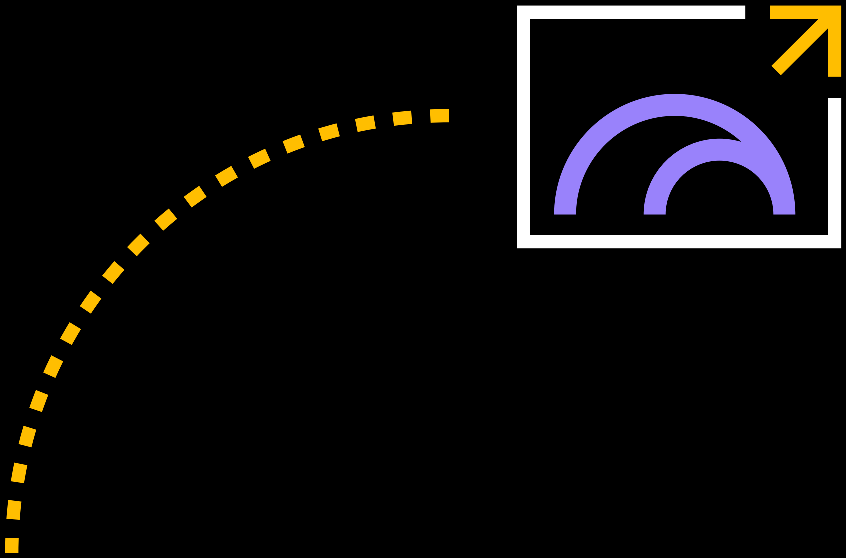
Auvik



Your guide to a successful Auvik deployment

Customer Guide

Getting started

Before we dive into onboarding networks, let's lay out some terminology and walk you through a couple of steps to help you get familiar with Auvik.

- **Global dashboard**
  The central location for managing your Auvik account. After you sign up, you'll automatically be logged directly into your global dashboard.
- **Site**
  A single site inside your global dashboard. Before doing anything else, you'll need to create a site. The site gives you full control of that specific network, client or location.
- **Multi-site**
  A special kind of site for advanced deployments.

The collector sends information to the Auvik servers through an SSL-encrypted web socket, following industry standards for secure data transmission on the internet. The collector uses certificate authentication to ensure it's communicating with the Auvik servers.

Now we're going to:

Add a new site

From your global dashboard

- Click **Add Site** (purple button at the top of your site list) to create a new site.
- Pick a domain prefix (URL) that has at least four characters. Only letters and numbers are allowed—no special characters.
- Select **Multi-site** as the type. Select Multi-site if you manage a large network or networks you want to silo into separate sites. (Think a college with multiple campuses, or a customer with multiple locations, for example).
- Click **Next.** Here's where you choose which Auvik users should have access to this site. Beside each user name, you'll also see the level of permission a user has. To change a user's permission level, select that person then use the Roles drop-down menu to pick a new level.
- Click **Save.** Your site has now been created.

TIP!
Want to know what permission sets each role has or create your own custom role? Go to Manage Users > Roles.
See How do I add, edit or delete user roles? in the Auvik Knowledge Base for full details and how-to instructions.

Adding more users

You may want to add more users to Auvik and give them access to this site.

- In the side navigation bar, click **Manage Users.** Invite any new users and set permission levels for their access on the site.

  See How do I manage invitations for new users? in the Auvik Knowledge Base for details.

TIP!
You can tie your Auvik account to your Google ID or your Microsoft Office 365 Business account, but don't do it yet. You first need an Auvik username and password to deploy the collector.

Choose your deployment method

Next, we need to figure out the best way of deploying Auvik based on your existing network architecture and the resources available within your own and your sites' facilities.

Wherever possible, we highly recommend:

- **Using the Windows service as your primary installer method,** as it's the fastest and easiest way to get Auvik running.
- **Installing one Auvik collector per site.**

Launch the Deployment Wizard

Once you've added a new site and selected your deployment method, you're ready to install your first collector.

Go to the dashboard for the new site. To get there from your global dashboard, you can:

- Click on the site's pin on the geographic map.
- Click on the site's name from the site list.

You're now in the deployment wizard. You'll see a few options for downloading your Auvik collector.

Deploy Auvik using the Windows installer

(Recommended)

What is it?

The Windows installer is a lightweight Windows service that can run on any server or workstation with network connectivity. It's the easiest Auvik deployment method.

Deployment process

Click Download the native service on the deployment wizard screen to download the AuvikService.exe file. Don't double-click the AuvikService. exe file! We all like GUIs because they're easy, but to keep the Auvik Windows service lightweight, we've left that out. Instead, here's how to install the Auvik collector:

1. Open up a command prompt as administrator.
2. Change the directory to where the collector was downloaded. This is usually something like `C:\Users\<username>\Downloads.`

TIP!

Don't install on an overloaded machine.

The Windows service uses ports 21 and 69. Putting it on a device where another service also uses these ports can result in a tug of war. For this reason, it's best to install the service on a device that isn't running another program that relies on these ports.

The Windows service can be easily deployed through an existing remote monitoring and management solution, such as ConnectWise Automate or Datto RMM.

3. Run the following command, replacing `<DOMAINPREFIX>` with the URL you picked when adding your site:

```
AuvikService -install -dir c:\auvik -tenant
https://<DOMAINPREFIX>.my.auvik.com
```

4. When requested, enter your Auvik email address and password. The email address must be for a user who has authorization on the Auvik domain the service is being installed for.

5. Make sure you use the **site** domain, not the one you picked for your global dashboard.

That's it! Now go back to your global dashboard in Auvik.

You can quickly confirm the collector is properly connected and approved by navigating to Auvik Collectors on the side navigation bar. There you'll find the collector's unique ID and IP address. You should see Connected and Approved in green.

For more information

- Windows installer: How to install the Auvik collector using the Windows service

Deploy Auvik using an advanced deployment method

If you can't or don't want to use the Windows service to deploy Auvik, you have a number of other deployment options to choose from. Since this is a quick start guide, we'll give you some references for the advanced deployments, but won't walk through all the steps.

OVA Installer

The OVA installer is an OVA file you download and install on a VMWare ESX / ESXi host. Download the OVA, import into vCenter, and you're good to go.

Detailed instructions: How to install the Auvik collector using the OVA file

Bash Installer

The bash installer is a script that installs Auvik on top of a stripped-down Ubuntu server. The server can be a physical or virtual server and can be installed on either x86 or ARM based devices.

This deployment method does take a bit longer—you should plan for 30 to 60 minutes. And make sure you use the exact Ubuntu server revision mentioned in the instructions.

Detailed instructions: How to install the Auvik collector from a bash script

Docker Image

Auvik also provides a Docker Container image that can be installed on either x86 or ARM based devices.

Detailed Instructions: Installing Auvik collector as a Docker image

Shared Collector

A shared collector is an Auvik collector installed in a central location (such as your data center) and can be shared across multiple sites. It's recommended for managing multiple small networks where you have Layer 3 connectivity to the client site, for example, through a VPN.

Detailed instructions: [How do I manage my shared collector?]()

POWER POINT!
Consider using a shared collector deployed on portable hardware. This gives you an "on demand" probe you can bring with you to client sites, speeding up initial discovery.

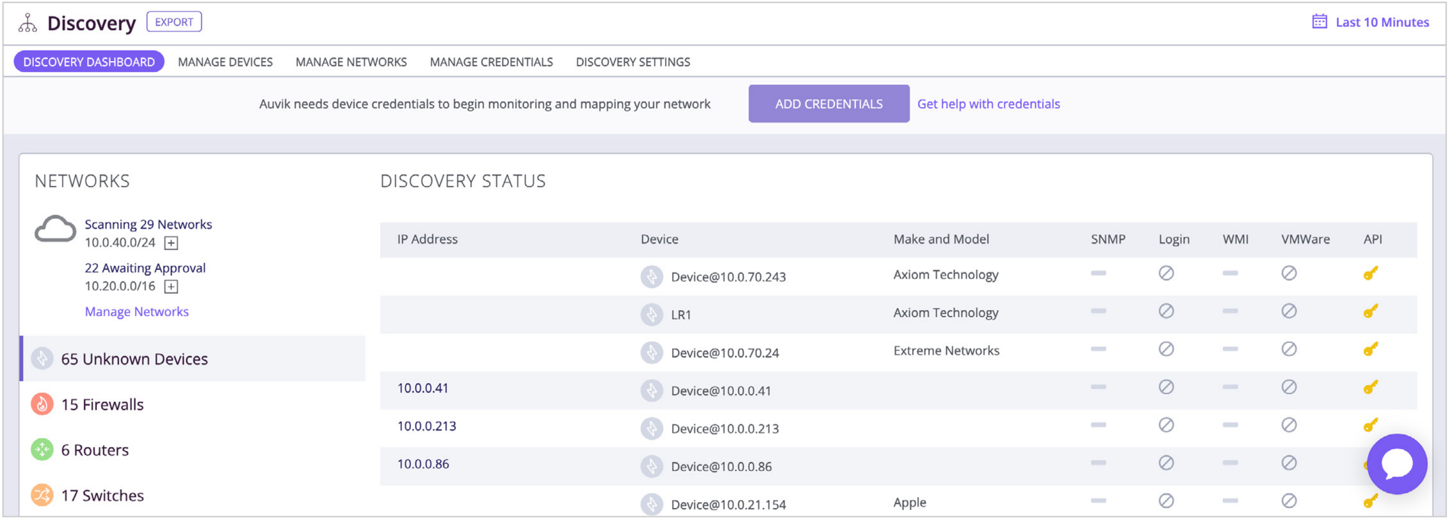
Auvik discovery begins

Auvik begins scanning on the subnet where the collector is installed, so those are the devices it will find first. On average, it takes vabout 15 minutes to fully discover a network but it does depend on the size of the network.

- Do you see a /16 or a /8 network? Consider scanning a couple of /24 networks instead as it will speed up discovery.
- Don't see any network listed at all? Click **Add Network** to manually add a subnet.

POWER POINT!
With such quick turnaround, you can start network discovery at the beginning of a prospect sales call and have some actionable data by the end.

TIP!
If you don't see any devices after 5 to 10 minutes, check under **Discovery > Manage Networks** to see the network we automatically started scanning.



Auvik needs device credentials to begin monitoring and mapping your network

Scanning 29 Networks
10.0.40.0/24 ⊞
22 Awaiting Approval
10.20.0.0/16 ⊞
Manage Networks

65 Unknown Devices
15 Firewalls
6 Routers
17 Switches

IP Address	Device	Make and Model	SNMP	Login	WMI	VMWare	API
	Device@10.0.70.243	Axiom Technology	—	⊘	—	⊘	🔑
	LR1	Axiom Technology	—	⊘	—	⊘	🔑
	Device@10.0.70.24	Extreme Networks	—	⊘	—	⊘	🔑
10.0.0.41	Device@10.0.0.41		—	⊘	—	⊘	🔑
10.0.0.213	Device@10.0.0.213		—	⊘	—	⊘	🔑
10.0.0.86	Device@10.0.0.86		—	⊘	—	⊘	
	Device@10.0.21.154	Apple	—	⊘	—	⊘	🔑

This is what a good Auvik map looks like.

In the end, we want a network diagram of predominantly blue wires (showing Layer 1 connectivity) rather than a diagram of all black wires (showing inferred connections).

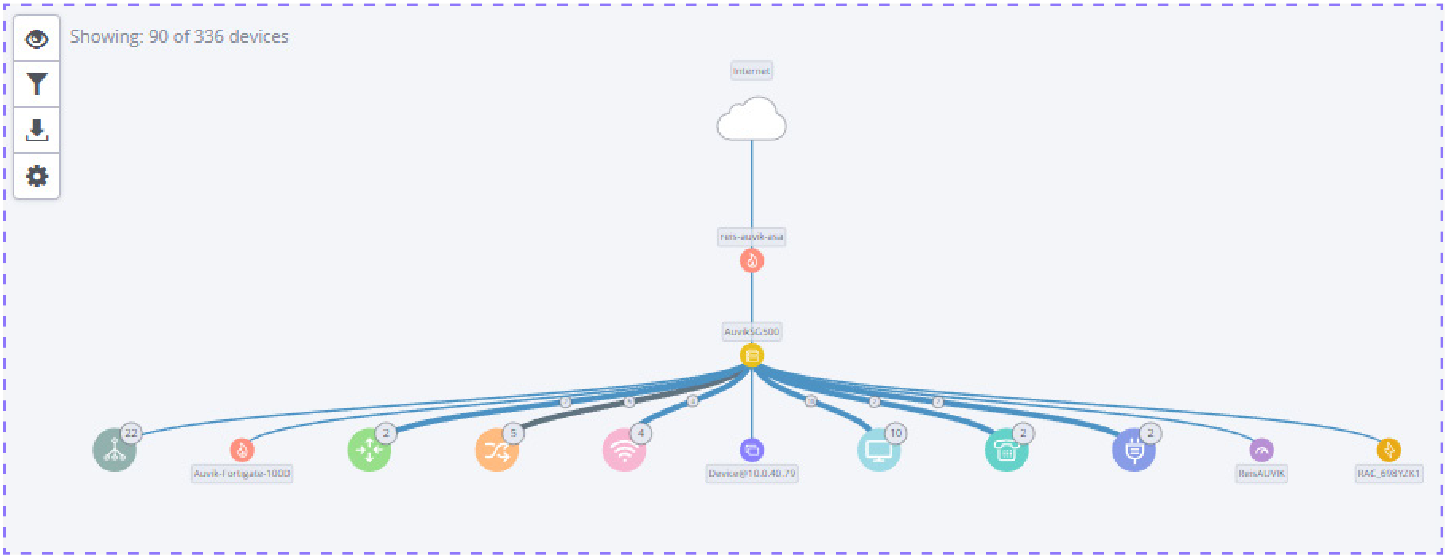
This is what a good Auvik map looks like. Notice all the blue wires. The firewall sits between the Internet and the rest of the network. The devices are properly identified and labeled.

POWER POINT!

Troubleshooting becomes simple when your entire technical team has instant visibility into how a client's network is configured and connected.

TIP!

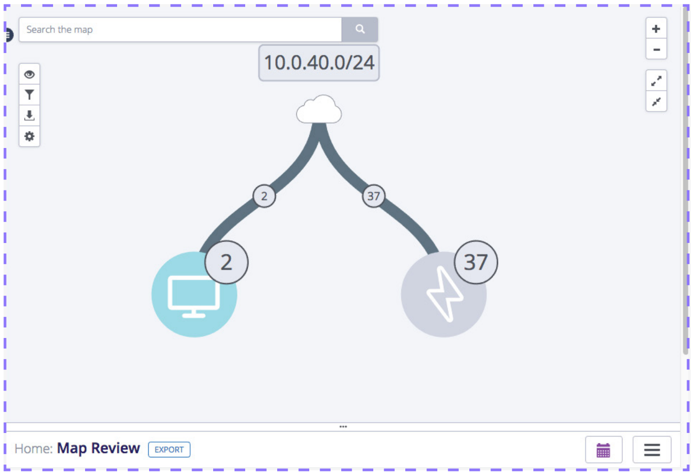
If you share credentials across multiple clients, entering these credentials at the global level, instead of the site level, can save you a lot of time.

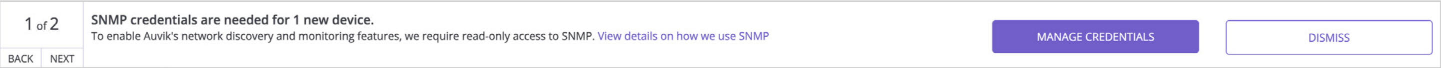


This is what a map with problems looks like.

This is what a map with problems looks like. Quite a difference! The wires are black. Most devices are represented by a generic grey lightning bolt, which means they haven't been identified. A map like this means Auvik needs more information from you. Read through the deployment tips below for guidance.

As discovery progresses you'll see a banner across the top of the page. These are discovery tips. Follow the prompts to add credentials, add networks to scan, and so on. This keeps the iterative discovery process moving.




1 of 2

SNMP credentials are needed for 1 new device.
To enable Auvik's network discovery and monitoring features, we require read-only access to SNMP. View details on how we use SNMP

Tips for a smooth Auvik discovery

While Auvik is discovering your site's network, here are a few things to check on or complete to ensure the resulting network map is as accurate as possible.

□ Make sure SNMP is enabled.

Auvik uses SNMP to collect performance statistics and get make and model information so we know what commands to send to the device. Enabling SNMP is also required for making configuration backups.

You should always enable SNMP on all network devices before adding login credentials for those devices.

If your initial scan shows a lot of black wires or gray "generic" devices, chances are you need to add SNMP credentials into Auvik or enable SNMP on one or more devices. If you aren't sure which devices need SNMP credentials added, Auvik lets you know during discovery by creating a new message in the banner across the top of the screen.

If you need to enable SNMP on network devices, log into the device's GUI interface, navigate to the SNMP section, and configure the relevant settings. Alternatively, if the device only has a terminal interface, log in and run the vendor-specific commands to turn it on.

If you aren't sure how to enable SNMP on a particular device, check Auvik's Knowledge Base. We have a large and growing number of articles on how to enable SNMP for various vendors and devices: Device setup and configuration.

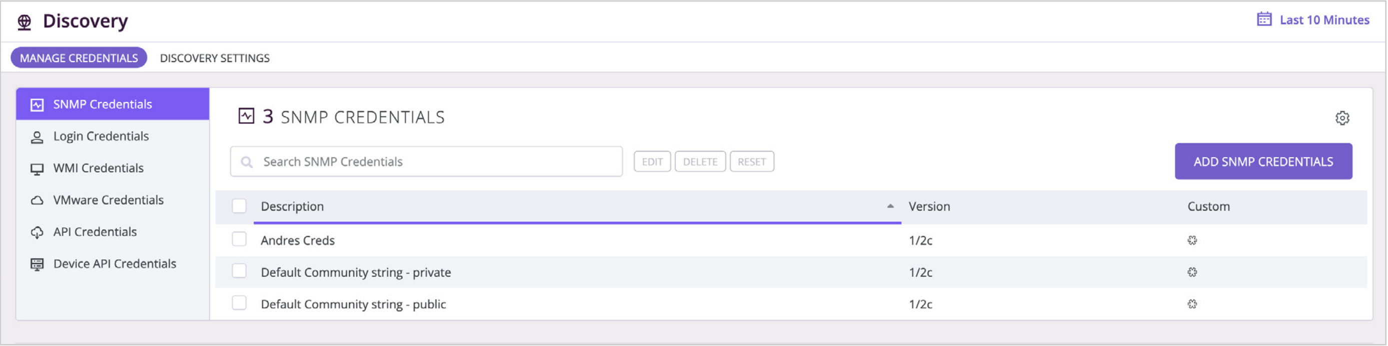
Not all vendors provide all management information over SNMP. Some vendors use APIs and non-standard protocols to access device data. Auvik is actively working on alternate ways of collecting device information, so check the Knowledge Base for your specific vendor to see if there are additional steps to complete.

□ Enable SNMP on wireless controllers and standalone APs

To pick up wireless connections to access points (APs), make sure wireless controllers or standalone thick APs have SNMP enabled. Wireless connections are drawn as blue dashed lines between APs and devices.

□ Manage SNMP credentials

Auvik automatically tries the default community strings of "public" and "private" on all devices for which it recognizes active SNMP. If the string is different, have it ready to input. Or, if you're using SNMPv3, have the username, auth protocol, and passphrase credentials ready.



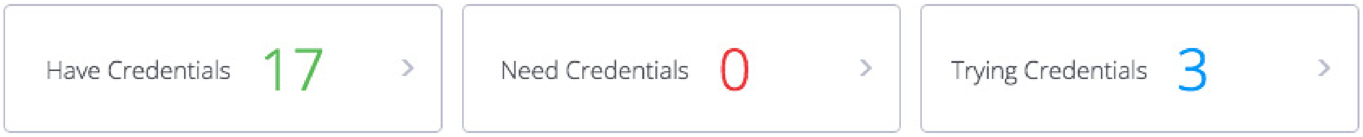
3 SNMP CREDENTIALS

	Description	Version	Custom
□	Andres Creds	1/2c	⚙
□	Default Community string - private	1/2c	⚙
□	Default Community string - public	1/2c	⚙

After Auvik's initial scan, you can go to Discovery > Credentials > SNMP Credentials to see how many devices have successful SNMP credentials, how many devices are missing credentials, and how many devices are currently trying credentials. Click on any of the numbers for a list of the devices in that category.

You can add additional SNMP credentials by clicking on the **Add SNMP Credentials** button.

We recommend leaving the Devices field blank so that Auvik tries that SNMP community string on any device that has SNMP enabled.


Have Credentials 17 ›

Need Credentials 0 ›

Trying Credentials 3 ›

□ Manage login credentials

Login credentials are important for features such as the terminal and configuration backup and restore. Login credentials also pull route, ARP, and FDB data from switches, which can help with accurate discovery.

There are four things that need to be in place before login credentials can be authenticated.

1. The credentials for the user you add must have full access, rather than read-only access, on the account. (You should be able to execute commands such as "show runningconfig." You can test this by going into the terminal and trying a few show commands.) You'll also need to add the device's CLI elevated "enable" credentials for Auvik to be able to run the necessary commands.
2. SNMP must be enabled on the device, and the device must be properly classified in Auvik. If it's not properly classified, you can change the Type field manually by editing device details through the Manage Devices menu.
3. Telnet or SSH must also be enabled on the device.
4. Auvik needs to be able to detect the service. The service status will show as a grey line instead of a circle with a line through it if the device is ready.

If the above four things are true, Auvik attempts to authenticate.

POWER POINT!

Automatic configuration backups increase team efficiency by reducing the amount of time your team spends on repetitive monthly device backups.

TIP!

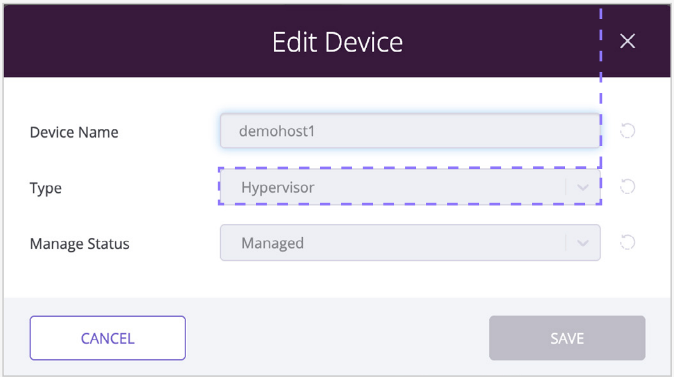
Auvik will attempt SSH on standard port 22 and Telnet on standard port 23. If you're using non-standard ports (or have a WatchGuard that uses port 4118 for SSH), then you need to make some small tweaks. Details here: How do I manage discovery services?

□ Manage VMware credentials

Have SNMP enabled on your VMware hypervisors? Great—you're likely already being prompted for VMware credentials.

The credentials you add should be the VMware credentials for the hypervisor host itself, not for a guest or the vCenter server. Once your credentials are properly entered, Auvik should show the hypervisor at the top and all hosts organized underneath it.

If you don't have SNMP enabled on your VMware hosts, it's easy to manually classify the host as a hypervisor. Search for the ESXi host IP address in Inventory > All Devices. Select the device name to open the device dashboard. Click **Edit** next to the device name and change the type field to Hypervisor.



Device Name: demohost1

Type: Hypervisor

Manage Status: Managed

POWER POINT!

Beyond performance stats, Auvik also pulls in hardware details from VMware hosts, giving you visibility into failed hard drives, power supplies, and fans.

TIP!

If you have Hyper-V, we can talk to those hosts using WMI. Follow the instructions on the following page for adding WMI credentials. Don't add Hyper-V credentials in the VMware credentials section of Auvik—they won't work there.

□ Manage WMI credentials

Servers often have WMI turned on by default, but not workstations. If you'd like to monitor all Windows endpoints, you'll want to turn on WMI through a group policy. Here's how to do it: How to enable WinRM with domain controller Group Policy for WMI monitoring

If you want WMI on just a few devices, follow these directions for enabling WMI on a single device: How to enable WMI monitoring on a single Windows device

Once you have WMI enabled, go to Discovery > Credentials > WMI Credentials to add a domain administrator or similar credential that has access to those servers.

□ Manage cloud controllers

Have devices that are managed via a Cloud Controller such as Meraki? You'll want to ensure that Auvik can talk to your cloud controller. Go to Discovery > Manage Cloud Controllers to set up the integration. Detailed instructions here: How do I manage cloud controllers?

POWER POINT!

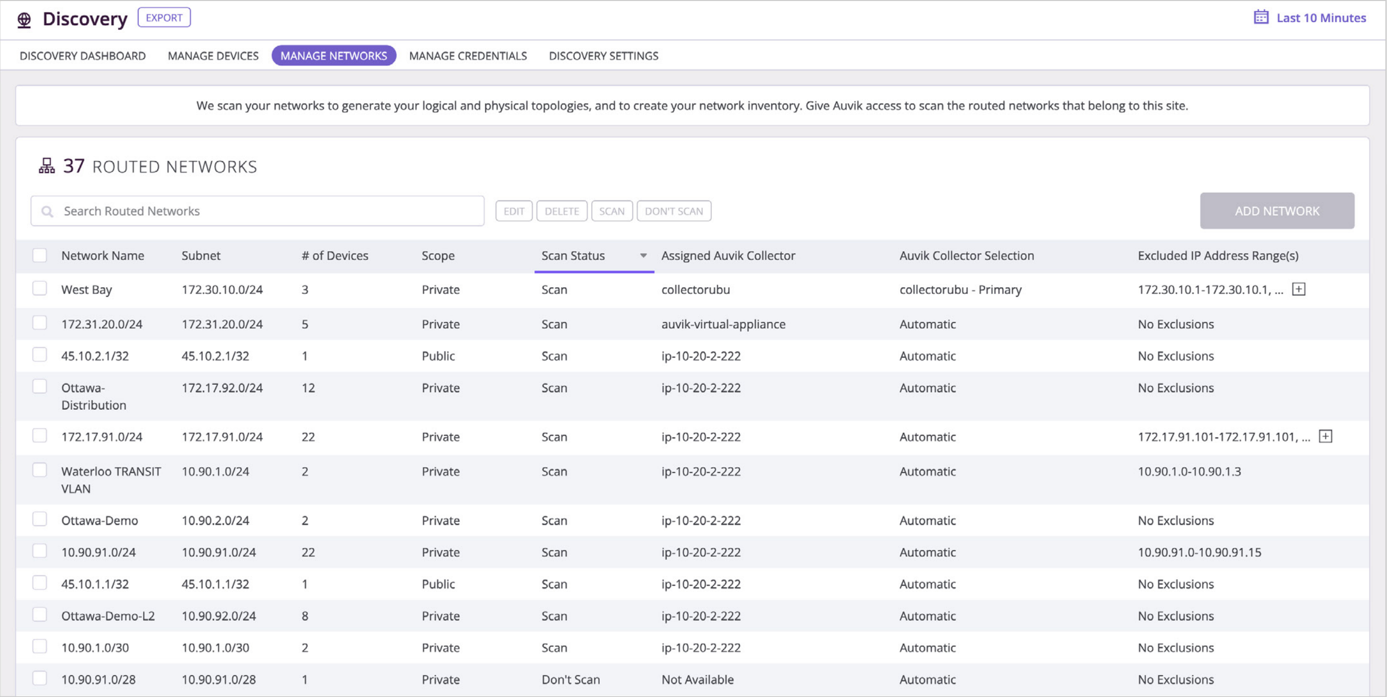
Auvik automatically pulls networks from managed network devices, and may find subnets you and your client didn't know existed.

□ Manage networks

If there are multiple subnets on your site, it's likely we've already found the additional networks. You can see the networks we found under Discovery > Manage Networks. You'll see some of the networks are awaiting approval.

Technically, you can scan public networks, but we don't recommend it—so if that's what you want to do, you'll need to actively opt in by adding the network manually. Keep in mind that Auvik defines a public subnet as anything not in an RFC 1918 address name, so any internal network that uses a non-RFC 1918 range will have to be manually added as well.

If a network you want to scan is missing from the list, you can add it using the **Add Network** button. Remember to add the subnet mask in its CIDR format. Auvik then begins its scan.



We scan your networks to generate your logical and physical topologies, and to create your network inventory. Give Auvik access to scan the routed networks that belong to this site.

37 ROUTED NETWORKS

□	Network Name	Subnet	# of Devices	Scope	Scan Status	Assigned Auvik Collector	Auvik Collector Selection	Excluded IP Address Range(s)
□	West Bay	172.30.10.0/24	3	Private	Scan	collectorubu	collectorubu - Primary	172.30.10.1-172.30.10.1, ... ⊞
□	172.31.20.0/24	172.31.20.0/24	5	Private	Scan	auvik-virtual-appliance	Automatic	No Exclusions
□	45.10.2.1/32	45.10.2.1/32	1	Public	Scan	ip-10-20-2-222	Automatic	No Exclusions
□	Ottawa-Distribution	172.17.92.0/24	12	Private	Scan	ip-10-20-2-222	Automatic	No Exclusions
□	172.17.91.0/24	172.17.91.0/24	22	Private	Scan	ip-10-20-2-222	Automatic	172.17.91.101-172.17.91.101, ... ⊞
□	Waterloo TRANSIT VLAN	10.90.1.0/24	2	Private	Scan	ip-10-20-2-222	Automatic	10.90.1.0-10.90.1.3
□	Ottawa-Demo	10.90.2.0/24	2	Private	Scan	ip-10-20-2-222	Automatic	No Exclusions
□	10.90.91.0/24	10.90.91.0/24	22	Private	Scan	ip-10-20-2-222	Automatic	10.90.91.0-10.90.91.15
□	45.10.1.1/32	45.10.1.1/32	1	Public	Scan	ip-10-20-2-222	Automatic	No Exclusions
□	Ottawa-Demo-L2	10.90.92.0/24	8	Private	Scan	ip-10-20-2-222	Automatic	No Exclusions
□	10.90.1.0/30	10.90.1.0/30	2	Private	Scan	ip-10-20-2-222	Automatic	No Exclusions
□	10.90.91.0/28	10.90.91.0/28	1	Private	Don't Scan	Not Available	Automatic	No Exclusions

□ Use the device troubleshooting pages

If credentials don’t authorize properly, you can diagnose the issue using the device dashboard. The troubleshooting screens under Discovery > Troubleshooting on the device dashboard walk you through the steps to authorize devices.

For more details on how to use the troubleshooting pages for each discovery service that requires credential authentication, please see:

- Troubleshoot SNMP credentials
- Troubleshoot login credentials
- Troubleshoot WMI credentials
- Troubleshoot VMware credentials

□ Whitelist Auvik’s IP address on your firewall or proxy

Has discovery not started yet? Are you not seeing anything on your Auvik dashboard? There could be a proxy blocking traffic.

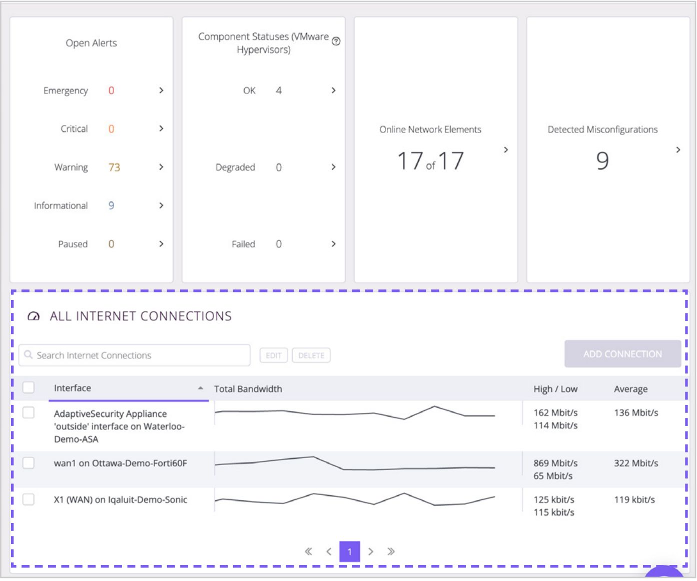
Users that have a proxy or do any SSL inspection will absolutely need to whitelist Auvik. If you’re unsure whether you have a proxy or how to whitelist on a proxy, please contact support@auvik.com.

□ Check the internet connections dashboard

Auvik discovers your Internet connections automatically but sometimes our discovery can be incomplete. From the home dashboard, look at the Internet Connections widget to make sure the interfaces listed are in fact associated with your Internetfacing WAN connections.

If not, you can edit the connection, delete it entirely, or add a new one through the Add Connection link within the widget.

From Inventory > Services > Internet Connection Check, also make sure the public IP address for the endpoint is correct and that when you click on the IP, the Packet Loss and Round Trip Time widgets are successfully polling data.



Open Alerts

Emergency	0	>
Critical	0	>
Warning	73	>
Informational	9	>
Paused	0	>

Component Statuses (VMware Hypervisors)

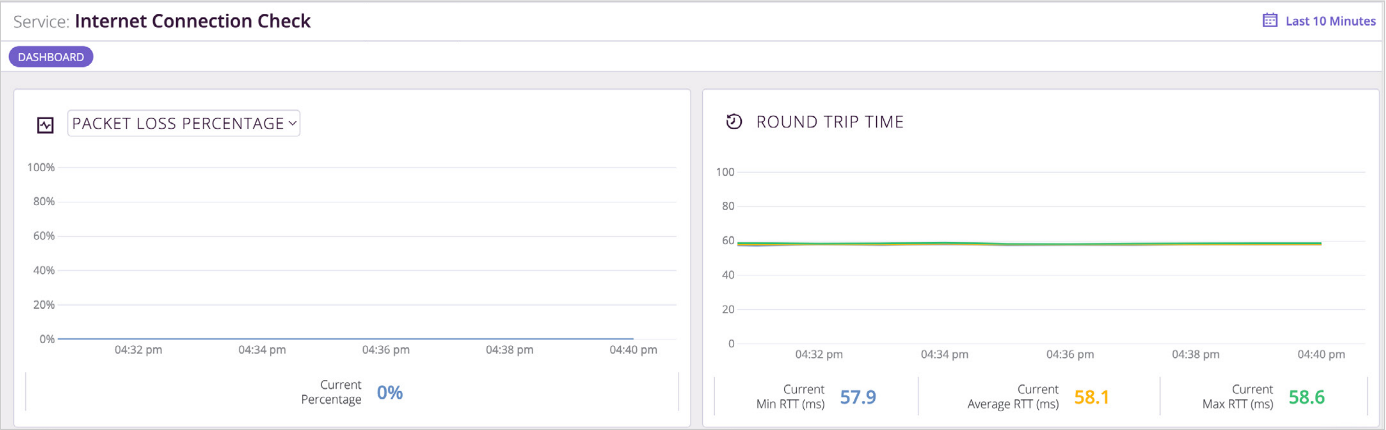
OK	4	>
Degraded	0	>
Failed	0	>

Online Network Elements 17 of 17 >

Detected Misconfigurations 9 >

ALL INTERNET CONNECTIONS

Interface	Total Bandwidth	High / Low	Average
AdaptiveSecurity Appliance 'outside' interface on Waterloo-Demo-ASA		162 Mbit/s 114 Mbit/s	136 Mbit/s
wan1 on Ottawa-Demo-Forti60F		869 Mbit/s 65 Mbit/s	322 Mbit/s
X1 (WAN) on Iqaluit-Demo-Sonic		125 kbit/s 115 kbit/s	119 kbit/s



Service: Internet Connection Check

Current Percentage 0%

Current Min RTT (ms) 57.9

Current Average RTT (ms) 58.1

Current Max RTT (ms) 58.6

□ Troubleshoot missing devices and networks

If there's a network missing from your map, it may be because that network is connected over a VPN or MPLS. See the point above on managing networks to get those networks added.

If you're missing a device, try to ping it from the Auvik console. If that doesn't work, use the Nmap command. If both results are negative, the device may be in stealth mode and blocking port scans. Make sure Auvik can use port scanning on that device.

Other known issues can be found in the Auvik Knowledge Base: Known issues.□

POWER POINT!

You'll always know the Internet is down before your customers or users call you. Auvik also helps you narrow down whether performance issues are ISP-related or internal.

□ Troubleshoot maps with lots of black wires

We mentioned earlier that we want to see blue wires showing physical connections. Your map may already show lots of blue wires and very few black wires. If so, that's great. But what if you're still seeing a lot of black wires?

You probably need to enable SNMP on some of your network devices. Here's how to find devices that might need SNMP enabled.

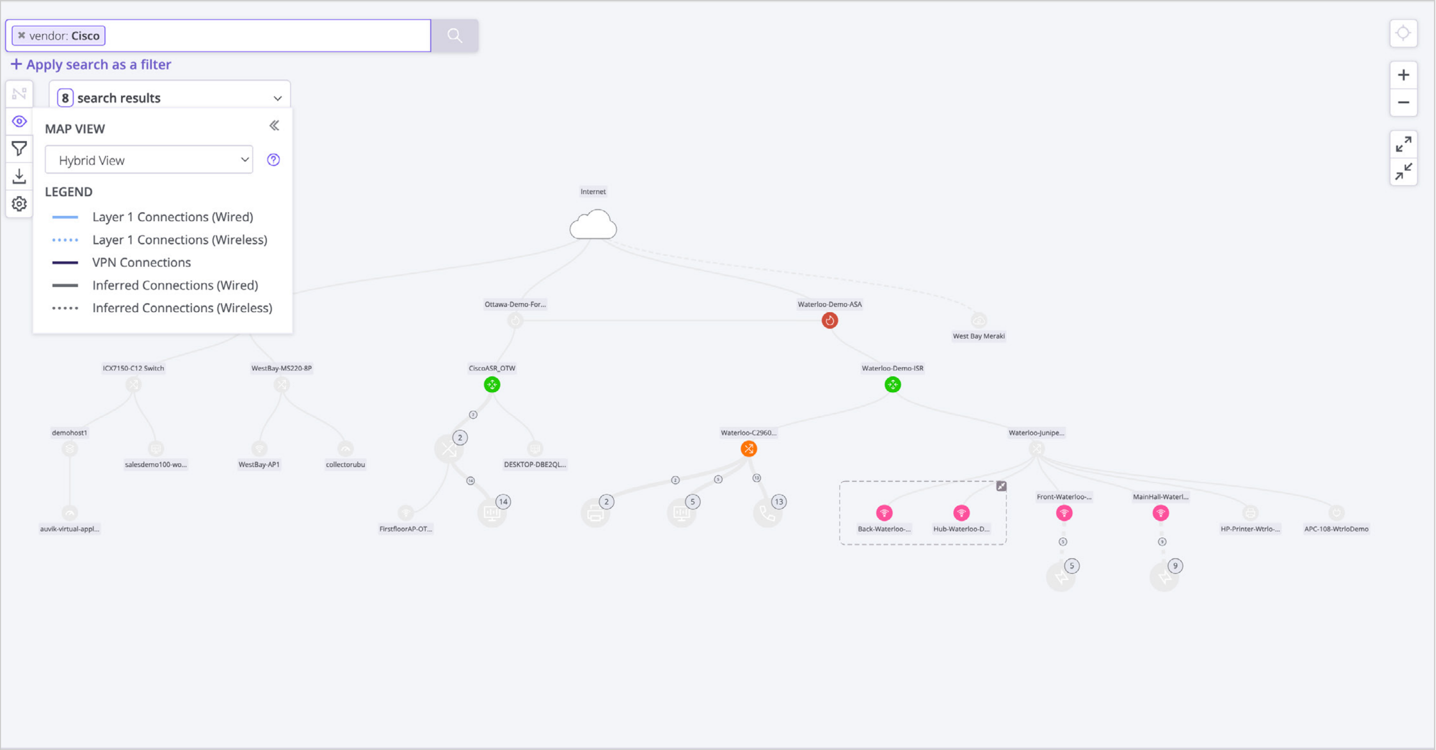
1. There are some special IP addresses that are often used for network devices. Check under Discovery > Manage Devices. Do you see any IP addresses ending in .1 or .254? These may be a firewall or router. Other IPs like .250 - .252 and .2 - .5 may be used as well.

2. Auvik can often discover the make of a device before we fully manage it. Under the Discovery > Manage Devices, you'll see make and model information. You can search for known network vendors like Cisco, Netgear, and Ubiquiti. You should see a green check mark beside all the network devices. If not, there's more credential-adding work to do.

   Alternatively, you can search the map for common vendors, such as Cisco. If a device from a known vendor is showing up on the map as a generic device, it might be a network element without SNMP enabled. Enable it.

POWER POINT!

These three action items can be used for prospecting and onboarding new networks. You definitely want to know what kind of network gear you're going to be expected to manage.



vendor: Cisco

+ Apply search as a filter

8 search results

MAP VIEW

Hybrid View

LEGEND

- Layer 1 Connections (Wired)
- Layer 1 Connections (Wireless)
- VPN Connections
- Inferred Connections (Wired)
- Inferred Connections (Wireless)

3. If you're not sure which devices are network gear, try using Auvik's remote browser feature to see the web interface on a device. This will often provide visual cues. Instructions here: [How do I launch a remote browser connection?]

Auvik also leverages discovery protocols like CDP and LLDP to discover physical connections. Review your switches and routers to confirm if they support CDP or LLDP and enable it if they do.

Still have questions?

We are here for you.

As a subscriber: Your Auvik success team is your main point of contact and can assist you with any questions! You can reach out to them directly via success@auvik.com.

If you need technical assistance, the Auvik support team is always available to help. You can reach out to them in several ways:

Use the chat box in the bottom right corner of the Auvik window.

Click Knowledge Base in the bottom left corner of the toolbar in your Auvik window. The Auvik Knowledge Base has a ton of articles to help with common issues.

Email support@auvik.com to create a ticket.

Call Auvik toll-free and hit 2 at the main prompt to connect to the support team, available from 4am ET to 10pm ET Monday to Friday (excluding Company holidays).

1-866-59-AUVIK (28845)	North America
+44 800 368 7578	UK & Europe
800 934 221	Australia
800 854 898	New Zealand

About Auvik

Auvik is a cloud-based IT management platform that helps IT departments proactively manage their networks, endpoints and SaaS applications. The key is absolute simplicity: seamless deployment, an intuitive interface, and effortless automation. The result is less friction for IT departments, so that everyone can work however and wherever they want.