

Document Version: 5.1

Published Date: 9<sup>th</sup> April 2022

## Table of Contents

<b>Overview of Network Scanner Feature in SanerNow .....</b>	<b>2</b>
<b>Pre-requisites.....</b>	<b>2</b>
<b>Workflow of Network Scanner Feature in SanerNow.....</b>	<b>3</b>
<b>Installing and Configuring Network Scanner Feature in SanerNow .....</b>	<b>3</b>
<b>Scanners .....</b>	<b>8</b>
<b>Scan Config .....</b>	<b>10</b>
<b>Scan Policy .....</b>	<b>13</b>
<b>Logs .....</b>	<b>17</b>

## Overview of Network Scanner Feature in SanerNow

An organization's IT infrastructure consists of various devices like endpoints, hubs, switches, routers, repeaters, gateways, and bridges. Vulnerabilities exist across all these devices, and the vulnerability management solution must be equipped to handle the security loopholes across all. SecPod Saner Now's in-built network scanner detects the vulnerabilities across all the IP-enabled devices in the network. This network scanner worked on a hub and spoke model and utilizes the existing devices to work as scanners. This saves additional investments on extra appliances or hardware.

SanerNow offers the industry's fastest vulnerability scanning and leverages the home-grown world's most extensive SCAP feed with over 130,000 plus vulnerabilities. With SanerNow, you can seamlessly scan, detect, assess, prioritize, and report network vulnerabilities from the same console. SecPod SanerNow provides a full-fledged vulnerability management solution with integrated patch remediation capability. The SanerNow patch management application allows you to remediate the software vulnerabilities across your endpoints.

Following are the top capabilities of the Network Scanner feature:

- Detect network topology, devices, operating system, and service fingerprinting across all IP-enabled devices.
- Automatic detection of potential network scanners and designate them as a network scanner.
- Discover vulnerabilities and misconfigurations in the network-enabled devices and network devices.
- Perform external security posture analysis of endpoint devices.
- No additional hardware procurement costs are involved. Our customers can use existing hardware and promote eligible endpoints to network scanners in SanerNow through simple steps.
- The scanner is built on a distributed hub and spoke model that distributes the scanning responsibility, thus reducing scan times and making the process effortlessly continuous.
- Automate daily scans to achieve increased productivity in maintaining overall security posture.
- Perform remediation checks for the discovered risks and include them in the remediation list.

## Pre-requisites

Network Scanner can be deployed on the devices with these platforms such as Windows Servers and Desktops (Both x64 and x86), Linux (RPM and DPKG) 64bit devices, and Mac OS. We currently do not support Network Scanner on Linux (32bit) and Alpine Linux (32bit and 64bit).

To access the Network Scanner feature, any one of the below services must be provisioned for your account in SanerNow:

- Vulnerability Management
- Compliance Management

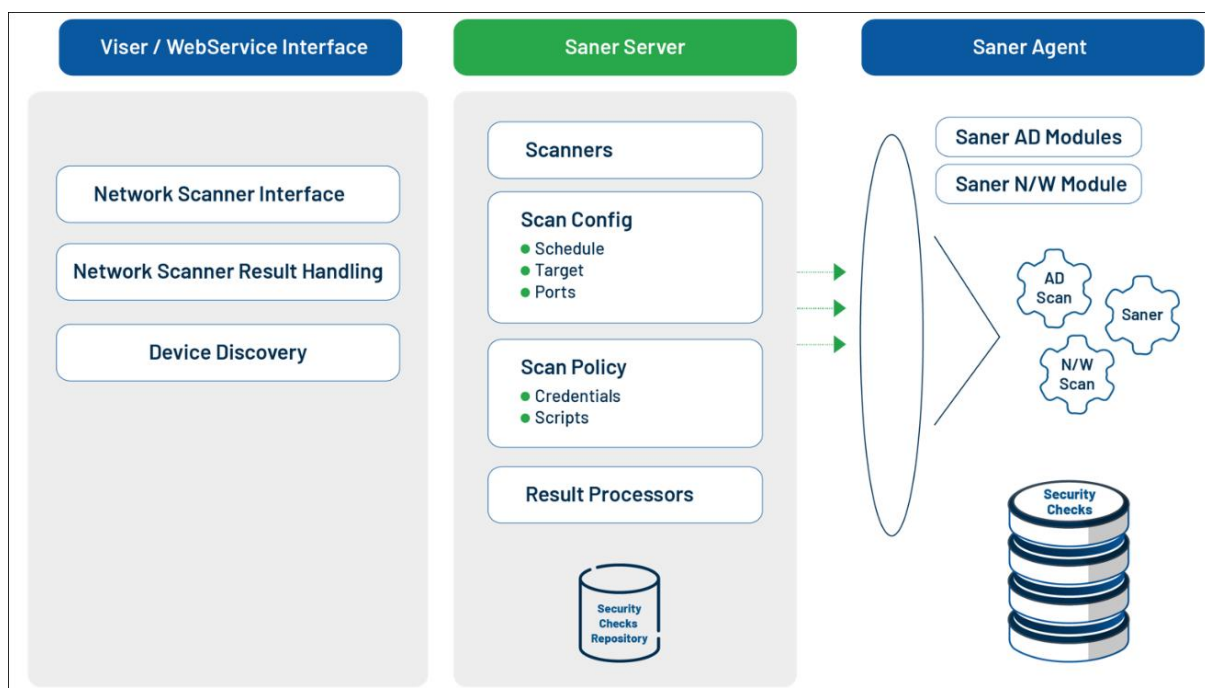
- Asset Exposure

Network Scanner feature is available in SanerNow 5.0.0.0 and newer versions.

## Workflow of Network Scanner Feature in SanerNow

**Upgrade Saner agent as a Network Scanner:** The user will designate the agent as a network scanner. The server will communicate to the agent, and the agent will download the network scanner module and upgrade it. The newly designated network is listed on the Scanner page in the SanerNow console.

**Configure Network Scanner:** The user configures the network scan and defines the scan policy. User selects IP ranges, various vulnerabilities, and misconfiguration scripts for a scan. Scan configuration defines the range of targets to scan and the schedule for performing the scan. Scan policy specifies the scripts to launch.



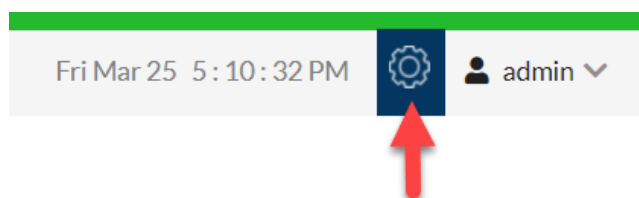
## Installing and Configuring Network Scanner Feature in SanerNow

Endpoint devices can be designated as network scanners in two ways:

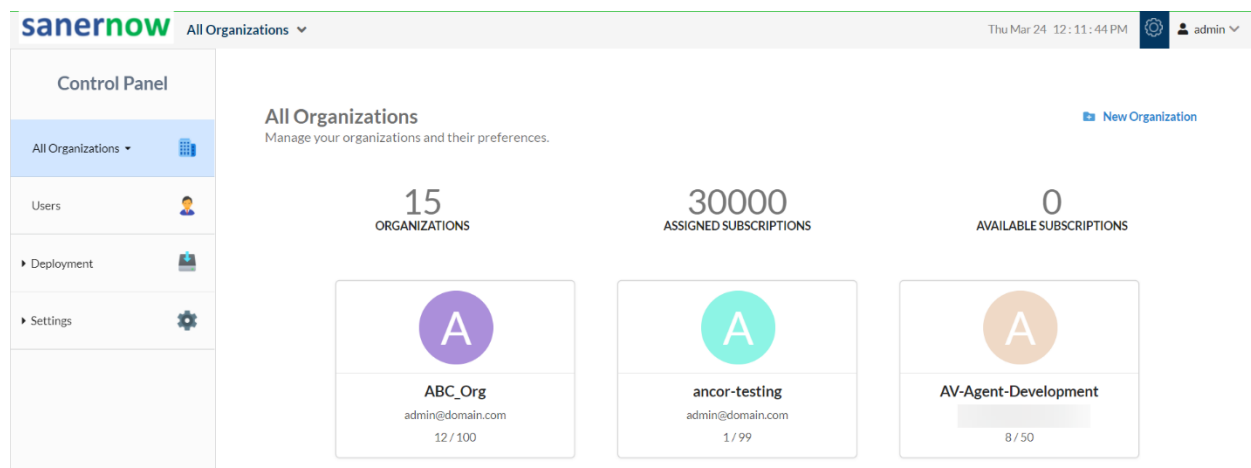
- **Designate endpoint device as a network scanner:** Select an existing Saner agent and upgrade it as a network scanner. Users can do this from the **wizard mode** or the **Scanners** page.
- **Deploy a new Saner agent and upgrade it as a network scanner:** Select the endpoint device, deploy a Saner agent, and then upgrade it as a network scanner. This will be done from the wizard mode.

**To designate the endpoint device as a network scanner from the wizard mode, follow the below steps:**

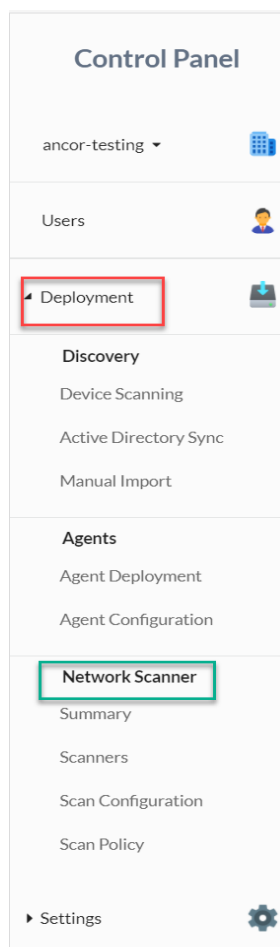
**Step 1:** Log in to SanerNow and then click **Control Panel** at the top-right to access the **Control Panel** page



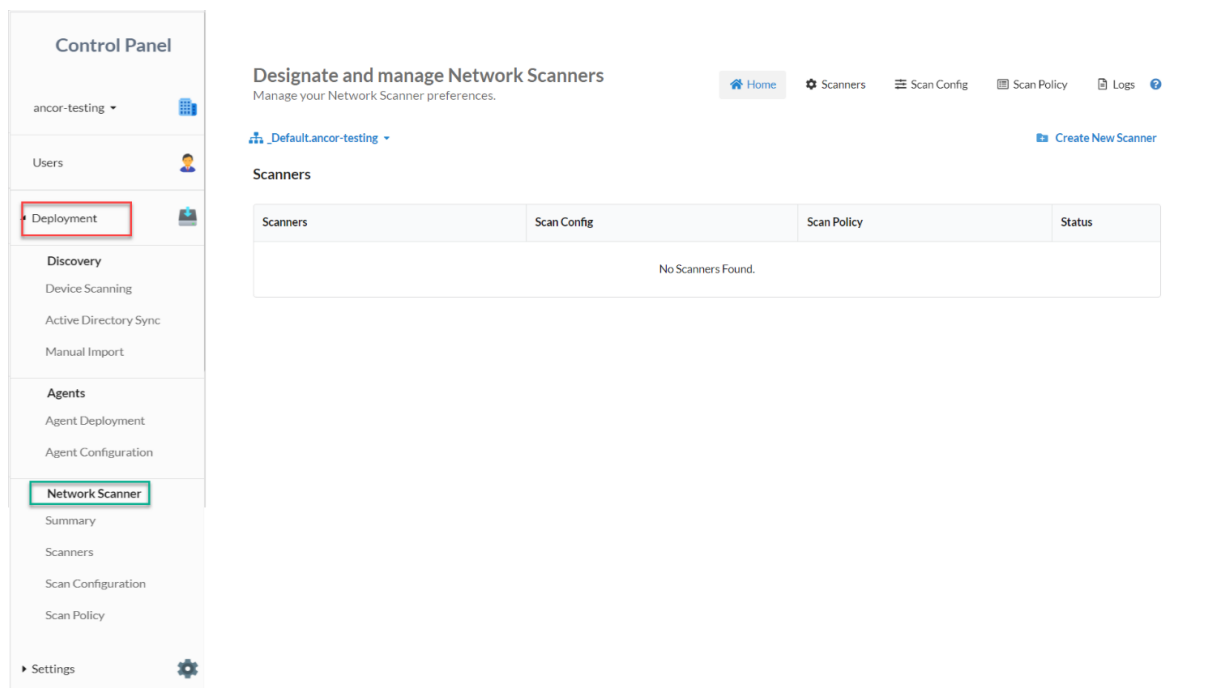
**Step 2:** Select an organization from the dropdown menu on the left under Control Panel.



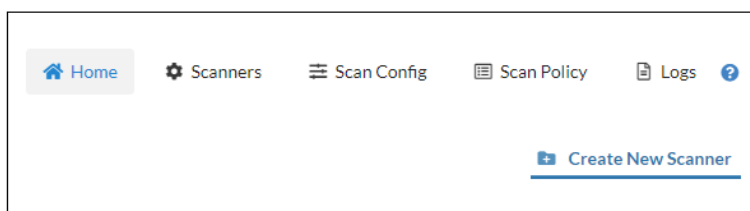
**Step 3:** After selecting the organization in the left sidebar, choose the **Network Scanner** option present in the deployment section.



**Step 4:** The **Home** tab will be empty since the **Network Scanner** is not configured yet.



**Step 6:** Click on the **Create New Scanner** option to create a new scanner.



**Step 7:** Complete the following three steps to create a new scanner: **Scanner Selection**, **Scan Config**, and **Scan Policy**.

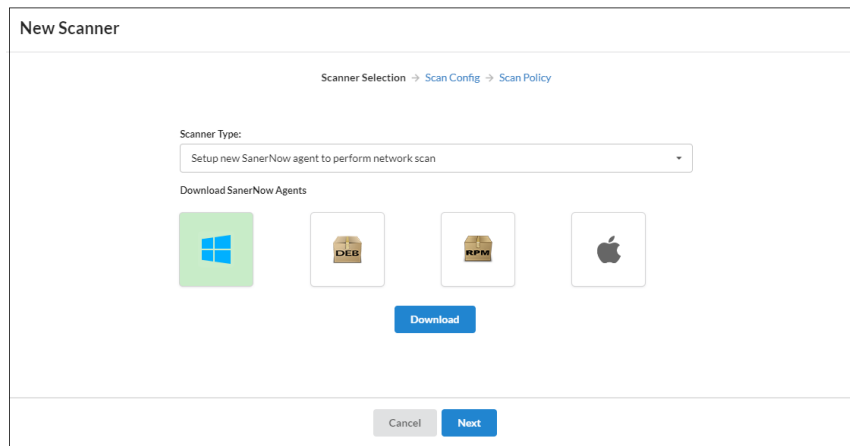
#### a) Scanner Selection

The Scanner Selection section selects the preferred method for choosing a device from the drop-down menu.

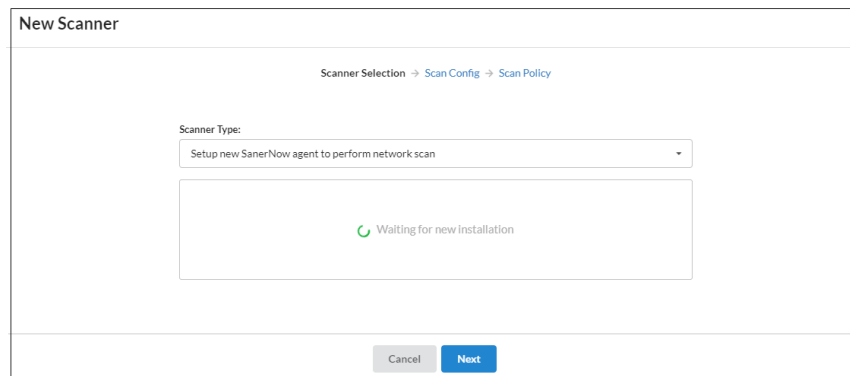
- **Designate SanerNow agent to perform network scan:** Select this option if the Saner agent is already installed and you want to upgrade this device as a network scanner.

The screenshot shows the 'New Scanner' form. At the top, it says 'New Scanner'. Below that, there's a breadcrumb trail: 'Scanner Selection → Scan Config → Scan Policy'. The 'Scanner Type:' dropdown menu is selected with 'Designate SanerNow agent to perform network scan'. The 'Choose a device:' dropdown menu is selected with 'qa-centos-7core-x64'. At the bottom, there are 'Cancel' and 'Next' buttons.

- **Setup a new SanerNow agent to perform network scan:** Select this option if you want to deploy the Saner agent in the device and upgrade it as a network scanner.



Select the operating system to deploy a Saner agent and click on the **Download** button. It will take a few seconds to download the zip file and install the Saner agent through the installer file.



After the installation, the device will be listed in the menu.

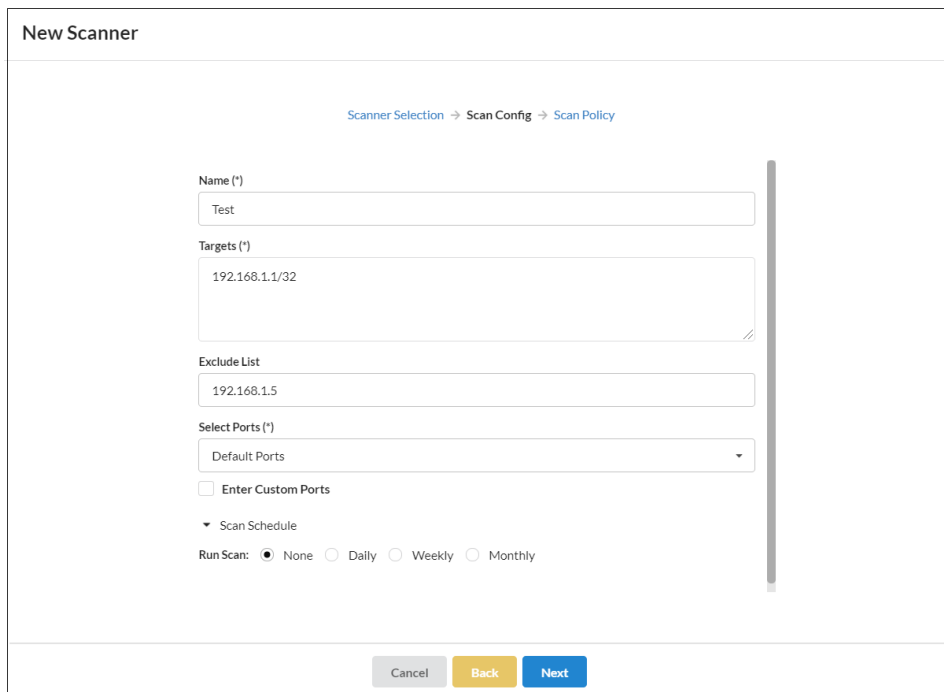
**Choose a device:** Select the device from the list and click on the **Next** button.

## b) Scan Config

Configure the scan by specifying the information in the following fields:

- **Name:** Specify the name to identify the scan configuration.
- **Target:** Specify the comma-separated list of target IP addresses for scanning. This member is an IPv4 address. This field supports CIDR format and domain name as inputs. For example, users can enter IP addresses in the following format: scan an individual IP (192.168.1.1), scan a range of IP (192.168.1.1/32), and scan a subnet (192.168.1.1-10).
- **Exclude List:** Specify a comma-separated list of target IP addresses to be excluded from the scan. This member accepts individual IPv4 addresses. E.g.: 192.168.1.5,192.168.1.6
- **Select Ports:** Specify a comma-separated list of ports to scan. Users can select default ports or customize their own set of TCP/UDP ports based on the configuration. Specify the ports to be scanned. By default, the **Default Ports** option is selected. Click on the drop-down menu to choose the following port options: Top 1000, Top 500, Top 100, and None. Click on the help (?) icon next to Select Ports for more details on the default ports options.

- **Enter Custom Ports:** Users can manually provide the ports to scan by clicking on the **Enter Custom Ports** check box.
  - **TCP Ports:** Specifies a comma-separated list of TCP ports to scan. E.g.: 80 or 21,80 or 1-65535 or 1-1023,3389
  - **UDP Ports:** Specifies a comma-separated list of UDP ports to scan. E.g.: 80 or 21,80 or 1-65535 or 1-1023,3389.
- **Scan Schedule:** The user can schedule a scan to run Daily, Weekly, and Monthly by clicking on the Scan Schedule option. By default, the None option will be selected. Refer to the Scan Config section for more details.



The screenshot shows the 'New Scanner' configuration window, specifically the 'Scan Policy' step. The breadcrumb trail at the top indicates the sequence: [Scanner Selection](#) → [Scan Config](#) → [Scan Policy](#). The form contains the following fields and options:

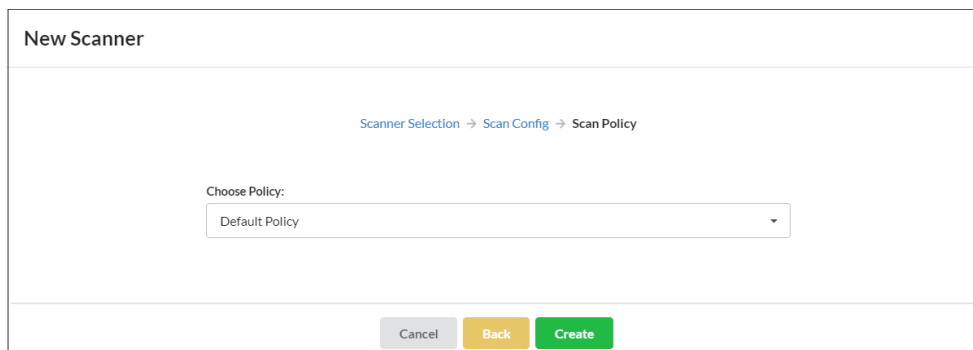
- Name (\*):** A text input field containing 'Test'.
- Targets (\*):** A text input field containing '192.168.1.1/32'.
- Exclude List:** A text input field containing '192.168.1.5'.
- Select Ports (\*):** A dropdown menu currently showing 'Default Ports'.
- Enter Custom Ports:** An unchecked checkbox.
- Scan Schedule:** A section with a dropdown arrow and four radio button options: 'None' (selected), 'Daily', 'Weekly', and 'Monthly'.

At the bottom of the window are three buttons: 'Cancel' (grey), 'Back' (yellow), and 'Next' (blue).

After specifying all the fields, click on the **Next** button.

### c) Scan Policy

Select a scan policy from the drop-down menu. By default, the **Default Policy** will be selected. The list of created policies will be available in the drop-down menu. Users can create their own set of policies for each network they wish to scan. Refer to the Scan Policy section for more details. After selecting the policy from the drop-down menu, click on the **Create** button.

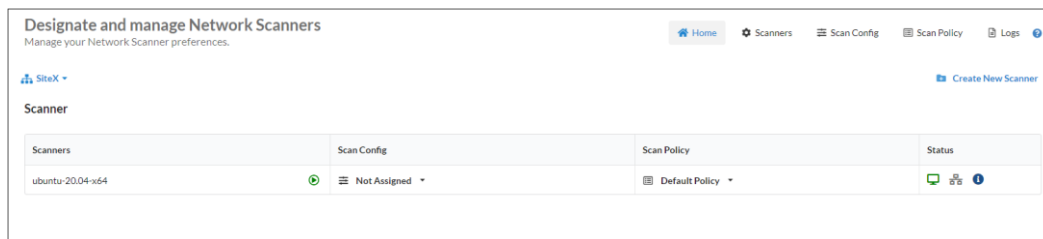


The screenshot shows the 'New Scanner' configuration window, specifically the 'Scan Policy' step. The breadcrumb trail at the top indicates the sequence: [Scanner Selection](#) → [Scan Config](#) → [Scan Policy](#). The form contains the following field and options:

- Choose Policy:** A dropdown menu currently showing 'Default Policy'.

At the bottom of the window are three buttons: 'Cancel' (grey), 'Back' (yellow), and 'Create' (green).

The **Back** option is available for the scan config and scan policy sections to modify any settings. Once the scan profile is completed, the **Home** page will list the newly added scanner and associated scan config and scan policy. Click on the **Scan Now** button from the scanners column to perform a scan.



The home page will list the designated scanners and associated scan config settings, scan policies, and the status. Following is the list of parameters present on the home page.

Parameter	Description
-----------	-------------

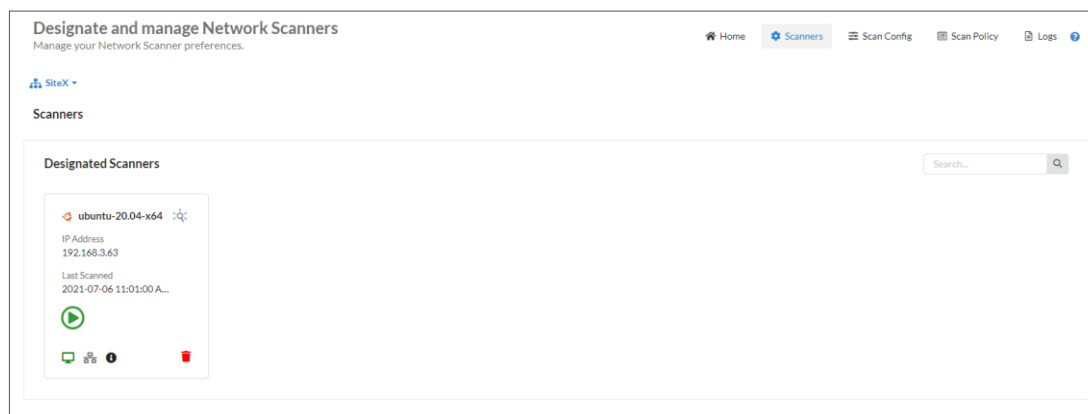
Scanners	It will display a list of designated network scanner devices. You can initiate a scan by clicking on the <b>Scan Now</b> icon. Refer to the Scanners section for more details.
Scan Config	It will display a list of scan configs assigned to the scanners. The drop-down menu will list all the available scan configs, which can be selected and assigned to the scanner. Refer to the Scan Config section for more details.
Scan Policy	It will display a list of scan policies assigned to the scanners. The drop-down menu will list all the available scan policies, which can be selected and assigned to the scanner. Refer to the Scan Policy section for more details.
Status	<p><b>Device Status</b> icon – This icon shows the status of the device – Active or Inactive.</p> <p><b>Network Scanner Status</b> icon – This icon shows the scan status of the Network Scanner.</p> <p><b>Information</b> icon – The last scan information is displayed by clicking on the "i" icon.</p>

## Scanners

The Saner agents can be upgraded as network scanners through the **Scanners** page. This page displays a list of designated scanners and endpoint devices.




- **Designated Scanners:** This section lists the designated network scanners. It will display the Hostname, IP address, last scan date, and each network scanner.





Users can perform the following actions from this section:

- **Scan Now** button: The scan is initiated by clicking the **Scan Now** button. Once the scan is started, the **Abort Scan** button will appear. Users can stop the scan by clicking on the abort scan button.
- **Device Status** icon: Shows the status of the device - Active or Inactive.
- **Network Scanner Status** icon: Display the status of the network scanner. Following is the list of scan statuses:
  - Upgrade waiting - Upgrading the device as a network scanner will initiate soon
  - Upgrading - Upgrading the device as a network scanner is in progress
  - Upgrade failed - Failed to upgrade device as a network scanner
  - Scan waiting - Perform a network scan will initiate soon
  - Scanning - Network scan is ongoing
  - Scan failed - Network scan failed
  - Abort waiting – Need to abort network scan
  - Scan aborted - Network scan is aborted
  - Idle - Device is idle (not performing any task)
- **Information** icon: Click the icon to get the last scan information.
- **Delete** icon: Remove the network scanner device from the designated scanners list.
- **Devices Available:** This section shows the list of endpoint devices and their device information - Hostname, IP Address, Mac address, Operating System, CPU, RAM, DHCP Status, device status - and Action column. Users can choose one or more devices by clicking the checkboxes on the left and clicking the **Designate** button on the right to promote these endpoints as network scanners.

Devices Available <input checked="" type="checkbox"/> Show only recommended devices 									
All Subnets		All Family		All Groups		All OS		Action: <b>Designate (1)</b>	
								Search...	
<input type="checkbox"/>	Host Name	IP Address	Mac Address	Operating System	CPU	RAM	DHCP Status	Status	Action
<input checked="" type="checkbox"/>	desktop-jrk1r4a	192.168.2.117	12-78-1D-04-1C-0E	Microsoft Windows 10 v2004 ar...	Common KVM processor	4.0 GiB	yes		<b>Designate</b>
<input type="checkbox"/>	desktop-h2bvv86 111...	192.168.3.110	3A-7D-5A-41-92-20	Microsoft Windows 10 v2004 ar...	Common KVM processor	4.0 GiB	yes		<b>Designate</b>

Showing 1 to 1 of 1 entries

Previous 1 Next

The search option is provided to list the devices. Users can also filter the devices by the subnets, family, group, Operating System, and device status. By default, the **"Show only recommended devices"** filter option is selected that will list the recommended devices based on the below parameters:

- One device per subnet
- Server system
- Desktop
- Based on high CPU and RAM capacity
- Device uptime

**Note:** Linux (32-bit) and Linux Alpine (32-bit and 64-bit) devices are not supported for upgrading as a Network Scanner.

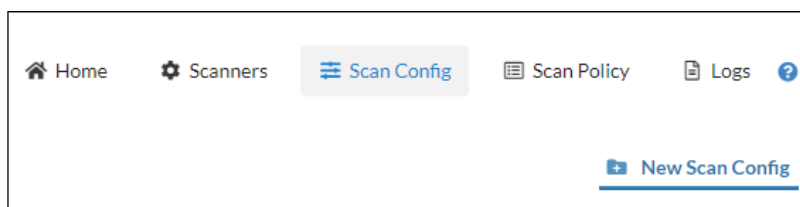
## Scan Config

Scan config is to define the range of targets and ports available in the network to perform a scan. Users can specify the targets and ports and schedule a scan from the Scan Config page. This page lists all the scan configs with a scan config name, description, targets, ports, and actions.

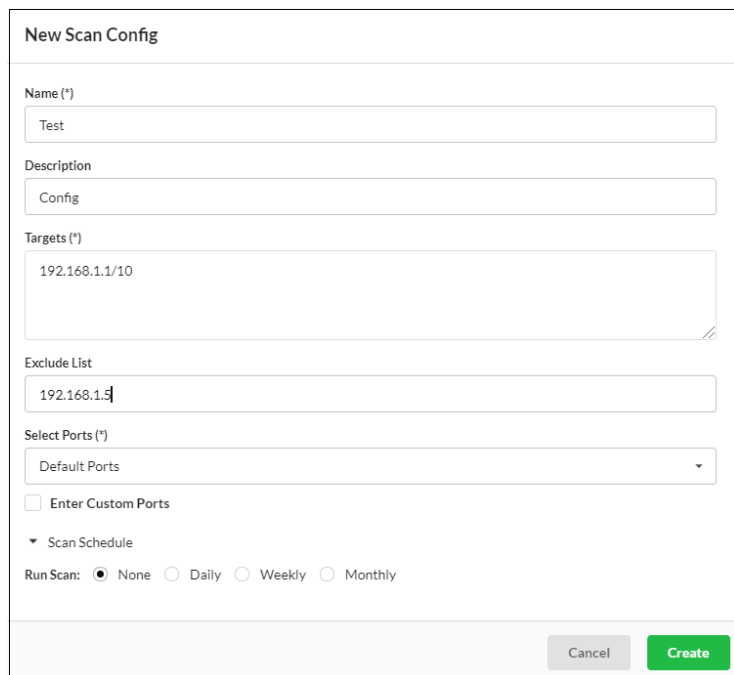
Designate and manage Network Scanners Manage your Network Scanner preferences.					
SiteX			<a href="#">Home</a> <a href="#">Scanners</a> <a href="#">Scan Config</a> <a href="#">Scan Policy</a> <a href="#">Logs</a>		
New Scan Config					
<input type="checkbox"/>	Name	Description	Targets	Ports	Action
<input type="checkbox"/>	Scan-config-01	Demo	192.168.3.176	Top 100 TCP: 2375,8080,9000,100,90,80,70,60,50,40,30,20,10 UDP: 2375,8080,161,9000,100,90,80,70,60,50,40,30,20...	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/>	three step wizard	three_step_wizard	192.168.2.185	Default Ports	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/>	full network scan	test-01	192.168.2.0/24	Default Ports	<a href="#">Edit</a> <a href="#">Delete</a>

**Complete the following steps to create a new scan config:**

**Step 1:** Click on the **New Scan Config** icon to create a new scan configuration.



**Step 2:** Provide the required information on the new scan config window below.



**New Scan Config**

Name (\*)

Description

Targets (\*)

Exclude List

Select Ports (\*)

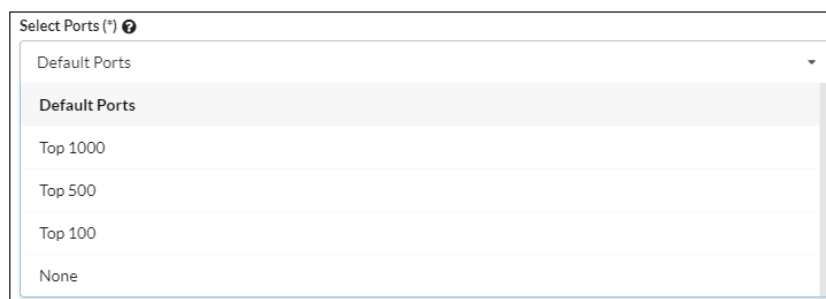
☐ Enter Custom Ports

▼ Scan Schedule  
 Run Scan: ☒ None ☐ Daily ☐ Weekly ☐ Monthly

Following is the list of fields with descriptions:

- a) **Name** – Specify the name for the scan configuration.
- b) **Description** – Specify the description of the scan configuration.
- c) **Targets** – Specify the comma-separated list of target IP addresses for scanning. This member is an IPv4 address. This field supports CIDR format and domain name as inputs. E.g.: 192.168.1.1 or 192.168.1.1/32 or 192.168.1.1-10.
- d) **Exclude List** – Specifies a comma-separated list of target IP addresses excluded from the scan. This member is an IPv4 address. E.g.: 192.168.1.5,192.168.1.6.
- e) **Select Ports** – Specify a comma-separated list of ports to scan. Users can select default ports or customize their own set of TCP/UDP ports based on the configuration.

Select the ports option from the **Select Ports** drop-down menu. By default, the **Default Ports** option is selected. Click on the drop-down menu to choose the port options: Top 1000, Top 500, Top 100, and None. Click on the help (?) icon next to Select Ports for more details on the default port options.

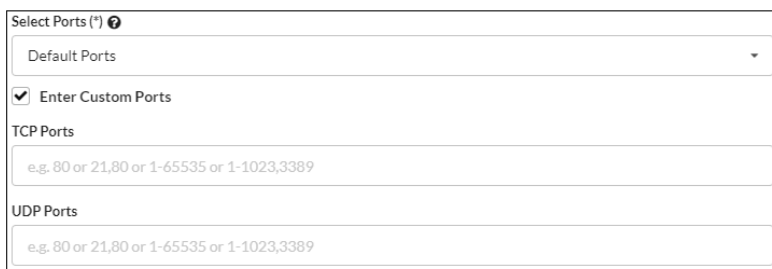


Select Ports (\*) ?

Default Ports ▼

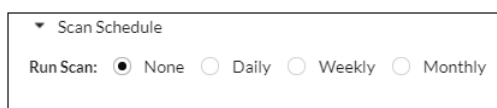
- Default Ports
- Top 1000
- Top 500
- Top 100
- None

- **Enter Custom Ports:** Click on the **Enter Custom Ports** check box to manually provide the TCP and UDP ports.
  - **TCP Ports:** Specifies a comma-separated list of TCP ports to scan. E.g.: 80 or 21,80 or 1-65535 or 1-1023,3389
  - **UDP Ports:** Specifies a comma-separated list of UDP ports to scan. E.g.: 80 or 21,80 or 1-65535 or 1-1023,3389

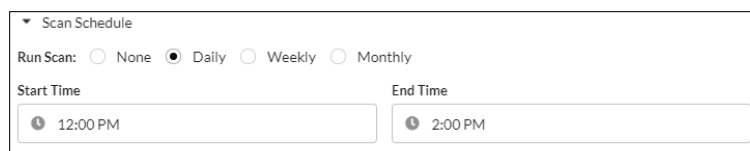


- f) **Scan Schedule** – The user can schedule a scan to run Daily, Weekly, and Monthly by clicking on the **Scan Schedule** option. By default, the **None** option will be selected.

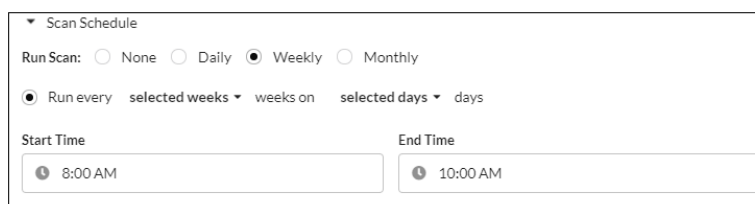
- **None:** A network scan has to be manually triggered.



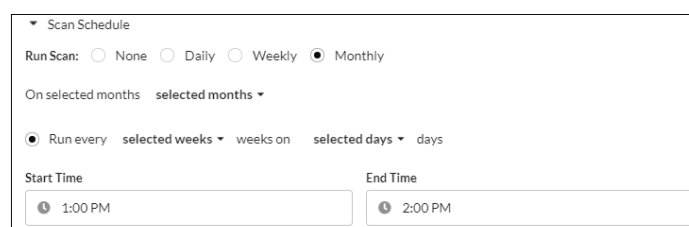
- **Daily:** Every day, a network scan will be initiated at a specific HH: MM time.



- **Weekly:** A network scan will be initiated on a specific day/s every week at HH: MM time.



- **Monthly:** A network scan will be initiated on a specific day/s of every month at HH: MM time.



**Step 3:** Click on the **Create** button after specifying all the fields. A new scan config entry is displayed on the **Scan Config** page.

**Step 4:** If you want to modify the scan config, click on the **Edit** icon from the Action column. Make the changes and click on the **Update** button to save the changes.

### Edit Scan Config

Name (\*)

Scan-config-01

Description

Demo

Targets (\*)

192.168.3.176

Exclude List

e.g. 192.168.1.10 (Comma separated IP address)

Select Ports (\*)

Top 100

☐ Enter Custom Ports

Scan Schedule

Cancel

Update

**Step 5:** If you want to remove the scan config, select the scan config and click on the **Delete** icon.

Designate and manage Network Scanners

Manage your Network Scanner preferences.







[Home](#)
[Scanners](#)
[Scan Config](#)
[Scan Policy](#)
[Logs](#)

[SiteX](#)

Actions:

New Scan Config

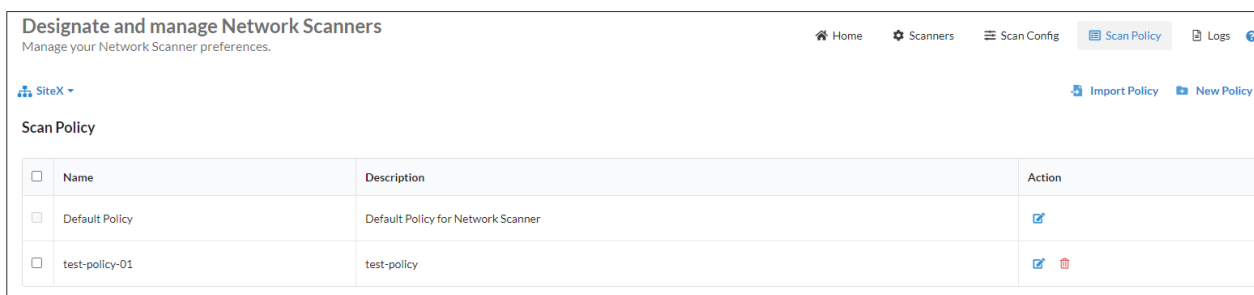
Scan Config

<input type="checkbox"/>	Name	Description	Targets	Ports	Action
<input checked="" type="checkbox"/>	Scan-config-01	Demo	192.168.3.176	Top 100 TCP: 2375,8080,9000,100,90,80,70,60,50,40,30,20,10 UDP: 2375,8080,161,9000,100,90,80,70,60,50,40,30,20,...	 
<input checked="" type="checkbox"/>	three step wizard	three_step_wizard	192.168.2.185	Default Ports	 
<input type="checkbox"/>	full network scan	test-01	192.168.2.0/24	Default Ports	 

**Note:** Edit and Delete options will be disabled for the Scan Config when the scan is ongoing on the assigned device.

## Scan Policy

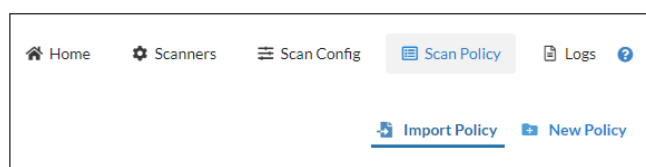
The scan policy is to run particular scripts to detect applications and vulnerabilities. Select a family and scripts based on the network. The scan policy page shows the specified name for the policy, description, and action columns. The default policy will be selected if the user has not created the scan policy. This default policy will execute all the applications and services that SanerNow supports.



Users can create a new policy or import the policy from different organizations/accounts.

The import option is available to copy the policy from other organizations/accounts instead of creating a new policy. Follow the below steps to import policy:

**Step 1:** Click on the **Import Policy** option from the Scan Policy page, as shown in the image.



**Step 2:** Select the organization, account, and policy and click on the **Import** button. The imported policy will be displayed on the scan policy page.

Import Policy

Organisation\*

Org 2

Accounts\*

SiteX

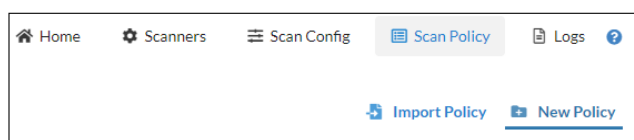
Policies\*

test-policy-01

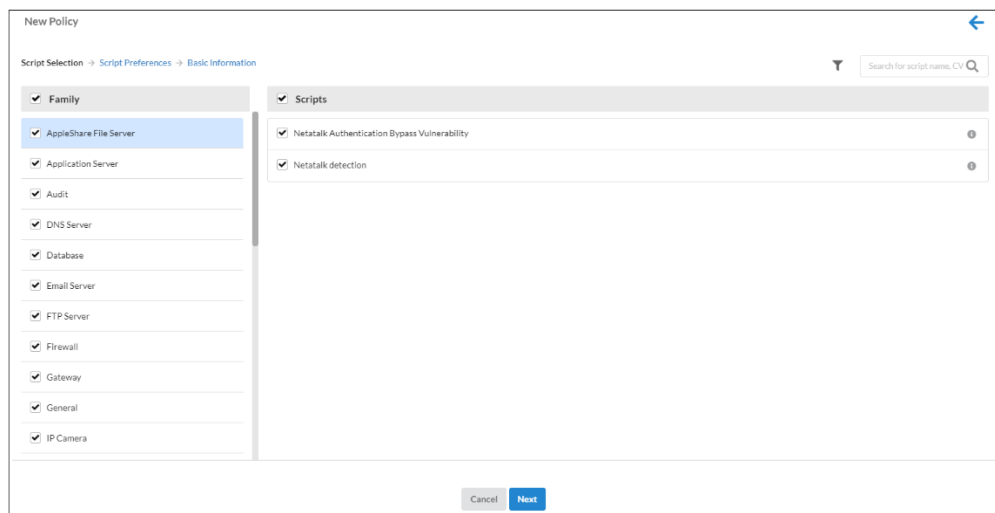
Import

To create a new scan policy, complete the following steps:

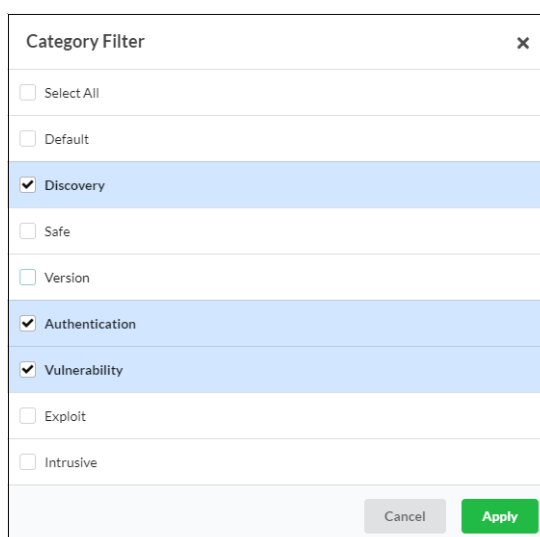
**Step 1:** Click on the **New Policy** option from the Scan Policy page to create a new scan policy.



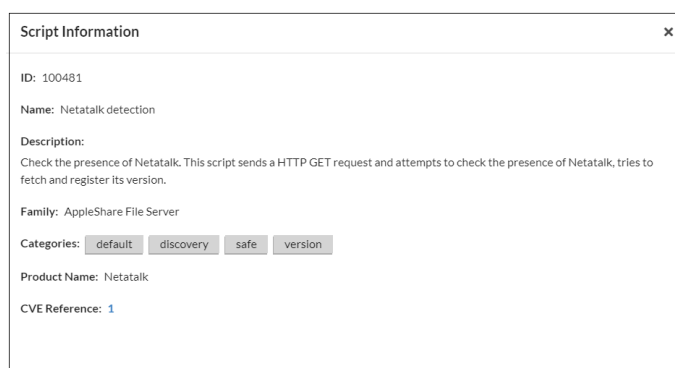
**Step 2: Script Selection:** This section list scripts required to run vulnerability check. Choose a Family and Scripts based on the devices and applications in the network. Exclude the family and scripts you don't want to run by unchecking the box.



Apply the filter to view specific scripts. Select one or more filters and click on the **Apply** option to filter the scripts based on the selected category.

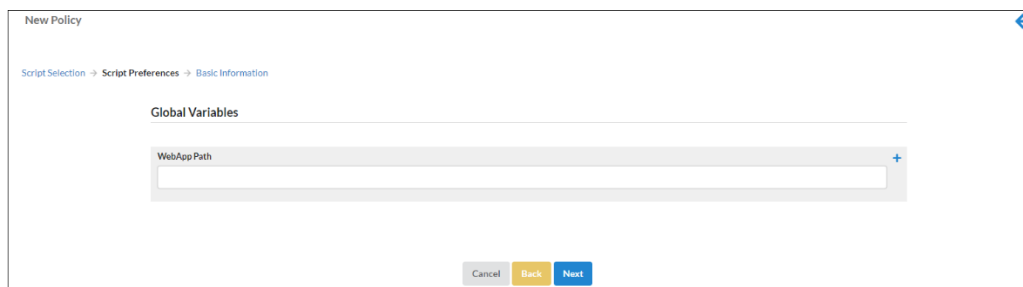


In addition, the search option is provided to search the scripts with multiple search options, along with the CVE and SVE numbers. The “i” icon will display detailed information about the script.

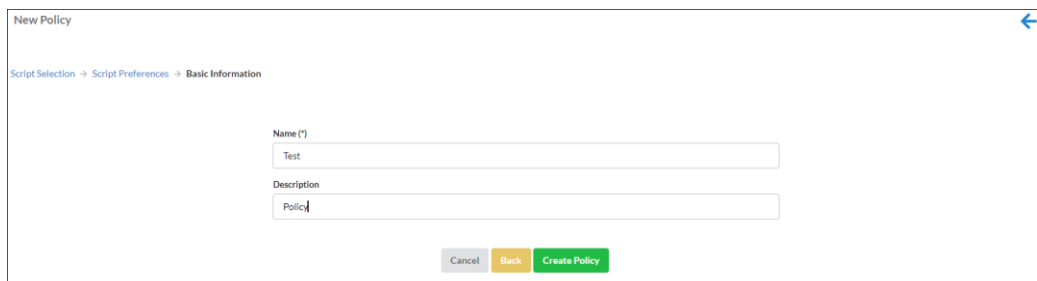


**Step 3:** Click on the **Next** button after selecting the scripts.

**Step 4: Script Preferences:** After the script selection, provide the **WebApp Path** to run scripts. This section will display the global variables based on the script selection.



**Step 5: Basic Information:** Enter the **Name** and **Description** in the respective field and click on the **Create Policy** button.



Once the policy is created successfully, it will appear on the Scan Policy page and its Name, Description, and Action columns.

Designate and manage Network Scanners  
Manage your Network Scanner preferences.

Home Scanners Scan Config **Scan Policy** Logs

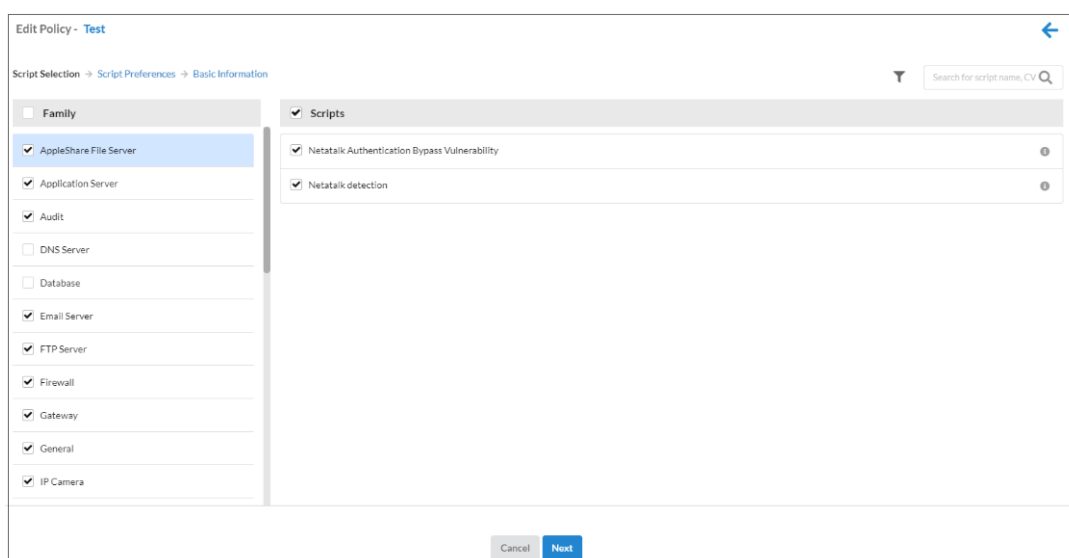
SiteX Import Policy New Policy

Scan Policy

<input type="checkbox"/>	Name	Description	Action
<input type="checkbox"/>	Default Policy	Default Policy for Network Scanner	<a href="#">✎</a>
<input type="checkbox"/>	test-policy-01	test-policy	<a href="#">✎</a> <a href="#">✖</a>
<input type="checkbox"/>	Test	Config	<a href="#">✎</a> <a href="#">✖</a>

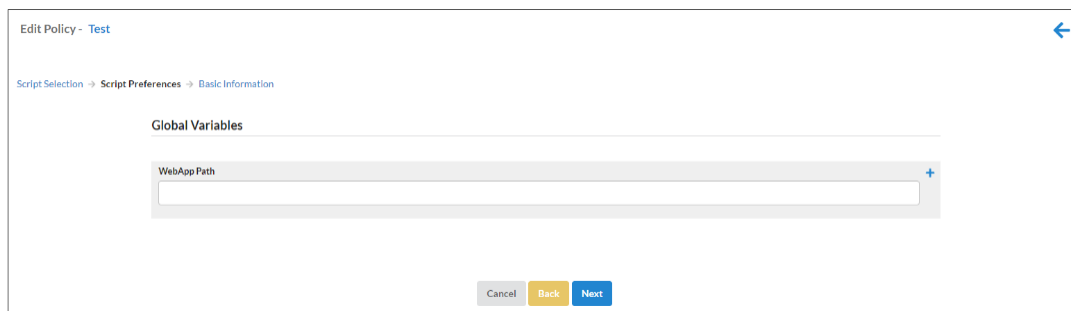
**Step 6:** To modify an existing scan policy, complete the following steps:

1. Click on the **Edit** icon from the **Action** column.

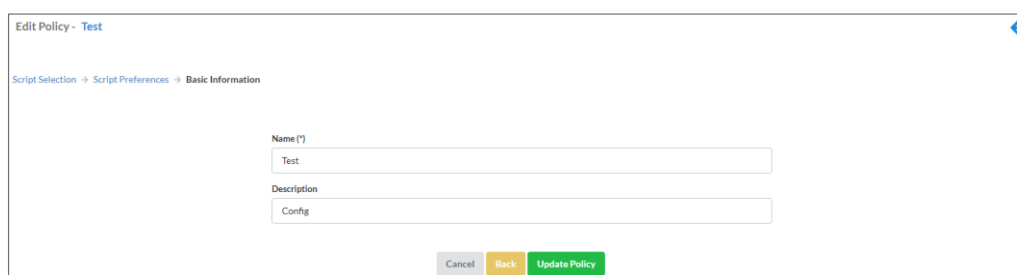




2. Make the changes in the script selection and click on the **Next** button.

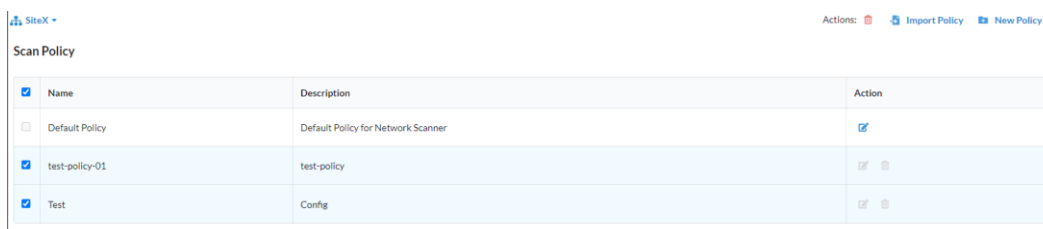


3. Make the changes in the **Basic Information** and click on the Update Policy button to save the changes.



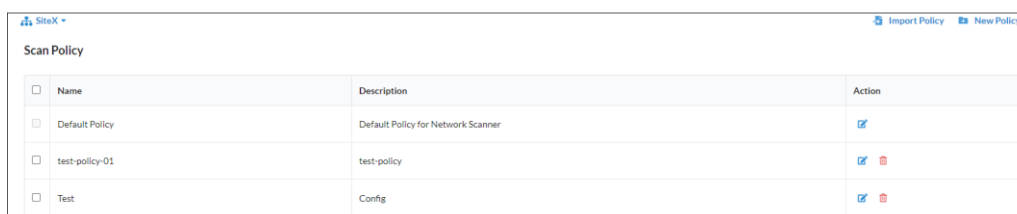
**Step 7:** To remove existing scan policies, complete the following steps:

1. Select the scan policies to be deleted and click on the **Delete** icon at the top.



<input checked="" type="checkbox"/>	Name	Description	Action
<input type="checkbox"/>	Default Policy	Default Policy for Network Scanner	
<input checked="" type="checkbox"/>	test-policy-01	test-policy	
<input checked="" type="checkbox"/>	Test	Config	

2. Alternatively, the Delete icon on the right of each individual policy can be clicked to delete that specific policy.



<input type="checkbox"/>	Name	Description	Action
<input type="checkbox"/>	Default Policy	Default Policy for Network Scanner	
<input type="checkbox"/>	test-policy-01	test-policy	
<input type="checkbox"/>	Test	Config	

**Note:** Edit and Delete options will be disabled for the Scan Policy when the scan is ongoing on the assigned device.

## Logs

Lists logs of all actions associated with the **Network Scanner feature**. It will display detailed information such as Job code, Date, Organization, Account, User, and Message. If the audit logs are more, users can

apply filters to view specific sections of the logs. Users can filter the logs – by the account on which actions were taken, the users who have taken action, a date range within which you want to trace the actions, and the number of lines to limit the log file.

Designate and manage Network Scanners					
Manage your Network Scanner preferences.					
<div> <a href="#">Home</a> <a href="#">Scanners</a> <a href="#">Scan Config</a> <a href="#">Scan Policy</a> <a href="#">Logs</a> </div>					
Logs					
<div> Size: 10 Filter By: Accounts Users Start Date End Date Clear All </div>					
Job Code	Date	Organization	Account	User	Message
14000-14023	2021-07-10 12:43:06 AM IST	Demo Organization	SiteX	demo	Initiated network scan in device ubuntu-20.04-x64
14000-14048	2021-07-10 12:43:15 AM IST	Demo Organization	SiteX	demo	Network scan failed in device ubuntu-20.04-x64
14000-14026	2021-07-10 12:43:56 AM IST	Demo Organization	SiteX	demo	Updated scan configuration for My Scan Config
14000-14023	2021-07-10 12:44:07 AM IST	Demo Organization	SiteX	demo	Initiated network scan in device ubuntu-20.04-x64
14000-14048	2021-07-10 12:44:16 AM IST	Demo Organization	SiteX	demo	Network scan failed in device ubuntu-20.04-x64

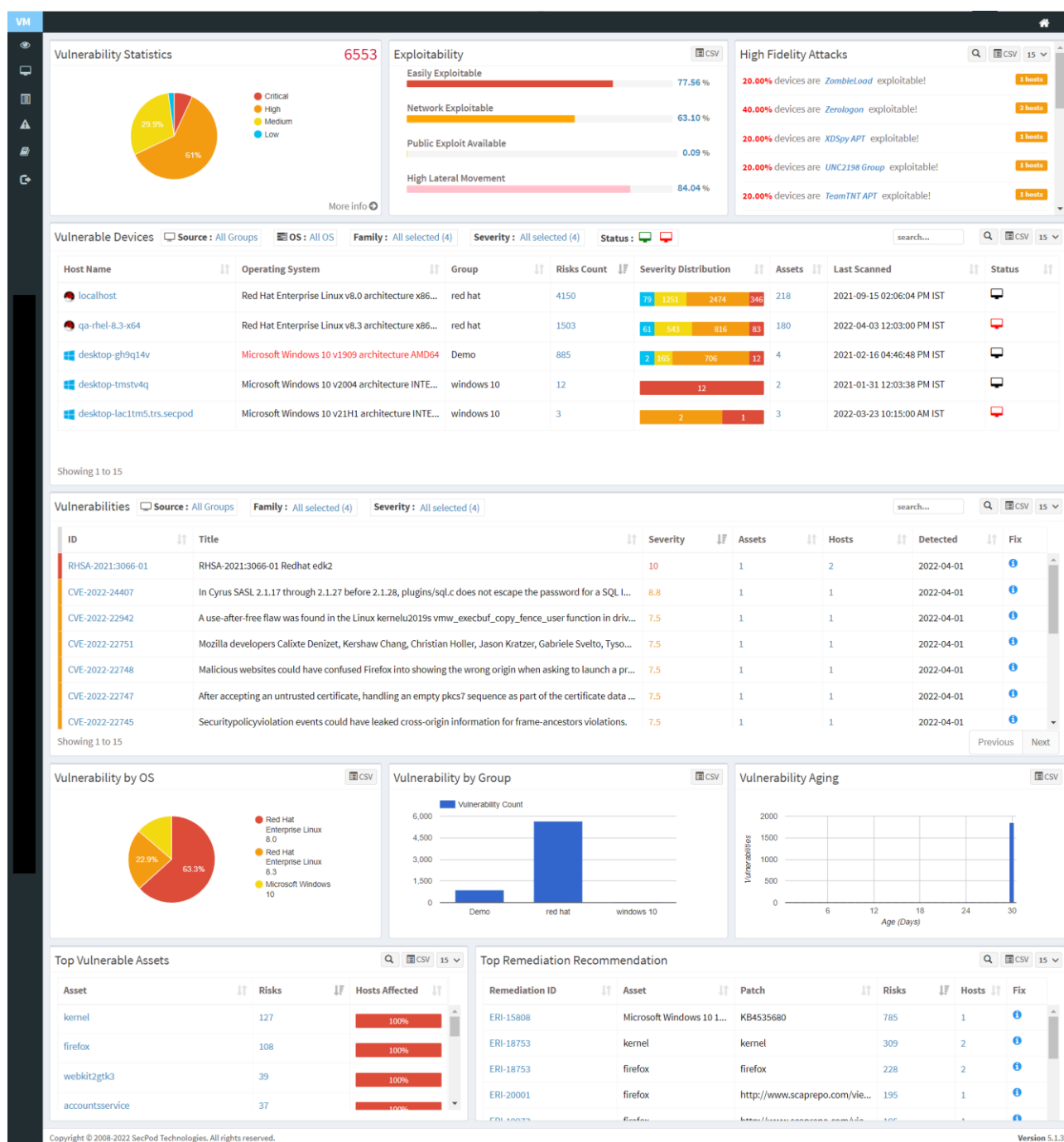
Congratulations! You have configured the Network Scanner feature in the SanerNow.

Once the network scanner is configured and the scan has been run, the following are uploaded to the SanerNow server: Discovered vulnerabilities, misconfigurations, and hardware/software assets in the network-enabled devices. You can view them by accessing Vulnerability Management (VM), Compliance Management (CM), and Asset Exposure (AE) dashboards.

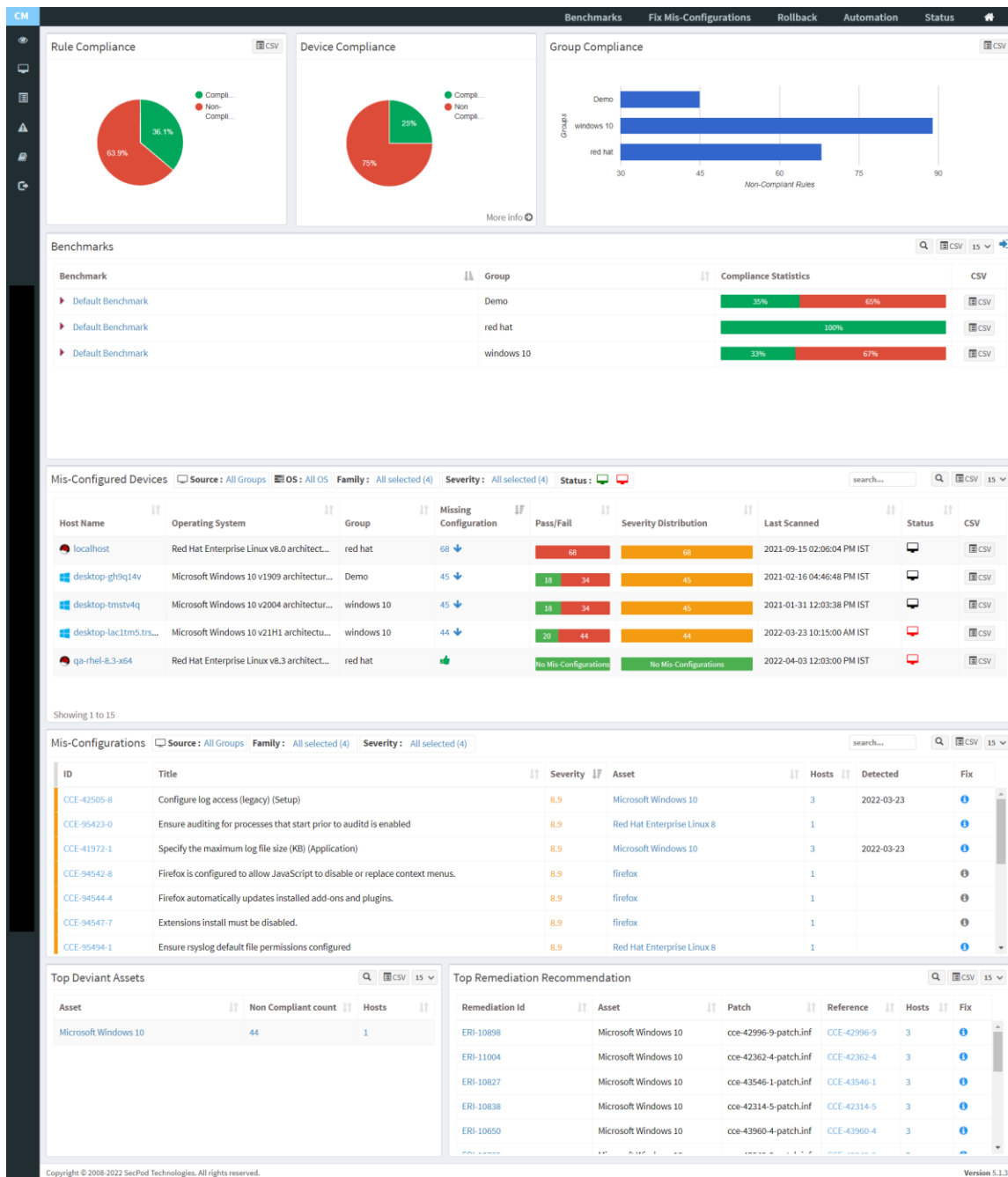
The Managed Devices page will list all agent-installed endpoint and network devices. The **Managed By** column will display the network scanner icon to identify the network scanned devices.

Managed Devices							
<div> Groups All Devices OS: All OS Family: All selected (4) search... CSV 15 </div>							
Host Name	IP Address	MAC Address	Operating System	Managed By	Group	Status	
qa-rhel-8.3-x64	192.168.1.107	86-44-C9-18-C7-23	Red Hat Enterprise Linux v8.3 architecture x86_64	5.1-0.1-noui-1-rpm-x64	red hat		
desktop-lac1m5.trn.secpod	192.168.1.130	C6-8B-BC-3D-B9-02	Microsoft Windows 10 v21H1 architecture INTEL32	5.1-0.1-noui-1-exe-x86	windows 10		
desktop-gh9q14v	192.168.3.73	00-0C-29-8F-8A-31	Microsoft Windows 10 v1909 architecture AMD64	4.8-0.0-noui-1-exe-x86	Demo		
desktop-tmstv4q	192.168.2.83	AE-85-2B-91-9C-07	Microsoft Windows 10 v2004 architecture INTEL32	4.8-0.0-noui-1-exe-x86	windows 10		
localhost	192.168.2.181	00-0C-29-CE-5C-E7	Red Hat Enterprise Linux v8.0 architecture x86_64	4.8-0.0-noui-1-rpm-x64	red hat		
Showing 1 to 5 of 5 entries							
Previous 1 Next							

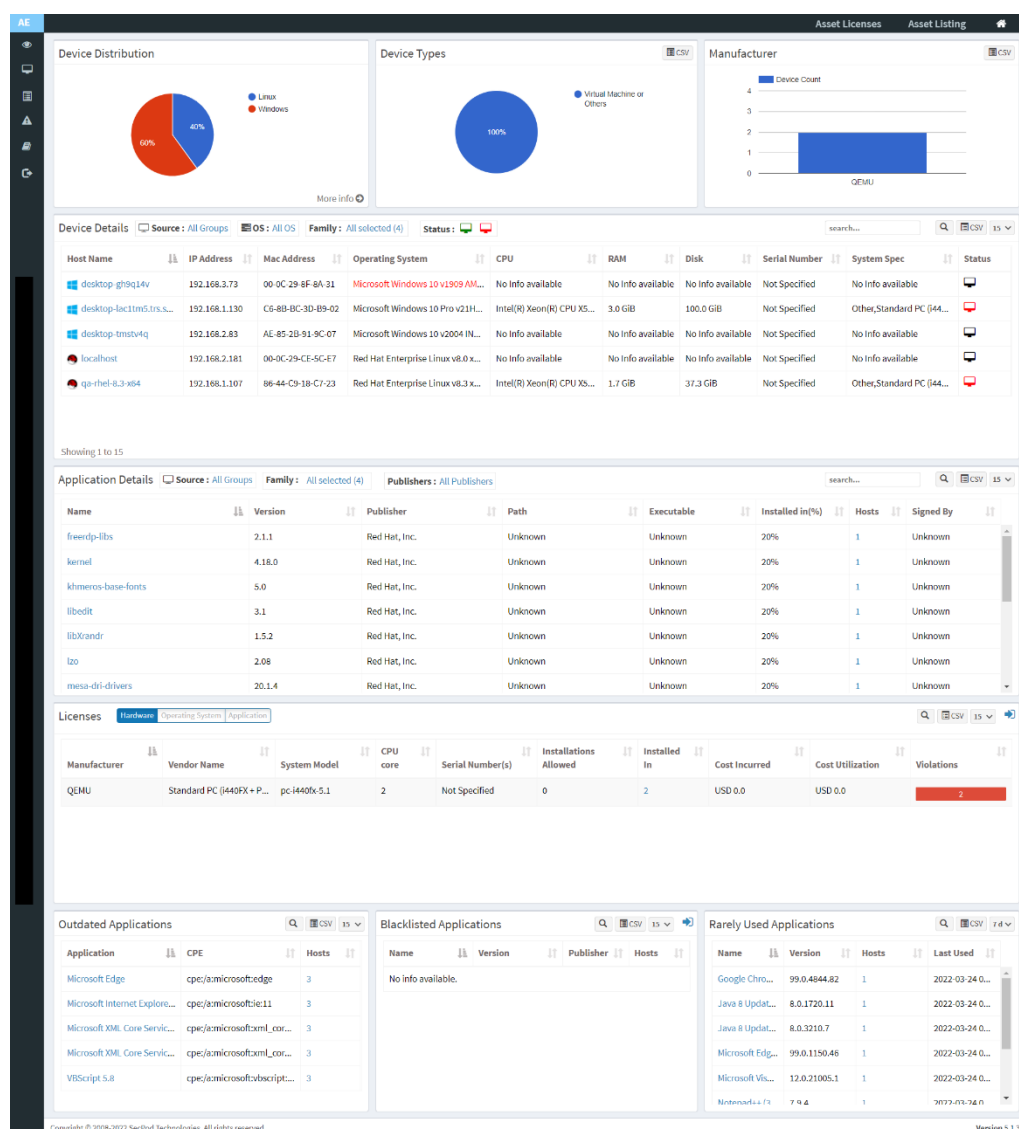
The vulnerabilities detected by the network scanner devices are listed on the **Vulnerability Management** dashboard. Users can view the complete information on the vulnerabilities detected by the VM dashboard's endpoint devices and network devices. Apply the **Others** option under the **Family** filter to view the list of vulnerable devices and the vulnerabilities detected by the network scanners.



Users can view the compliance information detected by the network scanners on the **Compliance Management** dashboard. This dashboard will display the compliance deviations detected by the endpoint and network devices. Apply the **Others** option under the **Family** filter to view the list of Mis-Configured Devices and the Mis-Configurations detected by the network scanners.



The hardware and software assets detected by the network scanners are displayed on the **Asset Exposure** dashboard. Users can get complete information on the AE dashboard on devices, applications, and asset licenses. Apply the **Others** option under the **Family** filter to view the devices and application details detected by the network scanners.



## About SecPod, Inc.

SecPod is a leading provider of endpoint security and management solutions. SecPod (Security Podium, incarnated as SecPod) has created a revolutionary SanerNow platform and tools used by MSPs and enterprises worldwide. SecPod also licenses security technology to top security vendors through its SCAP Content Professional Feed.

303 Twin Dolphin Drive,  
6th Floor, Redwood City,  
California 94065, USA.

To learn more about SecPod, visit:

[www.SecPod.com](http://www.SecPod.com)

## Contact

Sales : [info@secpod.com](mailto:info@secpod.com)  
Support : [support@secpod.com](mailto:support@secpod.com)  
Phone : (+1) 918 625 3023 (US)