Qualys Patch Management

Shyam Raj
Lead Technical Trainer

Qualys.

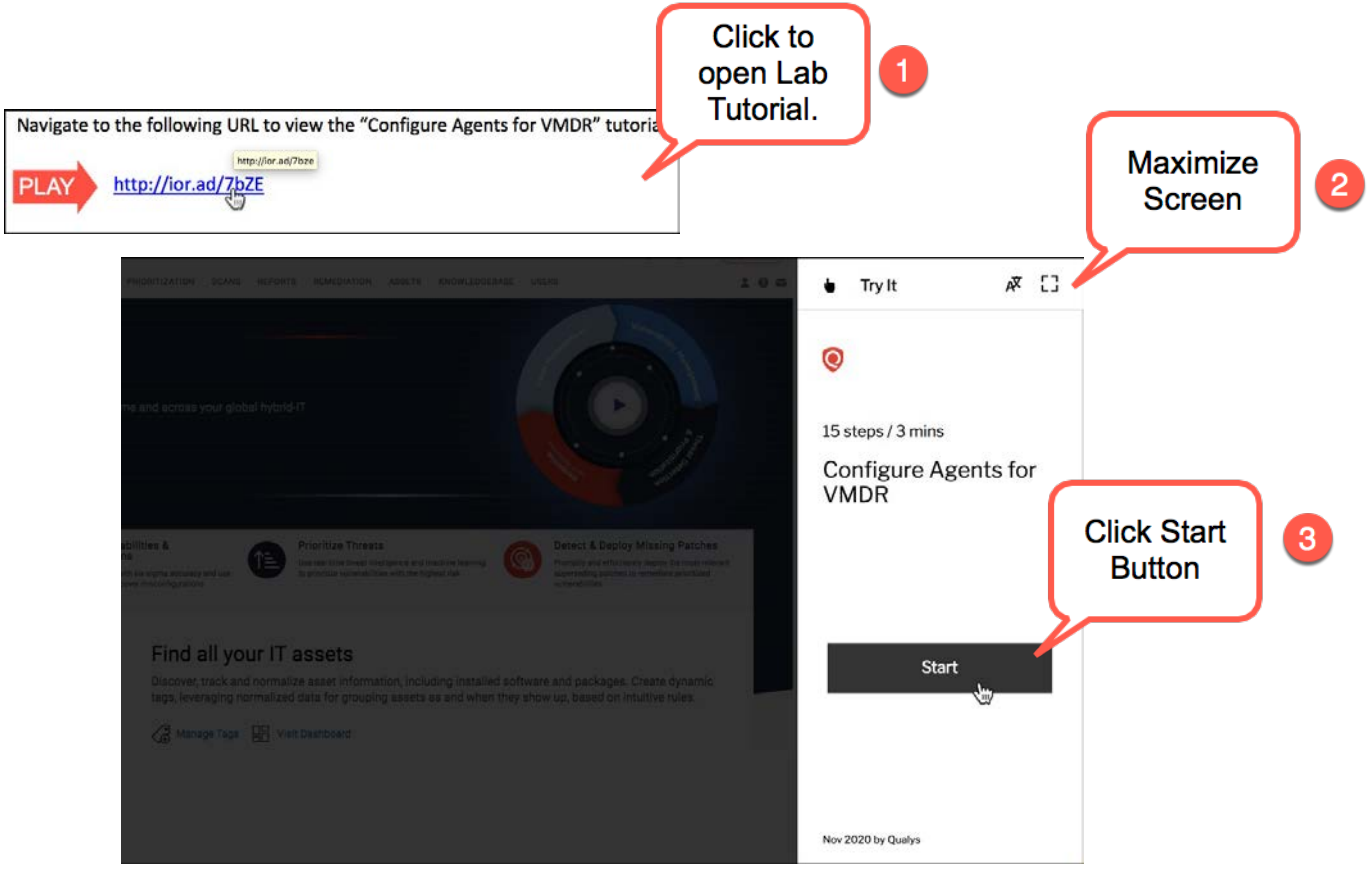
Training Documents

- Patch Management Lab Tutorial Supplement
- Patch Management Slides for Lab Tutorials

- You will find the training documents for this course below this training video (at the very bottom of the page)

- *No trial accounts are provided for this course, all labs are simulated*

Play Lab Tutorials



Agenda

- Introduction to Qualys Patch Management (PM)
- PM Activation & Setup
- PM Application Overview
- PM Deployment Job
- Prioritized Products
- Patching from VMDR and VM
- Zero-Touch Vulnerability Remediation
- Uninstall Job
- Patch Catalog
- PM Assets
- Certification Exam

Qualys.

Introduction

Qualys.

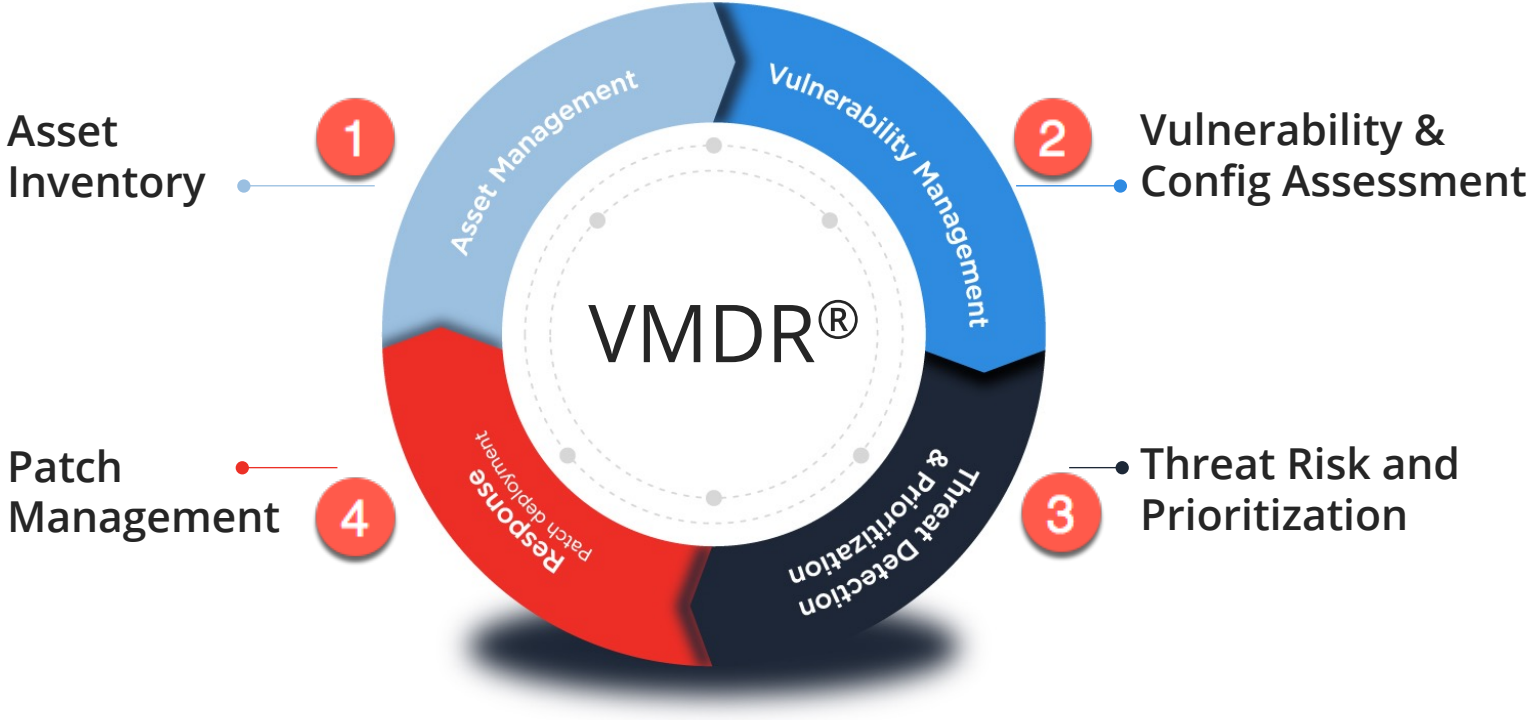
Qualys Patch Management

- Automatically correlates discovered vulnerabilities with their required patches
- Leverage existing Qualys Cloud Agents to deploy and uninstall patches
- Provides OS and Application patches, including patches from third-party software vendors (e.g., Adobe, Java, Google, Mozilla, Microsoft, etc...)

Qualys Patch Management

- Available for Windows, CentOS 6/7, and RHEL 6/7/8
- Provides patching just about anywhere an Internet connection is available (e.g., airports, coffee shops, remote offices, etc...)
- Qualys Agents determine which patches are missing or required and can identify superseded patches
- Build patch jobs that target specific vulnerabilities, severity levels, and known threats

Qualys VMDR Lifecycle



Qualys.

Patch Sources

- Windows patches are downloaded from Vendor Global CDNs (e.g., Oracle, Adobe, Microsoft, Apache, Google, etc...)
- Linux patches are downloaded from the configured YUM repository
- Qualys Gateway Server can be used as a local repository
  - Patch downloads requested by one agent, are cached on QGS and made available “locally” for other agents that need the same patch
  - QGS also provides a cache for manifests and agent binaries

Activation & Setup

Qualys.

Qualys Patch Management uses the Qualys Cloud Agent for deploying patches

Qualys.

Qualys PM Workflow

CA 1. Install Cloud Agent on target host

CA 2. Assign target agent host to a CA Configuration Profile that has PM enabled

CA 3. Activate PM module on target agent host

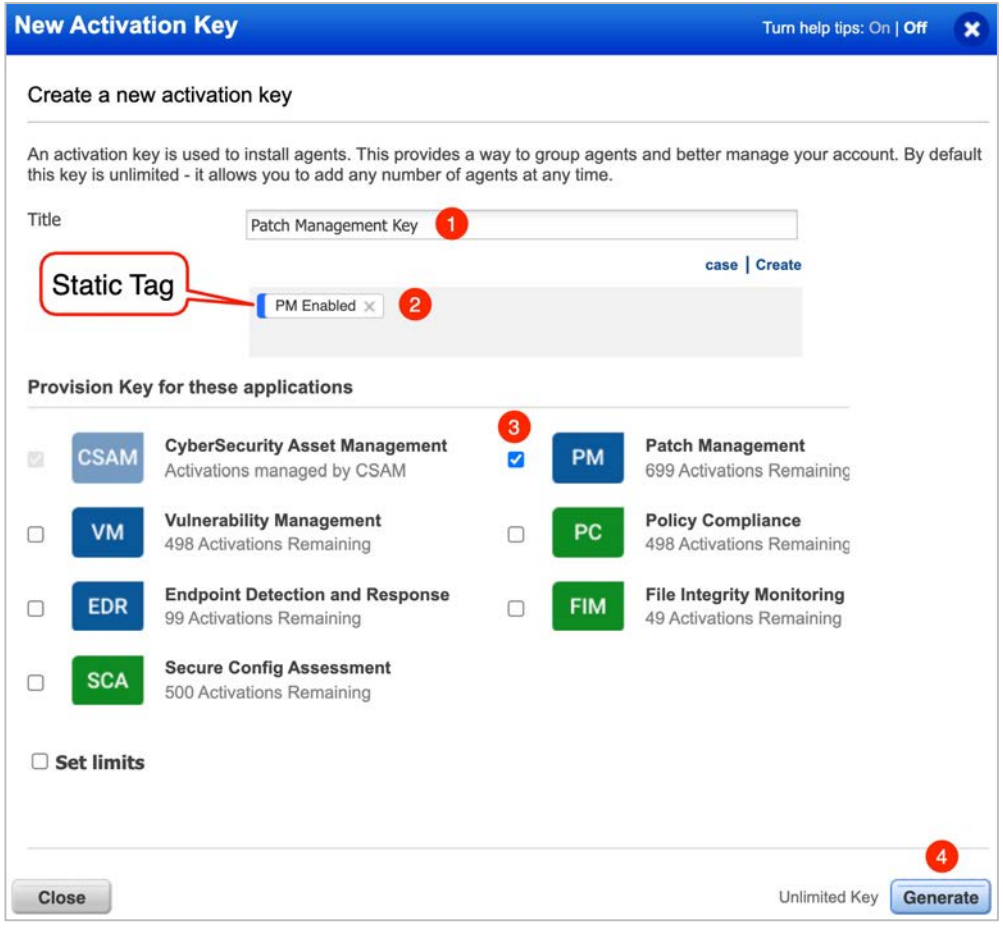
PM 4. Assign PM license to the host

PM 5. Assign target agent host to a PM Assessment Profile (optional)

PM 6. Configure patch deployment job

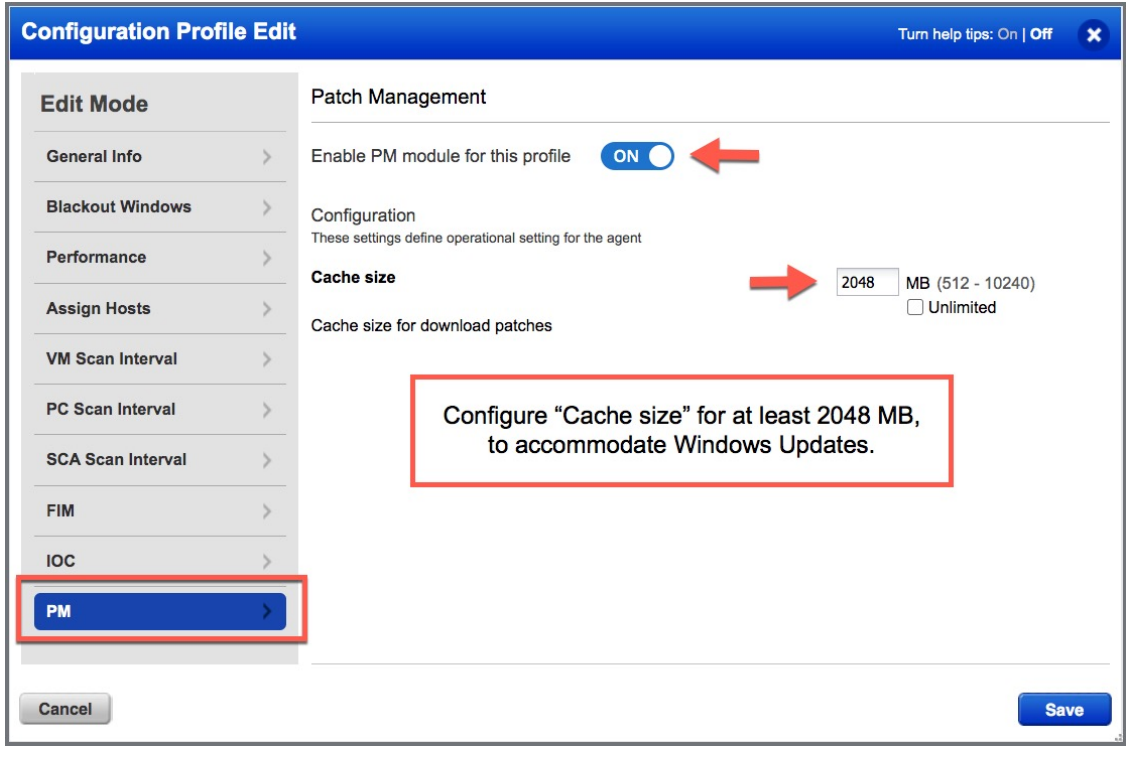
Qualys.

Activation Key



- As a best practice, assign a static tag when creating an Activation Key
- Create a new activation key or update existing key with Patch Management

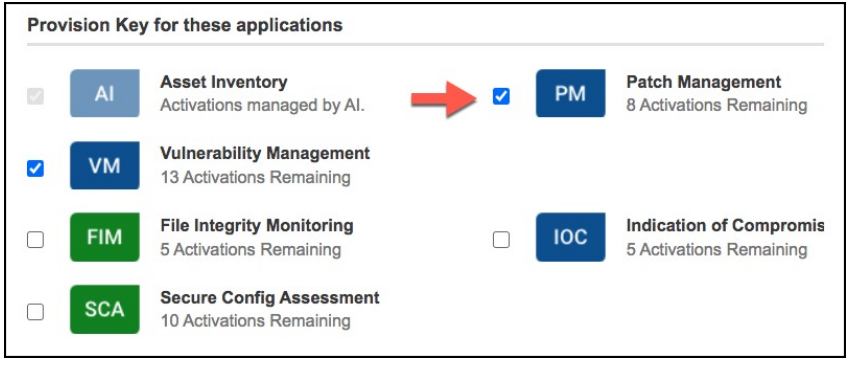
Configuration Profile

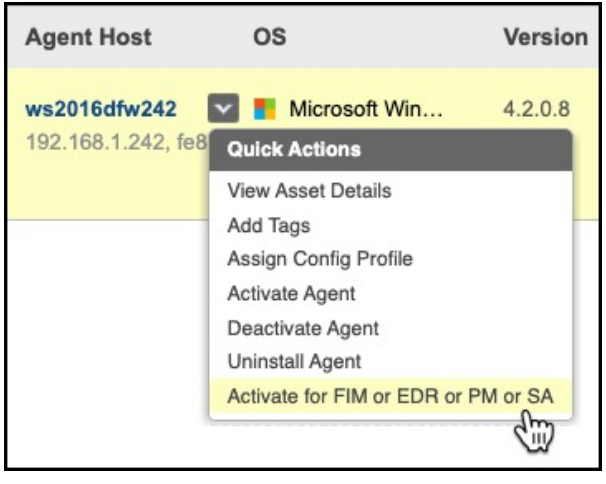


- Assign target hosts to CA Configuration Profile that has PM enabled.
- Set “Cache size” to at least 2048 MB, to accommodate Windows Updates.

Activate PM Module for Target Host

- Select the PM module in the Agent Activation Key, before and after agent deployment.





- Use the “Quick Actions” menu to activate PM for any agent host or use the Qualys Cloud Agent API.

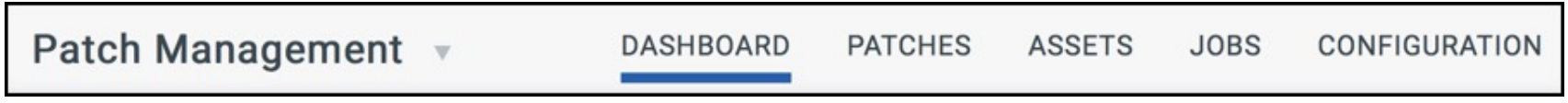
Lab Tutorial 1

PM Activation & Setup – Page 3

Application Overview

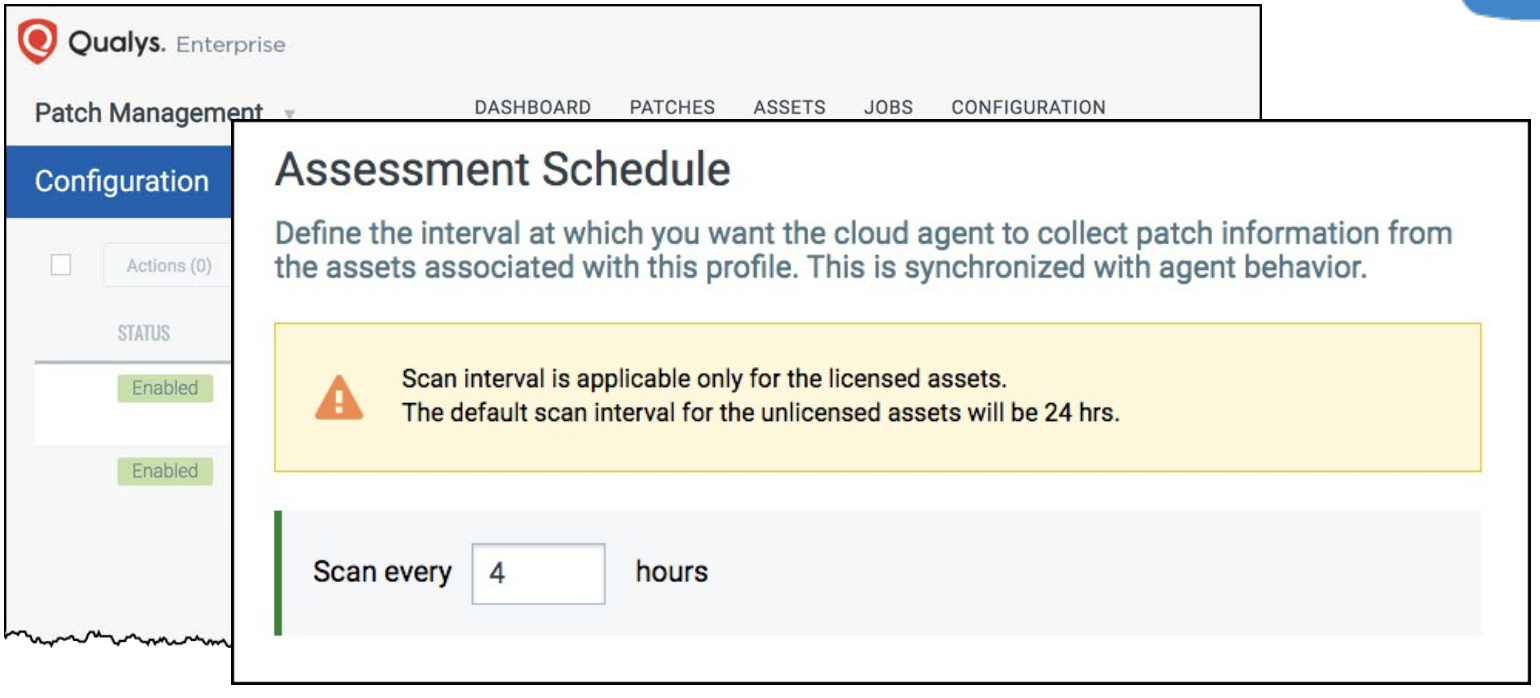
Qualys.

Patch Management UI



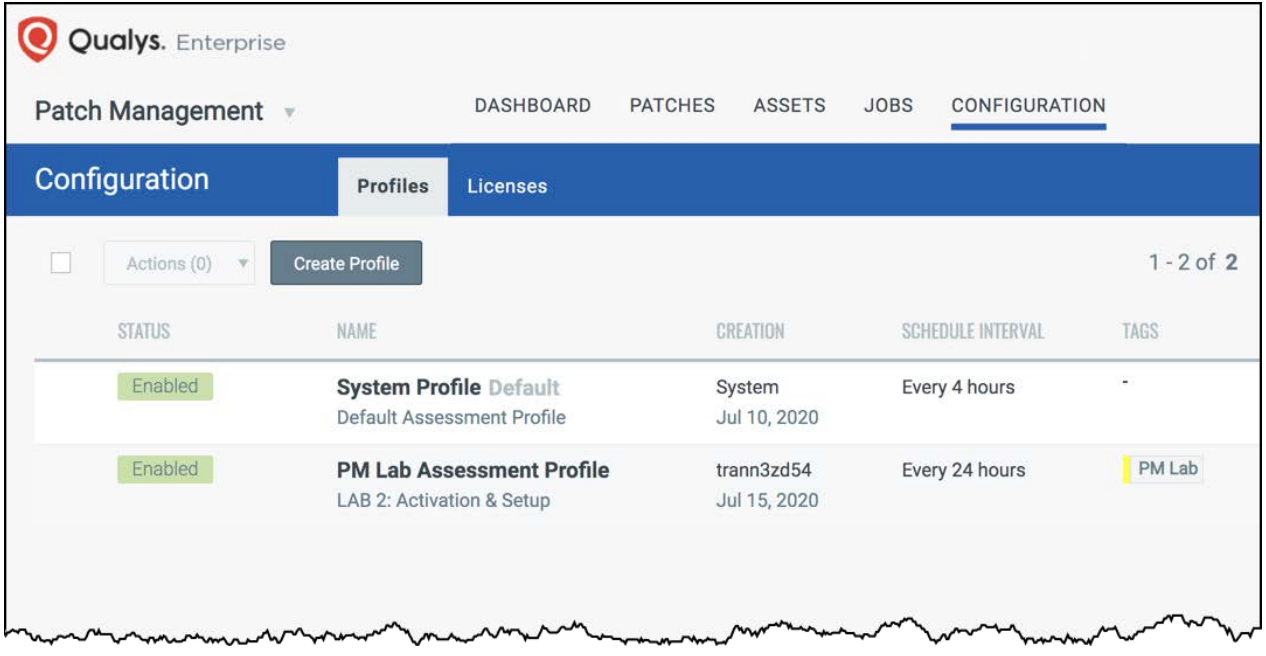
- **CONFIGURATION** – Configure the frequency in which patch assessments are performed and allocate patching licenses.
- **JOBS** – Deploy and/or uninstall specific patches for targeted groups of host assets using one or more PM Jobs.
- **ASSETS** – List of agent host assets the PM module activated.
- **PATCHES** – Catalog containing application and OS patches.
- **DASHBOARD** – Contains “widgets” that monitor important patch statistics.

Patch Assessment Profile



- Specifies frequency of patch assessment scans, which assess agent host assets for missing and/or installed patches.

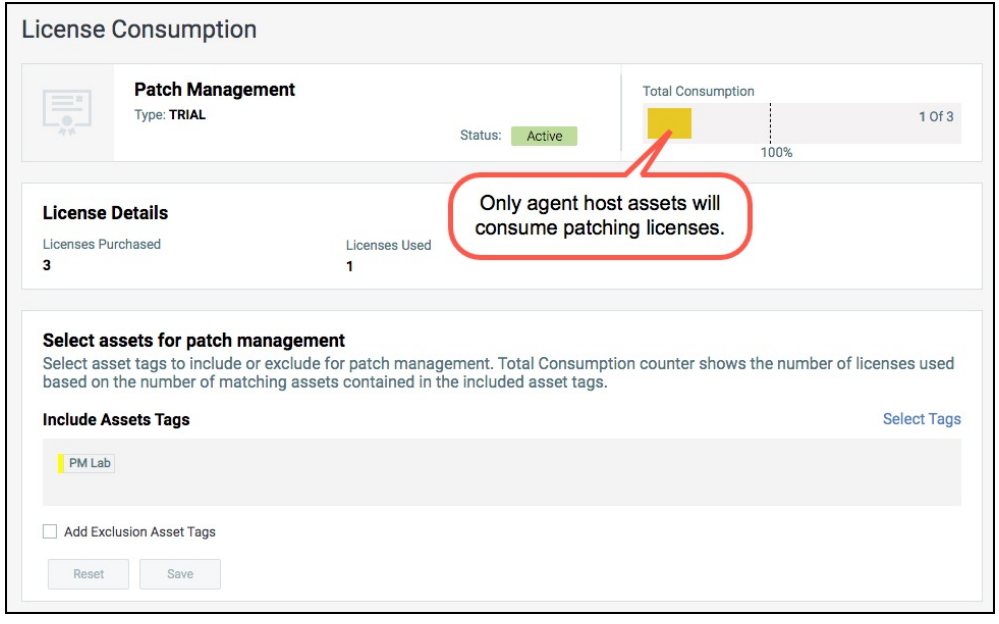
Configuration: Assessment Profile



- If you do not create one or more Assessment Profiles, the System Profile will be used (by default).
- Assessment scans identify the missing and installed patches for an agent host.

Qualys.

Configuration: License Consumption



- Use Asset Tags to specify which agent host assets are eligible for patching.
- Use the “Exclusion” check box to restrict patching on targeted assets.

Deployment Job

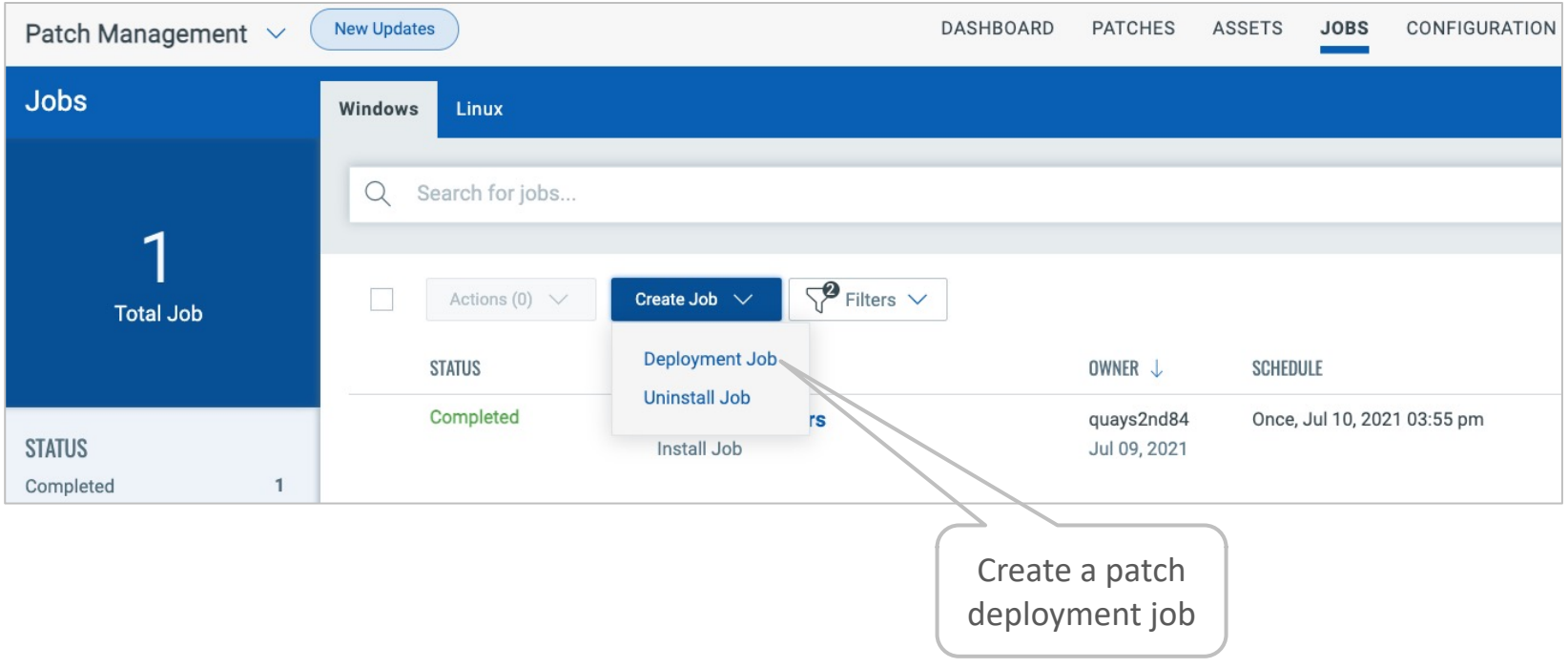
Qualys.

Deployment job

- Use asset tags as targets for patch deployment jobs
- As a recommended practice, **create and use test asset tags** for deployment
- Once verified, **clone the deployment job** and include production asset tags

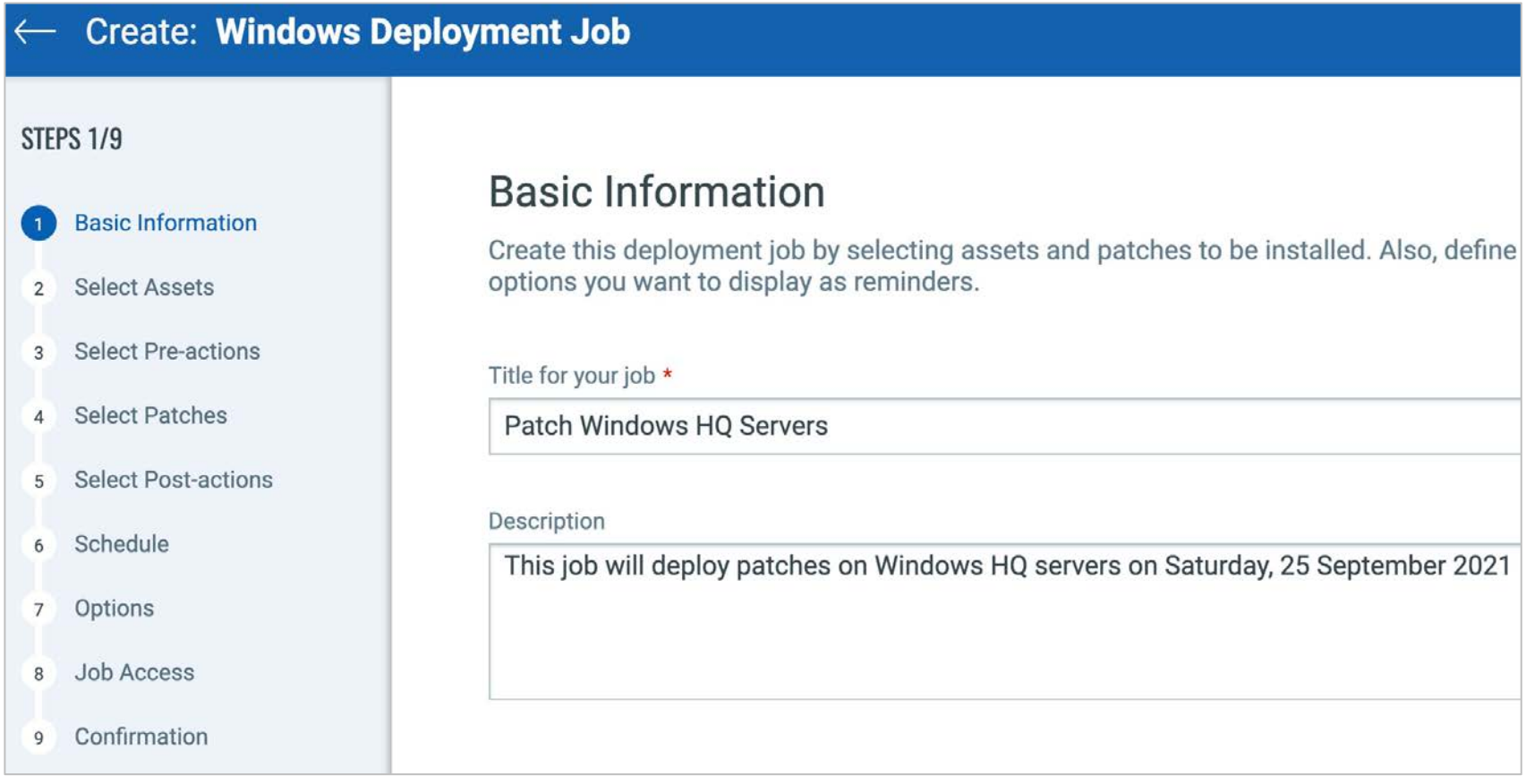
Qualys.

Deployment job



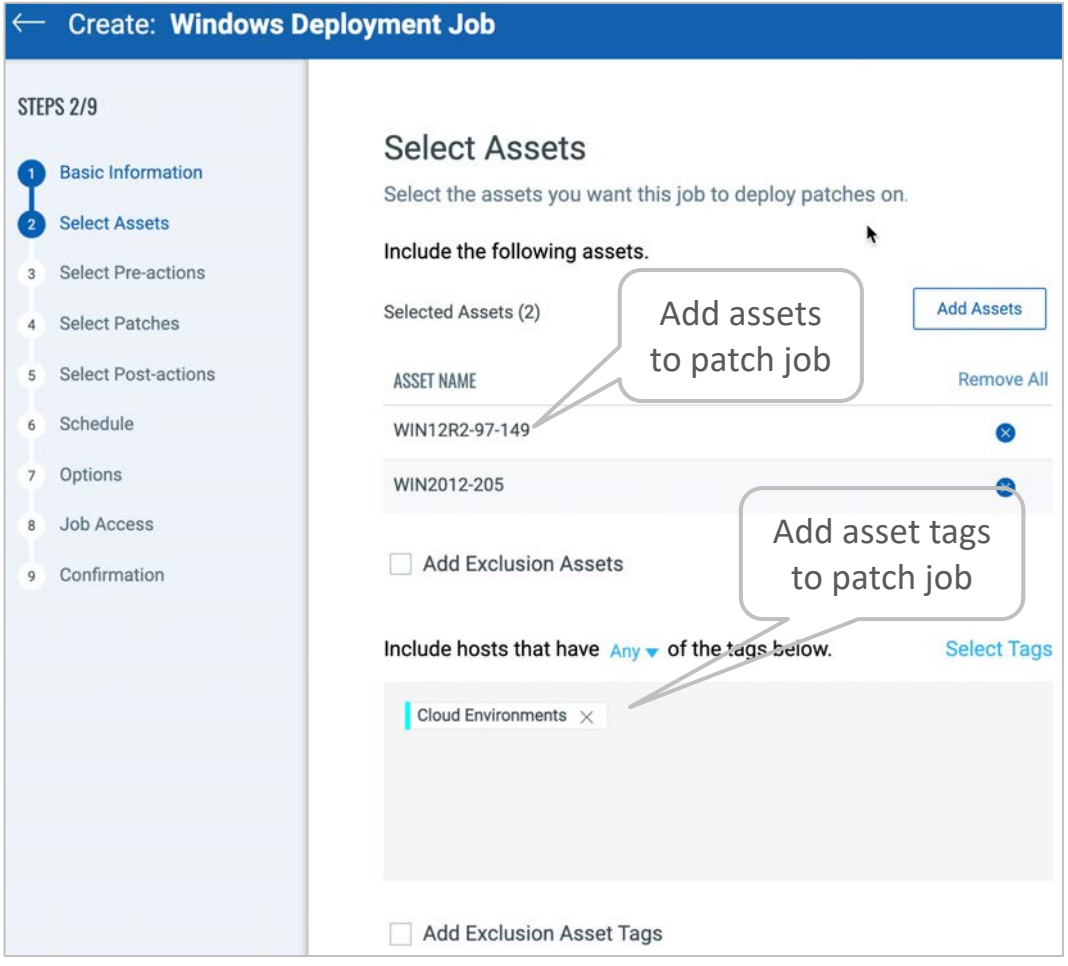
Qualys.

Deployment job – Basic Information



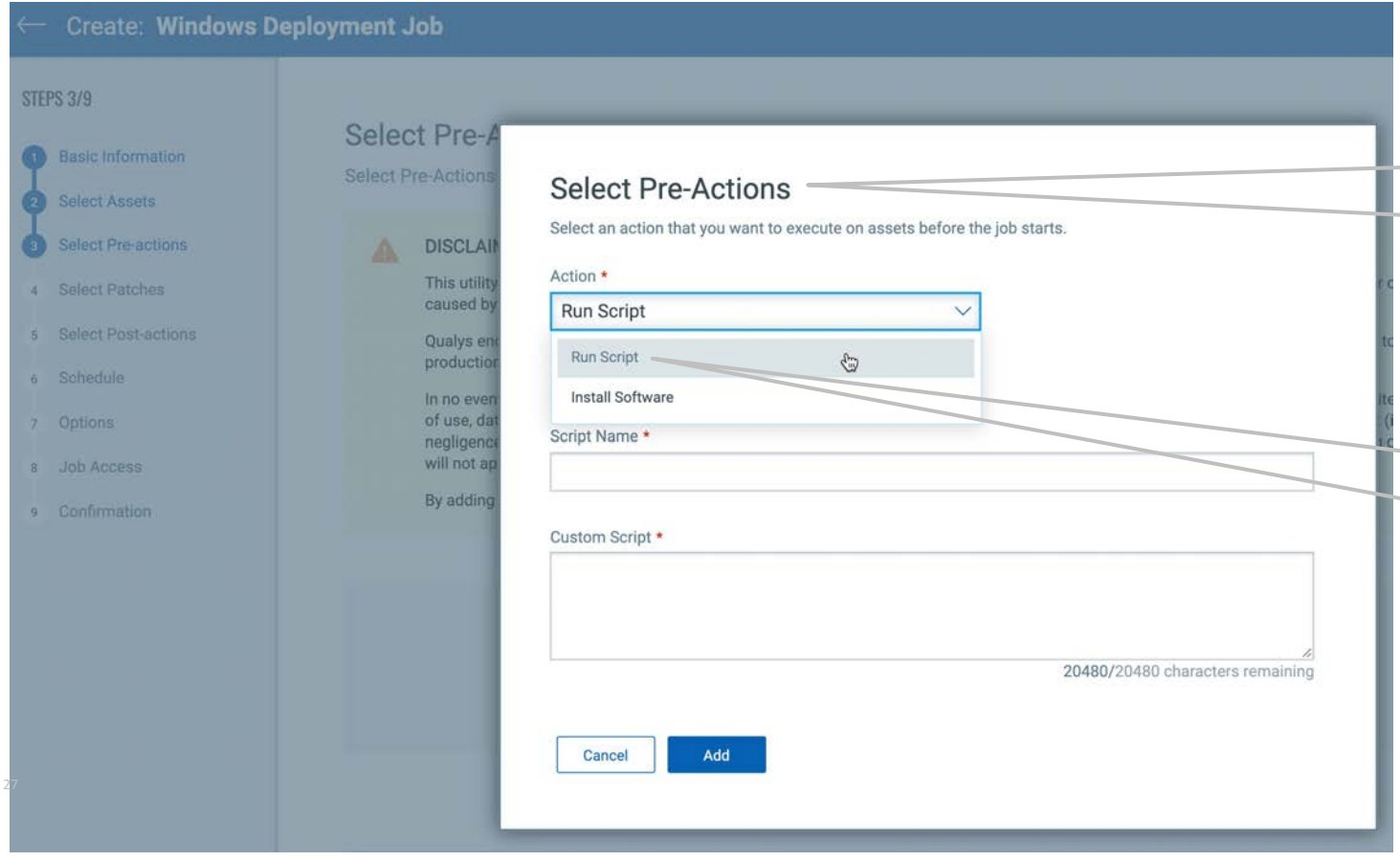
Qualys.

Deployment job – Select Assets



Qualys.

Deployment job – Pre and Post Actions

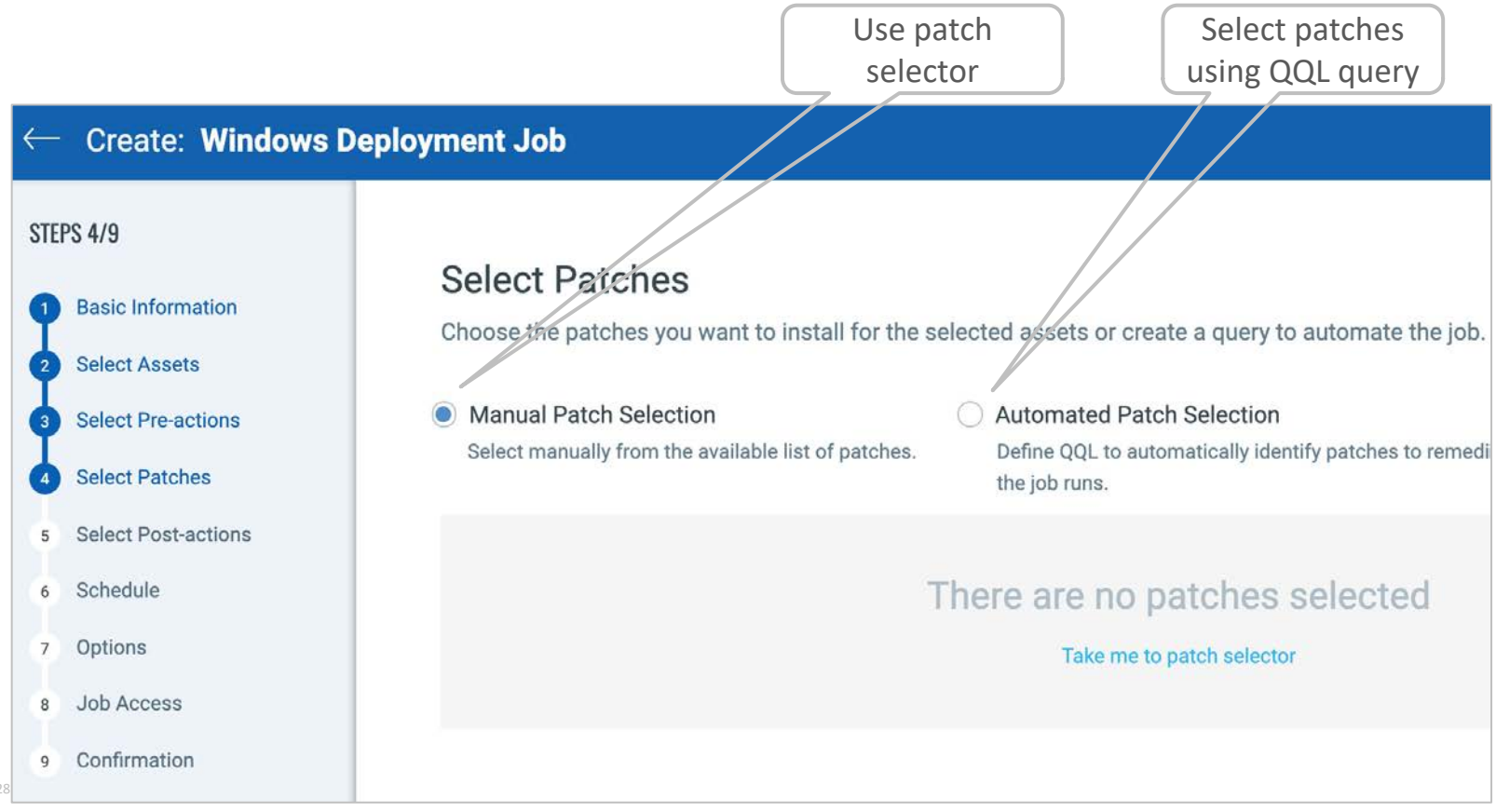


Configure action to execute before job starts

Run a PowerShell script or install software

Qualys.

Deployment job – Select Patches

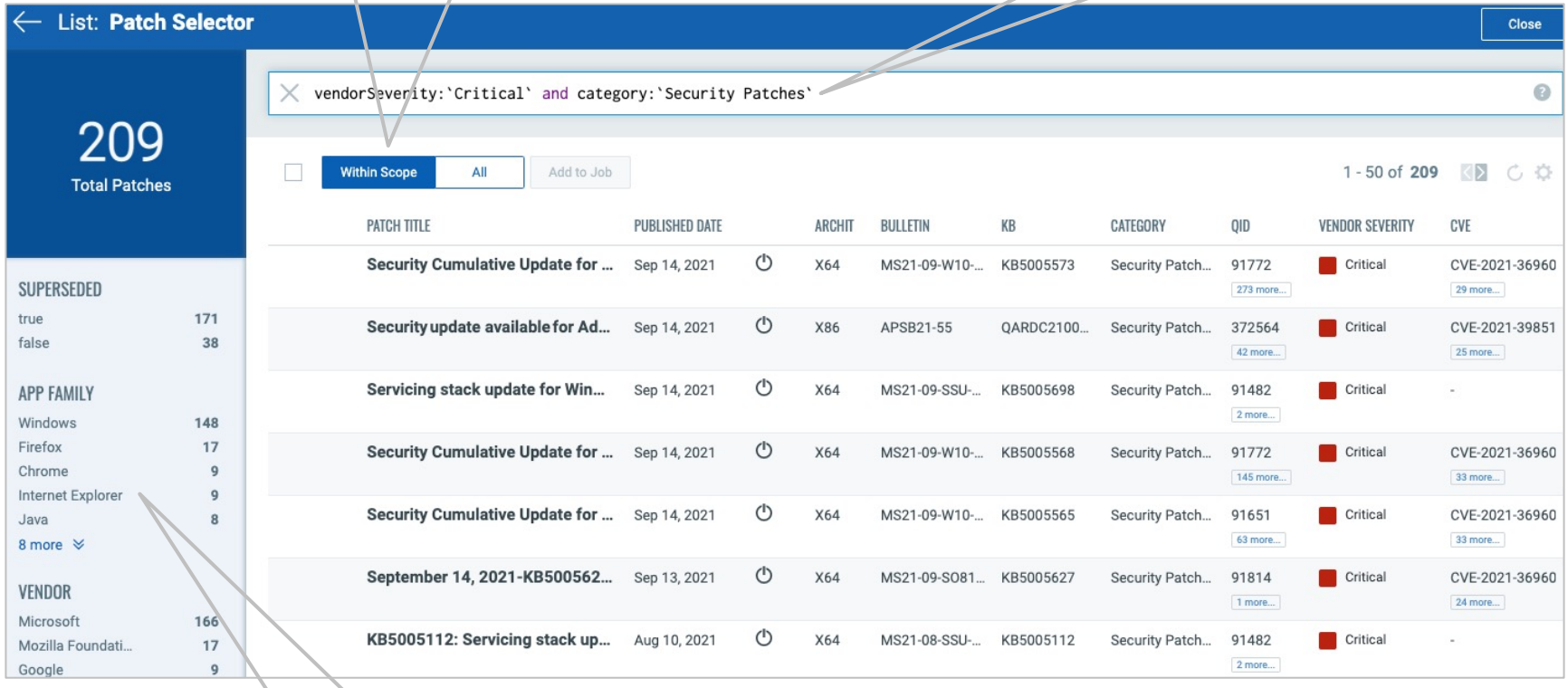


Qualys.

Deployment job – Manual Patch Selector

View patches within scope of selected assets

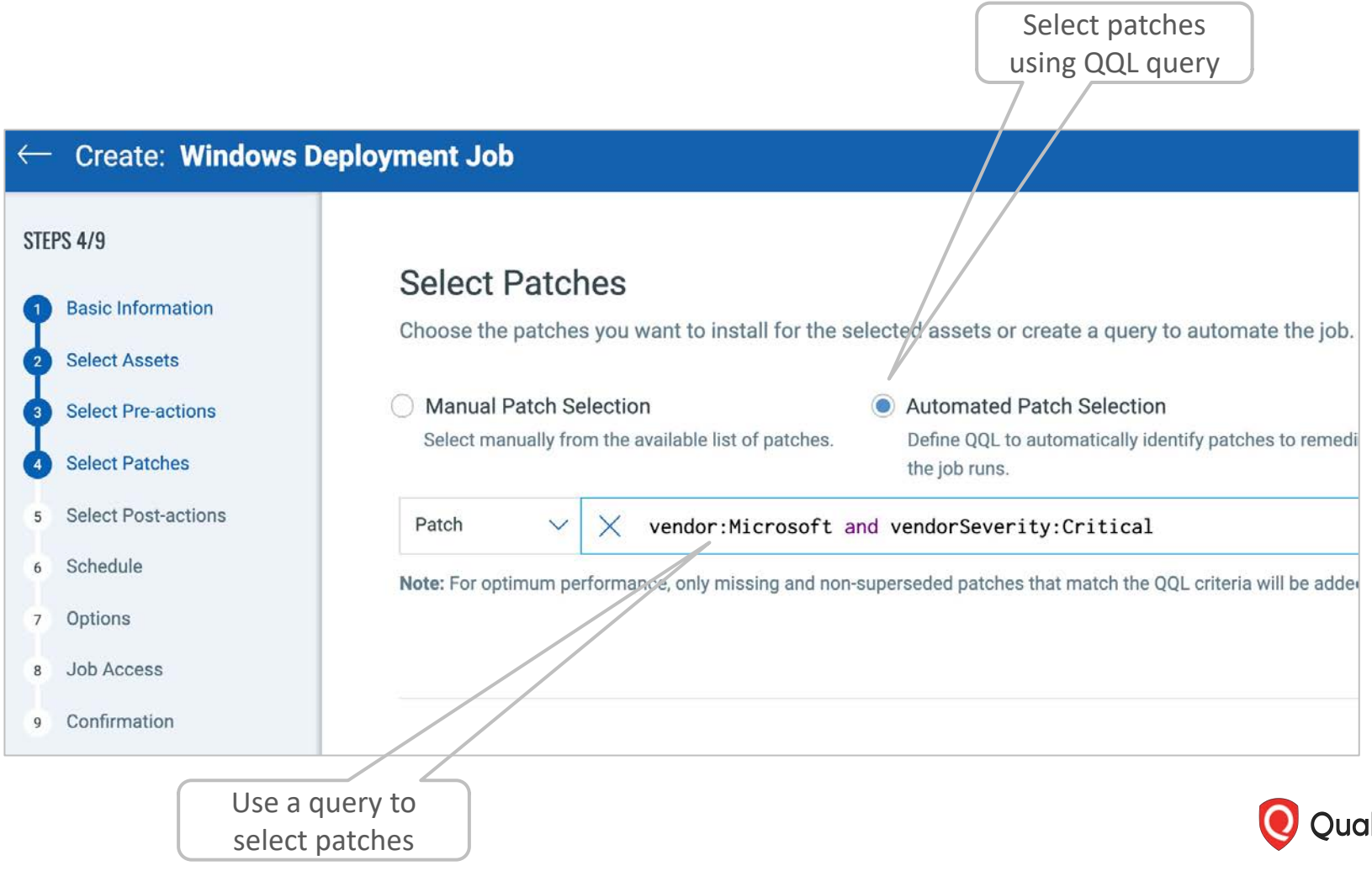
Use queries to narrow selections



Use filters to narrow selections

Qualys.

Deployment job – Automated Patch Selector

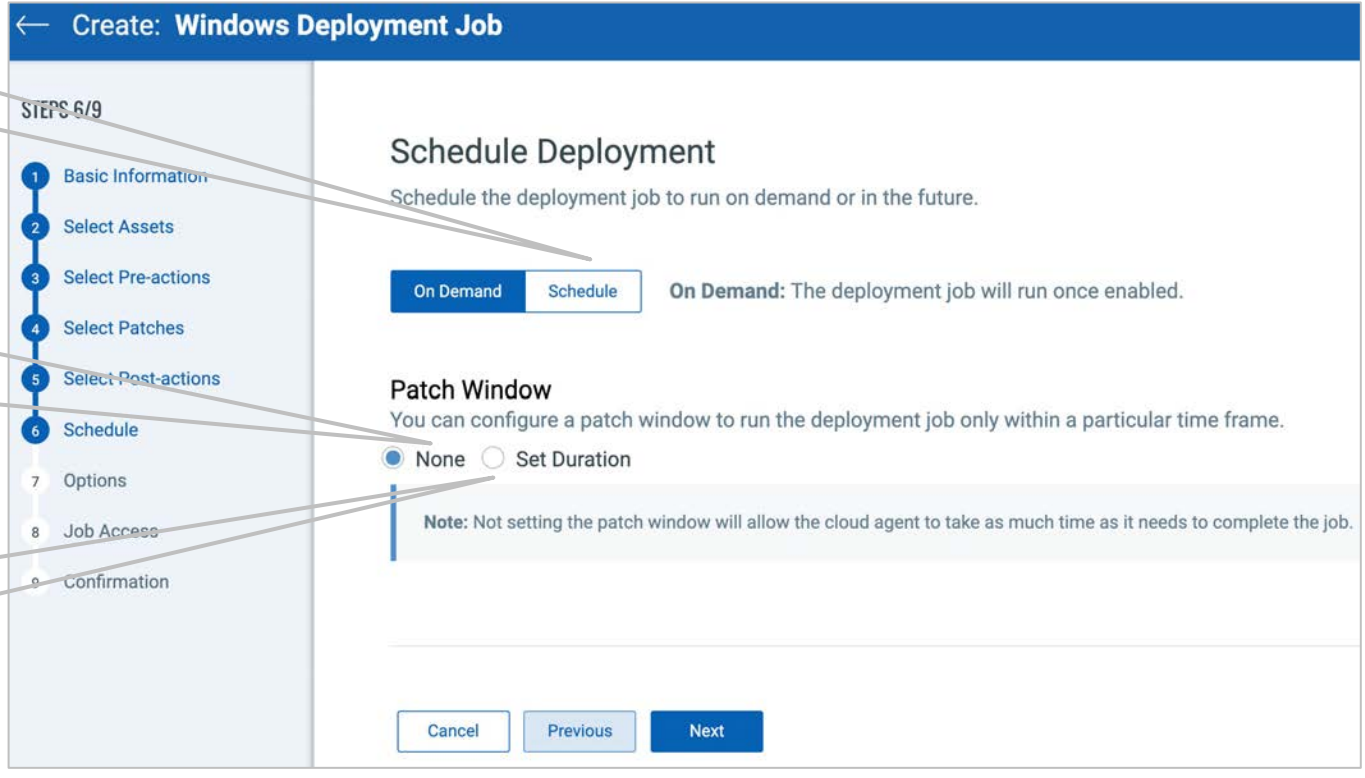


Deployment job – Schedule Deployment

Deploy patches on-demand or schedule for later

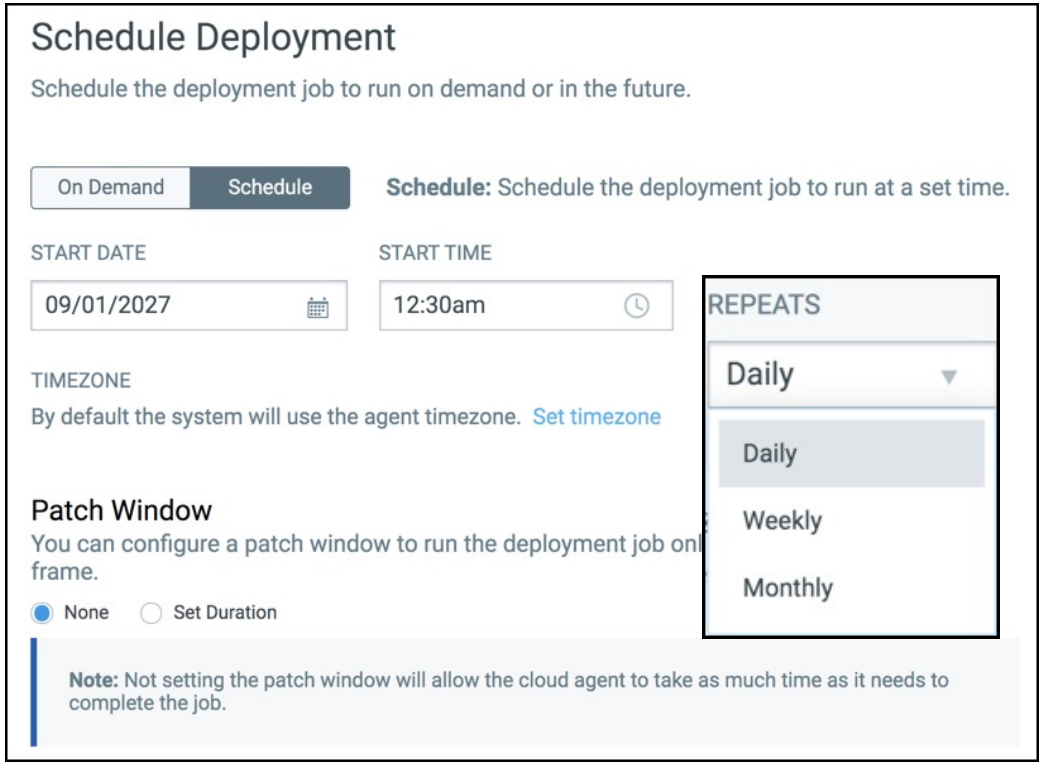
Set to None to allow Qualys the time needed to complete the job

Set duration for on-demand job



Qualys.

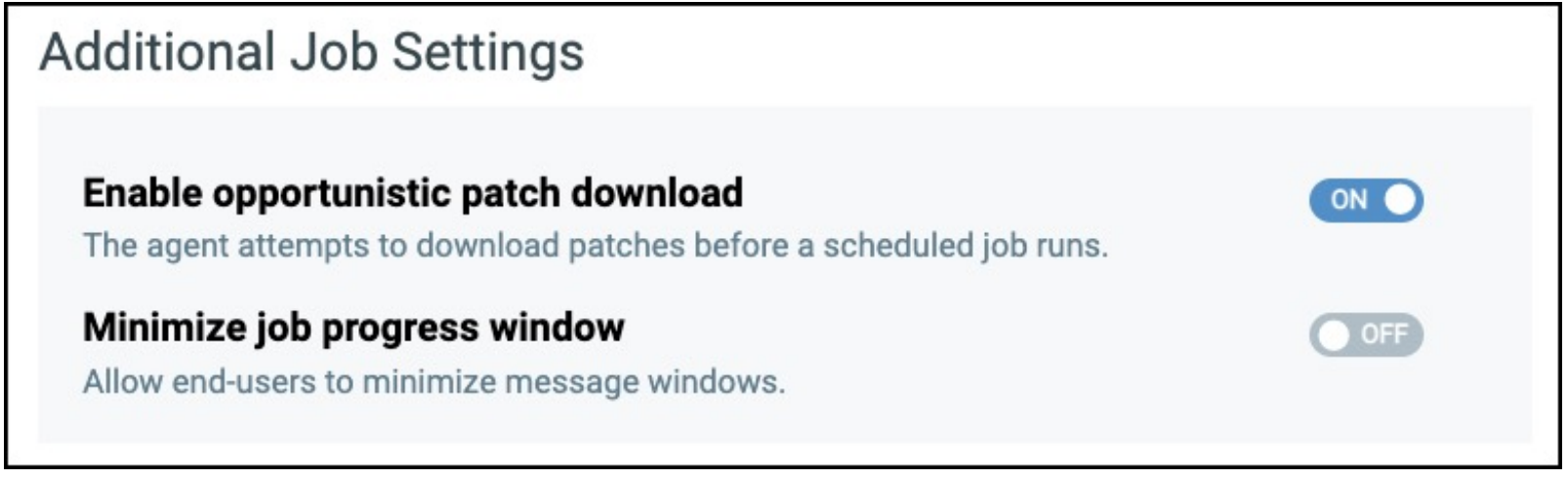
Schedule Deployment



- Run jobs ”on demand” or schedule them to run at regular frequencies.

Qualys.

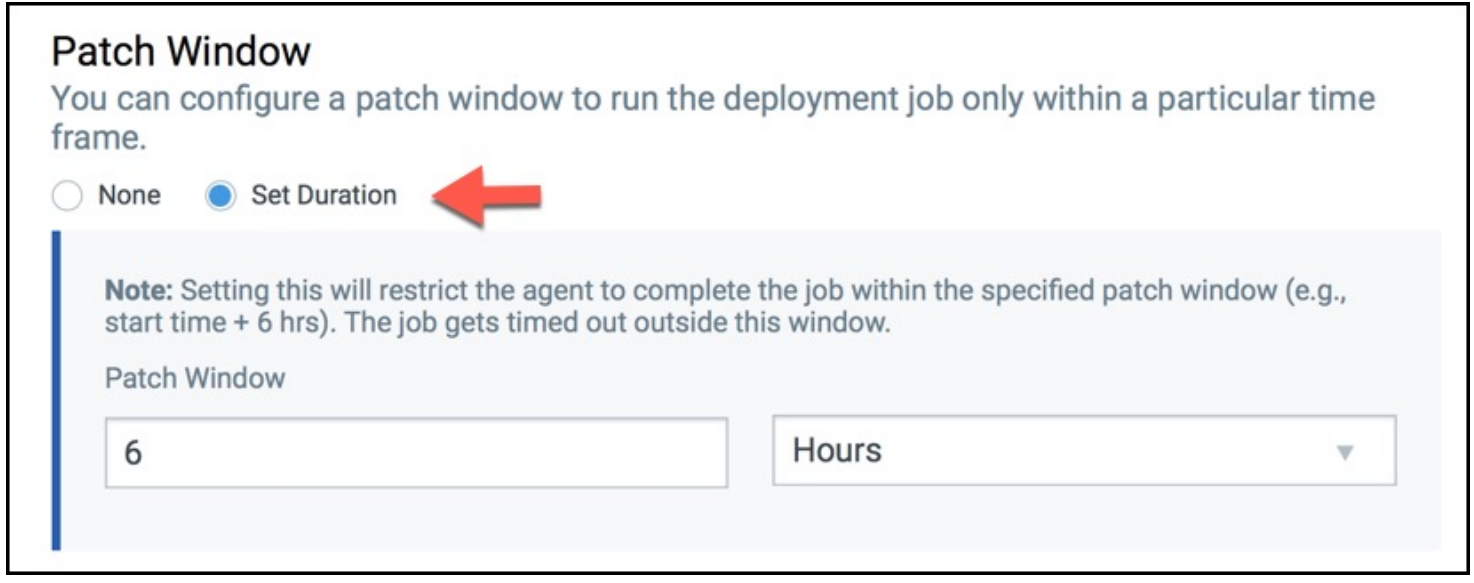
Opportunistic Patch Download



- You can “Enable opportunistic patch download,” to allow agents to download required patches prior to the start of a scheduled job.

Qualys.

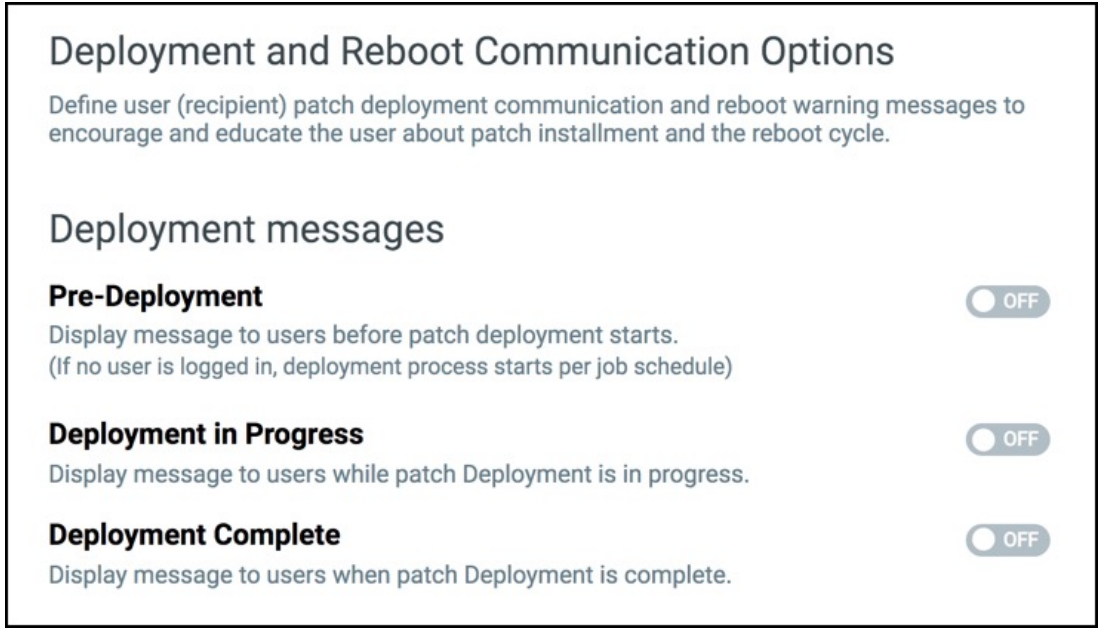
Patch Window



- A job will display the “Timed out” status, if the patch installation does not start within a specified patch window.
- Select the “None” option to give patch jobs an unlimited amount of time.

Qualys.

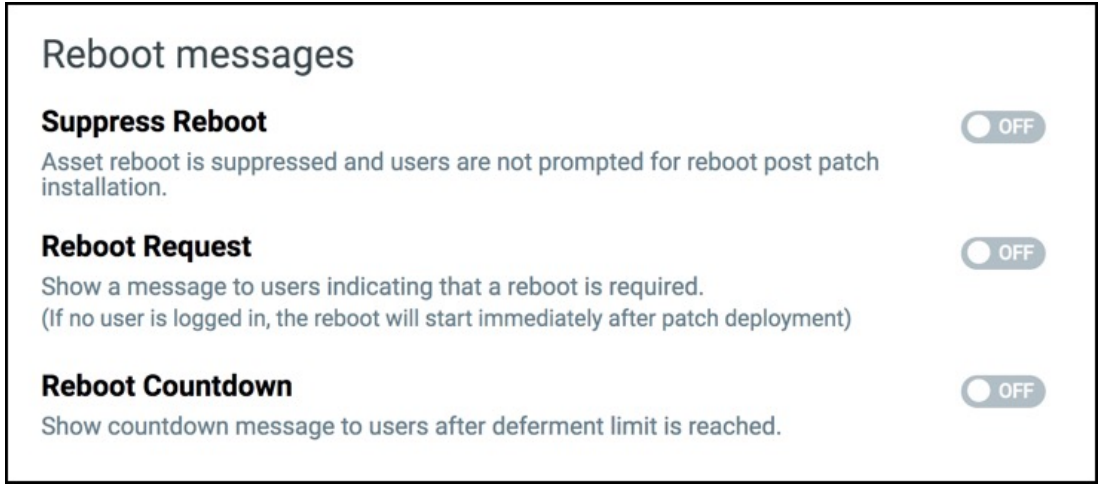
Communication Options



- Choose the type of “Deployment and Reboot Communication Options” for each Deployment Job.

Qualys.

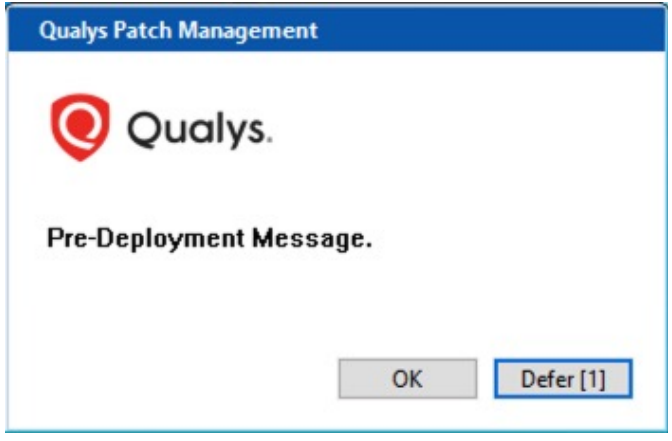
Communication Options

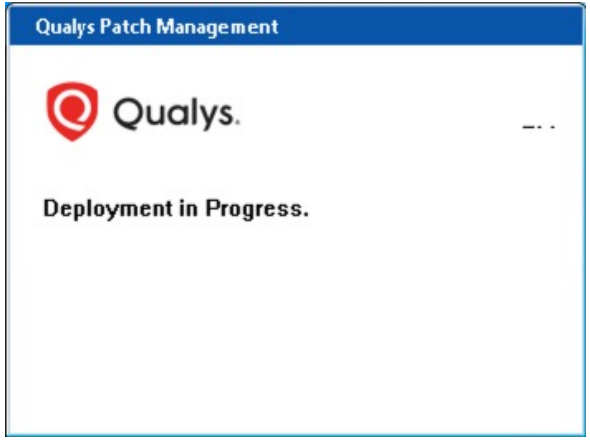


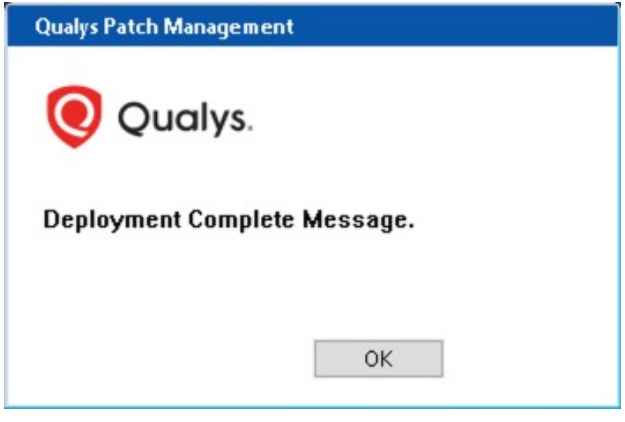
- Choose the type of “Deployment and Reboot Communication Options” for each Deployment Job.

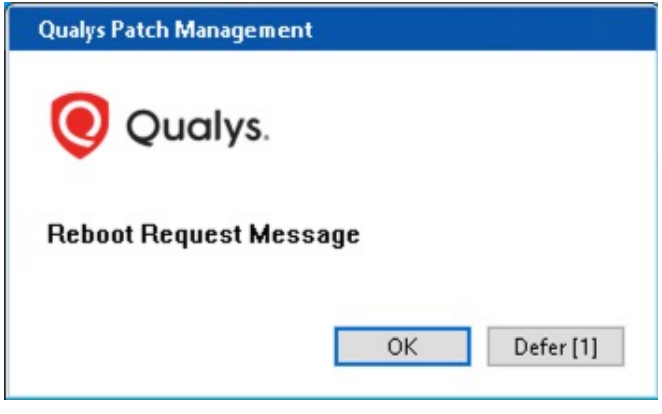
Host “Pop-Up” Messages

- “Pre-Deployment and “Reboot Request messages can be configured with deferment options.



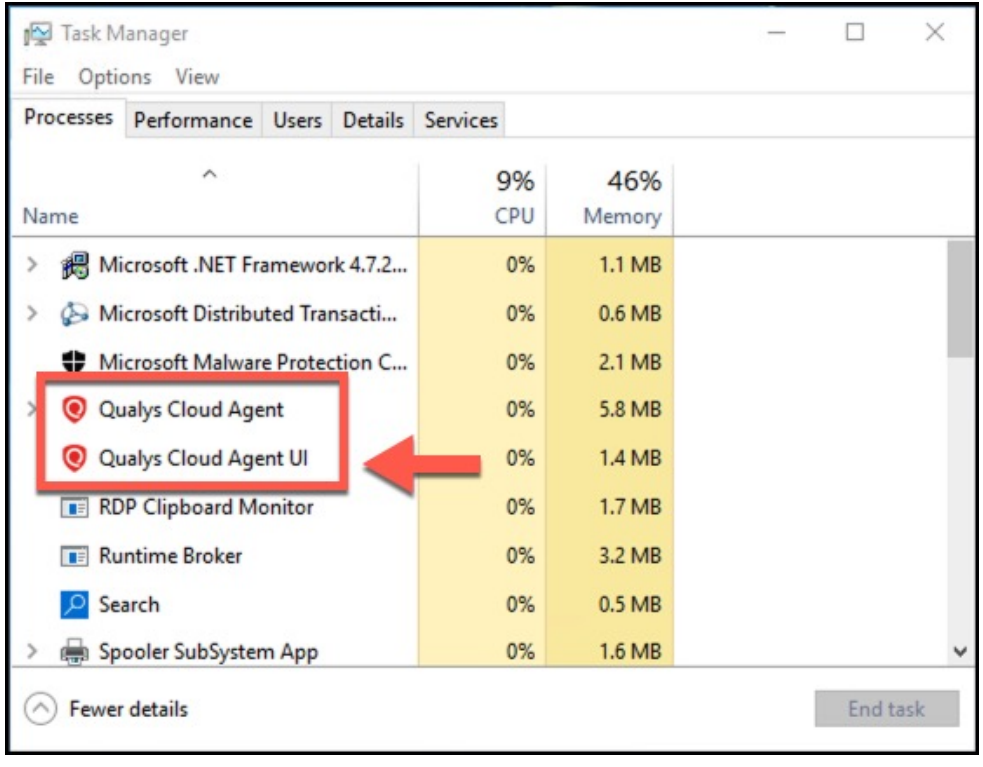






Qualys.

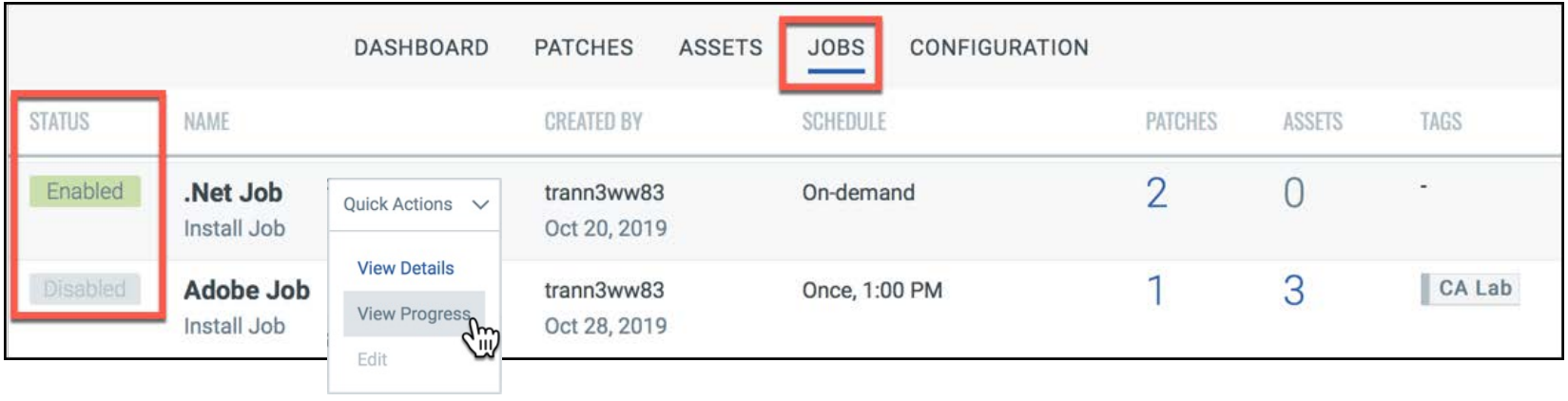
PM Processes & Executables



- When patching is active on a Windows host, patching messages and notifications are managed by the “Qualys Cloud Agent UI” process (QualysAgentUI.exe)
- ‘stdeploy.exe’ is the name of the patching executable.

Qualys.

Job Status



View Job Status:

- **Enabled** – Job is presently active.
- **Disabled** – Job is presently inactive.
- **Completed** – Job has completed.

Qualys.

View Job Progress

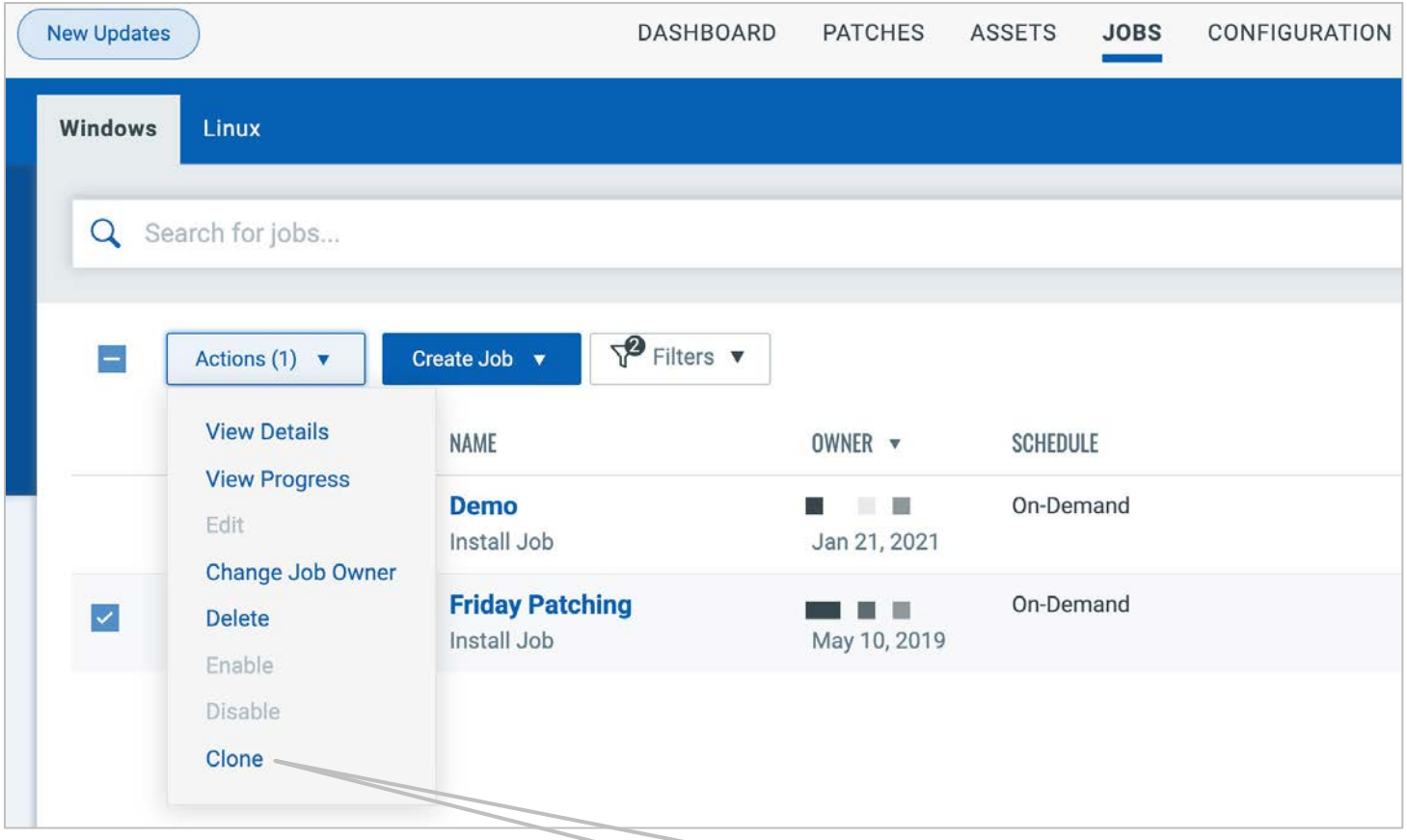
STATUS	ASSET NAME	OS	PATCHES INSTALLED	PATCHES FAILED	PATCHES SKIPPED
Pending Oct 28, 2019	**WS2016DFW242** fe80:0:0:0:d42d:825a:8140:153, 192.168....	Microsoft Windows Server 2016 Stand...	—	—	—
Completed Oct 28, 2019	**WS2012EVAL206** fe80:0:0:0:383a:fada:a31b:e92c, 192.168...	Microsoft Windows Server 2012 R2 Sta...	0	0	1
Completed Oct 28, 2019	**WS2016DFW251** fe80:0:0:0:fd21:1c55:3da9:ba53, 192.168...	Microsoft Windows Server 2016 Stand...	0	0	1

Qualys.

Job Status

Status	Description
Canceled – Blackout	Patch deployment job is canceled on the asset due to blackout window
Completed	Patch deployment job is completed on the asset
Downloaded	Patch file is successfully downloaded on the asset
Downloading – failed	Patch failed to download on the asset
Not licensed	Job manifest cannot be sent as the asset does not have PM license
Job started	Agent has started the job
Job resumed	Asset is restarted and agent has resumed the job
Job failed	Agent encountered an error while executing the job
Patching	Patch job is running on the asset
Pending	Patch job is pending for execution on the asset
Pending reboot	Reboot activity is pending for the asset
Rebooted	Asset is restarted after patch installation
Timed out	Job is timed out

Clone job



Clone an existing job

Qualys.

Lab Tutorial 2

PM Deployment Job – Page 6

Session Break

Qualys.

Prioritized Products

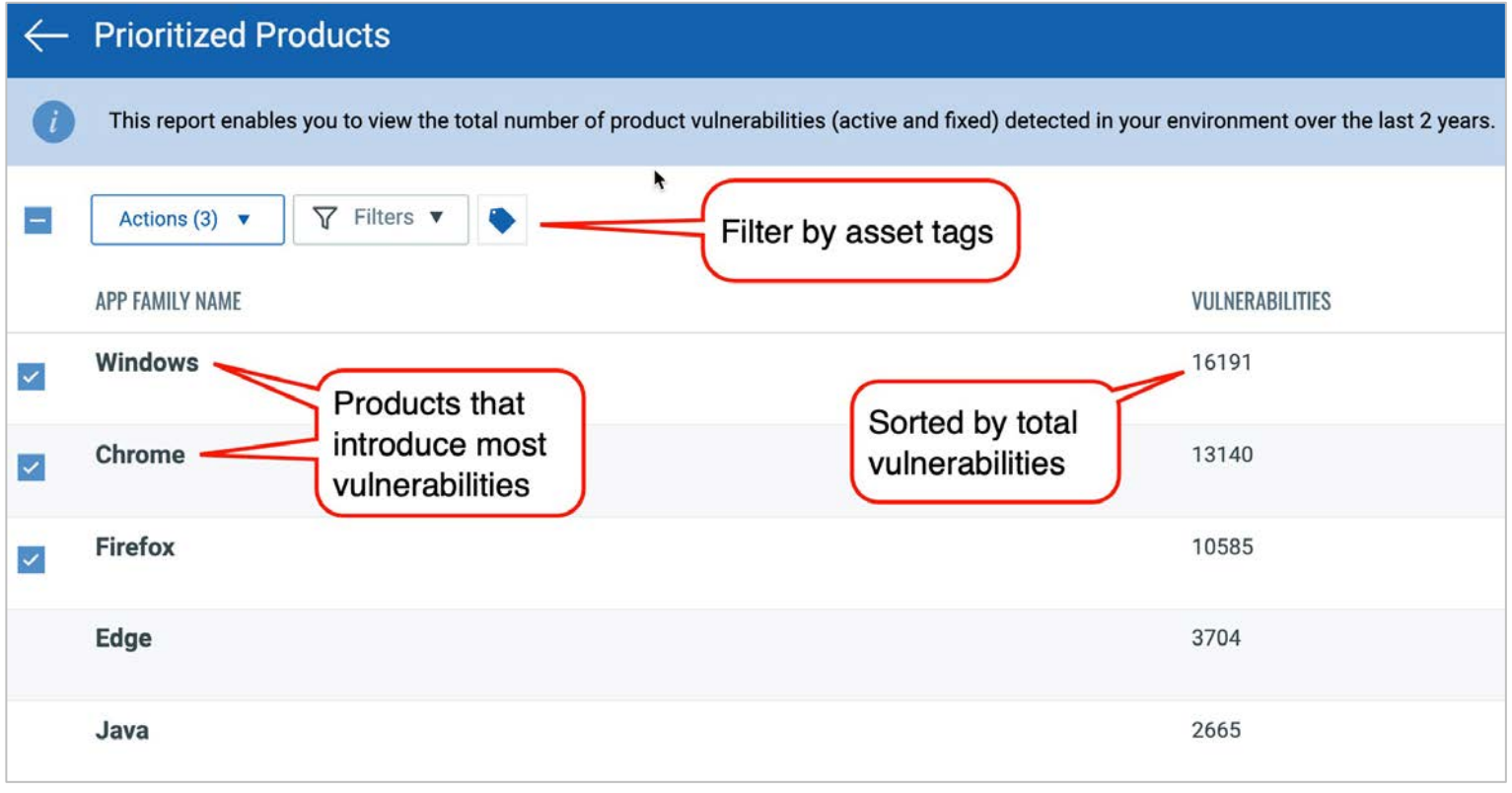
Qualys.

Prioritized Products

- Focus on products in your environment that are important to patch on a regular basis
- Prioritizes products that introduce the most vulnerabilities from the last 2 years
- Helps answer the question – **which products should I patch first**?
- Create a zero-touch recurring deployment job targeting products with most vulnerabilities

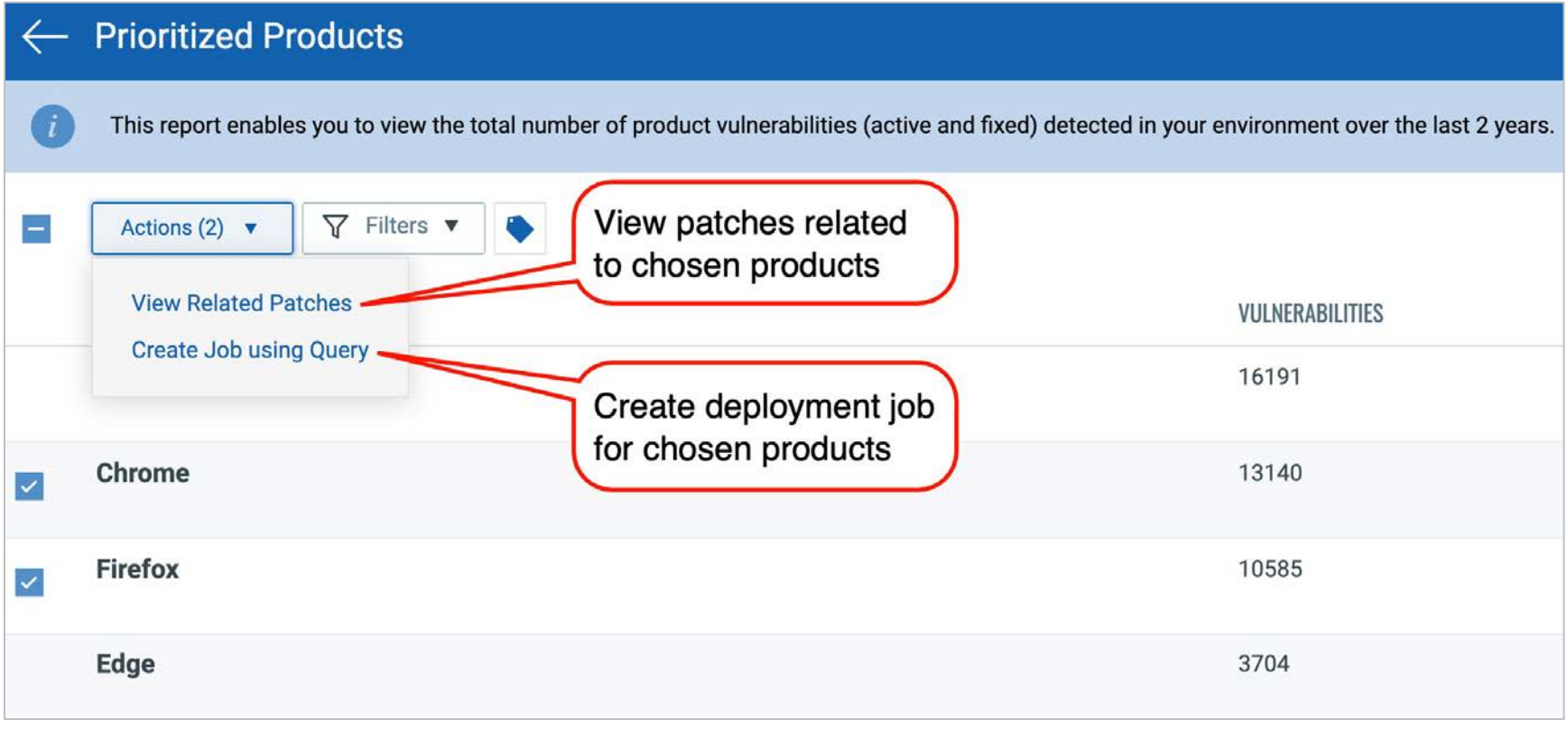
Qualys.

Prioritized Products



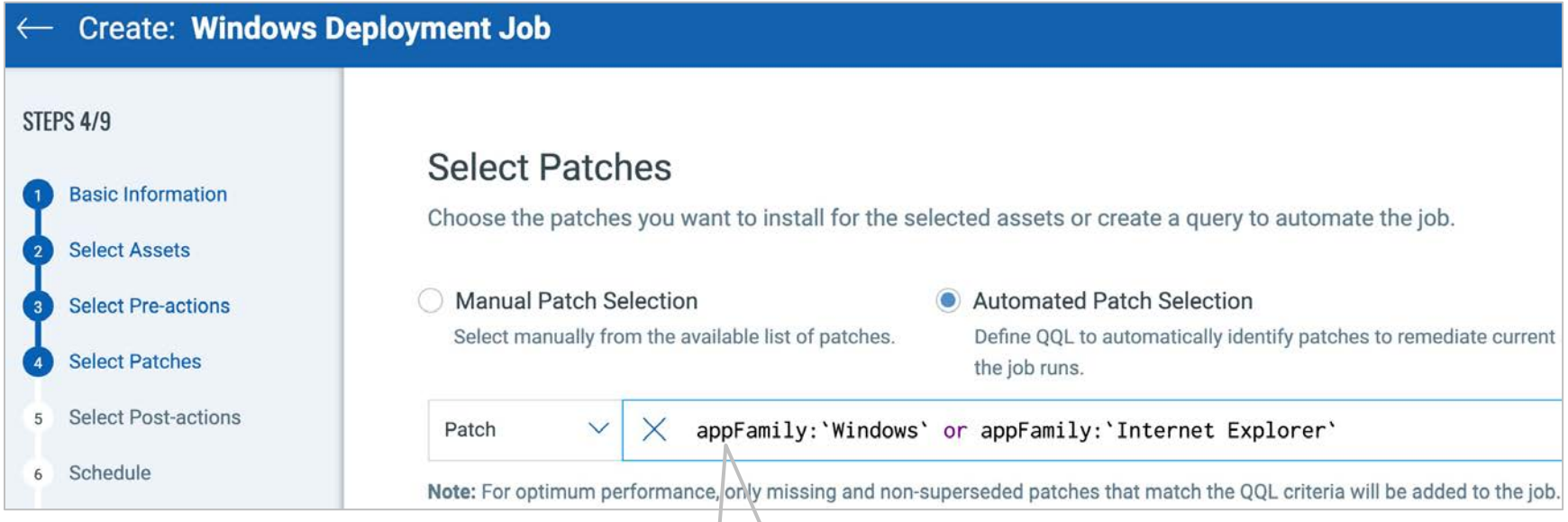
Qualys.

Prioritized Products



Qualys.

Prioritized Products



Query is automatically built based on chosen products

Qualys.

Lab Tutorial 3

Prioritized Products – Page 11

Patching from VMDR and VM

Qualys.

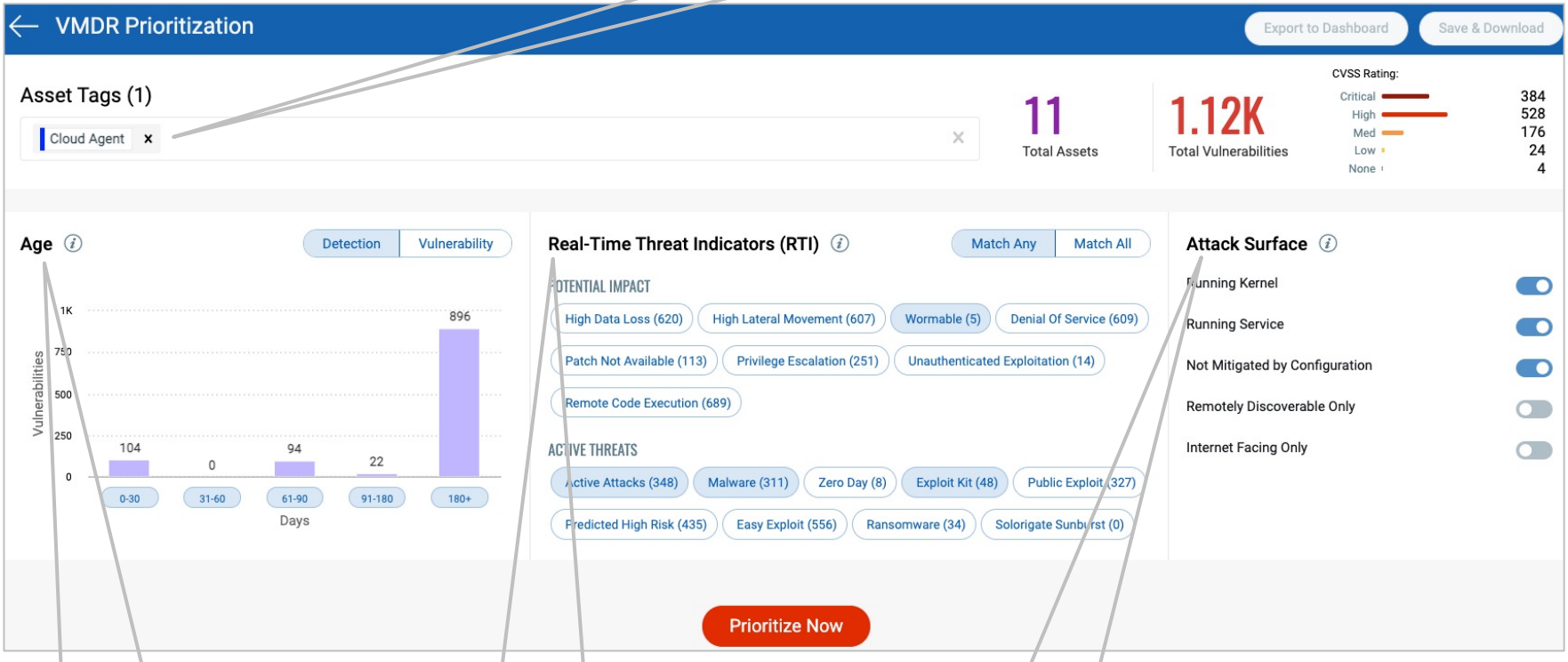
VMDR Prioritization Report

- Identify vulnerabilities that pose the maximum risk to your business
- Correlate vulnerability information with threat intelligence and asset context
- Identify patches required to fix high risk vulnerabilities
- Reduce remediation time with the integrated patch management workflow and zero-touch patching

Qualys.

VMDR Prioritization

Assets to prioritize



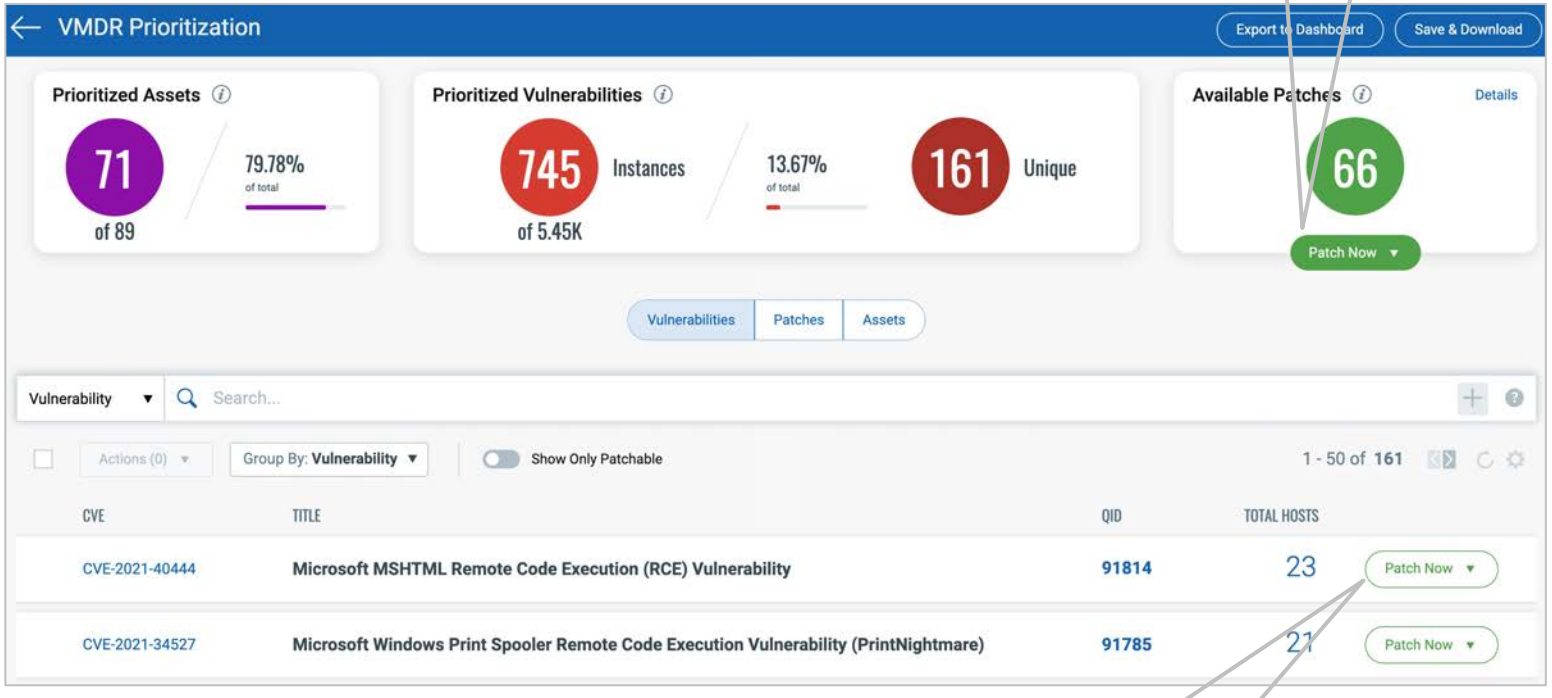
Prioritize vulnerabilities by age

Prioritize based on RTI's

Prioritize by Attack Surface

Qualys.

VMDR Prioritization

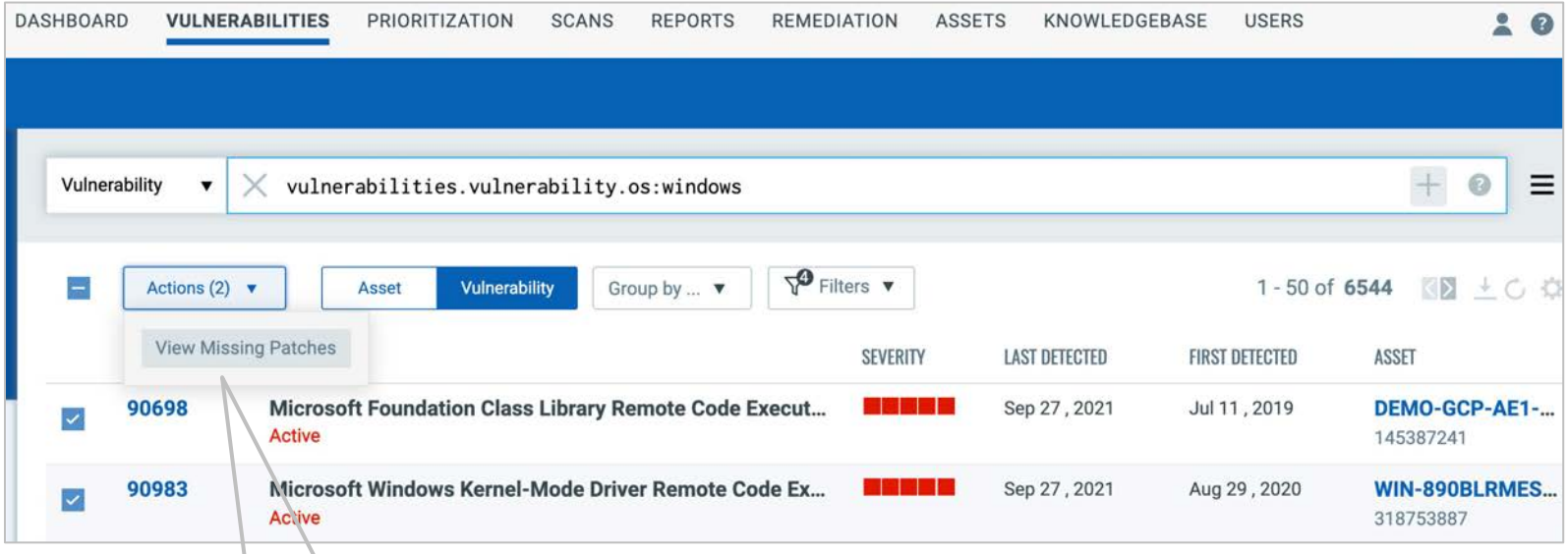


Patch all vulnerabilities

Select vulnerabilities for patching

Qualys.

Vulnerabilities Section

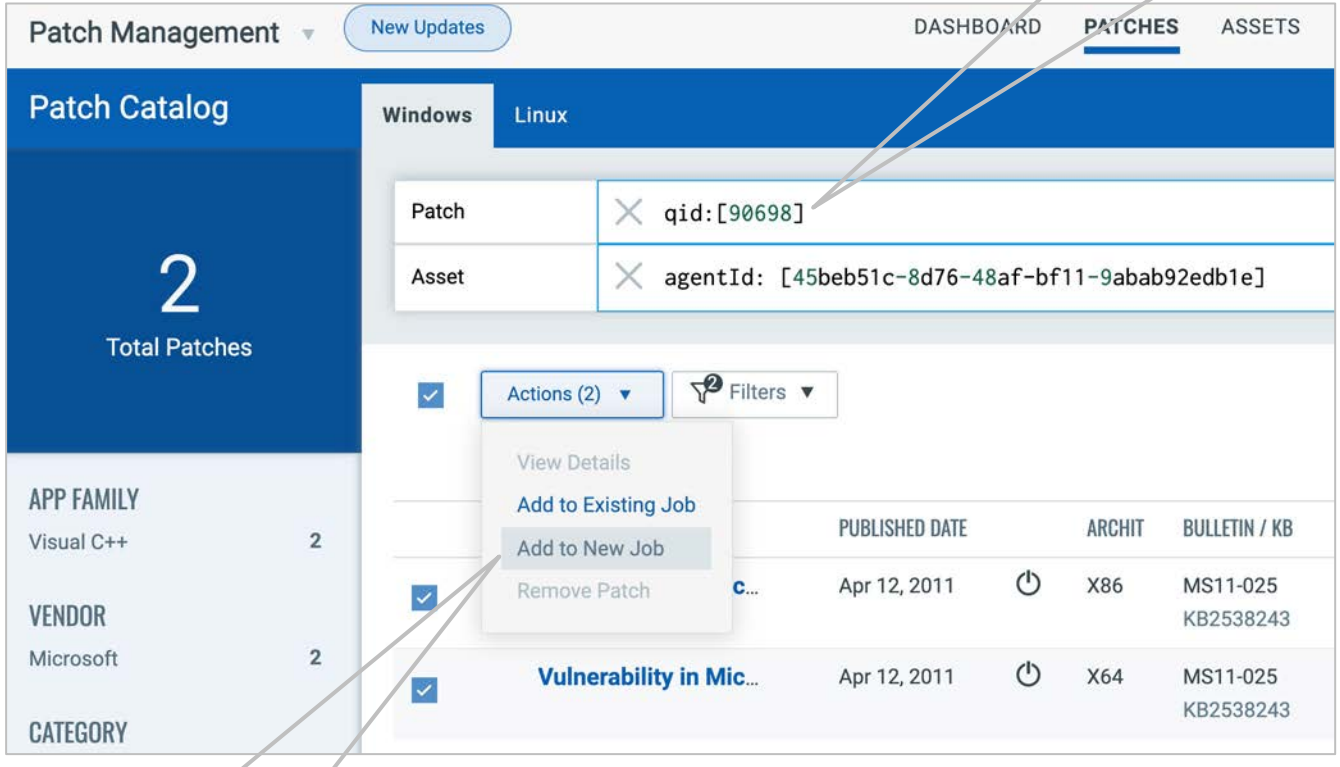


View missing patches for selected vulnerabilities

Qualys.

Vulnerabilities Section

A query is built based on your vulnerability selections



Apply missing patches causing vulnerabilities

Qualys.

Zero Touch Vulnerability Remediation

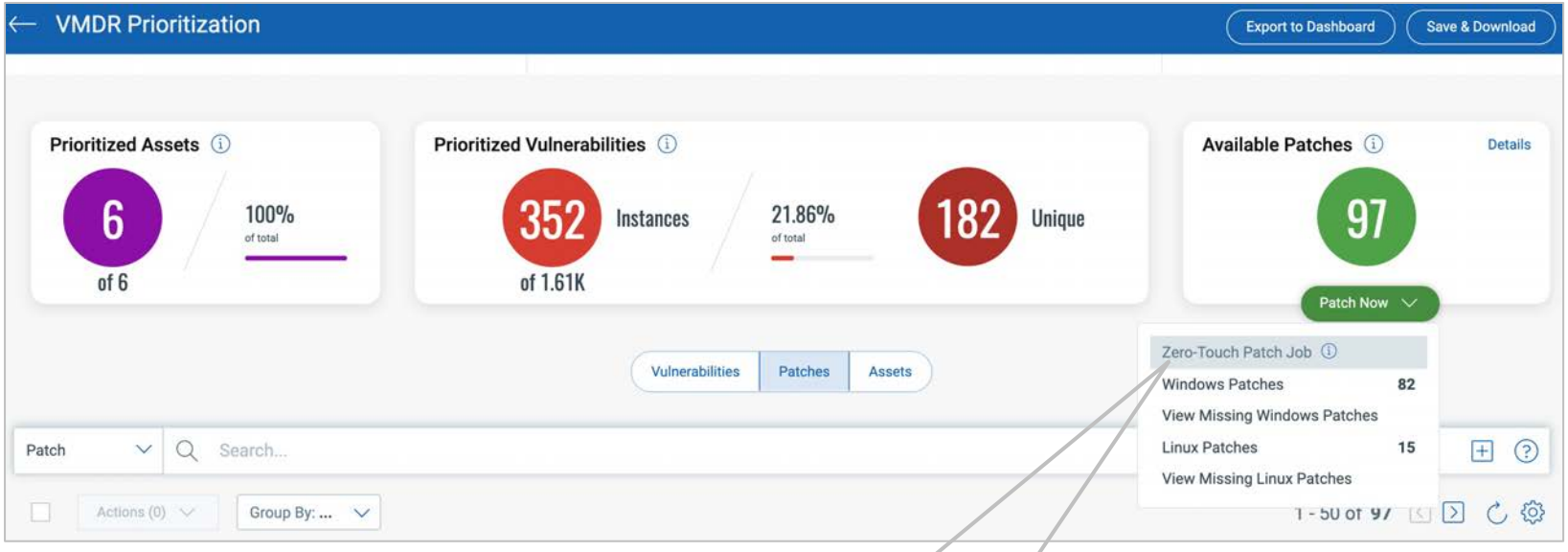
Qualys.

Zero Touch Patching

- Update endpoints and servers proactively as soon as patches are available
- Remediate new vulnerabilities even before security teams run scans
- Automate patch vulnerabilities based on the vulnerability RTI
- Can be initiated from “VMDR Prioritization” report or the “Prioritized Products” report

Qualys.

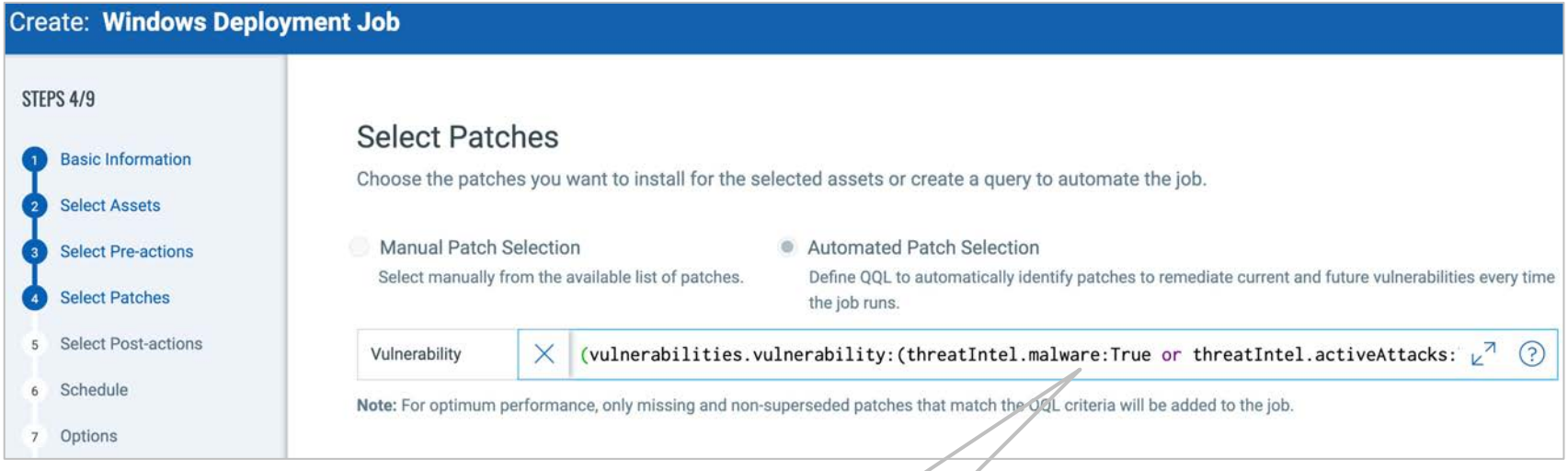
Zero Touch Patching



Initiate zero-touch patch job

Qualys.

Zero Touch Patching



QQL is automatically populated from the prioritization report

Qualys.

Lab Tutorial 4

Patching from VM and VMDR – Page 13

Zero-Touch Patch Job – Page 14

Qualys.

Uninstall Job

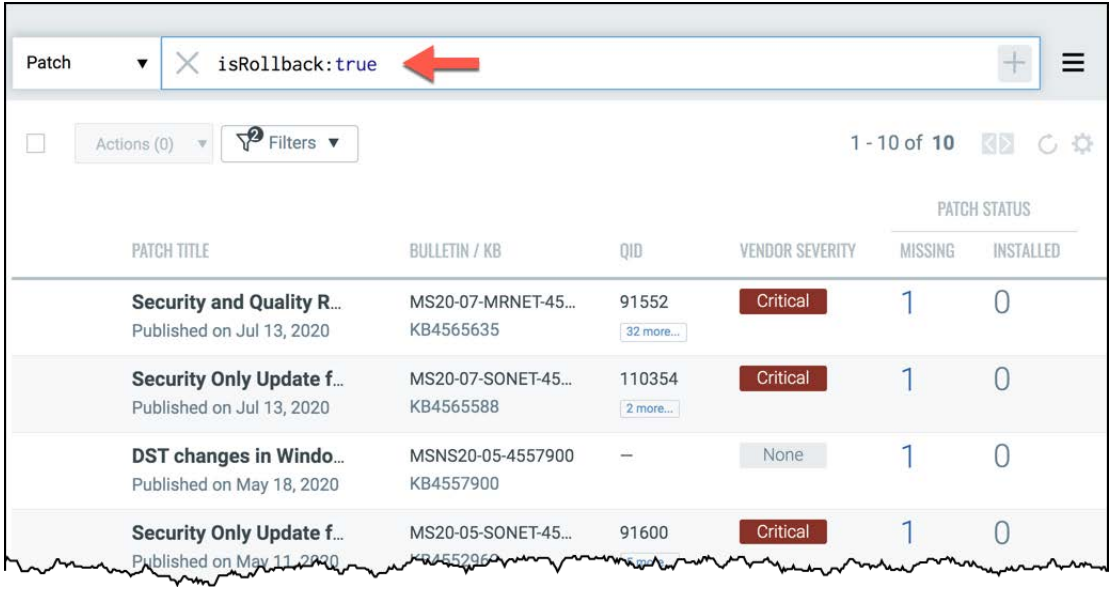
Qualys.

Patch Jobs

- Uninstall jobs are created exclusively in the Patch Management application.
- The workflow for creating uninstall jobs is very similar to deployment jobs.

Qualys.

Uninstall or “Rollback” Patches



- Only “rollback” patches are displayed when creating an uninstall job.
- Not all patches can be uninstalled.

Qualys.

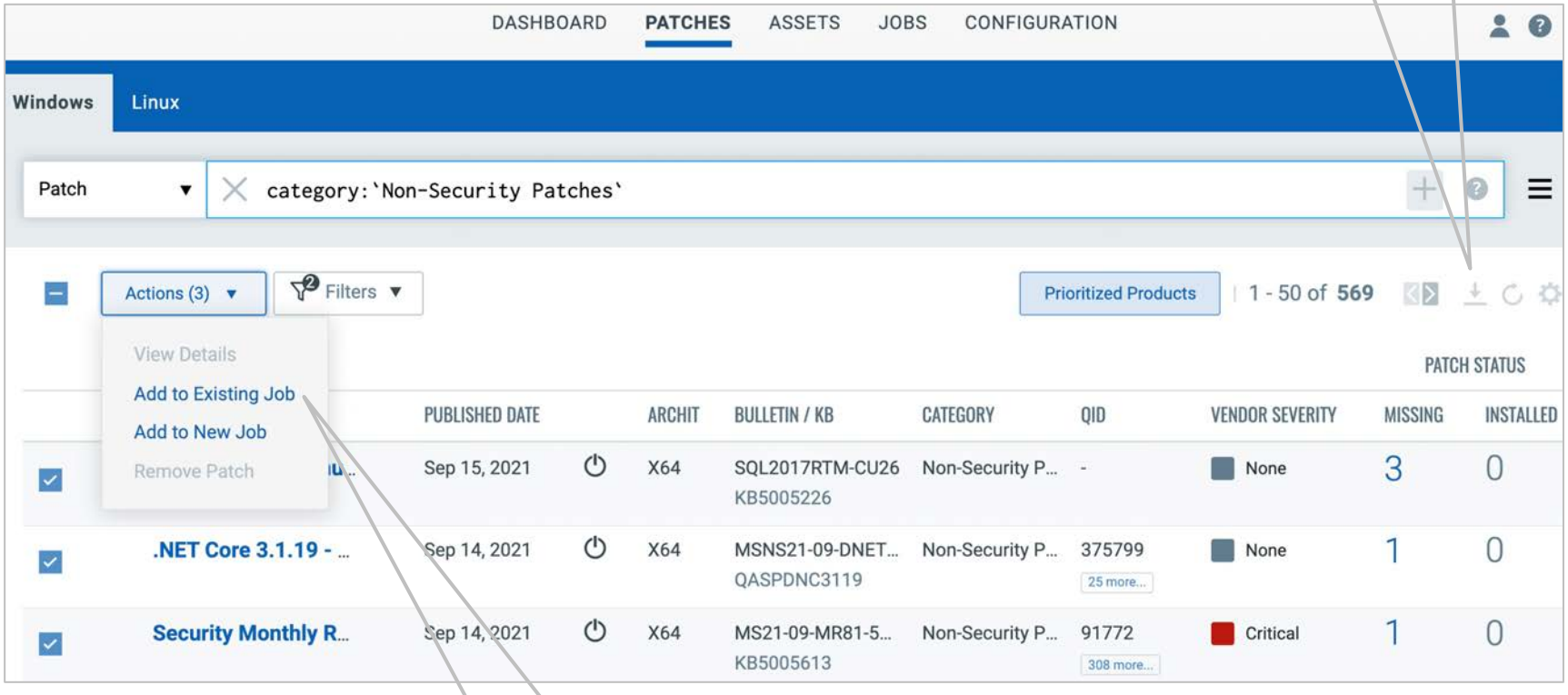
Lab Tutorial 5

Uninstall Job – Page 16

Patch Catalog

Qualys.

Patches

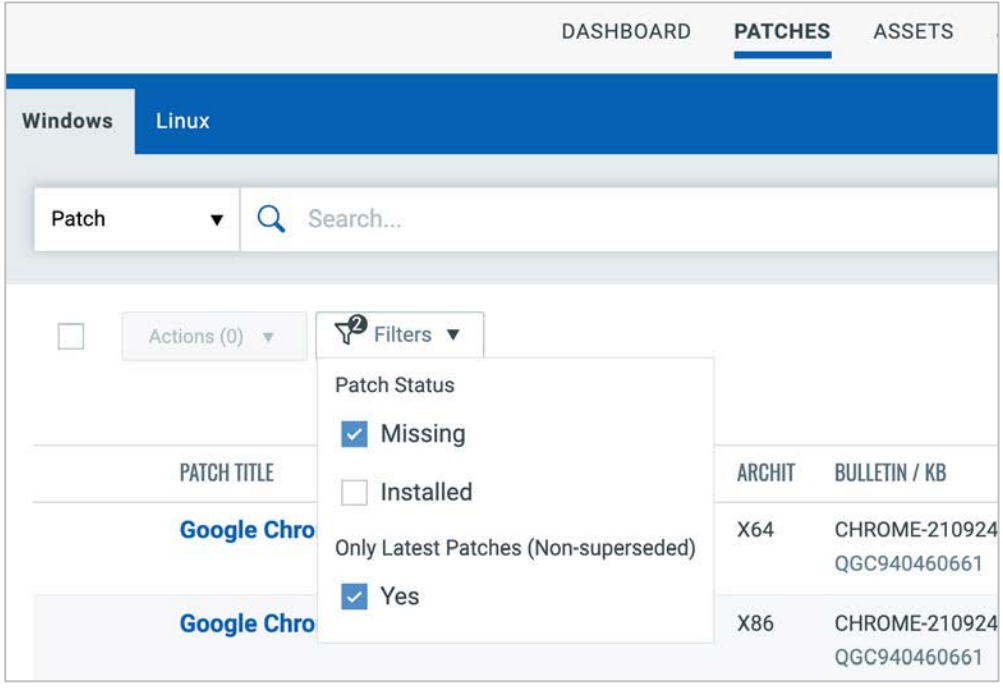


Download list of patches

Create patch job from the “Patches” tab

Qualys.

Catalog's Default Display Filters



Default view shows:

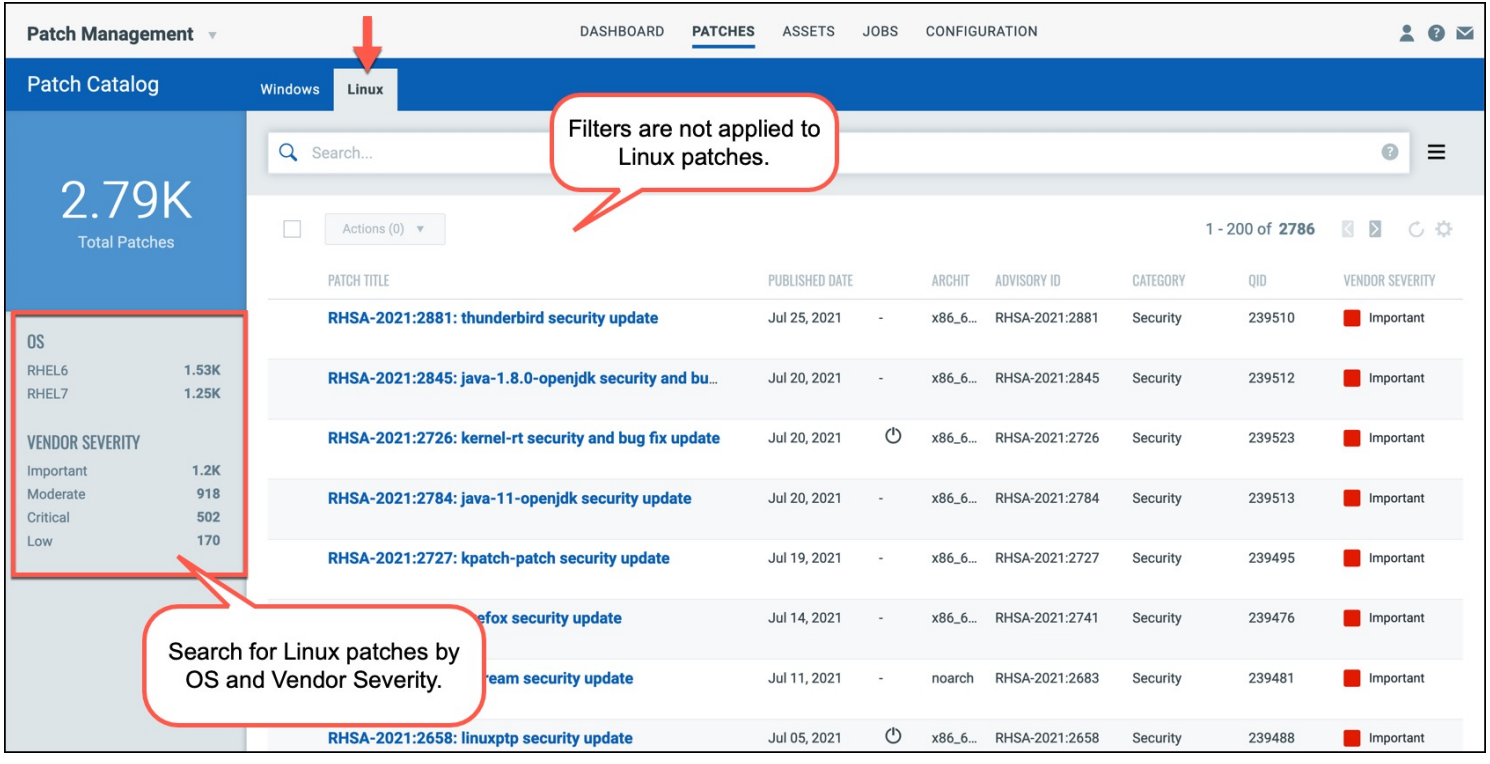
- Missing patches
- Non-superseded patches

Use filters to view:

- Missing and installed patches
- Superseded patches

Qualys.

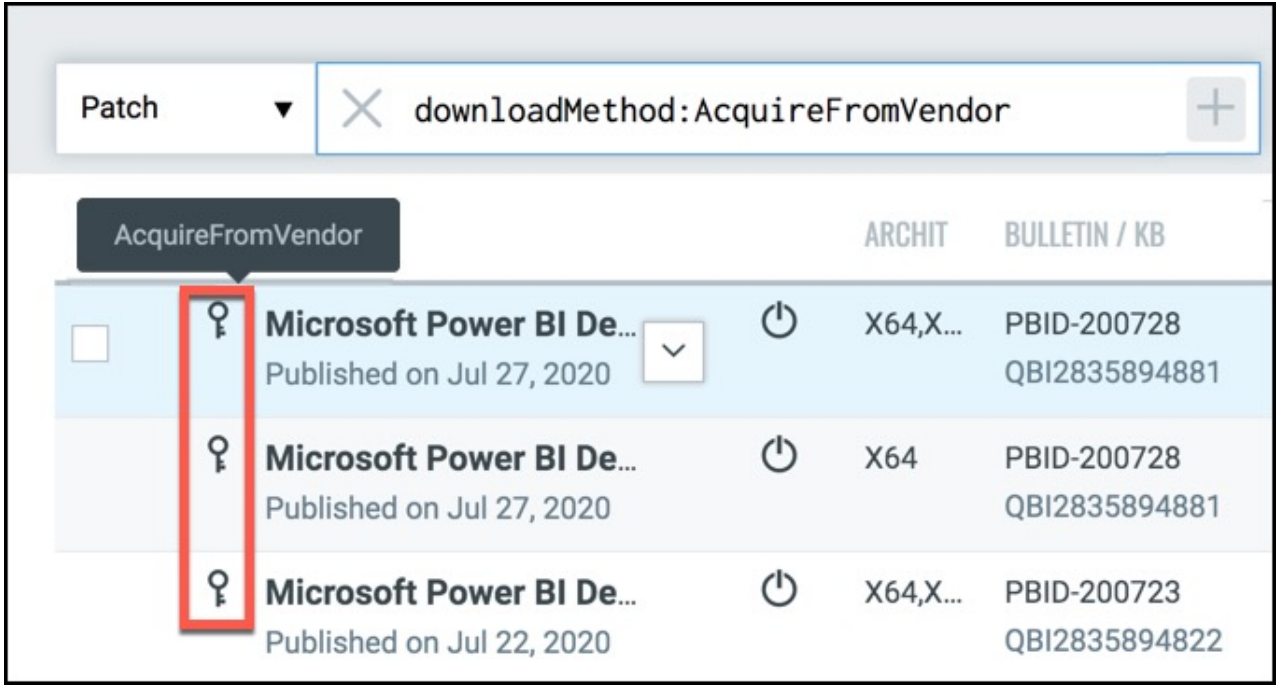
Linux Patches



Default filters are NOT applied when viewing Linux patches.

Qualys.

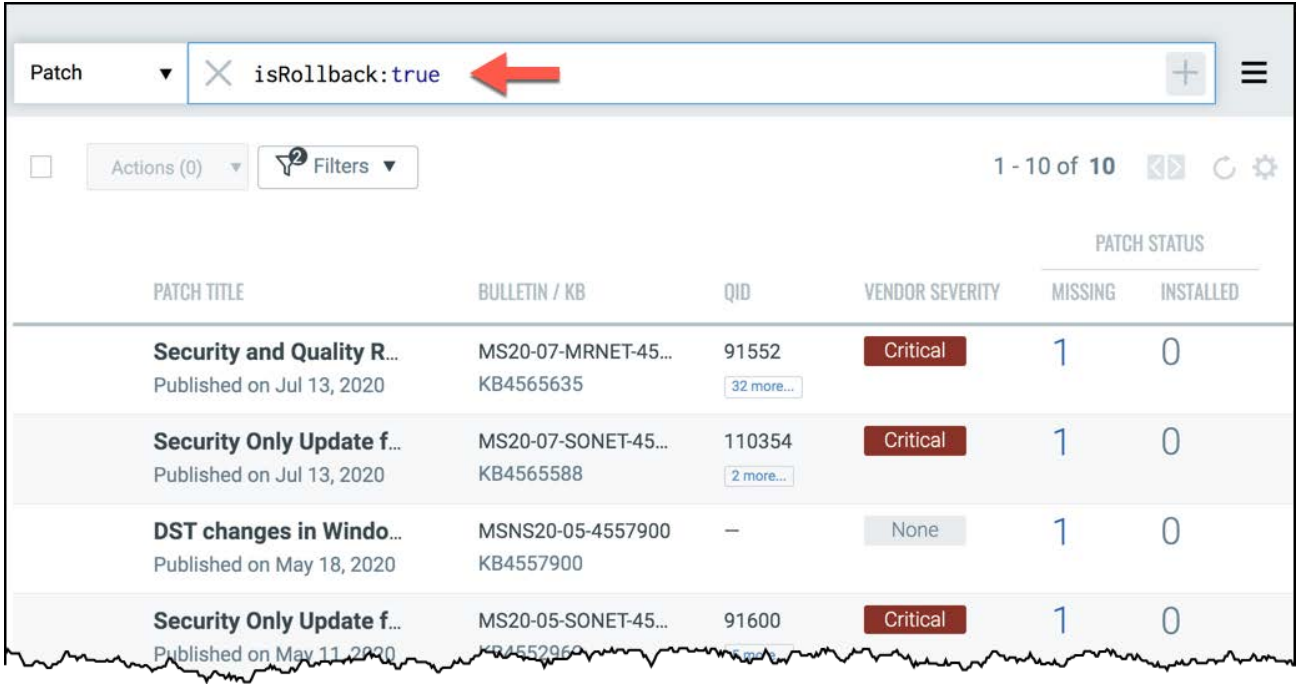
Acquire From Vendor



- Patches identified with the “key-shaped” icon, cannot be downloaded by Qualys’ Cloud Agent.

Qualys.

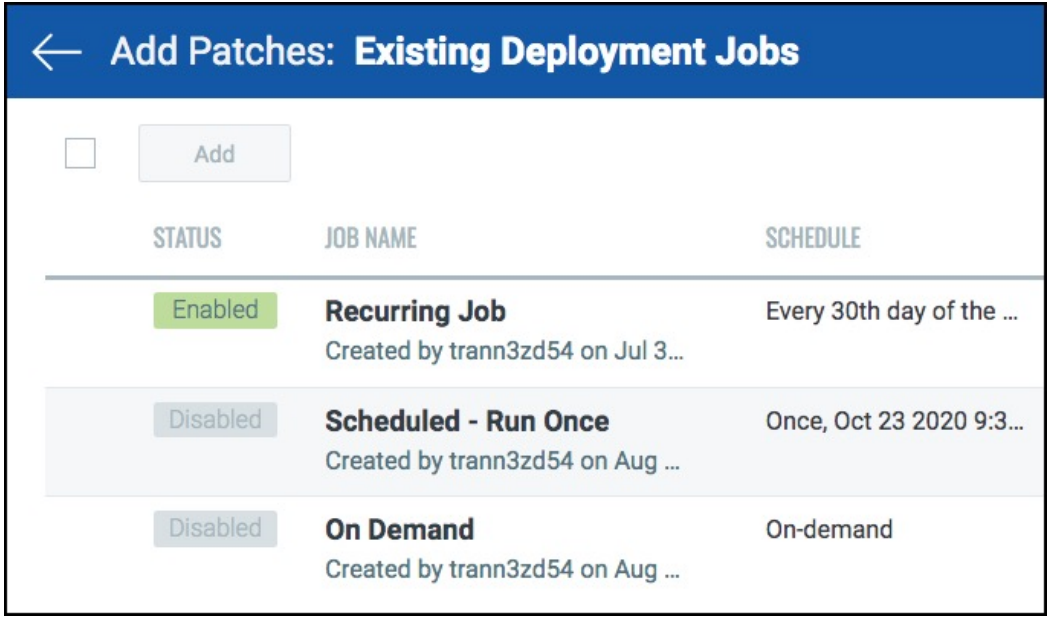
Uninstall or “Rollback” Patches




```
isRollback:true  /* patches that can be uninstalled */
```


Qualys.

Add Patches to Existing Jobs



- Additional patches can be added to any deployment job, before it is enabled
- Additional patches can be added to a “recurring” job, both before and after it is enabled.

Qualys.

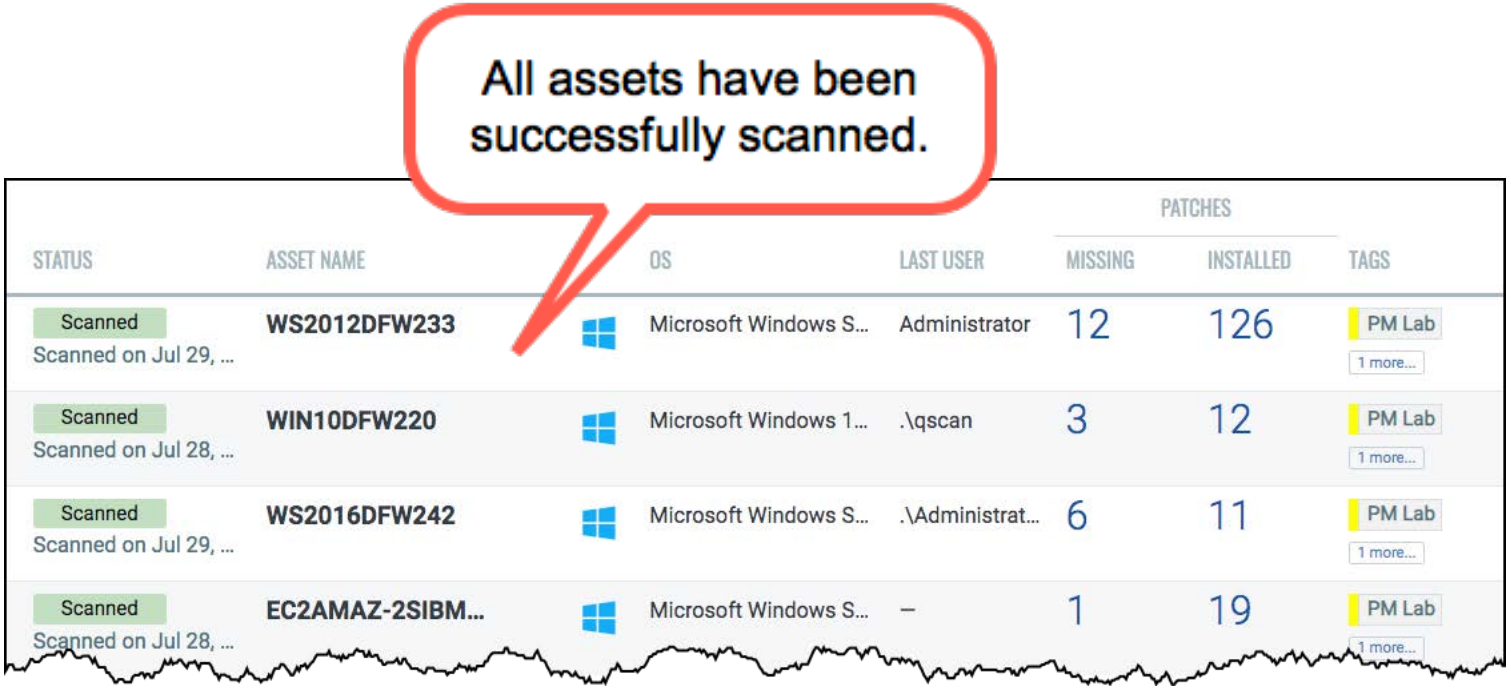
Lab Tutorial 6

Patch Catalog – Page 18

Assets

Qualys.

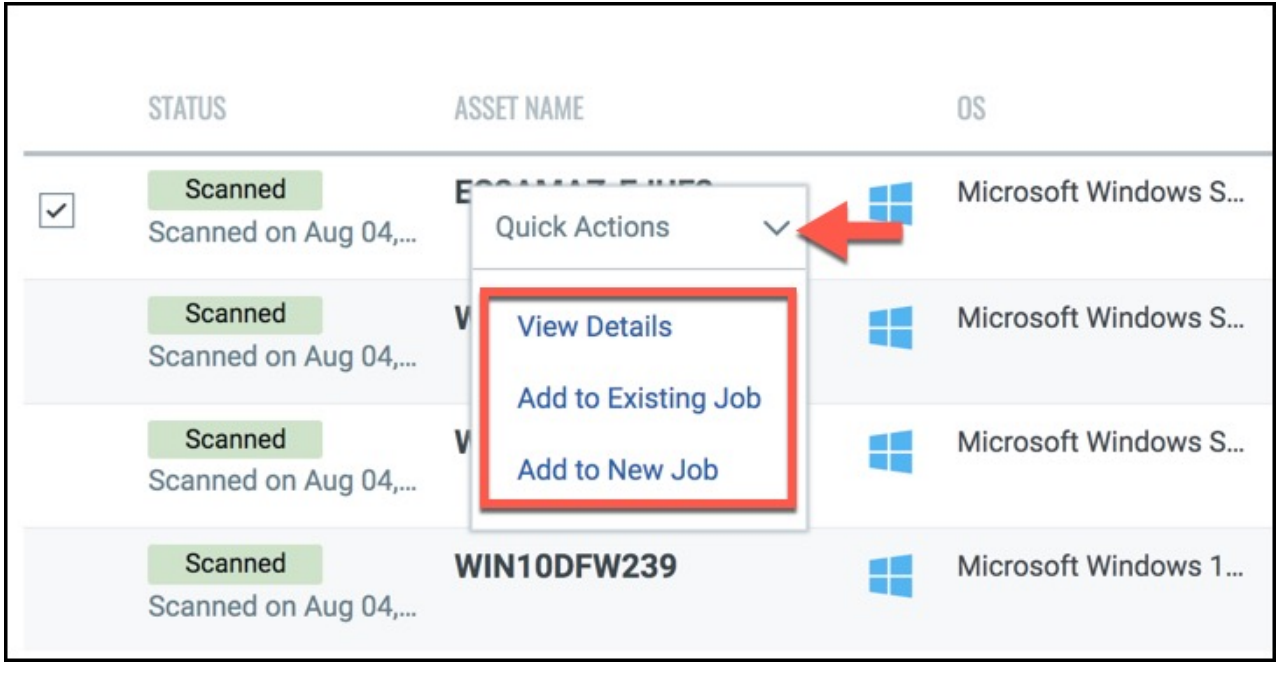
PM Assets



- Displays host assets with the PM module activated.
- A successful assessment scan will also display the number of MISSING and INSTALLED patches.

Qualys.

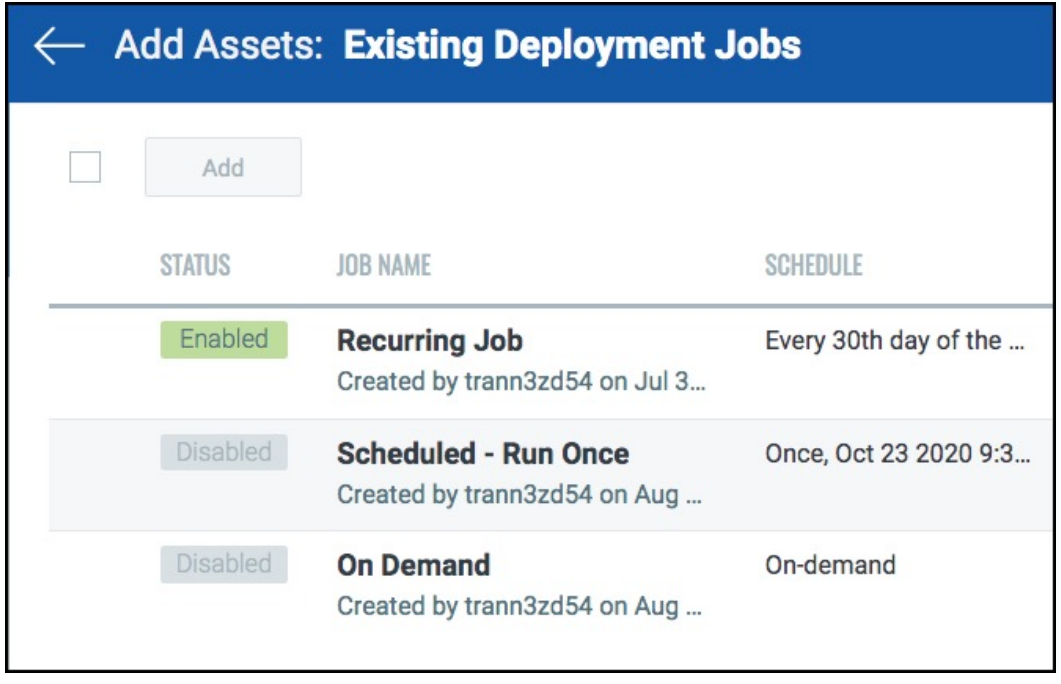
Quick Actions



- Use the “Quick Actions menu to view asset details, add assets to an existing job, or add assets to a new job.

Qualys.

Add Assets to Existing Jobs



- Additional assets can be added to any deployment job, before it is enabled
- Additional assets can be added to a “recurring” job, both before and after it is enabled.

Qualys.

Lab Tutorial 7

Assets – Page 20

Training Survey and Certification Exam

Training Survey → https://forms.office.com/r/rsy0Aja6Xz

Certification Exam → https://qualys.com/learning

Qualys.

PM Certification Exam

Participants in this training course have the option to take the PM Certification Exam:

- 30 multiple choice questions.
- Answer 75% of the questions correctly to receive a passing score.
- Candidates will receive 5 attempts to pass the exam.
- You may use the PM presentation slides and lab tutorial supplement to help you answer the exam questions.
- You may also use the “Help” menu (in the Qualys UI) to answer exam questions.

Qualys.

Qualys®

Thank You

training@qualys.com