

Managing Patches Using SanerNow

4.0 User Guide

Contents

PATCH MANAGEMENT	3
Missing Patches.....	3
<i>To install missing patches a single time</i>	<i>3</i>
<i>To install missing patches using an automated task.....</i>	<i>4</i>
Most Critical Patches	7
<i>To apply critical patches</i>	<i>8</i>
Patch by Operating System	8
Patch by Vendor.....	8
Patch by Criticality	9
Patch Aging	9
Patch Impact	9
Configuration Impact.....	10
Missing Configurations.....	10
<i>To install missing patches a single time</i>	<i>11</i>
<i>To install missing patches using an automated task.....</i>	<i>11</i>
Patches Installed Over Time	13
Installed Patches	13
<i>To Rollback Patches</i>	<i>14</i>
Reason for Failure	14
Job Status Summary.....	15
SETTING ALERTS FOR PATCH MANAGEMENT	16
To Set Alerts for Patch Management.....	16
PATCH REPORT	16
To generate a patch report	16
To Back Up Reports.....	17

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.

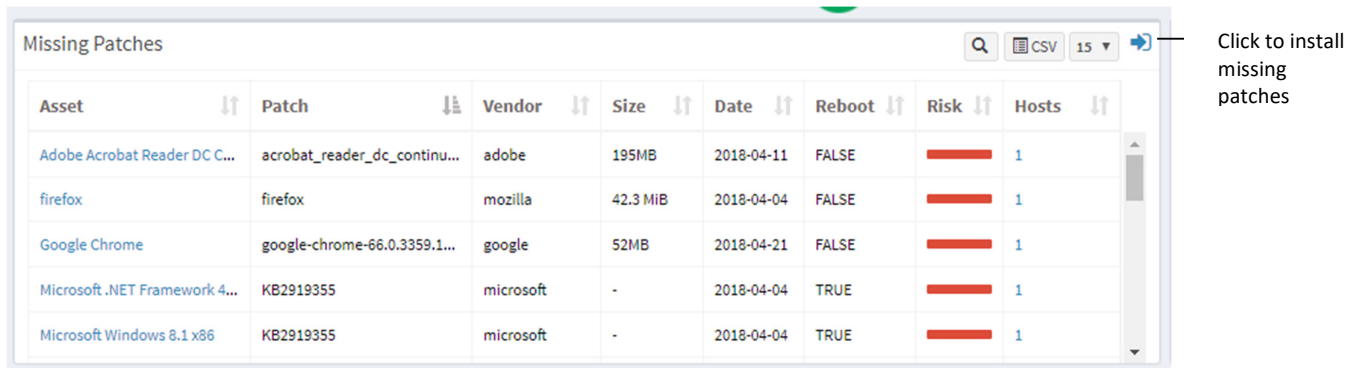
SanerNow provides access to the latest vendor patches that are tested by experts. With its capability to identify vulnerabilities and map appropriate patches to remove vulnerabilities, SanerNow automates the process of security patch management and keeps endpoint systems up to date. SanerNow also provides 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.



Asset	Patch	Vendor	Size	Date	Reboot	Risk	Hosts
Adobe Acrobat Reader DC C...	acrobat_reader_dc_continu...	adobe	195MB	2018-04-11	FALSE	<div style="width: 100%; height: 10px; background-color: red;"></div>	1
firefox	firefox	mozilla	42.3 MiB	2018-04-04	FALSE	<div style="width: 100%; height: 10px; background-color: red;"></div>	1
Google Chrome	google-chrome-66.0.3359.1...	google	52MB	2018-04-21	FALSE	<div style="width: 100%; height: 10px; background-color: red;"></div>	1
Microsoft .NET Framework 4...	KB2919355	microsoft	-	2018-04-04	TRUE	<div style="width: 100%; height: 10px; background-color: red;"></div>	1
Microsoft Windows 8.1 x86	KB2919355	microsoft	-	2018-04-04	TRUE	<div style="width: 100%; height: 10px; background-color: red;"></div>	1

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.

Asset	Patch	Vendor	Size	Date	Reboot	Hosts
Adobe Acrobat Reader DC Continuous	acrobat_reader_dc_continuous-1801120038-win3...	adobe	195MB	2018-04-11	FALSE	1
Google Chrome	google-chrome-66.0.3359.117-x64-deb.deb	google	52MB	2018-04-21	FALSE	1
Microsoft .NET Framework 3.5 sp1	2 patches	microsoft	-	2018-04-16	TRUE	1
Microsoft .NET Framework 4.5 SP2	4 patches	microsoft	-	2018-04-04	TRUE	1
Microsoft Edge	2 patches	microsoft	-	2018-04-16	TRUE	1
Microsoft Internet Explorer 11	KB4093109	microsoft	-	2018-04-16	TRUE	1
Microsoft Windows 8.1 x86	2 patches	microsoft	-	2018-04-04	TRUE	1
Microsoft XML Core Services 6.0	KB2919355	microsoft	-	2018-04-04	TRUE	1
VMware vSphere Client	VMware-viclient-all-6.0.0-7035-x86.exe	vmware	103MB	2018-04-04	FALSE	1
firefox	firefox	mozilla	42.3 MiB	2018-04-04	FALSE	1

Click to create a job to apply missing patches

Create Patching Task

Name:

Auto Reboot:

Schedule:

Remediation Time Frame: -

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.

Click automation to schedule a job

Asset	Patch	Vendor	Size	Date	Reboot	Hosts
Adobe Acrobat Reader DC Continuous	acrobat_reader_dc_continuous-1801120038-win3...	adobe	195MB	2018-04-11	FALSE	1
Google Chrome	google-chrome-66.0.3359.117-x64-deb.deb	google	52MB	2018-04-21	FALSE	1
Microsoft .NET Framework 3.5 sp1	2 patches ↓	microsoft	-	2018-04-16	TRUE	1
Microsoft .NET Framework 4.5 SP2	4 patches ↓	microsoft	-	2018-04-04	TRUE	1
Microsoft Edge	2 patches ↓	microsoft	-	2018-04-16	TRUE	1
Microsoft Internet Explorer 11	KB4093109	microsoft	-	2018-04-16	TRUE	1
Microsoft Windows 8.1 x86	2 patches ↓	microsoft	-	2018-04-04	TRUE	1
Microsoft XML Core Services 6.0	KB2919355	microsoft	-	2018-04-04	TRUE	1
VMware vSphere Client	VMware-vmiclient-all-6.0.0-7035-x86.exe	vmware	103MB	2018-04-04	FALSE	1
firefox	firefox	mozilla	42.3 MiB	2018-04-04	FALSE	1

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

The screenshot shows the 'Schedule a Task' interface. On the left, a 'Select Groups' list includes items like 'amazon linux', 'AV-Group', 'bk-test', 'centos', 'CONT-AUTOMATION-DNT-TOUCH', 'debian', 'Demo-group', 'mac os', 'MANISH', 'new-scan-sat', 'oracle linux', 'pk-mac', 'pk-windows7', 'preeti', 'red hat', 'rini-win10', 'sat-MAC', and 'sat-win-2012'. On the right, the 'Vulnerable and Non Vulnerable Assets' section shows a dropdown for 'Automatically remediate' set to 'Selected vulnerable and non-compliant assets'. Below this, a table lists assets with 'Include' and 'Exclude' checkboxes:

Asset	Include	Exclude
o2ps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
abrt	<input checked="" type="checkbox"/>	<input type="checkbox"/>
acpi-support	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Adobe Acrobat DC Continuous	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Adobe Acrobat Reader DC Continuous	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Adobe Flash Player	<input type="checkbox"/>	<input checked="" type="checkbox"/>

4. Click Create Scheduled Task. The Create Automation Task dialog is displayed.

The screenshot shows a 'Create Automation Task' dialog box with the following fields and options:

- Task Name:** Input field with placeholder 'name *'
- Task Description:** Input field with placeholder 'description *'
- Auto Reboot:** Toggle switch currently set to 'ON'
- Schedule:** Dropdown menu with 'custom' selected
- How often:** Dropdown menu with 'Weekly' selected
- Days of the week:** Dropdown menu with 'Select days' selected
- Remediation Time Frame:** Two sets of time selection boxes (HH, MM, AM) separated by a hyphen

Buttons at the bottom right: 'Schedule a Task' (green) and 'Cancel' (blue).

- Specify a task name and description and select whether SanerNow should auto reboot the systems after patching.
- 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.
- 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.

Asset	Patch	Hosts
Adobe Flash Player	flash-player-29.0.0.140_x64-...	5
Microsoft Internet Explorer 8	Vendor update	3
Microsoft Windows Server 2...	Vendor update	2
Mozilla Firefox ESR x86	firefox_esr-52.7.3-x86.exe	2
Microsoft Windows Server 2...	Vendor update	2

Click to create a job to apply critical patches

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.

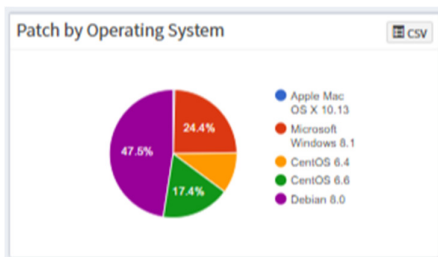
Asset	Patch	Vendor	Size	Date	Reboot	High Fidelity Attacks	Hosts
Microsoft Internet Explorer 11	KB4074598	microsoft	UNKNOWN	2018-03-07	TRUE	Obtain Exploit KILRIG Exploit Kit_Spartan Exploit Kit_Angler Exp...	1
Microsoft Windows 8.1 x86	5 patches	microsoft	325554	2018-03-07	TRUE	Obtain Exploit Kit_DoublePulsar BackDoor_Nebula Exploit Kit_N...	1

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

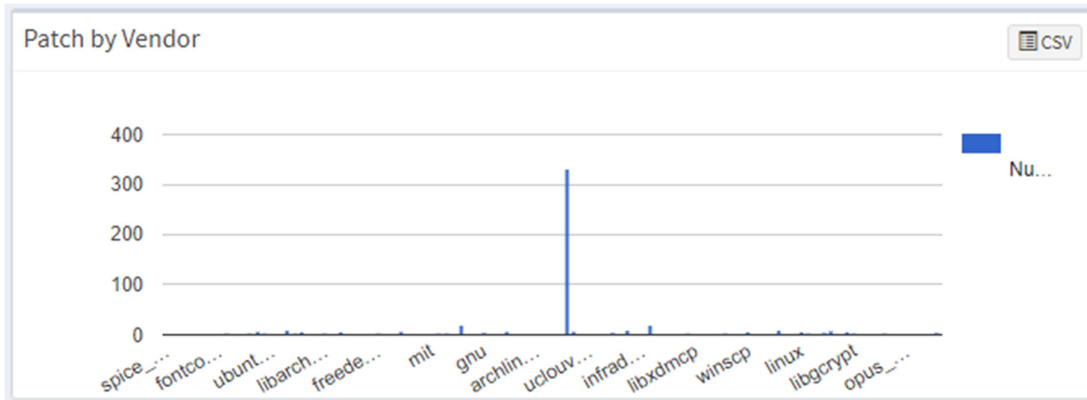
This pane shows the distribution of missing patches based on the operating system; it allows you to see which operating systems in your organization have the largest number of missing patches.



Patch by Vendor

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

the most updates.



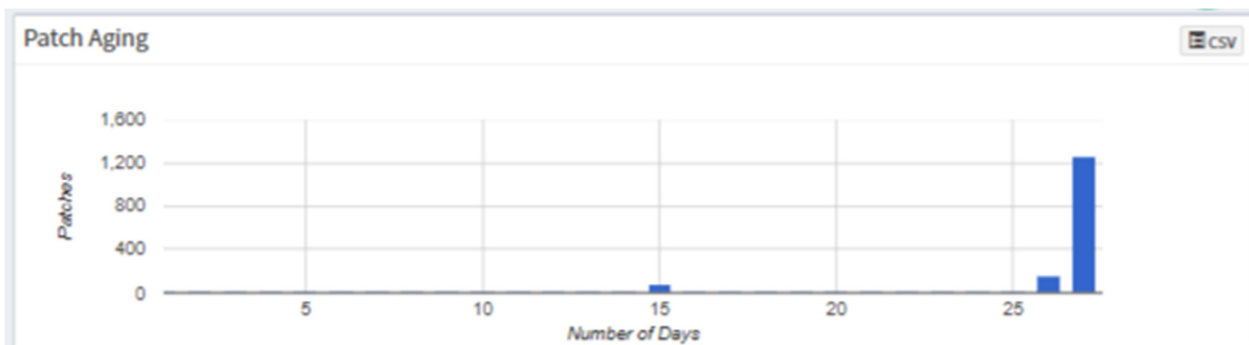
Patch by Criticality

This pane shows the patches by their criticality.



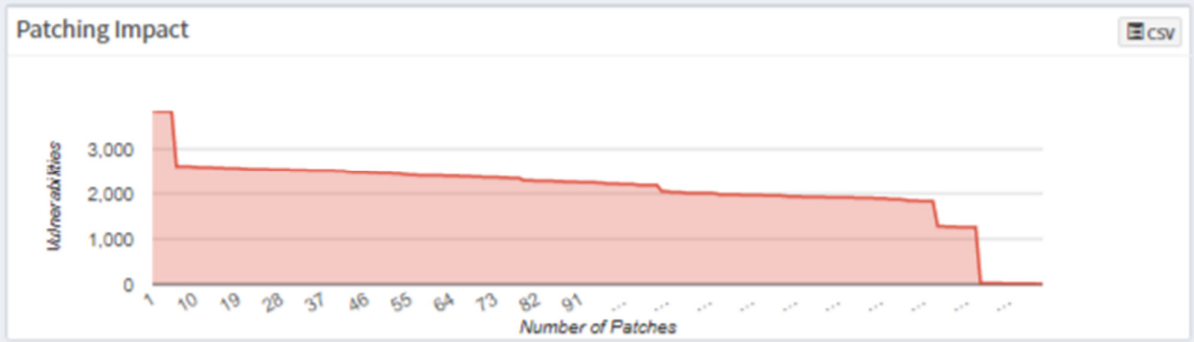
Patch Aging

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



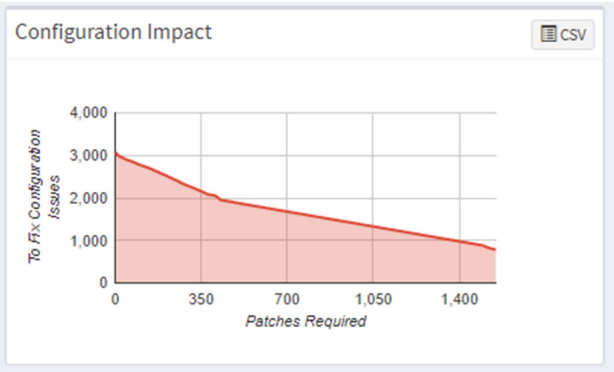
Patch Impact

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.

Asset	Patch	Vendor	Size	Date	Reboot	Risk	Hosts
Microsoft Windows 10	cce-41361-2-patch.inf	microsoft	4KB	2018-04-10	FALSE	High	1
Microsoft Windows 10	cce-42136-2-patch.inf	microsoft	4KB	2018-04-16	FALSE	High	1
Microsoft Windows 10	cce-41676-8-patch.inf	microsoft	4KB	2018-04-16	FALSE	High	1
Microsoft Windows 10	cce-42894-6-patch.inf	microsoft	4KB	2018-04-16	FALSE	High	1
Microsoft Windows 10	cce-43567-7-patch.inf	microsoft	4KB	2018-04-16	FALSE	High	1
Microsoft Windows 10	cce-42575-1-patch.inf	microsoft	4KB	2018-04-16	FALSE	High	1

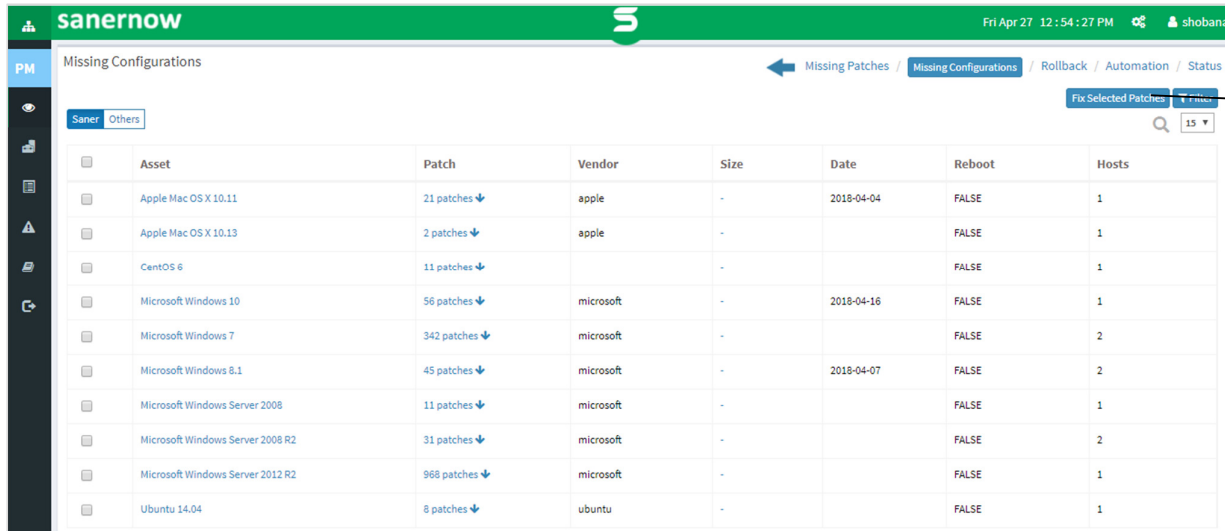
You can remediate configuration issues in two ways:

- 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

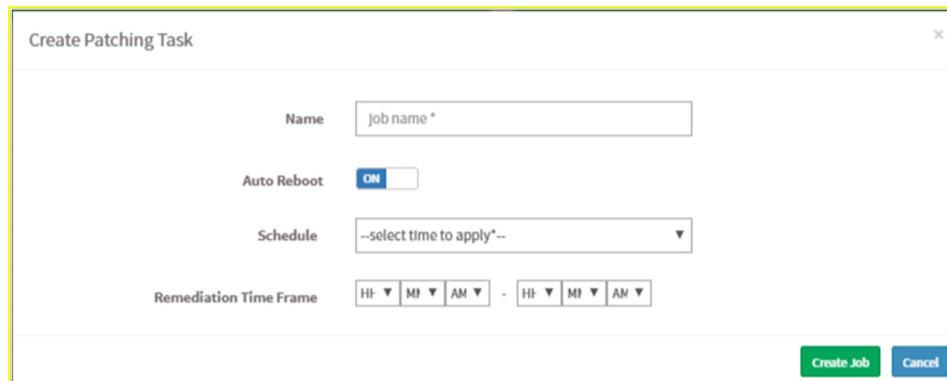
SanerNow Agent. In other words, you can create a scheduled task that will run according to defined parameters whenever configuration changes need to be applied.

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.

Click automation to schedule a job

Asset	Patch	Vendor	Size	Date	Reboot	Hosts
Adobe Acrobat Reader DC Continuous	acrobat_reader_dc_continuous-1801120038-win3...	adobe	195MB	2018-04-11	FALSE	1
Google Chrome	google-chrome-66.0.3359.117-x64-deb.deb	google	52MB	2018-04-21	FALSE	1
Microsoft .NET Framework 3.5 sp1	2 patches ↓	microsoft	-	2018-04-16	TRUE	1
Microsoft .NET Framework 4.5 SP2	4 patches ↓	microsoft	-	2018-04-04	TRUE	1
Microsoft Edge	2 patches ↓	microsoft	-	2018-04-16	TRUE	1
Microsoft Internet Explorer 11	KB4093109	microsoft	-	2018-04-16	TRUE	1
Microsoft Windows 8.1 x86	2 patches ↓	microsoft	-	2018-04-04	TRUE	1
Microsoft XML Core Services 6.0	KB2919355	microsoft	-	2018-04-04	TRUE	1
VMware vSphere Client	VMware-vclicent-all-6.0.0-7035-x86.exe	vmware	103MB	2018-04-04	FALSE	1
firefox	firefox	mozilla	42.3 MiB	2018-04-04	FALSE	1

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

The screenshot shows the 'Schedule a Task' interface. On the left, a 'Select Groups' list includes items like 'amazon linux', 'AV-Group', 'bk-test', 'centos', 'CONT-AUTOMATION-DNT-TOUCH', 'debian', 'Demo-group', 'mac os', 'MANISH', 'new-scan-sat', 'oracle linux', 'pk-mac', 'pk-windows7', 'preeti', 'red hat', 'rini-win10', 'sat-MAC', and 'sat-win-2012'. On the right, the 'Vulnerable and Non Vulnerable Assets' section shows a dropdown for 'Automatically remediate' set to 'Selected vulnerable and non-compliant assets'. Below this, a table lists assets with 'Include' and 'Exclude' checkboxes:

Asset	Include	Exclude
o2ps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
abrt	<input checked="" type="checkbox"/>	<input type="checkbox"/>
acpi-support	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Adobe Acrobat DC Continuous	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Adobe Acrobat Reader DC Continuous	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Adobe Flash Player	<input type="checkbox"/>	<input checked="" type="checkbox"/>

4. Click Create Scheduled Task. The Create Automation Task dialog is displayed.

Create Automation Task

Task Name: name *

Task Description: description *

Auto Reboot: ON

Schedule: custom

How often: Weekly

Days of the week: Select days

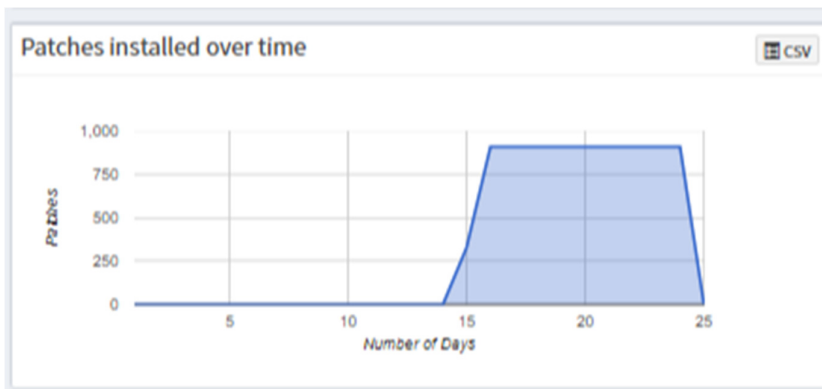
Remediation Time Frame: HH:MM:AM - HH:MM:AM

Schedule a Task Cancel

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.

Installed Patches

Asset	Patch	Installed Date	Size	Rollback Status	Hosts
.NET 3.5 Feature on Deman...	KB3109599	1970/01/01 00:00:00 UTC	0	TRUE	1
2017-05 Security Monthly Q...	KB4019264	2017/06/02 00:00:00 UTC	Unknown	UNKNOWN	1
2017-06 Update for Window...	KB4022405	2017/07/15 00:00:00 UTC	Unknown	UNKNOWN	1
2017-06 Cumulative Update...	KB4022727	2018/04/03 00:00:00 UTC	141649696	TRUE	1
2017-06 Cumulative Update...	KB4022727	2017/07/31 00:00:00 UTC	Unknown	UNKNOWN	1

Click to rollback patches

To Rollback Patches

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

Click to create a job to rollback installed patches

Asset	Patch	Installed Date	Size	Rollback Status	Hosts
Microsoft Windows 7	cce-10007-3-patch.inf	2018/03/08 11:23:17 UTC	unknown	TRUE	1
Microsoft Windows 7	cce-10011-5-patch.inf	2018/03/08 11:23:17 UTC	Unknown	TRUE	1
Microsoft Windows 7	cce-10022-2-patch.inf	2018/03/08 11:23:17 UTC	Unknown	TRUE	1
Microsoft Windows 7	cce-10059-4-patch.inf	2018/03/08 11:23:17 UTC	Unknown	TRUE	1
Microsoft Windows 7	cce-10061-0-patch.inf	2018/03/08 11:23:17 UTC	Unknown	TRUE	1
Microsoft Windows 7	cce-10064-4-patch.inf	2018/03/08 11:23:17 UTC	Unknown	TRUE	1
Microsoft Windows 7	cce-10077-6-patch.inf	2018/03/08 11:23:17 UTC	Unknown	TRUE	1
Microsoft Windows 7	cce-10090-9-patch.inf	2018/03/08 11:23:17 UTC	Unknown	TRUE	1
Microsoft Windows 7	cce-10093-3-patch.inf	2018/03/08 11:23:17 UTC	Unknown	TRUE	1
Microsoft Windows 7	cce-10103-0-patch.inf	2018/03/08 11:23:17 UTC	Unknown	TRUE	1
Microsoft Windows 7	cce-10130-3-patch.inf	2018/03/08 11:23:17 UTC	Unknown	TRUE	1
Microsoft Windows 7	cce-10136-0-patch.inf	2018/03/08 11:23:17 UTC	Unknown	TRUE	1
Microsoft Windows 7	cce-10137-8-patch.inf	2018/03/08 11:23:17 UTC	Unknown	TRUE	1
Microsoft Windows 7	cce-10140-2-patch.inf	2018/03/08 11:23:17 UTC	Unknown	TRUE	1
Microsoft Windows 7	cce-10150-1-patch.inf	2018/03/08 11:23:17 UTC	Unknown	TRUE	1

The Create Rollback Task dialog is displayed.

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.](#)

Reason for Failure	
Reason	Hosts
Remediation errors	1

Job Status Summary

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

Name	Assets	Date	Status
1KB-IR-win8.1	1	2018-04-05.06:11:04(UTC+0000)	Completed
1ss-cent	1	2018-04-06.13:06:15(UTC+0000)	Completed
1ss-pass	1	2018-04-06.13:33:57(UTC+0000)	Completed
2-cent-ss	2	2018-04-05.06:22:02(UTC+0000)	Completed
2-wrong-date	2	2018-04-05.07:07:50(UTC+0000)	Completed

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.

Host Name	Overall Status
support-pc	success
support-win7-s8	success

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.

The screenshot shows the SanerNow interface for configuring alerts. The top navigation bar is green with the 'sanerNow' logo and a user profile 'shobana'. The main content area is titled 'Alerts' and has several tabs: Vulnerability Management, Compliance Management, Endpoint Detection & Resp, Endpoint Management, Patch Management (selected), and Asset Management. The configuration form includes:

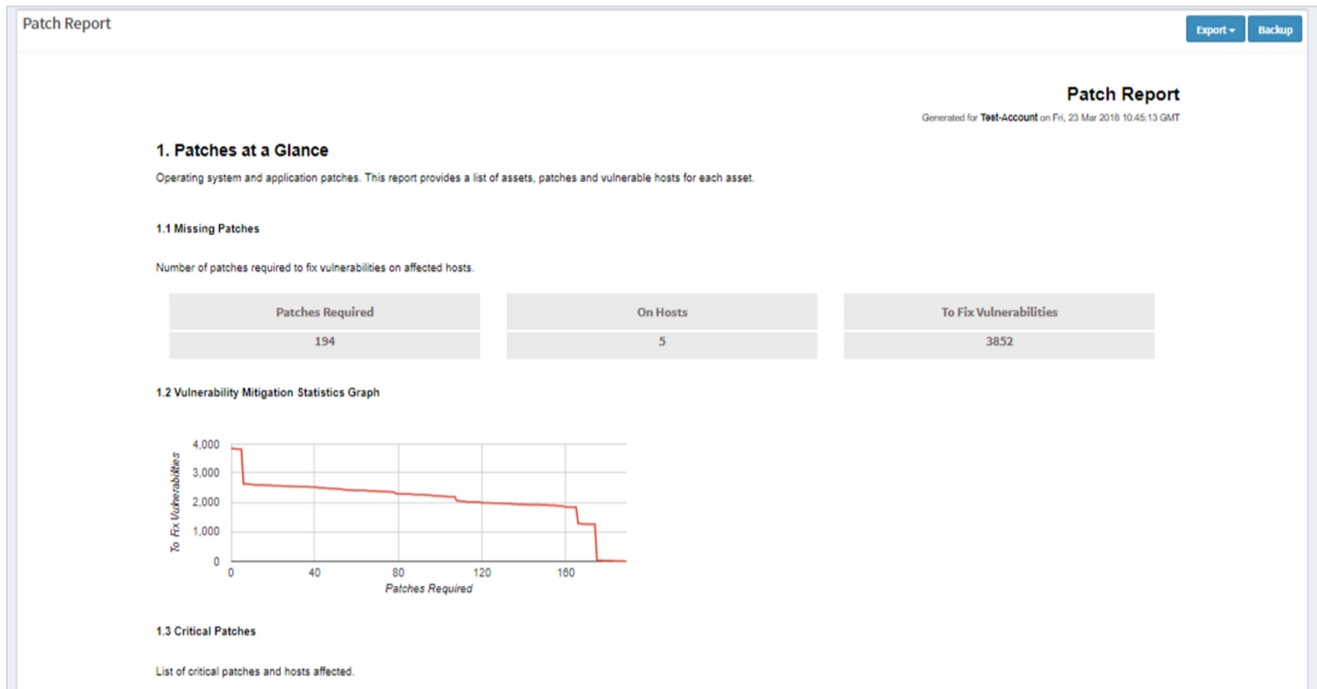
- Subscription status:** A dropdown menu currently set to 'OFF'.
- Send to E-mail*:** A text input field containing 'rsmitha@secpod.com'.
- Conditions*:**
 - Detection:**
 - Important and Critical Patches
 - All Missing Patches
 - Critical Missing Patches
 - Custom
 - Response:**
 - All failure actions
 - All successful actions
 - Custom
 - All actions
- Update:** A green button at the bottom right of the form.

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**.

The screenshot displays the SanerNow web interface. A central dialog box titled "Automatic Backup Settings" is open, allowing configuration of backup tasks. The background shows a "Patch Report" page with a sidebar of report types and a main content area with "Export" and "Backup" buttons.

Automatic Backup Settings

- How often: Weekly
- Days of the week: Tuesday, Wednesday, Thursday
- Keep only the latest: 15 backups (delete older ones)
- E-mail: tprakash@secpod.com,spreeti@secpod.c
- Backup Time: 8:00 (Server timezone offset: UTC +00:00)

Save **Close**

Reports

- Executive Report
- Endpoint Management Report
- Asset Report
- Vulnerability Report
- Patch Report**
- Compliance Report
- Endpoint Detection and Response Report

Patch Report

Export Backup

To Fix Vulnerabilities

33646

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