Source	Message
INFO	180	RMM-SMARTMON	RMSNTP: All time values are within spec.
INFO	180	RMM-SMARTMON	RMSNTP: STATUS: <message>
WARNING	181	RMM-SMARTMON	RMSNTP: Warning - Domain Time: <message>
ERROR	181	RMM-SMARTMON	RMSNTP: Alert - Domain Time: <message>
ERROR	182	RMM-SMARTMON	RMSNTP: Alert - NTP Time: Difference between Domain and NTP is greater than 2 minutes after resync!
ERROR	184	RMM-SMARTMON	RMSNTP: Alert - Multiple NTP Time Resync actions within 7 days!
WARNING	185	RMM-SMARTMON	RMSNTP: Warning - PDCe is not using NTP
WARNING	186	RMM-SMARTMON	RMSNTP: Warning - Member server is not using NT5DS
WARNING	187	RMM-SMARTMON	RMSNTP: Alert - W32Time service is missing.

Transient Suppression

Alerts are suppressed only if remediation is enabled and successful. This includes correcting the time sync configuration or performing a resync with the upstream server(s). If the combination of Transient Suppression and Self-Remediation resolves the alert condition, the successful remediation is logged with Event 180 and the event details in the <message> body.

Self-Remediation

Yes – If the time configuration is not correct, it is updated (NTP on PDCe only, NT5DS on all other devices). If the time is out of sync with the domain, a resync is performed.

Arguments

--V	Verbose – write extra information to log/console.
--tt	Abort if wrong time sync type (ie: do not alert if using NTP on a member server).
--s	Suppress alerts, just log results.
--a	Audit mode – report if a fault is present.
--t:l	Comma-delimited list of alternate NTP hosts to use for PDCe configuration. The default is 0-2.us.pool.ntp.org (3 separate host definitions).

Configuration File & Parameters

The configuration file for this Smart Monitor is optional and is used to override default settings. The file name is "**RMSNTP.INI**" and contains 4 parameters in the COMMON section.

COMMON Section

NtpHosts Comma-delimited list of alternate NTP hosts, same as --t: command-line argument. Unless using a GPS or Radio Clock, at least three separate time sources should be specified. We recommend using ntp.org, and specifically <#>.<region>.pool.ntp.org - where "<#> is 1, 2, and 3 (3 separate entries!), and <region> is your (or your client's) specific region. Examples of regions are "us", "ca", "uk", or "au".

IgnoreW32Time Bool - ignore service validation if true (also - IgnoreW32Time RegKey). When this is set, only the comparison of local and upstream server time is performed. This might be used when a custom time service is installed.

DontFixSvc Bool - don't fix the time service. Alerts are generated for non-compliant configurations, but no changes to the service configuration are made.

ResyncDelay Number of seconds to wait after a resync before re-checking - 90s default. If the time is still not in-spec with the upstream server after this delay, an alert event 182 is generated.

Administration

Setup Tasks

When first deploying the RMM Suite, the following configuration settings are strongly recommended to eliminate alerts from default settings that don't match your environment.

- RMSSSC - System Security Check
  - Set the Preferred antivirus product in the default settings, and define any client-specific overrides where a different product is deployed.
  - Confirm that the product you deploy is configured *if it uses downloaded definition tables.* The Smart Monitor should be able to request an update by referencing this app-specific data. This is not required if the AV product does not use definition tables.
- RMSSBM - Server Boot Monitor
  - Set the default business hours if different from 8 AM to 5 PM.
- RMSDCC - Disk Capacity Checks
  - Deploy custom configurations for any endpoint that has unusually small disks or software that managed the available disk space.
- RMSUSC - User Security Checks
  - Decide whether alerts should be generated for non-admin account changes.
  - Identify applications that create local accounts and add them to the Exceptions list.
- RMSNTP - Network Time Protocol Monitor
  - Define the NtpHosts value for locations outside of the United States/North America. Consult resources at www.ntp.org for information on selecting appropriate host groups.
  - Configure overrides for clients that use internal time sources.

Ongoing Administrative Tasks

The ongoing tasks are quite similar to the initial setup tasks except that they are performed in response to specific situations or environmental conditions. For the most part, operation of Smart Monitors is highly automated. New products, endpoints, and even customers may require a review of your default settings.

Common conditions where custom configuration may be necessary include:

Excessive "Not Preferred AV Product" alarms

- Does this client use a different AV product? They need a custom override to define their specific product name.
- Has the name that your standard product uses changed? You may need to list the old and new names until all endpoints update their software. This happens more frequently than you might expect. You MUST use the name that is registered with Microsoft Security Center and not the advertised product name as these are often different.

Server Reboot Not Alerted

- Verify that the startup task has been created and that Smart Monitors have not been suppressed.
- If the reboot occurred outside of the standard business hours, customize the business hours.
- If the reboot occurred on the weekend, enable weekend alerting

Disk Capacity Alarms Triggering (not Triggering)

- This may require a system or volume-specific override to be set. Volume-specific settings should be used on systems with multiple disk volumes.

Appendix I: Monitor Set Event IDs

Event IDs Assigned to Smart Monitors

Each Smart Monitor is assigned a range of Event IDs. The Event Log messages are defined below, along with the appropriate response to detection of the event. Event IDs ending with zero generally denote a status message that indicates that the task has run successfully. These are informational messages and are not alerted on.

All event log source values are “RMM-SMARTMON”.

Event Type Codes:

0 Success
1 Error
2 Warning
4 Information

Component	Source	Type(s)	Event	Message
RMSSSC	Endpoint Security Check	4	110	Security Checks Performed or STATUS: <message>
RMSSSC	Endpoint Security Check	1	111	Product not detected!
RMSSSC	Endpoint Security Check	1	112	Outdated definition
RMSSSC	Endpoint Security Check	1	113	Not Running
RMSSSC	Endpoint Security Check	1	114	Multiple products are running
RMSSSC	Endpoint Security Check	1	115	Protection is suspended
RMSSSC	Endpoint Security Check	1	116	Preferred product not installed
RMSSSC	Endpoint Security Check	1	117	Duplicate product definition in Security Center
RMSSBM	Server Boot Monitor	1	121	The system has booted into Safe Mode
RMSSBM	Server Boot Monitor	1	122	The system has booted into Directory Services Restore Mode
RMSSBM	Server Boot Monitor	1	123	The system has Safe Mode Boot enabled
RMSSBM	Server Boot Monitor	1	125	One or more monitored service have failed to start
RMSSBM	Server Boot Monitor	1	126	The system has booted during business hours
RMSSBM	Server Boot Monitor	1	129	Unable to calculate uptime
RMSICC	Internet Failover Monitor	2	131	On Primary Connection
RMSICC	Internet Failover Monitor	2	132	On Backup Connection
RMSICC	Internet Failover Monitor	1	135	Primary IP not set – NOT CONFIGURED
RMSICC	Internet Failover Monitor	1	136	Unsupported Platform!
RMSDCC	Disk Capacity Check	4	160	Disk Capacity Check passed or STATUS: <message>
RMSDCC	Disk Capacity Check	1	161	Disk Capacity Trend Alarm for <d:>
RMSDCC	Disk Capacity Check	2	162	Disk Capacity Warning
RMSDCC	Disk Capacity Check	1	162	Disk Capacity Alarm
RMSDCC	Disk Capacity Check	1	163	Disk Capacity CRITICAL Alarm
RMSDCC	Disk Capacity Check	2	165	Disk monitors suspended on drives:
RMSDCC	Disk Capacity Check	1	169	Invalid custom parameter specified
RMSUSC	User Security Check	2	171	RMSSBM: <message> reporting changes to users and groups
RMSUSC	User Security Check	1	172	RMSSBM: <message> reporting changes to admin users and groups
RMSUSC	User Security Check	2	173	RMSSBM: <message> reporting account lockouts
RMSNTP	Network Time Check	4	180	All values within spec or STATUS: <message>
RMSNTP	Network Time Check	2	181	Warning – Domain Time:
RMSNTP	Network Time Check	1	181	Alert – Domain Time:
RMSNTP	Network Time Check	1	182	Alert – NTP Time: Difference > 2 minutes after resync
RMSNTP	Network Time Check	1	183	Alert – NTPDATE.EXE is not present on client! Fatal error!
RMSNTP	Network Time Check	1	184	Alert – Multiple NTP Time Resync actions within 7 days
RMSNTP	Network Time Check	2	185	Warning – PDCe is not using NTP
RMSNTP	Network Time Check	2	186	Warning – Member server is not using NT5DS
RMSNTP	Network Time Check	2	187	Alert – W32Time service is missing

The RMSOAM Smart Monitor does not generate any Windows Event Log events.

Success (0) and Info (4) level events will not trigger alarms. These events are used to report status and successful completion of the monitoring task.

Smart Monitor Identification

Each Smart Monitor uses a unique ID for its application name and log file name.

Smart Monitor	App Name	Log Filename
System Security (AV) Checks	RMSSSC.BMS	Logs\RMSSSC_#-DAY.log
Server Boot Monitor	RMSSBM.BMS	Logs\RMSSBM_#-DAY.log
Internet Failover Check	RMSICC.BMS	Logs\RMSICC_#-DAY.log
Server Operational Availability	RMSOAM.BMS	Logs\RMSOAM_#-DAY.log
Disk Capacity Monitor	RMSDCC.BMS	Logs\RMSDCC_#-DAY.log
User Security Checks	RMSUSC.BMS	Logs\RMSUSC_#-DAY.log
Network Time Check	RMSNTP.BMS	Logs\RMSNTP_#-DAY.log

Logs always contain the weekday number (0=SUN through 6=SAT) followed by the 3-letter day abbreviation. Logs are overwritten each week. Logs contain a wealth of information related to where the event occurred, when it occurred, and the conditions under which it was triggered.