MSP BUILDER

Tools for MSP Success

The RMM Suite
Operations & Customization Guide

Patching & Updating

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

Last Updated: 2023/03/25

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The MSP Builder RMM Suite contains proprietary software, including unpublished source code.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 1
Third-Party Application Updating 1
Platform-Independent Patching & Updating 1
Platform Patching 3
Patch Scanning 3
Update Review 3
Server Patching 3
Reboot Suppression 4
Patch Cycles 4
Change Windows 4
Support/Management Tools 4
Workstation Patching 5
Schedules & Actions 5
Patch Reminder Notifications 5
Patch Reboot and Nag Messages 6
Application Updating 9
Administration 11
Patching 11
Approve Updates 11
Assign Patch Codes 11
Review Update Results 11
Updating 11

Introduction

The MSP Builder RMM Suite leverages the RMM platform's patching solution with Enterprise style patch schedules. Change windows for servers with multiple schedules allow sequential updating of complex application environments with both pre and post-update reboots to ensure the highest rate of successful updating. Nearly 80 individual schedules in 9 change windows deliver the flexibility to accommodate most environments.

Workstation updating is designed to deliver reliable updating with platform reboots within the same day as updates are deployed. This ensures that endpoints receive critical updates and users are not affected by operating with unapplied updates. The ability to perform pre and post-update reboots improves the success rate of workstation patching, and overnight schedules with daytime reminders minimizes the end-user inconvenience.

Third-Party Application Updating

Third-party application updating is performed just prior to operating system patching so that applications that require reboots can benefit from the post-update restart and not require an additional system reboot. The RMM Suite uses a proprietary solution for third-party updating that leverages the best features of Ninite Pro, Chocolaty, and direct file-based installation methods. The optimal method is selected automatically for install, update, or removal.

Third-Party Application Updating is an optional component available from MSP Builder. Contact the MSP Builder sales team for pricing and availability.

Platform-Independent Patching & Updating

MSP Builder offers an optional Patching and Updating solution that is independent of the RMM platform. This provides the flexibility to update both applications and patch the operating system in a single cycle. The schedule, being independent of the RMM's typical scan then patch process, allows complete control over the scheduling - any day, any time. This solution supports Windows, Mac, and Linux platforms and utilizes MSP Builder's standard change window method of precise scheduling for Windows servers.

Operation of this alternate patching solution is covered in an independent operations guide. Contact the MSP Builder sales team for pricing and availability.

This Page Intentionally Left Blank.

Platform Patching

The specific methods for patching that are platform-specific will be discussed in the appendix. This part of the guide will focus on the technology within the RMM Suite that is common among most RMM platforms.

Patch Scanning

Patch scanning is a requirement for Windows Updates to determine which patches are available, appropriate to the local machine, and have not yet been applied. This scan process typically works with the RMM platform patching system to download and stage the updates in advance of the installation. When updates are complete, the next scan will also report the status of the last series of updates. Patch scanning typically places a load on the RMM, the endpoint, and the client network, so frequent scanning is discouraged.

The RMM Suite configures all endpoints for once-weekly scanning. Scans on servers are done between 1 and 5 AM every Monday, while workstation scans occur between 10 AM and 4 PM on Mondays. This is a good balance between preparing for the updates to occur in 3-5 days and reporting on the prior update cycle from 1-3 days prior. It also minimizes the load on the RMM and client environment. ***As a result of this schedule, patching cannot be applied to any endpoint on Mondays as scans generally override any patch schedule when the times conflict.***

A secondary consideration for single-day scanning is that most RMM platforms need to enable Windows Update to perform the scan. Left enabled, Windows Update will take control of updating and can result in anything from unwanted updates being deployed to systems being rebooted at unplanned times. The RMM Suite patching system ensures that Windows Update is disabled once the scans have been completed.

Update Review

Most RMM platforms permit the MSP to review and approve updates that they deploy. Whenever possible, the RMM Suite provides configurations that minimize the effort needed by auto-approving critical and similar updates, auto-denying optional software updates, and leaving a small subset to be reviewed each month by the MSP. The categories that the RMM Suite configures for manual review have historically represented those with the highest chances of update failures that impact computer operation. MSPs have the choice of approving, denying, or temporarily ignoring updates. This allows a “wait and see” approach to non-critical updating where these updates are only approved 30-days after release.

Update review is a critical part of MSP patching. Regardless of the patching strategy (immediate, delayed, or critical only), we recommend that all updates eventually be reviewed and either approved or denied. This avoids any ambiguity as to why updates are unprocessed. We also recommend that the update review process be performed in the 2-3 days immediately following their release (Patch Tuesday). This will allow the updates to be processed during the next Monday patch scan. Delaying the review and approval process can result in updates not being applied until the following monthly cycle for servers. With the RMM Suite solution, this review and approval process should take no more than 15 minutes each month.

Server Patching

The RMM Suite Server Patching process follows enterprise best-practices. It provides 6 weekend and 3 weekday change windows with 9 schedules in each weekend change window and 6 schedules in the weekday change window. A typical change window follows a consistent format:

- Alarms are suspended for the duration of the change window when the change window begins, not when the server starts updating. This prevents alarms from peer systems not being able to communicate with dependent systems.
- The schedule starts with a platform reboot, followed by a 30-minute "quiesce" period.
- Updates are installed using the RMM platform's delivery method.
- The server is rebooted.

Patching schedules are defined by a Custom Data Field (RMM platform-dependent) using a mnemonic code that identifies the patching method (when alternates are available), the week, the day, and the start time. These 4-character codes look something like "P4A3", where "P" represents the standard patching method in the RMM platform; "4" is the 4th week of the month; "A" represents Saturday, and "3" is the third schedule in the change window. Schedules run on 30-minute intervals.

Reboot Suppression

Any server can have the reboot action suppressed simply by appending "-R" to the patch code. This prevents both the pre and post-update reboots. This allows servers that require additional manual tasks related to reboots to be updated on an automatic schedule and then verified and rebooted manually.

Patch Cycles

The "patch cycle" starts in week 3, after updates are typically released. This is when test and other low-criticality servers should be updated. If problems with updates are detected here, they can be withdrawn before being applied to more critical systems. The next sequence is week 4, when the important servers can be scheduled, followed by week 1 of the following month. This is when the most critical systems should be updated as it provides the longest period between release and installation to avoid issues from bad updates.

Change Windows

The standard change windows for servers managed by the RMM Suite are

- Saturday between 00:00 and 05:59 on the 3rd,4th, and 1st weeks of the month.
- Sunday between 07:00 and 12:59 on the 3rd,4th, and 1st weeks of the month.
- Wednesday - multiple change windows with limited schedules on the 3rd,4th, and 1st weeks of the month. Change windows run from 00:00 to 05:59, 07:00 to 12:59, and 14:00 to 19:59 with 2-3 schedules in each time period. These are designed for updating systems that cannot be offline overnight, such as video surveillance servers and backup servers.

The weekend change window schedules start 30 minutes after the change window begins. There are 9 schedules on 30-minute intervals, which ensures that at least 2 hours are available to reboot and start/finish patching within the assigned change window period. Note that we strongly recommend avoiding Week 3 for production server patching as there are occasional times each year where a patch scan will not occur before the 3rd weekend begins. Week 3 should be reserved for test systems.

Support/Management Tools

MSP Builder provides tools to extract the list of server class systems, by customer, along with any defined patch codes. This data is loaded into an Excel spreadsheet where it can be sorted, and codes assigned and verified. This data can then be pushed back into the RMM platform to assign the codes quickly and easily. This feature is RMM platform-dependent but allows a common management method on all platforms that provide the API support to allow this to function. Use of these tools is described in the **RMM Suite Operations Guide - 08 - Configuration Management** document.

Workstation Patching

Workstation updating and patching in the RMM Suite is designed to be effective and place a minimal impact on the end-user. The goal is to ensure that updates are installed and activated each week to keep systems current and protected. There are several tools and configuration items available to customize the workstation patching process.

Schedules & Actions

The base RMM Suite workstation patching system provides 4 configurations. Each configuration provides a 2-hour window for updates to be deployed and the start-time is distributed within this window. This helps to balance RMM platform and customer network loading.

KASEYA VSA: The workstation patch schedule is applied based on the machine group name containing "wkstns" and schedules are applied as noted below.

1. Thursday at 02:30 - Update if Online; if Offline, try next week. ("wkstns" group)
   This is considered a "best effort" method that will not ensure delivery of updates. It is our default setting because it represents the lowest end-user impact but is not the method we recommend.
2. Thursday at 02:30 - Update if Online; if Offline, resume updating at the next power-on. ("wkstns1" group)
   This is our preferred configuration to ensure timely delivery of updates. Patching will resume as soon as power is returned, and the user will be notified at logon that patching has commenced.
3. Thursday at 04:30 - Update if Online; if Offline, try next week. ("wkstns2" group)
   An alternate schedule appropriate for bars, restaurants, and the hospitality industry in general.
4. Thursday at 02:30 - Update if Online; if Offline, resume updating at the next power-on. ("wkstns3" group)
   An alternate schedule appropriate for bars, restaurants, and the hospitality industry in general with better chances for effective updates.

Category 1 & 3 or 2 & 4 can be used to patch 2 different groups of computers for customers that operate on a 24/7 schedule.

Patch Reminder Notifications

The RMM Suite leverages the Daily Maintenance tool to display a reminder to the end users each Wednesday. It informs them that updates will be applied that night, and to log off to minimize interruption the following day. An alternate message can inform the user of a forced reboot. All messages are fully customizable, and display offers a choice of text-based or BMP image based message formats.

When using the BMP format image display, the pop-up message can be configured to disable the OK button for several seconds, forcing the message to be displayed long enough to be acknowledged and not accidentally dismissed. The user and time are recorded when they acknowledge the message.

All messages are framed in a dialog box that features the MSP's logo, which can also be customized per-customer if required.

Patch Reboot and Nag Messages

The RMM Suite provides a comprehensive mechanism to control workstation reboots and display "nag" messages reminding the user that a reboot is required. The options are defined in the PATCH.INI config file. The nag messages can be customized via the Maintenance Interface language file, including creating language-specific messages that change automatically based on the user's Locale setting.

The nag messages are managed locally to avoid any delays and prevent any additional loading of the RMM platform. The messages display every hour, on the hour, and the display will self-close after a defined period of up to 30-minutes, and will automatically perform the designated action to either reboot or continue running.

Configuration Options

The first and most important setting is **PatchReboot**. This is a Y/N option that controls whether the workstation will be rebooted during patching or not.

- **PatchReboot=Y**
  The computer will be rebooted at 23:55 Wednesday. If a user is logged in, either remotely or on the console, they will be notified and given a 5-minute warning before the reboot is performed. The computer will also reboot after updates have been installed, leaving the workstation fully updated and ready for uninterrupted operation in the morning.
  ALL other parameters in PATCH.INI are ignored if PatchReboot=Y.
- **PatchReboot=N**
  The computer will be rebooted at 23:55 Wednesday *only if no user is logged in*. It will also be rebooted upon completion of updating. If a user is logged in, either locally or remotely, the computer will not be rebooted. Application updates and O/S patches will be applied, and the nag and reboot actions will be performed based on the remaining arguments.
    - **MaxNagStart=hh:mm**
      The time when the nag message changes to a countdown, based on the MaxNag value. If not defined, the countdown process is not performed. Minutes are ignored as messages are displayed only at the top of each hour.
    - **MaxNag=#**
      The maximum number of nag messages to display before a reboot:
      - -1 = nag until manually rebooted. This option is not recommended.
      - 0 = do not display nag messages. Used when an alternate nag process is employed.
      - # = the number of nag messages to display before forcing a reboot. This number is decremented each hour starting at either the completion of patching (if MaxNagStart is not defined), or when the MaxNagStart time is reached.

NOTE: We recommend a MaxNagStart of "16:00" and a MaxNag value of "6" to reboot by 9 PM. The combination of MaxNagStart and MaxNag must be chosen so that the reboot is performed by 11 PM of the day that updates were applied. Windows is incapable of scheduling tasks using the "once" operator beyond the current day.

    - **NagAction=Continue|Reboot**
      The default action button in the message dialog box and the default action to perform if no action is taken after the NagTimeout expires. Reboot will initiate an immediate restart of the computer without further warning. The default action is "Continue".
    - **NagTimeout=1-30**
      A value, in minutes, that defines how long the nag message will be displayed before closing the window and performing the defined NagAction. The default timeout is "30".

- **SchedReboot=hh:mm**
  Schedules the computer to be rebooted at the specified time of the current day. If a reboot is scheduled, a single message notifying the user of the scheduled reboot is displayed and **no further messages will be displayed until the reboot time**. If the user is still logged in at reboot time, they will be given 15-minutes to save their work.
- **UseNagImage=Y/N**
  Nag messages are usually displayed in a text-based dialog box. Multiple BMP images can be created to replace these standard messages and the appropriate image will be displayed instead of the text when this option is enabled. The following 3 images may be created. Images must be in BMP format and exactly 200px high by 550px wide. Any color-depth up to 24-bit is supported.
  PatchNag1.BMP - "Reboot Required in 15 minutes"
  PatchNag2.BMP - "Reboot Required", countdown hours displayed in title bar
  PatchNag3.BMP - "Reboot required - Reboot now or Continue working?"
- **RebootMessages**
  These messages cannot be customized. They will only appear in English, and are only displayed immediately after patching completes. The primary messages displayed hourly are defined in the MGUI_*.LNG files, which controls all messages and language-specific content used by the User Interface. Message IDs M48 through M51 represent the reboot nag and patch resume messages. See the Maintenance User Interface guide for more details on customizing the interface messages and the language they are displayed in. These messages are useful only in a 24/7 operational environment.

NOTE:
The MSP Builder User Interface must be enabled and allowed to display messages for Patch Nag and Patch Reminder messages to appear. If Very Quiet (--QQ) or Kiosk (--K) modes are selected, these messages will not appear.

The User Interface depends on a shortcut in the All Users Startup folder called MSPB_GUI.LNK. The WIN-Daily Tasks procedure will check for this shortcut on workstations daily and attempt to create it if it is missing. If the UI does not display, check for the presence of this shortcut. If the shortcut is not present, confirm that local AV software is not preventing it from being created.

Application Updating

The 3rd Party Application Management System used for application updating is an optional module available at additional cost. This tool combines the features of Ninite Pro, Chocolaty, and custom software to economically deliver a powerful and comprehensive application management solution. The App-Management component is billed by endpoint usage to minimize cost.

Customers can choose an alternate application management solution that suites their needs - this module is entirely optional.

Application updating is initiated at 00:15 (or 04:40 for the later workstation cycle) for workstations, or on the Second Saturday each month for servers. All supported applications will be updated if present.

Applications that are running will be terminated if a live-update is unsuccessful. The update process attempts to perform the application upgrade. If the upgrade fails and the application is found to be running, the application will be terminated, and the upgrade performed a second time.

MSP Builder can provide custom install and update packages if required where specific applications should be targeted or excluded. Contact support with your requirements.

Administration

The operation of the RMM Suite patching and updating is highly automated, requiring a minimal amount of configuration and monthly administration.

Patching

Approve Updates

Depending on the RMM platform, the endpoint updates will need to be reviewed and approved. This task is platform specific - refer to the appendix for specific actions needed. The review and approval process should occur at least 24 hours after release, but no longer than 4-days after updates are released.

Assign Patch Codes

Servers (and workstations that operate as servers) will need to have a Patch Code assigned. This should generally be done through our Offline Administration Tools. Key concepts to understand:

- All related servers should be patched in the same change window.
- Updates should be deployed first to test and non-critical systems (week 3), with systems that are progressively more critical scheduled during week 4 and week 1.
- Assign schedules within the change window based on dependencies.
    - Domain controllers - PDCe in the first schedule, second in the last schedule, and any others at any time in the same change window - this ensures that at least one DC is always available to service DNS and authentication requests.
    - Application groups - schedule in order of dependence, with 90 to 120 minutes between schedules. Database, then application server, then web/front-end server.
    - Non-dependent servers - any time in the change window when at least one DC is available.
    - Use the “-R” suffix on patch codes to suppress the reboots. This will allow any manual tasks needed to ensure a proper system restart.
- Patch codes can usually be assigned to workstations, allowing them to be patched on a specific schedule. This could be workstations that operate in a server role, but can also be applied to VIP users to minimize interruption of service without sacrificing security.

Review Update Results

This should be a monthly spot-check to ensure that updates are being installed properly and to identify any systems where updates are failing. Common failure causes are a lack of reboots and interference by AV/Security software.

Updating

The RMM Suite application update system is fully automated and will update any supported applications found on the machine without any manual configuration. The only configuration task that may be needed is to define an update blocker via a Cloud Script Variable to prevent specific applications from being updated. The “AMSBlock” CSV should contain a comma-delimited list of Application IDs. These IDs will be found in Appendix II of this document.