# Managing Compliance Using SanerNow

4.0 User Guide

secpod

# Contents


**COMPLIANCE MANAGEMENT ..... 3**

Compliance ..... 3

Benchmark ..... 4

***To apply existing benchmarks to device groups ..... 4***

***To create a new benchmark ..... 4***

Rule-based Distribution ..... 5

Top Non-compliant Hosts ..... 5

Top Non-compliant Assets ..... 5

Mitigation Impact ..... 6

Remediation Actions ..... 6

***To apply patches to remediate misconfigurations and non-compliance issues ..... 6***

**SETTING EMAIL ALERTS FOR COMPLIANCE ISSUES ..... 7**

**COMPLIANCE REPORTING ..... 7**

***To generate a compliance report ..... 7***

***To Back Up Reports ..... 9***

# Compliance Management

SanerNow includes regulatory compliance templates for PCI, HIPAA, ISO 27001, NERC, NIST 800-53, and NIST 800-171. Compliance profiles can be created and customized to suit an organization's needs. Once the profile is deployed, SanerNow monitors the organization's assets for deviations from the profile and helps fix deviations. SanerNow performs daily checks to detect configuration discrepancies that can then be manually or automatically fixed.

SanerNow supports three aspects of compliance:

- Default Compliance
- Generic Compliance
- Regulatory Compliance

**Default Compliance** - By default, each operating system will have individual rules. SanerNow sets the values for this.

**Generic Compliance** - Generic compliance is designed to correspond to the different operating systems and their security settings such as Account Lockout Policy, Administrative Templates, Authentication Types, etc.

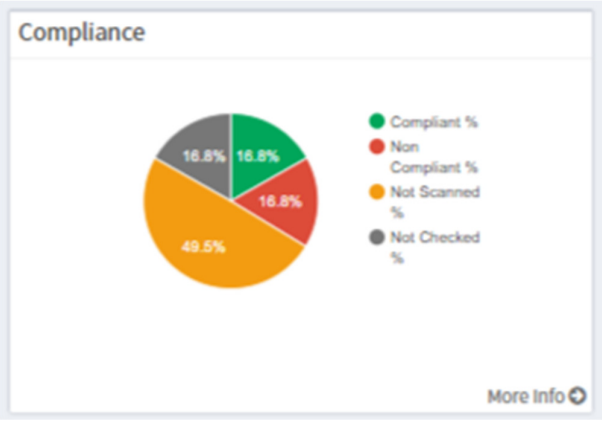
**Regulatory Compliance** - Regulatory compliance defines standards, such as the PCI, HIPAA, NIST, and NERC standards. Organizations are required to be aware of and to take steps to meet relevant laws and regulations.

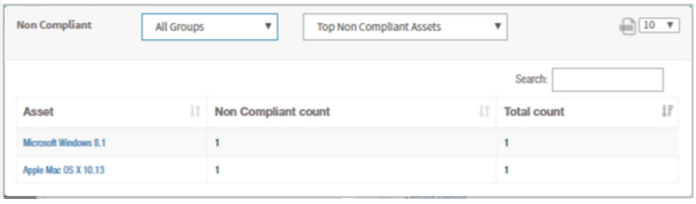
**To access the Compliance Management tool:**

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 Compliance Management icon. The Compliance Management dashboard is displayed.

## Compliance

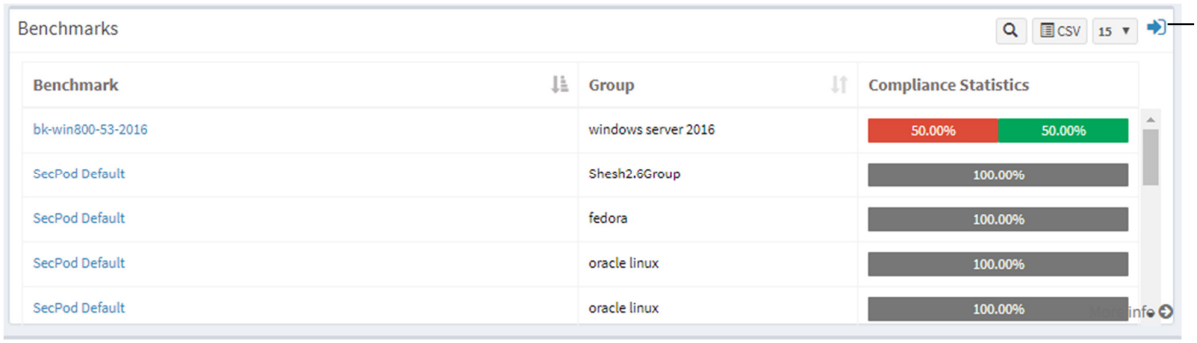
This pane shows the organization's compliance posture, and highlights the percentage of compliance, the percentage of non-compliance, the percentage of systems that have not been scanned for compliance, and the percentage of devices that are not yet a part of the SanerNow security services. Click More Info to view compliance details by groups or unassigned devices, by the top non-compliant hosts, top misconfigurations, or top non-compliant assets.



# Benchmark

This pane shows the benchmarks, the groups to which the benchmark is assigned, and the percentage compliance of the group.




Click the expand icon to apply benchmarks

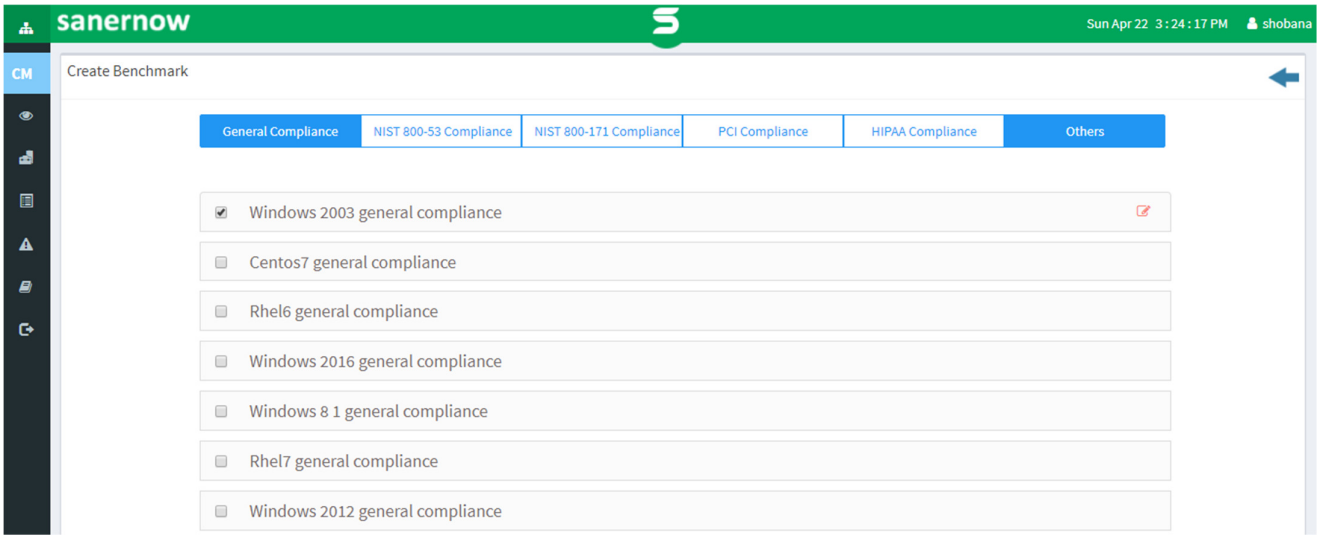
## To apply existing benchmarks to device groups

Do one of the following:

- Click a benchmark profile name in the list to quickly go to the Update Benchmark page and choose an existing benchmark to apply to a group of devices.
- Click the expand icon to go to the Benchmarks page and choose an existing benchmark to apply to a group of devices.

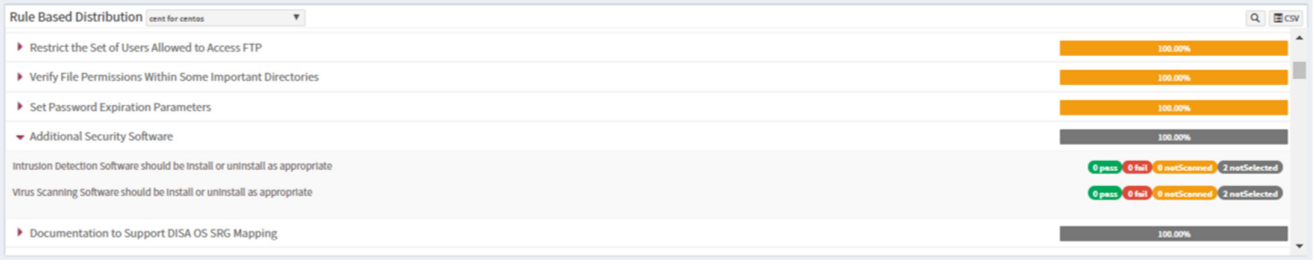
## To create a new benchmark

1. Click the expand icon on the Benchmarks pane to go to the Create Benchmark page. Click Create Benchmark. The Create Benchmark page is displayed.
2. Click a compliance category such as General, NIST 800-53, NIST 800-171, HIPAA, PCI, or Others. Under the selected category, select the benchmark rules you wish to apply.
3. Click Choose devices to apply selected Benchmarks. Specify a name for the benchmark in the Benchmark Name box. Choose the device groups you want to apply the benchmark to in the Assign To Groups drop-down.
4. Click Create to apply this benchmark to the selected devices.



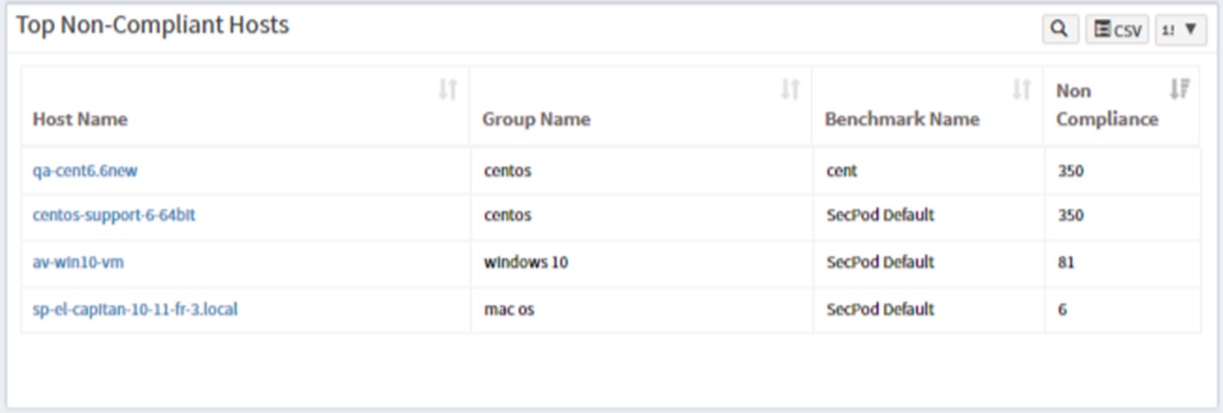
## Rule-based Distribution

This pane displays the rules of the benchmark that you select in the drop-down with the percentage of compliance. Expanding the rules shows the numbers for the devices that passed and failed this rule, as well as devices that were not scanned, and were not selected for this rule. Clicking these numbers will provide names of the hosts.




## Top Non-compliant Hosts

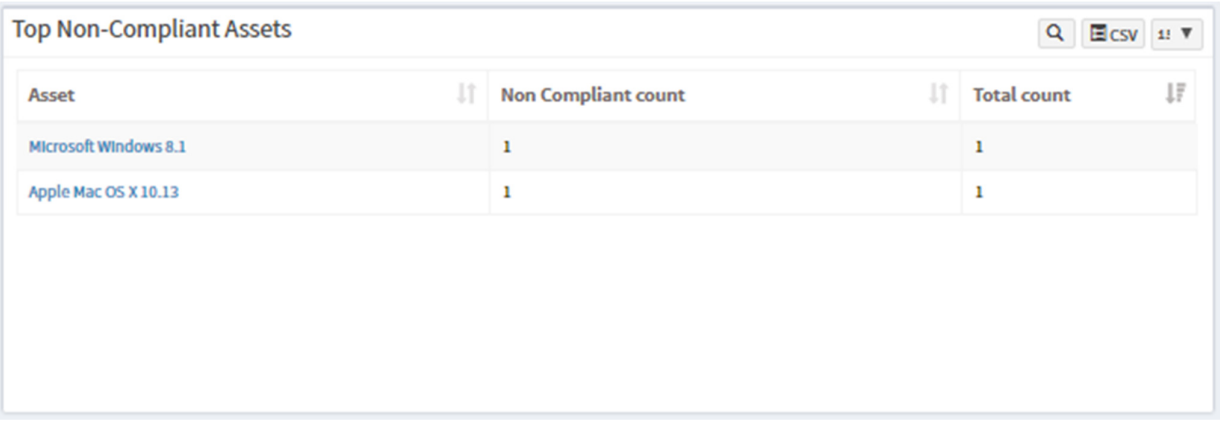
This pane shows the host name, the group to which the host belongs, the benchmark applied to the group, and a noncompliance number. Click a host name to go to the Device Info page; click the Compliance Management tab to see the individual host's compliance level to the assigned benchmark.




| Host Name | Group Name | Benchmark Name | Non Compliance |
|---|---|---|---|
| qa-cent6.6new | centos | cent | 350 |
| centos-support-6-64bit | centos | SecPod Default | 350 |
| av-win10-vm | windows 10 | SecPod Default | 81 |
| sp-el-capitan-10-11-fr-3.local | mac os | SecPod Default | 6 |

## Top Non-compliant Assets

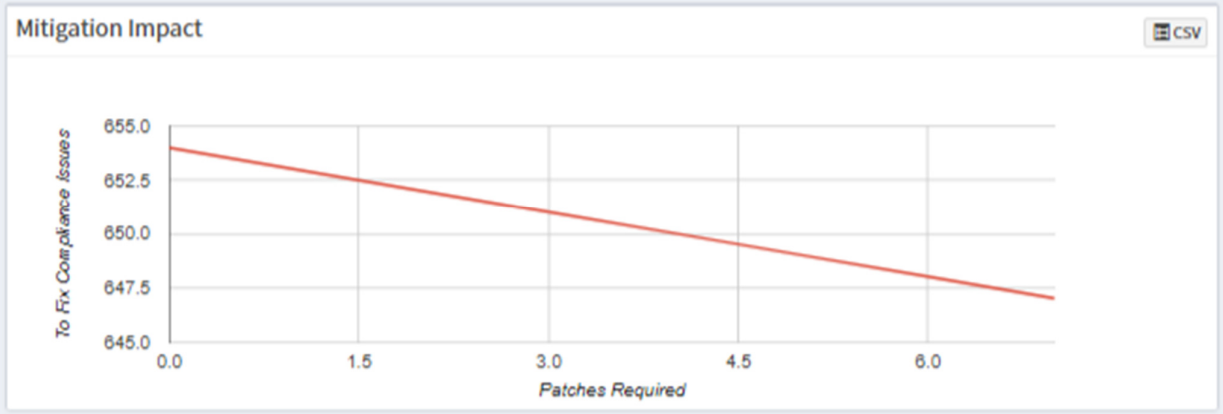
This pane shows the top non-compliant assets.




| Asset | Non Compliant count | Total count |
|---|---|---|
| Microsoft Windows 8.1 | 1 | 1 |
| Apple Mac OS X 10.13 | 1 | 1 |

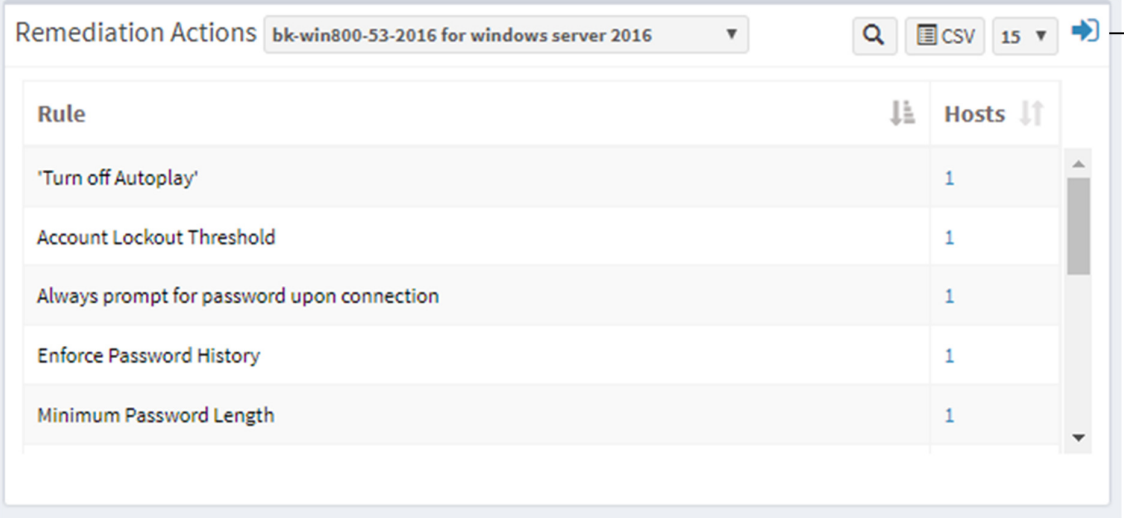
## Mitigation Impact

This pane shows the ratio of patches to compliance issues. For example, applying one patch across the organization can fix 653 compliance issues; applying 7 patches across the organization can bring down the compliance issue count to 647.




## Remediation Actions

After viewing all the non-compliance issues and statistics on the dashboard, you will need to fix the issues related to misconfigurations and compliance. This pane allows you to take remediation actions on a per rule basis for the benchmark selected in the drop-down.




### To apply patches to remediate misconfigurations and non-compliance issues

1. Click the Expand icon. The Remediation Actions page is displayed.
2. Select the rules you wish to remediate. Click **Fix Selected Issues**. You will be transferred to the Missing Patches page.
3. Select the patches you wish to install. Click **Fix Selected Patches** to open the Create Patching Task dialog.
4. Specify a job name and turn on auto reboot if you wish the devices to be restarted automatically after applying patches.
5. Specify a schedule for the job, either immediate or after the scheduled scan. Specify a corresponding time in the

time counter. You can also choose a custom or different date and time for the patching job.

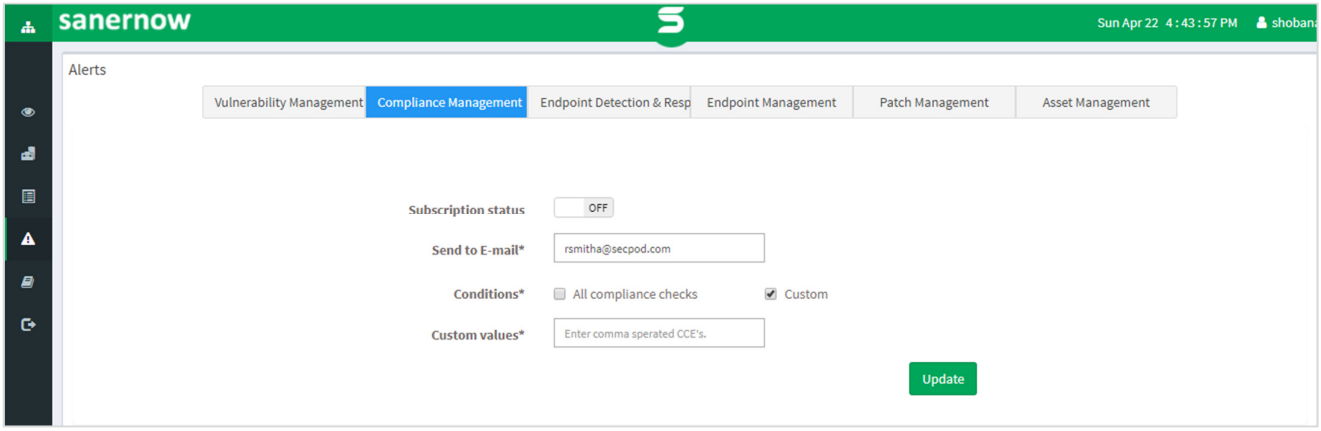
6. Click **Create Job**.

# Setting Alerts for Compliance Issues

The Alerts feature sends a notification to the specified email on compliance issues. This setting must be configured before the first scheduled scan.

## To set alerts for compliance issues

1. Click Alerts on the left pane.
2. Turn on “Subscription Status” to enable compliance alerts.
3. Specify an email address to which the alerts will be sent. You can have alerts sent for all compliance issues or custom conditions based on CCEs.
4. Click **Update**.




# Compliance Reporting

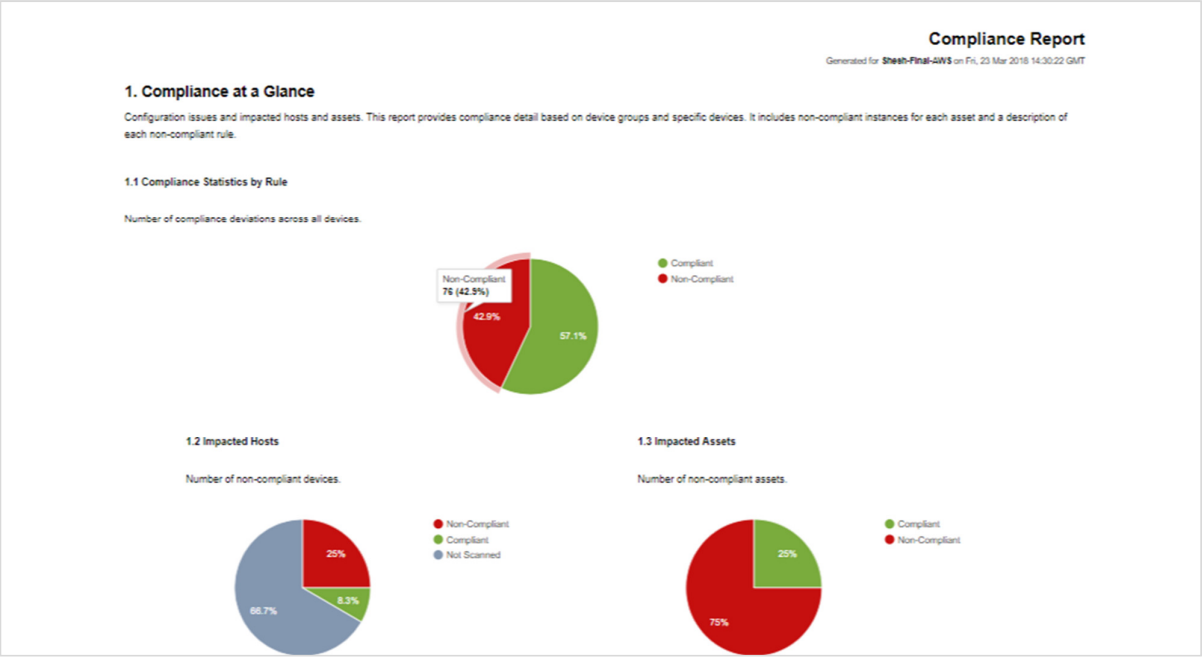
After the scheduled scan, the agent uploads the configuration compliance report. The Compliance Report displays the configuration issues and impacted hosts and assets. It provides compliance details based on the device groups and specific devices. It also includes non-compliant instances for each asset and a description of each non-compliant rule.

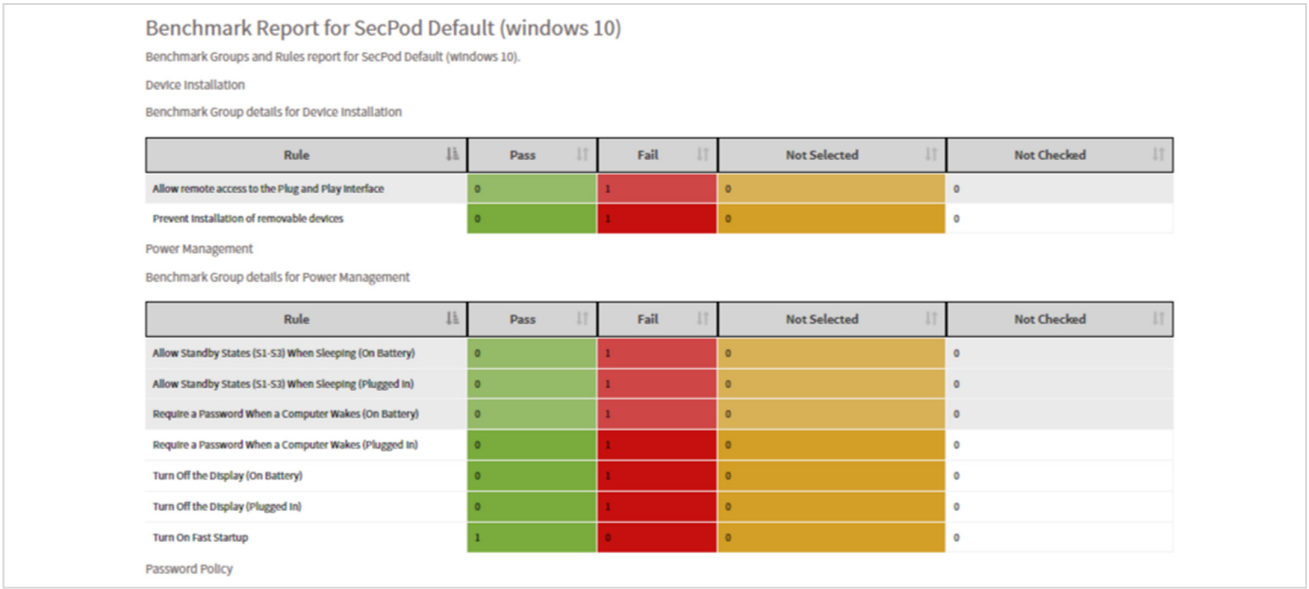
We recommend generating a compliance report before and after remediation actions to compare the status of the compliant devices and understand your organization’s compliance level.

The figures below show sections of the compliance report.

## To generate a compliance report

- Click Reports > Click Compliance Report.




**To export the report to a PDF**

- Click Export > PDF

**To export the report and send it via email:**

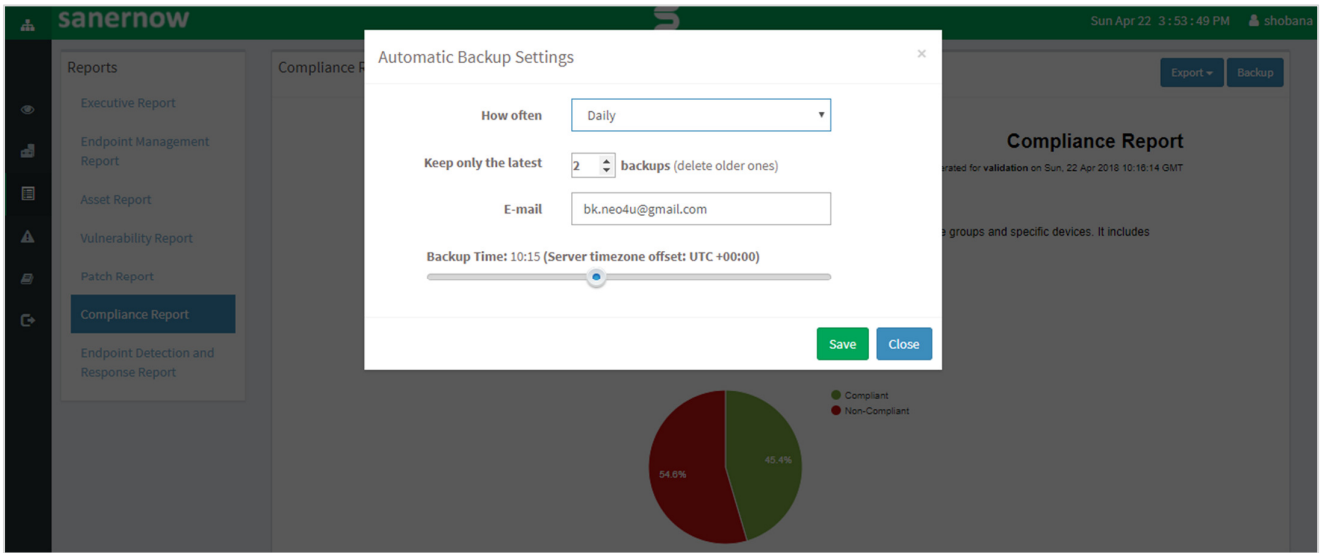
1. Click Export > Email.
2. Specify the email addresses.

## To Back Up Reports

The backup settings under Reports allow IT administrators to maintain a history of compliance. 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 **Compliance 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 an **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