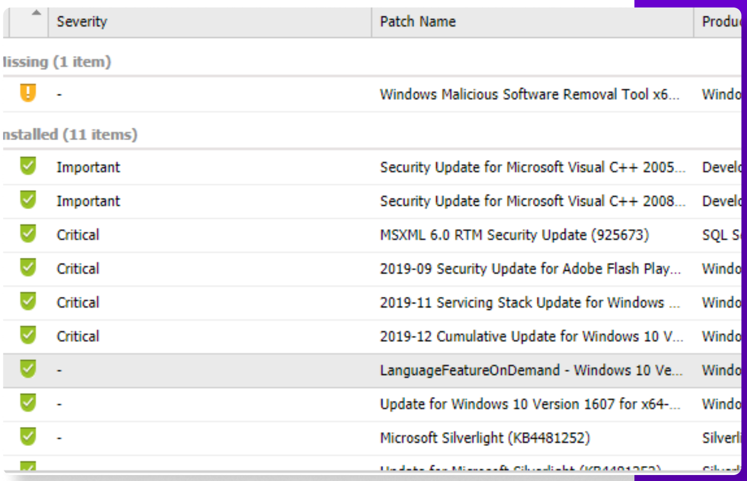
N-ABLE™ FEATURE SHEET

Patch Management

A feature available with N-able RMM



	Severity	Patch Name	Produ
lissing (1 item)			
!	-	Windows Malicious Software Removal Tool x6...	Windo
nstalled (11 items)			
✓	Important	Security Update for Microsoft Visual C++ 2005...	Develo
✓	Important	Security Update for Microsoft Visual C++ 2008...	Develo
✓	Critical	MSXML 6.0 RTM Security Update (925673)	SQL S
✓	Critical	2019-09 Security Update for Adobe Flash Play...	Windo
✓	Critical	2019-11 Servicing Stack Update for Windows ...	Windo
✓	Critical	2019-12 Cumulative Update for Windows 10 V...	Windo
✓	-	LanguageFeatureOnDemand - Windows 10 Ve...	Windo
✓	-	Update for Windows 10 Version 1607 for x64-...	Windo
✓	-	Microsoft Silverlight (KB4481252)	Silverl
✓		Update for Microsoft Silverlight (KB4481252)	Silverl

Fast, Safe, and Seamless Patching

MSPs know patch management is at the core of any effective, proactive cybersecurity policy. Though necessary, patching workstations and servers manually or with the wrong tool can quickly become complex—and possibly expose clients' systems to sluggish performance and serious security risks.

N-able™ RMM streamlines patch management by providing granular control over patching policies through a single, user-friendly console. Whether automating the entire process, customizing patches for certain devices, or manually approving or denying patches, RMM puts techs in the driver's seat for fast, safe patching.

More control from a single console

- **Easy-to-use console—**Complete patch management in one user-friendly interface.
- **Automation—**Auto-approve patches when they become available, so end-user devices stay safe and up-to-date.
- **Scheduling—**Set patching windows to update software without disrupting employees during times of high productivity.
- **Customizable policies—**Apply custom settings to individual devices, clients, or sites as needed.
- **Visibility—**View all patch details in "Management Workflow" window, including severity and current and new status—even filter by device type.

Update and protect more software

- **Patches for most business software—**Third-party patching support for the most common application families, including Apple®, Google®, Java®, Adobe®, zip tools, and Skype®.
- **Support for Microsoft products—**Continuous updates for Microsoft Windows® (security only and feature upgrades). Approve and install Windows drivers in maintenance windows.
- **Support for macOS® devices—**We test and validate patches from Apple and 200+ other vendors before releasing them.
- **Extra security for commonly exploited programs—**The latest security patches for vulnerable programs, such as Adobe and Java.

Benefit from additional features

- **Streamlined patch approvals—**Approve patches in batch across sites, networks, servers, and workstations.
- **Patch roll-back—**Easily revoke Microsoft® patches on one or more devices at a time to limit the impact of a bad patch.
- **Automated pushes for disabled devices—**Never miss an update for any device that might be disabled during a standard patch management window.
- **Deep scans to find new vulnerabilities—**Use deep scans to uncover new sources of risk or inefficiency in your network.

Patches for popular software

Including, but not limited to:

- SQL Server®, Internet Explorer® and Windows OS, Java, Adobe, Zoom, Mozilla® Firefox®, Google Chrome™, Apple iTunes®, and Apple QuickTime®.

This document is provided for informational purposes only and should not be relied upon as legal advice. N-able makes no warranty, express or implied, or assumes any legal liability or responsibility for the information contained herein, including for the accuracy, completeness, or usefulness of any information contained herein.