Adding a probe in SuperOps

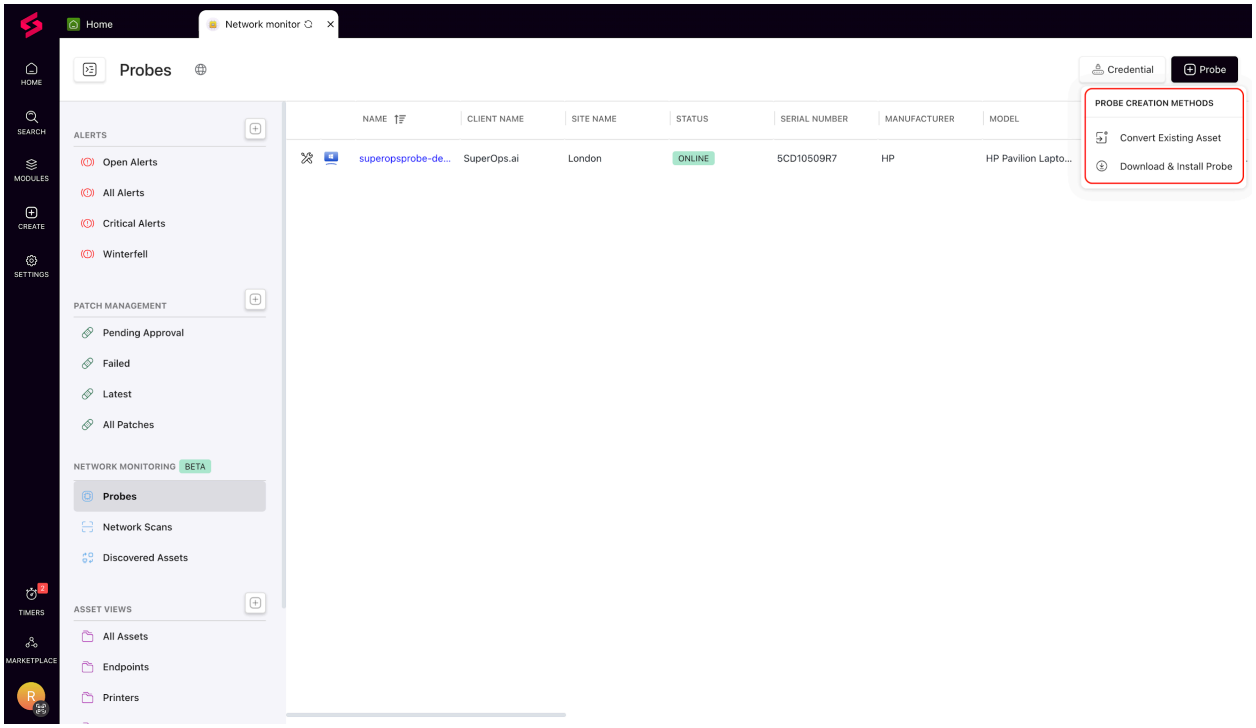
What is a probe?

A probe in SuperOps is a crucial tool used for scanning devices within a network. These probes perform regular scans to gather essential information, including performance and health metrics like CPU usage and memory status. By collecting such data from network devices, probes offer valuable insights that facilitate optimization efforts.
You can create a probe in two different ways. You can either convert an existing asset into a probe, or you can download and install a new probe. Keep reading to see how you can do both.

Adding a probe

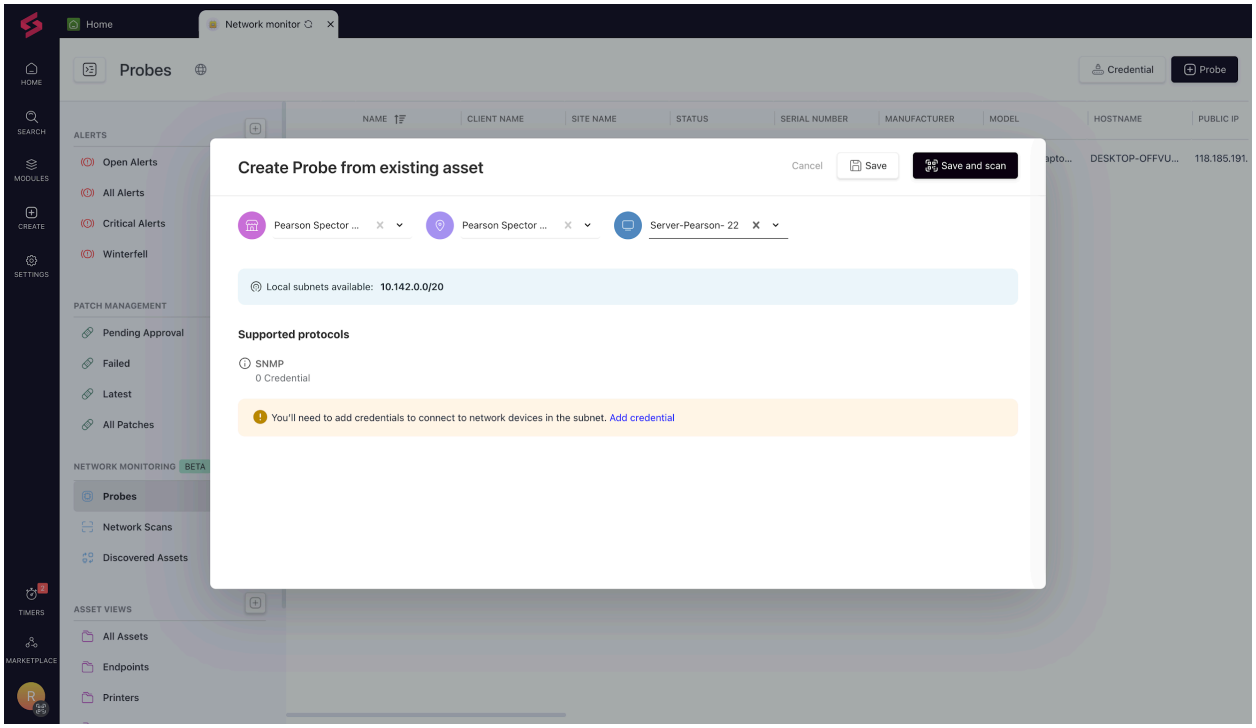
To add a new probe,

1. Navigate to Modules > Network Monitor > Probes.
2. Click the +Probe button in the top right corner as shown below.



To convert an existing asset into a probe:

1. Click the “Convert an existing asset into a probe” option.
2. Choose the client, site, and asset from the drop-down list as shown below.

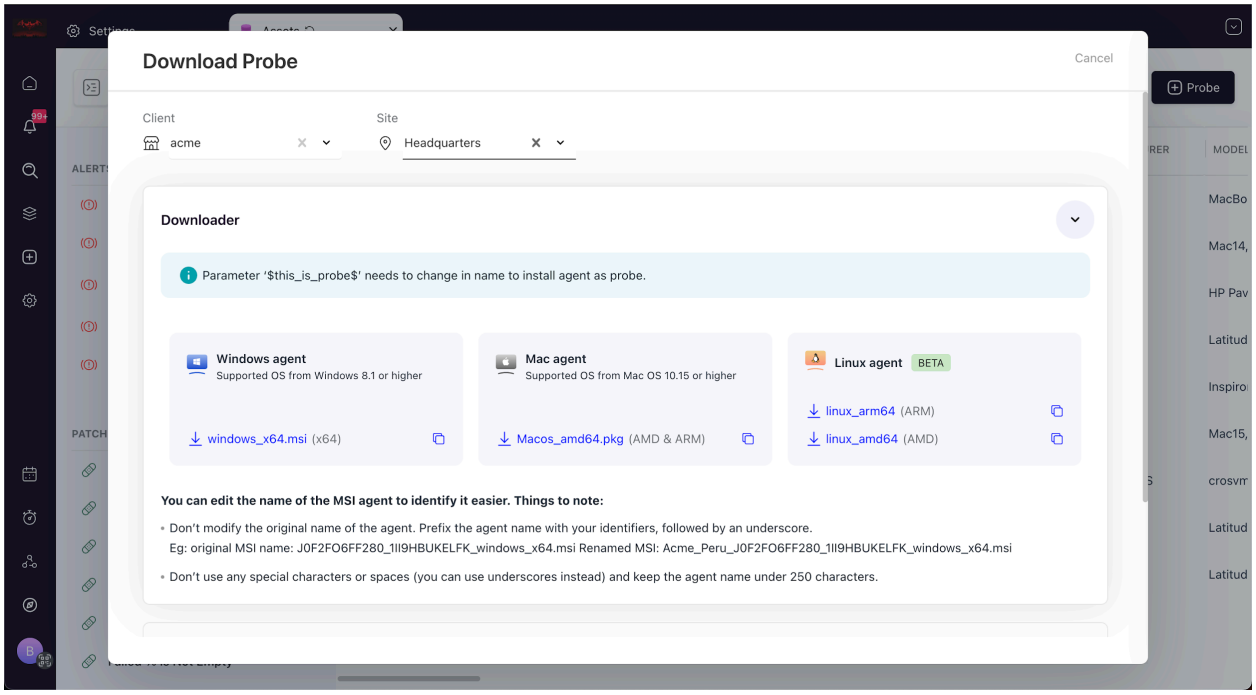


3. The subnet and the SNMP credentials will be automatically fetched from the asset information.
4. In case there are no credentials supported for that asset, you can click “Add Credential” to add new credentials for that probe.
5. Click here to learn more about Credentials in SuperOps
6. Once done, click “Save and Scan” to initiate network scans for that probe.

📝 Note: In some cases, the asset might not fetch subnets automatically and you will have to add subnets for those probes manually. Click here to learn how you can do this.

Downloading and Installing a new Probe:

1. Click on the “Download and Install Probe” option
2. Choose the client and site at which you want to install the probe.
3. Once you’re done, the installer files for the client and site will be displayed (for Windows, Mac, and Linux), ready for you to download.



4. Once the download is complete, install the downloaded MSI installer in the terminal with the attribute RUNASPROBE using the following command:

› install as a probe in Windows:

ntax:

siexec.exe /i PATH_OF_DOWNLOADED_MSI /QN /L*V "installation.log" LicenseAccepted=yes

JN_AS_PROBE=yes

:ample:

ısiexec.exe /i

:\Users\LENOVO\Downloads\GV6IOTWD9ERK_1N0X7AM2S43R4_windows_x64.msi /QN /L*V

ıstallation.log" LicenseAccepted=yes RUN_AS_PROBE=yes

5. If there are no credentials associated with the client and site you chose, make sure you create a new SNMP credential, by clicking on the “Add Credential” button below.

Managing your Subnets in SuperOps

What are subnets?

In network monitoring, subnets are smaller portions of a larger IP address range, that help technicians manage and monitor network devices more efficiently.
You can connect to subnets in two ways:

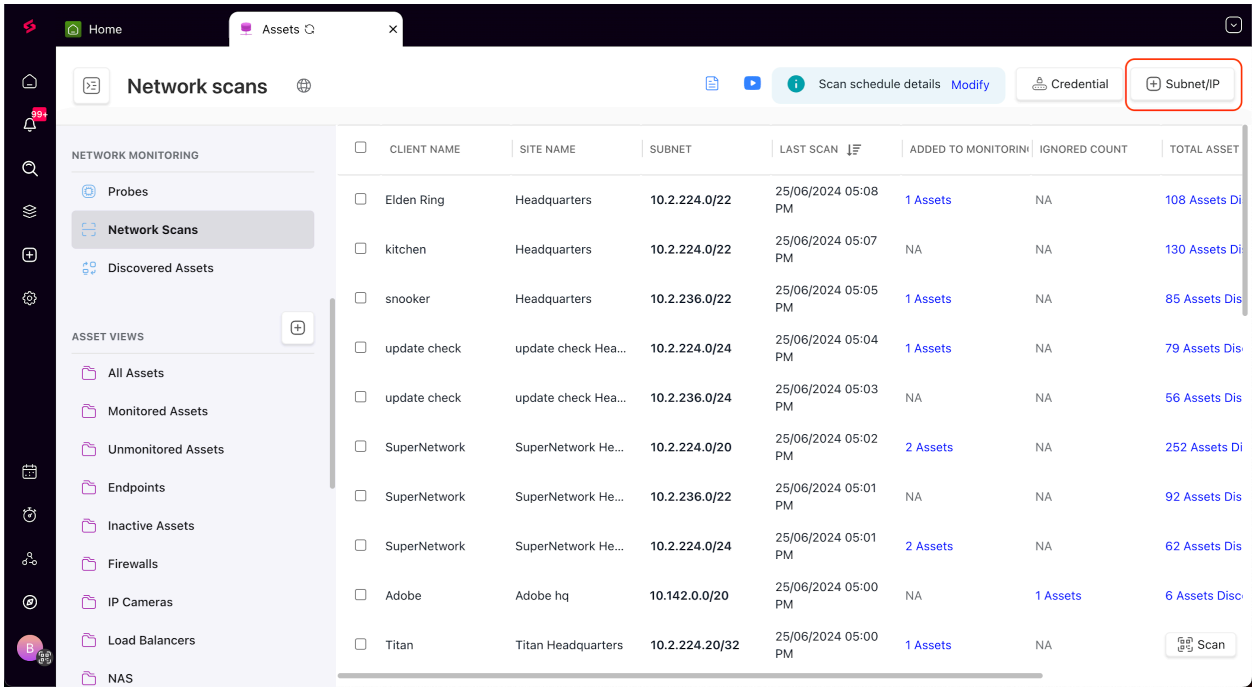
1. Through a probe: If a network’s probe is connected to a subnet, then you can use the probe to run a network scan and access all the network devices connected to that particular subnet
2. A subnet that is reachable by the probe but not directly connected to it can be manually added to scan network devices.

Since the first method of connecting to a subnet happens automatically, let’s look at how you can manually add subnets.

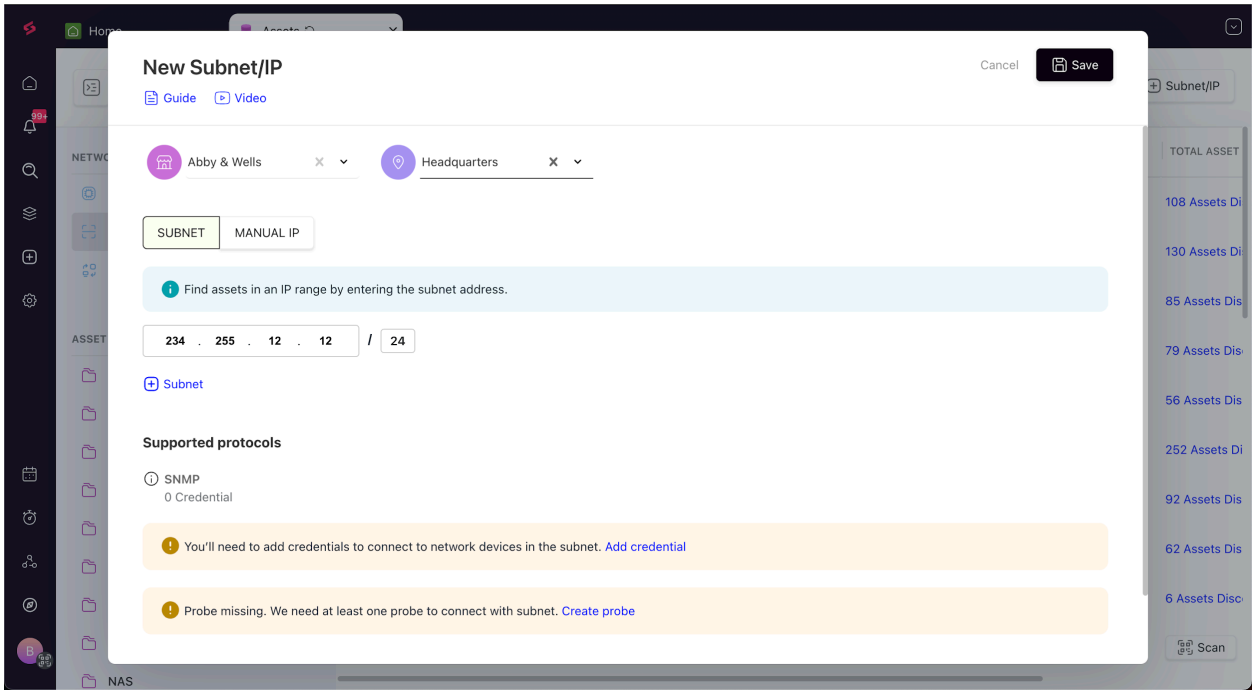
Manually adding subnets

While subnets are automatically fetched for some clients and sites, you can manually add custom subnets in the network that you want to monitor. Here's how:

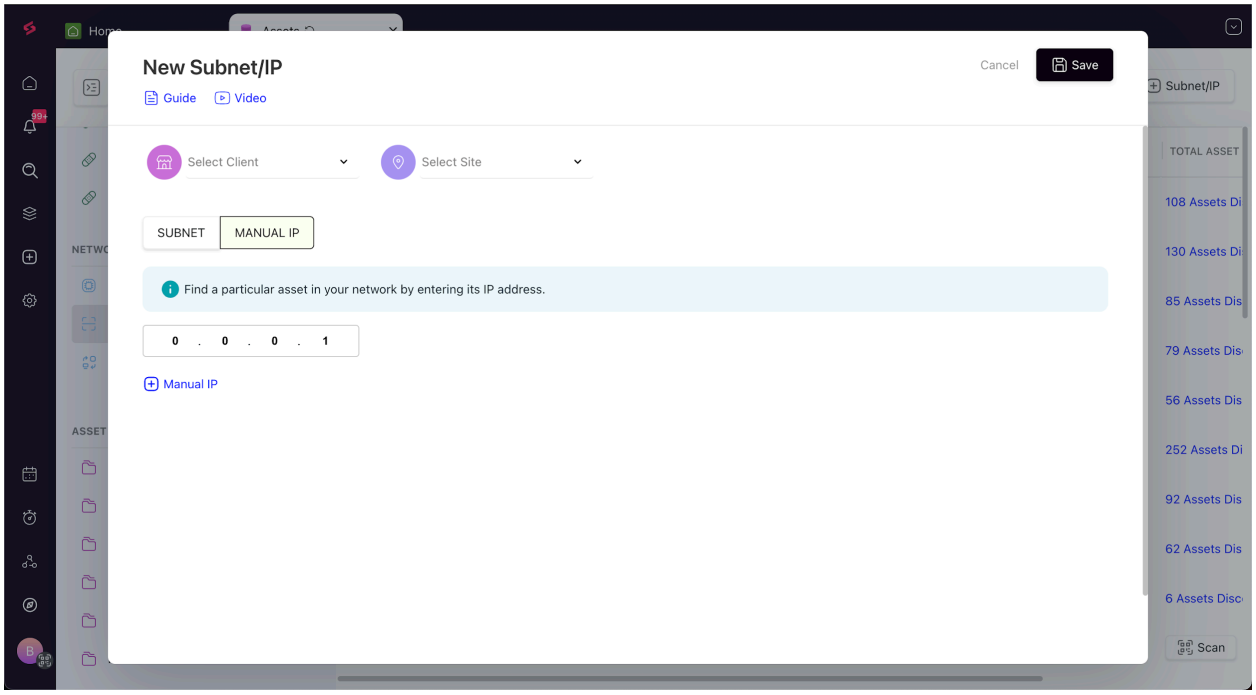
1. Navigate to Modules > Network Monitoring > Network Scans
2. Click the +Subnet/IP button on the top right corner, as shown below.



3. Now, select a client and site for which you want to associate the subnet.
4. Enter the subnet address and hit save once you are done. You can create multiple subnets at one go with the +Subnet button.



5. These subnets will now be linked to the specified client and site.
6. Keep in mind that for subnet scans to occur, there must be probes and credentials associated with the selected client and site.
7. You can create a new probe or credential from the same page by clicking on the Add Credential or Create Probe button.
8. If you would like to add a particular asset, you can use the Manual IP option to do so. Enter the IP address of the asset(s) and hit Save once done.



Running network scans

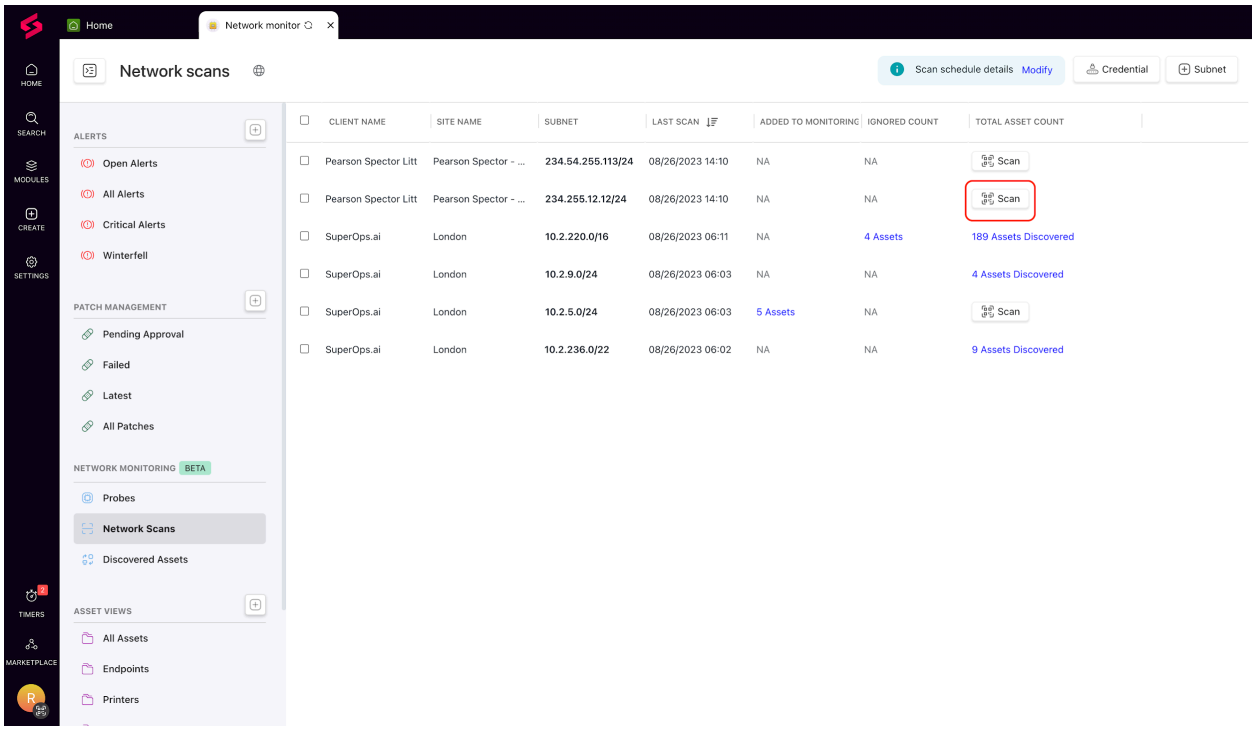
What are network scans?

A network scan is the process of discovering and identifying network devices within a specific network or subnet.
During a network scan, the SuperOps probe sends out a series of SNMP requests to different IP addresses marked under the network/subnet's range. The SNMP-enabled devices will respond back, and the probe gathers information on the performance, configuration, and health of those devices (provided that the device matches your credentials and gets added to monitoring.)

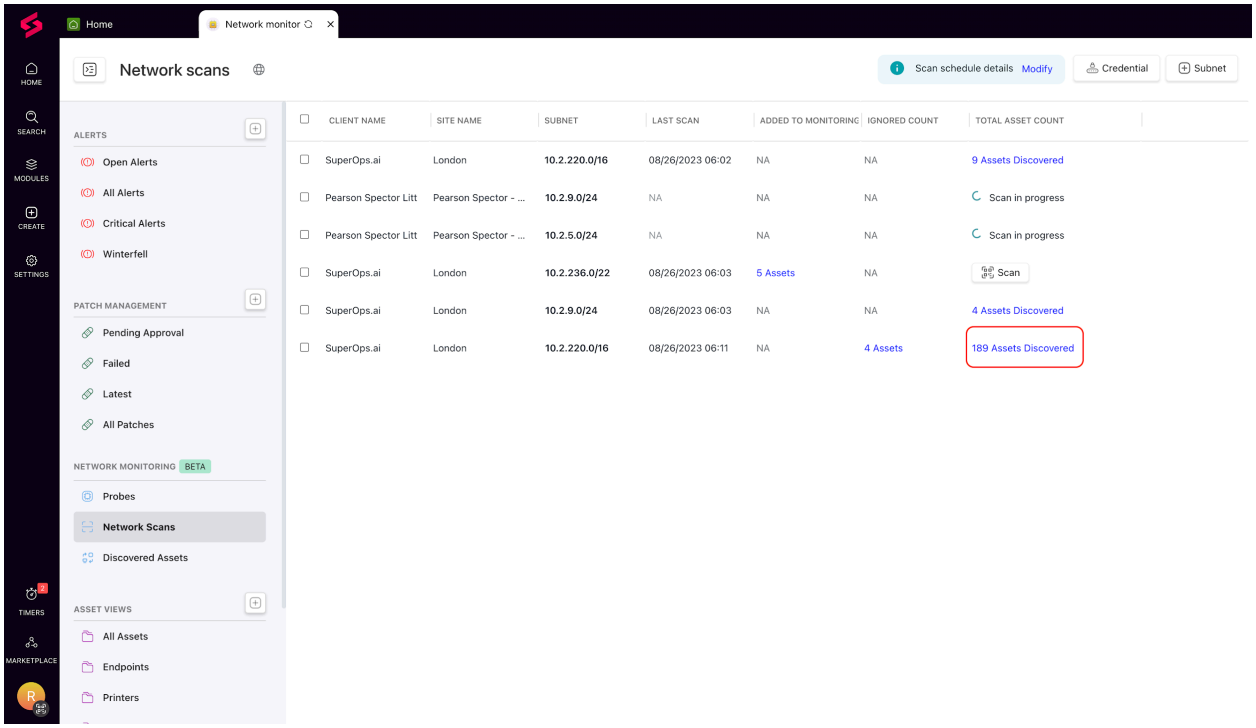
Running network scans in SuperOps

To run network scans in SuperOps, you must have already added a probe to the specific client and site for which you want to run the network scan.
Click here to learn how you can add a probe, credential, and subnet.
Once the probe is installed and the credentials and subnets are mapped, you will see a list of all the clients that have a probe. Here's how you can view that list:

1. Navigate to Modules > Network Monitor > Network Scans
2. In this list view, you can start running scans by clicking on the Scan button, as shown below.



3. Once the scan is done, you will see the number of assets discovered under the Total Asset Count tab.

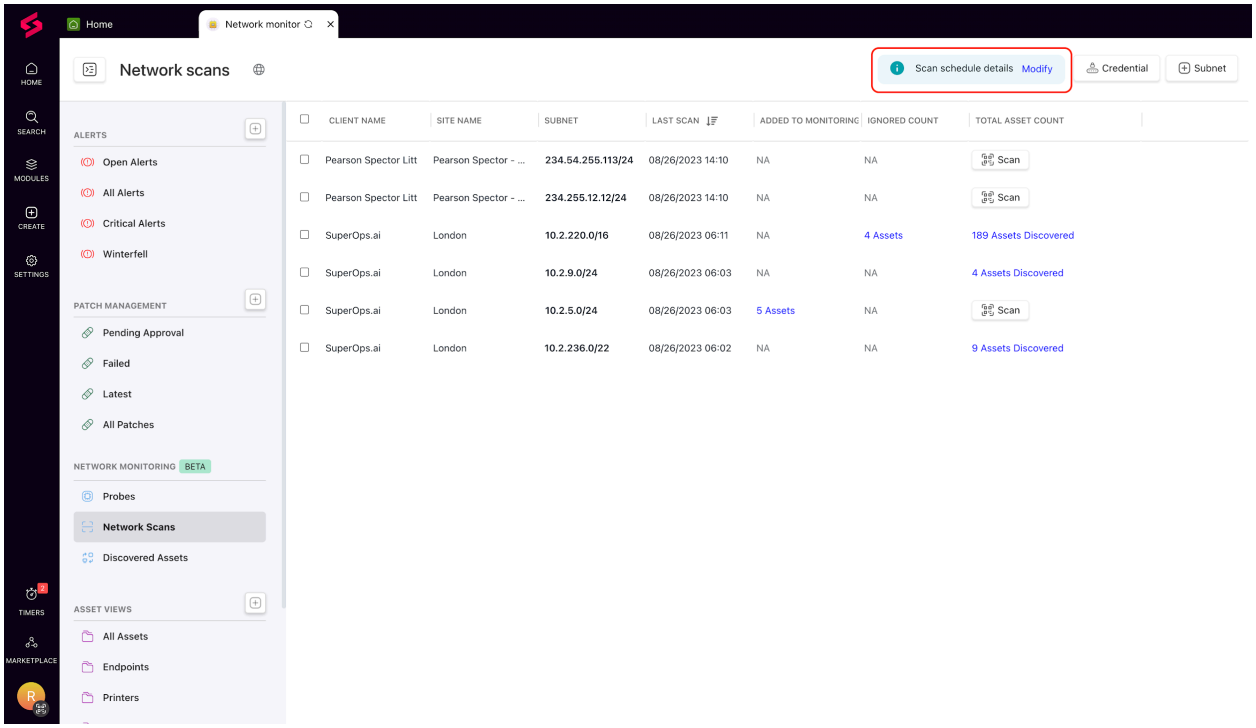


4. Click on assets discovered to view the list of all devices discovered from the scan. Here, You can see known, unknown, and failed assets.

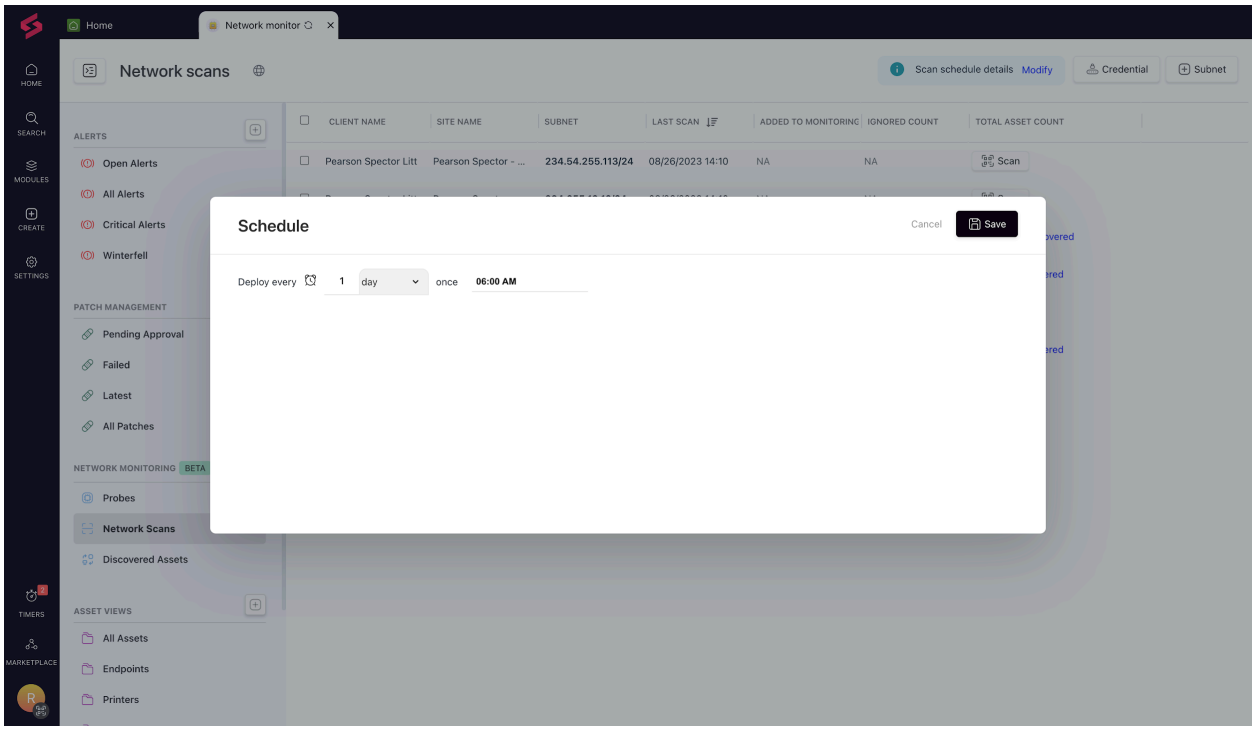
📝Note: Wondering what the asset categories we mentioned above are? We've written about them in detail here 👉 managing your known and unknown assets.

Managing the network scan schedule

1. SuperOps automatically runs network scans to spot any new devices that have been added to the network/subnet. You can modify this schedule into a cadence that fits your needs best. You can do so by clicking Modify on the top right.



2. Set your new schedule for the network scan and hit save.



Setting up SNMP credentials in SuperOps

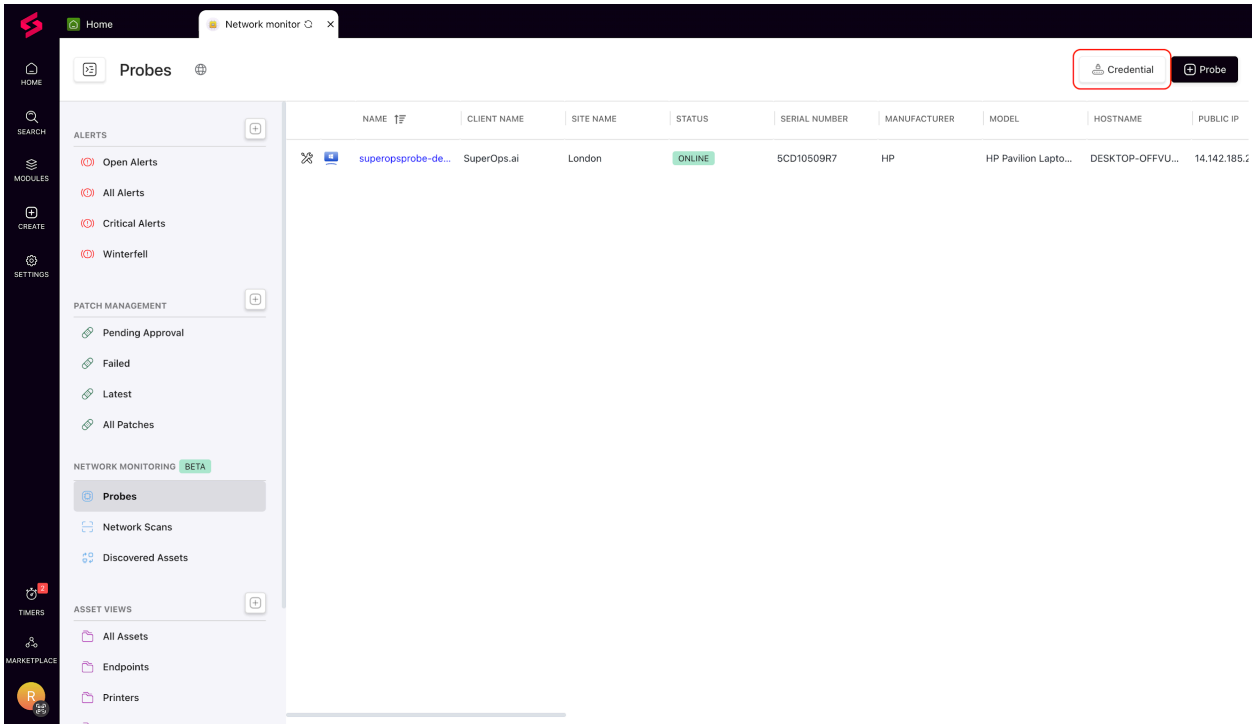
What are credentials?

A credential in SNMP is an authentication key, often in the form of a community string, used to securely access and manage network devices. It verifies the legitimacy of requests and controls the level of access granted. There are three types of credentials used in SNMP - Version 1 (v1), Version 2 (v2c), and Version 3 (v3).
Let's learn how you can set up credentials in SuperOps

Setting up credentials

To set up credentials in SuperOps,

1. Navigate to Modules > Network Monitor > Probes or Network Scans or Discovered Assets
2. Click the "Credential" button in the top right corner, as shown below.

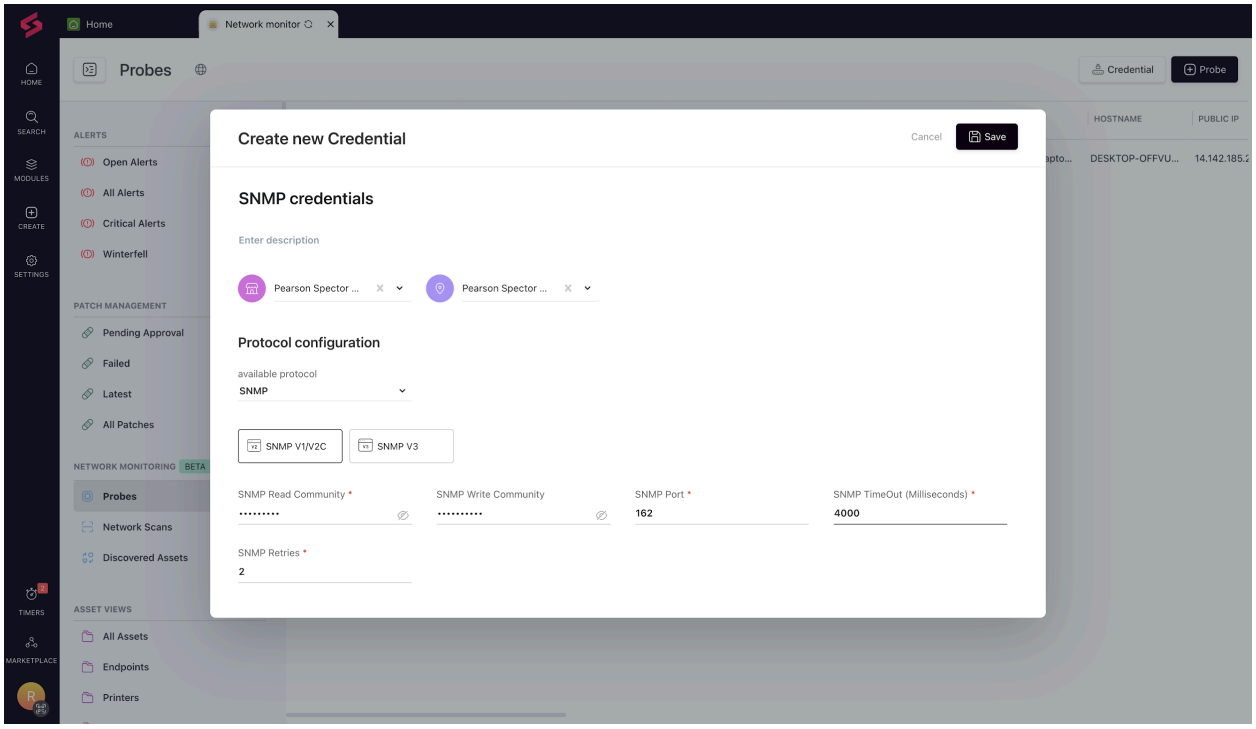


3. On the Create Credentials page, give a name and description for the credential and choose a client and site with which you want the credential to be associated.

4. Under Protocol Configuration, you need to select the protocol of the credential. Currently, the SNMP protocol is supported.

5. Choose the type of credential - V1/V2C or V3 and enter the values required for the corresponding credentials.

6. SNMP V1/V2C uses the following credentials:



- Read community: Password to access the device's data. You cannot make changes to the device's configuration with Read-Only credentials.
- Write community: Password to Update the device's configuration. You can retrieve information and make changes with Read-Write credentials.
- SNMP Port (161, 162, 163): The SNMP ports facilitate communication between the Probe and the devices.
- SNMP Timeout: This parameter specifies the maximum amount of time that the Probe is willing to wait for a response from the device after sending a request.

⚡ SuperTip: Recommended timeout is 5 to 7 seconds

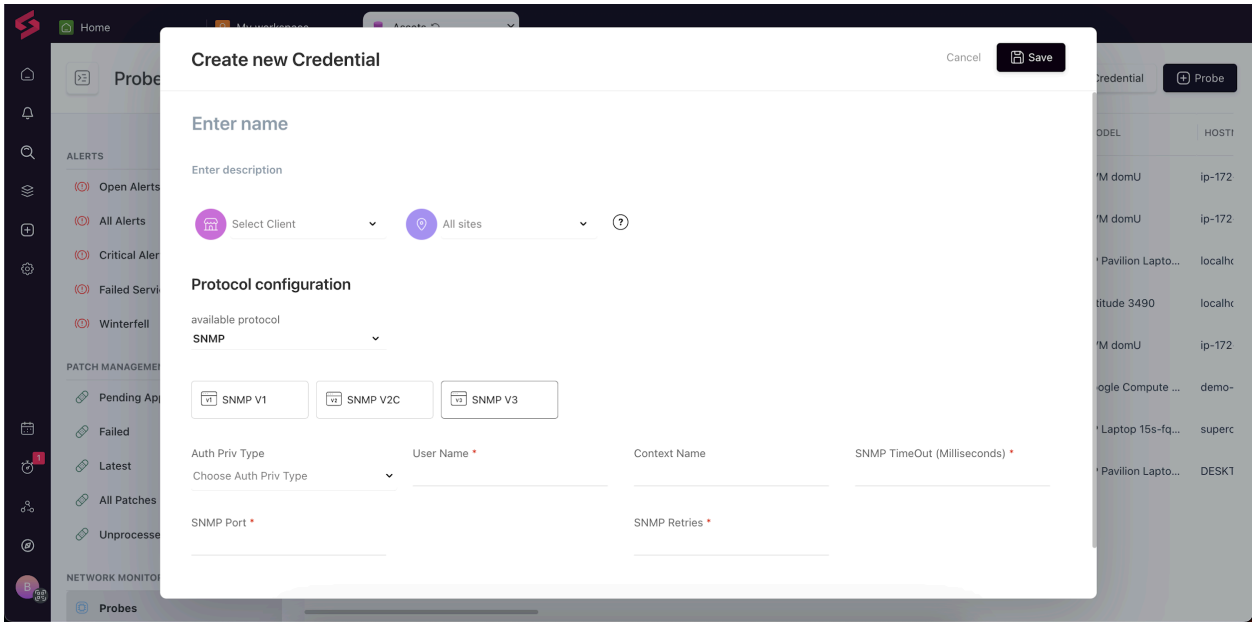
- SNMP retries: This value determines how many times the Probe will attempt to resend a request if it doesn't receive a response within the specified timeout. After the specified number of retries, it will mark the device as a failed asset.

⚡ SuperTip: The recommended number of retry attempts is 1 or 2.

📝Note: Within SuperOps, if you provide details exclusively for the Read-only community, it will be categorized as a V1 credential type. Conversely, when values are entered for both Read and Write communities, it will be designated as a V2 credential type.

---

7. SNMP V3 uses the following credentials:



- User Name: A unique identifier for the probe.
- Context Name: Used to differentiate multiple domains within a network.
- Authentication Method (MD5, SHA): Verifies that the data received by the probe is not tampered with during transmission.
- Encryption Method (DES, AES): Ensures that the transmitted data cannot be accessed by unauthorized agents.

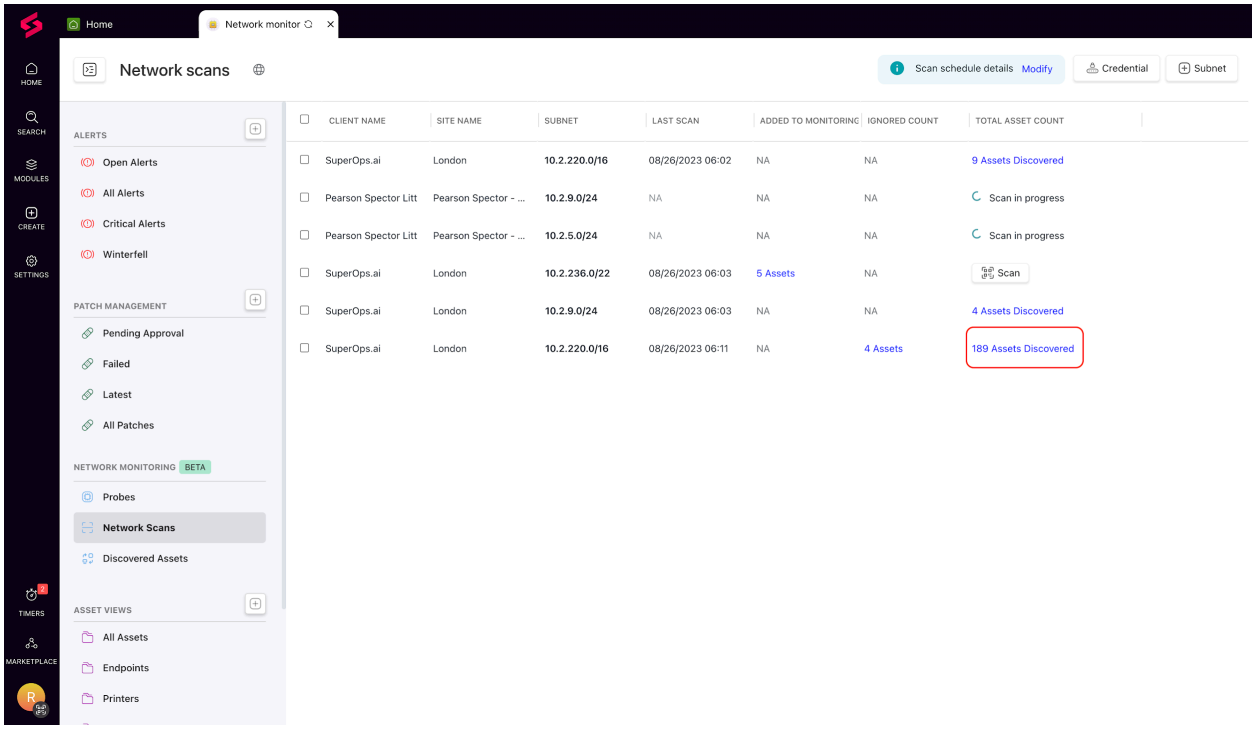
8. Once you've filled in all the required values, click save to add the credential.

Managing discovered assets and monitoring protocols

Updated over a year ago

Managing discovered assets

When you initiate a network scan, the probe will start looking for assets it can discover in your network. Once the scan is complete, all discovered assets will be pulled into SuperOps and listed according to their statuses.
Under Network Scans, you will see the list of scans that have been completed by the probe. Think of this as a view that contains all your subnets. For each subnet, the results of the scan can be seen by click on "x assets discovered" that you see under the total asset count column.



We also have a separate tab called Discovered Assets, which shows you a cumulative list of all scan results put together, irrespective of the client and site. When you click on a scan result, you will see the following tabs:

- Network Assets: All network devices discovered by the probe via SNMP fall under this tab.
- Endpoints (Coming Soon): All workstations and servers discovered by the probe via ICMP fall under this tab.

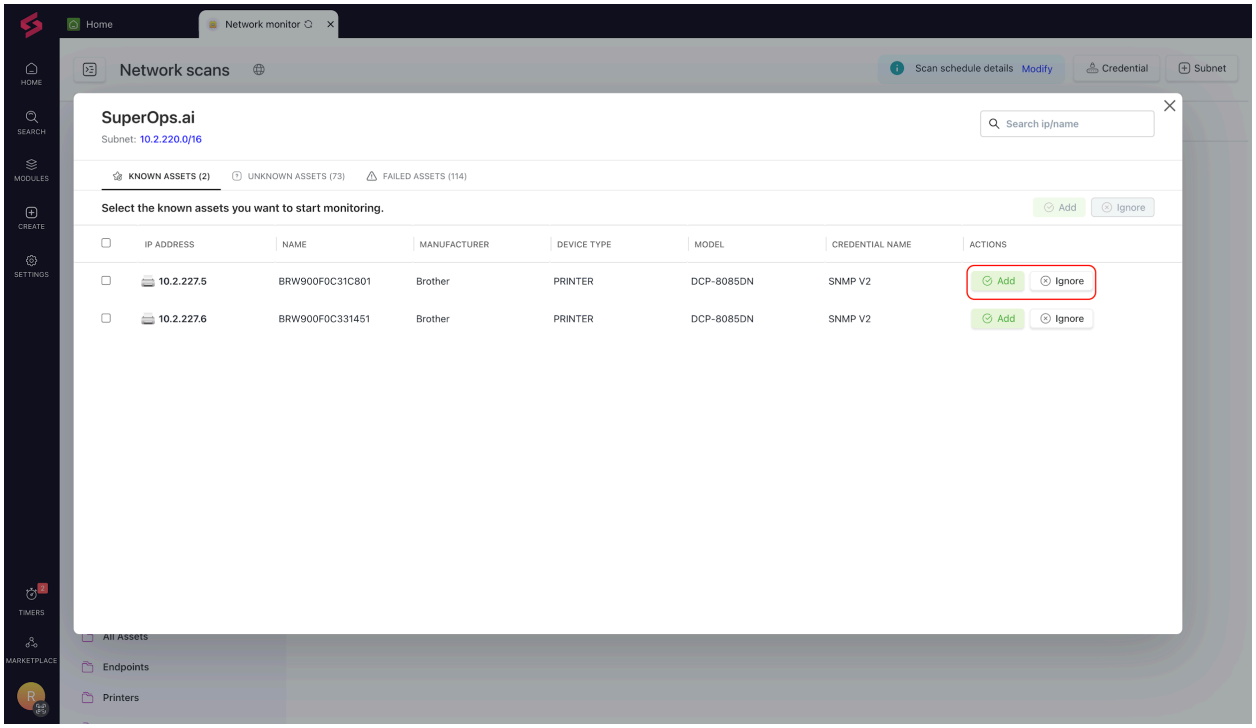
- Other Assets: Any asset whose IP is known but asset class is not known falls under this tab. This means that SuperOps is unable to decipher if the asset is an endpoint or a network device, but since the IP has been discovered, the asset has come into the scan result.

The assets are segregated by status as follows:

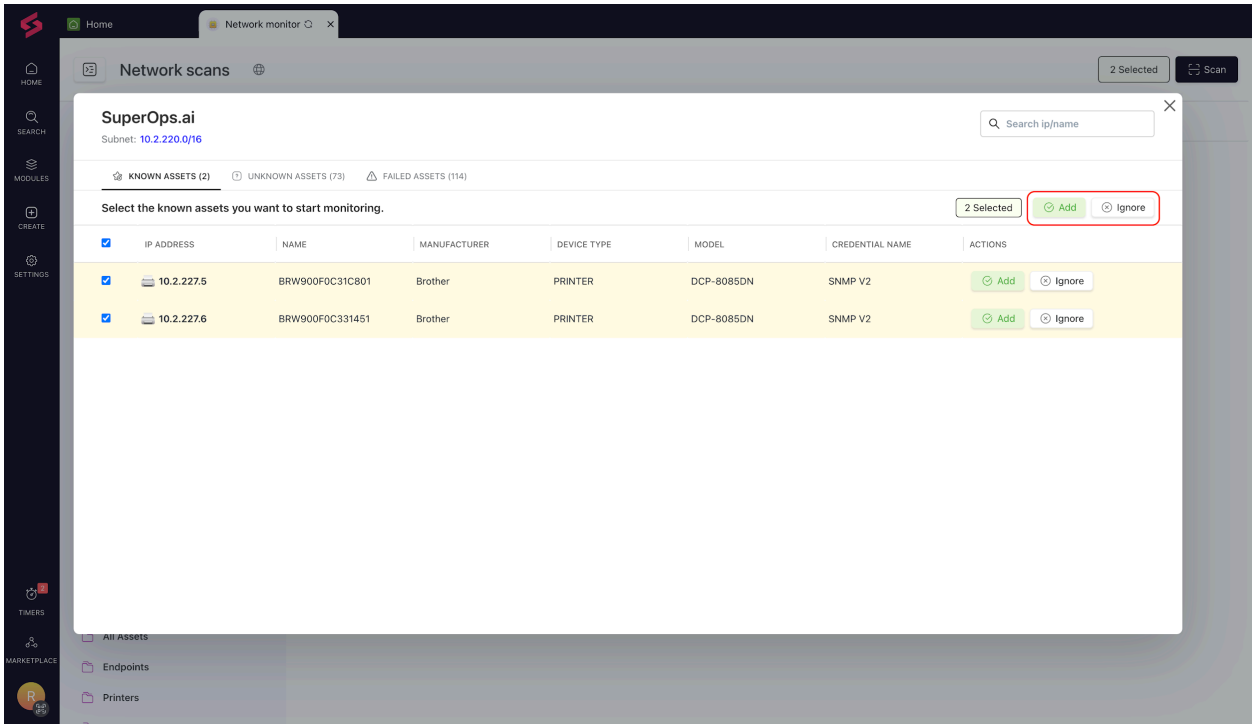
- Known assets: All assets that are recognized by SuperOps.ai and already a part of our SysObject library will be listed as known assets.
- Unknown assets: Network devices that respond to your probe but are not part of SuperOps' SysObject library will be listed under unknown assets.
- Ignored assets: Network devices you mark as Ignore after scanning fall into this category. These devices will not be monitored by the SuperOps probe.
- Added to monitoring: Network devices you mark as Add after scanning fall into this category. These devices will be monitored by the SuperOps probe.
- ICMP only assets: Network devices that have been discovered by the probe via ICMP but not SNMP are marked as ICMP only assets. There are multiple reasons why an asset falls into this category:
    - SNMP is not enabled for the asset
    - The credentials given for this client or site are invalid

Assets discovered via SNMP

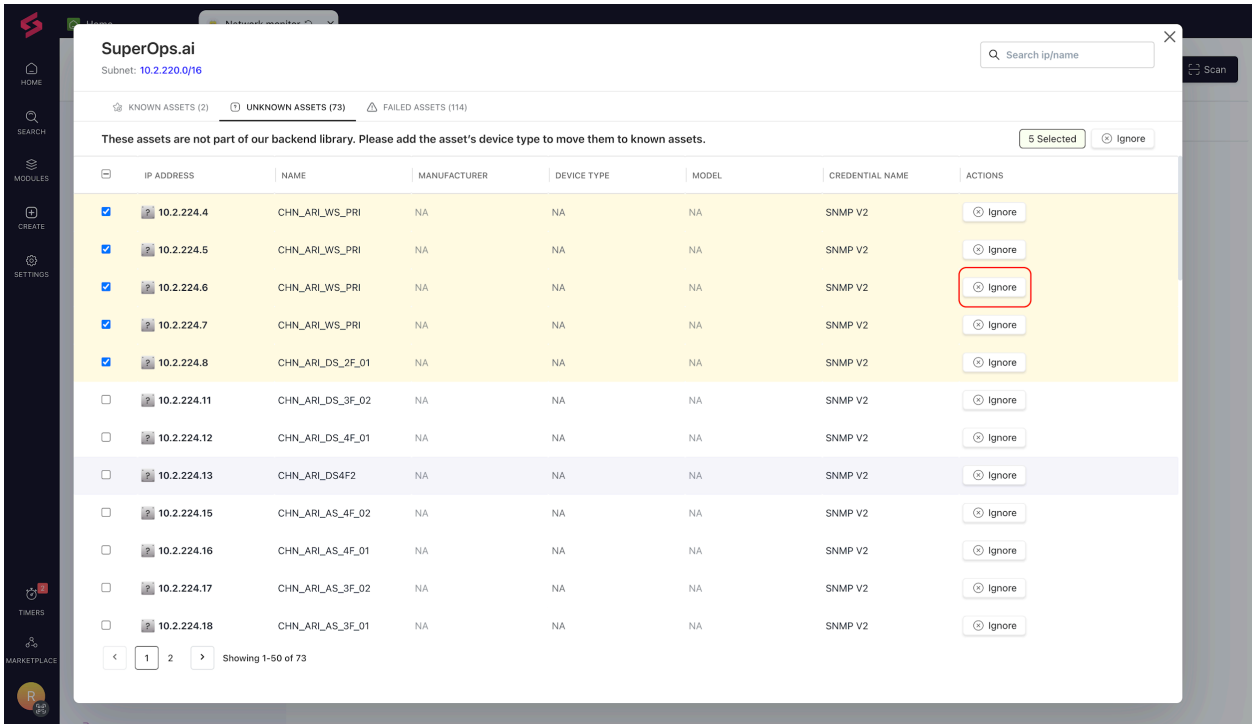
1. Under the Network Assets tab, Assets are segregated by status into Known, Unknown, Added to Monitoring, and Ignored.
2. The Known Assets tab allows you to add or ignore assets. The assets that are added will be monitored, while the assets that are ignored won't be. You can do this by clicking on the Add or Ignore buttons as shown below.



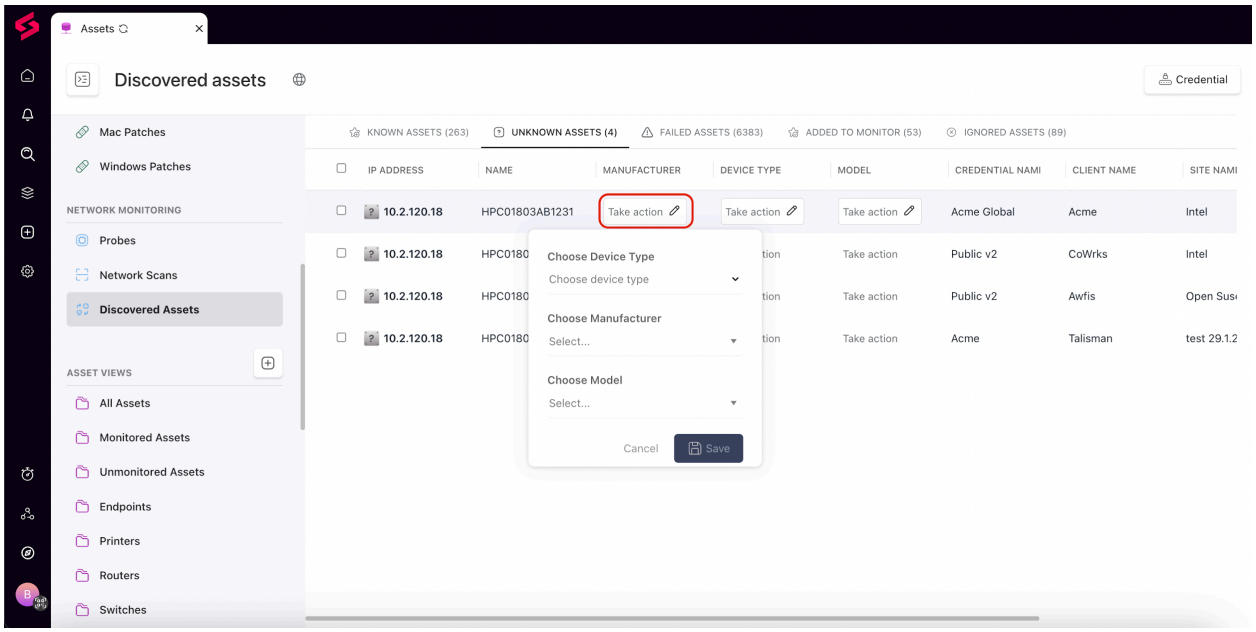
3. You can also bulk-select the assets you want to Add / Ignore.



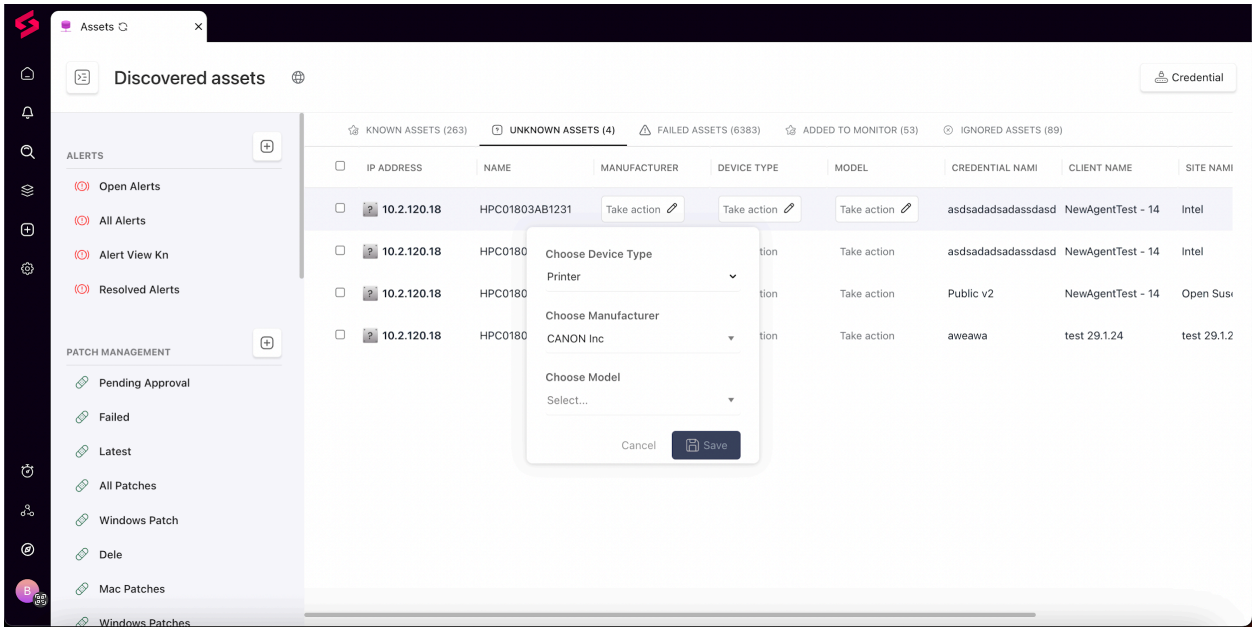
4. In the Unknown Assets tab, you'll be able to see the list of all unknown assets discovered. You can click the Ignore button to mark them as assets the probe will not monitor.



5. You can convert an unknown asset to a known asset manually, by adding the Manufacturer, Device Type, and Model details using the Take action button.



6. If your asset model is not available in the dropdown, you can create a new model as well.



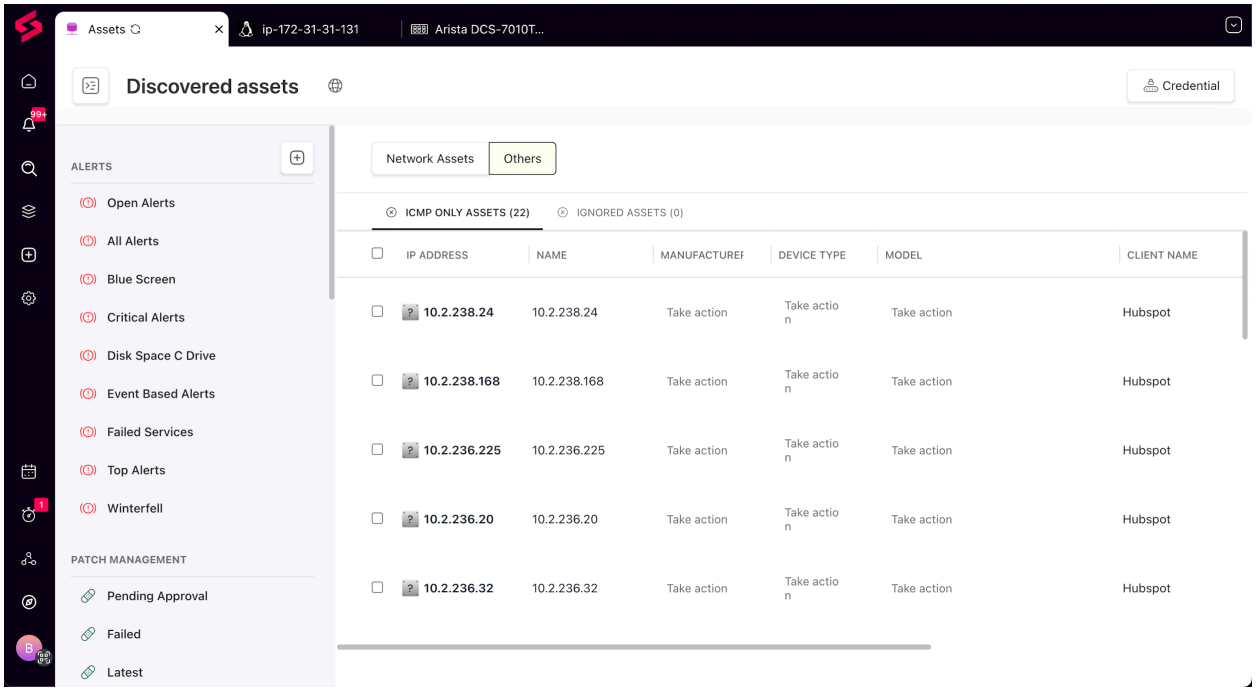
Assets discovered via ICMP

The following assets fall under the Others tab:

- Assets that the probe is unable to reach via SNMP but has successfully reached via ICMP. A network device that does not have SNMP enabled will also fall here.
- Assets for which SuperOps is unable to decipher the asset class.

If there are assets you want to monitor only using ICMP, you can do so from this tab. Here's how:

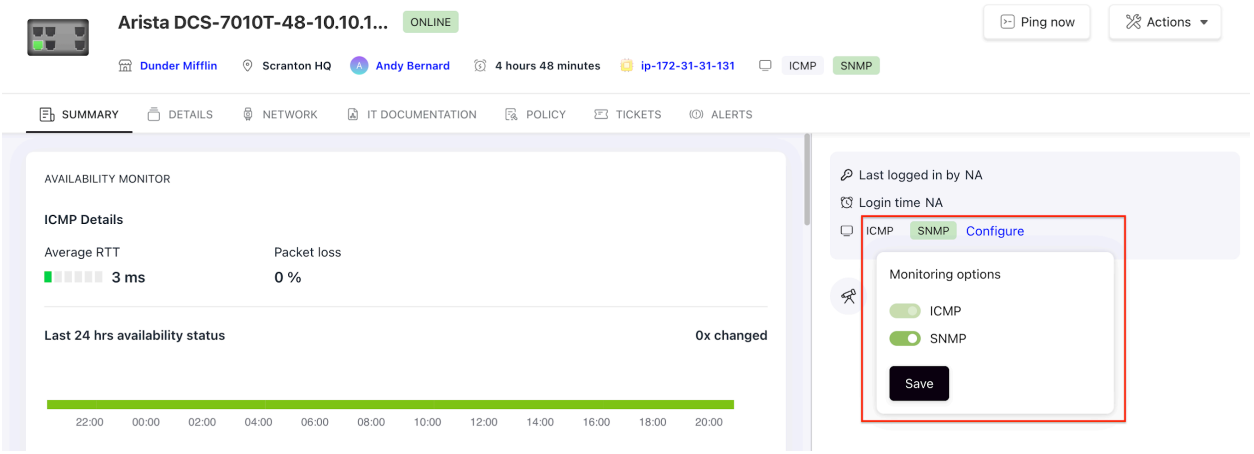
1. If you are able to identify the asset based on the IP address fetched by the probe, you can manually enter the manufacturer, device type, and model details. Once done, click on Add to enable ICMP monitoring for this asset.



2. If there are assets in the list you don't want to monitor, you can move them to the Ignored tab by hitting the Ignore button.

How to turn off SNMP

ICMP monitoring will be enabled for all network assets by default, however, you have the option to disable other monitoring options as you please at an asset level.
To disable SNMP for an asset, go to the asset page and click on the Configure button. Switch off SNMP here to remove SNMP monitoring for this asset.



Monitoring Network Devices in SuperOps

Similar to how you manage and monitor your endpoints, you can also manage network devices in SuperOps with the network monitoring module. In this article, we will look at the network device types that are supported along with the SNMP and ICMP details fetched by SuperOps for these devices.

Fully Supported Network Devices

The list of network device types that can be monitored are:

- Printer

- Router
- Switch
- Firewall
- UPS
- NAS
- Wireless Access Point
- Wireless LAN Controller
- Server Hardware Controller

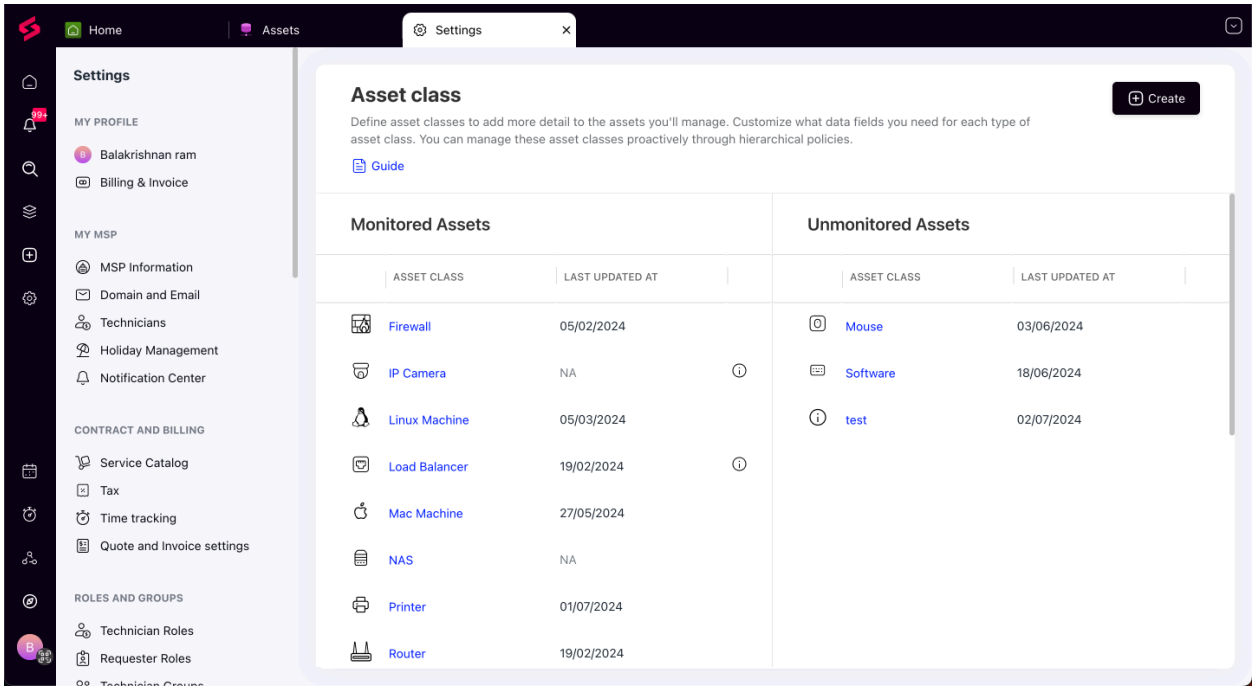
These device types come with an exhaustive list of default monitors. If there are other metrics you would like to monitor, you can do so by creating custom monitors.

Other Network Devices

On top of SuperOps' list of fully supported network devices, you can bring in more network devices and start monitoring them with custom monitors. SuperOps will fetch interface details for these device types by default. If you would like to monitor specific metrics, you can do so with custom OID monitoring. See how you can add custom monitors here.
List of additional network device types:

- Load Balancer
- WAN Accelerator
- VoIP
- IP Camera
- WAN Router
- Network Video Recorder

- Ethernet/IP Bridge
- Temperature Sensor
- Domain Controller
- Vmware ESXI
- Environmental Monitoring Device
- Serial Device Server
- Presentation Gateway
- VoIP Gateway
- USB Hub
- X Terminal
- Ethernet Gateway
- PBX
- Ethernet Card
- Audio Codec
- RF Transmitter
- Tape Library
- KVM Switch
- Zero Client
- Barcode Printer
- Power Distribution Unit

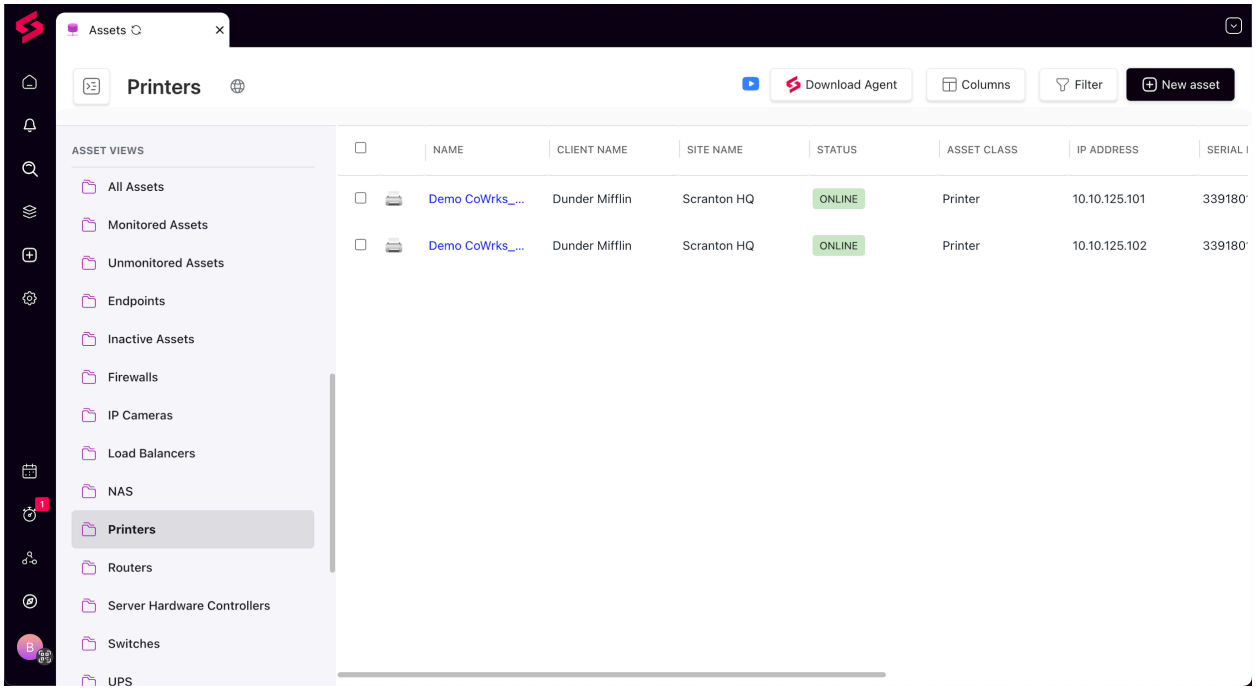


We will soon be adding more monitors for all the device types listed above, and minimize the need for you to create custom monitors.

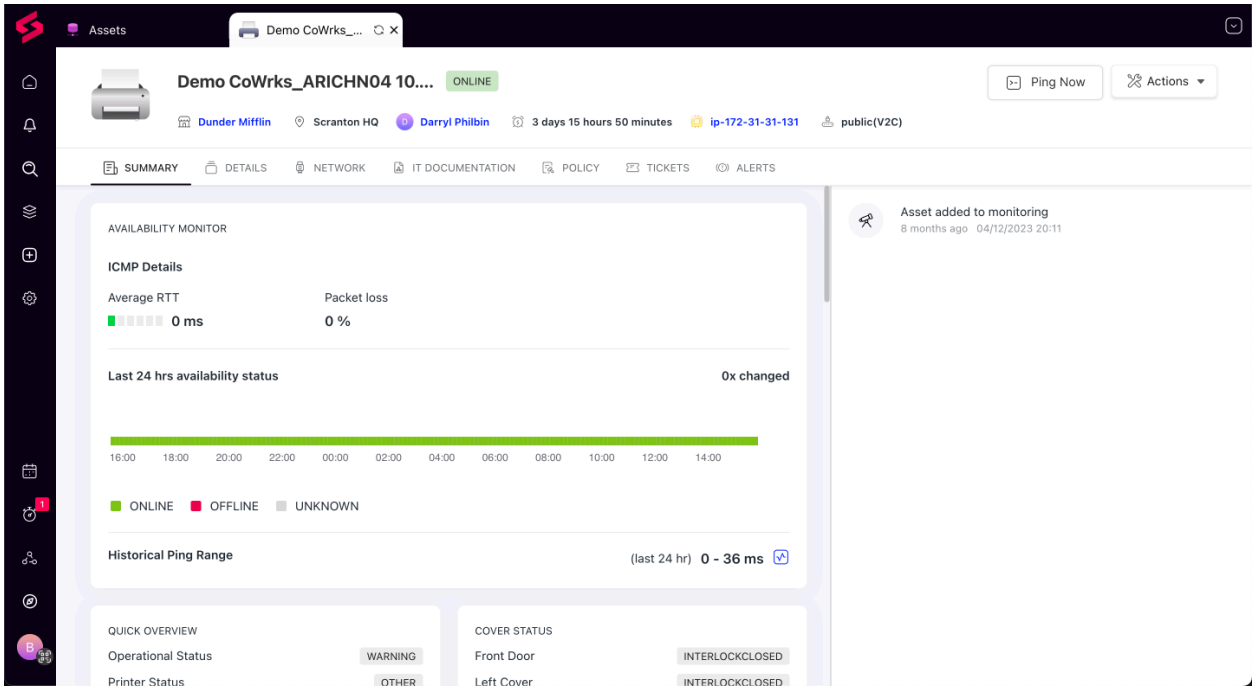
How to Monitor a Network Device

SuperOps uses SNMP and ICMP to fetch metrics and details from a network device. ICMP is enabled for all network devices by default, and you have the flexibility to turn on/off SNMP based on your monitoring needs.

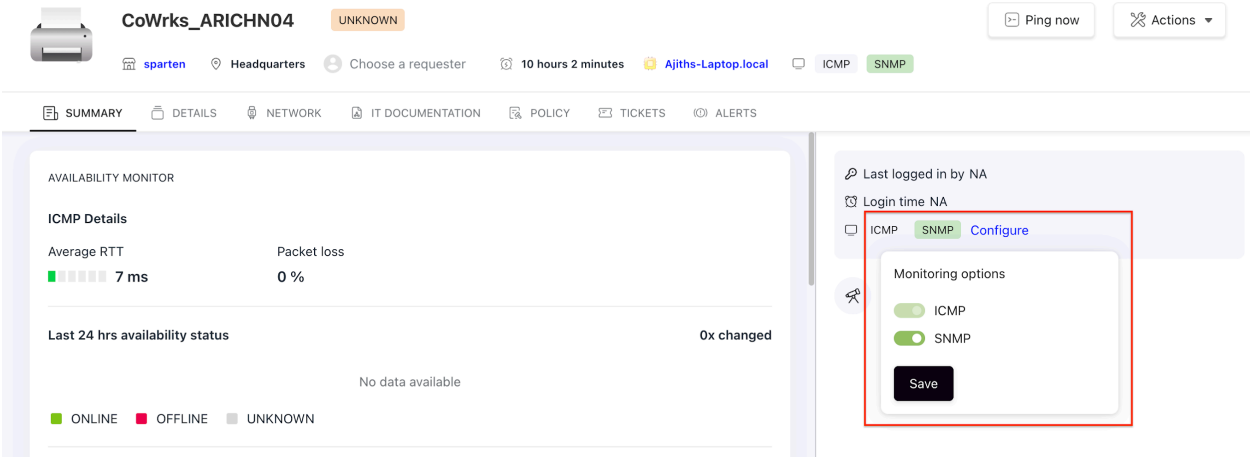
1. Navigate to Modules > Assets
2. Under Asset Views, you will see a separate view for each network device. Let's click on Printers and see what details are available.
3. In the Printers view, you will see a list of all discovered printers.



4. Select the printer you'd like to monitor. On the Summary page, you'll see metrics and status updates such as ICMP Details, Toner details, Cover status, and more that deliver insights on the printer's condition and health.



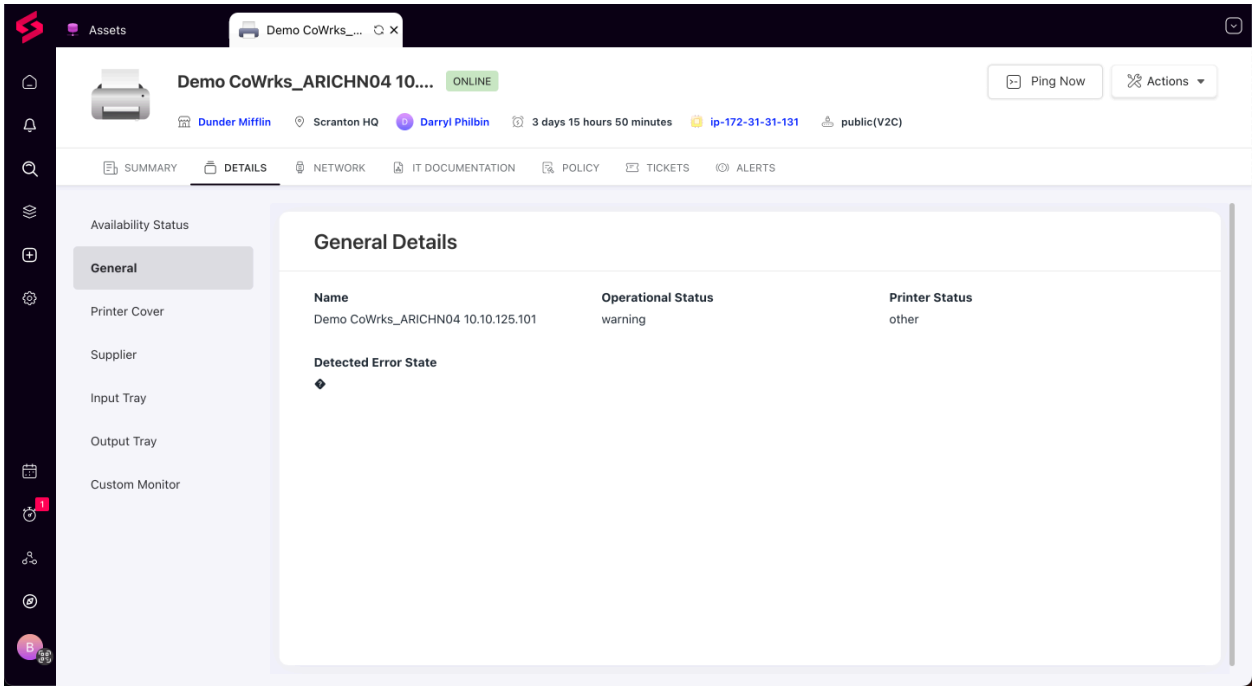
All network devices will have the ICMP protocol enabled by default. If you have devices that you would like to monitor only using ICMP, you can choose to disable SNMP using the Configure option.



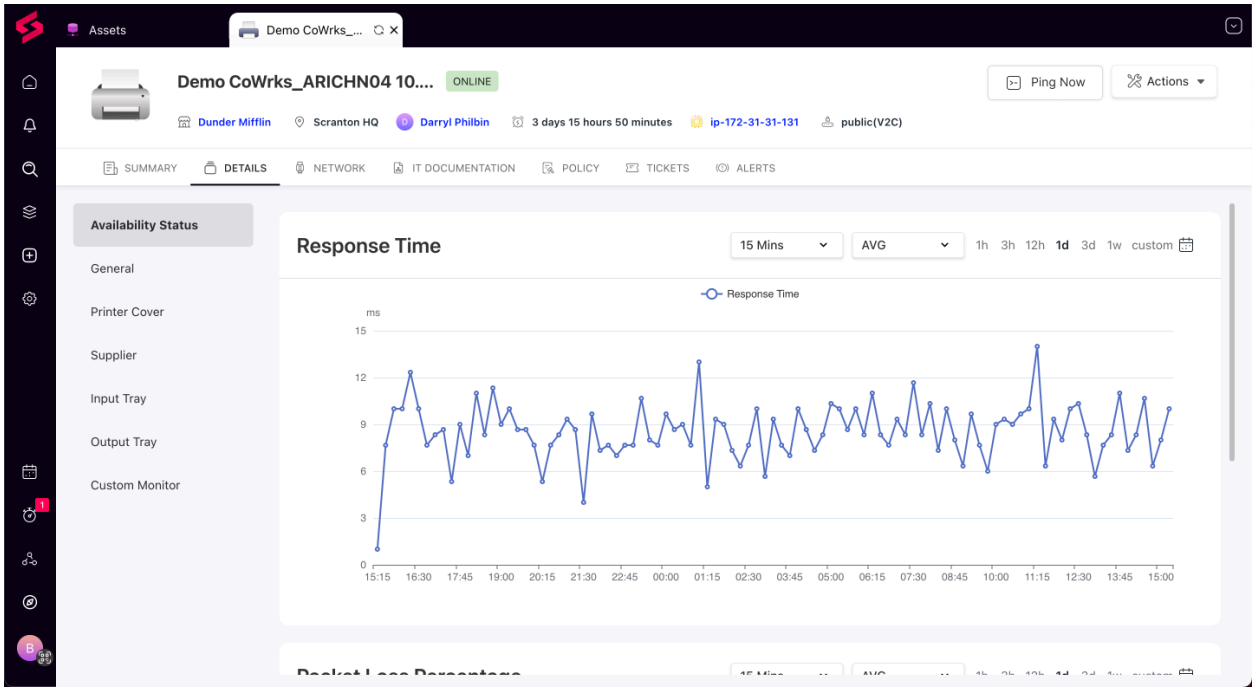
5. On the details page, you'll be able to see Availability Status and data fetched by default monitors provided for printers. These default monitors for printers include:

1. General
2. Printer cover
3. Supplier
4. Input Tray
5. Output Tray

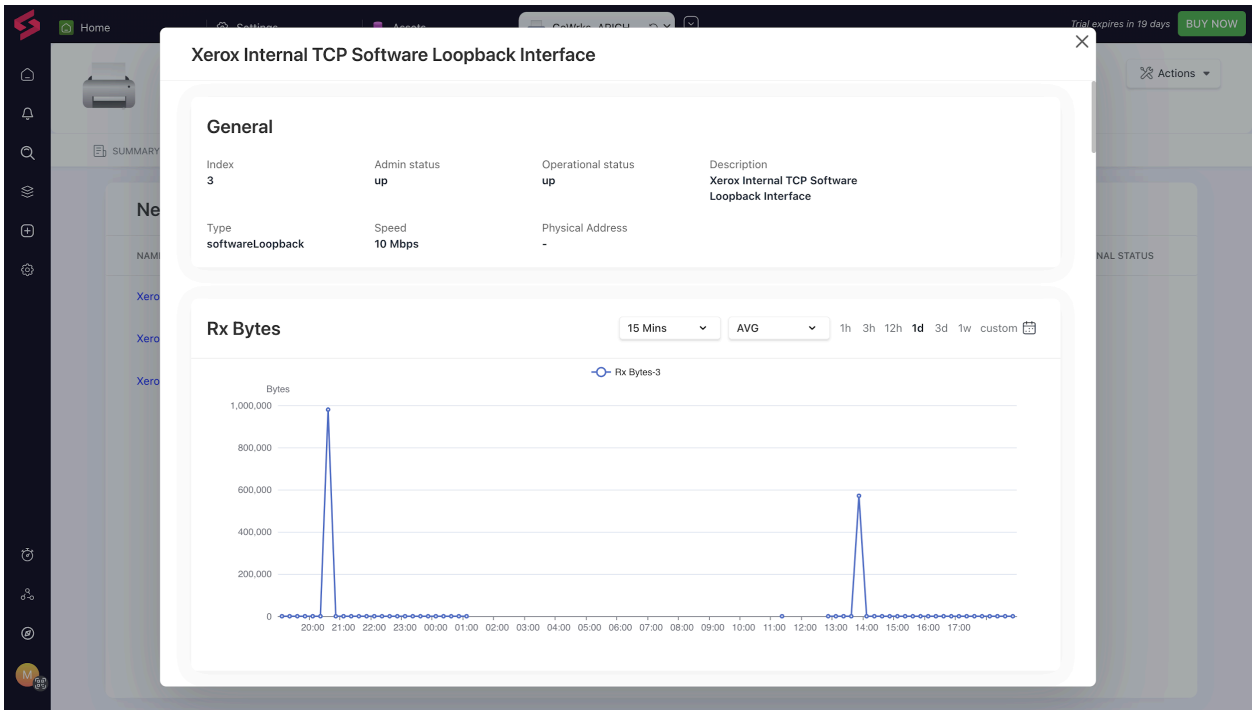
You can also set up custom monitors to track and monitor additional metrics. Learn more about custom monitors here.



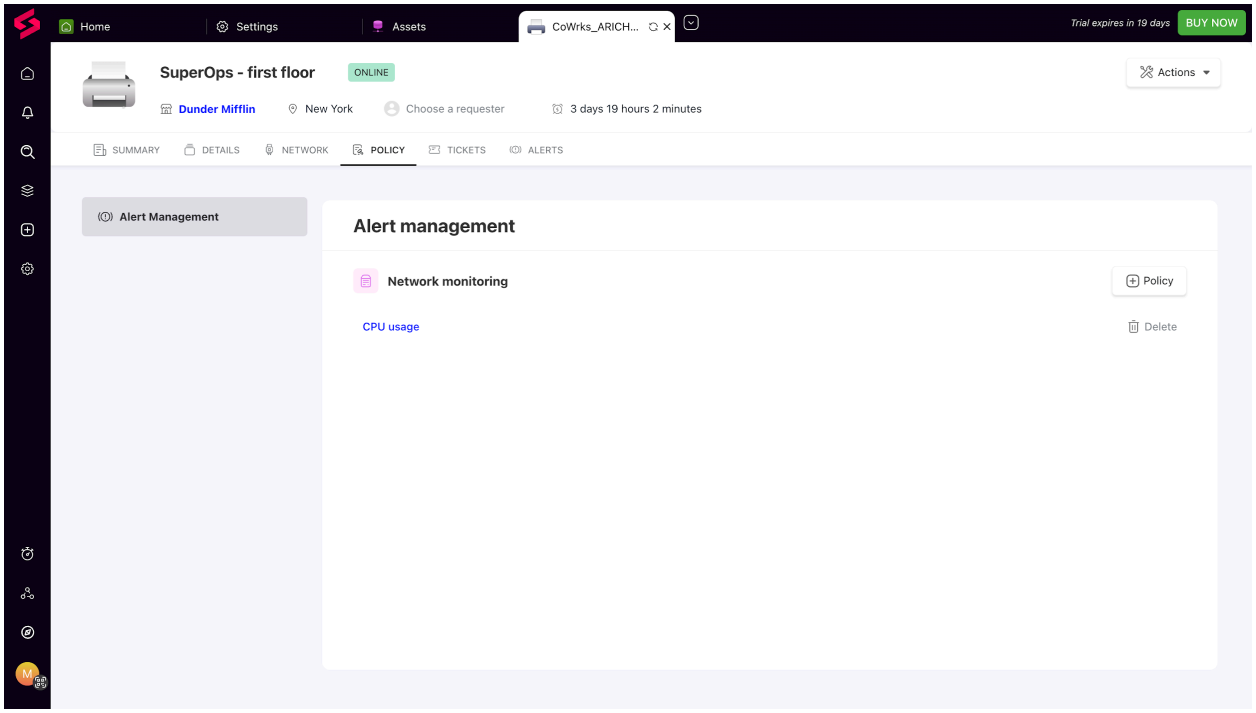
For each category, the enabled monitors in your settings will be visible on this page. Additionally, Availability Status details can be seen for all network devices in the form of plotted graphs, showing Response Time and Packet Loss data.



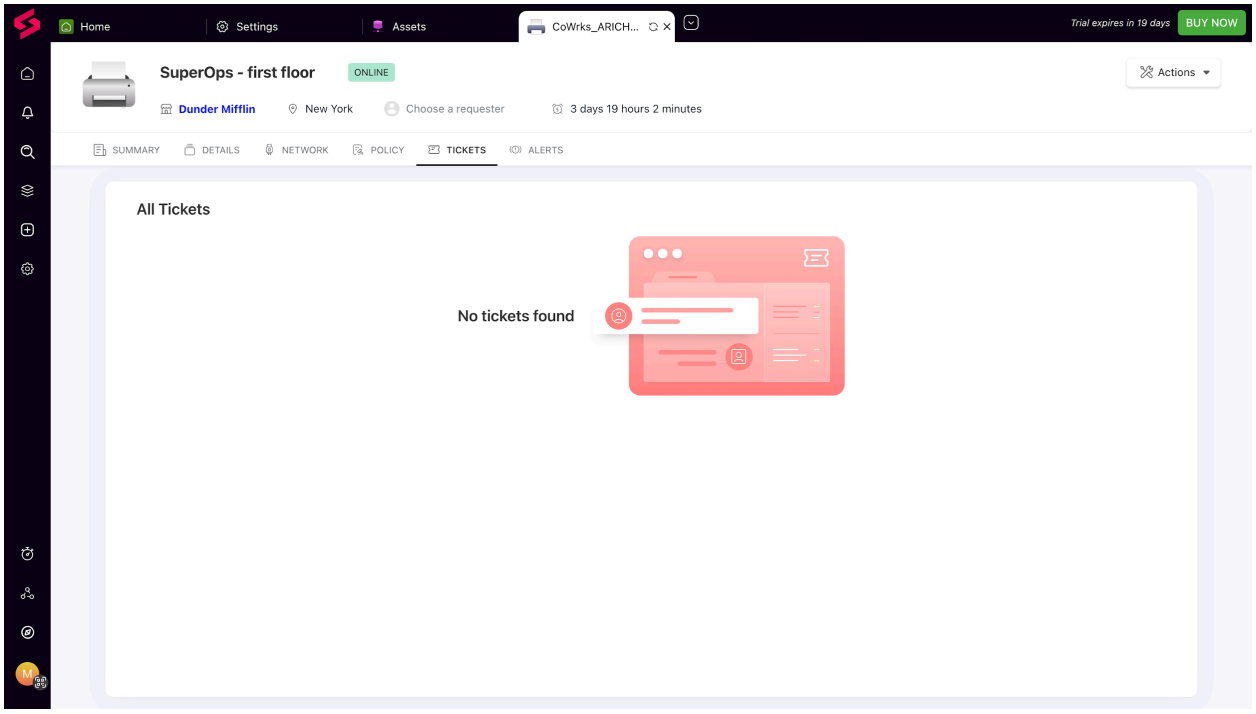
6. Under the Network tab, you'll find an overview of the different types of network interfaces available for that printer. For example, Ethernet, Wi-Fi, Bluetooth, etc.



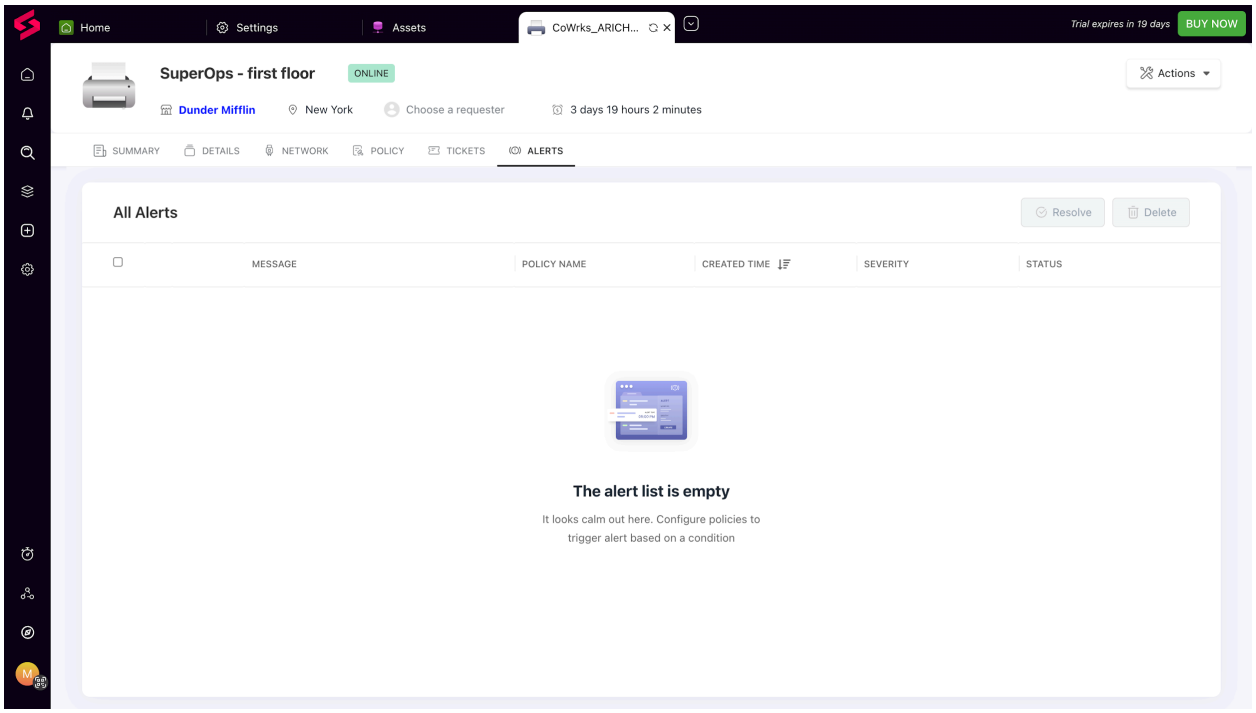
7. Under the Policy tab, you'll find all the printer policies available. You can also create new policies by clicking on the +Policy button.



8. You'll find the list of tickets associated with this printer in the Tickets tab.



9. Under the Alerts tab, you'll find all the alerts generated for this printer. You can resolve individual alerts or bulk resolve or delete multiple alerts too.



Setting up default and custom monitors

In this article, we delve into:

- Understanding custom and default monitors
- Interpreting time-series graphs, and
- Efficiently using derived monitors

Understanding custom and default monitors

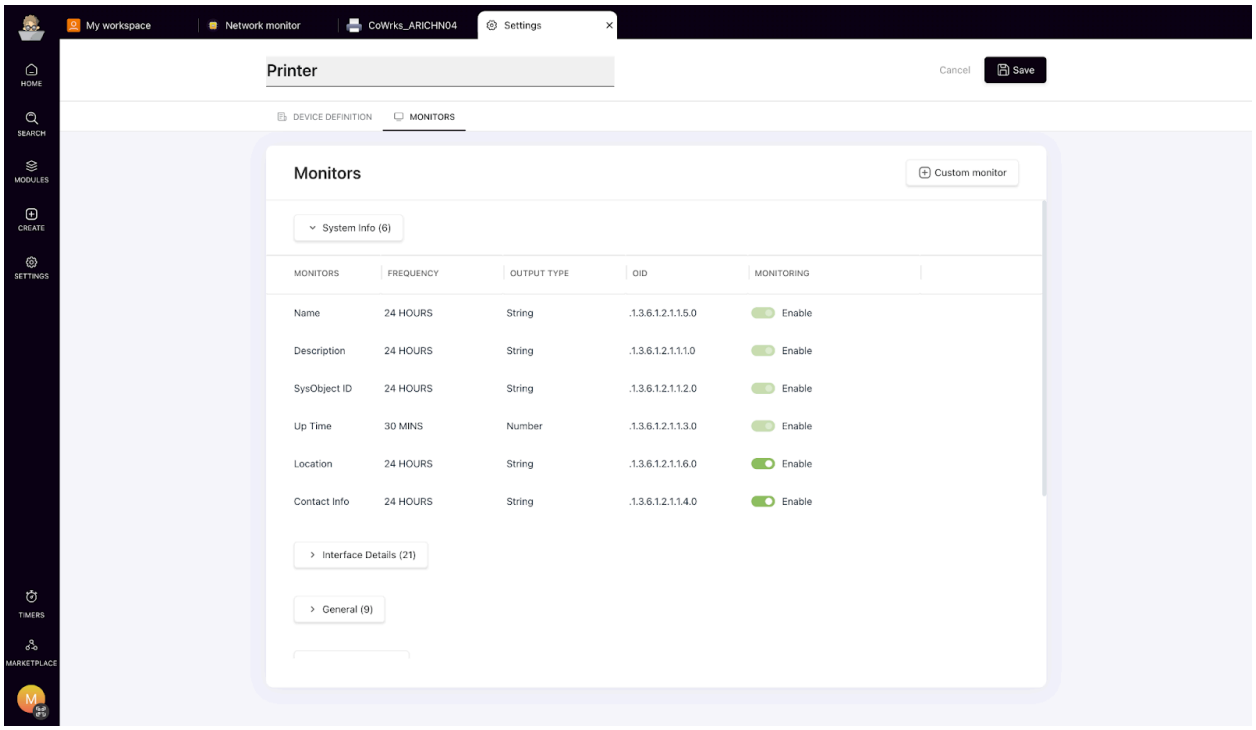
But first, what is a monitor?
Monitors help you track individual metrics of a network device. A combination of these monitors helps you accurately gauge the performance and health of a network device.
There are two types of monitors available in SuperOps.ai:
Default monitors: These are in-built monitors provided by SuperOps, that are designed to collect common metrics like System information, Interface details, etc., about the network device.
Custom monitors: These are monitoring configurations that you create or tailor to specific requirements of your network environment. These monitors allow you to track specific metrics like the performance and health of your device.

Setting up Default monitors for printers

To set up default monitors,

1. Navigate to Settings > Asset class > Printers > Monitors

2. Under the Monitors tab, you'll be able to see the list of all default monitors. You can enable or disable the monitors of your choice.



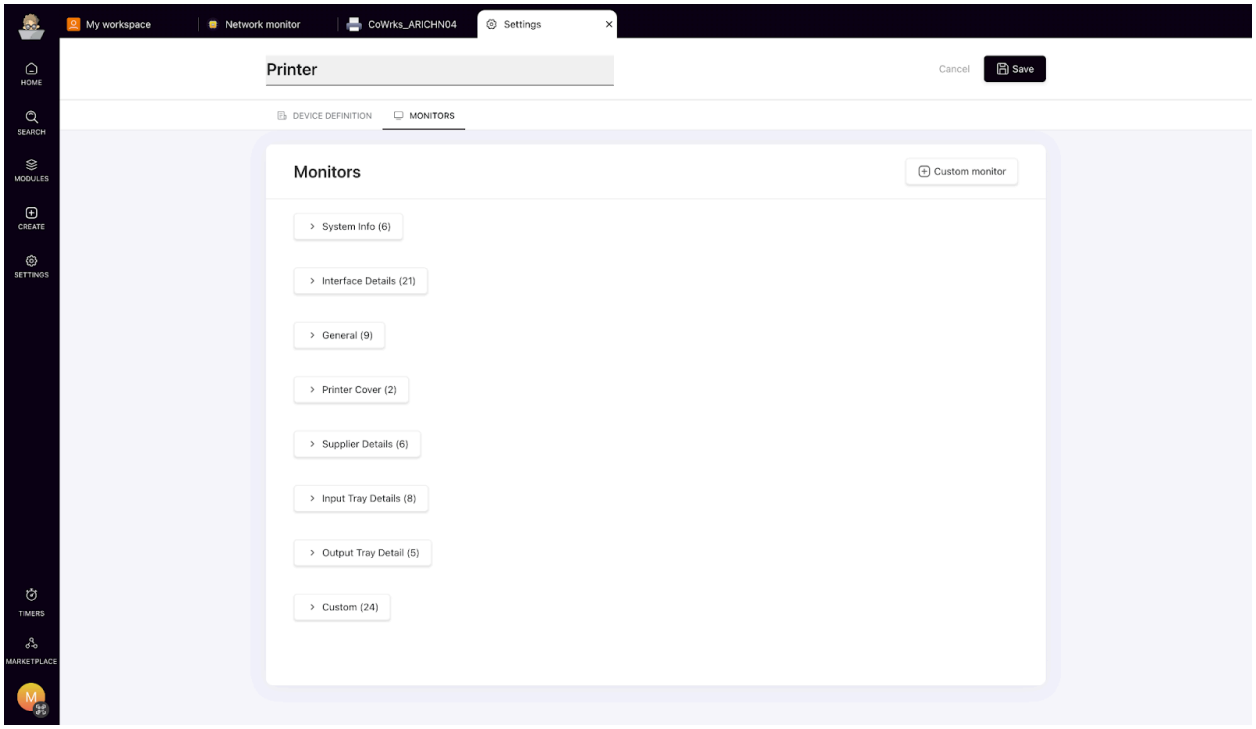
3. The following is the list of Default monitors provided by SuperOps.ai

- System Info
- Interface Details
- General
- Printer cover
- Supplier Details
- Input tray details
- Output tray details

Setting up Custom monitors for Printers

To set up a custom monitor,

1. Navigate to Settings > Asset class > Printers > Monitors
2. Under the Monitors tab, you'll find the +Custom Monitor button on the top right corner.
3. Click on that to add a new custom monitor.

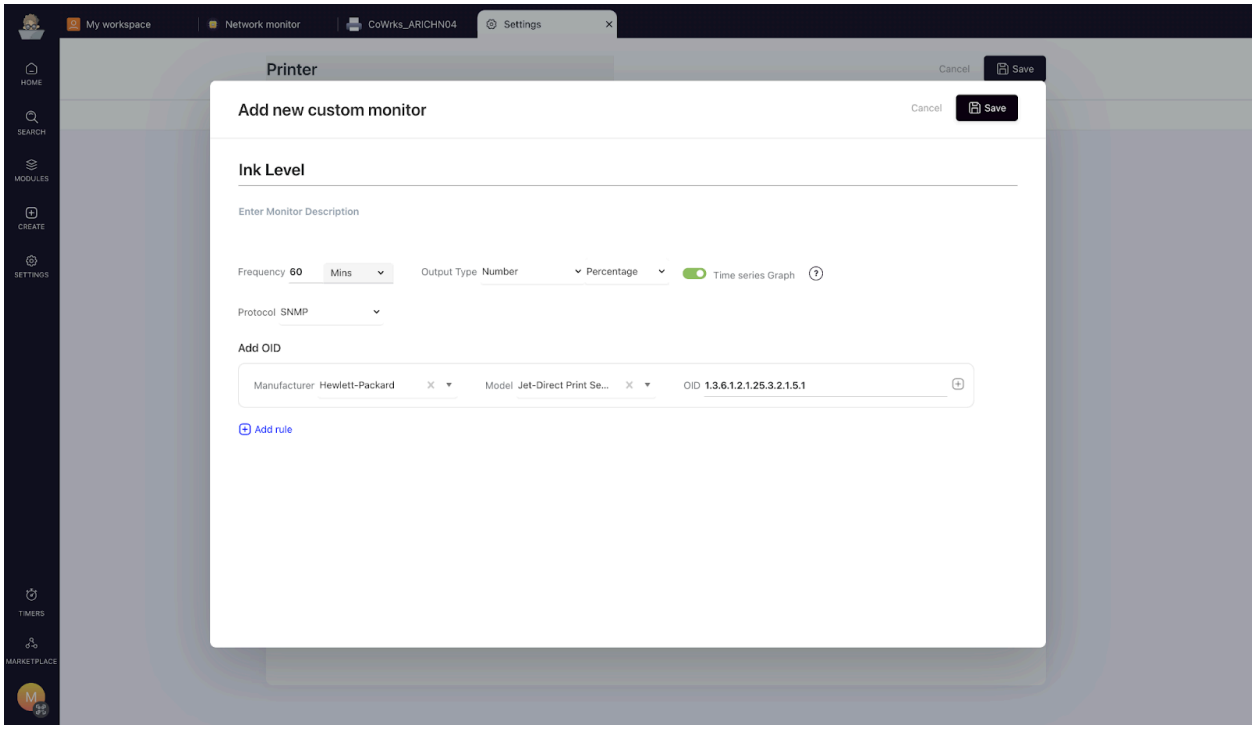


1. Give a name and description of the monitor.
2. Enter the frequency at which the data should be fetched. This interval can be defined in either minutes or hours.
3. Select the desired output type, which can be a String, Number, or Enum. Please note that enabling time-series graphs is not possible for string outputs.

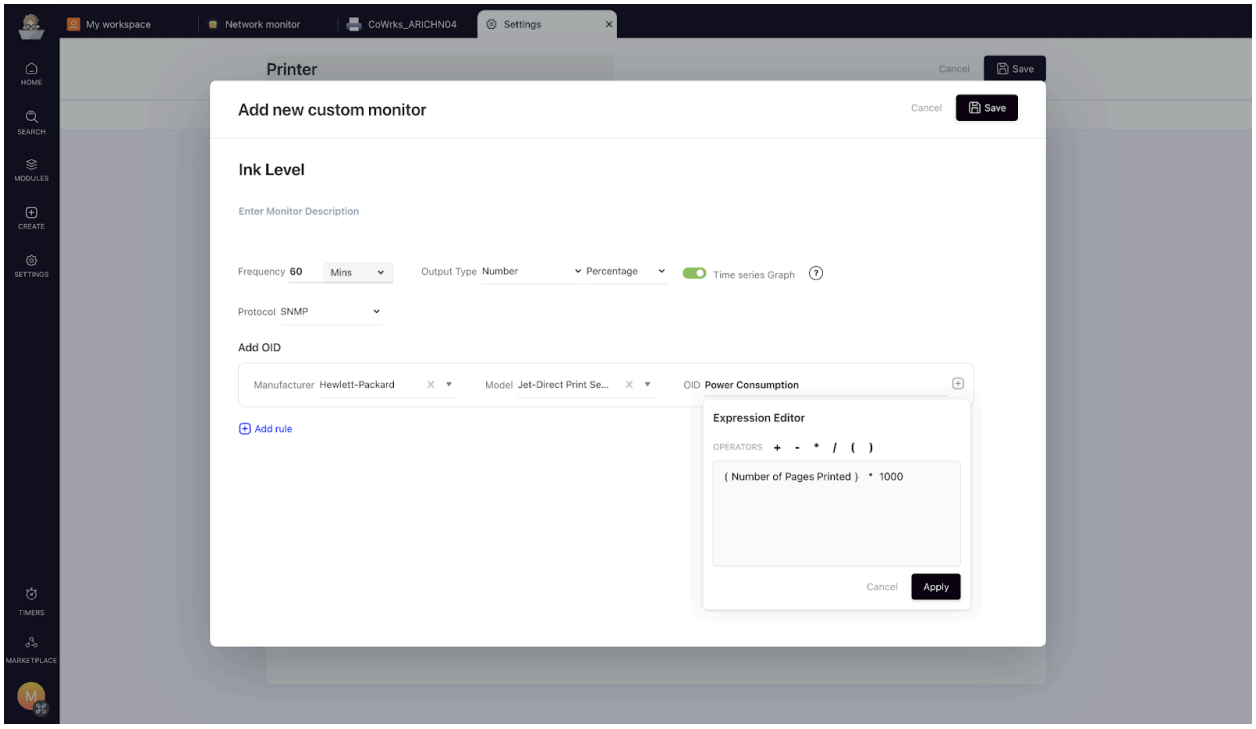
📉 Time-series graph: Enabling the time-series graph allows you to see the output data in a graph format.

---

4. For now, SuperOps supports only the SNMP protocol. So you can only choose SNMP from the drop-down list.
5. Once these settings are in place, start adding the OIDs to the monitor. You can add multiple OIDs to a Custom monitor.



6. If you click on the + icon near the OID, you'll be able to add Derived Monitors. Derived Monitors are a combination of multiple monitors. For example, you can create a Derived Monitor by calculating the product of the Number of pages printed and a factor, such as 1000. Here, the number of pages must be monitored as well.

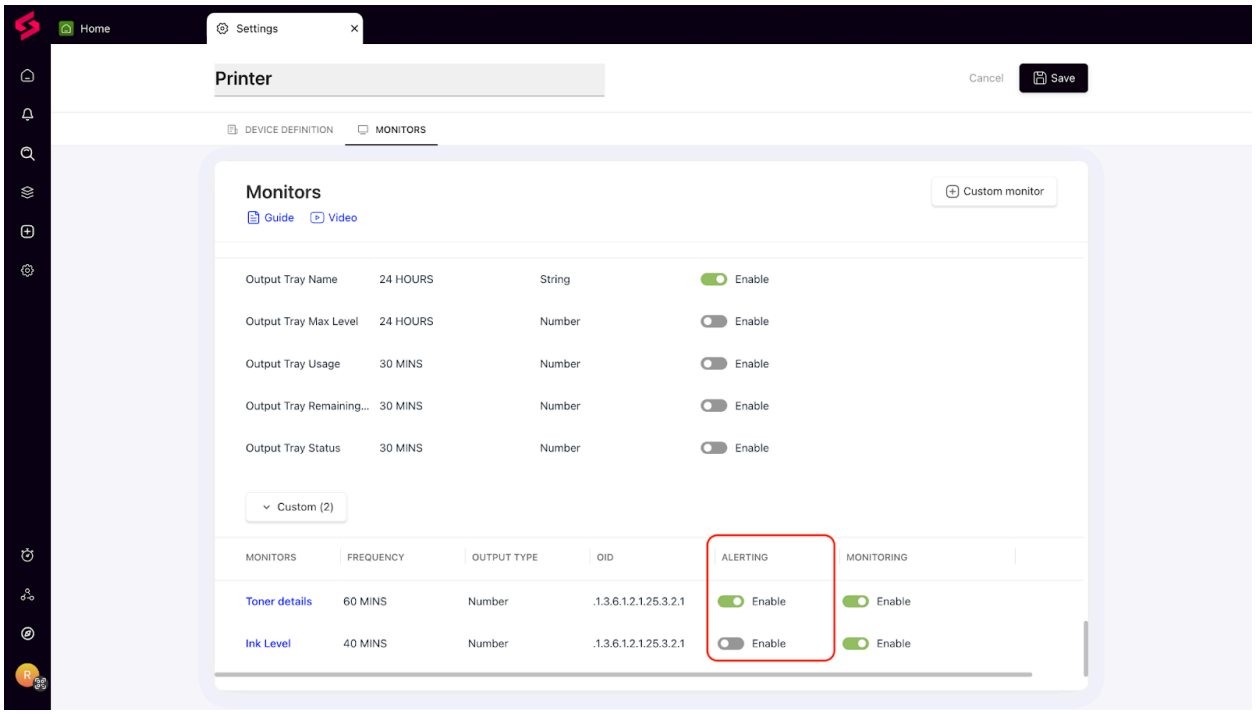


7. Once you are done adding all the details, hit Save to successfully create a new custom monitor.

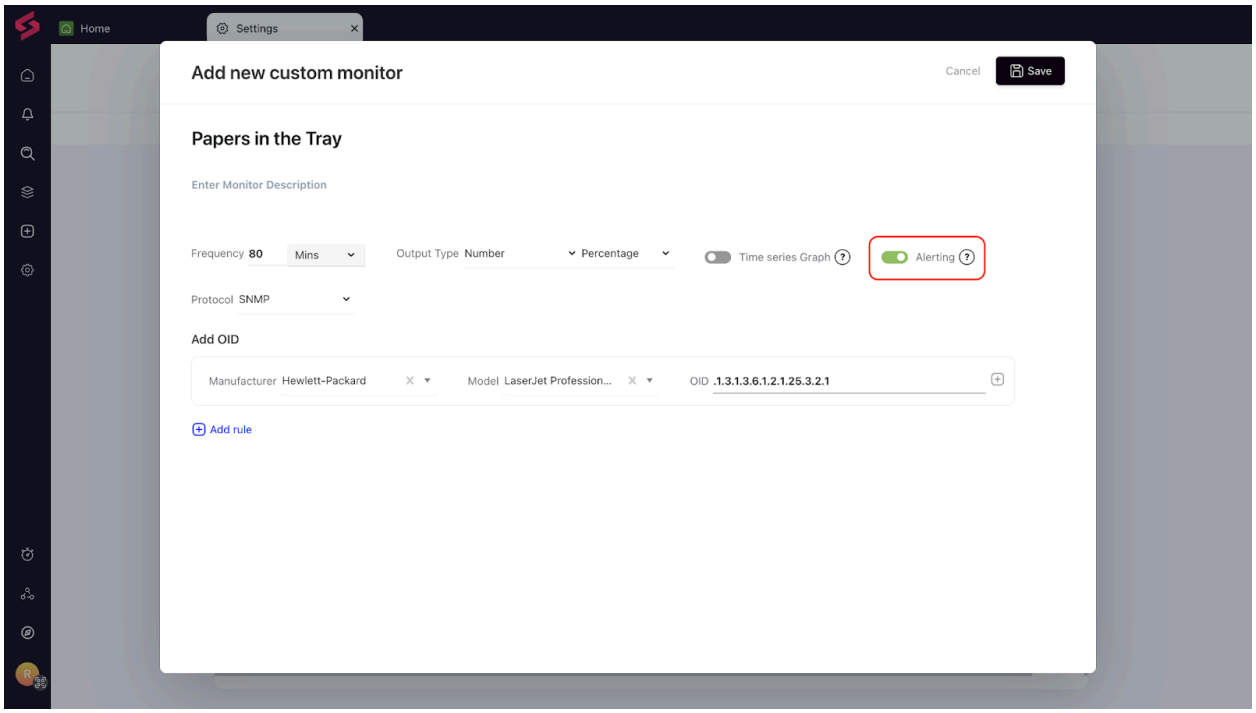
8. You can see the list of all custom monitors under the Monitors tab.

Configuring Custom Monitors for Alerting in Policies:

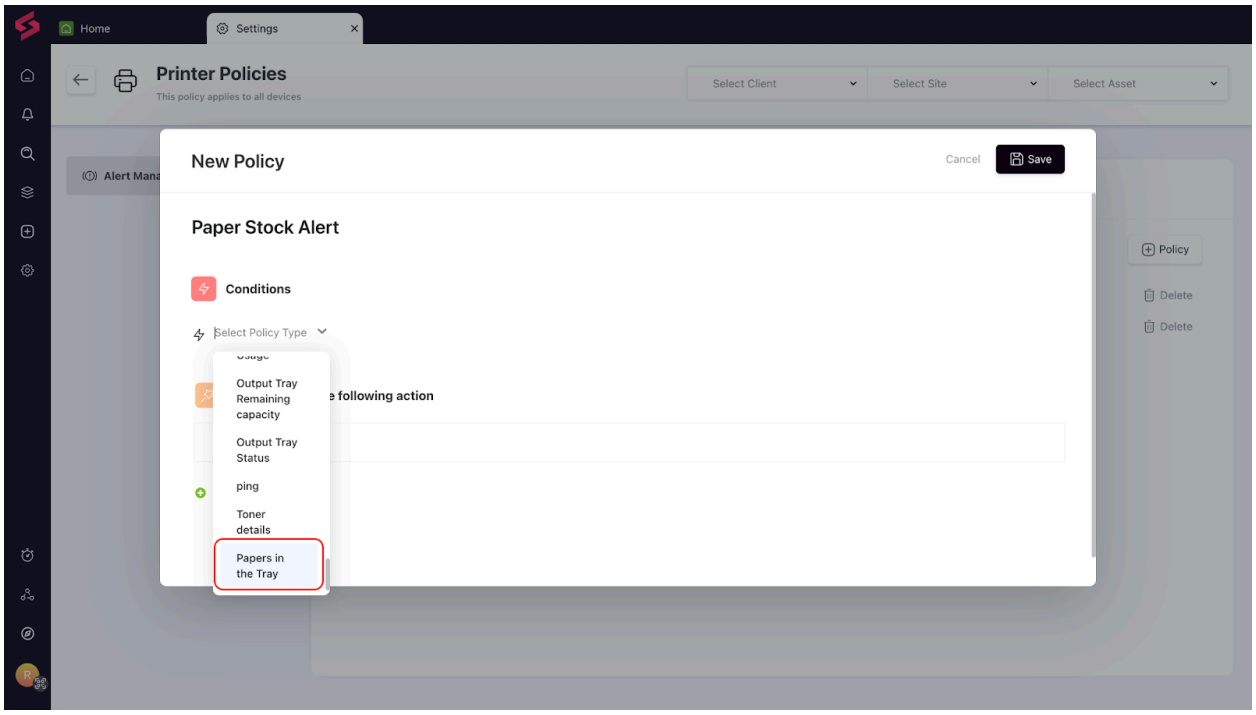
1. You can also set up custom monitors as alert conditions in policies by enabling the alerting toggle for the desired monitors.



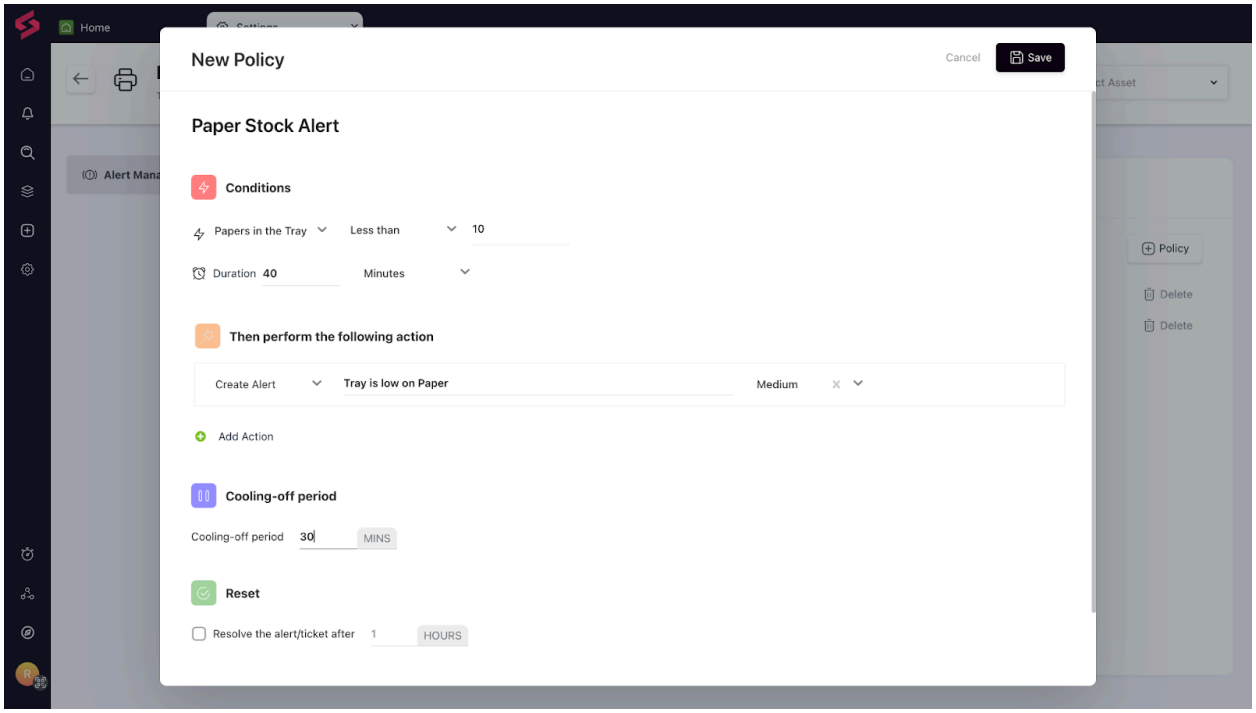
2. You can also do this while creating a new custom monitor. Once you activate the toggle, the alert policy can be configured based on the monitor's parameters.



3. To initiate alert generation, you must first configure Policies. Within the Policy page, the alerting-enabled custom monitors will serve as filter conditions.



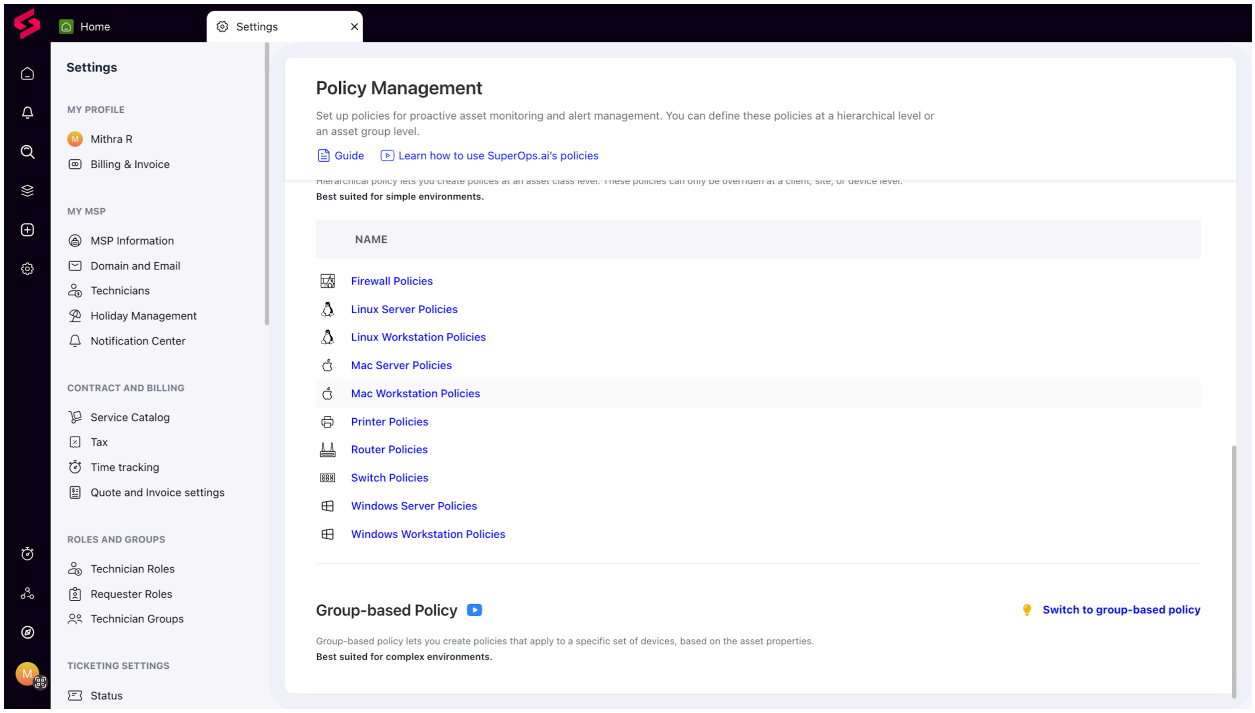
4. Select the monitor you wish to base alerts on and provide alert details. Upon saving, the alert policy will be established based on the chosen monitor.



Setting up network policies in SuperOps

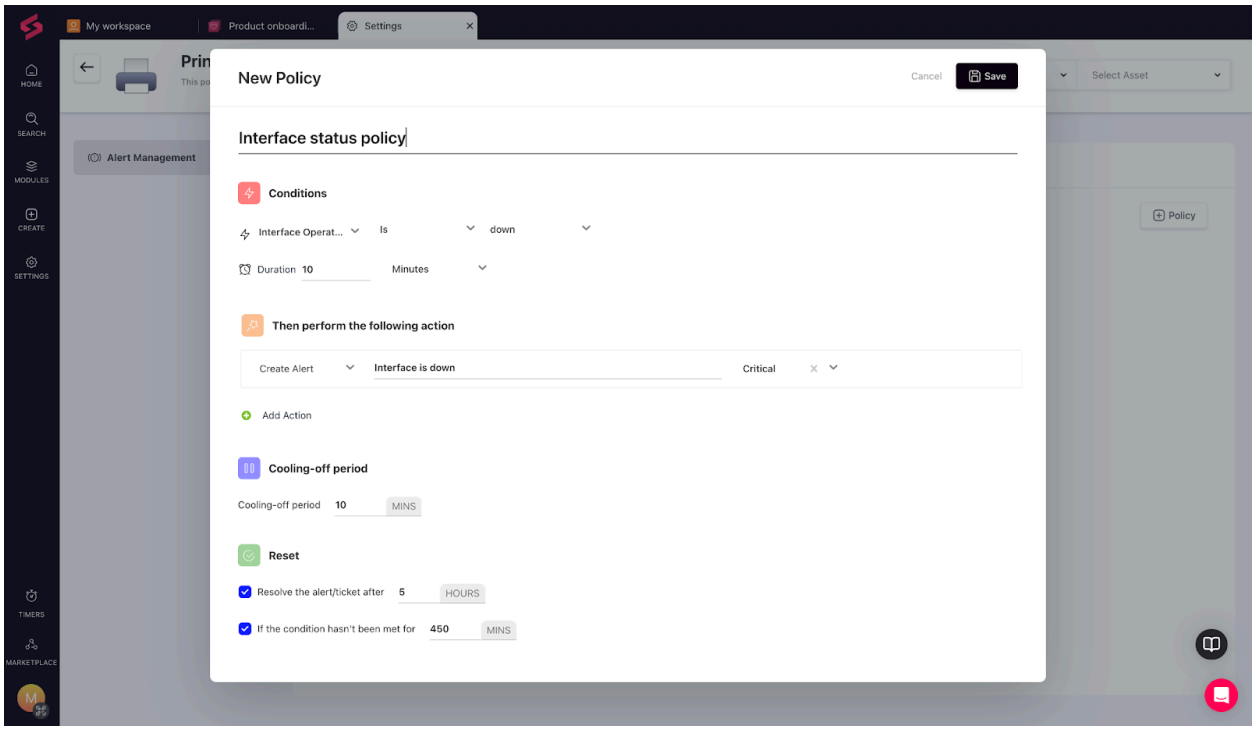
Network policies keep you in the loop about the health of your network devices by alerting you whenever something goes wrong. Here's how you can set them up:

1. Navigate to Settings > Policy Management
2. Choose Printer/Router/Switches/Firewall Policies



3. You can set up global or client/site/asset level printer policies from this page.
(But wait—if this is your first time configuring a policy, then we recommend checking out this explainer on policies and how to get the best out of them.)

4. Click on the +Policy to create a new policy, as shown below.

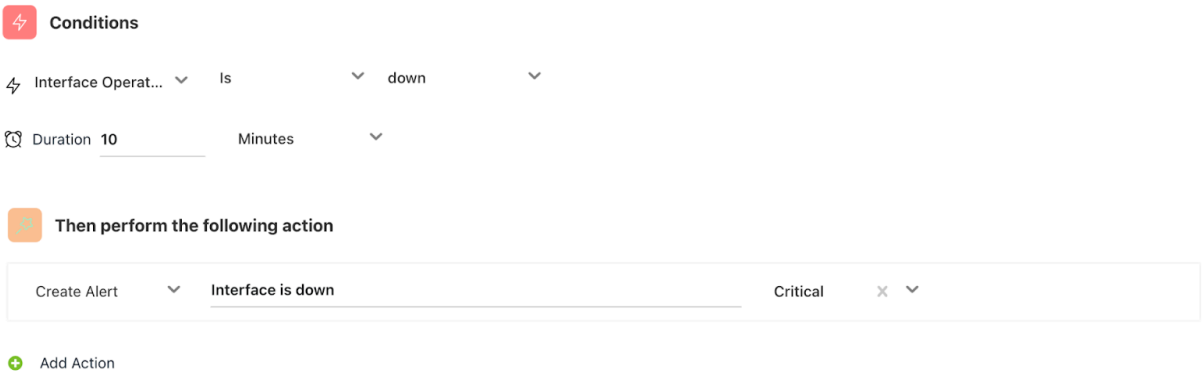


5. Give a name to the policy and set up conditions and actions to be performed when those conditions are met.

6. You can create an alert, send an email, or create a ticket through these actions.

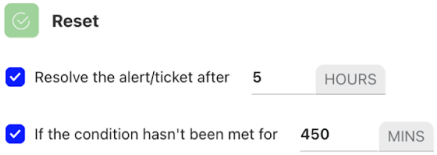
For example, when the interface operator is down for more than 10 minutes, you can create an alert of critical importance, so that you can focus on getting things back online ASAP.

The alert configuration is flexible too—you can set more than one condition to create an alert to help you cover multiple use cases.



7. The cool-off period reduces noise by preventing repeated alerts for the same condition. Once an alert has been created, the next alert for this issue will be created only after the cooling-off period has passed.

8. Moreover, you can also resolve an alert or ticket automatically by checking the checkbox under Reset.

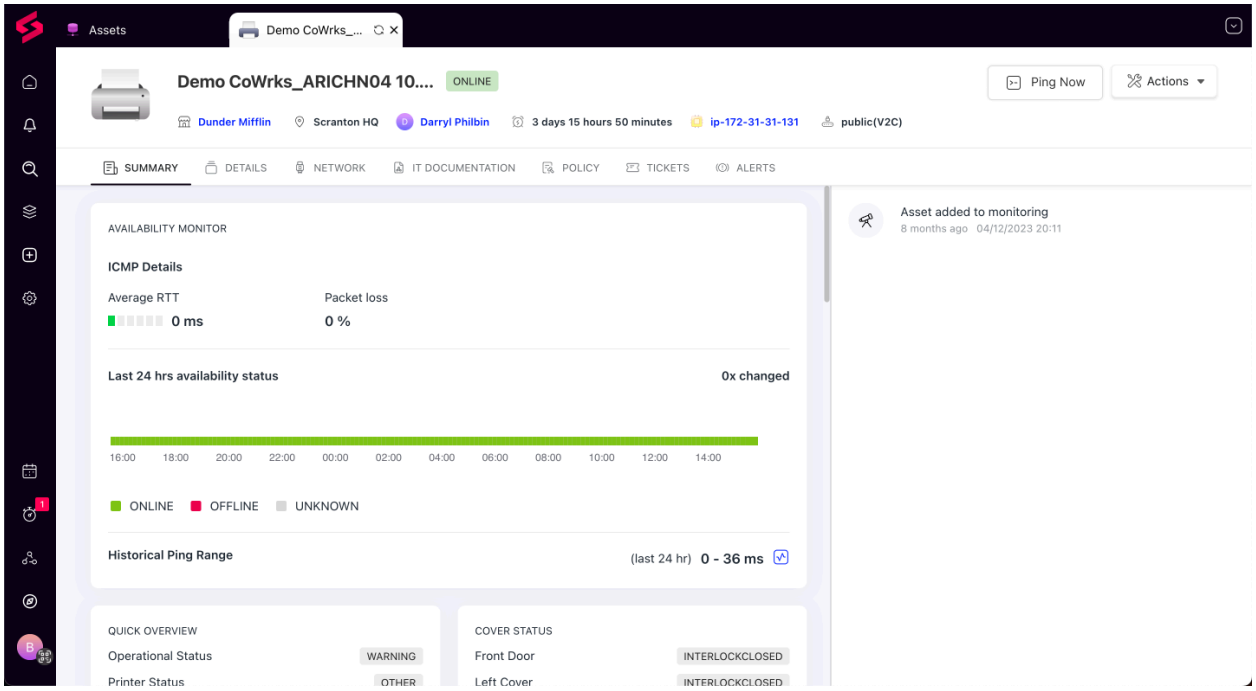


9. Once you are done, hit save to successfully create a new policy for your printers.
Constantly iterating to make your alerts more accurate? No worries, you can come back to these policies and edit them to make them better at any time.

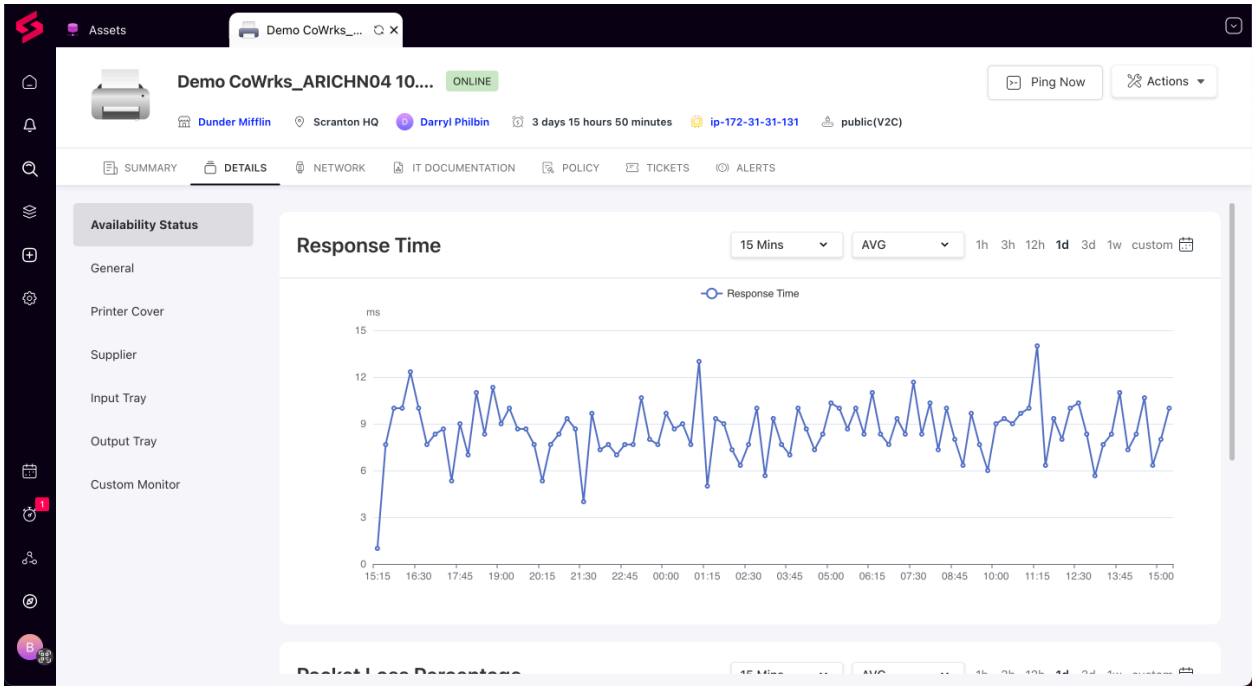
Troubleshooting network issues with ICMP Ping and SSH

ICMP

The Internet Control Message Protocol (ICMP) is used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner. The Ping command in ICMP is a troubleshooting tool used to manually test for connectivity between network devices, and also to test for network delay and packet loss. The ping command sends an ICMP echo request to a device on the network, and the device immediately responds with an ICMP echo reply. With ICMP Ping, SuperOps fetches the following data for any network device:
Round-Trip Time (RTT): The time taken between sending a ping request and receiving a reply. High RTT indicates high latency. It is measured in milliseconds.
Packet Loss: When a ping request does not receive a reply, the ping packet or the reply packet may have been lost. Packet Loss is the percentage of ping packets that get lost in a network when a ping request is made. High Packet Loss indicates a poor network connection.
Historical Ping Range: Displays the ping range in a 24 hour interval, with the minimum and maximum ping values.



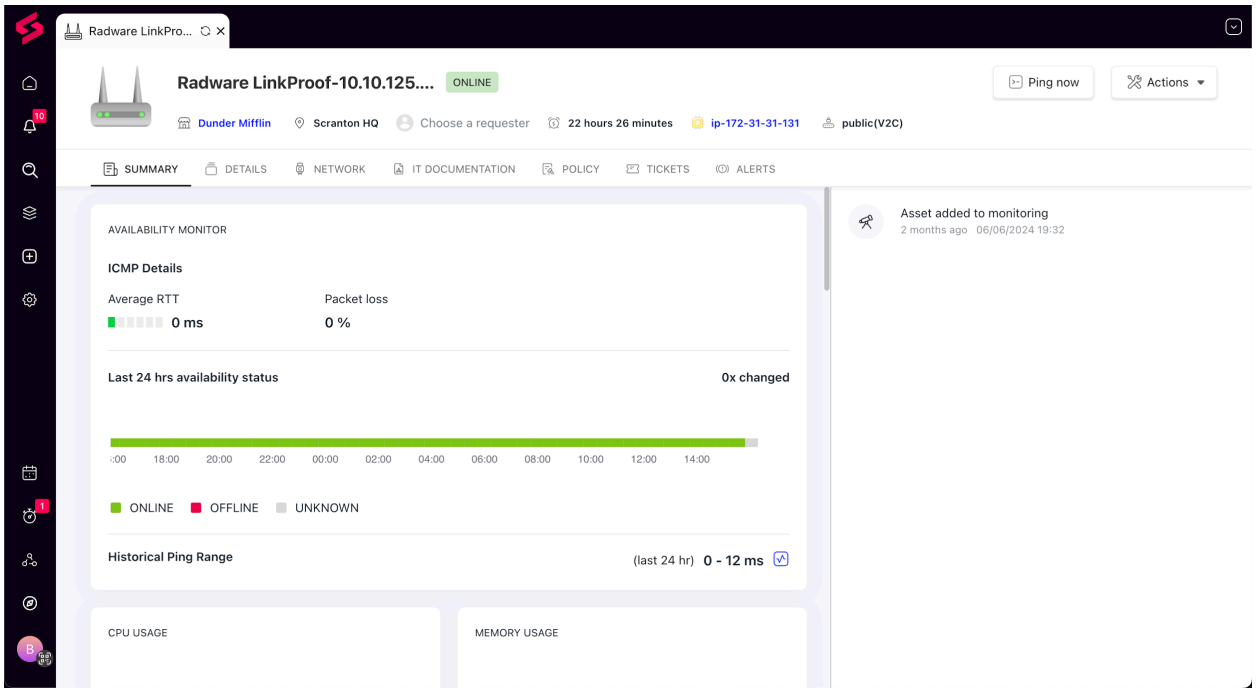
Availability Status: Round-Trip Time and Packet Loss data plotted in a graph, over a specified time interval. You can access this monitor directly from the asset summary tab by clicking on the ping icon under Historical Ping Range.



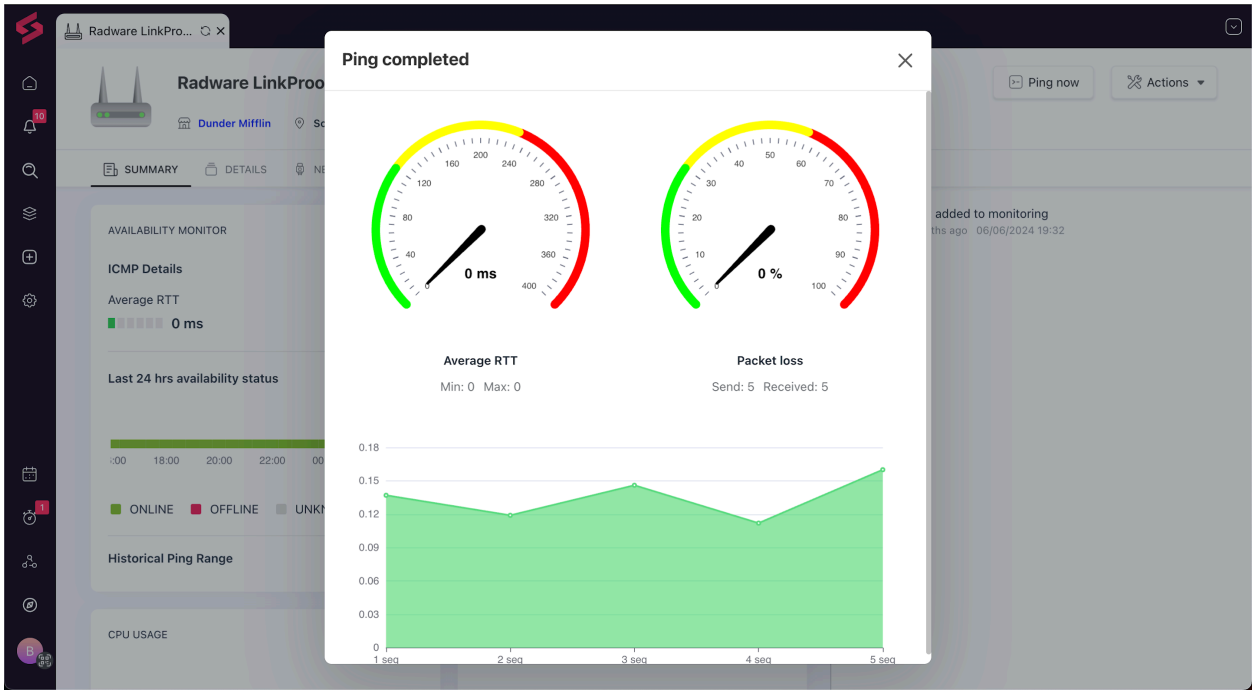
Note: All troubleshooting features will be available to use only if your SuperOps agent is on the latest version. We roll-out agent updates in a staggered manner over the course of a few days to ensure stability and to avoid issues. If you don't see these options in your SuperOps account, it means that you are not on the latest agent version yet, and that you will soon be upgraded. If you would like to use these features immediately, please reach out to us and we will enable it for you.

Using the Ping now option

If you experience slowness in a network device such as a router, you can diagnose the issue with Ping now and find out if there's latency on your network. Hitting Ping now will send 5 packets to the destination device, and report back on the RTT and Packet Loss data.



Once the ping request is completed, you will see the result as shown below. The graph depicts the ping value (in milliseconds) on the y-axis and the packet sequence in the x-axis.



The range depiction is as follows:

Ping:

0-120 ms: Good (green)

120-240 ms: Okay (yellow)

240-400 ms: Bad (red)

Packet Loss:

0-30%: Good (green)

30-60%: Okay (yellow)

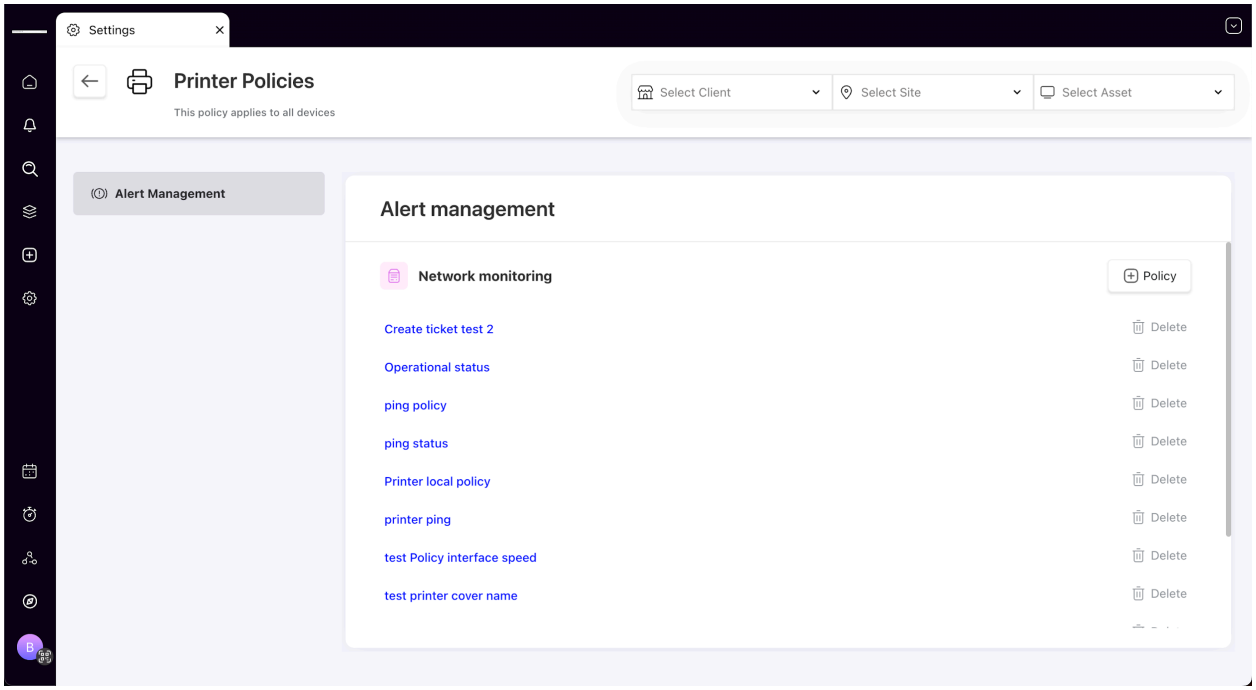
60-100%: Bad (red)

Setting up alerts based on ICMP Ping

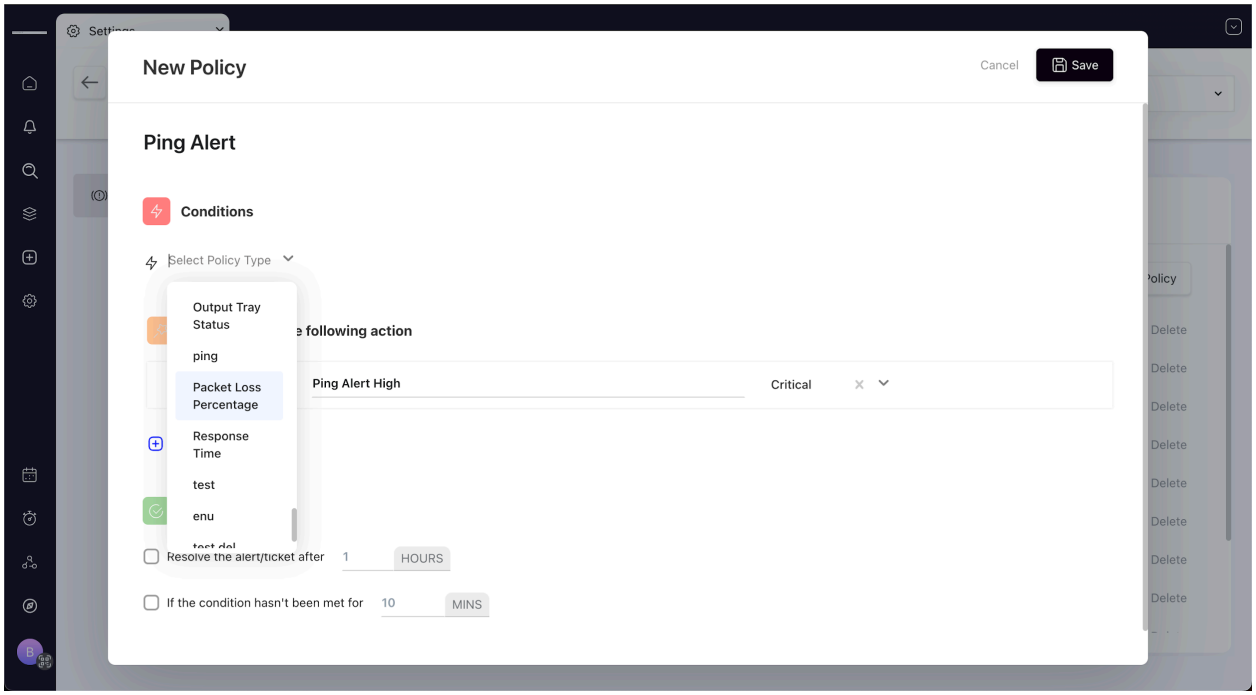
For network devices, you can set up alerts to monitor Ping, RTT, and Packet Loss. To set up an alert,

1. Go to Settings > Policy Management > Select the network policy of your choice.

2. Go to Alert Management and click +Policy.

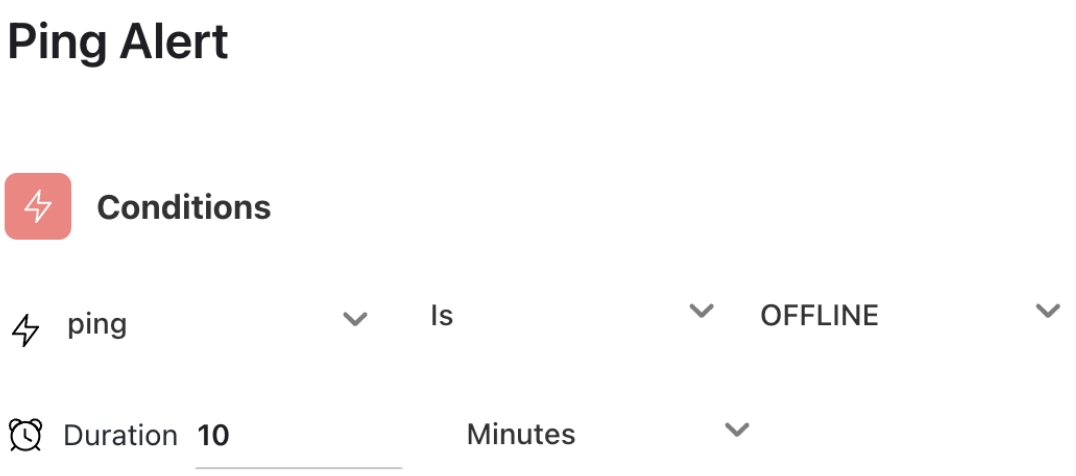


3. In the Condition dropdown, select Ping, Packet Loss Percentage, or Response Time based on what you metric want to monitor.



4. Specify the duration for which this condition should be met before your alert is triggered. For example, if you want to be alerted by a device that has

been offline for 10 minutes, you can set the Duration to 10 minutes and the condition to Ping Is OFFLINE.



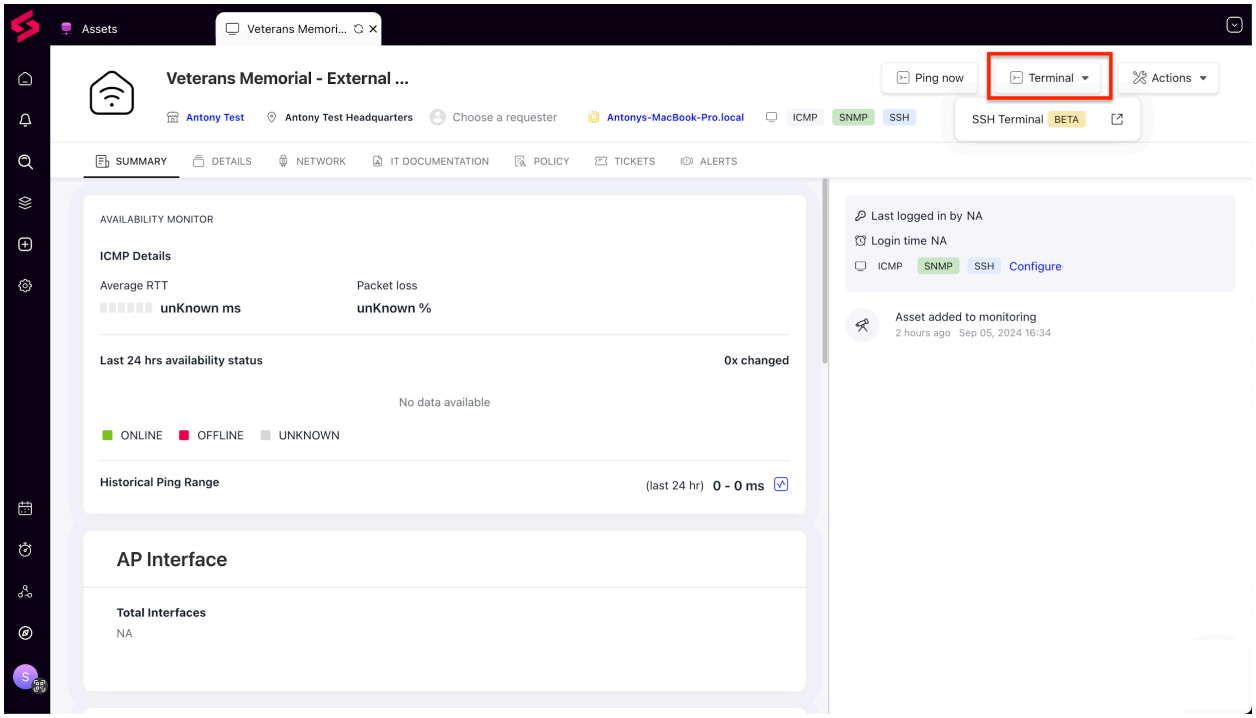
Troubleshooting with SSH (Secure Shell)

Note: If you have purchased the network monitoring add-on but don't see the Terminal button in your SuperOps account, it means that you are not on the latest agent version yet, and that you will soon be upgraded. If you would like to use SSH immediately, please reach out to us and we will enable it for you.

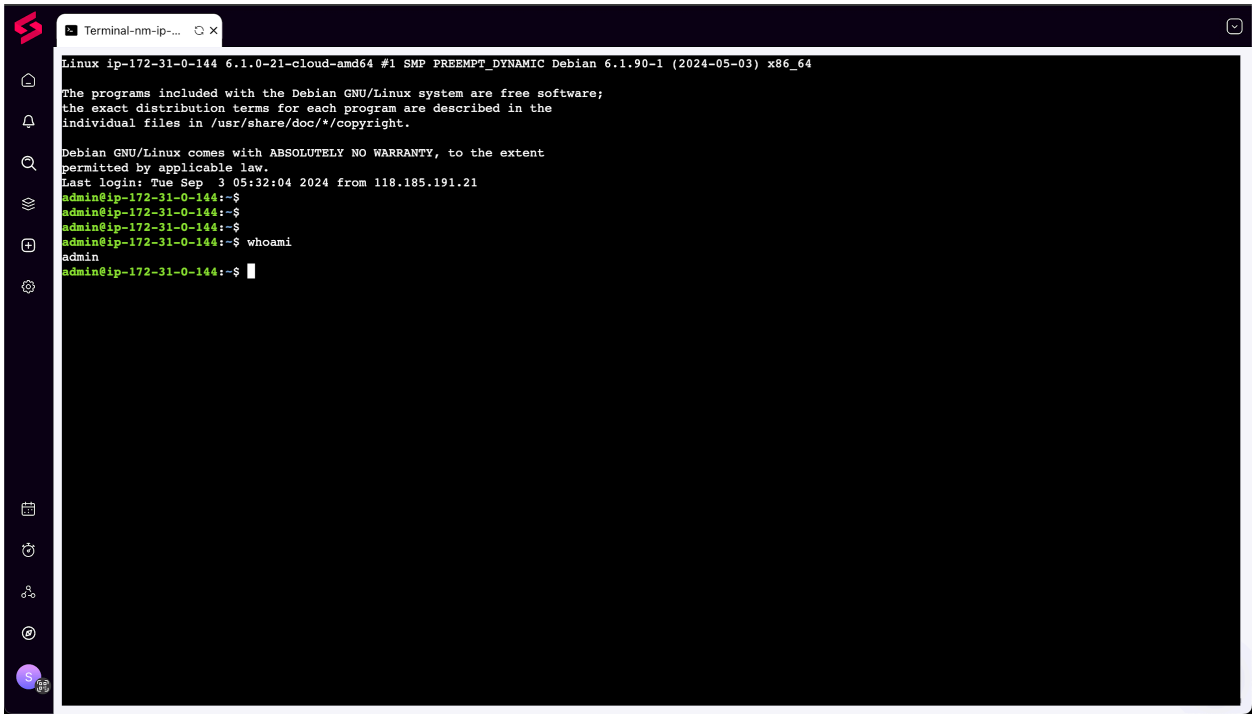
SSH (Secure Shell) is a network protocol that lets you access and operate a network device securely through a remote connection.
For SSH-enabled devices, you can securely access the terminal right within SuperOps. In a click of a button, SuperOps pulls up the terminal window and logs you into the network device. Without leaving SuperOps, you can remotely access and modify/check a network device to troubleshoot issues.
How to troubleshoot an issue with SSH:
1. To access the SSH terminal for a device, you will have to define its SSH credentials. Go to Settings > Credential Definition. Select the protocol as SSH

and enter your details. You could also do this by going to Assets > Probes > Credential.

2. Open the network device for which you want to access the terminal and click on the Terminal button at the right top. The SSH terminal will open as a new tab inside SuperOps.



3. With the SSH terminal opened, you can run commands to perform actions that will help you troubleshoot the issue with your network device. We have built a full-fledged terminal that you can access right within SuperOps, so you don't have to use a different platform to troubleshoot issues.



Common Network Monitoring Errors

In the table below, we have collated the list of possible errors you may encounter with SuperOps' network monitoring along with a description for each error.

Error	Description

redential is currently in use	ou are trying to delete a network redential that is associated with a networ evice.
o probe(s) found	he network scan cannot be triggered ecause no active probe exists in the ubnet. Add a probe before attempting the can.
annot delete probe. At least one prob ust remain active for this site	here needs to be at least one active prob a site. This error is thrown if you try to elete the only probe available in a articular site.
redential does not exist	he credential you are trying to access oes not exist or has been deleted.
lonitor is currently in use in an xpression	he custom monitor you are trying to delet being used in an expression of another ustom monitor. Delete or edit the xpression first in order to delete the onitor.

ubnet already exists	he subnet you are trying to create alread xists under the client and site.
his monitor configuration has already een added	he OID configuration you are trying to ad lready exists.

Network Discovery

Network discovery lets you scan a client's network on demand, and discover all the connected endpoints and network assets. With a single click, you can onboard the assets into SuperOps and start monitoring them.

Prerequisites

1. Ensure that the SuperOps agent is on the latest version.
2. Valid user credentials for WMI/SSH
3. To enable WMI on a client device, execute the command below:

```
netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes
```

4. Set the network type/domain to private, then execute

```
winrm quickconfig
```

5. Please ensure that winRM service is running on the probe as well as the client device. You can check the status of the service with the below command:

```
Get-Service -Name WinRM
```

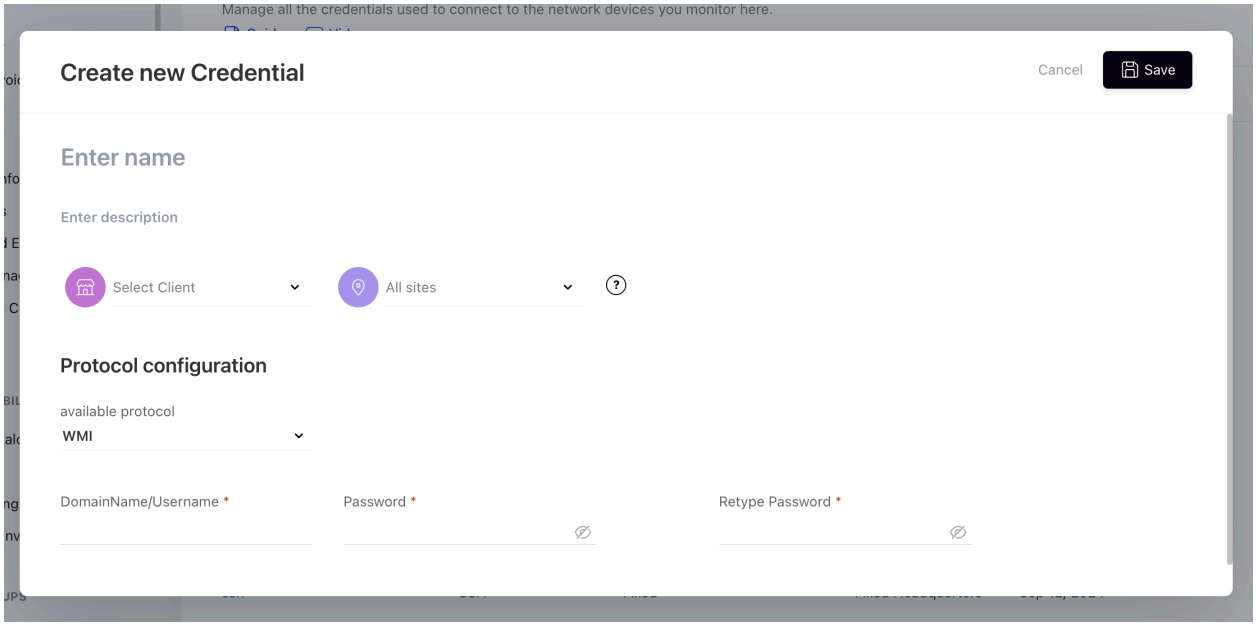
6. If the WinRM service isn't running, execute the below command (on both the probe and the client device) to start the service:

```
Start-Service -Name WinRM
```

7. If you would like to run a test network scan, please ensure you have at least one other device connected to the subnet besides the probe. A network scan will not pick up the probe machine as a device on the network.

Add WMI/SSH Credentials

A valid WMI or SSH credential is required for SuperOps to discover endpoints on a network and fetch asset information. Here's how you can enter your credential information into SuperOps:
1. Go to Settings > Credential Definition. Give your credential a name and select the client and site.
2. Select the protocol (WMI or SSH) and enter your credential information.



3. On entering WMI credentials, please ensure you enter DomainName\Username correctly. To find the DomainName\Username of a client device, execute the command below (on the client device):

```
whoami
```

Add a probe

Next, add a probe or convert an existing asset (that already has the SuperOps agent installed on it) into a probe. Check out this article for step-by-step instructions to add a probe.
If your probe is unable to reach a subnet, you can add this subnet manually by following the instructions here.

Scan for devices

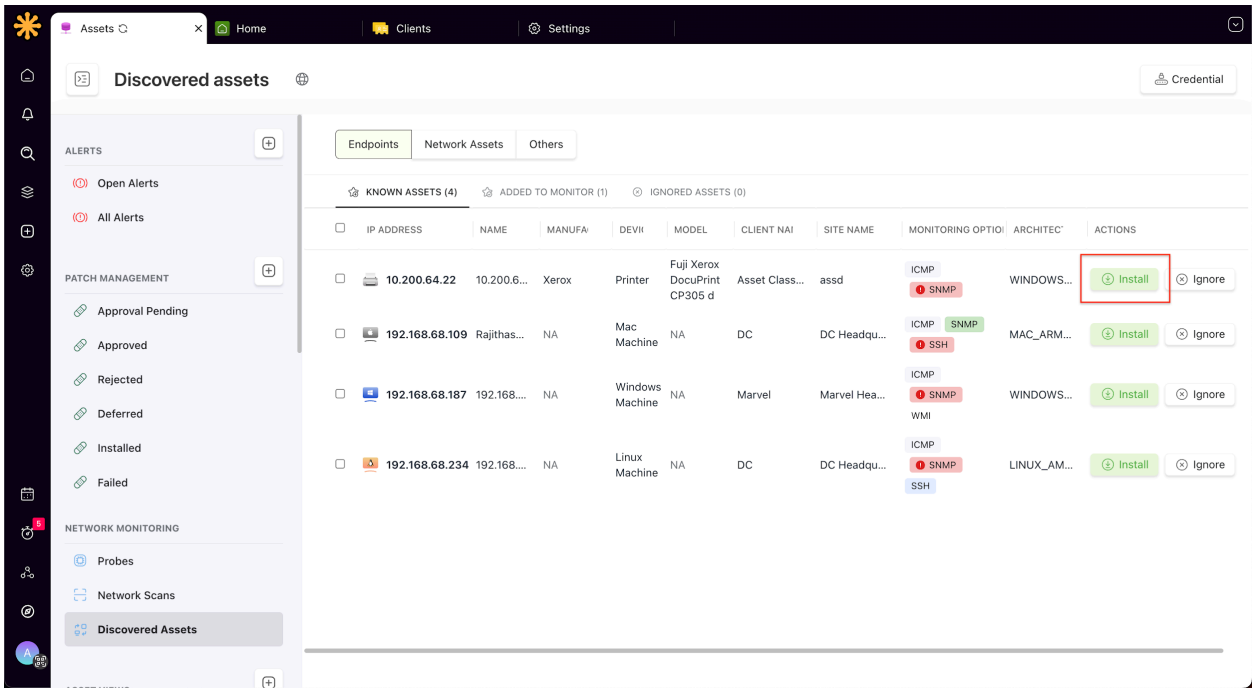
Once your probe is created, initiate a scan. Check out this article for step-by-step instructions.

Start monitoring your discovered assets

In the Discovered Assets tab, you will see the list of assets that the probe was able to discover in your client's network. You will see that the discovered assets are split into three tabs:
Endpoints: Workstations and servers
Network Assets: Network infrastructure devices such as printers, routers, etc.
Others: Devices that were discoverable only via ICMP

Endpoints

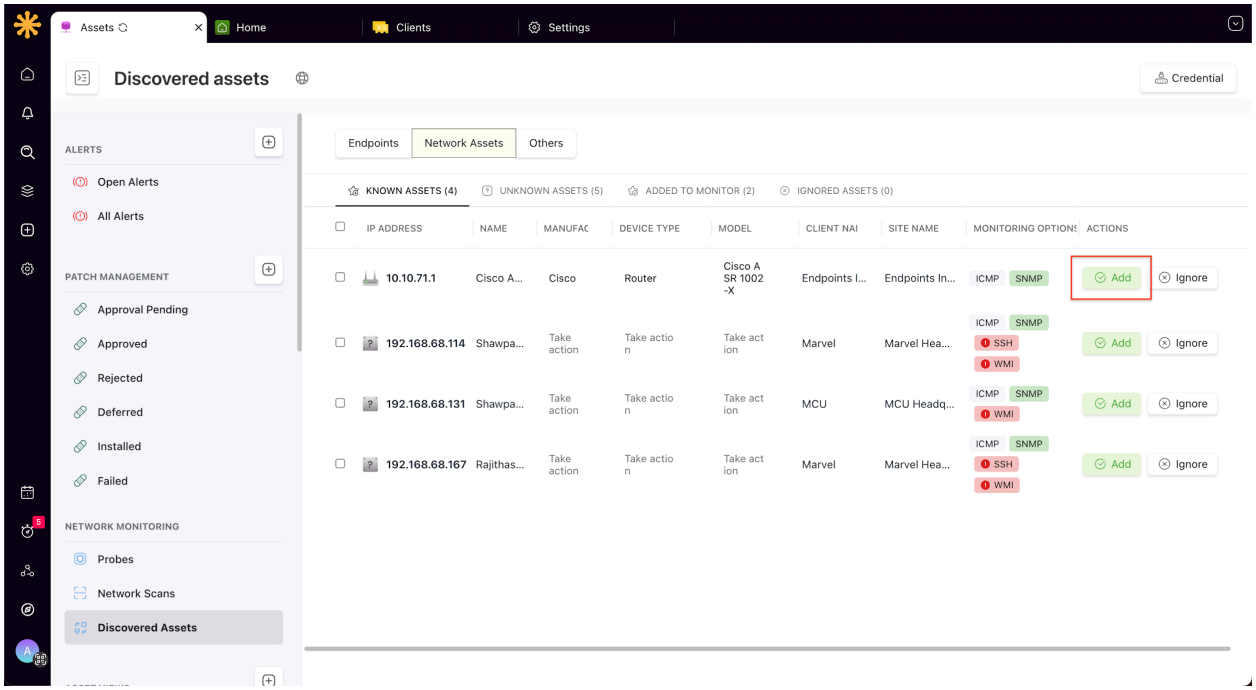
You can start monitoring workstations and servers discovered by the probe using the Install option. You can select your assets in bulk and install the agent with a single click.



Network Devices

You can start monitoring network assets using the Add option.

Note: An active network monitoring add-on pack is required to monitor network devices.


Assets
Home
Clients
Settings
Discovered assets
Credential
ALERTS
Open Alerts
All Alerts
PATCH MANAGEMENT
Approval Pending
Approved
Rejected
Deferred
Installed
Failed
NETWORK MONITORING
Probes
Network Scans
Discovered Assets
Endpoints
Network Assets
Others
KNOWN ASSETS (4)
UNKNOWN ASSETS (5)
ADDED TO MONITOR (2)
IGNORED ASSETS (0)
IP ADDRESS
NAME
MANUFAC
DEVICE TYPE
MODEL
CLIENT NAI
SITE NAME
MONITORING OPTIONS
ACTIONS
10.10.71.1
Cisco A...
Cisco
Router
Cisco A SR 1002 -X
Endpoints I...
Endpoints In...
ICMP
SNMP
Add
Ignore
192.168.68.114
Shawpa...
Take action
Take actio n
Take act ion
Marvel
Marvel Hea...
SSH
WMI
192.168.68.131
Shawpa...
MCU
MCU Headq...
192.168.68.167
Rajithas...
Marvel
Marvel Hea...