Managing Patches Using SanerNow
4.0 User Guide
Patch Management

Applying security patches is the primary method for eliminating vulnerabilities in software. Patch management involves deciding what patches should be applied, when they should be applied, and applying the patches.

SanerNow provides access to the latest vendor patches that are tested by experts. With its capability to identify vulnerabilities and map appropriate patches to remove vulnerabilities, SanerNow automates the process of security patch management and keeps endpoint systems up to date. SanerNow also provides crucial information on the severity of detected vulnerabilities, which is useful in deciding whether or not to apply patches.

To access the Patch Management tool:
1. Logon to SanerNow using your SanerNow credentials.
2. Select an account to manage by clicking the icon at the upper left corner of the window. A dashboard with the summary view of the account is displayed.
3. Click the SanerNow icon on the header. Click the Patch Management icon. The Patch Management dashboard is displayed, which provides an overview of missing, critical, and installed patches. And it helps you take action to install patches to remediate vulnerabilities, update endpoint configurations, or roll back patches.

Missing Patches

This pane displays missing patches for assets installed on systems. It highlights the level of risk due to the missing patch, the size, date and vendor who publishes the patch, and whether a reboot will be required to apply the patch. It also shows the number of affected hosts and by clicking you will see the affected hosts.

Click the expand icon to install the missing patches. The Missing Patches page is displayed. You can filter the list of patches by groups of devices to easily traverse the list, or you can search for the required device or group.

You can remediate missing patches in two ways:

- As a one-time task to apply patches on a device or devices. In other words, you create a Job every time you need to apply missing patches.
- As an automated task scheduled to apply any missing patches discovered by the last scan executed by the Saner Agent. In other words, you can create a scheduled task that will run according to defined parameters whenever missing patches need to be applied.

To install missing patches a single time
1. Select the patches you want to install. Click **Fix Selected Patches**. The Create Patching Task dialog is displayed.

![Create Patching Task dialog](image)

Click to create a job to apply missing patches

2. Specify a job name and select whether SanerNow should auto reboot the systems after patching.
3. Schedule the job to take place immediately or after a scan and set the time counter accordingly in the **Remediation Time Frame** boxes. You can also choose to set the job to execute on a different date.
4. Click **Create Job**.

**To install missing patches using an automated task**

1. In the Missing Patches page shown below, click Automation. The Schedule a Task page is displayed.
2. Select the device groups that you want to install patches for. Click the arrow to add the groups or devices to the Vulnerable and Non-Vulnerable assets pane.

3. Select one of the following from the Automatically Remediate drop-down:
   - All vulnerable and non-compliant assets
   - Selected vulnerable and non-compliant assets – SanerNow will remediate only the assets you have selected.
   - All vulnerable assets
   - All non-compliant assets

4. Click Create Scheduled Task. The Create Automation Task dialog is displayed.
5. Specify a task name and description and select whether SanerNow should auto reboot the systems after patching.

6. Schedule the task to take place after a scan and set the time counter accordingly in the Remediation Time Frame boxes. You can also choose to set the task to execute on a different date, either weekly, monthly or daily. If weekly, specify the days and time. If monthly, specify the dates, and time.

7. Click Schedule a Task.

SanerNow supports patch management for Windows, Linux and the Mac operating systems, and for third-party applications.

Operating System Patches

1. Microsoft Updates

Patch Management for Microsoft updates works in two ways:

WSUS Server

If Windows update is configured to contact the WSUS Server, the Saner agent directly contacts the WSUS Server to get the latest available patches. Otherwise, it will contact the Microsoft Update Server. To configure ‘Windows Update’ to contact the WSUS Server, visit https://thwack.solarwinds.com/community/application-and-server_tht/patchzone/blog/2013/05/02/configuring-your-first-wsus-client.

Default Microsoft Update Server

If Windows update is configured to contact the Microsoft Update Server, the Saner agent directly contacts the Microsoft Update Server to get the latest available patches.

2. Linux Machines

For RPM Machines

The Saner solution uses the YUM repository to install RPM package updates, which contacts the respective update server to get the latest patches.

For DPKG Machines

SanerNow uses apt-get package which is a default package present in dpkg machines. The agent contacts the respective update server to get the latest patches.
### 3. Mac OS X Packages

SanerNow uses the `softwareupdate` command to update OS X packages. The agent contacts the MAC OS X Update Server.

#### Third-party Application Patches

The Saner solution supports the following 85 applications for Patch Management. The application list is constantly updated.

- All Microsoft products
- All Linux distros packages
- All Mac OS X packages
- Adobe Dreamweaver
- Adobe InDesign
- Adobe JRun
- Adobe PageMaker
- Adobe Photoshop
- Adobe RoboHelp
- Adobe Presenter
- Adobe FMS
- Adobe AIR
- Adobe Flash Player
- Adobe Captivate
- Adobe Shockwave Player
- Adobe Reader
- Adobe Acrobat
- Adobe Illustrator
- Adobe Digital Edition
- AOL Instant Messenger
- Apache HTTP Server
- Apache Tomcat
- Apache Subversion
- Apple iTunes
- Apple QuickTime
- Apple Safari
- Apple Xcode
- BlackBerry Desktop
- Elasticsearch
- Enterprise Applications, Servers - Vulnerability Content
- Foxit Reader
- gZip
- Google Chrome
- Mozilla FireFox
- Mozilla SeaMonkey
- Mozilla Thunderbird
- MySQL
- GhostScript
- Google Desktop
- Google Earth
- Google Picasa
- Google SketchUp
- GPG4Win
- IBM DB2
- IBM Lotus Domino
- IBM Lotus Notes
- OpenSSH
- OpenSSL
- Open JDK
- Open Office
- OpenVPN Client
- Opera
- Oracle Application Server
- Oracle WebLogic Server
- Oracle Database Server
- Pidgin
- PowerZip
- Putty
- Perl (Active Perl)
- PHP
- PGP Desktop
- Python
- RealPlayer
- RealVNC
- Ruby
- Skype
- Sun Java JDK
- Sun VirtualBox
- VMware Player
- VMware Fusion
- VMware Horizontal Client
- VMware ESXi
- VMware View
- VMware Workstation
- VMware Movie Decoder
- VLC Media Player
- Win amp
- WinRAR
- WinZip
- Wireshark
- Adobe Reader DC classic
- Adobe Reader DC continuous
- Adobe Acrobat DC Classic
- Adobe Acrobat DC continuous

### Most Critical Patches

This pane highlights the patches that are most critical to the security of the system and organization, so that you can
prioritize patching.

Click the Expand icon to start patching. The most Critical Patches page is displayed, with information on the exploit kits that are available for the corresponding vulnerability.

To apply critical patches

1. Select the assets you want to patch and click **Fix Selected Patches**. The Create Patching Task dialog is displayed.
2. Specify a job name and select whether SanerNow should auto reboot the systems after patching.
3. Schedule the job to take place immediately or after a scan and set the time counter accordingly in the **Remediation Time Frame**. You can also choose to set the job to execute on a different date.
4. Click **Create Job**.

**Patch by Operating System**

This pane shows the distribution of missing patches based on the operating system; it allows you to see which operating systems in your organization have the largest number of missing patches.

**Patch by Vendor**

This pane shows the patches categorized by the vendor, allowing you to understand which assets or vendors have
the most updates.

**Patch by Criticality**

This pane shows the patches by their criticality.

**Patch Aging**

This pane shows the number of days since a patch has been available but not applied.

**Patch Impact**

This pane highlights the number of vulnerabilities that are removed by applying patches. This helps prioritize patching based on factors such as the vulnerability count that is acceptable, security audits, safety and criticality of the unpatched systems, etc.
Configuration Impact

This pane shows the patches that should be applied to fix system configuration issues.

Missing Configurations

This pane shows assets that require an update or patch, the level of risk, the hosts or devices that need the update or patch, and other related details.

You can remediate configuration issues in two ways:

- As a one-time task, to apply configuration changes on a device or devices. In other words, you must create a Job every time you need to apply configuration changes.
- As an automated task, scheduled to apply configuration changes discovered by the last scan executed by the
SanerNow Agent. In other words, you can create a scheduled task that will run according to defined parameters whenever configuration changes need to be applied.

To install configuration changes a single time

1. Select the configuration patches you want to install. Click **Fix Selected Patches**. The Create Patching Task dialog is displayed.

2. Specify a job name and select whether SanerNow should auto reboot the systems after patching.
3. Schedule the job to take place immediately or after a scan and set the time counter accordingly in the **Remediation Time Frame** boxes. You can also choose to set the job to execute on a different date.
4. Click **Create Job**.

To install missing patches using an automated task

1. In the Missing Patches page shown below, click Automation. The Schedule a Task page is displayed.
2. Select the device groups that you want to install patches for. Click the arrow to add the groups or devices to the Vulnerable and Non-Vulnerable assets pane.

3. Select one of the following from the Automatically Remediate drop-down:
   - All vulnerable and non-compliant assets
   - Selected vulnerable and non-compliant assets – SanerNow will remediate only the assets you have selected.
   - All vulnerable assets
   - All non-compliant assets

4. Click Create Scheduled Task. The Create Automation Task dialog is displayed.
5. Specify a task name and description and select whether SanerNow should auto reboot the systems after patching.

6. Schedule the task to take place after a scan and set the time counter accordingly in the Remediation Time Frame boxes. You can also choose to set the task to execute on a different date, either weekly, monthly or daily. If weekly, specify the days and time. If monthly, specify the dates, and time.

7. Click Schedule a Task.

**Patches Installed Over Time**

This pane shows the number of patches that have been installed over time, so that the organization has a patch history that it can refer to, to understand its security health and plan its actions.

**Installed Patches**

This pane shows a list of patches that have been applied to assets, along with the installation date, the size of the patch, the rollback status, and the system that has the asset.

Click the expand icon if you want to rollback any patches. The Installed Patches page is displayed. You can filter the list of installed patches by groups of devices to traverse the list easily, or you can search for the required device or group.
To Rollback Patches

1. Select the assets for which you want to rollback patching and click **Revert Selected Patches**.

2. Specify a job name and select whether SanerNow should auto reboot the systems after rolling back the patches.

3. Specify whether you want the job done immediately or after a scan and set the time counter accordingly. You can also choose to set the job to execute on a different date.

4. Click **Create Rollback Task**.

Reason for Failure

Sometimes during patch management, patches may not be successfully installed for various reasons. This pane shows the number of hosts on which the patch has failed, and categorizes the failed patches under remediation errors, application errors, device errors, download errors, etc. Click the host number or name to see more detail, such as which job failed, or which patch was not installed. For an exhaustive list of errors, see Error! Reference source not found..
Job Status Summary

This pane shows the status of all the patch installation or rollback jobs that were scheduled.

Click the Expand icon to see a list of all scheduled patch and rollback jobs. Click on any job to view the completion status of the job, or the job creation information.

You can scan devices manually at any time. As seen in the tasks above, once the scan is done and vulnerabilities are known, remediation is performed by creating a job for misconfigurations, critical updates, or installed patches. The remediation job includes vulnerable/non-compliant assets that can be applied to a set of groups. The remediation job can be executed immediately, can be scheduled or performed after the scheduled scan.

To Scan Devices Manually
1. Click Manage > Devices on the left pane.
2. Select device groups and click Scan Now.
Once the Remediation Job is executed, you can generate a patch report again after 20-30 minutes. Compare this report with the report generated prior to the remediation job to identify how many hosts were affected and how many hosts have been remediated successfully.

**Setting Alerts for Patch Management**

To stay on top of the patching tasks that are vital to maintaining security, you can set alerts.

**To Set Alerts for Patch Management**

1. Click Alerts > Patch Management.
2. Set the subscription status to On.
3. Specify the email address to which you want the alerts sent.
4. Specify which conditions you want to receive alerts for:
   - Patches - You can choose to receive alerts for important and critical patches, all missing patches, all critical patches only, or custom patches. If you choose custom, you must specify the custom values in the Custom Detection box.
   - Response fields – You can choose to receive alerts for all actions, or when actions on the endpoints pass, fail, or for a custom condition. If you choose custom, you must specify the custom values in the Custom Detection box.
5. Click Update to complete.

**Patch Report**

The patch report shows a summary of all the patch information such as the missing patches, the critical patches, etc.

**To generate a patch report**

- Click Reports > Patch Report.
To export the report to a PDF

- Click Export > PDF

To export the report and send it via email:

6. Click Export > Email.
7. Specify email addresses.

To Back Up Reports

The backup settings under Reports allow IT administrators to maintain a history of compliance in the organization. The backup time should be scheduled. The backup report can be scheduled to run automatically daily or weekly.

To configure backup settings for reports:

1. Click Reports on the left pane.
2. Click Patch Report.
3. Select Backup.
4. Specify the frequency of backup in the How Often drop-down. You can back up reports daily, or weekly. If you choose weekly, you can specify the days.
5. Specify the number of days that a backup should be maintained in the Keep Only the Latest box. Files older than the specified value will be deleted. You can maintain backups for a maximum of 30 days.
6. Specify the Backup Time, that is, the time when SanerNow will create an archive of the report. Specify Email addresses.
7. Click Save.
About Us

SecPod Technologies creates cutting edge products to ensure endpoint security. Founded in 2008 and headquartered in Bangalore with operations in USA, the company provides computer security software for proactively managing risks and threats to endpoint computers.

Contact Us

Web: www.secpod.com
Tel: +91-80-4121 4020 | +1-918-625-3023
Email: info@secpod.com

© SecPod Technologies 2018. All Rights Reserved.