MSP BUILDER

Tools for MSP Success

The RMM Suite
Operations & Customization Guide

Configuration Management

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

Last Updated: 2024/09/16

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The MSP Builder RMM Suite contains proprietary software, including unpublished source code.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

MSP BUILDER

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

Contents

Introduction

The MSP Builder RMM Suite utilizes configuration data files for most of its tools. This allows configuration settings to be applied in a tiered approach. The goal is to define the system defaults so they apply to the largest population and meet the broadest requirements. Then, additional configuration settings can be applied to computers at specific customers, customer locations, or even individual computers.

This provides a high degree of flexibility and accuracy of operation. If good planning isn't used, however, it can easily turn into a daunting task. Always configure the actions and settings so they fit the largest audience, and then only the special situations will need additional effort.

The configuration process is web-based for the RMM Suite tools. MSP Builder collects the names of organizations, sites, and agents nightly to provide simple and direct drop-down selection to target override configurations.

The RMM Suite also uses local management tools that help automate some of the RMM Platform administration tasks. These tools use Microsoft Excel - a tool that nearly everyone is comfortable with using - to provide a easy to manage configuration database for adding customers or setting server patching schedules.

This document will cover both of these configuration tools.

NOTE:
This release of this Operations Guide contains screenshots from a development system. It may show example data or values that are not available in production. These images will be updated as soon as possible. If in doubt, consult the Management Interface directly for configuration parameter settings.

This Page Intentionally Left Blank.

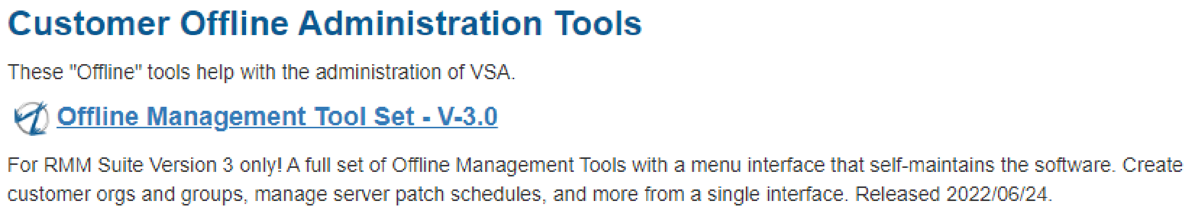
Platform Administration Tools

These tools help simplify the operation of your RMM platform by providing automated methods to create customer accounts, configure customer site groups, and schedule server patching. These run from a local computer in your environment, either on a local disk or on a local file server.

Installing the Platform Management Tools

Installation is simple, and once installed is self-maintaining. Before you start, make sure that the agent where these tools will be used has an RMM agent and has had the RMM Suite Daily Tasks script run at least once to deploy our applications.

1. Start by creating a folder to hold the tools. C:\MSPB_Tools is a good choice to start, and this folder can be moved to another location or even another system or network share with no additional configuration or effort. The folder is self-contained and the tools do not require any “installation” process before they can be used.
   If you have multiple team members that will use these tools, then a local file share is strongly recommended for operation. Cloud-based drives and many NAS “servers” will not support COM connections to Excel and are not recommended.
2. Navigate to www.mspbuilder.com and log in with your customer account. Click on the products menu, then expand Downloads and select Software. Click the **Offline Management Tool Set** link and download the zip file.



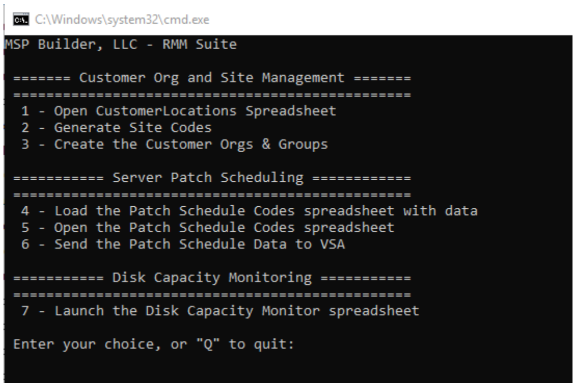
Customer Offline Administration Tools

These "Offline" tools help with the administration of VSA.

Offline Management Tool Set - V-3.0

For RMM Suite Version 3 only! A full set of Offline Management Tools with a menu interface that self-maintains the software. Create customer orgs and groups, manage server patch schedules, and more from a single interface. Released 2022/06/24.

3. Right-click the Zip file that was downloaded, select Properties, and then click the *Unblock* checkbox if it is displayed, then click OK. Some download methods do not turn on blocking, so this may not be required in all cases.
4. Extract all of the files from the zip file into the MSPB_Tools folder.
5. Browse to the MSPB_Tools folder and double-click the AdminTools(.bat) file. Depending on your settings, the BAT extension may not be visible. A command prompt will open, the tools will download, and the menu will display as shown here. The tasks are arranged in the most common sequence of operation.



C:\Windows\system32\cmd.exe

```
MSP Builder, LLC - RMM Suite

 ======= Customer Org and Site Management =======
 ================================================
  1 - Open CustomerLocations Spreadsheet
  2 - Generate Site Codes
  3 - Create the Customer Orgs & Groups

 ========== Server Patch Scheduling ===========
 ================================================
  4 - Load the Patch Schedule Codes spreadsheet with data
  5 - Open the Patch Schedule Codes spreadsheet
  6 - Send the Patch Schedule Data to VSA

 ========== Disk Capacity Monitoring ==========
 ================================================
  7 - Launch the Disk Capacity Monitor spreadsheet

 Enter your choice, or "Q" to quit:
```

That’s all it takes - the administrative tools are now installed, and each time the AdminTools batch file is run, the application will check for and download any updates to the tools. Note that there may be updates that change the Excel documents. The application will create a backup of these files with an “OLD_” prefix before downloading the new versions, and will warn you during the update checks that these have been updated. Data from the old files may need to be copied into the new files for use. This would generally be unnecessary unless the files were modified but not processed prior to the update. Contact MSP Builder support if you have questions or need assistance updating your data.

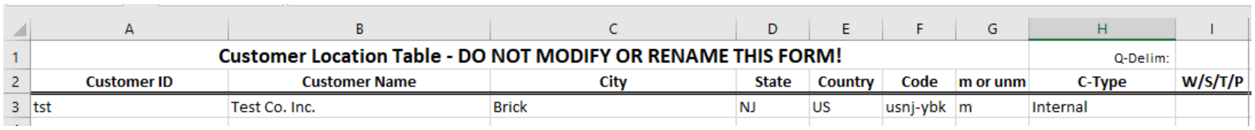
Using the Management Tools (Local)

To perform the management task, simply press the number that corresponds with the desired task displayed in the menu.

Org and Site Creation

For Organization and Site management, the tasks are usually processed in sequence:

1. Open the CustomerLocations spreadsheet, define your new customer, and then save & close the spreadsheet. The spreadsheet has an **Instructions** tab that references the options and configuration tasks. In this spreadsheet, you will define:
    a. Customer ID - short and descriptive if possible
    b. Customer Name - the actual customer name, with punctuation. This name in the RMM must *exactly match* the Customer Name in the PSA platform. The RMM Suite uses this name to match RMM alarms to PSA customers as this field is usually easily changed.
    c. Country, Region/State, and City name. This information is used to look up the LOCODE value. Country is always a 2-character abbreviation, defined as the tab name in the LOCODE.xlsx spreadsheet.
    d. A customer "class" that defines their hours of operation. The RMM Suite uses this to determine if an on-call technician should be notified immediately for a high-priority alarm. Classes should be assigned by customer working hours and whether they have paid for after-hours priority response.
    e. Workstation patching action and schedule can be defined via a patch code.
    f. Some RMM platforms use groups to organize computers within a customer account. Other platforms may use sub-accounts. Depending on what type of support is provided by the RMM, a code can be entered to suppress creating groups or sub-accounts for classes of computers that don't exist in a specific location.
    Refer to the Instructions tab in the CustomerLocations spreadsheet for platform-specific options and settings. See the image below for an example of the configuration data.



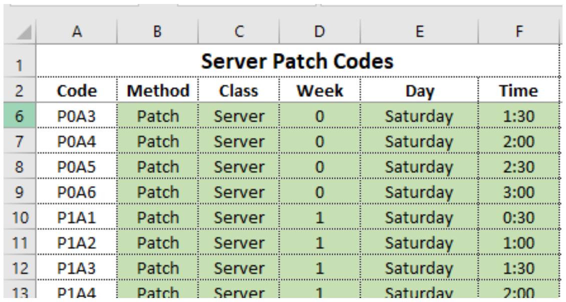
	A	B	C	D	E	F	G	H	I
1	**Customer Location Table - DO NOT MODIFY OR RENAME THIS FORM!**							Q-Delim:	
2	**Customer ID**	**Customer Name**	**City**	**State**	**Country**	**Code**	**m or unm**	**C-Type**	**W/S/T/P**
3	tst	Test Co. Inc.	Brick	NJ	US	usnj-ybk	m	Internal	

2. Generate Site Codes. This step is optional but highly recommended. Defining site codes allows the system to deploy configuration data and perform automation on a site-by-site basis. Site Codes generated by this process use an 8-character code based on the United Nations LOCODE standard. This global standard provides a country, region, and city code for nearly every city in the world and is the perfect automation solution. It is not, however, intuitive. *Customers are free to use alternate code methods, but as these are primarily for supporting automation and not users, this is discouraged as requiring excessive manual effort*.
   In the screenshot above, the **Code** column shows the LOCODE value for Brick, NJ in the US.
3. Create Customer Orgs and Site Groups. This will use the APIs to connect to the RMM platform and create a new customer account and site groups or sub-accounts (depending on the platform). *This will display a green "Authentication is successful" message, followed by the details of each organization and site-group or sub-org that is created.*

Using this tool to create the customer accounts and organizational structure used by the RMM Suite will simplify operation and ensure that the account data is correct and consistent.

Server Patch Schedule Management

Selections 4-6 are used to manage server patch schedules. The RMM Suite utilizes the enterprise method of Change Windows with 9 individual schedules within each change window. Each combination of day, period, and schedule is represented by a 4-character code. Every supported code is listed on the **Codes** tab.

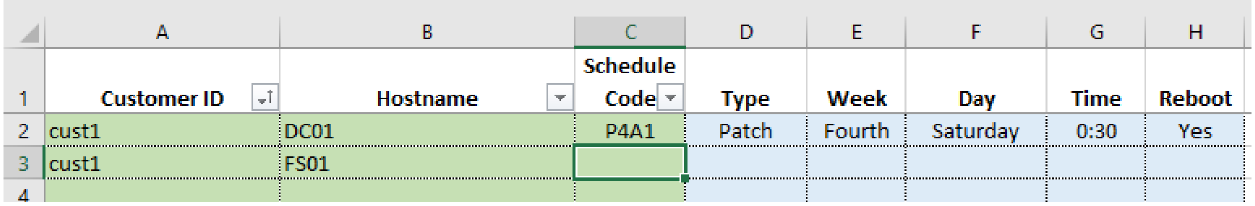


	A	B	C	D	E	F
1	Server Patch Codes					
2	Code	Method	Class	Week	Day	Time
6	P0A3	Patch	Server	0	Saturday	1:30
7	P0A4	Patch	Server	0	Saturday	2:00
8	P0A5	Patch	Server	0	Saturday	2:30
9	P0A6	Patch	Server	0	Saturday	3:00
10	P1A1	Patch	Server	1	Saturday	0:30
11	P1A2	Patch	Server	1	Saturday	1:00
12	P1A3	Patch	Server	1	Saturday	1:30
13	P1A4	Patch	Server	1	Saturday	2:00

This image shows a small sample of the 77 standard schedules provided by the RMM Suite. Any code listed on this tab can be used to define a server's patch schedule. You can see that the week, day, and time are listed on this tab. When defining a schedule, it is important to remember that the patch cycle starts on week 3 of each month, progressing to week 4, and ending on week 1 of the following month before the entire cycle repeats.

The first step to perform is to collect the current schedule data from the RMM platform. The RMM Suite allows defining a computer by class, so even workstation operating systems that operate in a server role can be assigned to a server class. The application will replace all of the data on the Server Schedule tab, and will prompt you to confirm that action by entering "Yes". This data replacement is intentional because the data "lives" in the RMM platform, where it can be set, removed, or changed directly. Those changes need to be synchronized with the spreadsheet data!

Once the data is loaded into the spreadsheet, you can open the spreadsheet to review, define, or modify the schedules. This is a sample of the content:



	A	B	C	D	E	F	G	H
1	Customer ID	Hostname	Schedule Code	Type	Week	Day	Time	Reboot
2	cust1	DC01	P4A1	Patch	Fourth	Saturday	0:30	Yes
3	cust1	FS01						
4								

The second server - FS01 - does not have a code, so patching will be suppressed. When a code (from the Codes tab) is entered into the Schedule Code field, the data in the blue-shaded fields will be displayed to verify the selection. RMM Suite tools use this format consistently - green shaded fields allow data entry, blue fields contain formulas and are protected, and unshaded fields are headers and other information.

Update all fields so that they contain a schedule code. These codes should never be undefined, more for administrative purposes than anything. An empty field is ambiguous - was it forgotten? Should patches be done manually, or not at all? The RMM Suite provides special codes for this:

MANUAL — Automatic patch schedule is disabled. Used to indicate that special patching processes should be followed via manual effort. *The MSP is still responsible for patching!*

NONE — Automatic patch schedule is disabled. This is used to indicate that the server should not be patched. This is often the case when another vendor maintains the system but an RMM agent is installed for remote support.

When the schedule is blank, automatic patching is also disabled to prevent any unexpected restarts of server class platforms.

Once all servers have a code, save and close the spreadsheet. Option 6 will then read the spreadsheet data and send the codes to the RMM platform to schedule the servers at the designated times.

Configuration Management (Web)

Every Maintenance and Smart Monitor application in the RMM Suite utilizes a local configuration file to determine their actions and thresholds. Many other tools also utilize these configuration files to alter their operation. It’s this configuration data that allows the RMM Suite tools to be customized to a very precise level.

Configuration Files

All applications use an INI-format file to maintain their configuration data. The data in these files is stored securely on the MSP Builder cloud infrastructure in a ciphered format, and deciphered locally, where they are stored in clear-text to allow review and troubleshooting. Any security data stored in these files, such as tokens or passwords, remains in a ciphered state until it is read, deciphered, and used.

The web management interface provides a GUI to manage and customize the content of these files. The content manager can select the application they wish to customize, then choose the company defaults or customer, location, or agent-specific configuration levels via drop-down selections.

Introducing Cloud Script Variables

Cloud Script Variables (CSVs) is a powerful capability that allows data to be inserted into scripts or applications automatically, at default, customer, location, or agent-specific levels. The RMM Suite includes some CSVs that the core tools use, and these cannot be removed or renamed. All other CSVs can be custom created and defined as needed. RMM Suite tools have the ability to decipher password data stored in CSVs. This data is always in a ciphered state, except while being edited by an authorized user in the Management Interface or actually used by an endpoint application.

The RMM Suite includes a tool to read and output a CSV value, allowing the data to be used by custom scripts or procedures. This tool will NOT, however, output ciphered values in clear text. Doing so could potentially allow exposure of sensitive data. The primary purpose of this tool is to allow customers to create scripts that can reference customer-specific data such as license keys, identity data, or custom configuration options. This is a powerful capability to eliminate the need to create custom scripts to support these situations. See the RMUCSV app in the RMM Suite Operations Guide - 7 - Utilities for details on using this tool.

Access to the Configuration Interface

There are three access levels for each customer in the MSP Builder website:

Customer Allows access to customer-only resources, such as the ticket portal, How Do I document library, and training materials. It also allows the user to view the Telemetry portal and the Configuration Management data. They cannot make any changes in this portal.

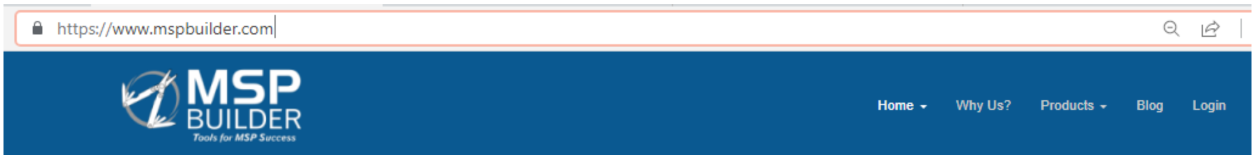
Config Admin This extends the basic Customer access and allows the user to create, modify, or delete configurations in the Configuration Management portal.

Cust-Admin This access is granted to the principal customer account and allows all portal access, plus the ability to subscribe/unsubscribe to fee-based services such as Third-Party Update licensing.

The interface will allow the designated Cust-Admin account to view and configure their employee accounts, including dis-associating accounts when employment is terminated.

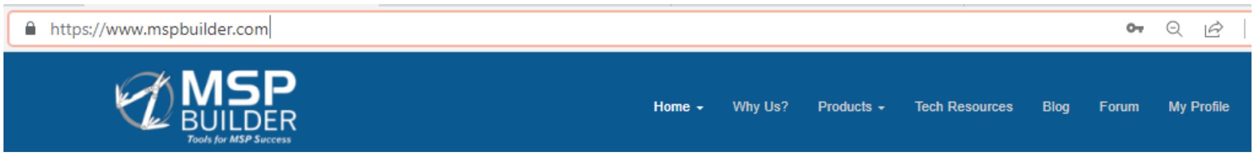
Accessing the Management Portal

Start by connecting to the MSP Builder website (www.mspbuilder.com) and clicking the Login button on the menu at the top-right position.

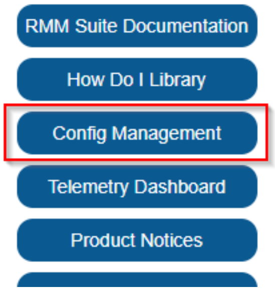


Once you successfully log in, the Login option will change to “My Profile”, and the Tech Resources link will appear in the menu. Click the Tech Resources link to proceed.

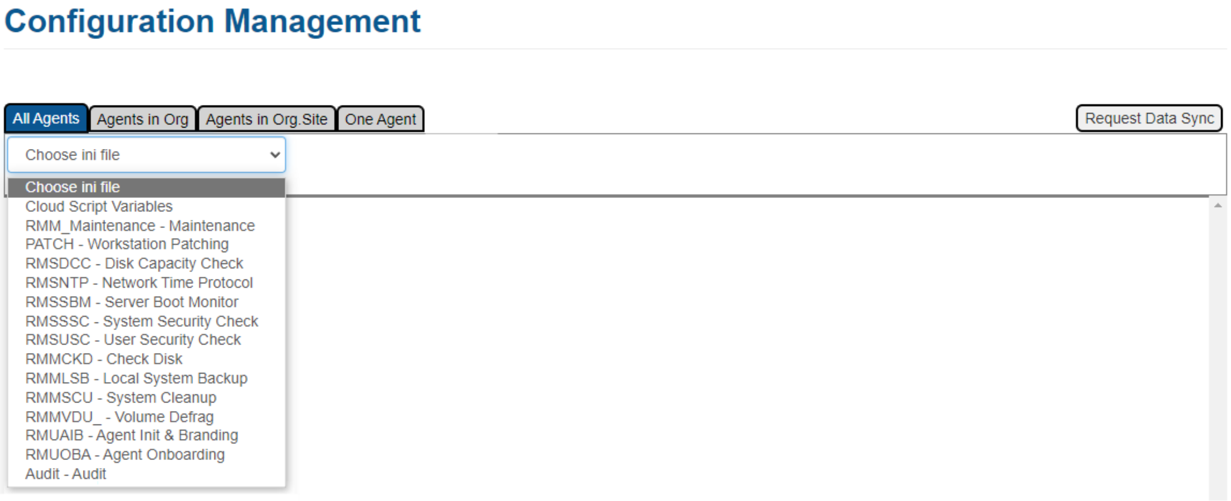
If you don’t have an account, you can register for a new account by clicking the Login link and using the Register link on the login page. Be sure to have your manager contact MSP Builder Sales and ask to have your account associated with your company.



After clicking on the link, a page with Quick-Links will appear. Click on the **Config Management** button. If the Config Management option is not present, request that your manager contact MSP Builder (sales@mspbuilder.com) and ask to have your account associated with your company.



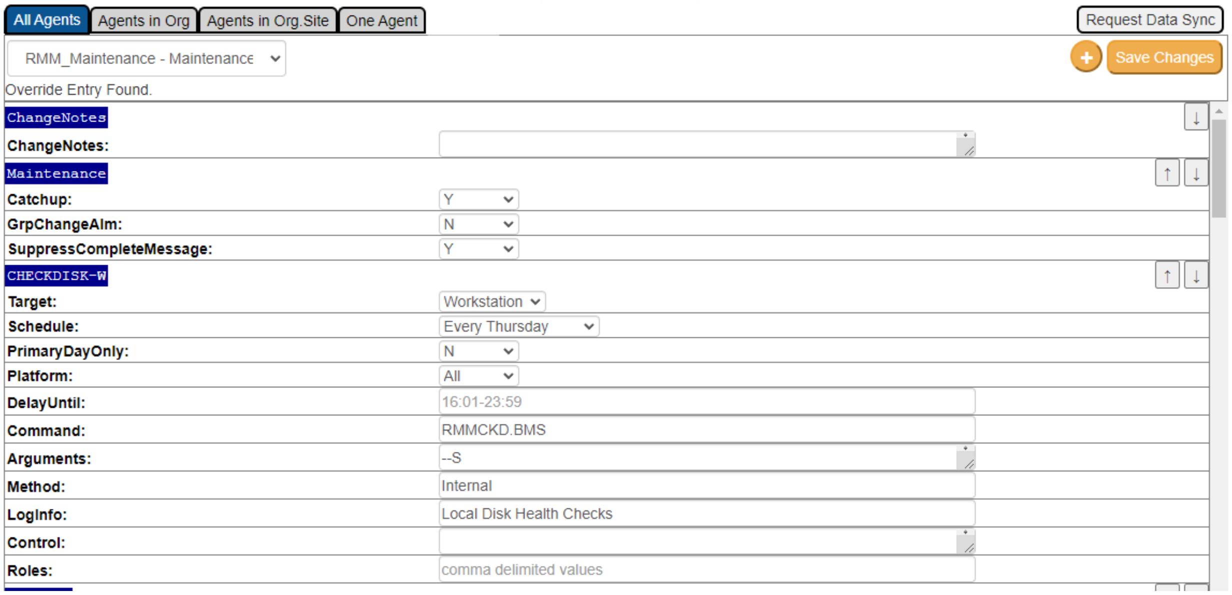
The Configuration Management interface will display:


Configuration Management
All Agents
Agents in Org
Agents in Org.Site
One Agent
Request Data Sync
Choose ini file
Choose ini file
Cloud Script Variables
RMM_Maintenance - Maintenance
PATCH - Workstation Patching
RMSDCC - Disk Capacity Check
RMSNTP - Network Time Protocol
RMSSBM - Server Boot Monitor
RMSSSC - System Security Check
RMSUSC - User Security Check
RMMCKD - Check Disk
RMMLSB - Local System Backup
RMMSCU - System Cleanup
RMMVDU_ - Volume Defrag
RMUAIB - Agent Init & Branding
RMUOBA - Agent Onboarding
Audit - Audit

The default tab represent the default values that are deployed to all customer agents unless an override configuration is defined. These defaults are created by MSP Builder during the installation of the RMM Suite software. *It is strongly advised that these settings be reviewed and potentially adjusted to suite the specific needs of your practice or IT department.*

When the **Choose ini file** field is clicked, a list of RMM Suite application IDs and descriptions is displayed. Select the application/configuration that you wish to view or configure. Once selected, the configuration is displayed with the current data values.

After selecting the RMM_Maintenance configuration option, the following is displayed:



RMM_Maintenance - Maintenance

Override Entry Found.

ChangeNotes

ChangeNotes:

Maintenance

Catchup: Y

GrpChangeAlm: N

SuppressCompleteMessage: Y

CHECKDISK-W

Target: Workstation

Schedule: Every Thursday

PrimaryDayOnly: N

Platform: All

DelayUntil: 16:01-23:59

Command: RMMCKD.BMS

Arguments: --S

Method: Internal

LogInfo: Local Disk Health Checks

Control:

Roles: comma delimited values

Working from top to bottom, we see:

- Override Entry Found (only shows on pages other than “All Agents”.)
- + / Save Changes
  - Click the “+” to add a new parameter or parameter collection.
  - Save Changes will write all of the updates to the database and generate a new ciphered data file to be delivered to the endpoints.
- ChangeNotes section - this is part of every configuration set and can be used to describe what was customized and why the customization was required. This will be written to the delivered configuration data and can help in diagnosing configuration issues.
- Maintenance - this is a common section for this configuration file and defines global settings. Most configuration files have a similar section for this purpose.
- CHECKDISK-W is a maintenance task parameter collection. This represents a single task or configuration collection, with all parameters related to that task or collection. Only select configuration files have the ability to define parameter collections - refer to the specific configurations later in this guide.

On the right side of each configuration collection are arrows that can change the order of the sections. The configuration file does not care about the sequence and neither do most applications, but applications like Daily Maintenance *do* and will perform tasks in the order listed. Since maintenance can perform sequential tasks like download, unzip, and execute, it is important that they are listed in the correct sequence.

Most configuration collections allow the data to be edited directly in the primary interface. There are option buttons on the right side that allow editing or deleting the collection (only custom collections can be deleted, as some collections are required for proper operation of the tool). Whenever possible, the values are selected through drop-down lists to ensure accuracy. Some fields allow free-form data entry and thus cannot be validated by the Management Interface. It is the client’s responsibility to ensure that these fields contain valid and accurate data!

Data Overrides

Whenever possible, the most common settings should be defined at the broadest levels to minimize the effort needed to manage the automation. This is not always possible, and the RMM Suite accommodates this by allowing configuration settings to be defined at the customer (org), location (org site), or specific endpoint (agent).

As the different tabs are selected, the interface changes to allow selecting the customer org, location, or specific agent. All data for customer orgs, sites, and agents is pre-populated and updated nightly. If a new customer was just added and configuration is needed, the **Request Data Sync** button can be clicked to initiate a new collection. The collection process can take several minutes to complete.

To create a client override, select the Agents in Org tab and click the Choose Organization drop-down to select a customer.

To create a location override for a client, first select the Agents in Org Site tab, select the customer as described above, and then click the Choose Site drop-down and select a site for that customer.

To create an override for a specific endpoint, select the One Agent tab. Select the Org and Site to narrow down the list of agents to choose from. Select the desired endpoint.

Complete the process by clicking the **Add Override** button. This creates a new collection of data pre-loaded from the next higher level of defined data. For example, if you create an Agent Override and there are no other overrides, it will inherit the data from the All Agents level, but if there is an override defined at the Customer Org or Site level, it will inherit the values from that level instead. This allows the configuration to be quickly set and override values easily defined.

When an override is present, the option to delete the override is available. When overrides are deleted, the configuration returns to the next higher level of data.

Data Hierarchy

Data is delivered to an endpoint via a very clear hierarchy.

- All Agents - This represents the default settings (initially set by MSP Builder during installation) deployed to all endpoints. Each configuration file is defined separately within the hierarchy, so configurations can be overridden individually.
- Agents in Org - a customer-specific override for a specific configuration file. Data at this level will replace the settings in a specific configuration file for a specific customer.
- Agents in Org-Site - defines the settings for a specific config file at a targeted customer and location.
- One Agent - overrides the specific configuration file data on the defined agent.

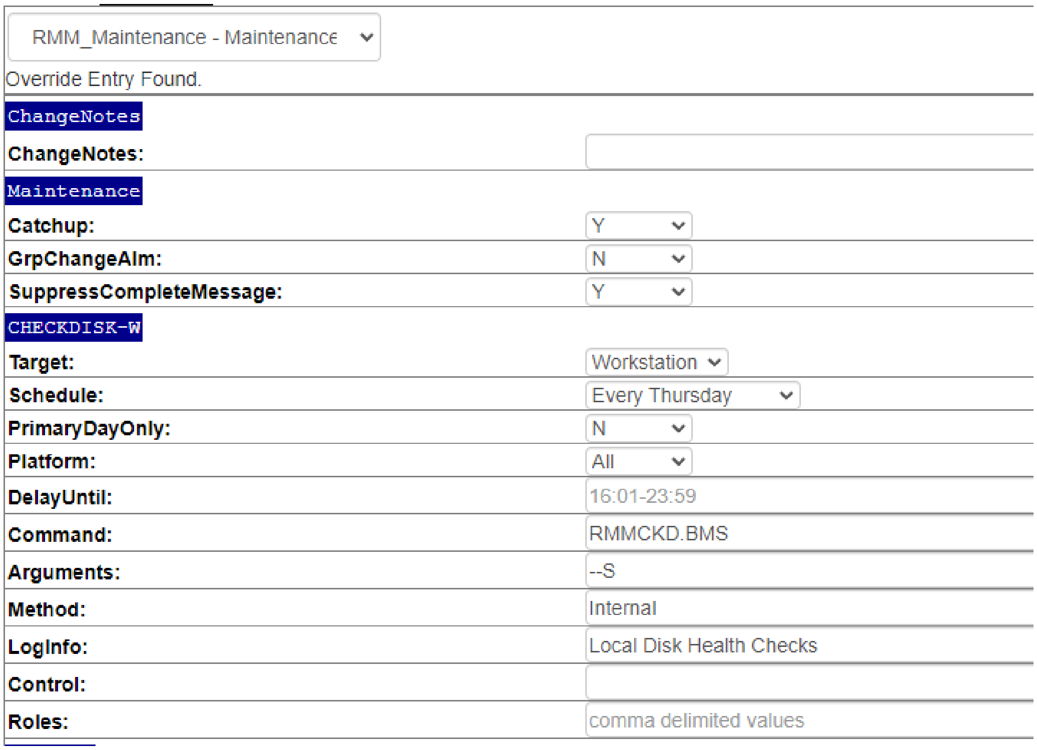
It is possible to define overrides for different configuration files at different levels. There is no need to define data in all configuration files, nor is it necessary to define overrides at Org or Site levels to create an agent-specific override. The RMM Suite software automatically determines the level of override needed for each file to deliver the correct configuration content for every individual agent.

Configuration File Settings

The settings in each configuration file are detailed in the Operation Guide where the application is described - Maintenance, Smart Monitors, or Audit. Those documents should be consulted whenever detailed information is needed.

RMM Maintenance

This configuration defines the operation and individual tasks performed by the Daily Maintenance tool.



RMM_Maintenance - Maintenance

Override Entry Found.

ChangeNotes	
ChangeNotes:	
Maintenance	
Catchup:	Y
GrpChangeAlm:	N
SuppressCompleteMessage:	Y
CHECKDISK-W	
Target:	Workstation
Schedule:	Every Thursday
PrimaryDayOnly:	N
Platform:	All
DelayUntil:	16:01-23:59
Command:	RMMCKD.BMS
Arguments:	--S
Method:	Internal
LogInfo:	Local Disk Health Checks
Control:	
Roles:	comma delimited values

MAINTENANCE

Configures the global operational settings

- Catchup - allows any task(s) that were missed during the prior 7 days to be run the next time that the computer is online. Primarily for workstation systems that are not always powered on.
- GrpChangeAlm - generates an alarm when the endpoint moves from one organizational group to another. Depends on this feature being supported by the RMM platform.
- SuppressCompleteMessage - If true, will not display a “Maintenance has completed” message. This is the default, but some users/customers like to see this closure message.

TASKNAME

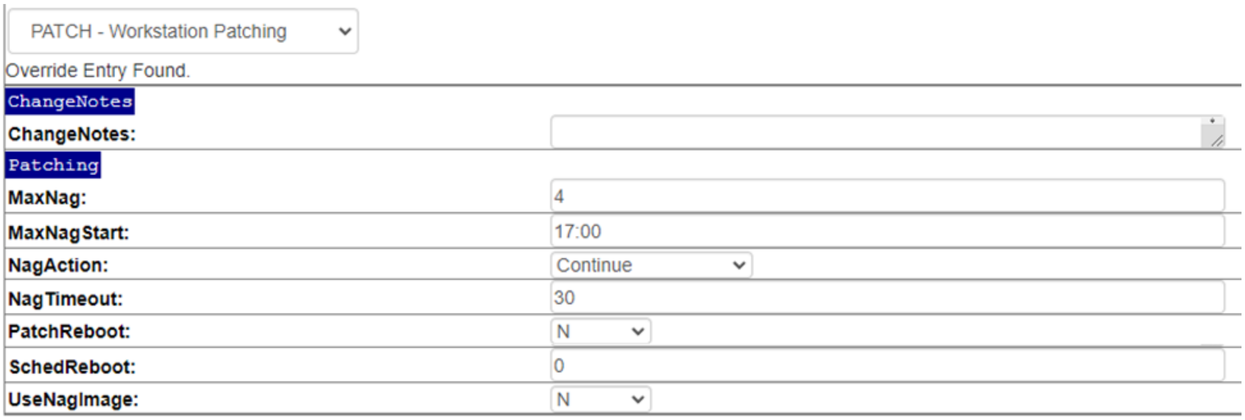
Defines all of the settings for a given maintenance task. The name may include a “-W” or “-S” to distinguish between Workstation and Server tasks that have different parameters. Likewise, tasks that perform platform-specific operations might use a “-32” or “-64” suffix. The taskname must be unique within a maintenance configuration.

- Target - Where the task is allowed to run - All, Workstation, or Server endpoints.
- Schedule - when does the task run
  - Never - the task is disabled
  - Once - the task runs one-time and then is ignored. Usually for application maintenance or zero-day remediation tasks.

  - Daily - runs every day
  - Every <DAY> - runs weekly on the named day.
  - Nth <DAY> - runs monthly on the first, second, third, fourth, or last named day of the month.
- PrimaryDayOnly - allows the task to only run on the defined schedule, and never via a Catch-Up operation. Often used for reminder messages that would not be useful on alternate days.
- Platform - can restrict the operation to x86 or x64 platforms. The default is all platforms. This allows two tasks to perform similar actions but deploying platform-specific software.
- DelayUntil - allows the task to be delayed until later in the day. The time must be between 16:00 and 23:59.
- Command - the command to execute. This can be any EXE, BAT, PS1, or VBS script. It can also be an RMM Suite BMS app, an internal maintenance command, or an RMM Platform script.
- Arguments - the arguments passed to the command. Environment variables and macros are supported - see the Maintenance Operations Guide for details.
- Method - Either Shell or Run, applicable only to EXE, BAT, PS1, and VBS scripts.
  - Shell - execute and wait for completion.
  - Run - execute, detach, and return immediately, continuing with the next task.
  - RMM - the Command is the name of an RMM Platform Script and should be executed from the RMM.
- LogInfo - a short description of the task (<50 chars) that is written to the User GUI tasks list.
- Control - Defines a control parameter, such as Registry or File to determine if the task should execute.
- Roles - Controls the execution of the task based on the presence or absence of a specific control tag in the System Roles field (read from local registry). Used extensively for zero-day remediation tasks.

Patching

This configuration file controls several of the RMM Suite patching options, including if, when, and how workstations are rebooted during a patch cycle and how Flexible Patching operates on both servers and workstations. It is a critical part of the RMM Suite patching system.



PATCH - Workstation Patching

Override Entry Found.

ChangeNotes	
ChangeNotes:	
Patching	
MaxNag:	4
MaxNagStart:	17:00
NagAction:	Continue
NagTimeout:	30
PatchReboot:	N
SchedReboot:	0
UseNagImage:	N

WKSTN REBOOT

This section controls the operation of workstation rebooting and optional reboot nag messages.

- PatchReboot - If set to "Y", the workstation will be rebooted before and after patching. The pre-update reboot will display a 10-minute grace warning before the reboot if a user is logged in. No other options in this file are used when set to "Y". This is the preferred configuration for effective patching with minimal user interruptions. If this option is set to "N", the options below are enabled.
- MaxNagStart - The user is nagged hourly, on-the-hour, to reboot their computer. This specifies a time when the message changes to a count-down before a reboot is forced. Recommended is 16:00-17:00.
- MaxNag - The maximum number of count-down messages to display before forcing a reboot. This MUST be set so that it occurs no later than 11 PM. Schedule cannot cross a day boundary. If the combination of MaxNagStart and MaxNag does not occur by 11 PM it will be forcibly set to 11 PM by the application.
- NagTimeout - the number of minutes to display the nag message before taking the default action and closing the message window.
- NagAction - the default action to take if the user does not respond to the nag message - options are Continue or Reboot; default is Continue.
- UseNagImage - If true, displays a BMP image instead of a text based nag message. There are 3 messages available - reminder, countdown, and rebooting now.
- SchedReboot - A time value to perform the reboot; used as an alternative to the MaxNagStart / MaxNag configuration method and takes priority if set.

FLEX-PATCH_CONFIG

This section defines the operational parameters for RMM Suite Flexible Patching. These settings apply to both workstations and servers.

- Pre-UpdateScript -
- Post-UpdateScript -
- AllowPreview - Y|N option that allows the deployment of updates marked "Preview" if enabled. The default is to NOT deploy preview updates.

FLEX-PATCH_DENY

This section allows the definition of terms, phrases, and/or KB article numbers that should be denied. The terms in the ALL section are combined with the terms defined in the platform type definitions.

- All - defines terms that apply to all platform types. If a term is specified here, it should not be included in other sections.
- Servers - defines terms that apply only to server platforms. A server platform is determined by Operating System.
- Workstations - defines terms that apply only to workstation platforms.

FLEX-PATCH_FORCE

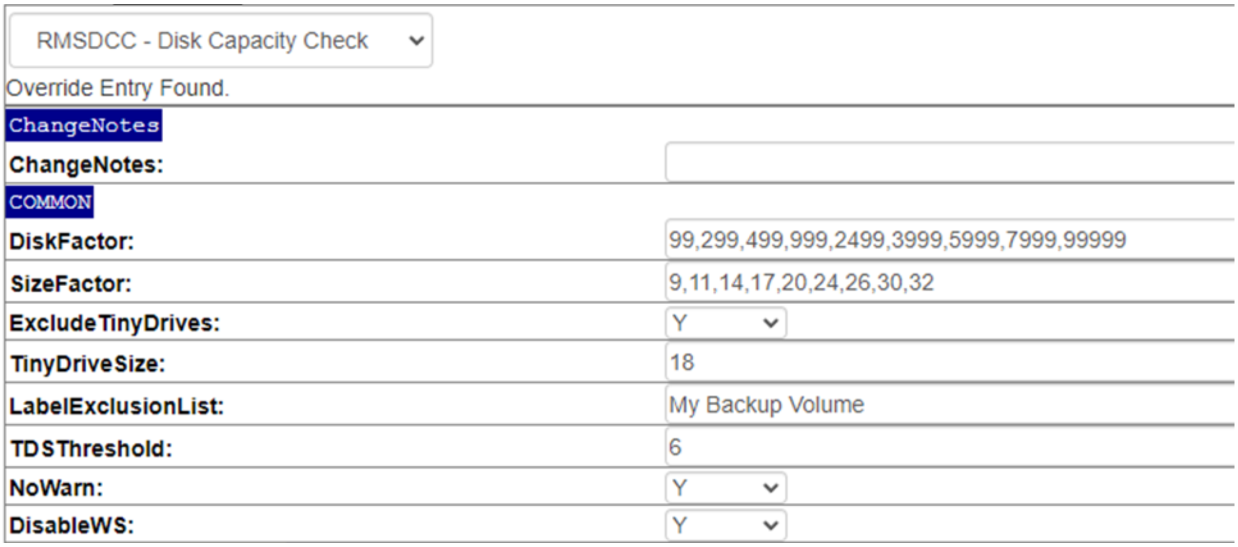
This section allows the definition of terms, phrases, and/or KB article numbers that should be deployed even if a less specific term exists in a deny section. This allows a generic term like “DotNET” to deny most DotNET updates but a specific “DotNET version 4.8.6” to be deployed.

The terms in the ALL section are combined with the terms defined in the platform type definitions.

- All - defines terms that apply to all platform types. If a term is specified here, it should not be included in other sections.
- Servers - defines terms that apply only to server platforms. A server platform is determined by Operating System.
- Workstations - defines terms that apply only to workstation platforms.

Disk Capacity Check

This controls the default settings for the operation of the Disk Capacity Smart Monitor. Consult the Disk Capacity Configuration Spreadsheet for determining the required settings.



RMSDCC - Disk Capacity Check

Override Entry Found.

ChangeNotes

ChangeNotes:	

COMMON

DiskFactor:	99,299,499,999,2499,3999,5999,7999,99999
SizeFactor:	9,11,14,17,20,24,26,30,32
ExcludeTinyDrives:	Y
TinyDriveSize:	18
LabelExclusionList:	My Backup Volume
TDSThreshold:	6
NoWarn:	Y
DisableWS:	Y

COMMON

- DiskFactor - a set of 9 capacity sizes to define the "Goldilocks" disk size assessment. The threshold is calculated based on fitting into one of these disk sizes. This value should not be changed without consulting MSP Builder support as the tool will auto-adjust these values for server and workstation platforms.
- SizeFactor - a set of 9 values that factor into calculating the low-space threshold based on the DiskFactor volume size. This is the most commonly adjusted value. Changing this value defines the operation for all disk volumes. For servers, it is recommended to identify the Volume ID and define a specific Volume_Name section to create a volume-specific override.
- ExcludeTinyDrives - The default operation will ignore volumes smaller than the TinyDriveSize. Set this to "N" to monitor all volumes regardless of size. *Not recommended.*
- TinyDriveSize - defines the minimum size of a disk volume, in GB, that will be monitored. Anything smaller than this size will be ignored unless the prior setting is disabled.
- LabelExclusionList - defines a comma-delimited list of drive volume labels that should not be monitored, such as Recovery or Backup.
- NoWarn - disables alarms for space warnings. This is the default, but enabling this (set to N) will provide advance warning of low disk space events.
- DisableWS - globally disables this monitor on workstation platforms.

Optional Sections

Optional sections can be added to the configuration file to define volume-specific overrides and exclusions.

VOLUME_NAME

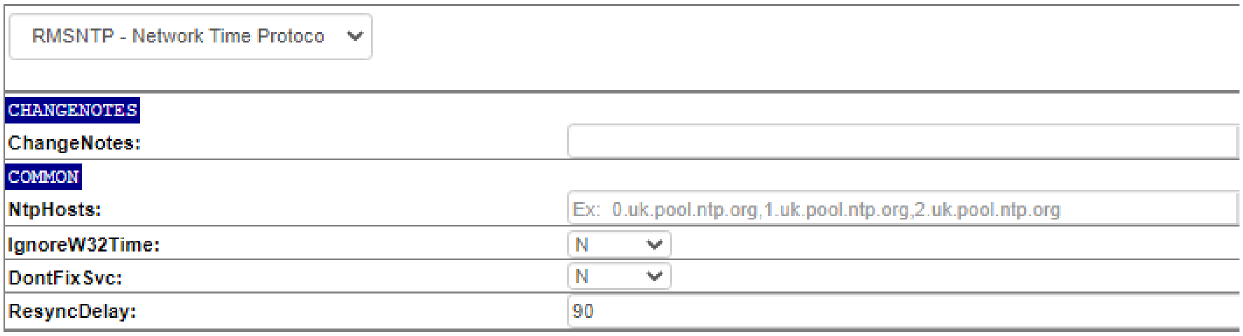
This defines a unique, optional section named by the Volume ID, such as "D/" for the D: drive. Note the use of forward slashes, which is the internal default format for Microsoft registry data relating to volumes. Most often defined when a SizeFactor must be assigned to a specific volume.

EXCLUDE

The Exclude section can be created and then populated with values identifying the Volume ID, such as "D:/" (note the use of Forward Slash!). Each entry can have a Y/N value to control the processing of specific disk volumes. These volumes will not be monitored or tracked for utilization.

Network Time Protocol

This configures the Smart Monitor the checks and updates the Time Sync configuration. The default settings use the “us.pool.ntp.org” servers. Customers outside of the US, or US customers supporting clients outside of the US should adjust this to reflect the proper time servers for the target region.



RMSNTP - Network Time Protoco

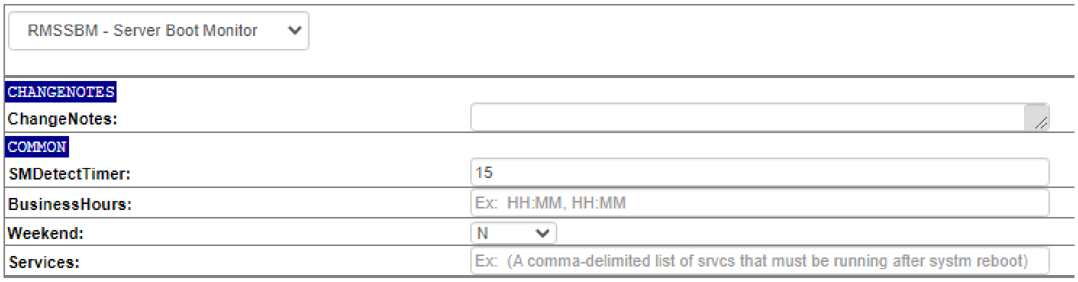
CHANGENOTES	
ChangeNotes:	
COMMON	
NtpHosts:	Ex: 0.uk.pool.ntp.org,1.uk.pool.ntp.org,2.uk.pool.ntp.org
IgnoreW32Time:	N
DontFixSvc:	N
ResyncDelay:	90

COMMON

- NtpHosts - a comma-delimited list of time servers used to configure the PDCe host for proper time sync. This may also be used to define a hardware resource. When specifying public time sources, a minimum of 3 hosts are required.
- IgnoreW32Time - when TRUE, the tests for proper W32Time service configuration are skipped. Use this option when an alternate time sync service is used.
- DontFixSvc - prevents the Smart Monitor from making changes to the W32Time service configuration when the settings do not follow recommended standards. Enable this option when a custom configuration is deployed and must be maintained.
- ResyncDelay - the amount of seconds to wait after a Resync command is issued to the time server to verify that the time has been corrected.

Server Boot Monitor

This smart monitor reports when servers restart during business hours, and can also alarm when critical services do not start a reasonable time after the reboot.



RMSSBM - Server Boot Monitor

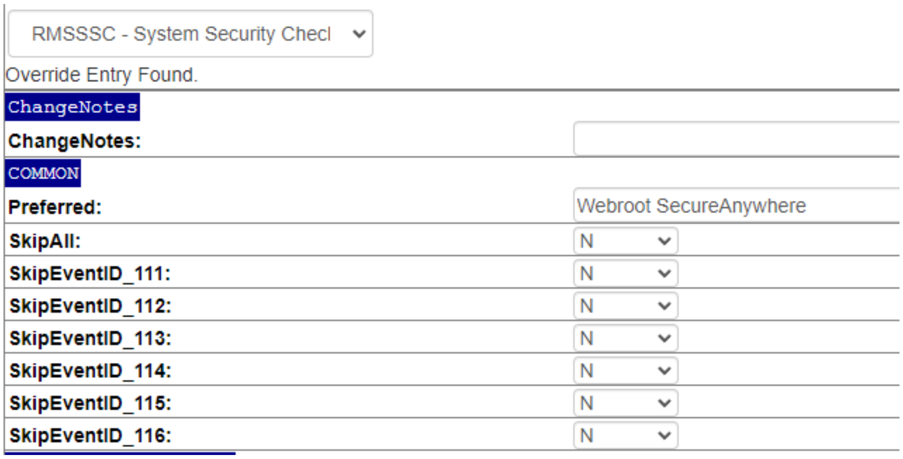
CHANGENOTES	
ChangeNotes:	
COMMON	
SMDetectTimer:	15
BusinessHours:	Ex: HH:MM, HH:MM
Weekend:	N
Services:	Ex: (A comma-delimited list of srvcs that must be running after systm reboot)

COMMON

- SMDetectTimer - the time, in minutes, after the reboot before the Service Monitor should check for critical services in a running condition. 15-minutes is a reasonable (and default) value.
- BusinessHours - a comma-delimited pair of time values to define the start and end time of business operating hours. End times should be defined as ##:59.
- Weekend - if “T”, the hours include weekends, otherwise only weekdays are monitored.
- Services - A comma-delimited list of services that must be running after a system reboot.

System AV Security Check

This configures the Antivirus Status Smart Monitor.



RMSSSC - System Security Checl

Override Entry Found.

ChangeNotes

ChangeNotes:	

COMMON

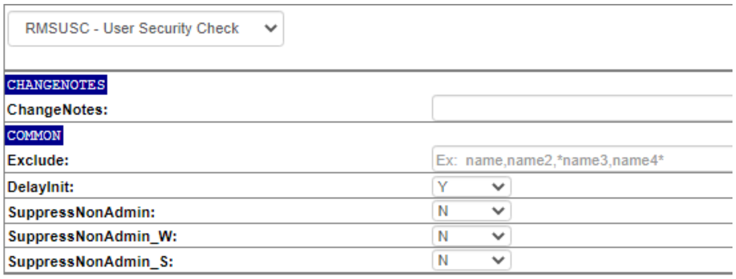
Preferred:	Webroot SecureAnywhere
SkipAll:	N
SkipEventID_111:	N
SkipEventID_112:	N
SkipEventID_113:	N
SkipEventID_114:	N
SkipEventID_115:	N
SkipEventID_116:	N

COMMON

- Preferred - the name - as reported from MS Security Center - of the preferred antivirus product. If defined, an alarm is triggered if this product is not installed. Can be a comma-delimited list of old/new product names to accommodate transitions, but should never list different product brands.
- SkipAll - disables ALL alarms while allowing the Smart Monitor to report the product status to the Daily Audit utility.
- SkipEventID_### - disables the specific monitor from creating an alarm when enabled (Y).

User Security Check

This defines the operation of the Smart Monitor that detects changes to local and domain accounts, particularly changes to the local administrators group.



RMSUSC - User Security Check

CHANGENOTES	
ChangeNotes:	
COMMON	
Exclude:	Ex: name,name2,*name3,name4*
DelayInit:	Y
SuppressNonAdmin:	N
SuppressNonAdmin_W:	N
SuppressNonAdmin_S:	N

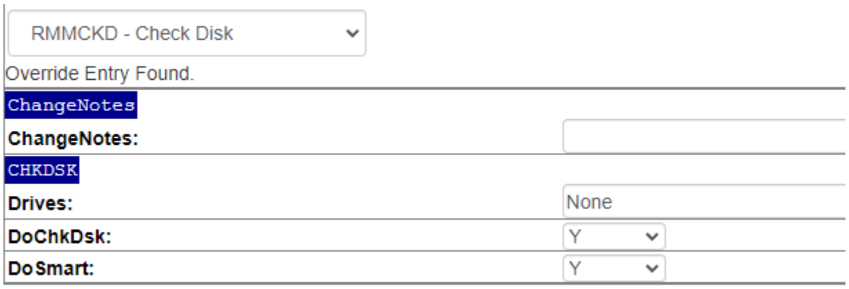
COMMON

- Exclude - a list of account names to exclude from the alarm.
    - Name - an exact match
    - *name - an account that ends with “name”
    - Name* - an account that begins with “name”

    Double wildcards are not supported.
- DelayInit - will not start monitoring until 48 hours have passed since the first execution if enabled. This is the default, and it prevents reporting on new RMM accounts being created.
- SuppressNonAdmin - suppresses alerting for non-admin account changes on all systems, just workstations, or just servers.

Disk Check

This Smart Monitor can perform SMART and CHKDSK tests on all or specific disk volumes.



RMMCKD - Check Disk

Override Entry Found.

ChangeNotes

ChangeNotes:	

CHKDSK

Drives:	None
DoChkDsk:	Y
DoSmart:	Y

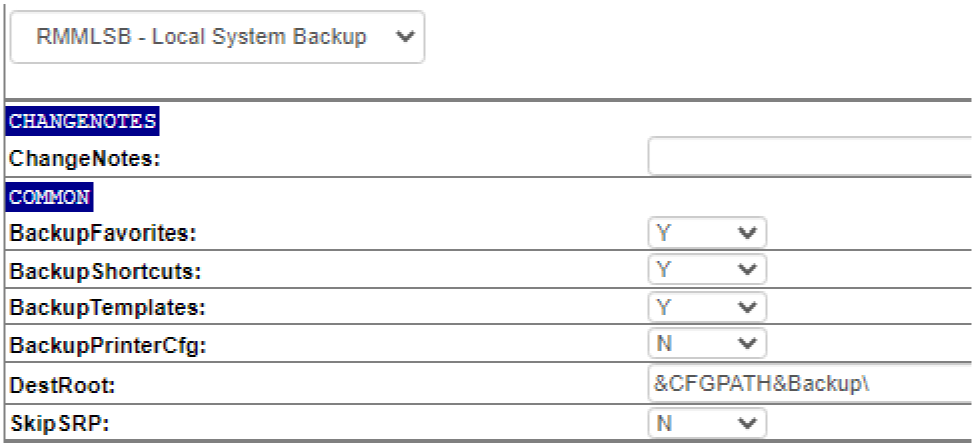
COMMON

- Drives - Specify a list of drives to test, default is ALL.
- DoChkDsk - Runs the Windows CHKDSK command if enabled, and if it detects errors it will attempt to fix and reboot.
- DoSmart - Runs a SMART disk check if enabled.

All tests are enabled on all disks by default.

Local System Backup

This is a Maintenance tool that will create local copies of critical user files such as Templates, Shortcuts, Favorites, and makes sure a System Restore Point is available.



RMMLSB - Local System Backup

CHANGENOTES

ChangeNotes:	

COMMON

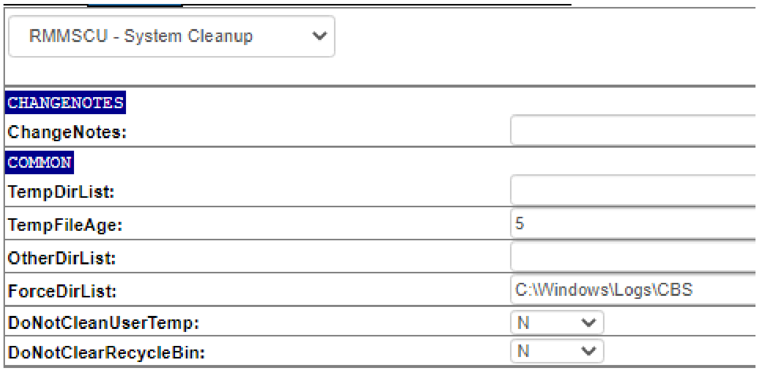
BackupFavorites:	Y
BackupShortcuts:	Y
BackupTemplates:	Y
BackupPrinterCfg:	N
DestRoot:	&CFGPATH&Backup\
SkipSRP:	N

COMMON

- DestRoot - the destination for the backup copies.
- SkipSRP - skips the System Restore Point check and creation.
- Backup<Option> - controls whether certain user file types should be copied.

System Cleanup

This maintenance task performs local disk sanitation services, removing outdated files from Temp locations and emptying the recycle bin.



RMMSCU - System Cleanup

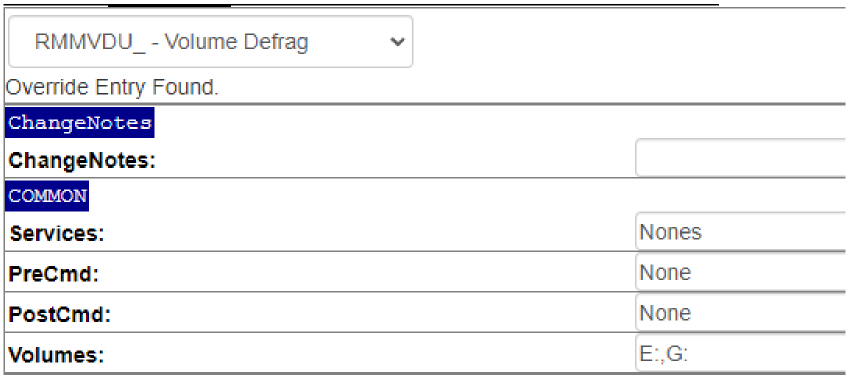
CHANGENOTES	
ChangeNotes:	
COMMON	
TempDirList:	
TempFileAge:	5
OtherDirList:	
ForceDirList:	C:\Windows\Logs\CBS
DoNotCleanUserTemp:	N
DoNotClearRecycleBin:	N

SETTINGS

- TempDirList - allows overriding or adding to the default list, which is shown above.
- TempFileAge - the age of a file, in days, before it can be removed.
- OtherDirList - specifies other directories to be scanned and cleaned.
- ForceDirList - forcibly clears the specified folder(s) of files
- DoNotCleanUserTemp - disables clearing any user temp folders.
- DoNotClearRecycleBin - disables emptying the recycle bin when enabled (all drives). Default is to empty the recycle bin.

Volume Defrag

A maintenance tool that can perform a defrag of selected volumes, intelligently detecting and ignoring SSD volumes.



RMMVDU_ - Volume Defrag

Override Entry Found.

ChangeNotes

ChangeNotes:	

COMMON

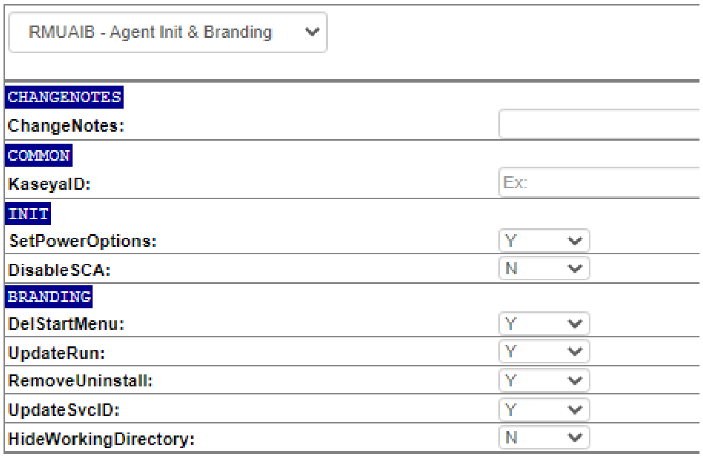
Services:	Nones
PreCmd:	None
PostCmd:	None
Volumes:	E:,G:

COMMON

- Services - a comma-delimited list of services to stop before defragging and restart when defrag completes.
- PreCmd - a command to run before starting the defrag operation.
- PostCmd - a command to run after completing the defrag operation.
- Volumes - a comma-delimited list of disk drives to target.

Agent Init & Branding

This initialization tool defines commonly requested actions when an RMM agent is first deployed. This action occurs automatically the first time Daily Tasks runs.



RMUAIB - Agent Init & Branding

CHANGENOTES	
ChangeNotes:	
COMMON	
KaseyaID:	Ex:
INIT	
SetPowerOptions:	Y
DisableSCA:	N
BRANDING	
DelStartMenu:	Y
UpdateRun:	Y
RemoveUninstall:	Y
UpdateSvcID:	Y
HideWorkingDirectory:	N

COMMON

- KaseyaID - the Agent GUID to target if multiple agents are installed. This tells the RMM Suite tools to use the specific agent.

INIT

Performs one-time initialization tasks

- SetPowerOptions - Used to disable the default action of disabling Sleep and Hibernate actions while on AC Power. This allows the RMM platform to perform maintenance at any time without power settings interfering with operation.
- DisableSCA - Options are No, Yes, or ALL. This disables Security Center Alarm notifications in the status tray.
  - No - all notifications are displayed.
  - Yes - Only critical notifications are displayed.
  - All - No notifications are displayed.

BRANDING

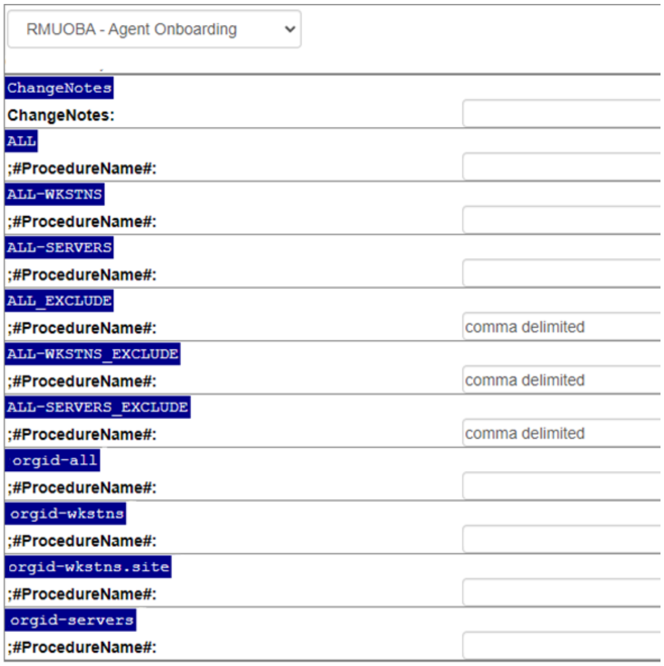
Performs one-time client branding and configuration tasks. Some tasks are dependent on the RMM platform functionality.

- DelStartMenu - Deletes the RMM Agent from the start menu
- UpdateRun - Removes the RMM's user-specific RUN settings from the registry
- RemoveUninstall - Removes the RMM Agent package from Add/Remove Programs
- UpdateSvcID - Modifies the RMM Agent service description to "*MSP Name* Monitoring Agent"
- HideWorkingDirectory - Hides the RMM Agent Working Directory

Onboard Automation

Where RMM platform supported, performs a series of RMM Script calls via API to customize the endpoint to the needs of the MSP and the specific customer.

There are 7 possible configuration sections available, 4 of which are customer-specific. There are three additional Exclude sections that override the default actions for specific customers.



RMUOBA - Agent Onboarding

ChangeNotes	ChangeNotes:		
ALL	;#ProcedureName#:		Procedures to run on all new agents
ALL-WKSTNS	;#ProcedureName#:		Procedures to run on all new workstations
ALL-SERVERS	;#ProcedureName#:		Procedures to run on all new servers
ALL_EXCLUDE	;#ProcedureName#:	comma delimited	Exclude this script from specific customer computers
ALL-WKSTNS_EXCLUDE	;#ProcedureName#:	comma delimited	Exclude this script from specific customer workstations
ALL-SERVERS_EXCLUDE	;#ProcedureName#:	comma delimited	Exclude this script from specific customer servers
orgid-all	;#ProcedureName#:		Run on all endpoints at this customer
orgid-wkstns	;#ProcedureName#:		Run on all workstations at this customer
orgid-wkstns.site	;#ProcedureName#:		Run on all workstations at this customer site.
orgid-servers	;#ProcedureName#:		Run on all servers at this customer

The last 4 sections can be defined for each customer separately. Note that this image represents the entire set of sections, including optional sections. The default contents of this file are empty and must be custom-configured to be operational.

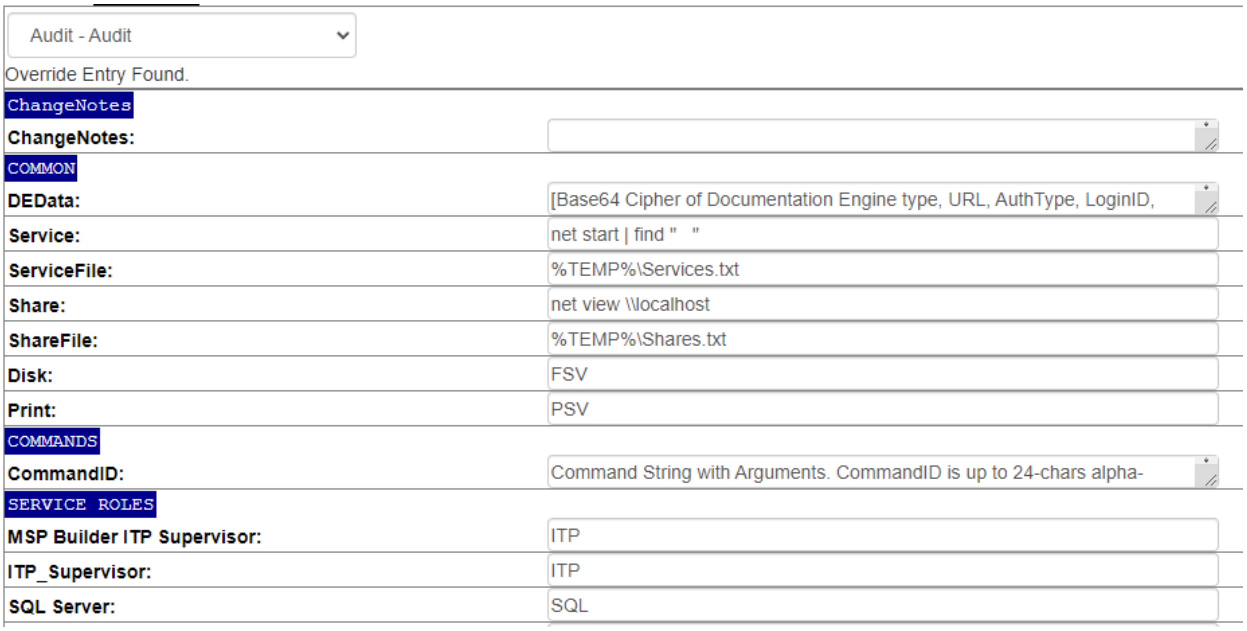
Each procedure named can have the following options:

- NO The procedure will not be run. Used to temporarily deactivate a script.
- Yes The procedure will be run on MANAGED agents if the operation and group matches.
- All The procedure will be run on ALL agents if the operation and group matches.

The ALL, ALL-WKSTNS and ALL-SERVERS sections require manual entry of the options, and also permit the use of “SC:<COS_TAG>” to limit operation to customers with specific Service Class IDs. Multiple tags can be specified, such as: “SC:Silver SC:Gold”.

Audit

The audit configuration file defines the operation of the daily audit task, assignment of TAGs to specific roles, services, or applications, and maps the audit data collected to custom fields in the RMM platform.



Audit - Audit

Override Entry Found.

ChangeNotes	
ChangeNotes:	
COMMON	
DEData:	[Base64 Cipher of Documentation Engine type, URL, AuthType, LoginID,
Service:	net start | find " "
ServiceFile:	%TEMP%\Services.txt
Share:	net view \\localhost
ShareFile:	%TEMP%\Shares.txt
Disk:	FSV
Print:	PSV
COMMANDS	
CommandID:	Command String with Arguments. CommandID is up to 24-chars alpha-
SERVICE ROLES	
MSP Builder ITP Supervisor:	ITP
ITP_Supervisor:	ITP
SQL Server:	SQL

This configuration is discussed in detail in the Daily Audit Operation Guide, so only a summary of content will be referenced here.

COMMON

Defines the basic operational parameters of the tool. These settings should generally not be modified and are presented for special situations.

COMMANDS

A pair of ID and Command to execute. These commands often perform specific scan and detection actions and record data to the registry or an INI file for collection by the audit tool.

SERVICE ROLES

This section maps service names to specific TAG values which are then used by automated actions.

IGNORE SERVICES

A list of service names to ignore. This allows skipping secondary services that have a common name part with a service that should be detected. An example is “SQL SERVER”, which is desired, but “SQL SERVER VSS Writer” would also match but should not trigger a match.

APP VERSION ROLES

This searches the list of installed applications and defines TAGs for both the application and for specific versions of an application.

MSP SERVICE ROLES MSP / APP VERSION ROLES

These sections perform identical collection of service and application data but write their TAG values to a System Data custom field instead. This field is intended more for reporting than automation control.

CFMAP

A mapping of RMM Platform Custom Field name to content. Content is specified as text and macros. Each macro represents a specific audit collection value. Content can contain multiple macros and text references.

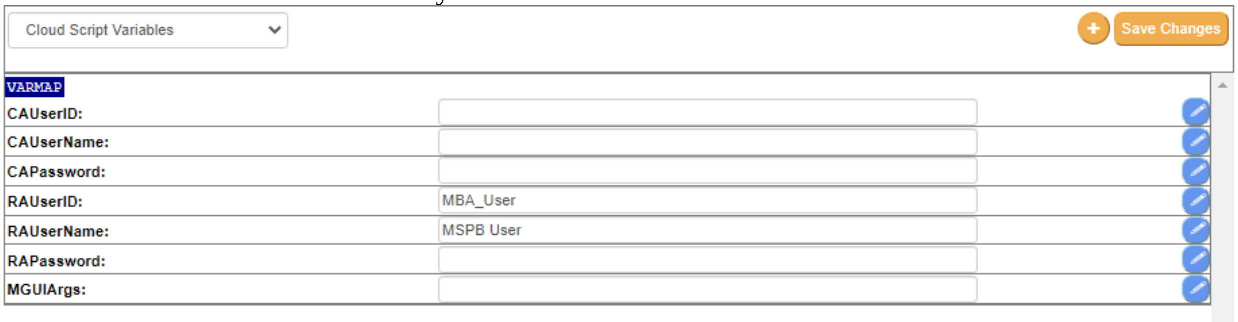
SystemDataQuery

This is the mapping of Macro Names to Data Sources. The audit data collected is written to a cache file, and this can reference any value in a specific collection of data in the cache file. It can also dynamically obtain data from the registry or an arbitrary INI file.

Cloud Script Variables

Cloud Script Variables allow data to be defined at any level, from All Agents to a specific agent and can be used to inject asset-specific data such as credentials and license keys into any automation script.

These are the default variables used by RMM Suite utilities:



VARMAP	
CAUserID:	
CAUserName:	
CAPassword:	
RAUserID:	MBA_User
RAUserName:	MSPB User
RAPassword:	
MGUIArgs:	

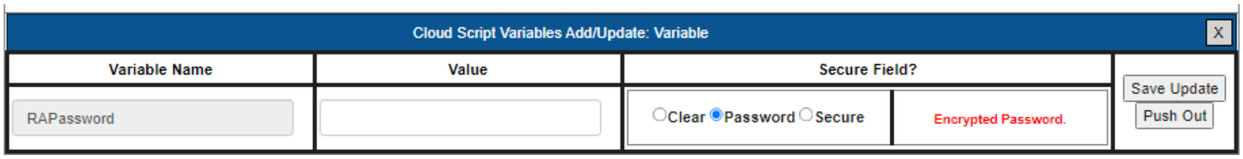
These represent the account credentials used for local Customer or MSP/IT admin accounts and the arguments that control the operation of the User Maintenance Interface. Any number of additional variables can be defined at the All Agents level, and defining them here with no data will ensure that they are created when Org, Site, or Agent overrides are created. This eliminates the need to manually create the same variables at each override level and customer.

There are three types of variables:

- Text — The data is stored in clear text and can be edited directly in the main form.
- Password — The data represents a password used by the RMM Suite account management tools. This data is ciphered upon saving and remains ciphered at all times. It can only be deciphered by the RMM Suite RMUUAM application when creating or updating local accounts. Note that the password is deciphered and displayed in clear text in the edit panel that opens when clicking the blue Edit button.
- Secure — This data represents any content that the RMM Suite user wishes to obfuscate, such as license keys. This works the same as the Password mode except that the data can be deciphered using the RMUCSV utility. The local cache file will hold the ciphered version.

The RMUCSV application (run with RSRUN RMUCSV *varname*) will look for the named variable in the RMUCMV.INI data file. If found, it will output the data to STDOUT allowing any other application to capture the result. Passwords will NOT be deciphered and will output "-SECURE-" instead.

Password and Secure variables cannot be edited in the main form. The field is shown with a gray background and text represented by "•••••••". To edit, click the blue Edit button on the right side of the data field. The edit box appears at the top of the page:



Variable Name	Value	Secure Field?	
RAPassword		○Clear ●Password ○Secure	Encrypted Password.

You MUST select the Password option for any passwords used by the RMM Suite Account Management tool! The password displayed in the Value field will be shown and edited in clear text.

The Secure option works similarly but allows the ciphered data to be deciphered by the RMUCSV application.

Recommendations for Use

- Define common values used by all customers at the All Agents level.
- Create all variables at the All Agents level so they exist when creating an override.
- If you use the same RAUserID everywhere, define it at the All Agents level - it will appear automatically when creating an override file.
- Create client-specific passwords by creating an override at the Agents in Org level. Be sure to click the Edit button and enable the Password option to secure the data!
- If you need to add a new variable after creating several overrides, first create the empty entry at the All Agents level. Use the "Push Out" button to push the new (empty) variable into all of the current override files so it doesn't need to be created each time.