Qualys | Patch Management | Documentation

Written: July 30th, 2020 | Contributors: Terrence A., Billy R., Yugank P., Melvin T., Milan C., Gage F.

Patching Overview

Qualys Patch Management saves you time and effort by automating patch management on Windows assets, for both Microsoft and Non-Microsoft patches, using a single patch management application. It provides instant visibility on patches available for your assets and tells you whether these patches are already installed. You can automatically deploy new patches as and when they are available. The Cloud Agent downloads the required patches from external sources.

Patching Schedule & Procedures

- **Overview:** Keeping Windows devices patched and up-to-date is a continuous, never-ending, process. Best practice is to embrace this cycle by designing and developing a patching schedule mirroring the release of patches.
- **Patching Cycle:** Both Windows-OS and 3rd party patches rotate on a 30-day cycle.

Phase 1: Windows-OS Devices

- **Information:** The 2nd Tuesday of each month is often referred to as "Patch Tuesday." On this day, Microsoft releases operating system Security Update patches for all supported versions and editions of Windows. This begins our 30-day patching cycle.
- **Schedule:** In an effort to mitigate wide-spread errors or failures, patches will be deployed following a 10/100/Production structure. In other words, patches will initially be deployed to only 10 devices to verify integrity of the patches. If no errors are found, the patches will be deployed to a larger group containing 100 devices. Finally, once approved, the patches will be deployed to all devices in production.
    - Please see an example of the 10/100/Production structure below.
    - **Initial Deployment:** 10 Devices
        - **Goal:** Determine whether patches cause any system instability issues.
        - **Allocated Patch Integrity Verification Time:** 3 days
    - **Second Deployment:** 100 Devices
        - **Goal:** Deploy patches to AIM and request feedback on any instability issues.
        - **Allocated Patch Integrity Verification Time:** 5 days
    - **Final Deployment:** All Devices in Production Environment

        - **Goal:** Remediate security vulnerabilities at an enterprise scale
        - **Allocated Patch Deployment Time:** Remaining days until next patch cycle begins.

Phase 2: 3rd Party Applications

- **Information:** Patching of 3rd party applications begins two-weeks after the 30-day patching cycle begins.
- **Schedule:** In an effort to mitigate wide-spread errors or failures, patches will be deployed following a 10/100/Production structure. In other words, patches will initially be deployed to only 10 devices to verify integrity of the patches. If no errors are found, the patches will be deployed to a larger group containing 100 devices. Finally, once approved, the patches will be deployed to all devices in production.
    - Please see an example of the 10/100/Production structure below.
    - **Initial Deployment:** 10 Devices
        - **Goal:** Determine whether patches cause any system instability issues.
        - **Allocated Patch Integrity Verification Time:** 3 days
    - **Second Deployment:** 100 Devices
        - **Goal:** Deploy patches to AIM and request feedback on any instability issues.
        - **Allocated Patch Integrity Verification Time:** 5 days
    - **Final Deployment:** All Devices in Production Environment
        - **Goal:** Remediate security vulnerabilities at an enterprise scale
        - **Allocated Patch Deployment Time:** Remaining days until next patch cycle begins.

Patching Process

Step 1: Creating a Job

- The foundation of Qualys' Patch Management module is constructed from one fundamental function – Deployment Jobs.
- Deployment Jobs are created through the Qualys Patch Management Module UI for the Qualys Cloud Agent to download and parse. The following items are included in the patch job:
    - **Deployment Name**
    - **Targeted Assets** – The machines to be patched
    - **Targeted Patches** – The updates to be deployed (including security patches, bug fixes, quality of life changes, etc. [1]
    - **Deployment Schedule** – The date and time for the job to start and patching to take place. Options include *"On Demand"* for immediate patching or *"Scheduled"* for selecting the date and time the job should launch.
    - **Patch Window** – If the patch job (including downloading and installing of patches) needs to occur within a specific time frame, enabling "Patch Window" allows specifying the

amount of time, in hours, the job is allowed to run its course. If required, the Qualys Cloud Agent may utilize more system resources to meet this deadline.
    - **Options and Customization** – This final section holds the configuration determining whether the end-user's machine will reboot when required, suppress the reboot entirely or give the end-user notification that their machine needs to reboot. If notifying the end-user, additional features become available like allowing the end-user to delay reboot and/or forcing a reboot after a specified number of deferrals.
- Once the job has been successfully created, it will appear in the list of deployment jobs and must be enabled before the Qualys generates the patch job and notifies the endpoints. It will also show a small overview of the number of patches, and assets, targeted for deployment.

Step 2: Monitoring Progress

- In the list of deployment jobs, Qualys shows the status of the job on the left-hand side.
- In order, the possible statuses are listed below:
    - **Disabled** – This job either has never been ran or has been stopped from running.
    - **Enabled** – This job was very recently enabled and has not yet been acted upon.
    - **Job Sent** – The job is generated and the endpoints have been notified.
    - **Patching** – This job is in-progress.
    - **Completed** – This job has run its course and all endpoints have returned results.
    - **Failed** – This job failed to run, and its errors will be listed in the job details.

Step 3: Remediating Errors and Failures

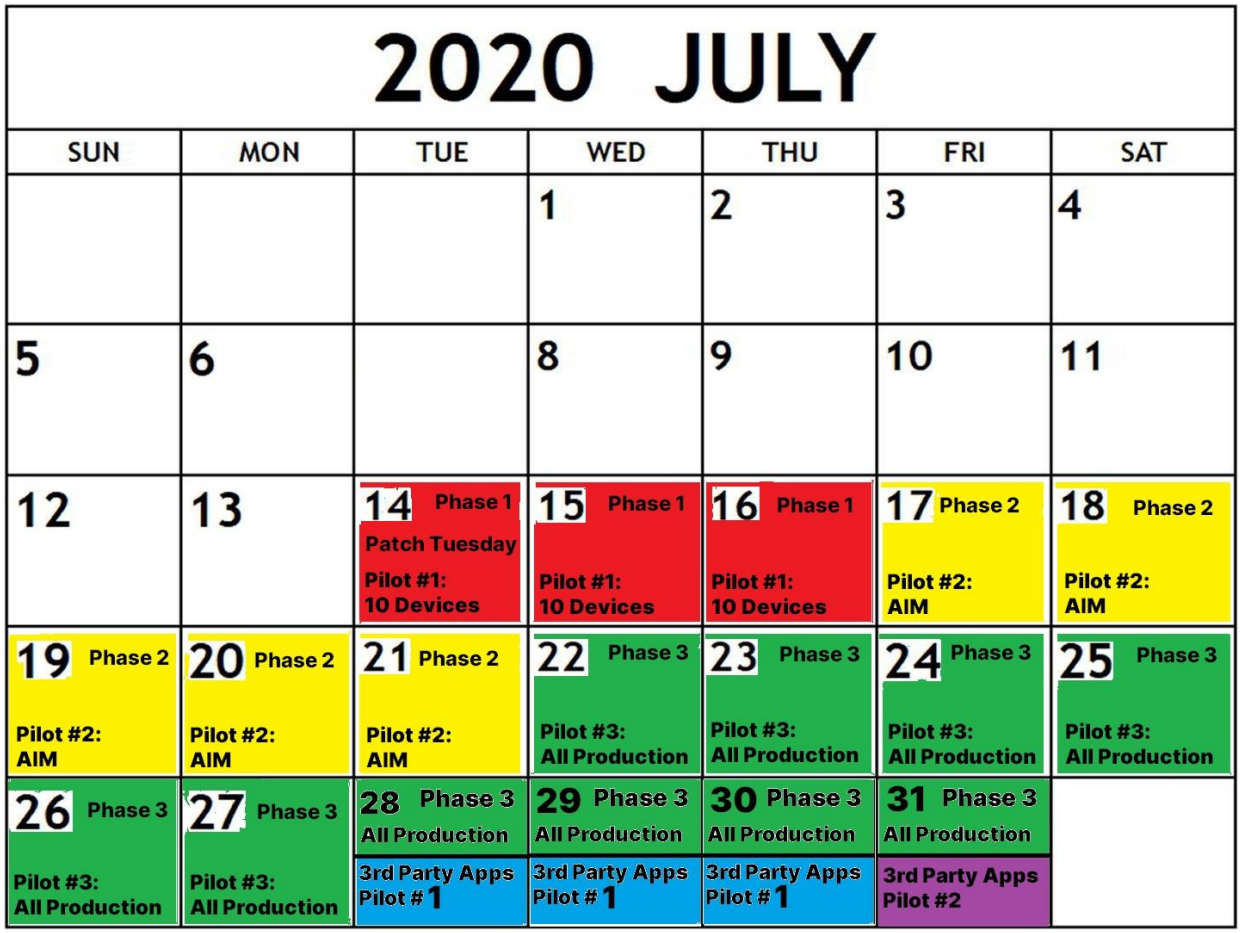
- **Troubleshooting**
    - If some patches fail to install, the Standard Operating Procedure (SOP) is to re-run the patching job. If the amount of failures are reduced after the re-run of the job, the technician should continue the effort until either all failures have been resolved or the amount of failures is no longer being reduced.
    - In the event of one or more persistent failures, follow the escalation process.
    - Verify last system reboot, and reboot accordingly.
    - Gather the Qualys Cloud Agent log file from the impacted device(s) by navigating to C:\ProgramData\Qualys\QualysAgent\ and copying the file “logs.txt” to your local machine.
    - Create a ticket with Qualys with an explanation of the issue along with what troubleshooting steps have been applied. Before submitting the ticket, attach the “logs.txt” file obtained from the impacted device(s.)

Citations

- **1** – Currently, the only excluded patch type is “feature updates” from Microsoft which apply large changes to Windows 10 and come with a different build number. For example, Windows 10 v1903 -> Windows 10 v1909.

Calendar

July 2020



August 2020

2020 AUGUST

SUN	MON	TUE	WED	THU	FRI	SAT
						1 Phase 3 All Production 3rd Party Apps Pilot #2
2 Phase 3 All Production 3rd Party Apps Pilot #2	3 Phase 3 All Production 3rd Party Apps Pilot #2	4 Phase 3 All Production 3rd Party Apps Pilot #2	5 Phase 3 All Production 3rd Party Apps All Production	6 Phase 3 All Production 3rd Party Apps All Production	7 Phase 3 All Production 3rd Party Apps All Production	8 Phase 3 All Production 3rd Party Apps All Production
9 Phase 3 All Production 3rd Party Apps All Production	10 Phase 3 All Production 3rd Party Apps All Production	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					