Network Scanner Feature

Technical Guide for SanerNow

Document Version: 5.0.0.0-R01

Published Date: 10 July 2021

Table of Contents

Overview of Network Scanner Feature in SanerNow 2

Pre-requisites 2

Workflow of Network Scanner Feature in SanerNow........ 3

Installing and Configuring Network Scanner Feature in SanerNow 3

Scanners 8

Scan Config 10

Scan Policy 13

Logs 17

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 it is important that the vulnerability management solution is equipped to handle the security loopholes across all. SecPod SanerNow's in-built network scanner detects the vulnerabilities across all the IP-enabled devices in the network. This network scanner works 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 largest 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 in the network 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 any of 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

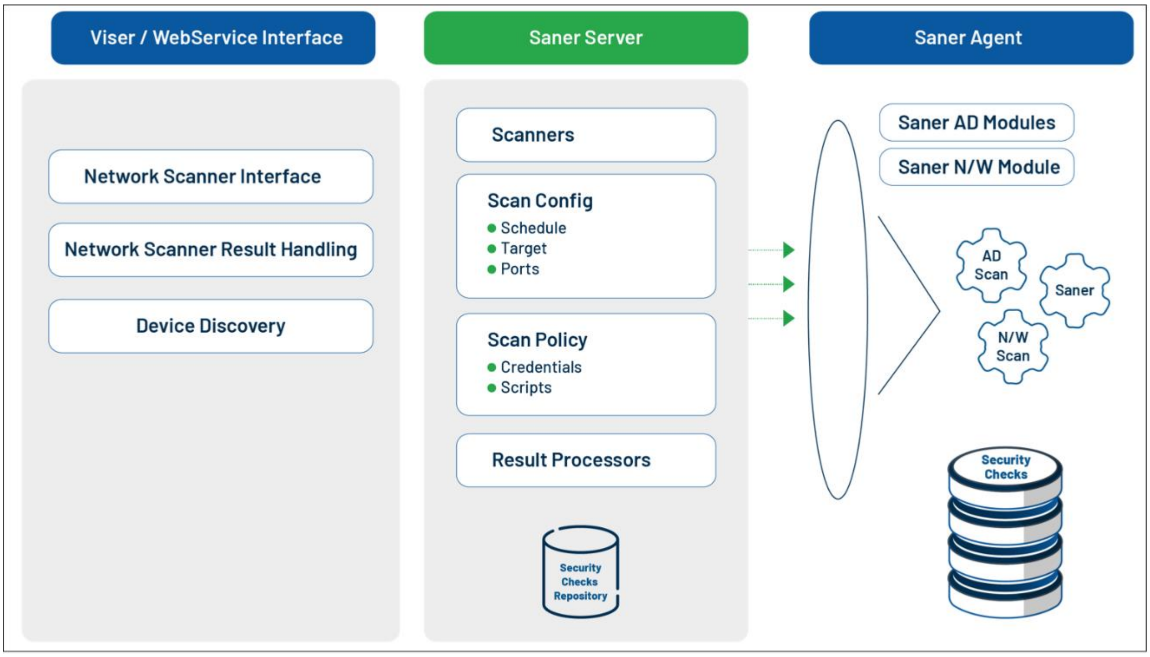
- Asset Management

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: User will designate the agent as a network scanner. 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 SanerNow console.

Configure Network Scanner: The user configures the network scan and defines the scan policy. Users select IP ranges (in a convenient format of their choice), various vulnerability 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

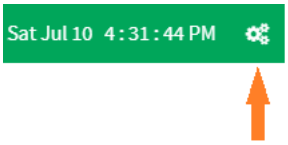
Endpoint devices can be designated as network scanners in two ways:

- **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.

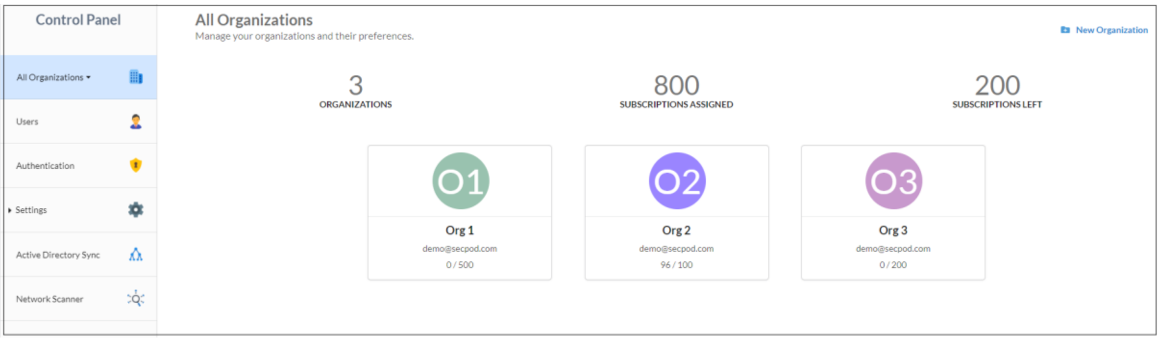
To designate the endpoint device as a network scanner from the wizard mode, follow the below steps:

Step 1: Login to your SanerNow account. The organizational level dashboard will be displayed.

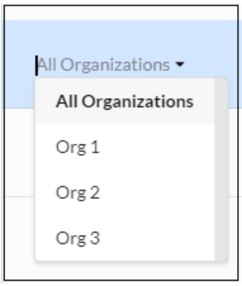
Step 2: Click on the **gear** icon at the top-right corner of the organization level dashboard to open the **Control Panel** page.



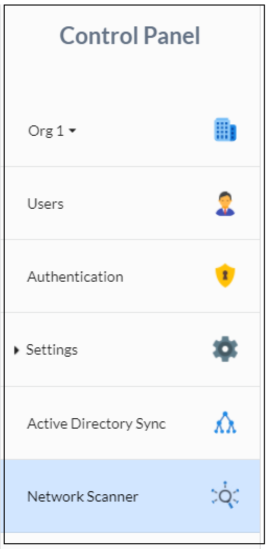
Step 3: All Organizations option in the left sidebar is selected by default. If the admin has created only one organization, the page will automatically select that organization and show its accounts.



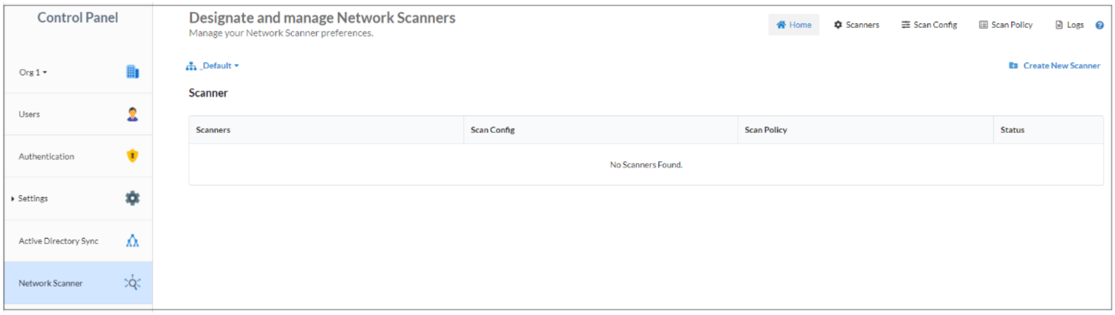
Step 4: If there are multiple organizations, select an organization from the drop-down menu.



Step 5: After selecting the organization in the left sidebar, choose the **Network Scanner** option.



Step 6: The **Home** tab will be empty since the Network Scanner is not configured yet.



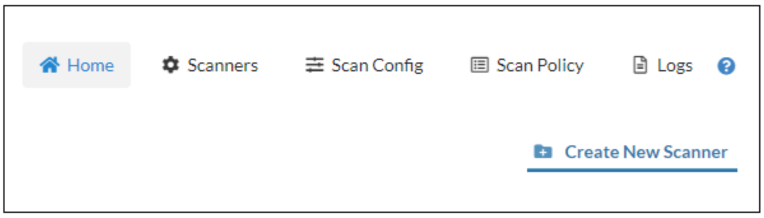
Designate and manage Network Scanners

Manage your Network Scanner preferences.

Scanner

Scanners	Scan Config	Scan Policy	Status
No Scanners Found.			

Step 7: Click on the **Create New Scanner** option to create a new scanner.

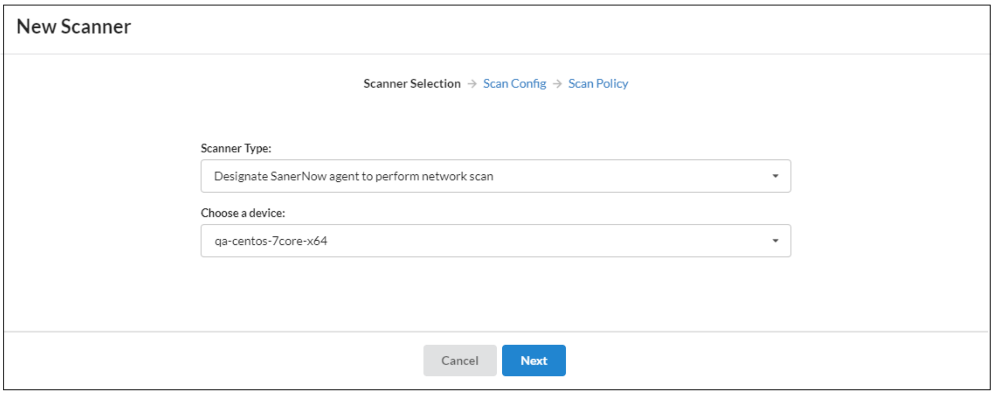


Step 8: Complete the following three steps to create a new scanner: **Scanner Selection, Scan Config,** and **Scan Policy**.

a) Scanner Selection

In the Scanner Selection section, select the preferred method for choosing a device from the drop-down menu.

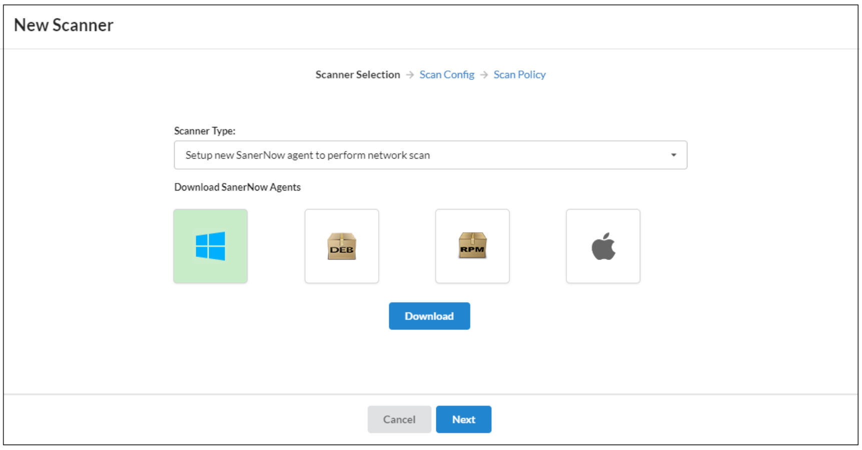
- **Designate SanerNow agent to perform network scan:** Select this option if the Saner agent is already installed in the device and you want to upgrade this device as a network scanner.



Scanner Type: Designate SanerNow agent to perform network scan

Choose a device: qa-centos-7core-x64

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



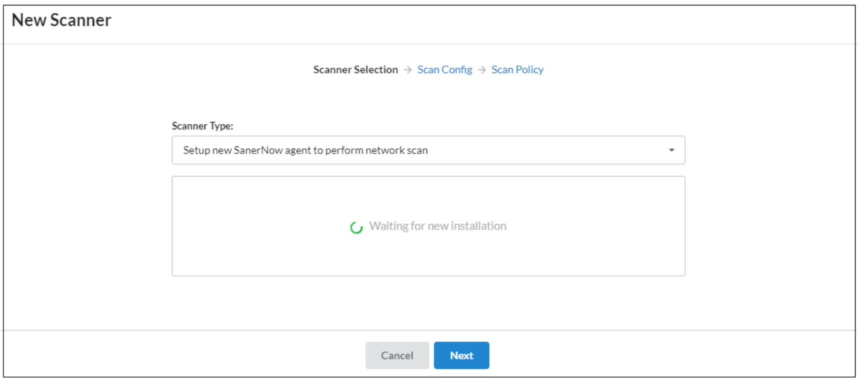
New Scanner

Scanner Selection → Scan Config → Scan Policy

Scanner Type: Setup new SanerNow agent to perform network scan

Download SanerNow Agents

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.



New Scanner

Scanner Selection → Scan Config → Scan Policy

Scanner Type: Setup new SanerNow agent to perform network scan

Waiting for new installation

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

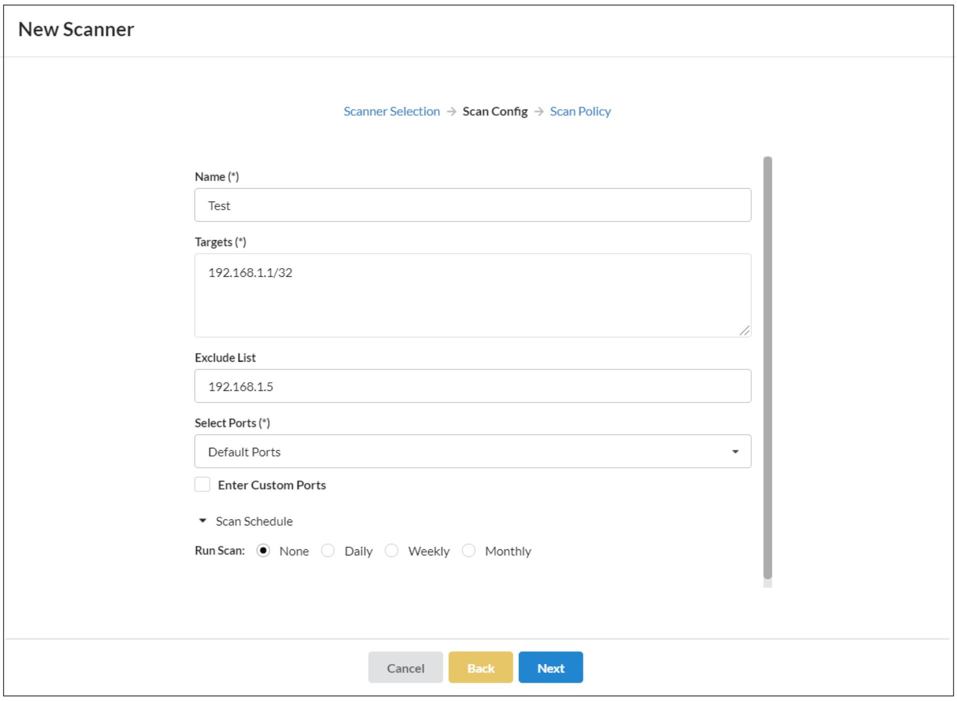
Choose a device: Select the device from the list and click on the **Next** button.

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 they can 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 select the following ports 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.



New Scanner

Scanner Selection → Scan Config → Scan Policy

Name (*): Test

Targets (*): 192.168.1.1/32

Exclude List: 192.168.1.5

Select Ports (*): Default Ports

□ Enter Custom Ports

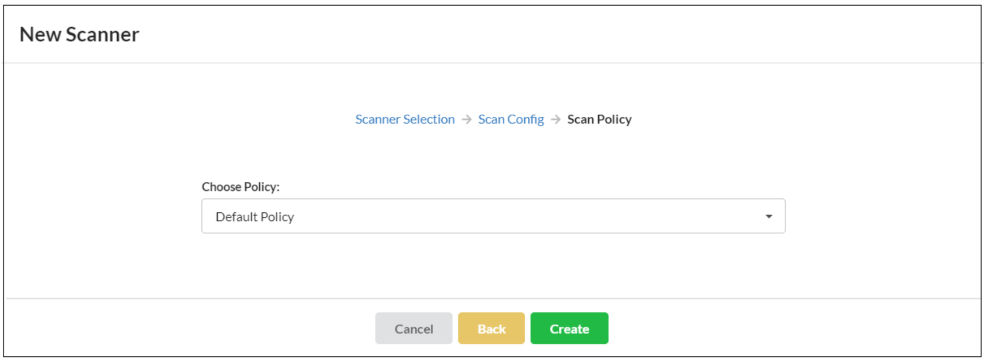
Scan Schedule

Run Scan: ● None ○ Daily ○ Weekly ○ Monthly

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.

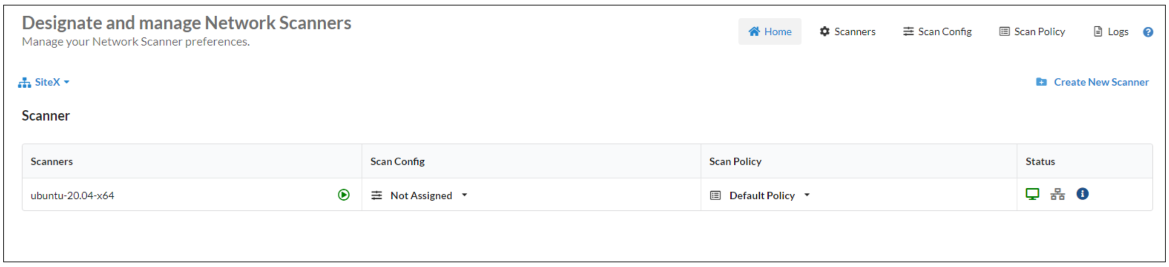


New Scanner

Scanner Selection → Scan Config → Scan Policy

Choose Policy: Default Policy

The **Back** option is available for the scan config and scan policy sections to modify any settings. Once the scan profile is complete, 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.



Designate and manage Network Scanners
Manage your Network Scanner preferences.

Scanner

Scanners	Scan Config	Scan Policy	Status
ubuntu-20.04-x64	Not Assigned	Default Policy	

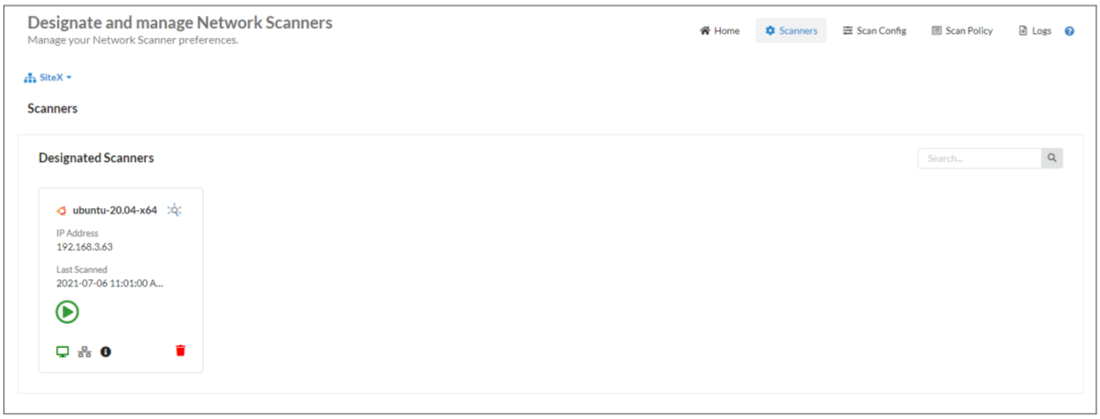
The home page will list the designated scanners and associated scan config settings, scan policies, and the status. Following is the list of parameters present on the home page.

Parameter	Description
Scanners	It will display a list of designated network scanner devices. You can initiate a scan by clicking on the **Scan Now** 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	**Device Status** icon – This icon shows the status of the device – Active or Inactive. **Network Scanner Status** icon – This icon shows the scan status of the Network Scanner. **Information** icon – The last scan information is displayed by clicking on the "i" icon.

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, and last scan date and for each network scanner.



Designate and manage Network Scanners

Manage your Network Scanner preferences.

SiteX

Scanners

Designated Scanners

ubuntu-20.04-x64

IP Address

192.168.3.63

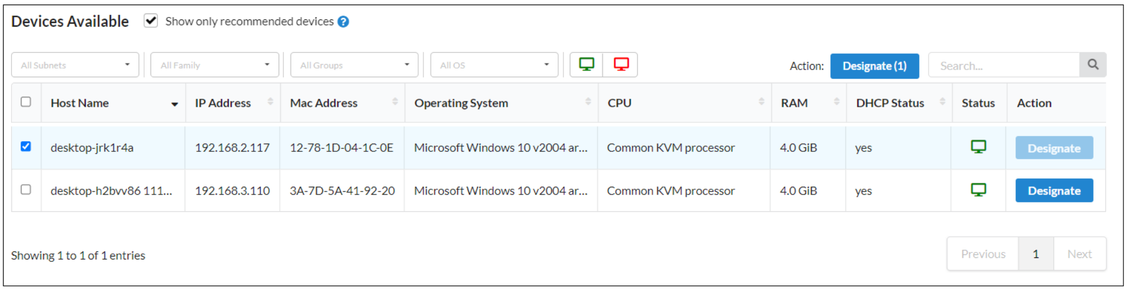
Last Scanned

2021-07-06 11:01:00 A...

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 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 along with 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 check boxes on the left and click on the **Designate** button on the right to promote these endpoints as network scanners.



☐	Host Name	IP Address	Mac Address	Operating System	CPU	RAM	DHCP Status	Status	Action
☑	desktop-jrk1r4a	192.168.2.117	12-78-1D-04-1C-0E	Microsoft Windows 10 v2004 ar...	Common KVM processor	4.0 GiB	yes		Designate
☐	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		Designate

Showing 1 to 1 of 1 entries

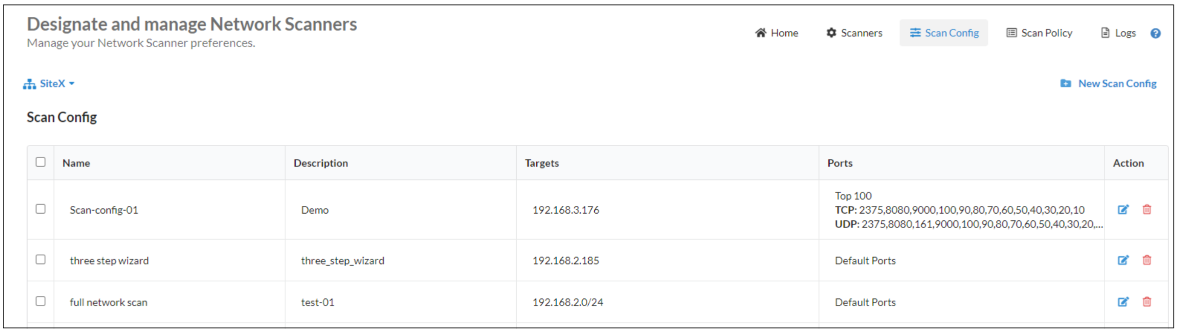
The search option is provided to list the devices. Users can also filter the devices by the subnets, family, group, Operating System, and device status. By default, the "**Show only recommended devices**" filter option is selected that will list the recommended devices based on the below parameters:

- 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, 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

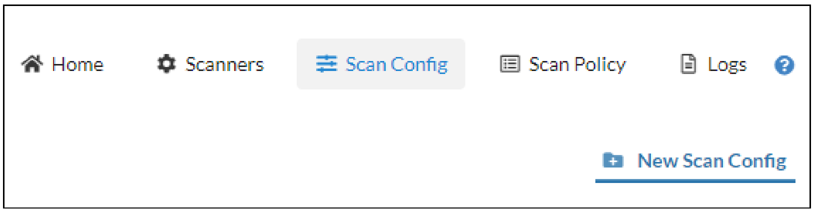
Manage your Network Scanner preferences.

Scan Config

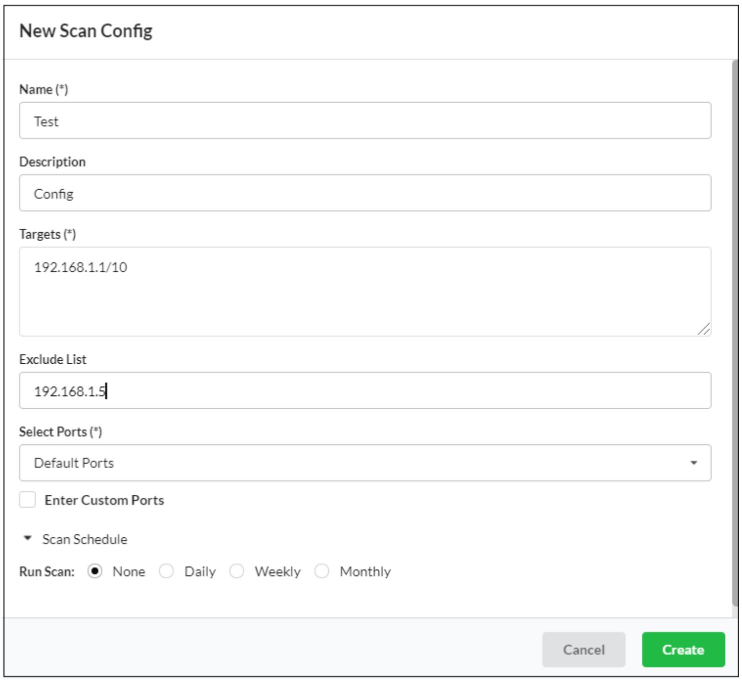
☐	Name	Description	Targets	Ports	Action
☐	Scan-config-01	Demo	192.168.3.176	Top 100 **TCP:** 2375,8080,9000,100,90,80,70,60,50,40,30,20,10 **UDP:** 2375,8080,161,9000,100,90,80,70,60,50,40,30,20,...	
☐	three step wizard	three_step_wizard	192.168.2.185	Default Ports	
☐	full network scan	test-01	192.168.2.0/24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

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, as shown in the below image.



New Scan Config

Name (*): Test

Description: Config

Targets (*): 192.168.1.1/10

Exclude List: 192.168.1.5

Select Ports (*): Default Ports

□ Enter Custom Ports

Scan Schedule

Run Scan: ● None ○ Daily ○ Weekly ○ Monthly

Following is the list of fields with description:

a) **Name** – Specify the name for the scan configuration.

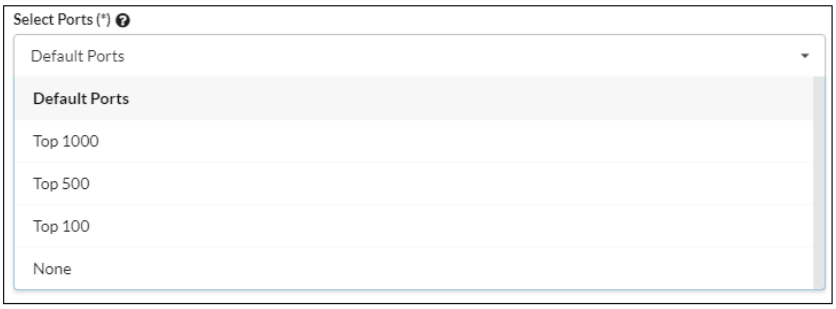
b) **Description** – Specify the description of the scan configuration.

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 to be excluded from the scan. This member is an IPv4 address. E.g.: 192.168.1.5,192.168.1.6.

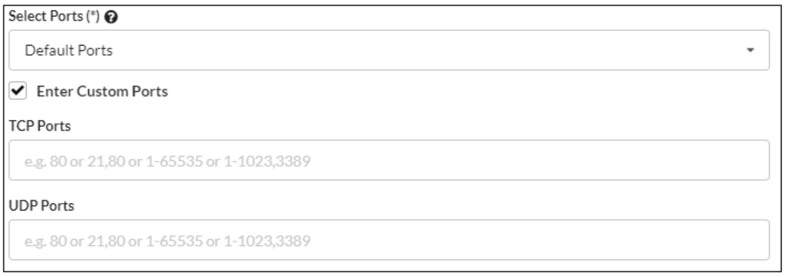
e) **Select Ports** – Specify a comma-separated list of ports to scan. Users can select default ports, or they can customize their own set of TCP/UDP ports based on the configuration.

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 ports 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

- **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



Select Ports (*)

Default Ports

☑ Enter Custom Ports

TCP Ports

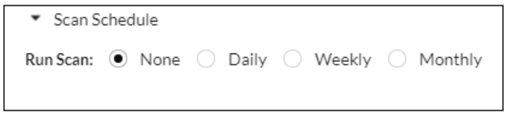
e.g. 80 or 21,80 or 1-65535 or 1-1023,3389

UDP Ports

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.

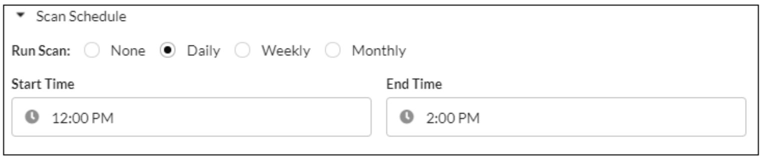
- **None:** A network scan has to be manually triggered.



Scan Schedule

Run Scan: ● None ○ Daily ○ Weekly ○ Monthly

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



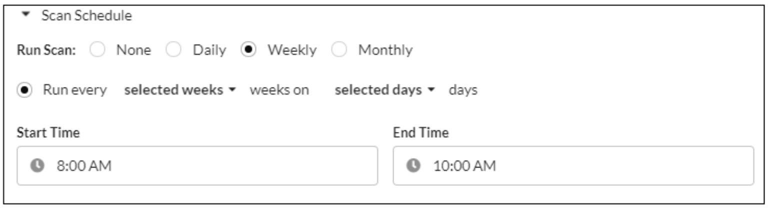
Scan Schedule

Run Scan: ○ None ● Daily ○ Weekly ○ Monthly

Start Time: 12:00 PM

End Time: 2:00 PM

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



Scan Schedule

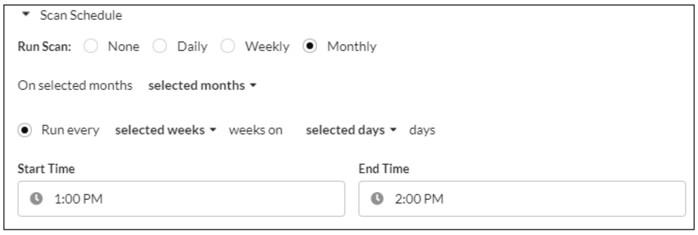
Run Scan: ○ None ○ Daily ● Weekly ○ Monthly

● Run every selected weeks weeks on selected days days

Start Time: 8:00 AM

End Time: 10:00 AM

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



Scan Schedule

Run Scan: ○ None ○ Daily ○ Weekly ● Monthly

On selected months selected months

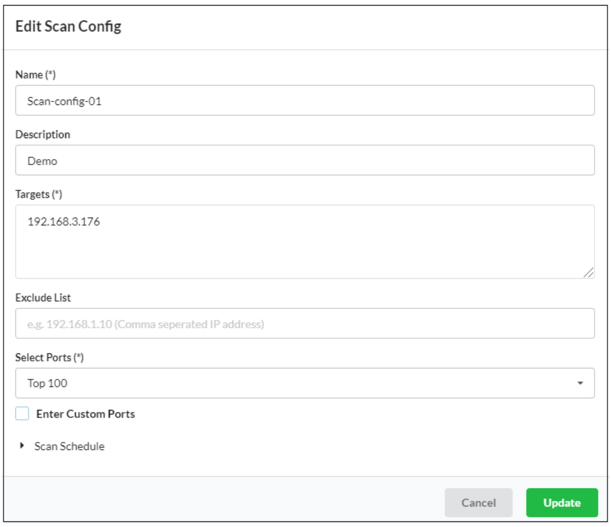
● Run every selected weeks weeks on selected days days

Start Time: 1:00 PM

End Time: 2:00 PM

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

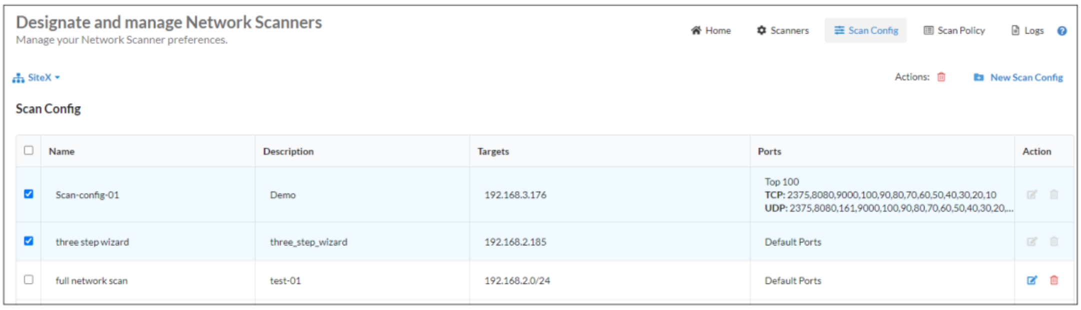
Exclude List
e.g. 192.168.1.10 (Comma seperated IP address)

Select Ports (*)
Top 100

□ Enter Custom Ports

Scan Schedule

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



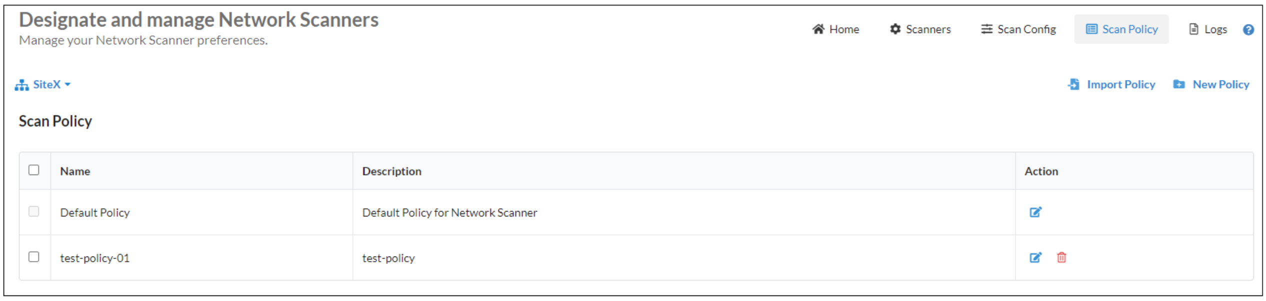
Designate and manage Network Scanners
Manage your Network Scanner preferences.

Scan Config

□	Name	Description	Targets	Ports	Action
☑	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,...	
☑	three step wizard	three_step_wizard	192.168.2.185	Default Ports	
□	full network scan	test-01	192.168.2.0/24	Default Ports	

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. If the user has not created the scan policy, the default policy will be selected. This default policy will execute all the applications and services that SanerNow supports.



Designate and manage Network Scanners
Manage your Network Scanner preferences.

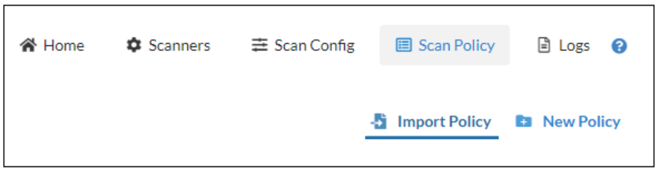
Scan Policy

□	Name	Description	Action
□	Default Policy	Default Policy for Network Scanner	
□	test-policy-01	test-policy	

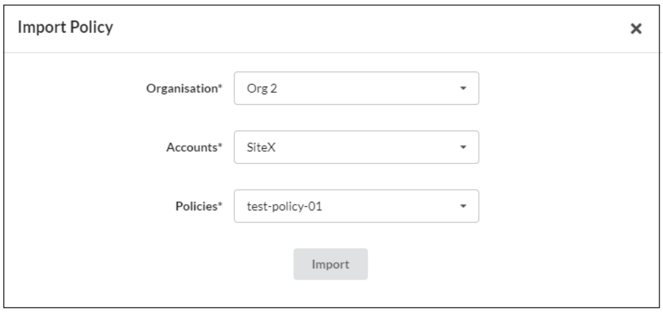
Users can create a new policy, or they can import the policy from different organizations/accounts.

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

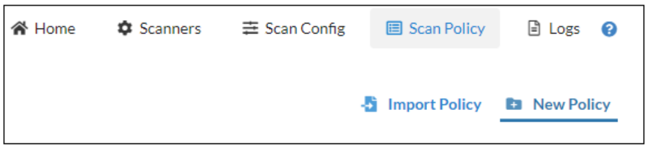
Organisation* Org 2

Accounts* SiteX

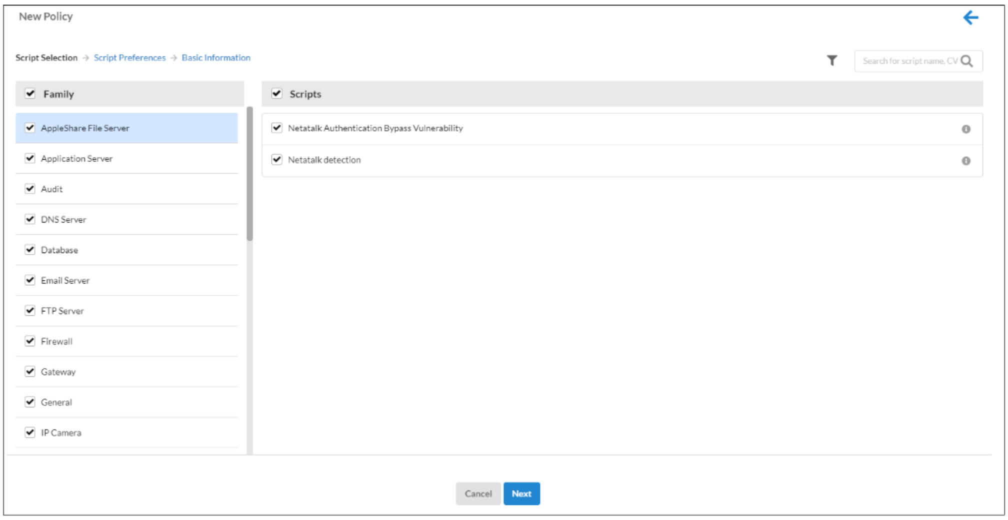
Policies* test-policy-01

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 which you don’t want to run by unchecking the box.



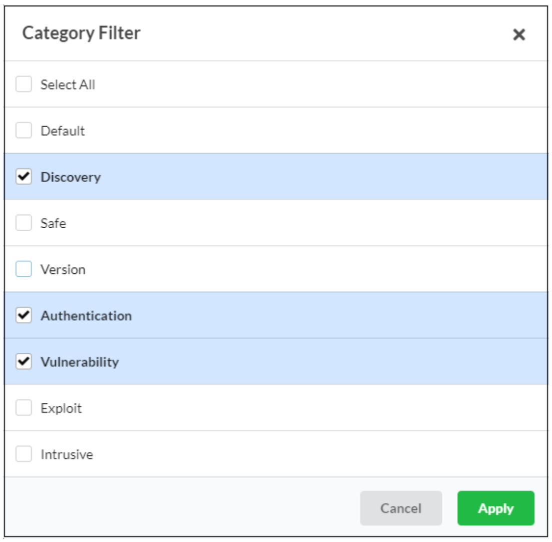
New Policy

Script Selection → Script Preferences → Basic Information

☑ Family
- ☑ AppleShare File Server
- ☑ Application Server
- ☑ Audit
- ☑ DNS Server
- ☑ Database
- ☑ Email Server
- ☑ FTP Server
- ☑ Firewall
- ☑ Gateway
- ☑ General
- ☑ IP Camera

☑ Scripts
- ☑ Netatalk Authentication Bypass Vulnerability
- ☑ Netatalk detection

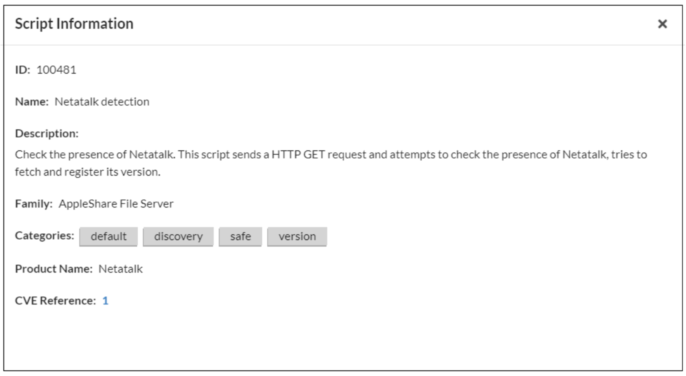
Apply the filter to view specific scripts. Select one or more filters and click on the **Apply** option to filter the scripts based on the selected category.



Category Filter

□ Select All
□ Default
☑ Discovery
□ Safe
□ Version
☑ Authentication
☑ Vulnerability
□ Exploit
□ Intrusive

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.



Script Information

ID: 100481

Name: Netatalk detection

Description:
Check the presence of Netatalk. This script sends a HTTP GET request and attempts to check the presence of Netatalk, tries to fetch and register its version.

Family: AppleShare File Server

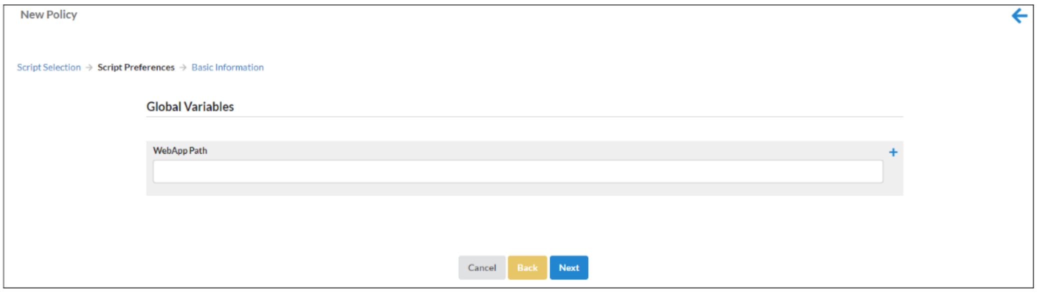
Categories: default discovery safe version

Product Name: Netatalk

CVE Reference: 1

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.



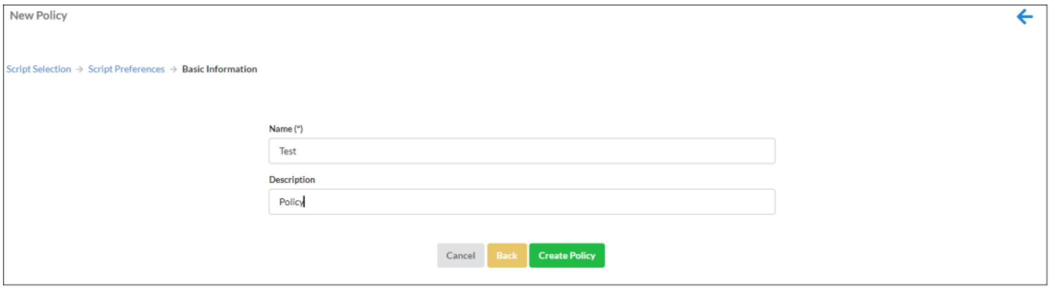
New Policy

Script Selection → Script Preferences → Basic Information

Global Variables

WebApp Path

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



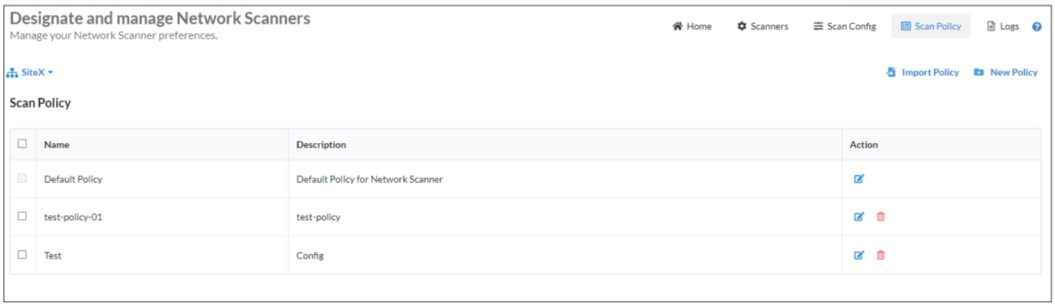
New Policy

Script Selection → Script Preferences → Basic Information

Name (*)
Test

Description
Policy

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



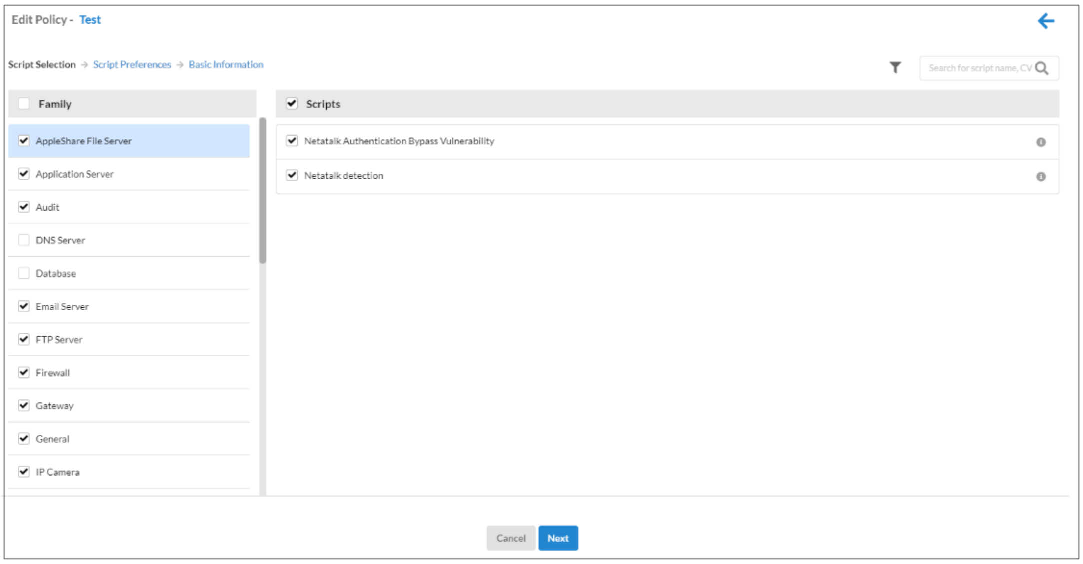
Designate and manage Network Scanners
Manage your Network Scanner preferences.

Scan Policy

☐	Name	Description	Action
☐	Default Policy	Default Policy for Network Scanner	✎
☐	test-policy-01	test-policy	✎ 🗑
☐	Test	Config	✎ 🗑

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

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



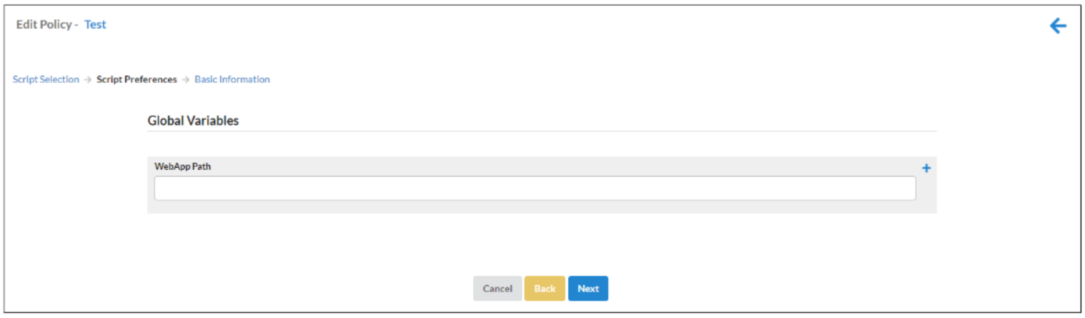
Edit Policy - Test

Script Selection → Script Preferences → Basic Information

☐ Family
- ☑ AppleShare File Server
- ☑ Application Server
- ☑ Audit
- ☐ DNS Server
- ☐ Database
- ☑ Email Server
- ☑ FTP Server
- ☑ Firewall
- ☑ Gateway
- ☑ General
- ☑ IP Camera

☑ Scripts
- ☑ Netatalk Authentication Bypass Vulnerability
- ☑ Netatalk detection

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



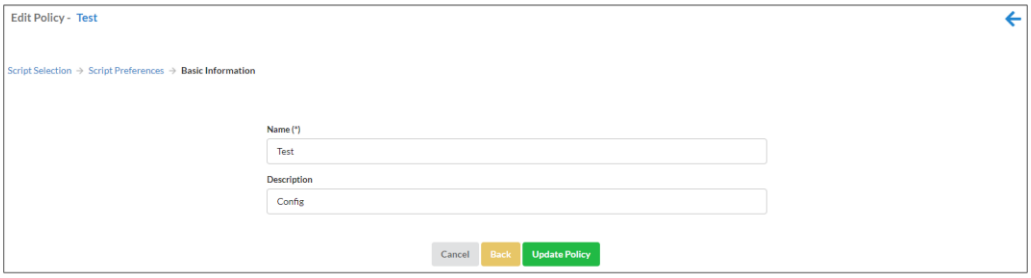
Edit Policy - Test

Script Selection → Script Preferences → Basic Information

Global Variables

WebApp Path

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



Edit Policy - Test

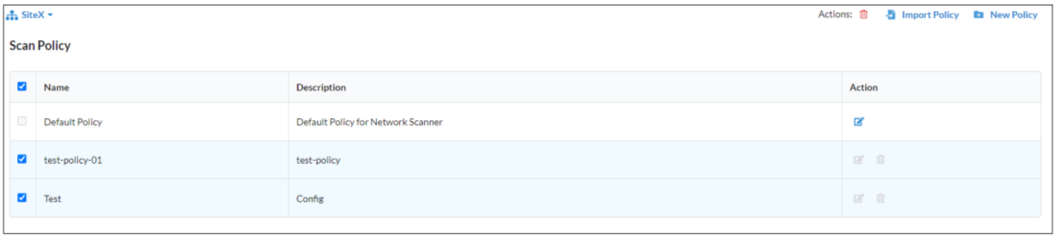
Script Selection → Script Preferences → Basic Information

Name (*): Test

Description: Config

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

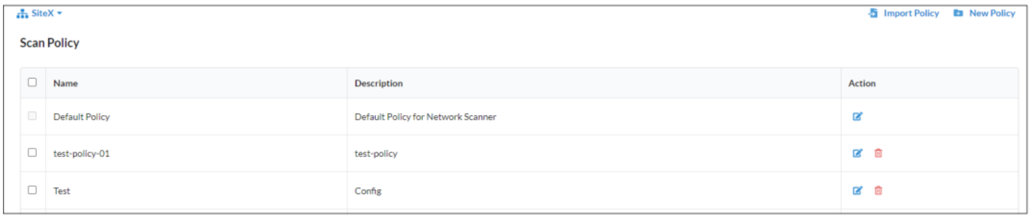
1. Select the scan policies to be deleted and click on the **Delete** icon at the top.



Scan Policy

☑	Name	Description	Action
□	Default Policy	Default Policy for Network Scanner	
☑	test-policy-01	test-policy	
☑	Test	Config	

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

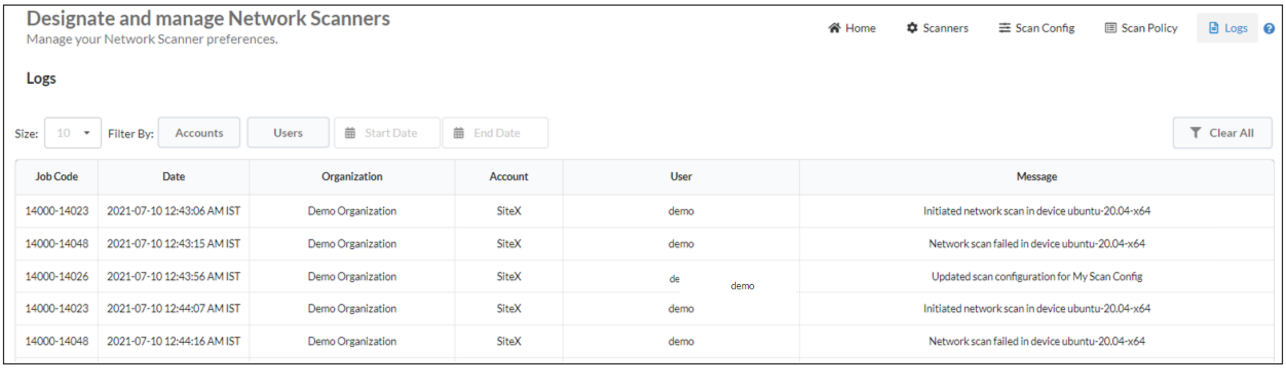


Scan Policy

□	Name	Description	Action
□	Default Policy	Default Policy for Network Scanner	
□	test-policy-01	test-policy	
□	Test	Config	

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 to.



Designate and manage Network Scanners
Manage your Network Scanner preferences.

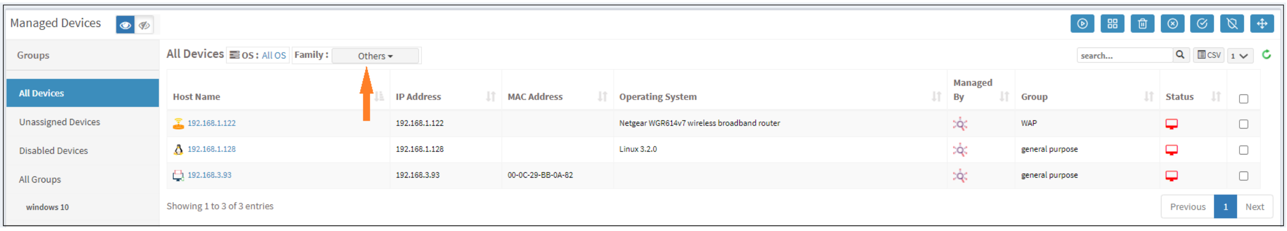
Logs

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	de 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. Discovered vulnerabilities, misconfigurations, hardware/software assets in the network-enabled devices gets uploaded to the SanerNow server. You can view them by accessing Vulnerability Management (VM), Compliance Management (CM), and Asset Management (AM) dashboards.

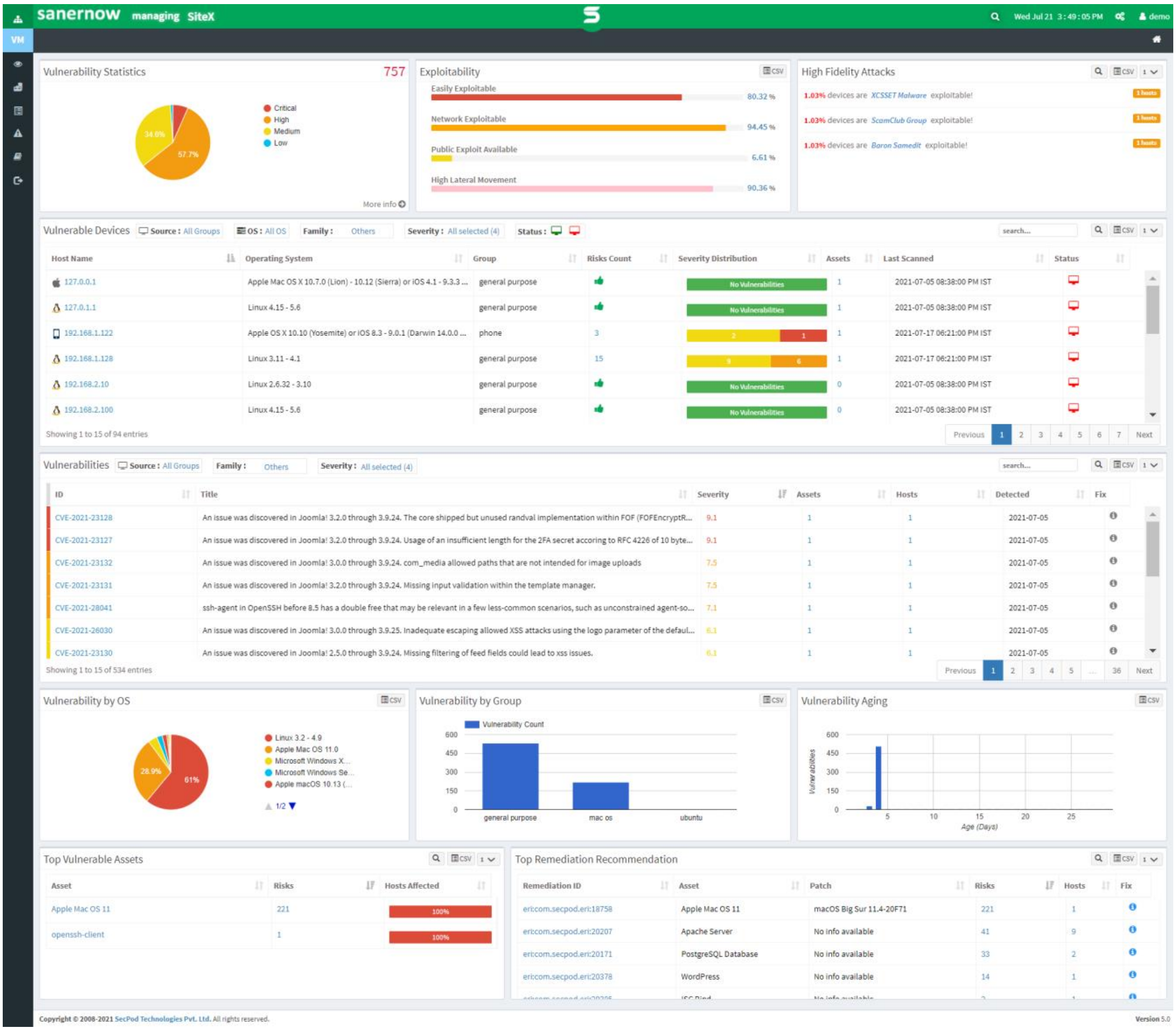
The Managed Devices page will list all agent-installed endpoint and network devices. Users can apply the **Others** option under the family filter to view the network scanner devices. The **Managed By** column will display the network scanner icon to identify the network scanned devices.



Host Name	IP Address	MAC Address	Operating System	Managed By	Group	Status	□
192.168.1.122	192.168.1.122		Netgear WGR614v7 wireless broadband router		WAP		□
192.168.1.128	192.168.1.128		Linux 3.2.0		general purpose		□
192.168.3.93	192.168.3.93	00-0C-29-BB-0A-82			general purpose		□

Showing 1 to 3 of 3 entries

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 endpoint devices and network devices on the VM dashboard. Apply the **Others** option under the **Family** filter to view the list of vulnerable devices and vulnerabilities detected by the network scanners.



1.03% devices are *XCSSET Malware* exploitable! 1 hosts

1.03% devices are *ScamClub Group* exploitable! 1 hosts

1.03% devices are *Baron Samedit* exploitable! 1 hosts

Vulnerable Devices — Source : All Groups — OS : All OS — Family : Others — Severity : All selected (4) — Status : — search...

Host Name	Operating System	Group	Risks Count	Severity Distribution	Assets	Last Scanned	Status
127.0.0.1	Apple Mac OS X 10.7.0 (Lion) - 10.12 (Sierra) or iOS 4.1 - 9.3.3 ...	general purpose	👍	No Vulnerabilities	1	2021-07-05 08:38:00 PM IST	🟥
127.0.1.1	Linux 4.15 - 5.6	general purpose	👍	No Vulnerabilities	1	2021-07-05 08:38:00 PM IST	🟥
192.168.1.122	Apple OS X 10.10 (Yosemite) or iOS 8.3 - 9.0.1 (Darwin 14.0.0 ...	phone	3	2 1	1	2021-07-17 06:21:00 PM IST	🟥
192.168.1.128	Linux 3.11 - 4.1	general purpose	15	9 6	1	2021-07-17 06:21:00 PM IST	🟥
192.168.2.10	Linux 2.6.32 - 3.10	general purpose	👍	No Vulnerabilities	0	2021-07-05 08:38:00 PM IST	🟥
192.168.2.100	Linux 4.15 - 5.6	general purpose	👍	No Vulnerabilities	0	2021-07-05 08:38:00 PM IST	🟥

Showing 1 to 15 of 94 entries — Previous 1 2 3 4 5 6 7 Next

Vulnerabilities — Source : All Groups — Family : Others — Severity : All selected (4) — search...

ID	Title	Severity	Assets	Hosts	Detected	Fix
CVE-2021-23128	An issue was discovered in Joomla! 3.2.0 through 3.9.24. The core shipped but unused randval implementation within FOF (FOFEncryptR...	9.1	1	1	2021-07-05	ℹ
CVE-2021-23127	An issue was discovered in Joomla! 3.2.0 through 3.9.24. Usage of an insufficient length for the 2FA secret accoring to RFC 4226 of 10 byte...	9.1	1	1	2021-07-05	ℹ
CVE-2021-23132	An issue was discovered in Joomla! 3.0.0 through 3.9.24. com_media allowed paths that are not intended for image uploads	7.5	1	1	2021-07-05	ℹ
CVE-2021-23131	An issue was discovered in Joomla! 3.2.0 through 3.9.24. Missing input validation within the template manager.	7.5	1	1	2021-07-05	ℹ
CVE-2021-28041	ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-so...	7.1	1	1	2021-07-05	ℹ
CVE-2021-26030	An issue was discovered in Joomla! 3.0.0 through 3.9.25. Inadequate escaping allowed XSS attacks using the logo parameter of the defaul...	6.1	1	1	2021-07-05	ℹ
CVE-2021-23130	An issue was discovered in Joomla! 2.5.0 through 3.9.24. Missing filtering of feed fields could lead to xss issues.	6.1	1	1	2021-07-05	ℹ

Showing 1 to 15 of 534 entries — Previous 1 2 3 4 5 ... 36 Next

Top Vulnerable Assets

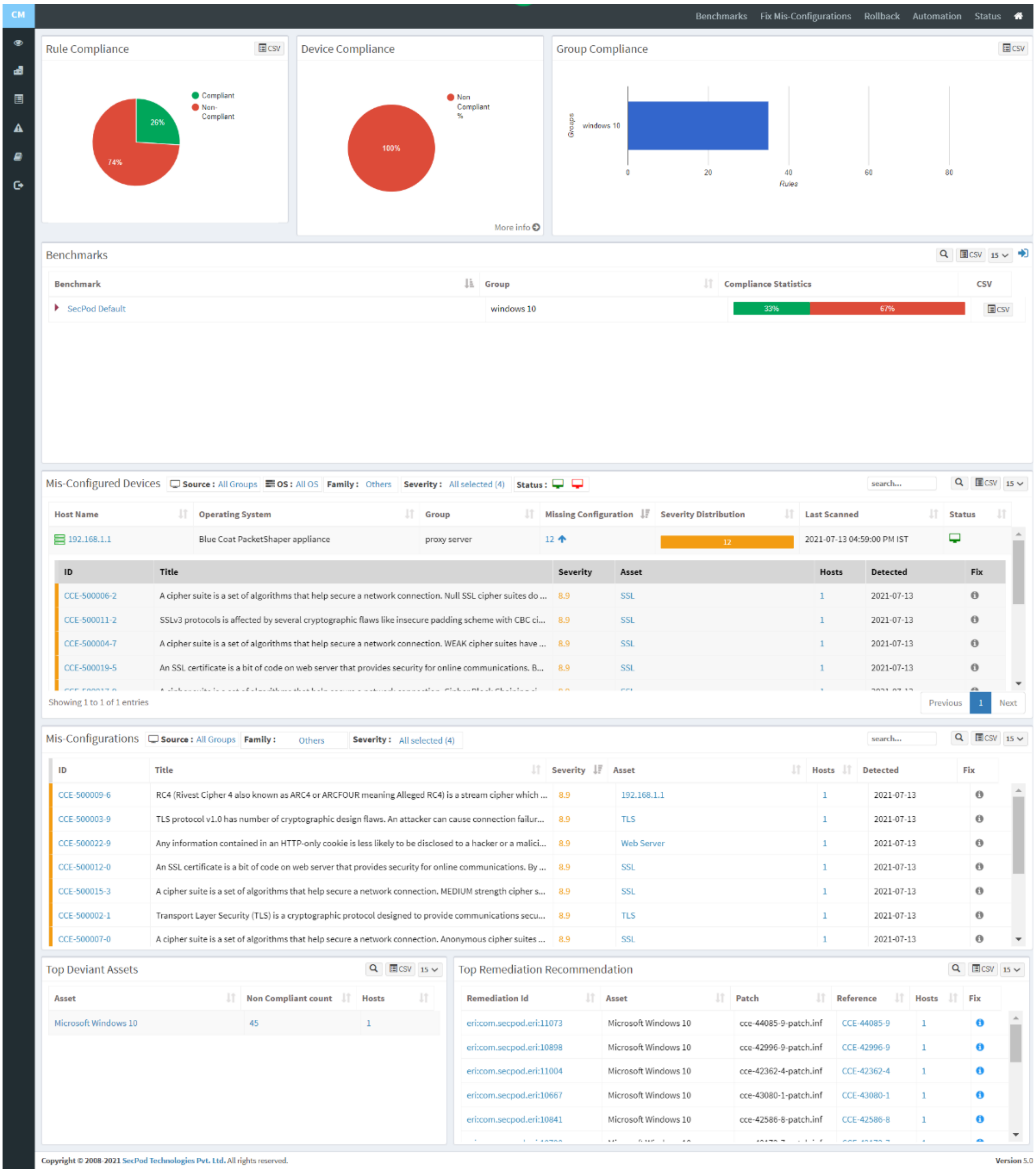
Asset	Risks	Hosts Affected
Apple Mac OS 11	221	100%
openssh-client	1	100%

Top Remediation Recommendation

Remediation ID	Asset	Patch	Risks	Hosts	Fix
eri:com.secpod.eri:18758	Apple Mac OS 11	macOS Big Sur 11.4-20F71	221	1	ℹ
eri:com.secpod.eri:20207	Apache Server	No info available	41	9	ℹ
eri:com.secpod.eri:20171	PostgreSQL Database	No info available	33	2	ℹ
eri:com.secpod.eri:20378	WordPress	No info available	14	1	ℹ

Copyright © 2008-2021 SecPod Technologies Pvt. Ltd. All rights reserved.

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



Benchmarks

Benchmark	Group	Compliance Statistics	CSV
SecPod Default	windows 10	33% 67%	CSV

Mis-Configured Devices Source : All Groups OS : All OS Family : Others Severity : All selected (4) Status :

Host Name	Operating System	Group	Missing Configuration	Severity Distribution	Last Scanned	Status
192.168.1.1	Blue Coat PacketShaper appliance	proxy server	12	12	2021-07-13 04:59:00 PM IST	

ID	Title	Severity	Asset	Hosts	Detected	Fix
CCE-500006-2	A cipher suite is a set of algorithms that help secure a network connection. Null SSL cipher suites do ...	8.9	SSL	1	2021-07-13	
CCE-500011-2	SSLv3 protocols is affected by several cryptographic flaws like insecure padding scheme with CBC ci...	8.9	SSL	1	2021-07-13	
CCE-500004-7	A cipher suite is a set of algorithms that help secure a network connection. WEAK cipher suites have ...	8.9	SSL	1	2021-07-13	
CCE-500019-5	An SSL certificate is a bit of code on web server that provides security for online communications. B...	8.9	SSL	1	2021-07-13	

Showing 1 to 1 of 1 entries

Previous 1 Next

Mis-Configurations Source : All Groups Family : Others Severity : All selected (4)

ID	Title	Severity	Asset	Hosts	Detected	Fix
CCE-500009-6	RC4 (Rivest Cipher 4 also known as ARC4 or ARCFOUR meaning Alleged RC4) is a stream cipher which ...	8.9	192.168.1.1	1	2021-07-13	
CCE-500003-9	TLS protocol v1.0 has number of cryptographic design flaws. An attacker can cause connection failur...	8.9	TLS	1	2021-07-13	
CCE-500022-9	Any information contained in an HTTP-only cookie is less likely to be disclosed to a hacker or a malici...	8.9	Web Server	1	2021-07-13	
CCE-500012-0	An SSL certificate is a bit of code on web server that provides security for online communications. By ...	8.9	SSL	1	2021-07-13	
CCE-500015-3	A cipher suite is a set of algorithms that help secure a network connection. MEDIUM strength cipher s...	8.9	SSL	1	2021-07-13	
CCE-500002-1	Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications secu...	8.9	TLS	1	2021-07-13	
CCE-500007-0	A cipher suite is a set of algorithms that help secure a network connection. Anonymous cipher suites ...	8.9	SSL	1	2021-07-13	

Top Deviant Assets

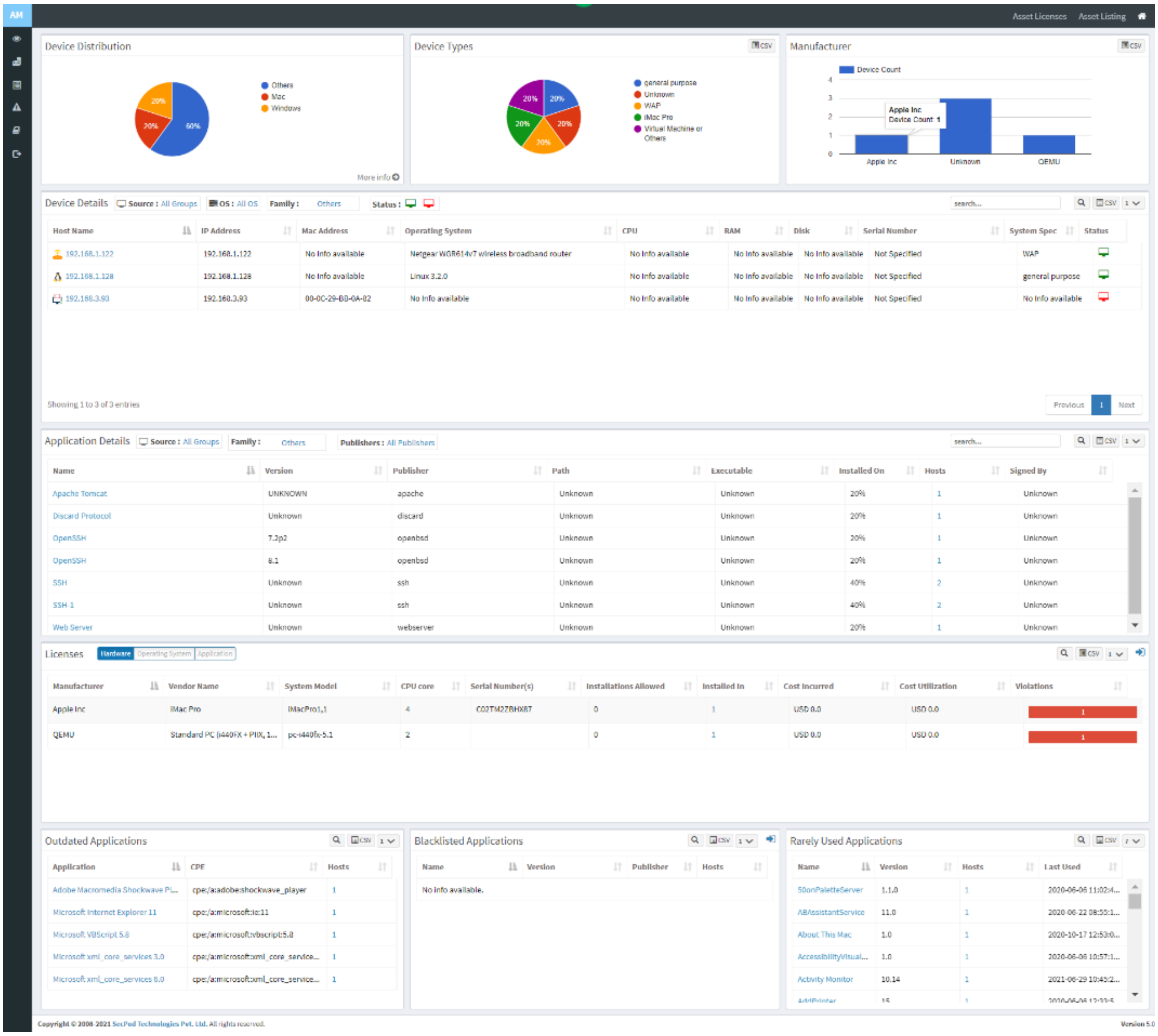
Asset	Non Compliant count	Hosts
Microsoft Windows 10	45	1

Top Remediation Recommendation

Remediation Id	Asset	Patch	Reference	Hosts	Fix
eri:com.secpod.eri:11073	Microsoft Windows 10	cce-44085-9-patch.inf	CCE-44085-9	1	
eri:com.secpod.eri:10898	Microsoft Windows 10	cce-42996-9-patch.inf	CCE-42996-9	1	
eri:com.secpod.eri:11004	Microsoft Windows 10	cce-42362-4-patch.inf	CCE-42362-4	1	
eri:com.secpod.eri:10667	Microsoft Windows 10	cce-43080-1-patch.inf	CCE-43080-1	1	
eri:com.secpod.eri:10841	Microsoft Windows 10	cce-42586-8-patch.inf	CCE-42586-8	1	

Copyright © 2008-2021 SecPod Technologies Pvt. Ltd. All rights reserved. Version 5.0

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



Device Details Source : All Groups OS : All OS Family : Others Status :

search...

Host Name	IP Address	Mac Address	Operating System	CPU	RAM	Disk	Serial Number	System Spec	Status
192.168.1.122	192.168.1.122	No Info available	Netgear WGR614v7 wireless broadband router	No Info available	No Info available	No Info available	Not Specified	WAP	🟩
192.168.1.128	192.168.1.128	No Info available	Linux 3.2.0	No Info available	No Info available	No Info available	Not Specified	general purpose	🟩
192.168.3.93	192.168.3.93	00-0C-29-B0-0A-82	No Info available	No Info available	No Info available	No Info available	Not Specified	No Info available	🟥

Showing 1 to 3 of 3 entries

Previous 1 Next

Application Details Source : All Groups Family : Others Publishers : All Publishers

search...

Name	Version	Publisher	Path	Executable	Installed On	Hosts	Signed By
Apache Tomcat	UNKNOWN	apache	Unknown	Unknown	20%	1	Unknown
Discard Protocol	Unknown	discard	Unknown	Unknown	20%	1	Unknown
OpenSSH	7.2p2	openbsd	Unknown	Unknown	20%	1	Unknown
OpenSSH	8.1	openbsd	Unknown	Unknown	20%	1	Unknown
SSH	Unknown	ssh	Unknown	Unknown	40%	2	Unknown
SSH-1	Unknown	ssh	Unknown	Unknown	40%	2	Unknown
Web Server	Unknown	webserver	Unknown	Unknown	20%	1	Unknown

Licenses Hardware Operating System Application

Manufacturer	Vendor Name	System Model	CPU core	Serial Number(s)	Installations Allowed	Installed In	Cost Incurred	Cost Utilization	Violations
Apple Inc	iMac Pro	iMacPro1,1	4	C02TM2ZBHX87	0	1	USD 0.0	USD 0.0	1
QEMU	Standard PC (i440FX + PIIX, 1...	pc-i440fx-5.1	2		0	1	USD 0.0	USD 0.0	1

Outdated Applications

Application	CPE	Hosts
Adobe Macromedia Shockwave Pl...	cpe:/a:adobe:shockwave_player	1
Microsoft Internet Explorer 11	cpe:/a:microsoft:ie:11	1
Microsoft VBScript 5.8	cpe:/a:microsoft:vbscript:5.8	1
Microsoft xml_core_services 3.0	cpe:/a:microsoft:xml_core_service...	1
Microsoft xml_core_services 6.0	cpe:/a:microsoft:xml_core_service...	1

Blacklisted Applications

Name	Version	Publisher	Hosts
No info available.			

Rarely Used Applications

Name	Version	Hosts	Last Used
50onPaletteServer	1.1.0	1	2020-06-06 11:02:4...
ABAssistantService	11.0	1	2020-06-22 08:55:1...
About This Mac	1.0	1	2020-10-17 12:53:0...
AccessibilityVisual...	1.0	1	2020-06-06 10:57:1...
Activity Monitor	10.14	1	2021-06-29 10:45:2...
AddPrinter	15	1	2020-06-06 12:33:5

Copyright © 2008-2021 SecPod Technologies Pvt. Ltd. All rights reserved. Version 5.0

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 that are 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

Contact

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