

Patch Management

A critical component in maintaining systems integrity.

Network environments are dynamic, constantly changing, and systems integrity is not a static state.

Customer networks feature different versions of operating systems, different languages, different patch levels, different applications and may operate over different time zones, not to mention the ever-changing threat landscape.

Staying on top of the acquisition, testing, approval and application of patches is a daunting challenge.

When it comes to vulnerabilities in customer networks, it is no longer a question of **if** they will be exploited but **when**.

A Patch Management strategy informed through data, governed by a robust process, supported by automation gives you back the control you need to ensure the systems integrity of customer networks.

Benefits

Automation offers:

- **Patch Monitoring** - dashboards and reports keep you informed with real-time data
- **Management** - manage vulnerabilities through timely application of patches to Operating Systems and applications
- **Setup Wizard** - setup patch management with best practices quickly
- **Demonstrable compliance** - reporting and dashboards for audit purposes
- **Automation** - automated approvals lower the risk of vulnerabilities
- **Maximized uptime** - schedule patches for fastest install and lowest interruption



Introduction

The goal of patch management is to ensure a consistently configured environment that is secure against known vulnerabilities in terms of operating systems and application software.

The patch management process includes setup, acquiring, testing, approving and installing patches on managed devices to create and maintain required systems integrity and meet compliance requirements.

Setting up Patch Management

Initial setup of patch management is performed using a wizard. The wizard will present options and will configure patch management based on these options.

Once setup, the settings may be changed (if required) for synchronization intervals approval, storage location, scheduling, automatic install, machine reboot, etc. to customize the process to your exact needs.

Acquiring Patches

Managed Workplace downloads patches specifically based on OS version/language, and applications for the devices under patch management.

Once downloaded, patches may be optionally stored locally for further distribution.

Storing patches locally on the Onsite Manager requires additional disk space but offers time saving and reduced internet bandwidth usage versus a distribution from the patch author(s) for each machine.

Installing Patches

For additional security, before patches can be installed they must be approved, either manually or automatically. Approval may be by an individual patch basis, by device, or by approval group.

Approval Groups

Approval groups are groups of devices built for ease of approval and management. During setup, devices are placed in pre-existing default groups. New groups can be created to handle different scenarios and devices can be moved between groups easily.

For example, an approval group could be used to differentiate between user workstations based on geographic location.

Patches could be scheduled by group for application immediately after working hours to minimize disruption.

Devices may be added manually to groups or through rules-based auto-grouping.

Manual Patch Approval

Manual approval allows you to test patches and approve them before they are installed.

Automating the Approval

Automating approval using approval groups presents a great deal of flexibility in automatically applying patches based on a patch policy.

Device Patch Policies

A device patch policy defines specific options regarding patch application. These policies may be applied per device, or against an approval group. Options include the ability to;

- Download only,
- Download & auto-install, or
- Immediate install (for updates that do not require restart or interrupt Windows services).



Scheduling Patches

Scheduling of patch application must be tightly controlled to ensure the smallest gap between patch availability and patch application.

Managed Workplace provides a variety of scheduling options. For example, the ability to tightly couple with the Microsoft® 'Patch Tuesday' & schedule patches for '2nd Saturday of the month' to minimize this gap.

Scheduling also specifies times that are convenient to the customer.

Careful scheduling allows the balance between customer demand for high availability and protection against vulnerabilities to be achieved.

Ensuring Patch Compliance

On a regular basis, individual machines communicate patch status back to the Onsite Manager.

A single dashboard shows the patch status of each and every device under management.

This display of information shows which patches are needed, which ones have been installed, and which patches may have failed.

Patch Compliance Reporting

Managed Workplace includes several reports that drive informed decisions. The Patch Status report and the Managed Device report are two particularly useful reports to provide information.

When used together, they inform and prioritize tactics supporting the patch strategy as well as providing the necessary documentation required by auditors seeking confirmation of regulatory and/or governmental compliance.



Overview	Installed	Needed	Failed	Last Updated	Total Devices
Patch					
Microsoft Security Update for Internet Explorer 10 for Windows 7 Service Pack 1 for x64-based Systems (KB2977621)					Not Approved
Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2994944)					Not Approved
Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x86-based Systems (KB2972121)					Not Approved
Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2977121)					Not Approved
Security Update for Microsoft .NET Framework 3.5.1 on Windows 7, Vista, Server 2008, Server 2008 R2 and (KB2994944)					Not Approved
Security Update for Microsoft .NET Framework 4.5, 4.5.1 and 4.5.2 on Windows 7, Vista, Server 2008, Server 2008 R2 x64 (KB2972110)					Not Approved
Security Update for Windows 7 for x64-based Systems (KB2972110)					Not Approved

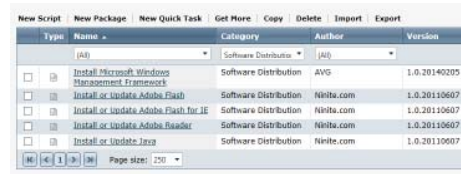
Managed Device Report

Application software updates

In Managed Workplace, patch management is not limited to Windows and Microsoft applications.

Patch management for non-Microsoft® software and applications are handled directly through a set of specific automation scripts.

A variety of scripts are provided in the Automation Library to handle a wide range of 3rd party applications.



Type	Name	Category	Author	Version
(All)		Software Distribution	(All)	
<input type="checkbox"/>	Install Microsoft Windows Management Framework	Software Distribution	AVG	1.0.20140205
<input type="checkbox"/>	Install or Update Adobe Flash	Software Distribution	Ninite.com	1.0.20110607
<input type="checkbox"/>	Install or Update Adobe Flash for IE	Software Distribution	Ninite.com	1.0.20110607
<input type="checkbox"/>	Install or Update Adobe Reader	Software Distribution	Ninite.com	1.0.20110607
<input type="checkbox"/>	Install or Update Java	Software Distribution	Ninite.com	1.0.20110607

Sample software update scripts

Patch Now

Despite the best planning and scheduling, patches can often be released with little or no notice and so it is important that device or sets of devices can be patched immediately, if required.

The 'Patch Now' feature, accessed directly from the Managed Device Report, provides the ability to patch a device or approval group on demand. This ensures that issues such as critical vulnerabilities are addressed quickly.

Summary

Managed Workplace Patch Management combines the information, the flexibility, and the automation you need to stay in control and to ensure the systems integrity of customer networks.



About AVG Technologies (NYSE: AVG)

AVG is the online security company providing leading software and services to secure devices, data and people. AVG has over 187 million active users, as of March 31, 2014, using AVG's products and services including Internet security, performance optimization, and personal privacy and identity protection. By choosing AVG's products, users become part of a trusted global community that engages directly with AVG to provide feedback and offer mutual support to other customers.

Keep in touch with AVG



BLOGS

United States:

AVG Technologies USA, Inc.
2105 Northwest Blvd.
Newton, NC 28658,
U.S.A.

✉ casales@avg.com
☎ 1-855-254-6987

United Kingdom & Ireland:

AVG Technologies UK Ltd
Olympic House,
995 Doddington Road
Lincoln, LN6 3SE
United Kingdom

✉ ashley@avg.com
☎ +44(0)1522 803260

Canada:

AVG Technologies Canada Inc.
309 Legget Drive,
Ottawa, ON, K2K 3A3,
Canada.

✉ casales@avg.com
☎ 1-855-254-6987

Australia & New Zealand:

AVG Technologies AU Pty Ltd
47 A Wangara Rd
Cheltenham Victoria 3192
Australia

✉ resellerau@avg.com
☎ Australia: 1800 230 463
☎ New Zealand: 0800 452 980

Rest of World:

AVG Technologies CZ, s.r.o.
Karla Engliš 3219/4
Praha, 150 00,
Czech Republic

✉ reseller@avg.com
☎ +420 549 524 011

Head Office:

AVG Technologies, N.V.
Gatwickstraat 9 -39
1043 GL Amsterdam
Netherlands



AVG Business Managed Workplace®