SanerNow General Settings

4.0 User Guide

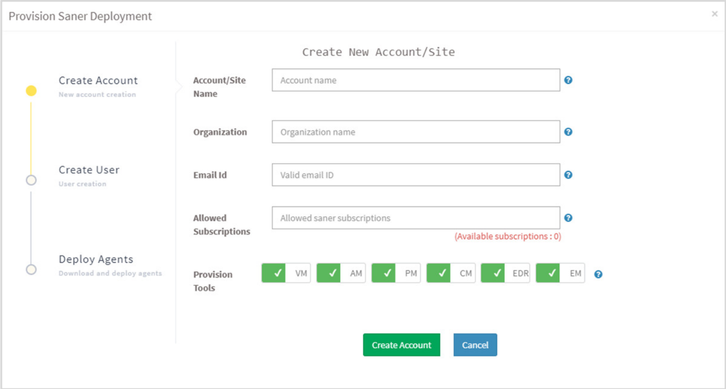
Contents

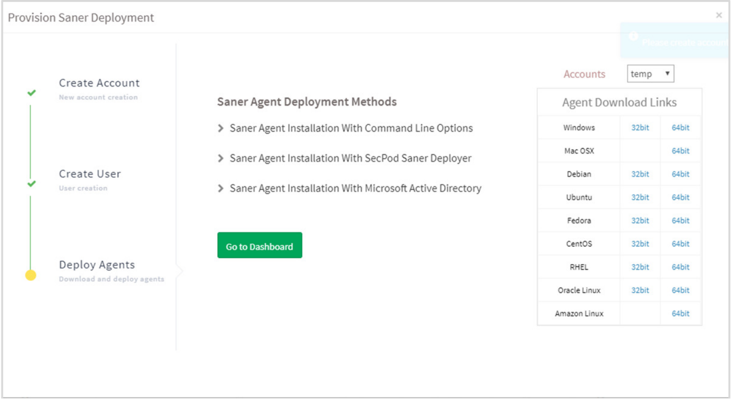
Getting Started with SanerNow

Welcome to SanerNow 4.0, a cloud-enabled Endpoint Security Management Solution. SanerNow offers a comprehensive toolset to support Vulnerability, Compliance, Endpoint, Patch, Asset, and Endpoint Detection and Response management.

To start using SanerNow, log on to the dashboard and deploy SanerNow agents on endpoint nodes. Once you have deployed the agent on the endpoints, you can create a SanerNow agent profile to quickly and easily apply the Saner agent settings across devices and device groups. Additionally, you may need to add accounts, add users.

If this is a first use of SanerNow, when you click the S icon, the easy 3-step wizard shown below will guide you through tasks to create an account and provision tools, add users, and deploy Saner agents on endpoints.





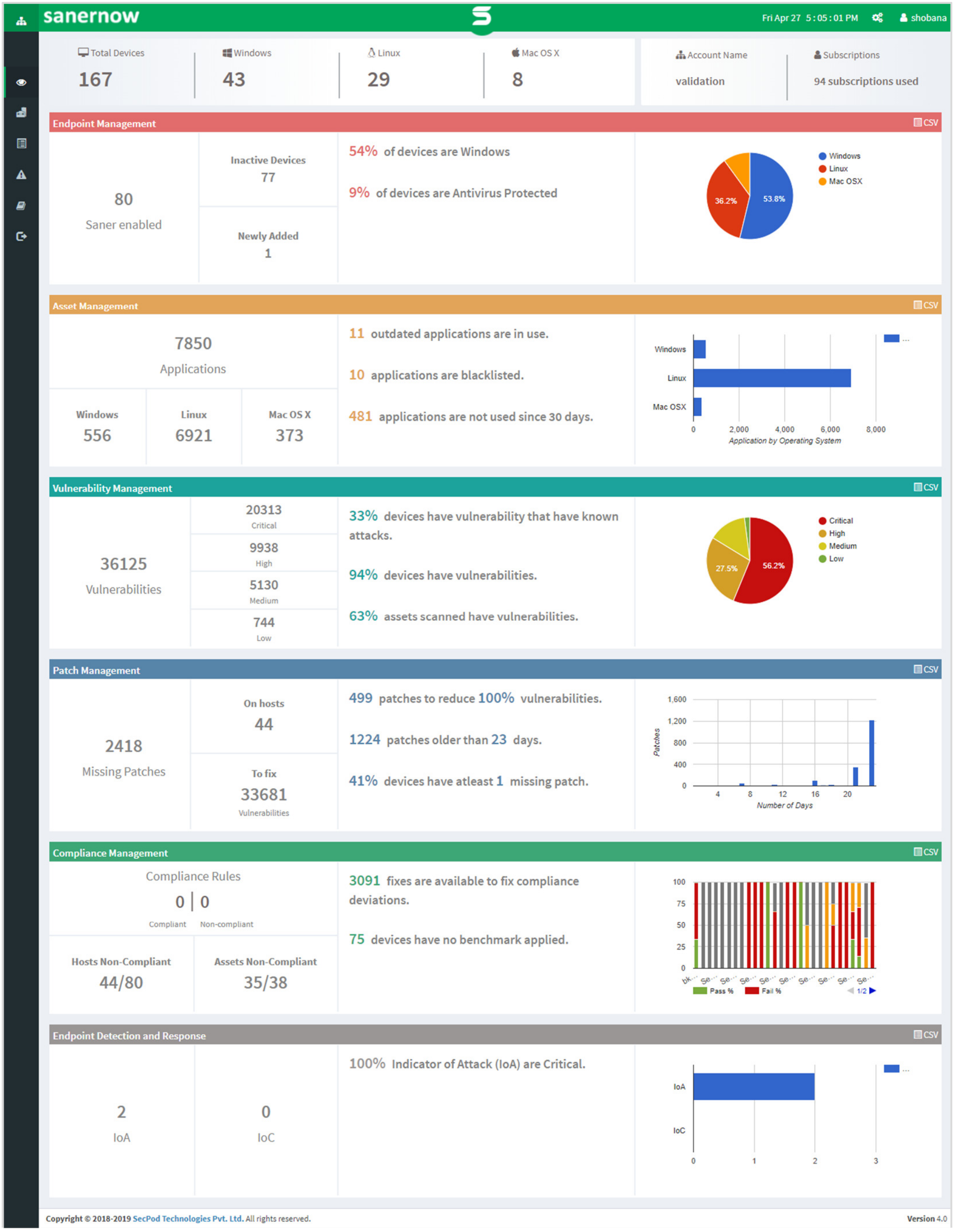
Saner Agent Deployment Methods

- Saner Agent Installation With Command Line Options
- Saner Agent Installation With SecPod Saner Deployer
- Saner Agent Installation With Microsoft Active Directory

Agent Download Links		
Windows	32bit	64bit
Mac OSX		64bit
Debian	32bit	64bit
Ubuntu	32bit	64bit
Fedora	32bit	64bit
CentOS	32bit	64bit
RHEL	32bit	64bit
Oracle Linux	32bit	64bit
Amazon Linux		64bit

To log on to the SanerNow dashboard

- Go to https://saner.secpod.com/ and log on with the credentials provided. The SanerNow dashboard is displayed. If an account already exists and the Saner Agent has been deployed on the endpoints, the Visibility dashboard is displayed, which is a bird’s eye view of the security status of the devices and assets on your managed endpoints.



Total Devices 167 | Windows 43 | Linux 29 | Mac OS X 8

Account Name: validation | Subscriptions: 94 subscriptions used

Endpoint Management

80 Saner enabled

Inactive Devices 77

Newly Added 1

54% of devices are Windows

9% of devices are Antivirus Protected

Asset Management

7850 Applications

Windows 556 | Linux 6921 | Mac OS X 373

11 outdated applications are in use.

10 applications are blacklisted.

481 applications are not used since 30 days.

Vulnerability Management

36125 Vulnerabilities

20313 Critical | 9938 High | 5130 Medium | 744 Low

33% devices have vulnerability that have known attacks.

94% devices have vulnerabilities.

63% assets scanned have vulnerabilities.

Patch Management

2418 Missing Patches

On hosts 44

To fix 33681 Vulnerabilities

499 patches to reduce 100% vulnerabilities.

1224 patches older than 23 days.

41% devices have atleast 1 missing patch.

Compliance Management

Compliance Rules 0 | 0 (Compliant | Non-compliant)

Hosts Non-Compliant 44/80

Assets Non-Compliant 35/38

3091 fixes are available to fix compliance deviations.

75 devices have no benchmark applied.

Endpoint Detection and Response

2 IoA

0 IoC

100% Indicator of Attack (IoA) are Critical.

Copyright © 2018-2019 SecPod Technologies Pvt. Ltd. All rights reserved.

Version 4.0

To edit your user profile

1. Your user profile is on the top right corner of the dashboard. Click the User info dialog to see details such as the license expiry date for SanerNow, the number of subscriptions available, and the account you are logged on to.
2. You can quickly edit your name and email details if required by clicking the Edit Profile icon at the top of the dialog.
3. You can also turn on two-factor authentication or reset your password from here.

   - Two factor authentication – Download the Google Authenticator App on to your mobile, scan the QR code, and enter the 6-digit code provided by the app in the Code box. Click Enable.
   - Reset Password - Type in your old and new passwords in the Change Password dialog and click Update.

Deploying the SanerNow Agent

To manage devices, it is necessary to install the SanerNow Agent. The Saner agent can be deployed in two ways:

- Show Agent Download URL
- Download the Deployer Tool

To deploy the SanerNow Agent on endpoints

To deploy the agent using the Download deployer tool:

1. Click Manage > Devices > Deployment.
2. Select Download deployer tool, from the Deployment Method drop-down.
3. Click Download. The SecPod Saner deployment tool download page is displayed.
4. Select the Deployer corresponding to the OS on which you wish to install the agent.
5. Click Download. The deployment tool is downloaded in .zip format.
6. Unzip the file and run the deployment tool in the following way:

```
$python inhouse_saner_deployer.py --host=192.168.1.82 --smb_user=administrator --
smb_pass=secpod

--remove=false --installers=./Saner-Installers
```

To deploy the agent using the Show Agent Download URL:

1. Click Manage > Devices > Deployment.
2. Select Show Agent Download URL.
3. Click Go To URL. The Saner Agent Installers page is displayed.
4. Select the Deployer for the OS corresponding to the endpoints on which you will install the Agent.
5. Click Download. The installer is downloaded. Click the installer to deploy the agent on the endpoints.

Once the agent is installed and activated, the managed endpoints are displayed in the device table. The devices are grouped by default according to the OS. You can create a custom group and drag and drop the devices to the group.

To undeploy the SanerNow Agent from endpoints

The Saner agent can be undeployed either manually or through the SanerNow dashboard.

1. Click Manage > Devices > Deployment.
2. Select **UnDeploy Agent**.
3. Select **Delete Device** from the Deployment Method drop-down.
4. Under the Add Criteria group, specify the Host Name, IP address, Family, Operating System or a custom filter.
5. Click **Delete Device**. The agent is deactivated.

To disable the SanerNow Agent from endpoints

1. Click Manage > Devices > Deployment.
2. Select UnDeploy Agent.
3. Select **Disable Device** from the Deployment Method drop-down.
4. Under the Add Criteria group, specify the Host Name, IP address, Family, Operating System or a custom

filter.

5. Click Disable Device. The agent is disabled on the specified endpoints.

Managing Devices

Devices on your network are automatically grouped by the OS and displayed in the devices table. You can create custom groups and drag and drop devices from the Device Table into it. You can deploy the SanerNow Agent on devices as described in the section above. After the SanerNow Agent is installed on devices, you can manage the devices.

To create a custom group and add devices to it

1. Select Manage > Devices.
2. Click Create Group. Specify a name and description for the group in the Group Name and Group Description boxes.
3. Identify the devices that should be a part of the group by applying filter criteria based on host names, IP addresses, operating system, family or custom criteria to unassigned devices or all devices. Click Show Devices to view the search results. Click Create to create the group with the identified devices.

To scan devices

1. Select Manage > Devices.
2. Select the devices you want to scan from the Device Table. Click Scan Now.

Managing Accounts

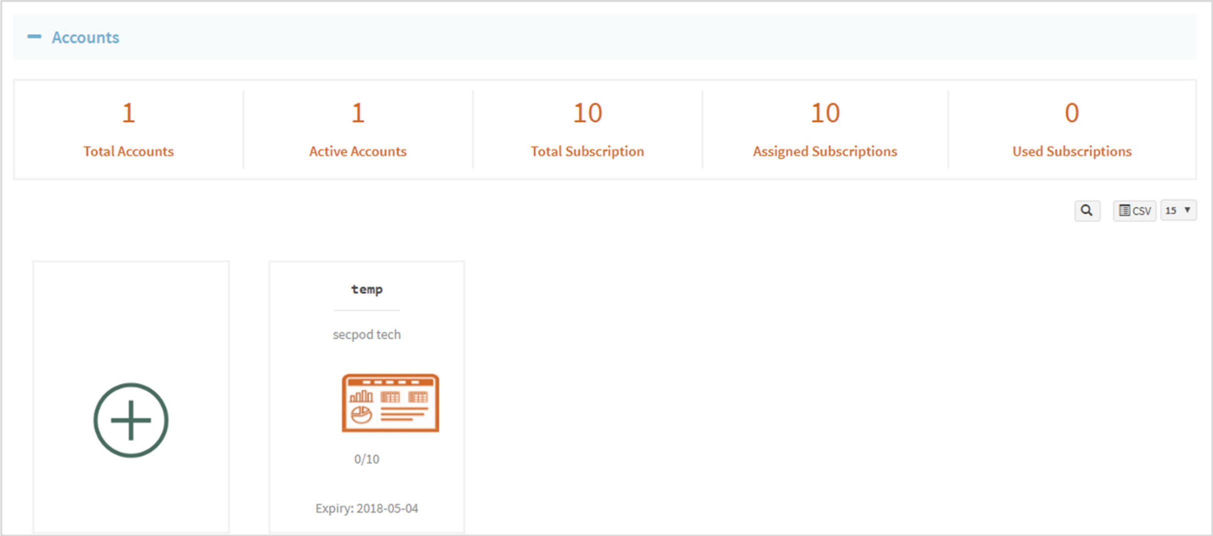
SanerNow is a multi-tenant solution. As an MSSP, you can manage multiple accounts from SanerNow. You can also add your logo to the solution to brand it.

The Accounts page provides the following information at a glance:

- Total number of accounts that you have created.
- Total number of accounts that are in an active state or in use currently.
- Total number of SanerNow subscriptions allowed.
- Total number of subscriptions that you have allotted to a particular account.
- Total number of used subscriptions, that is, subscriptions that have been assigned to a device.

You can add an account, modify an account or delete an account from this page.

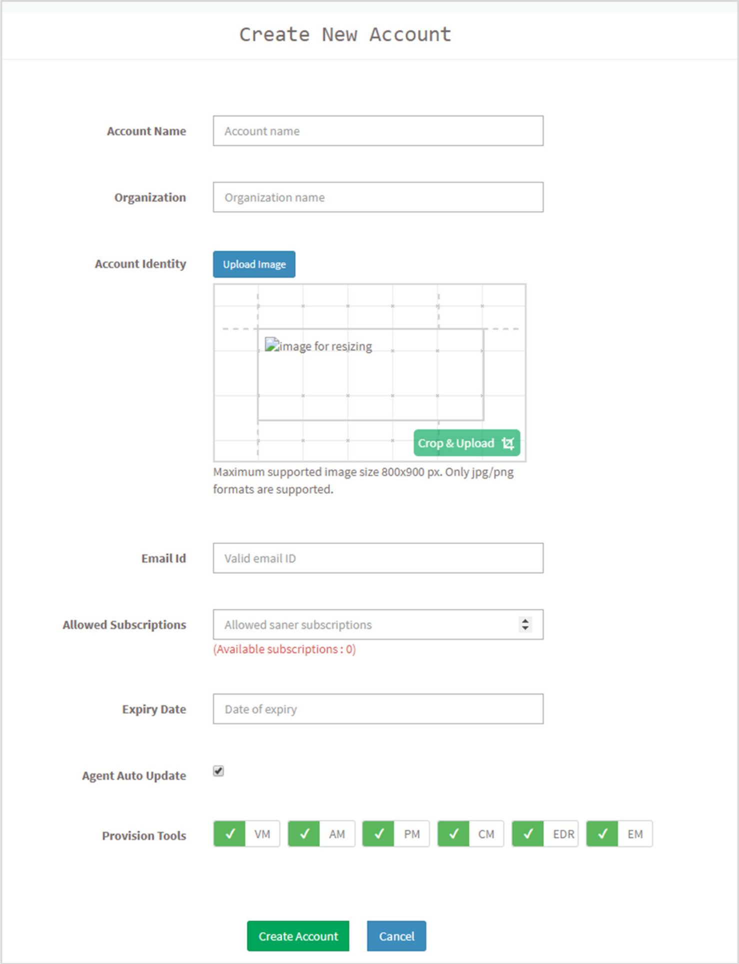
Note: As an admin user, you can only add as many accounts as you have subscriptions. If you exhaust the total number of subscriptions allowed, you cannot add a new account.



To add a new account or modify an account

1. Click the Control Panel (gears) icon on the top right.
2. Click the plus sign next to Accounts to display the Accounts page.
3. Do one of the following:
   - Click the plus sign to add an account.
     - OR -
   - Click an account to modify the account details.

   The Create Account page is displayed.
4. Specify the following information in the text boxes: account name, organization name, a logo or image to visually identify the account, an email ID to uniquely identify the account, the number of subscriptions you want to assign to this account, and the expiry date of the subscriptions.
5. Select the Agent AutoUpdate checkbox if you want SanerNow to automatically install updates to the Saner Agent.
6. Select the tools that you want to provision for this account.
7. Click Create Account.



Create New Account

Account Name: Account name

Organization: Organization name

Account Identity: Upload Image

Maximum supported image size 800x900 px. Only jpg/png formats are supported.

Email Id: Valid email ID

Allowed Subscriptions: Allowed saner subscriptions

(Available subscriptions : 0)

Expiry Date: Date of expiry

Agent Auto Update: ☑

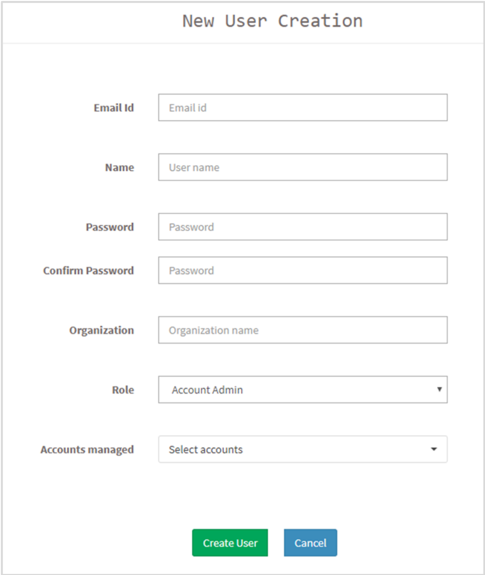
Provision Tools: ✓ VM ✓ AM ✓ PM ✓ CM ✓ EDR ✓ EM

Managing Users

SanerNow supports two types of users for accounts. Only Admin users have privileges to add other users and new accounts, as well as to enforce mail and authentication settings, and specify branding through a custom logo. They also have edit or delete privileges, unlike “normal” users. Admin users can add as many users as required.

To add new users

1. Click the Control Panel (gears) icon on the top right
1. Click the plus sign next to Users. The user information for this account is displayed, such as the total number of users of this account, the number of admin accounts, and the number of end users.
2. To add a user, click New User. The Create User page is displayed.
3. Specify the email ID with which the user will log on to SanerNow, the name, password, and organization to which the user belongs. Select the role of the user from the Role drop-down. Select the accounts that the user will have access to.
4. Click Create User. The user is added to the specified accounts, and the user details are populated in the User Info table.



New User Creation

Email Id: Email id

Name: User name

Password: Password

Confirm Password: Password

Organization: Organization name

Role: Account Admin

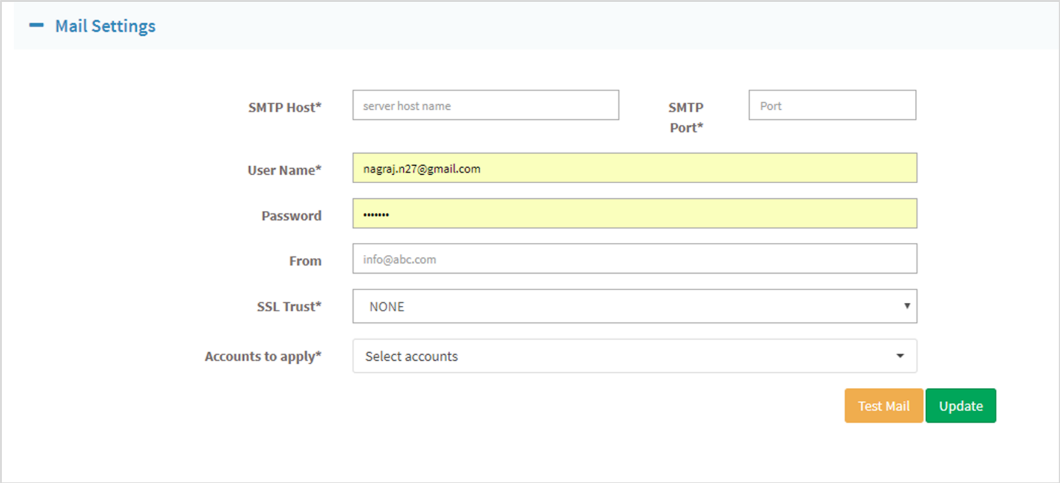
Accounts managed: Select accounts

Configuring Mail Settings

The mail settings in the SanerNow dashboard allows administrators to send alerts related to vulnerability, non-compliance, threats and malware, critical patches or necessary updates, new assets, new devices, and the failure and success of queries and actions related to these, as well as to send reports. The mail server should be set before deploying the agent on the network. You can configure a public or local mail server.

To configure mail server settings

1. Click the Control Panel (gears) icon on the top right
2. Click the plus sign next to Mail Settings.
3. Specify the SMTP Host. For example, smtp.gmail.com. The SMTP supported hosts are 25, 465, 587. In this case, the supported port for Gmail is 465.
4. Enter the email ID from which the mail will be sent, and the password in the **Username** and **Password** boxes.
5. Enter the **From** email address that will be displayed to the receiver. This is optional.
6. Specify an authentication type in the **SSL Trust** drop-down:
   - Select None if you do not want to set any security protocol.
   - Select STARTTLS or SSL/TLS to set a security protocol.
7. Click Update.
8. Test the setting by clicking Test Mail.



− Mail Settings

SMTP Host* server host name

SMTP Port* Port

User Name* nagraj.n27@gmail.com

Password •••••••

From info@abc.com

SSL Trust* NONE

Accounts to apply* Select accounts

Two-factor Authentication

To turn off or turn on two-factor authentication for all users

1. Click the Control Panel (gears) icon on the top right
2. Click the plus sign next to Two-Factor authentication.
3. Do one of the following:
   - Click Enforce to turn on two-factor authentication for all users.
   - Click Revoke to turn off two-factor authentication for all users.

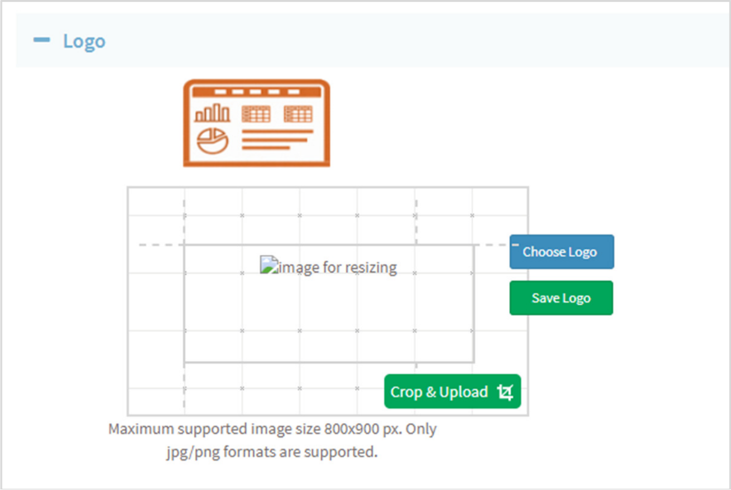
   When a user logs on to SanerNow after an admin user has enabled two-factor authentication, he or she will be prompted to scan the QR code on the mobile and enter the code, to proceed.

Adding your Logo to SanerNow

To brand the solution, as an MSSP, you can replace the SanerNow logo with your own company logo.

To add your logo to SanerNow

1. Click the Control Panel (gears) icon on the top right.
2. Click the plus sign next to Logo to display the Logo panel.
3. Click Choose Logo to browse to your hard drive and select a jpeg or png file of your logo. The maximum allowed size is 800 x 900 pixels.
4. Resize and adjust the logo to fit within the grid guidelines.
5. Click Crop and Upload to upload the logo to the server.
6. Click Save Logo to replace the SanerNow logo with your own logo.



Maximum supported image size 800x900 px. Only jpg/png formats are supported.

Configuring the SanerNow Agent Settings

The Saner agent provides a number of settings and attributes that you must configure before it can function optimally. This section explains the settings and how to apply them to the Saner agent.

This section is for SecPod Enterprise users and MSPs (Managed Service Providers) who want to manage Saner Endpoint Security.

The **Settings** option on the left pane of the SanerNow dashboard allows you to create a Saner agent configuration profile that can be applied to a group of Saner devices.

To create a Saner Agent profile and apply it to devices

1. Click Manage > Settings to display the Settings page. Click Create Settings.
2. Configure the Saner Agent settings as explained in the following section.
3. Specify a name and description in the **Settings Name** and **Settings Description** boxes. Select a group to apply the profile to and click **Create**.

Scan

- **Scan Mode** – You can choose to do a scan in Full Throttle mode or in Low mode. The Full Throttle mode consumes maximum system resources while scanning, which slows down system performance, whereas the low scan mode consumes minimal system resources. By default, the Full Throttle is selected. A Full Throttle scan takes around five minutes.
- **Scan** for **Vulnerability** – Scan for vulnerabilities present in the OS and assets. By default, it is turned on.
- **Scan for Compliance** – Scan for misconfigurations present in the OS. By default, it is turned on.

Schedule

- **Scheduled Scan Time** – Specify a time for the Saner agent to start scanning devices for vulnerabilities or compliance issues. By default, the scan is scheduled to start at 12:00 PM.
- **Scheduled Download Time** – Specify a time for the Saner Agent to start downloading updates to the

vulnerability and compliance content. By default, downloads are set to start at 11.00 AM.

- **Agent Messaging** – This setting specifies how and when the Saner agent and Ancor server will communicate.
- Job polling interval (in minutes) – The server polls Saner every five minutes by default. You can change the polling interval.

Remediate

- **Vendor Products Patch Server** - For Windows products, the Microsoft patch server is the default patch server. You can specify a secondary patch server. Linux and Mac OS X patches are served up by the respective company patch servers.
- **Third-party Products Patch Server** – The SanerNow agent contacts the Ancor server by default for the latest available patches to third-party products. Administrators can change this to a local server.
  - **Protocol** – If you choose to specify a local server, provide the server URL.
- **Buffer Patches** – Turn it on to save on network bandwidth during remediation. As soon as the agent is done scanning the system, it starts downloading the patches. Whenever remediation is performed, it collects patches from the downloaded directory instead of contacting the Ancor server. By default, Saner allows up to 1GB of patches to download with 70% of network bandwidth consumption. You can change the percentage of network bandwidth consumption.

Network

- **Enable Proxy –** Select to enable the SanerNow agent to use the network's proxy server to communicate with the Ancor server.
- **Proxy URL –** Specify the IP address or domain name.
- **Proxy Port** – Specify the port number.
- **Authenticate –** Select to enable authentication. Specify the **User ID** and **Password** that the SanerNow agent should use.

Upgrade

- Saner Agent Upgrade Mode:
  - Select **Manual** if you want to upgrade to the latest Saner version at the scheduled download time.
  - Select **Enabled** if you want to upgrade to the latest Saner version automatically whenever an upgrade is available on the Ancor server.
  - Select **Disabled** if you do not want to upgrade Saner even when there is an upgrade available.

Language

- **Language Preference** - The language is set to English.

Logs

- **Enable Log** – Turn it on to see agent activities. By default, it is turned off.
- Log Type:
  - Turn on **Audit** to see the sequence of events related to the Saner agent's activities. These are logs

with minimal information, and therefore, Audit is turned on by default.

- Turn on **Debug** to get logs with detailed information that can help you identify and solve issues.

Setting Up Alerts

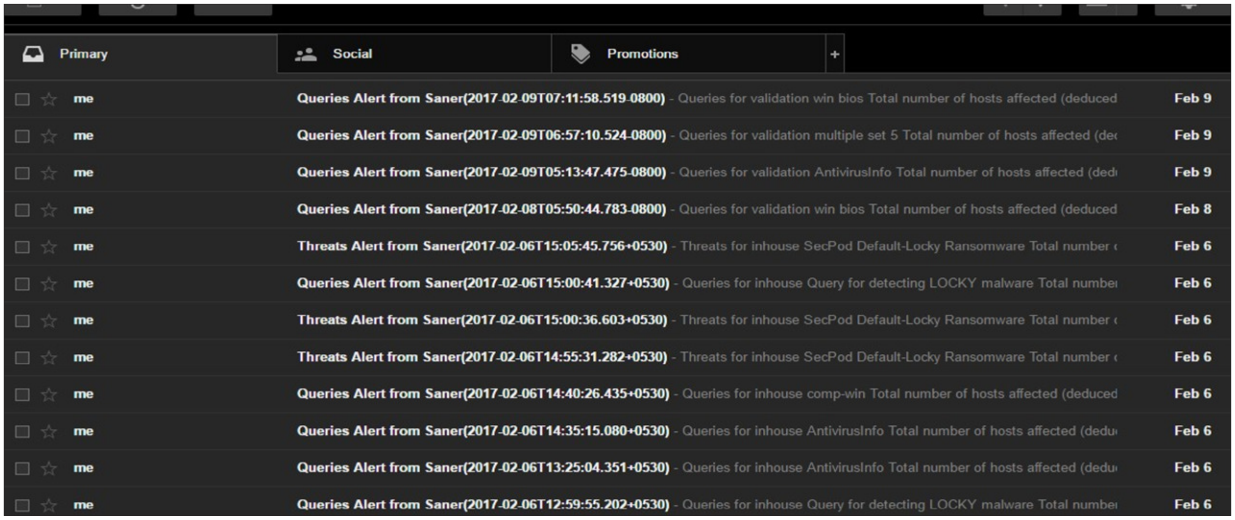
Alerts keep administrators informed about new vulnerabilities, misconfigurations and any new non-compliance in agent installed machines. If alerts are configured after the agent is deployed, the existing vulnerabilities will not be displayed.

To Set Alerts

1. Click Alerts on the left pane. The Alerts page displays the alert types (Vulnerability, Compliance, Endpoint Detection and Response, Patch, and Asset) and the option to subscribe to an alert, as well as the individual settings for each alert type.
2. Turn the **Subscription Status** on for the alert type you wish to receive.
3. Enter an email ID to which the corresponding alerts must be sent, in the **Send to E-mail** box. You can enter multiple email addresses separated by commas.
4. Select the **Conditions** you wish to receive alerts for. The conditions of each alert type are explained below.
5. Click **Update**.

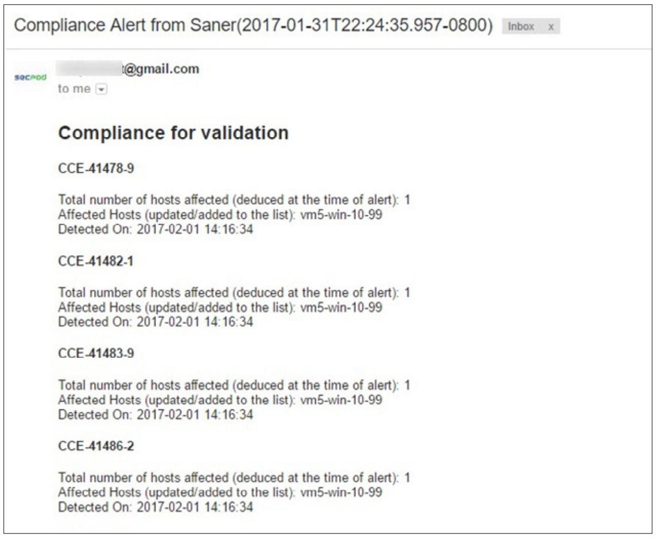
Note: For alerts to work successfully, make sure you have configured your mail server as described in Configuring Mail Settings.

Alerts will be sent to the specified email IDs.



□	☆	me	**Queries Alert from Saner(2017-02-09T07:11:58.519-0800)** - Queries for validation win bios Total number of hosts affected (deduced	Feb 9
□	☆	me	**Queries Alert from Saner(2017-02-09T06:57:10.524-0800)** - Queries for validation multiple set 5 Total number of hosts affected (de	Feb 9
□	☆	me	**Queries Alert from Saner(2017-02-09T05:13:47.475-0800)** - Queries for validation AntivirusInfo Total number of hosts affected (ded	Feb 9
□	☆	me	**Queries Alert from Saner(2017-02-08T05:50:44.783-0800)** - Queries for validation win bios Total number of hosts affected (deduced	Feb 8
□	☆	me	**Threats Alert from Saner(2017-02-06T15:05:45.756+0530)** - Threats for inhouse SecPod Default-Locky Ransomware Total number	Feb 6
□	☆	me	**Queries Alert from Saner(2017-02-06T15:00:41.327+0530)** - Queries for inhouse Query for detecting LOCKY malware Total number	Feb 6
□	☆	me	**Threats Alert from Saner(2017-02-06T15:00:36.603+0530)** - Threats for inhouse SecPod Default-Locky Ransomware Total number	Feb 6
□	☆	me	**Threats Alert from Saner(2017-02-06T14:55:31.282+0530)** - Threats for inhouse SecPod Default-Locky Ransomware Total number	Feb 6
□	☆	me	**Queries Alert from Saner(2017-02-06T14:40:26.435+0530)** - Queries for inhouse comp-win Total number of hosts affected (deduced	Feb 6
□	☆	me	**Queries Alert from Saner(2017-02-06T14:35:15.080+0530)** - Queries for inhouse AntivirusInfo Total number of hosts affected (dedu	Feb 6
□	☆	me	**Queries Alert from Saner(2017-02-06T13:25:04.351+0530)** - Queries for inhouse AntivirusInfo Total number of hosts affected (dedu	Feb 6
□	☆	me	**Queries Alert from Saner(2017-02-06T12:59:55.202+0530)** - Queries for inhouse Query for detecting LOCKY malware Total number	Feb 6

Email Alerts



Compliance Alert from Saner(2017-01-31T22:24:35.957-0800)

[redacted]@gmail.com
to me

Compliance for validation

CCE-41478-9

Total number of hosts affected (deduced at the time of alert): 1
Affected Hosts (updated/added to the list): vm5-win-10-99
Detected On: 2017-02-01 14:16:34

CCE-41482-1

Total number of hosts affected (deduced at the time of alert): 1
Affected Hosts (updated/added to the list): vm5-win-10-99
Detected On: 2017-02-01 14:16:34

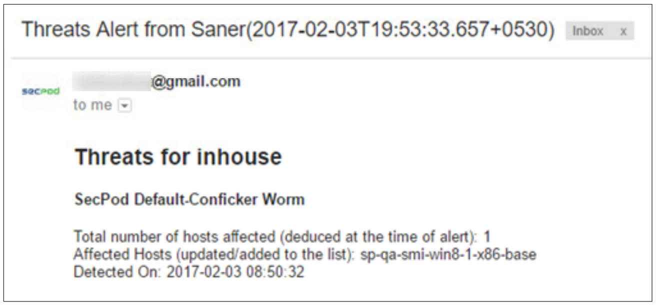
CCE-41483-9

Total number of hosts affected (deduced at the time of alert): 1
Affected Hosts (updated/added to the list): vm5-win-10-99
Detected On: 2017-02-01 14:16:34

CCE-41486-2

Total number of hosts affected (deduced at the time of alert): 1
Affected Hosts (updated/added to the list): vm5-win-10-99
Detected On: 2017-02-01 14:16:34

Compliance E-Mail Alert



Threats Alert from Saner(2017-02-03T19:53:33.657+0530)

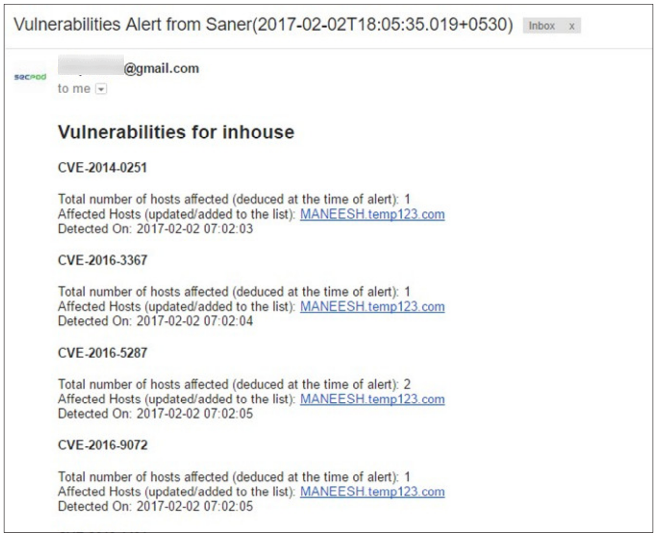
[redacted]@gmail.com
to me

Threats for inhouse

SecPod Default-Conficker Worm

Total number of hosts affected (deduced at the time of alert): 1
Affected Hosts (updated/added to the list): sp-qa-smi-win8-1-x86-base
Detected On: 2017-02-03 08:50:32

Threat Feed E-Mail Alert



Vulnerabilities Alert from Saner(2017-02-02T18:05:35.019+0530)

[redacted]@gmail.com
to me

Vulnerabilities for inhouse

CVE-2014-0251

Total number of hosts affected (deduced at the time of alert): 1
Affected Hosts (updated/added to the list): MANEESH.temp123.com
Detected On: 2017-02-02 07:02:03

CVE-2016-3367

Total number of hosts affected (deduced at the time of alert): 1
Affected Hosts (updated/added to the list): MANEESH.temp123.com
Detected On: 2017-02-02 07:02:04

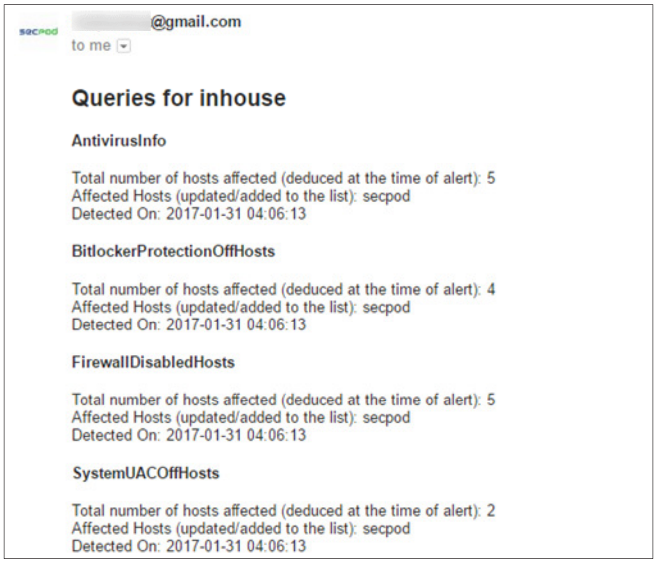
CVE-2016-5287

Total number of hosts affected (deduced at the time of alert): 2
Affected Hosts (updated/added to the list): MANEESH.temp123.com
Detected On: 2017-02-02 07:02:05

CVE-2016-9072

Total number of hosts affected (deduced at the time of alert): 1
Affected Hosts (updated/added to the list): MANEESH.temp123.com
Detected On: 2017-02-02 07:02:05

Vulnerabilities E-Mail Alert



[redacted]@gmail.com
to me

Queries for inhouse

AntivirusInfo

Total number of hosts affected (deduced at the time of alert): 5
Affected Hosts (updated/added to the list): secpod
Detected On: 2017-01-31 04:06:13

BitlockerProtectionOffHosts

Total number of hosts affected (deduced at the time of alert): 4
Affected Hosts (updated/added to the list): secpod
Detected On: 2017-01-31 04:06:13

FirewallDisabledHosts

Total number of hosts affected (deduced at the time of alert): 5
Affected Hosts (updated/added to the list): secpod
Detected On: 2017-01-31 04:06:13

SystemUACOffHosts

Total number of hosts affected (deduced at the time of alert): 2
Affected Hosts (updated/added to the list): secpod
Detected On: 2017-01-31 04:06:13

Queries E-Mail Alert

Viewing Reports

The report settings on the SanerNow dashboard allows administrators to receive or send reports on vulnerabilities, misconfigurations, compliance, assets, devices, and threat indicators. You can email the report or export them to a pdf file. You can configure different backup options for each type of report to maintain, view and analyze the history for security planning and asset optimization.

Note: For reports to be emailed successfully, make sure you have configured your mail server as described in Configuring Mail Settings.

To Generate Reports

- Click **Reports** on the left pane of the dashboard. The report section shows various reports. Select a report you want to view, for example, **Executive Report.**
  - **Executive Report** — This report provides a summary of monitored devices, vulnerability, configuration, and compliance risks, and threat indicators.
  - **Endpoint Management Report** — This report highlights new and unscanned devices, the device group and types, the device details, and the actions taken on specific devices and their status.
  - **Asset Report** - This report provides a count of all assets, a count of all operating system, software and hardware licenses with details, and a list of blacklisted and rarely used applications.
  - **Vulnerability Report** - This report provides vulnerability details based on the device groups and specific devices, categorized by severity, as well as the vulnerabilities grouped by asset.
  - **Patch Report** - This report provides a list of missing patches and vulnerable hosts for each asset, patch aging, patch history, and a list of failed patches
  - **Compliance Report** - This report provides compliance benchmark for hosts and assets, and displays details based on the benchmark rule.
  - **Threat Indicator Report** - This report provides a view of all threats, and a summary of all actions taken to fix vulnerabilities, misconfigurations, and threats.

To export the report to a PDF

- Click Export > PDF

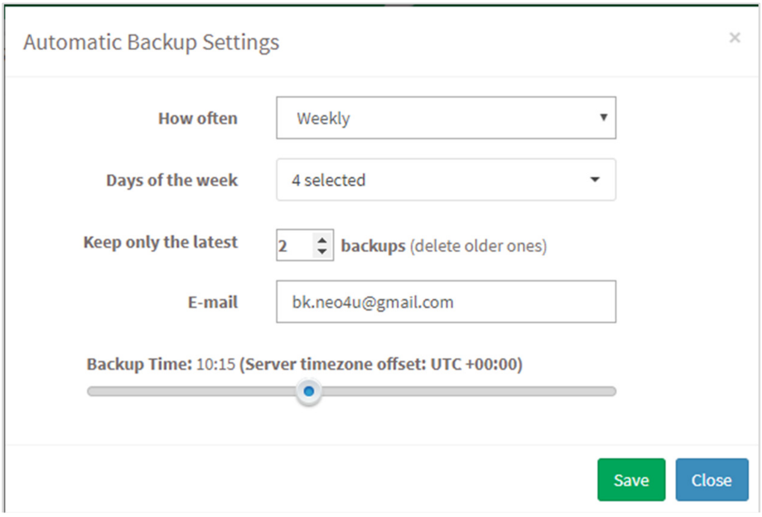
To send the report via email:

1. Click Export > Email.
2. Specify the email IDs to which you wish to send the report.

To Back Up Reports

The backup settings under Reports allow IT administrators to maintain a history of the security posture and endpoint devices on the network. The backup time should be scheduled. The backup report can be scheduled to run automatically daily or weekly.

1. Select the desired report, for example, **Executive Report.**
2. Click **Backup**.
3. Select the weekly or daily option to back up the reports in the **How often** drop down.
4. In the **Keep only the latest entry**, set a number. The report for the specified number of days is archived. If the number is "3" and the backup option is daily, then the reports from the last 3 days are maintained. Older files are deleted.
5. Enter the email address to which the report must be sent.
6. Set the time when the backup should take place, for example 10:00. The backup report is generated every day at 10:00 and is sent to the email address entered in the e-mail field.
7. Click **Save**.



Automatic Backup Settings

How often: Weekly

Days of the week: 4 selected

Keep only the latest: 2 backups (delete older ones)

E-mail: bk.neo4u@gmail.com

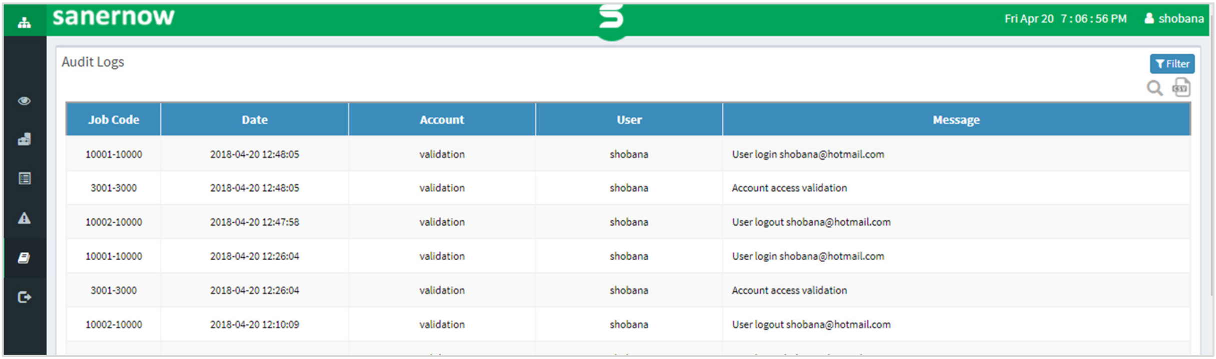
Backup Time: 10:15 (Server timezone offset: UTC +00:00)

Following the Audit Trail

SanerNow supports multiple client accounts and multiple users for each account; and each user can take varied actions based on the privileges of the role. Therefore, in order to maintain security and compliance or to fix issues, it may become necessary to trace the history of actions.

To view, download or filter the audit logs

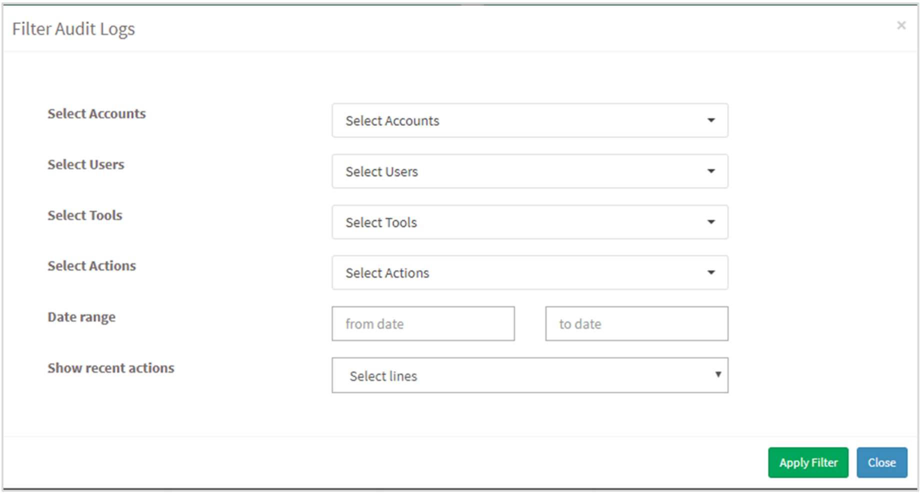
- Click **Audit Logs** on the left pane of the dashboard. The Audit Logs page is displayed with the details of date on which an action was taken, the user who performed that action, and the account on which it was performed.



Audit Logs

Job Code	Date	Account	User	Message
10001-10000	2018-04-20 12:48:05	validation	shobana	User login shobana@hotmail.com
3001-3000	2018-04-20 12:48:05	validation	shobana	Account access validation
10002-10000	2018-04-20 12:47:58	validation	shobana	User logout shobana@hotmail.com
10001-10000	2018-04-20 12:26:04	validation	shobana	User login shobana@hotmail.com
3001-3000	2018-04-20 12:26:04	validation	shobana	Account access validation
10002-10000	2018-04-20 12:10:09	validation	shobana	User logout shobana@hotmail.com

- You can download the audit log as an Excel file or you can search through the audit log.
- If the audit log is long, you can apply filters to view only specific sections of the log – by the account on which actions were taken, the users who have taken action, the area or tool to which the action was related such as vulnerability management, patch management, etc., the specific actions of the users related to that tool, a date range within which you want to trace the actions, and the number of lines you want to limit the log file to.



Click Apply Filter to narrow your search.

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