SanerNow Network Scanner User Guide

Product Overview

SanerNow Network Scanner helps you identify vulnerabilities and misconfigurations across all IP-enabled devices in your Organization. And to do this – you don't have to invest in additional hardware.

Network Scanner scans your network by leveraging the endpoints that exist in your network. SanerNow's Network Scanner is built on a hub and spoke model – which effectively reduces the scan time required to scan and discover vulnerabilities in your network – making the entire process seamless and continuous.

Features of SanerNow Network Scanner

- Network Scanner tool can detect network topology, devices, and operating systems and perform service fingerprinting across all IP-enabled devices.
- Using Network Scanner, you can identify vulnerabilities and misconfigurations in network devices. Additionally, you can perform an external security posture analysis of endpoint devices.
- With SanerNow Network Scanner, you don't need to invest in additional hardware to have network scanning capability. Instead, the Network Scanner tool automatically identifies endpoints and designates them as network scanners.
- You can automate daily scans using Network Scanner to perform periodic scans on your network.
- SanerNow Network Scanner supports authenticated network scans. You can provide credentials to the network scripts and perform a scan on network devices in your infrastructure to identify the vulnerabilities existing on these devices.
- SanerNow Network Scanner supports agentless scan – you don't have to deploy SanerNow Agent on target devices and still perform vulnerability and compliance scans.

SanerNow Network Scanner Pre-requisites

Endpoints running the below-mentioned OSs can be designated as Network Scanners.

- Windows (32bit and 64-bit)
- macOS
- Linux (only 64-bit is supported)

Endpoints running Linux OS (32-bit), Alpine Linux (32-bit and 64-bit) and AIX (32-bit and 64-bit) can't be designated as network scanners.

Also, you must have an active subscription to either one of the tools – Vulnerability Management, Compliance Management, or Asset Exposure- to use the Network Scanner feature.

Designating an Endpoint as a Network Scanner

You need to designate endpoints within your network as network scanners. You can do this in two ways

1. Using the Wizard available in the SanerNow tool to designate an endpoint as a network scanner automatically.
2. Designating endpoints as network scanners from the list of SanerNow recommended devices.

Using the Wizard to designate an Agent as a Network Scanner

In this method, we use the SanerNow Agent installed on an endpoint device and designate it as a Network Scanner.

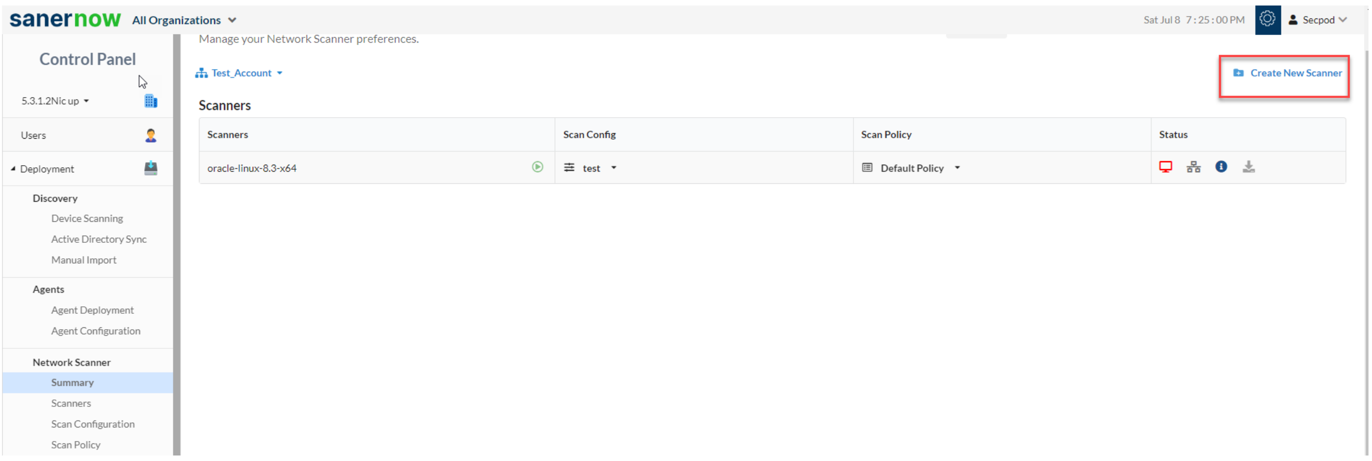
Follow the below steps to designate an endpoint as a Network Scanner using the wizard.

Step 1: Log in to the SanerNow web console. Click the Control Panel icon ⚙ located at the top right corner of the screen.

Step 2: The Network Scanner is located on the left side of the Control Panel page.

Step 3: Click the ***Summary*** button. A screen showing all network scanners in the selected Account will pop up. You will see an empty list if no network scanners are configured in an Account.

Step 4: Click the **Create New Scanner** button at the top right of the page.



Manage your Network Scanner preferences.

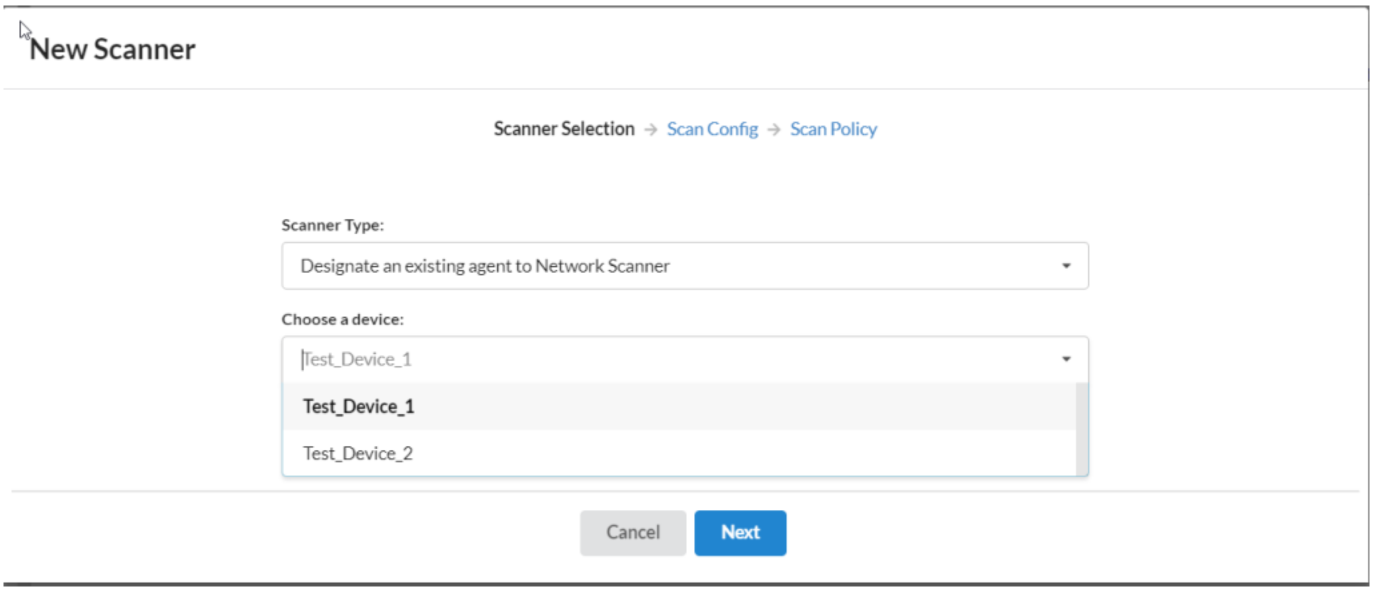
Scanners

Scanners	Scan Config	Scan Policy	Status
oracle-linux-8.3-x64	test	Default Policy	

Step 5: A pop-up screen with a drop-down menu appears. You will see two options here listed under Scanner Type.

a. Designate an existing agent to Network Scanner.
b. Setup and designate a new agent to Network Scanner.

Step 6: Select the *option* – **Designate an existing agent to Network Scanner**. *A* drop-down box with all the SanerNow Agents available in the Account that can be designated as a Network Scanner appears.


New Scanner

Scanner Type: Designate an existing agent to Network Scanner

Choose a device: Test_Device_1

Step 7: Select the device you want to be designated as a Network Scanner and click the **Next** button. And then, you will see the **Scan Config** screen.

Step 8: You must fill in the information in the text boxes marked with an asterisk (*). Let’s look at each of these textboxes present on the screen and the type of information you need to provide.

Name: – You must specify a name for the Scan Config

Targets – Mention the IP addresses of the targets you wish to scan. The IP addresses must be specified in a comma-separated list of target IP addresses or domain names for scanning. Target IP addresses can also be specified using CIDR notation. For example, 192.168.1.1 or 192.168.1.1/32 or 192.168.1.1-10.

Exclude List: Mention the IP addresses of the targets that need to be excluded by the network scanner while performing a network scan. You can specify multiple IP addresses separated by a comma that needs to be excluded by the Network Scanner.

Select Ports: This drop-down box provides you with five options. You need to select one of these five options.

1. Default Ports
2. Top 1000
3. Top 500
4. Top 100
5. None

However, if you want to specify your own set of custom ports, select the checkbox **Enter Custom Ports** and specify the TCP and UDP ports you want to be scanned by the Network Scanner.

S**tep 9:** Select the **Scan Schedule**. You can select the scan to run at the below intervals.

1. None
2. Daily
3. Weekly

4. Monthly

Step 10: Select the **Run Scan schedule**. Once you do that, you will see a pop-up screen where you must choose the Scan Policy. By default, the **Default Policy** gets selected in the drop-down box. SanerNow configures the Default Policy. Any other Scan Policy that you have configured for the selected account will be shown here in the drop-down list. Click the **Create** button once you have chosen the Scan Policy.

> **Note**:
> You can opt to change the Scan Config and Scan Policy whenever you launch a network scan using SanerNow Network Scanner.

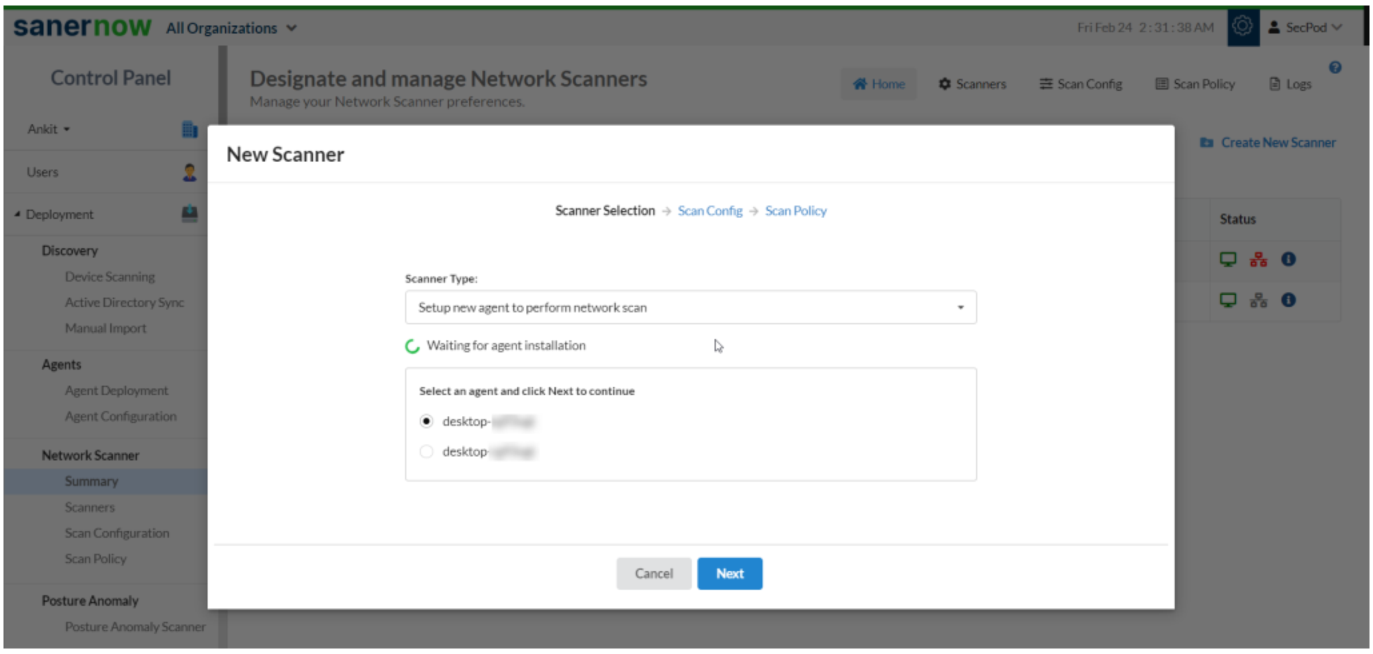
Using the Wizard to setup a New SanerNow Agent as a Network Scanner

In this method, we install the SanerNow Agent on an endpoint device and then promote the agent as a Network Scanner.

Step 1: Select the option **Setup new agent to perform network scan**. And select the **SanerNow Agent Installer** depending on the operating system installed on the endpoint.

Step 2: Install SanerNow Agent on the device. In the meantime, while SanerNow Agent is getting installed, the wizard will wait for the SanerNow Agent to get installed and communicate back to the wizard.

Step 3: SanerNow Agent installed device pops up on the wizard. Select the device and click the **Next** button.



New Scanner

Scanner Selection → Scan Config → Scan Policy

Scanner Type: Setup new agent to perform network scan

Waiting for agent installation

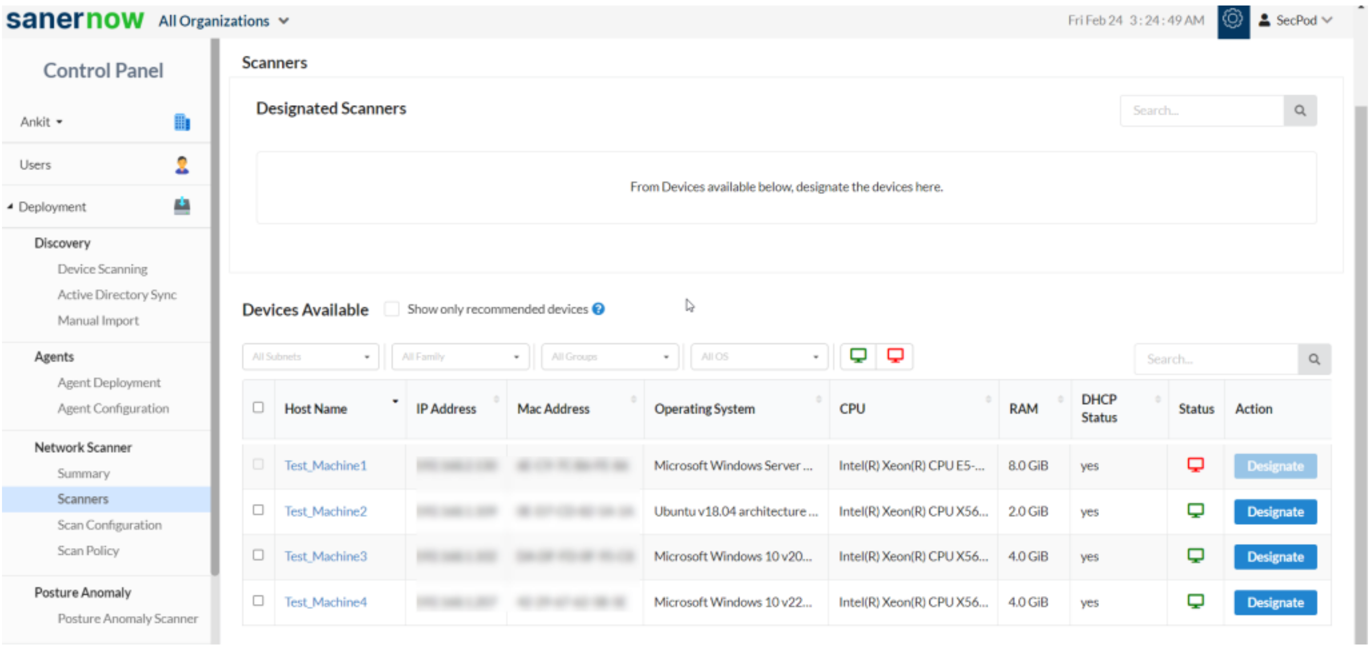
Select an agent and click Next to continue

● desktop-[redacted]
○ desktop-[redacted]

Step 4: Now follow the instructions specified in Steps 7- 10 from the section – [Using the Wizard to designate an Agent as a Network Scanner.]() And you're Network Scanner is now ready to perform a network scan on your network.

Manually designating endpoints as Network Scanners

Step 1: Click the **Scanners** menu under Network Scanner on the left side of the page. A list of devices from the Account that can be designated as Network Scanners is shown here.



From Devices available below, designate the devices here.

□	Host Name	IP Address	Mac Address	Operating System	CPU	RAM	DHCP Status	Status	Action
□	Test_Machine1	[redacted]	[redacted]	Microsoft Windows Server ...	Intel(R) Xeon(R) CPU E5-...	8.0 GiB	yes	🟥	Designate
□	Test_Machine2	[redacted]	[redacted]	Ubuntu v18.04 architecture ...	Intel(R) Xeon(R) CPU X56...	2.0 GiB	yes	🟩	Designate
□	Test_Machine3	[redacted]	[redacted]	Microsoft Windows 10 v20...	Intel(R) Xeon(R) CPU X56...	4.0 GiB	yes	🟩	Designate
□	Test_Machine4	[redacted]	[redacted]	Microsoft Windows 10 v22...	Intel(R) Xeon(R) CPU X56...	4.0 GiB	yes	🟩	Designate

Step 2: Check the box **Show only recommended devices** to allow SanerNow's recommendation engine to choose the best endpoints designated as Network Scanners.

Step 3: SanerNow shows the endpoints that can be used to designate as Network Scanners. You can do this by clicking the **Designate** button under the Action column.

The Device Available table displays the below information:

Column	Description
Host Name	This column displays the hostname of the endpoint.
IP Address	This column displays the ip address of the endpoint.
Mac Address	This column displays the mac address of the endpoint.
Operating System	This column displays the operating system on the endpoint.
CPU	This column displays the processor available on the endpoint.
RAM	This column displays the Random Access Memory available on the endpoint.
DHCP Status	This column shows if DHCP is enabled on the device. If DHCP is enabled, DHCP Status will be displayed as *yes.*
Status	This column displays the Status of the endpoint. The green system icon indicates that the endpoint is online. And red system icon indicates that the endpoint is offline.
Action	This column contains the Designate button. You can use this button to designate an endpoint as a Network Scanner.

Step 4: Click the **Designate** button, and the selected endpoint gets designated as a Network Scanner. The Network Scanner is listed under the Designated Scanners section above the Device available table.

The Designated Network Scanner section has multiple icons. The below table describes the usage of each icon.

Icons	Description
▶	This icon will start the Network Scan when clicked. If this icon is disabled, the device is either shut down or the SanerNow Agent on the device is inactive.
⏹	This icon will abort the ongoing Network Scan.
🖥	This icon indicates that the SanerNow Agent on the designated network scanner is active.
🖥	This icon indicates an inactive SanerNow Agent on the designated network scanner.
🖧	This icon indicates that the Network Scanner is active and scanning.
🖧	This icon indicates that the last Network Scan was aborted.
🖧	This icon indicates that the Network Scanner is idle.
ℹ	This icon provides the details of the last network scan.
🗑	This icon deletes the Network Scanner.
📥	This icon downloads the last two network scan reports. However, deleting the designated Network Scanner will delete the reports as well. At the same time, re-designating the Network Scanner will not restore old network scan reports.

Last Scan Information

Network Scanner stores the results of the network scan performed on the devices on the SanerNow Server. You can find the last scan details by clicking the ℹ icon.

The Last Scan Information window displays the following information after every successful network scan:

1. **Scanner** – The name of the scanner used for scanning the network is displayed here.
2. **Scan Configuration** – This label shows the scan configuration used by the network scanner.

3. **Scan Status** – This label shows whether the last scan was successful.
4. **Scan Summary** – This label shows the date, time, the number of hosts scanned, and the total time required to perform the scan.
5. **Last Scan** – This label shows the date and time the previous network scan occurred.
6. **Next Scan** – This label shows the date and time for the next network scan.
7. **Scan Duration** – This label shows the total time required to perform the last network scan.
8. **Targets scanned** – This label shows the count of the total number of devices scanned during the last network scan.
9. **Targets not scanned** – This label shows the total number of devices not scanned during the last network scan.
10. **Scripts Scanned** – This label shows the total number of scripts /policies used during the last network scan.
11. **Results Uploaded** – The status of the SanerNow Network Scanner uploads the network scan results to the SanerNow Server.
12. **Failed to Upload** – The SanerNow Network Scanner could not upload the network scan results to the SanerNow Server. If the upload fails, it will be shown here.

Managing Scan Configuration

SanerNow Network Scanner uses a scan configuration to identify targets to scan and exclude the ones not to scan. Click the **Scan Configuration** menu located on the left-hand side. This will direct you to the Scan Config page.

Creating a new Scan Configuration

Step 1: Click the **New Scan Config button** at the top right side of the page.

Step 2: A new pop-up appears on the screen. Fill in the information in the text boxes marked with an asterisk (*). Let’s look at each of these textboxes present on the screen and the type of information you need to provide.

Name: – You must specify a name for the Scan Config

Targets – Mention the IP addresses of the targets you wish to scan. The IP addresses must be specified in a comma-separated list of target IP addresses or domain names for scanning. Target IP addresses can also be specified using CIDR notation. For example, 192.168.1.1 or 192.168.1.1/32 or 192.168.1.1-10.

Exclude List: Mention the IP addresses of the targets that need to be excluded by the network scanner while performing a network scan. You can specify multiple IP addresses separated by a comma that needs to be excluded by the Network Scanner.

Select Ports: This drop-down box provides you with five options. You need to select one of these five options.

1. Default Ports
2. Top 1000
3. Top 500
4. Top 100

5. None

However, if you want to specify your own set of custom ports, select the checkbox Enter Custom Ports and specify the TCP and UDP ports you want to be scanned by the Network Scanner.

Step 3: Select the Scan Schedule. You can select the scan to run at the below intervals.

1. None
2. Daily
3. Weekly
4. Monthly.

Step 4: Click the **Create** button once you have provided all the information. The Scan Config policy is created and is listed on the Scan Config page.

Editing and Deleting a Scan Config

The Action column on the Scan Config page has two options – Edit and Delete.

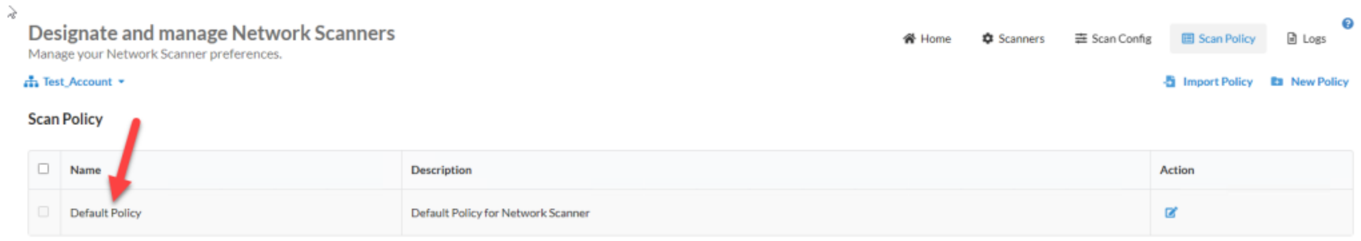
Icon	Usage
✎	To edit an existing Scan Config.
🗑	To delete an existing Scan Config.

Managing Scan Policy

By default, Network Scanner uses *Default Policy* to scan devices. Default Policy – a collection of multiple scripts belonging to different families helps Network Scanner to identify vulnerabilities across devices. You can import a new policy, create one, and modify the existing Default Policy.

Creating a New Policy

A Default Policy exists in the SanerNow Network Scanner. The Default Policy consists of preselected scripts. You can modify the scripts you want to be part of the Default Policy. However, you can’t delete the Default Policy; you can change it.



Designate and manage Network Scanners

Manage your Network Scanner preferences.

Test_Account

Scan Policy

□	Name	Description	Action
□	Default Policy	Default Policy for Network Scanner	✎

Follow the below steps to create a new policy:

Step 1: Click the **New Policy** button on the top right of the page.

Step 2: A new screen appears, prompting you to select the scripts you want to be part of the New Policy.

You can filter the scripts by using the category filter. The scripts fall into the following categories.

1. Safe
2. Vulnerability
3. Exploit
4. Default
5. Discovery
6. Version
7. Authentication

Select the scripts category and click the **Apply** button. A list of scripts relevant to the selected category appears on the page. You can manually deselect scrips you don't want to be part of the Scan Policy. Click the **Next** button.

Step 3: Provide the path for the web apps hosted in your environment. The **Global Variables** input fields will allow you to input the absolute path for these web apps. This step is not mandatory and should be skipped if you have no web apps in your environment. And then provide the set of credentials for the protocol you want the script to authenticate. HTTP/HTTPS and SSH protocols are currently supported. If you're using HTTP protocol for authentication, you must provide the username and password.

Similarly, if using SSH, you must provide the username, password, private key, and passphrase. Specifying credentials is a mandatory step and cannot be skipped. You can save credentials which will appear on the right side under Saved Credentials section.

Step 4: Specify the Name of the New Policy and provide a brief description in the Description box. Click the **Create Policy** button, and a new policy is created.

You've successfully created a new Scan Policy!

Importing Policy

You can import a scan policy from different Accounts within the same Organization. Also, you can import scan policies from Accounts in other Organizations.

Follow the below steps to import a policy from another account:

Step 1: Click the **Import Policy** button.

Step 2: Select the Organization and the relevant Account from where you want to import the policy. You can only select one policy at a time, even if the Account has multiple policies.

Step 3: Click the **Import** button. The selected policy gets imported into the current Account and will be visible on the Scan Policy screen.

Performing Authenticated Network Scans

SanerNow Network Scanner supports authenticated network scanning. New network scripts that support authentication are introduced under the **Authenticated** *category*. These scripts allow you to provide credentials and perform an authenticated scan on network devices. Also, the SanerNow Network Scanner allows you to store credentials that can be used by network scripts that support authentication.

You can create a new policy and add network scripts from the Authenticated category to perform an Authenticated Network Scan. At the same time, you can modify the existing policy to incorporate Authenticated network-scripts to perform an authenticated network scan.

Follow the below steps to create a new policy for performing an Authenticated Network Scan:

Step 1: Click the **New Policy** button on the top right of the page.

Step 2: A new screen appears, prompting you to select the scripts you want to be part of the New Policy.

Step 3: Click the filter icon and select the Authentication category. And click the **Apply** button.

Step 4: Network scripts from all the existing categories supporting authentication appear on the screen. Select the scripts and click the **Next** button.

Step 5: If the network script supports web apps scan, you need to provide the path where the web app resides. SanerNow Network Scanner will scan the web app using your selected network scripts.

Step 6: If the selected network script supports authentication, you can specify the credentials. SanerNow Network Scanner supports the following protocols.

a. HTTPS/HTTPS
b. SSH

For HTTP-type Authentication, you need to provide the following information:

a. HTTP Username
b. HTTP Password

For SSH-type Authentication, you need to provide the following information:

a. SSH Username
b. SSH Password OR

a. SSH Private Key

b. SSH Passphrase

Saving Credentials in Network Scanner

While creating a new scan policy, your credentials are stored and available only within the created policy. However, SanerNow Network Scanner allows you to store credentials separately that are not tied to any scan policy and can be used with network scripts that support authentication.

Follow the below steps to save credentials in Network Scanner.

Click the plus icon next to the **Saved Credentials** label. Previously saved credentials appear below the **Saved Credentials** label.

A pop-up window appears on the screen.

Before saving the credentials, select the **Authentication Type**; you can choose between HTTP and SSH.

If you select **HTTP authentication**, you need to provide the following information.

Name – Provide the name under which you want the credentials to be saved.

Authentication Type – Select the authentication type as HTTP.

HTTP Username – Provide the username you want the network script to authenticate. **HTTP Password** – Provide the password for the network script to authenticate.

If you select SSH authentication, you must provide the following information.

Name – Provide the name under which you want the credentials to be saved.

Authentication Type – Select the authentication type as SSH.

SSH Username – Provide the username you want the network script to authenticate.

SSH Password – Provide the password you want the network script to authenticate.

Alternatively, you can provide the **Private Key** and **Passphrase** instead of SSH Password.

Performing Agentless Scans on Endpoints

We’ve introduced the SanerNow Agentless Scanner – a unique scanner that allows you to perform an on-demand scan for vulnerabilities and misconfigurations on your devices without deploying an agent. You can also use the SanerNow Agentless Scanner to schedule periodic scans.

SanerNow Agentless Scanner can authenticate to the target devices using SMB and SSH to remote targets. However, the target machines need to meet specific prerequisites.

Pre-requisites needed for performing Agentless Scans

For Linux and Mac Devices

The device should have an SSH Server running on it.

For Windows Devices

a. SMB service should be running on the device.
b. You must ensure that inbound TCP communication on port 445 on the device's firewall is allowed.
c. The user logged into the device must have read/write access to the ADMIN$ share.
d. For devices not part of a domain, the ***LocalAccountTokenFilterPolicy*** must be provisioned to allow a full token on remote login. No changes need to be made in the case of devices that are part of an Active Directory domain.

> **Note**:
> The above requirements apply to target devices where you want to perform Agentless Scans. Endpoints designated as Network Scanners need not meet the prerequisites mentioned above.

Launching an Agentless Scan on Targeted Devices

You need to ensure that a Network Scanner exists in the Account. Follow the steps in the **Designating an Endpoint as a Network Scanner** section if a Network Scanner doesn't exist.

You can create a new Scan Configuration or edit an existing Scan Configuration to specify the target devices' IP address/ IP address range for the SanerNow Agentless Scanner to scan. You can refer to the **Managing Scan Configuration** section to know how to create/edit scan configuration in the SanerNow Network Scanner.

Creating a Scan Policy for Agentless Scanner

Step 1: Click the **New Policy** button on the top right of the page.

Step 2: A new screen appears, prompting you to select the scripts you want to be part of the New Policy.

Step 3: Click the filter icon and select the Authentication category. Click the **Apply** button.

Step 4: Uncheck the **Family** checkbox. Select the **Local Security Check** checkbox. You have two scripts under the Local Security Check family – Compliance and Vulnerability Scan. You need an active SanerNow VM subscription to perform a vulnerability scan. Similarly, you need an active SanerNow CM subscription to issue a compliance scan on the target devices.

SanerNow Agentless Scanner allows you to perform an individual scan, such as the Compliance Scan or Vulnerability Scan, or you can perform both scans on the target devices.

Step 5: Select the Authentication type. SanerNow Agentless Scan supports both SSH and SMB-type authentication on target devices.

For SSH-type Authentication, you need to provide the following information:

a. SSH Username
b. SSH Password OR

a. SSH Private Key

b. SSH Passphrase

For SMB-type authentication, you need to provide the username and password.

Also, you can use the saved credentials in the SanerNow Network Scanner to authenticate to target devices. Refer to the **Saving Credentials in the Network Scanner** section to learn how to save credentials in the SanerNow Network Scanner.

Click the **Next button** after providing the credentials.

> **Note**:
> SanerNow Agentless Scanner only supports SSH and SMB-type authentication. While saving credentials, ensure you don't use **HTTP**-type authentication to authenticate to target devices.

Step 7: Provide a Name for the newly created policy. You can briefly describe the policy, although it's not mandatory. Click the **Create Policy** button to create the Scan Policy.

Assigning the Scan Configuration and Scan Policy to the Agentless Scanner

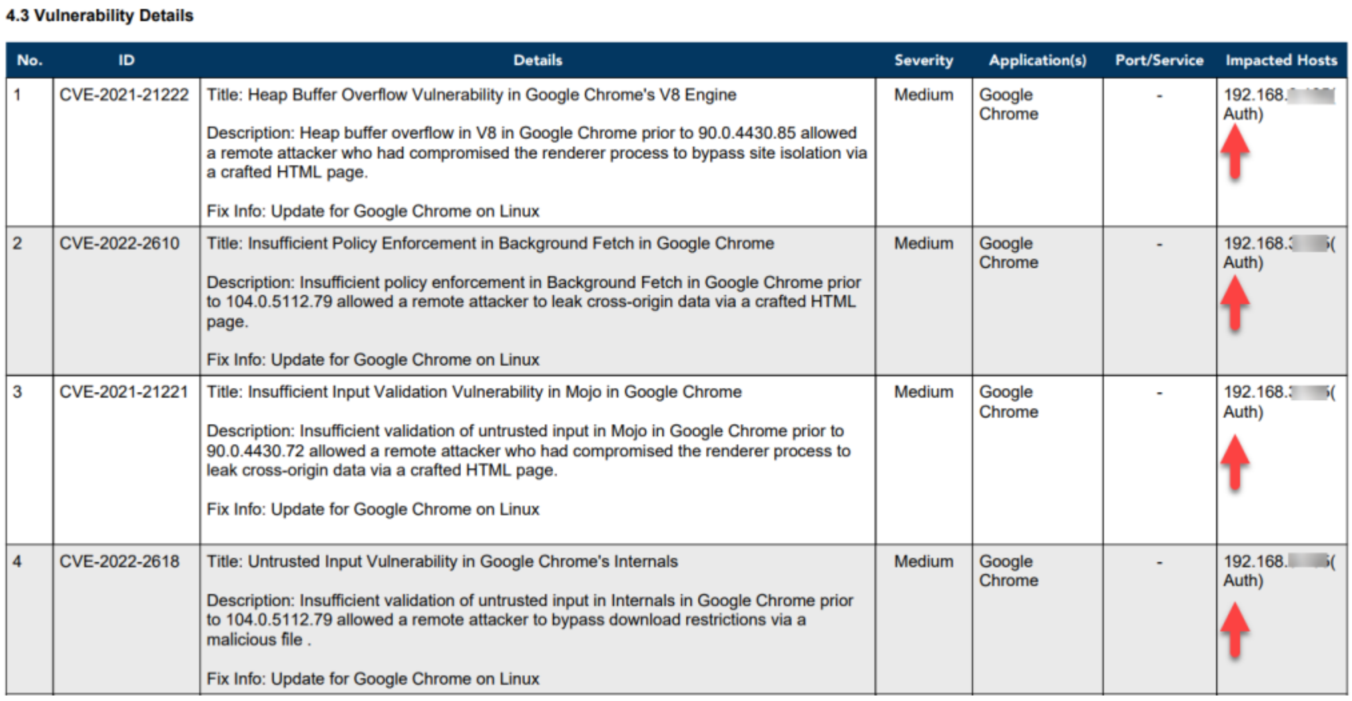
Click the **Summary** button and assign the **Scan Config** and **Scan Policy** to the Agentless Scanner.

Launch the scan by clicking the play ▶ button located right next to the Agentless Scanner. The Agentless Scanner will launch the scan on the target devices specified in the Scan Config.

Viewing the Agentless Scanner Results

SanerNow Agentless Scanner stores the scan results performed on the target devices. You can access this information by clicking the ℹ button. You can also download the result in PDF format by clicking the ⤓ button.

The Network Scan Report PDF file has a Vulnerability and Misconfigurations Details section. The target device IP Address is listed in the Impacted Hosts table. Right next to the IP Address, in the bracket, it will be specified as **Auth** – this indicates the target device was scanned using the SanerNow Agentless Scanner.



4.3 Vulnerability Details

No.	ID	Details	Severity	Application(s)	Port/Service	Impacted Hosts
1	CVE-2021-21222	Title: Heap Buffer Overflow Vulnerability in Google Chrome's V8 Engine Description: Heap buffer overflow in V8 in Google Chrome prior to 90.0.4430.85 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. Fix Info: Update for Google Chrome on Linux	Medium	Google Chrome	-	192.168.[redacted](Auth)
2	CVE-2022-2610	Title: Insufficient Policy Enforcement in Background Fetch in Google Chrome Description: Insufficient policy enforcement in Background Fetch in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to leak cross-origin data via a crafted HTML page. Fix Info: Update for Google Chrome on Linux	Medium	Google Chrome	-	192.168.[redacted](Auth)
3	CVE-2021-21221	Title: Insufficient Input Validation Vulnerability in Mojo in Google Chrome Description: Insufficient validation of untrusted input in Mojo in Google Chrome prior to 90.0.4430.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. Fix Info: Update for Google Chrome on Linux	Medium	Google Chrome	-	192.168.[redacted](Auth)
4	CVE-2022-2618	Title: Untrusted Input Vulnerability in Google Chrome's Internals Description: Insufficient validation of untrusted input in Internals in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to bypass download restrictions via a malicious file . Fix Info: Update for Google Chrome on Linux	Medium	Google Chrome	-	192.168.[redacted](Auth)

Discovering Devices Using Network Scanner

Go to the Control Panel Page. Click the **Deployment.** Under Deployment, click **Device Scanning**.

On the right side of the page, select the **Network Scanner** and provide the IP address range. Click the **Discover** button. SanerNow Network Scanner will search for devices within the specified range.

You can schedule the Network Scanner to run the discovery scan periodically. The following options are available for scheduling a Device Discovery scan:

a. Daily
b. Weekly
c. Monthly

The devices found by the SanerNow Network Scanner are listed under the **Unmanaged Devices** section on the Managed Devices page. This helps you get better clarity on the number of devices that don't have SanerNow Agent installed.

You can perform actions on the devices listed under Unmanaged Devices using the Action buttons.

Button	Usage
⊕	The Add Device button adds discovered devices into SanerNow. A system administrator can use this button to add multiple devices to SanerNow by importing a CSV file that contains information related to the device.
⬇	The Deployment button deploys SanerNow Agents onto a device. A system administrator can deploy SanerNow Agent onto a device using the 'Show Agent Download URL' or 'Download Deployer Tool.'
⊞	The Create Group button creates custom groups. You can add devices to these custom groups.

🗑	The Delete Device button deletes a device permanently from SanerNow.

Viewing Network Devices Vulnerabilities

Network Scanner stores the results of the network scan on the SanerNow server. These results contain the vulnerabilities discovered in devices scanned as part of the network scan by the Network Scanner. You can view all the details associated with the network device (that includes Vulnerabilities, Misconfigurations, Assets, Ports, and Services on the Device Details Page.)

You can access the Device Details page using the below-mentioned pages.

1. Managed Device Page.
2. Vulnerability Management Dashboard.
3. Compliance Management Dashboard.
4. Asset Exposure Dashboard.

Note:
Network Scanner only identifies vulnerabilities and misconfigurations in a device. To remediate a vulnerability found in a network device, you must manually remediate it. We recommend using SanerNow tools to remediate the discovered vulnerabilities and misconfigurations.

Viewing Network Devices vulnerability on the Device Details Page

On the **Menu bar**, click the display icon 🖥 on the left side of the Admin Dashboard. You will be redirected to the **Managed Devices** page.

On the Managed Devices page, on the right side, you will see all the managed devices available for the selected Account presented in a tabular format.

Here, you can see the devices that SanerNow Agent and SanerNow Network Scanner manage.

For devices managed by Network Scanner, under the **Managed By** column, you can see 🔍 icon right next to them. This means that these are network devices and don’t have SanerNow Agents installed on them. The vulnerabilities discovered in these network devices need manual remediation. We recommend subscribing to SanerNow tools to help you in remediation.

Click the **Host Name**. This will take you to the **Device Details** page. You can find all the information related to the device, including CHS Score, Vulnerabilities, Misconfigurations, Assets, Ports, and Services, on this page.

Click here to learn more about the Device Details page.

Device Details Page

You will find all the details related to the network device on the Device Details page. Let’s break down the details displayed on the Device Details Page.

The top section of the page displays the following details:

a. **Cyber Hygiene Score**: The CHS Score for the device will be displayed right below the device icon.
b. **Device Name**: This label displays the host's name detected during the network scan.
c. **Operating System**: This label displays the name of the operating system detected running on the host during the network scan.
d. **Mac Address**: This label displays the host's mac address detected during the network scan by the Network Scanner.
e. **IP Address**: This field displays the IP Address assigned to the device.
f. **Last Scan**: This label displays the date and time Network Scanner scanned the device.
g. **Export Device Report**: This button downloads all the details about the host presented on the screen in a .pdf format.

You will find four menu options on the left side of the Device Details page. They're as

a. Device Details
b. Posture Anomaly
c. Vulnerabilities
d. Patches

Assets

This section displays all the software present on the network device with their relevant version number.

Vulnerabilities

This section displays all the vulnerabilities detected in the device.

Misconfigurations

This section displays all the Common Configuration Enumeration (CCE) IDs related to the device.

Ports /Services

This section displays the various ports on the network device, the protocol running on each, and the local address mapped to these ports. Also, this section shows all the services on the device with their current status.

Viewing vulnerable network devices in the Vulnerability Management tool

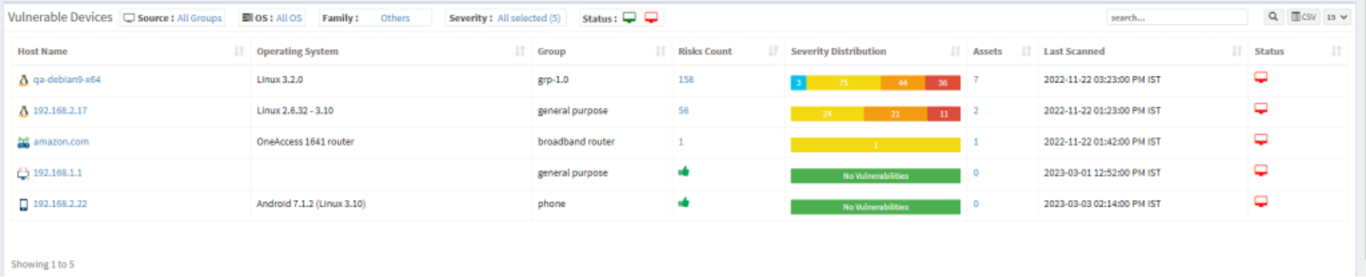
In the two sections below, you can view vulnerable devices connected to your network in the SanerNow VM tool.

1. Vulnerable Devices Section
2. Vulnerabilities Section

Vulnerable Devices Section

On the SanerNow VM tool dashboard, go to the **Vulnerable Devices** section. Click the **Family** filter and select **Others** to list all the vulnerable networks in your Account.

Once you apply the **Others** filter, your screen will look like the screen below.



Vulnerable Devices Source : All Groups OS : All OS Family : Others Severity : All selected (5) Status : 🖥 🖥 search...

Host Name	Operating System	Group	Risks Count	Severity Distribution	Assets	Last Scanned	Status
qa-debian9-x64	Linux 3.2.0	grp-1.0	158	3 75 44 36	7	2022-11-22 03:23:00 PM IST	🖥
192.168.2.17	Linux 2.6.32 - 3.10	general purpose	56	24 21 11	2	2022-11-22 01:23:00 PM IST	🖥
amazon.com	OneAccess 1641 router	broadband router	1	1	1	2022-11-22 01:42:00 PM IST	🖥
192.168.1.1		general purpose	👍	No Vulnerabilities	0	2023-03-01 12:52:00 PM IST	🖥
192.168.2.22	Android 7.1.2 (Linux 3.10)	phone	👍	No Vulnerabilities	0	2023-03-03 02:14:00 PM IST	🖥

Showing 1 to 5

Below mentioned information is presented in the table under the Vulnerable Devices section:

1. **Host Name** ––This column displays the hostname of the device. You can click on the hostname, which will take you to the Device Details Page, where you can find detailed information about all the vulnerabilities detected in the device.
2. **Operating System** –– This column displays the operating system running on the device.
3. **Group** –– This column displays the group to which the device belongs.
4. **Risks Count** –– This column displays the total number of vulnerabilities found in the device.
5. **Severity Distribution** –– This column displays the breakdown of the total number of vulnerabilities found in the device. The vulnerabilities are categorized into Critical, High, Medium, and Low. And these categories are color coded. They are as follows:

Vulnerability Category	Color Code
Critical	Red
High	Orange
Medium	Yellow
Low	Blue

6. **Assets** — This column displays the name and the number of vulnerable software running on the device. You can view the list of vulnerable applications running on the device by clicking the number in the column.

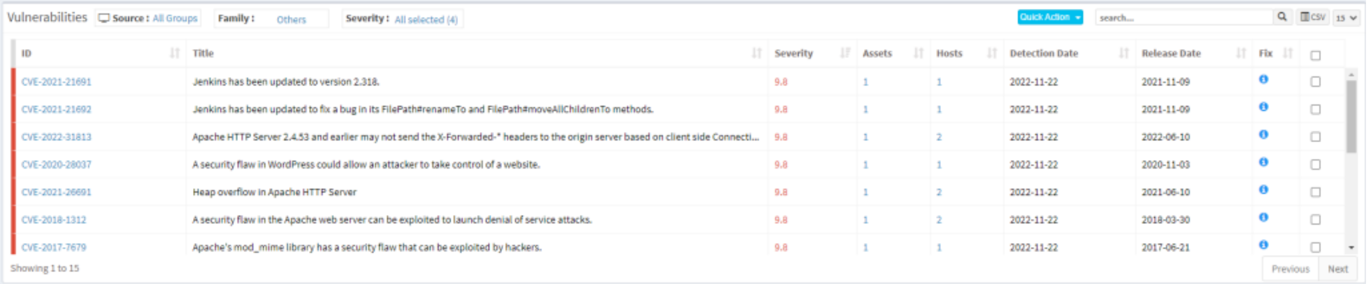
7. **Last Scanned** — This column displays the date and time a scan was performed on the device.

8. **Status** — This column displays whether the device is Active or Inactive.

Note:
You will see a thumbs-up icon for devices with no associated vulnerabilities in the Risks Count column and a *No Vulnerabilities* progress bar in the Severity Distribution column.

Vulnerabilities Section

In the Vulnerabilities section, you can view the vulnerabilities listed by Common Vulnerabilities and Exposures (CVE) ID. The table displays **Assets**, **Hosts**, and the day the vendor publicized the vulnerability. Also, the table shows the date on which the SanerNow VM tool detected the vulnerability and the relevant fix.



ID	Title	Severity	Assets	Hosts	Detection Date	Release Date	Fix	□
CVE-2021-21691	Jenkins has been updated to version 2.318.	9.8	1	1	2022-11-22	2021-11-09	🛈	□
CVE-2021-21692	Jenkins has been updated to fix a bug in its FilePath#renameTo and FilePath#moveAllChildrenTo methods.	9.8	1	1	2022-11-22	2021-11-09	🛈	□
CVE-2022-31813	Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connecti...	9.8	1	2	2022-11-22	2022-06-10	🛈	□
CVE-2020-28037	A security flaw in WordPress could allow an attacker to take control of a website.	9.8	1	1	2022-11-22	2020-11-03	🛈	□
CVE-2021-26691	Heap overflow in Apache HTTP Server	9.8	1	2	2022-11-22	2021-06-10	🛈	□
CVE-2018-1312	A security flaw in the Apache web server can be exploited to launch denial of service attacks.	9.8	1	2	2022-11-22	2018-03-30	🛈	□
CVE-2017-7679	Apache's mod_mime library has a security flaw that can be exploited by hackers.	9.8	1	1	2022-11-22	2017-06-21	🛈	□

Showing 1 to 15

Below mentioned information is presented in the table under the Vulnerable Section:

1. **ID** — This column shows the unique CVE ID associated with the vulnerability detected in the devices.
2. **Title** — This column shows a brief description of the detected CVE.
3. **Severity** — This column shows the *Severity* score given to the CVE.
4. **Assets** — This column shows the total number of assets the CVE affects in the selected Account.
5. **Hosts** — This column shows the total number of hosts affected by the CVE in the selected Account.
6. **Detection Date** – This column shows the date the vulnerability related to the CVE was detected by the SanerNow VM tool.
7. **Release Date** – This column shows the date on which the vendor released the CVE related to the vulnerability.
8. **Fix** – This column displays the necessary action to fix the relevant vulnerability.

SanerNow Network Scanner Logs

SanerNow Network Scanner records all the actions performed within the tool and assigns a unique code to each action.

To access the Logs section, click the **Logs** button on the top right of the Network Scanner page.

SanerNow Network Scanner logs are displayed in a tabular format. The table below displays the following information:

a. **Job Code** – The Job Code associated with the action performed within the SanerNow Network Scanner tool.
b. **Date** – The date and time the action was performed within Network Scanner.
c. **Organization** – The Organization to which the Account belongs is displayed here.
d. **Account** – The Account to which the User belongs is displayed here.
e. **User** – The user's name who performed the action in Network Scanner is displayed here.
f. **Message** – The action performed using the Network Scanner is described here.

You can filter the logs presented in the Log table. The following filters are available:

a. **Accounts** – This filter will display Account-specific logs. You can specify more than one Account at a time while filtering logs by Account.

b. **Users** – This filter displays User-specific logs. You can specify more than one User at a time while filtering logs by User.
c. **Start Date and Date**: This filter can show logs within a specified date range.

To remove any applied filters, click the **Clear All** button on the top right of the page. If there are multiple log entries, you can limit the log entries displayed on the screen by selecting the value from the **Size** drop-down box. You can choose 10, 25, 50, and 100 log entries to be shown simultaneously.

The table below lists SanerNow Network Scanner job codes with their brief description.

Job Code	Description
14000	Network Scanner Management
14001	Initiate Discovery Scan
14002	Add Discovery Scan Configuration
14003	Update Discovery Scan Configuration
14004	Delete Discovery Scan Configuration
14005	Upload Discovery Scan Data
14006	Failed to Upload Discovery Scan Data
14007	Add Network Scan Device
14008	Failed to Add Network Scan Device
14009	Updated Network Scan Device
14010	Failed to Update Network Scan Device
14011	Failed to Add Discovery Scan Configuration
14012	Failed to Update Discovery Scan Configuration
14013	Failed to Delete Discovery Scan Configuration
14014	Stop Network Scan
14015	Delete Device
14016	Failed to Delete Device
14017	Rename Network Scan Device
14018	Failed to Rename Network Scan Device
14019	Updated Device as Network Scanner
14020	Failed to Update Device as Network Scanner
14021	Removed Device as Network Scanner
14022	Failed to Remove Device as Network Scanner
14023	Initiate Network Scan
14024	Add Network Scan Configuration
14025	Failed to Add Network Scan Configuration
14026	Update Network Scan Configuration
14027	Failed to Update Network Scan Configuration

14028	Delete Network Scan Configuration
14029	Failed to Delete Network Scan Configuration
14030	Add Network Scan Policy
14031	Failed to Add Network Scan Policy
14032	Update Network Scan Policy
14033	Failed to Update Network Scan Policy
14034	Delete Network Scan Policy
14035	Failed to Delete Network Scan Policy