MSP BUILDER

Tools for MSP Success

The RMM Suite
Operations & Customization Guide

Regular Maintenance
and
New Customer Setup

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

Last Updated: 2023/12/28

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The MSP Builder RMM Suite contains proprietary software, including unpublished source code.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 delivers a high level of automation to both the endpoint and to the RMM Platform, reducing the amount of administrative effort required to fully leverage your RMM solution. It does not, however, eliminate all regular maintenance, and there are specific manual tasks that must be performed when adding new customers or locations to existing customers. Each RMM will require specific steps to be performed or may not need (or support) the feature being configured.

This guide is divided into two sections - regular RMM Platform maintenance tasks that should be performed on specific intervals, and New Customer/Location tasks that are required to allow the automation to function effectively.

This Page Intentionally Left Blank.

Regular RMM Platform Maintenance Tasks

There are 4 basic types of platform maintenance tasks that must be performed by the RMM Suite customer, including:

- Platform Initiated - performed when the RMM platform is updated, usually through software updates or upgrades.
- Weekly Tasks - a set of maintenance tasks that ensure that all of the automation is operating as expected. Each RMM platform presents unique challenges that are coupled to endpoint platform changes. These tasks make sure that everything stays “in sync” to correctly deliver the automation to each endpoint. These tasks generally take just 5-10 minutes but are essential to the smooth operation of the RMM and the RMM Suite software.
- Monthly Tasks - generally related to reviewing and managing application and Operating System patches and updates. This requires 15-20 minutes in a typical environment.
- Occasional Health Checks. These should be performed on a regular basis - monthly to quarterly - and “spot-check” that the RMM platform is accurately performing the tasks that the RMM Suite has requested. The RMM Suite reports on operational health each day when the tasks complete, so reviewing this data occasionally will make sure that your system is performing at peak levels.

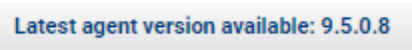
Overall, the RMM Suite requires a minimal amount of regular maintenance to keep the RMM platform running optimally. Most environments require an hour or less each month to fully maintain the RMM platform, including patch and update administration.

After RMM Platform Updates/Upgrades

When the RMM platform is updated, some platforms need RMM Suite settings to be reconfigured or updated. These mostly relate to RMM Suite applications or automation related to initiating endpoint software updates.

Kaseya VSA-9:

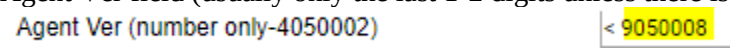
There are two views that must be updated any time the VSA platform is upgraded. To determine the VSA Agent Version, navigate to the Manage Agents screen - locate the message similar to the one shown below:



Update the following views:

- _!_Agent - Agent Version is Current
- _!_Agent - Agent Version is Outdated

Select each of the views in the View Definitions editor, click the Define Filter button, then update the Agent Ver field (usually only the last 1-2 digits unless there is a version upgrade).



The version number is defined as a main number with no leading zero, then the three minor release numbers with leading zeros to make each value be represented as two digits. Thus, if the Latest agent version available value is 9.6.1.23, you would define the value in the view as “9060123”.

Other RMM Platforms:

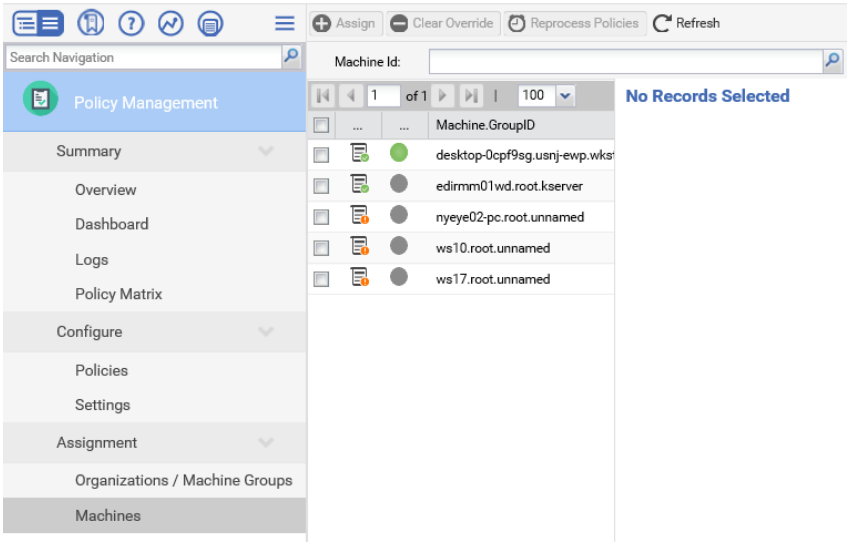
No special post-update actions are required.

Weekly Tasks

These tasks are primarily to verify that automation is being applied and processed correctly.

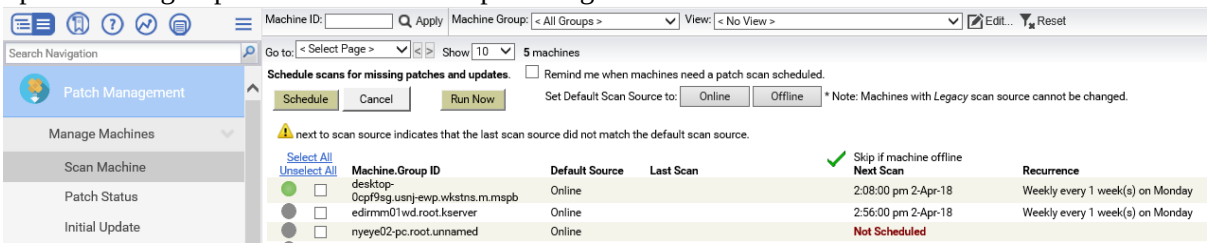
Kaseya VSA-9:

- Check Policy Compliance - recommended first thing each Monday morning:



  - Navigate to **Policy Management – Assignment – Machines**
  - Select the Policy Compliance Status column "…", select Filter, then select ONLY the Override (Orange) option. *You must select overrides first as overrides are also non-compliant and will be shown with that filter enabled as well, which can mask the override condition and prevent fully resolving the issues.*
  - Select all agents and click the Clear Overrides button. Wait a few minutes for the process to complete.
  - Change the filter to display ONLY non-compliant settings (red).
  - Select all agents, then click **Reprocess Policies**
    You should make note of the agents that are initially displayed when the filters are applied. If the same agents repeatedly report non-compliance, investigate which settings are in conflict and adjust the policies or policy application. Request support assistance from MSP Builder if necessary.
    Overrides are the result of performing manual configuration actions. All configuration needs to be done through system policies to be effective. Non-Compliance can result from several conditions, including conflicting VSA settings (check for custom policies), conflicts with Active Directory, or even SQL issues that can arise after certain update actions.

- Check the Patch Scan schedule:
  Spot check a group of machines or a couple of organizations.



  - Verify that each agent has a scan schedule applied – these times may be different if you customized the patching module.
    - Workstations – Every Monday between 10 AM and 4 PM
    - Servers – Every Monday between 12:30 AM and 4:30 AM*
    - Systems without scheduled scans – verify the reason – unmanaged or special group, PATCH setting in the Policy Control field?

*Servers in an unmanaged group will scan on the same schedule as workstations - 10 AM-4 PM Monday.

If MSP Builder's Flexible Patching is utilized, scanning for updating is run automatically. The VSA is used only for status reporting, and either Patch Management or Software Management scans can be used.

Other RMM Platforms:

No special weekly actions are required.

Monthly Tasks

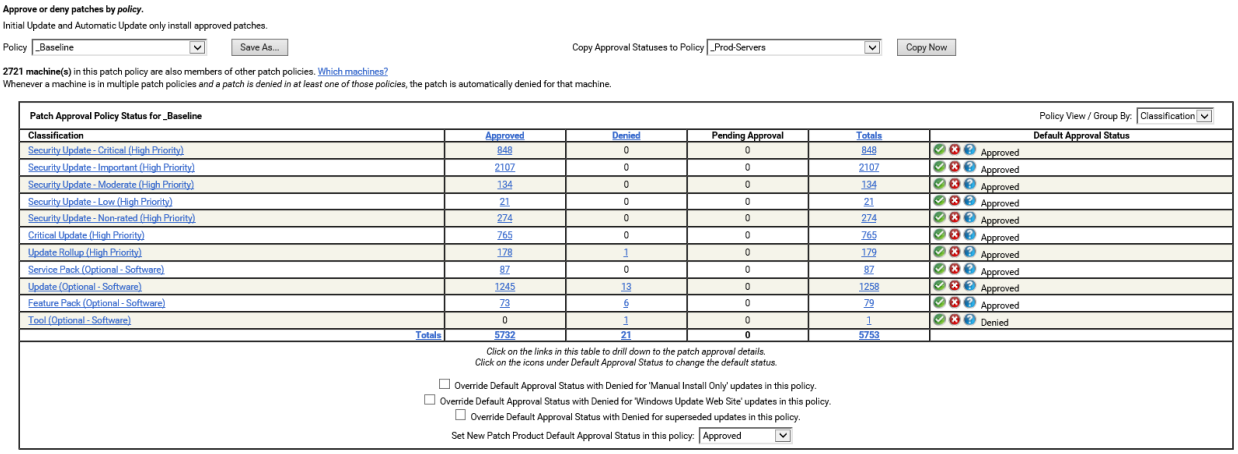
These tasks are primarily related to endpoint patching, application updating and Operational Status. These tasks can take 15-30 minutes depending on the RMM platform.

Kaseya VSA-9:

The following tasks are required if using VSA native patching. If using MSP Builder Flexible Patching, these tasks are not required.

The RMM Suite generally auto-approves most updates, but those categories that have historically caused problems are set to require manual review and approval whenever possible. The RMM Suite generally uses three overlapping policies to reduce the amount of effort to configure typical server or workstation updating

Review and Approve Patches by Policy



Approve or deny patches by *policy*.

Initial Update and Automatic Update only install approved patches.

Policy _Baseline | Save As... | Copy Approval Statuses to Policy _Prod-Servers | Copy Now

2721 machine(s) in this patch policy are also members of other patch policies. Which machines?
Whenever a machine is in multiple patch policies *and a patch is denied in at least one of those policies*, the patch is automatically denied for that machine.

Patch Approval Policy Status for _Baseline — Policy View / Group By: Classification

Classification	Approved	Denied	Pending Approval	Totals	Default Approval Status
Security Update - Critical (High Priority)	848	0	0	848	Approved
Security Update - Important (High Priority)	2107	0	0	2107	Approved
Security Update - Moderate (High Priority)	134	0	0	134	Approved
Security Update - Low (High Priority)	21	0	0	21	Approved
Security Update - Non-rated (High Priority)	274	0	0	274	Approved
Critical Update (High Priority)	765	0	0	765	Approved
Update Rollup (High Priority)	178	1	0	179	Approved
Service Pack (Optional - Software)	87	0	0	87	Approved
Update (Optional - Software)	1245	13	0	1258	Approved
Feature Pack (Optional - Software)	73	6	0	79	Approved
Tool (Optional - Software)	0	1	0	1	Denied
Totals	5732	21	0	5753	

Click on the links in this table to drill down to the patch approval details.
Click on the icons under Default Approval Status to change the default status.

Override Default Approval Status with Denied for 'Manual Install Only' updates in this policy.
Override Default Approval Status with Denied for 'Windows Update Web Site' updates in this policy.
Override Default Approval Status with Denied for superseded updates in this policy.
Set New Patch Product Default Approval Status in this policy: Approved

- Navigate to Patch Management – Patch Policy – Approval by Policy
- Select each Policy from the drop-down list
- Select any classification from the Pending Approval column, select all patches from the approval window, and either approve or deny as per the Default Approval Status column. These are patches that have been discovered on agents after the auto-approval period and require manual approval or denial.
- Select the classifications where the default status is ‘Pending Approval”
    - Review the updates, looking for any that should be denied. Select these and click Deny.
    - Select All remaining updates and click Approve
- Repeat for each policy in the drop-down list that has pending approvals.

Use the filter to focus on what you need to select. Set the “Published” field to something like < "20180430" to exclude updates from the current month (set to the end of the prior month) – giving you time to identify problematic updates before you approve them. The Security Bulletin field can also be filtered to look for things like “.Net” or “IE” depending on the policy you are validating.

Note that the Block DotNET policy requires two search / deny cycles. Search first for “.NET” in the policy and deny all updates found, then search for “DotNET” and deny all those updates. You can safely clear the filter and approve all remaining updates for that policy. This dual-pass method is needed because Microsoft doesn’t consistently name these updates.

Operational Health Checks

These checks make sure that the automation is functioning properly and isn't being blocked by local Antivirus/security software. These checks should be done so that issues are identified and resolved at least once per quarter, although a monthly cycle is preferrable where possible.

Verify Configuration Steps were followed

- Review the steps for new customer or site and ensure that all settings are defined properly.
    - Cloud Script Variables are correctly defined for client-specific settings.
    - Automation Controls are properly defined:
        - Org Workstation Patching Schedule (Flexible Patching)
        - Org custom field setting "Is Managed" is enabled
          For VSA-9, the root group name must not be "unm" - any other name indicates a managed group of devices. Search for agents that are directly in the root group and move them to the correct sub-group.
        - Platform host class override (using Workstation O/S in a Server role) by setting the **Host Class** device custom field.
          For VSA-9 - ensure that all agents are in proper groups. Placing workstations into the "servers" group applies server operational monitoring.

Check the RMM Suite Operational Health Status

Review the **RMM Health Status** field and check the following at least once monthly:

- Auth: Reports PASS (Home Edition systems report "WARN")
  This confirms that the computer is obtaining a valid RMM Suite license.
- Maint: PASS
  A FAIL message could occur if the local AV or security software is blocking the RMM Suite tools. Make sure that the C:\ProgramData\MSPB folder is whitelisted.
- Audit - check 3 items:
    - Ver. - all computers should show the same version if they are online. Note that a slightly older version could be displayed if the system had been offline and has not yet run its updates or daily automation.
    - Collect: PASS - verifies that the data collection was successful
    - Update PASS-date - Verify that the date listed is within 1-2-days of the current day. If the date is older, then the audit is not actively running.
- AD: <date>
  This is the date of the newest RMM Suite application. All systems should show a consistent date in this field. Again - this can vary slightly for mobile systems. The goal is for the majority of systems to be at or close to the same date.

If using RMM Suite patching (VSA-9 Patch Management or MSPB Flexible Patching) - verify that all servers have a defined **Patch Schedule** code. This field should ***never*** be blank on servers. Use MANUAL or NONE if automated patching is not desired.

Check the **Policy Control** field. This field defines tags that disable monitoring and automation components. It is a good idea to verify that the automation and monitoring overrides are still required.

If this field is BLANK, verify that the RMM Suite tools are deployed.

If this field contains "UNKNOWN", confirm that your AV/security product has whitelisted both C:\Temp\mbrs and C:\ProgramData\MSPB folders.

New Customer/Site Configuration Tasks

These steps are needed to ensure that all automation functions after adding a new customer or a new location (site) to an existing customer.

Kaseya VSA-9:

Use the Offline Management tool to automatically create the customer organization and site group(s) – this will ensure that groups are created and named properly. Group names are used to control the automation, and improper naming can prevent the automation from functioning. ***The manual creation of clients and machine groups is strongly discouraged.*** The automation will also define the organization's primary location information and set the customer's operating hours by applying the correct Set-up Type.

Other RMM Platforms

Manually create the customer/site configurations as per your platform requirements.

New Customer - RMM Configuration

These manual steps MUST be performed after the automation has created the customer and group structure.

- Set the Is Managed custom field to "No". (VSA-9 uses the root group name "unm" instead). This allows you to onboard a new customer without the automation and patching taking effect immediately. Once all review and prep actions are complete, you can "go live" by simply setting this field to "Yes" (VSA-9 - rename the group from "unm" to "m").
- If using Flexible Patching, define the WS Patch org-level custom field using an appropriate schedule code. (VSA-9 uses the "wkstns" group name to define the schedule if using the VSA Patch Management system.)
- Identify any "special" systems and apply

New Customer - MSPB Portal Configuration

These steps are RMM platform-independent and should be configured in the MSP Builder Cloud Configuration Portal.

- Define the Cloud Script Variables for the new customer and site(s). Other variables may be required by the client for local customer credentials and various application licensing used by installation procedures.
    - Navigate to **Tech Resources - Config Mgmt** to access the MSP Builder Cloud Configuration Portal.
    - Select the **Cloud Script Variables** configuration option
    - Define the following required variables:
        - RAUserID The local admin user ID used by the MSP
        - RAPassword The local admin account password used by the MSP
        - RAUserName The (optional) First / Last name of the account
        - Define the CA UserID, Password, and UserName values if required
        - Optionally set the MGUIArgs variable to control the User Interface operation.

  Configure any other required Managed Variables to deliver customer-specific data as per your local standards. This may include software license keys and other such settings.

- Review the Maintenance and Smart Monitor configurations and determine if the new client requires any custom settings. Create the necessary configurations using the MSP Builder Cloud Configuration Portal.

Administration via Offline Management Tools - VSA-9

These tools are used on Kaseya VSA-9 to simplify and automate the creation of the client machine-group hierarchy. As VSA has limited support for org level custom fields (not accessible to scripts/procedures), the group structure is used to provide configuration settings that are available from the moment an agent is installed. The RMM Suite utilizes a minimum of 4 levels of organization:

`CUSTID . CLASS . HOST_TYPE . LOCATION`

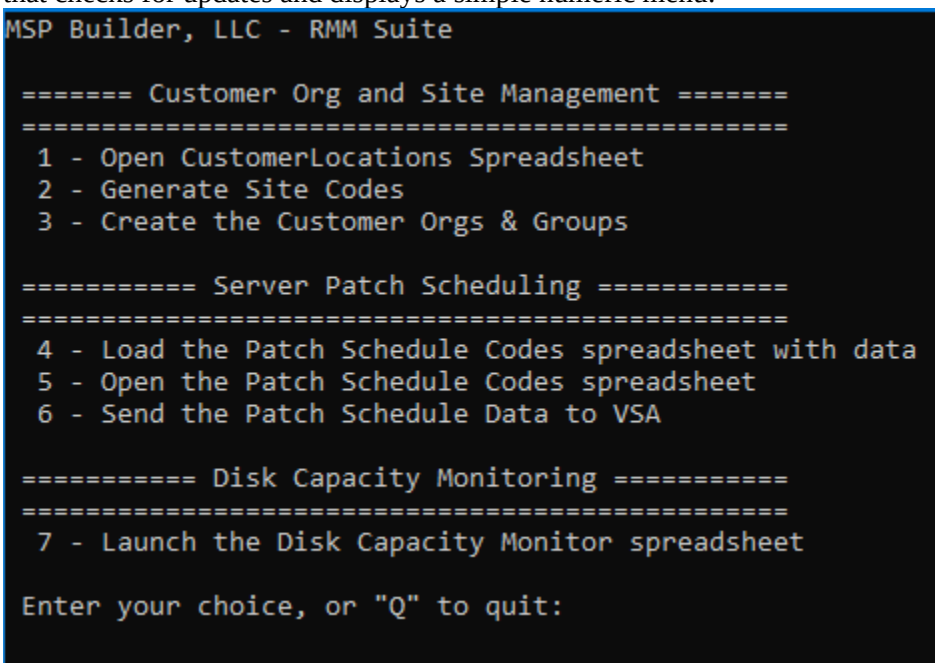
(spaces added above for clarity)

- CustID — the short Customer ID (Org Ref) assigned when the customer is created
- Class — "unm" for an unmanaged (automation disabled) client. Rename to any other name to set the customer as "managed" (automation enabled).
- Host_Type — Either "servers" or "wkstns" and is used to define the *role* of the device. Placing a workstation into the servers group applies server monitoring and related actions that would typically only be appropriate for a server.
- Location — This defines the site and location (or department) where a group of computers is located. The *sole purpose* of this level is to provide an ability to control the deployment of automation to a specific GROUP of computers.

NOTE:
You must update your OMT package for use with V3.0! You can delete all of the .BAT and .BMS files, then download and extract the 3.0 package into your current folder (be sure to unblock the ZIP file first!). The first time and every time thereafter, the tool will automatically check for and download any updates. The first time, it will rename your .XLSX files - simply delete the files it downloaded and rename the backed-up copies.

The offline tools allow a simple management method that provides a consistent configuration and ensure proper operation of the RMM Suite automation. These should be used whenever possible to create new organizations or location groups for existing organizations. The scripts and data files should be located on a local file share, as the applications will not run and access data from most cloud-based storage platforms (Google Drive, SharePoint, etc.).

All tools and functions are accessible through the AdminTools.BAT script. This launches the main app that checks for updates and displays a simple numeric menu.



Org & Site Management

1- Open CustomerLocations Spreadsheet
Scroll to the end of the worksheet to add the customer org or site.

For a new organization:

- Complete the Customer ID, Name, City, State, Country, M or UNM, and C-Type fields. See the Instructions tab in the spreadsheet for further information.
    - The City must be spelled correctly. Common issues are hyphen/space, abbreviations (St. vs Saint). When in doubt, open and review the LOCODE.xlsx spreadsheet.
    - C-Type can be blank to default to Standard coverage.
    - W/T/S/P can be blank – this will create the site group under both Servers and Workstation groups. Do not enter the slashes into the data field. If you specify any value other than "P" in this field, you must explicitly define all agent types:
        - "S" creates a site group below the Servers group
        - "W" creates a site group below the Wkstns group
        - "T" creates the TClients group if not present, then creates a site group below TClients. This is used to separate thin-client systems, which often require special methods for updating or configuration changes. We recommend using this option whenever there are more than a few thin-client systems.

For additional sites for new or existing organizations:

- If the customer has multiple locations, duplicate the Customer ID and Name values, then define the remaining fields to uniquely identify the location. The Customer ID and Name must be the same for all locations associated with a customer organization!
    - If this is a second location in the same city/state, provide a custom ID tag in the "Qualifier" column.
    - Perform this step if you are adding a new location to an existing customer.

Save and close the spreadsheet

2- Generate Site Codes
This runs the GenSiteCodes process, mapping the country, city, and state/region to the UN LOCODE data. Note any locations that failed to be identified – these are often misspellings or are defined slightly differently in the LOCODE spreadsheet. If the location does not exist in the LOCODE spreadsheet, you can either use an alternate location that does exist or define your own code. If you create a custom code that follows the LOCODE standard, make sure it does not already exist in the LOCODE spreadsheet! Re-run this step if you made corrections to city names.

Open the CustomerLocations spreadsheet (menu option 1) and verify the Code column contains Site-ID data. For any customer with multiple locations in the same city, edit the site code that was generated and add the identifier that you defined in the Qualifier column. We suggest using a "locn" format – a short location qualifier based on the site's purpose or street name. Save any changes and close the spreadsheet. Note that the Qualifier will be forced to all lower case and cannot contain spaces or periods. We recommend limiting special characters to the underscore or dash. The qualifier is appended to the location group with an underscore character.

3- Create Customer Orgs & Groups
Run the Create Org Grps task to create all of the organizations and locations not already defined in the VSA. Verify that all orgs and groups have been created by checking the VSA orgs list.

Server Patch Schedule Management

4 - Load the Patch Schedule Codes spreadsheet with data

This will query the RMM platform and return a list of client Org IDs and Servers. You will be prompted to type "YES" to confirm that the data in the spreadsheet will be replaced. The spreadsheet is a tool to manipulate the data. The actual current data is stored in the RMM, so overwriting it the correct action.

5 - Open the Patch Schedule Codes spreadsheet

This will launch the spreadsheet using Excel. The data may be in a random order as returned from the RMM platform. Select the green-shaded fields and using the Data = Sort menu option, sort the data. The default is to sort by OrgID, then Server Name.

Apply or Modify the Patch Codes as appropriate. Every agent should have a code! Use "MANUAL" for manual patching, and "NONE" for servers that are not patched by the MSP. An empty patch code leaves room to question whether it is an oversight in planning.

Save and close the spreadsheet when all codes have been set.

6 - Send the Patch Schedule Data to the RMM

This pushes the codes defined in the spreadsheet into the RMM. This triggers the RMM automation to apply the schedule.

Note that using the RMM Suite's System Updating tool will perform both application and O/S updating using any RMM Suite schedule code. When using RMM-specific patching, then only specific schedules are supported. See the spreadsheet for information about platform specific (Pxxx) codes and RMM Suite's Universal codes (Uxxx). The RMM Suite Updating tool supports Windows, Mac, and Linux platforms with the flexibility to use any schedule on any endpoint without worrying about separate scan schedules.