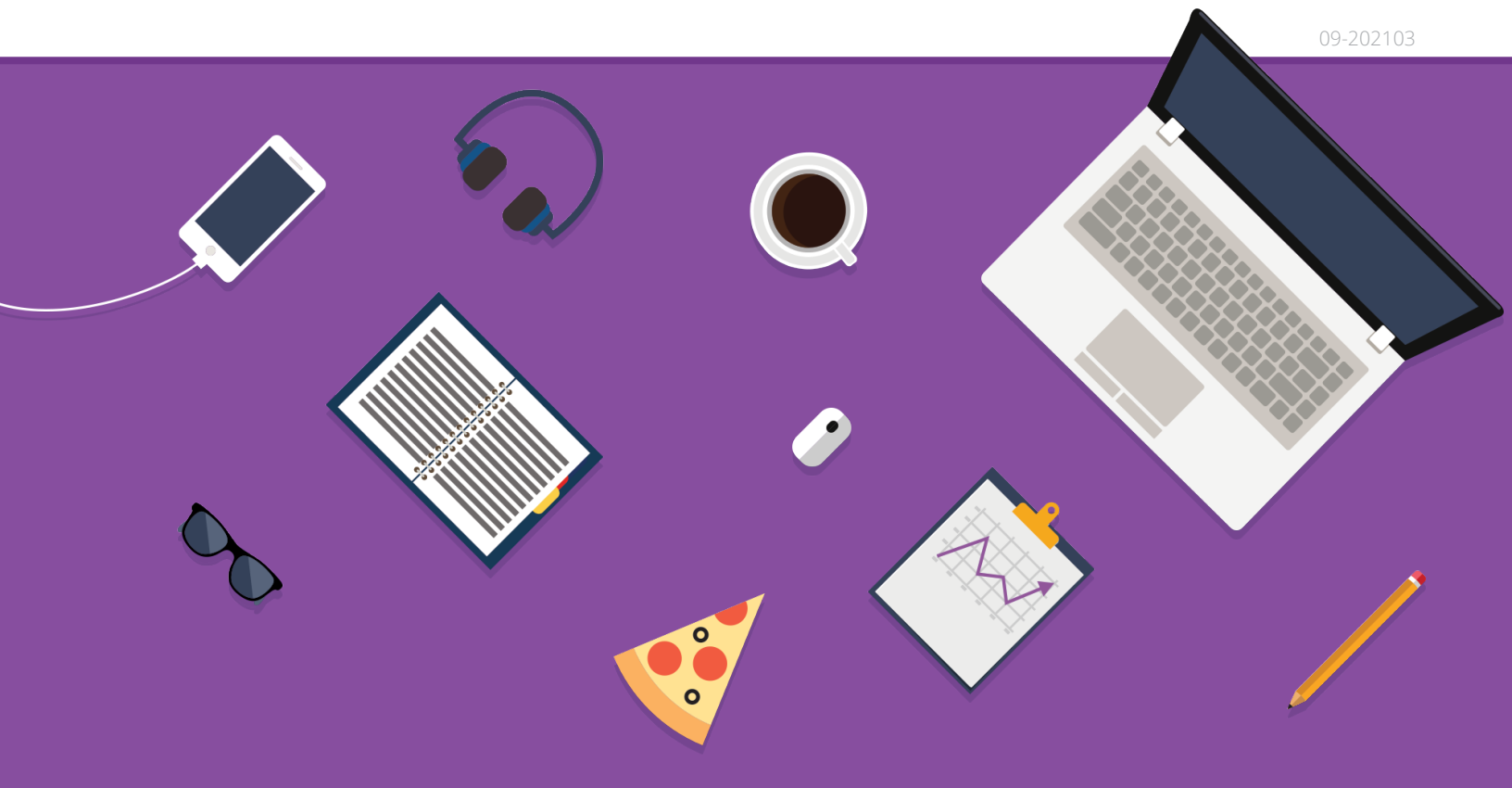




# Your Guide to a Successful Auvik Deployment

09-202103



# A FEW WORDS ABOUT GETTING YOUR AUVIK ACCOUNT STARTED

*If you've already set up your Auvik account, skip to page 3 to get started with deployment.*

To get started with an Auvik account, you first need to sign up for one. Use the link given to you by your Auvik account manager and follow the instructions on screen.

(If you don't have the link, send an email to [sales@auvik.com](mailto:sales@auvik.com) and we'll send you one.)

As you fill out the form, you should see green check marks beside each field. If you don't, you may need to enable JavaScript or try a different browser.

After you sign up for your account, you'll be required to set up two-factor authentication when you next log in. Auvik uses a time-based one-time password protocol (TOTP). For more information on getting two-factor authentication set up, see the Auvik [Knowledge Base](#).

The first 14 days with your Auvik account are unlimited. You can deploy to as many sites as you'd like and monitor as many devices as you like. Before the free period ends, you can work with your Auvik account manager to set up a subscription and continue using your account.

Not ready to talk to an Auvik human yet? Don't worry, you can also click the **View Plans** button on your Auvik dashboard to see available plan options and get your subscription started.

The rest of this guide focuses on deploying your first network and helping you get up to speed as quickly as possible.



# GETTING STARTED

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

<b>Global view</b>	The central area for managing your Auvik account. After you sign up, you'll automatically be logged directly into your global view.
<b>Site</b>	The location of the network you're managing.
<b>Site-level dashboard</b>	The area for monitoring and managing the network for a specific site. It's set up this way to make it easy for you to add and manage multiple sites.
<b>Multi-site</b>	A special kind of site for advanced deployments.
<b>Collector</b>	A lightweight application that uses a number of protocols to gather information about a network, such as topology details, configurations, and network statistics. The collector summarizes and sends that information to the Auvik servers over an encrypted connection.

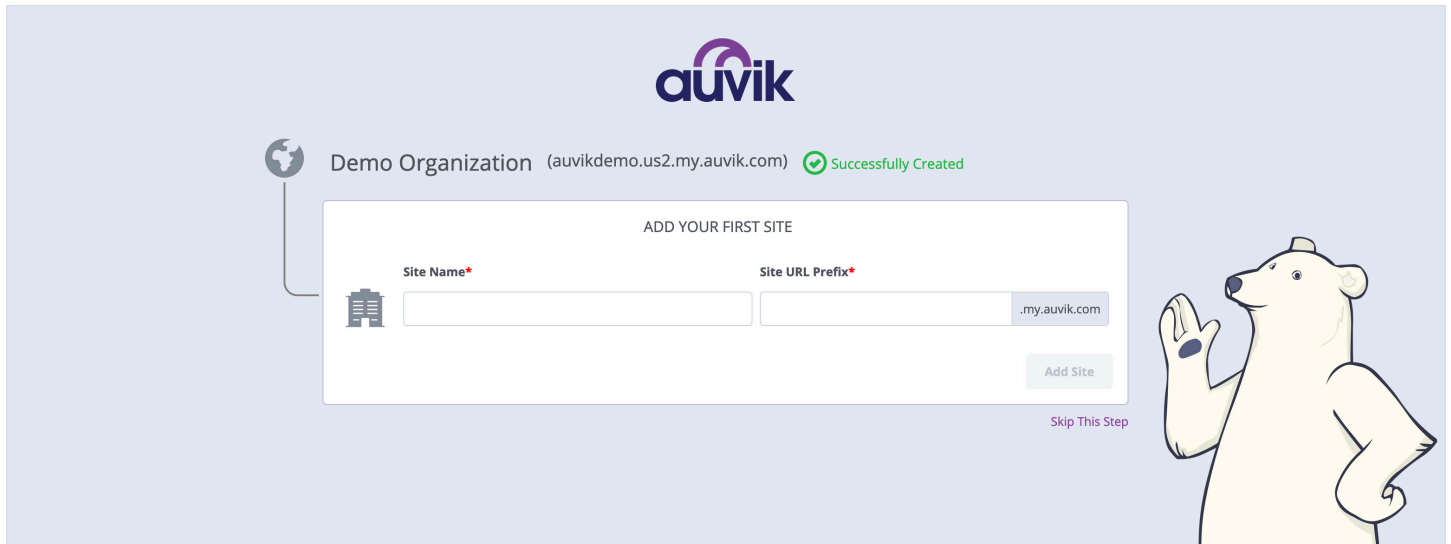
---

## NOW WE'RE GOING TO:

- Add your first site to Auvik (p. 4)
- Launch the collector setup (p. 5)
- Install Auvik (p. 6)
- Work through some tips for smooth discovery (p. 13)

# ADD YOUR FIRST AUVIK SITE

For your first Auvik site, you'll see the First Site Setup wizard.



- Enter a site name that corresponds with one location that you'll deploy Auvik to.
- Pick a site URL prefix with at least four characters. Only letters and numbers are allowed—no special characters.
- Click **Add Site**.

If this isn't your first Auvik site, then follow these steps from your global view:

- Click **Add Site** (blue button on the All Sites page) to create a site.
- Pick a domain prefix (URL) that has at least four characters. Only letters and numbers are allowed—no special characters.
- Select *Site* as the type. Don't select *Multi-site* for your first installation. This is an advanced option you can revisit later.
- 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.

# LAUNCH THE COLLECTOR SETUP WIZARD

Once you've added a new site, Auvik will automatically redirect you to the deployment wizard, as you're now ready to install your first collector.

You'll see a few options for downloading your Auvik collector but **we highly recommend using the Windows service as your primary installer method**, as it's the fastest and easiest way to get Auvik running.

If you can't or don't want to use the Windows service to deploy Auvik, you have other deployment options to choose from, as outlined on page 8.



# DEPLOY AUVIK USING THE WINDOWS SERVICE

(recommended)

## WHAT IS IT?

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

## DEPLOYMENT PROCESS

Click **Install Windows service** on the deployment wizard screen to see the detailed instructions for installing Auvik with the Windows service.

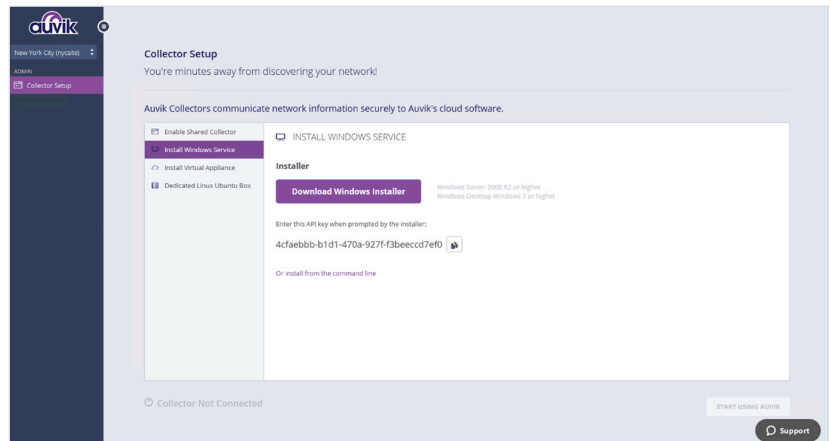
Here's how to install the Auvik collector:

1. Click **Download Windows Installer** to download the AuvikInstaller.exe file.
2. Click **Save File** to finish the installer download.
3. Open your downloads folder from your browser, or navigate to your downloads folder. This is usually something like **C:\Users\\Downloads**.
4. Double-click on the Auvik installer file.
5. You may see a prompt asking to allow the Auvik installer to make changes to the device. Click **Yes**.
6. Depending on your Windows Defender Firewall settings (or your third-party Windows firewall), you may see a prompt requesting to allow the Auvik installer access to private and public networks. Select both, and click **Allow access**.
7. Enter your email address—the same one you used to sign up for your Auvik account.

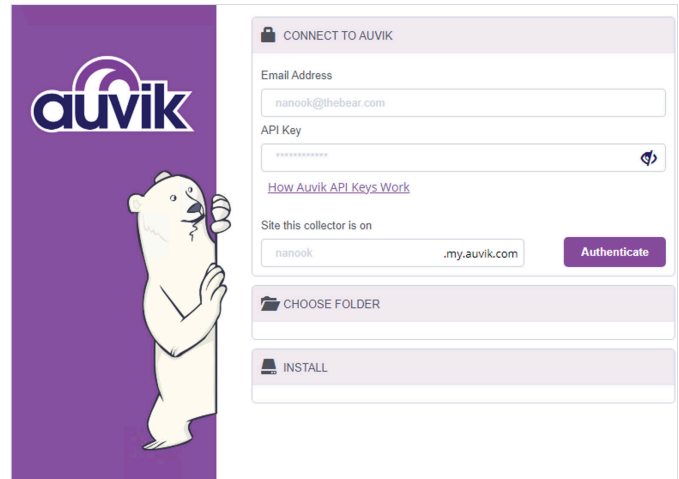


### TIPS!

- Don't install on an overloaded machine.
- The Windows service uses ports 21, 69, 514, and 2055, among others. It's best to install the service on a device that isn't running another program that relies on these ports. The Auvik installer will warn you if a potential conflict is detected.



8. Enter the API key that's displayed on the collector setup wizard by clicking the **Copy** icon in the collector setup wizard and pasting the key into the Auvik installer.
9. Enter the site URL prefix you selected in the first site setup wizard. You can validate this site prefix by reviewing the URL.



```
https://<siteURLPrefix>.us1.my.auvik.com/
```

10. Click **Authenticate**.
11. Click **Confirm** to use the default installation folder of **C:\Auvik**. Alternatively, you can select a different folder through the drop-down, then click **Confirm**.

That's it! Now go back to the dashboard for this site in Auvik. Once the collector is connected, you'll be automatically redirected to your Auvik site-level dashboard.

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.

If you get stuck, click the **Support** icon in the bottom right of your screen. Our team will be happy to help you get the collector installed.

## FOR MORE INFORMATION

- Windows installer: [Installing the Windows collector using the Windows installer](#)

# DEPLOY AUVIK USING AN ADVANCED DEPLOYMENT METHOD

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.

## WINDOWS COMMAND LINE INSTALLER

The Windows command line installer is a simple Windows service that enables you to install the collector from the command line, rather than the Auvik installer.

Detailed instructions: [How to install the Auvik collector using the Windows command line](#)

## 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, but note that Auvik requires an x86-based processor. Sorry, no ARM-based devices like Raspberry Pi.

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](#)



## SHARED COLLECTOR

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

You can also use a shared collector to get optimal performance when managing a large site (more than 1,000 users). It's best to segment based on physical or logical attributes, like separate buildings at your campus or parts of the network that don't share physical network infrastructure.

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 different 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 about 15 minutes to fully discover a network but it does depend on the size of the network.

While discovery is happening, consider doing these two things:

## 1. Adding more users

You may want to add more users to Auvik and give them access to your dashboard.

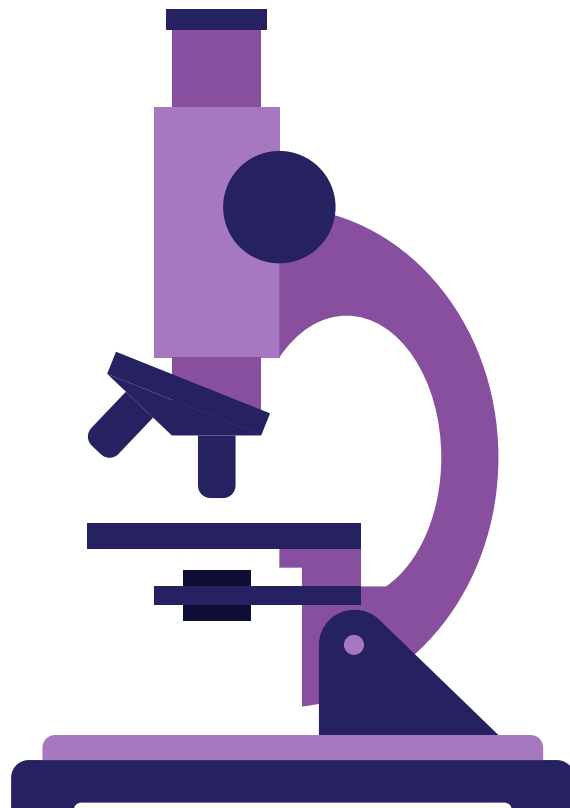
- In the side navigation bar, click Manage Users. Invite any new users and set permission levels for their access to your Auvik dashboard.

See [How do I manage invitations for new users?](#) in the Auvik Knowledge Base for details.



### POWER POINT!

With such quick turnaround, you can start network discovery at the beginning of a network assessment and have some actionable data within 30 minutes.



## 2. Add network device credentials

If you have SNMP credentials, login credentials, or VMware credentials for devices on your network, you may want to add those in now.

- In the side navigation bar, click **Manage Credentials**, then **SNMP Credentials** or **Login Credentials**.
- Click **Add SNMP Credentials**, or **Add Login Credentials** to continue adding them.



### 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.

- 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.

In the end, we want a network diagram of predominantly blue wires (showing Layer 1 to 3 connectivity) rather than a diagram of all black wires (showing Layer 3 only).

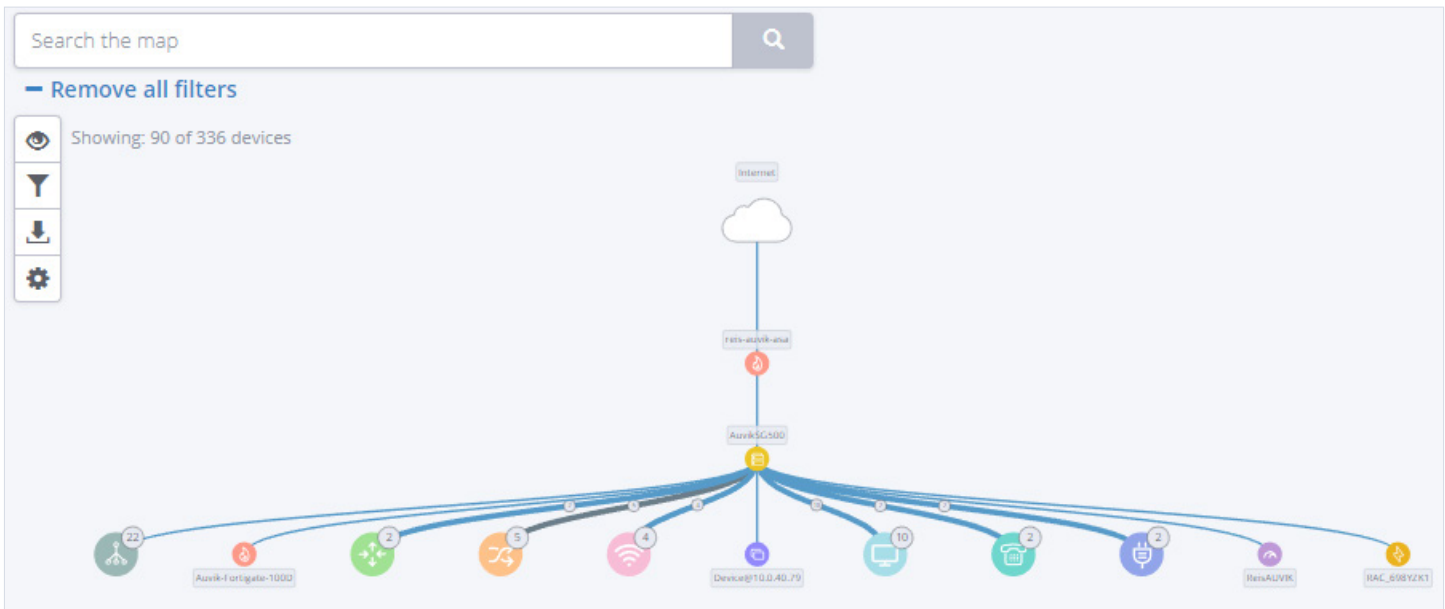
26 ROUTED NETWORKS								
Search Routed Networks			EDIT	DELETE	SCAN	DON'T SCAN	ADD NETWORK	
<input type="checkbox"/>	Network Name	Subnet	# of Devices	Scope	Scan Status	Assigned Auvik Collector	Auvik Collector Selection	Excluded IP Address Range(s)
<input type="checkbox"/>	192.168.0.0/24	192.168.0.0/24	1	Private	Awaiting Approval		Automatic	No Exclusions



### POWER POINT!

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

## 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 labelled.

## 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.

## LOOK FOR DISCOVERY TIPS

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. [MANAGE CREDENTIALS](#) [DISMISS](#)

As discovery progresses you'll see blue banners 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.



### TIP!

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

# TIPS FOR A SMOOTH AUVIK DISCOVERY

While Auvik is discovering your site's network, you'll want to start from the outside in. Start with the firewall, then switch infrastructure, followed by the access points, and finally endpoints, such as servers. As you're configuring devices, 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 automated configuration backups.

Auvik supports SNMP v2c and v3. SNMPv3 is a slightly newer and more secure protocol, but is a little more complex to set up. If you're not familiar with SNMP, we recommend you start with SNMPv2c.

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 blue 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. 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 APs have SNMP enabled. Wireless connections are drawn as blue dashed lines between APs and devices.

## □ ENABLE NETFLOW OR sFLOW

Auvik TrafficInsights uses flow data to provide an overview of network traffic, and lets you see who's on the network, what they're doing, and where their traffic is going. TrafficInsights currently supports NetFlow v5 and v9, IPFIX, J-Flow, and sFlow.

You'll need to configure your network devices to send flow data to the Auvik collector. To find your collector's IP address, click Auvik Collectors from the side navigation bar. If you aren't sure how to enable flow data on a particular device, see [Device configuration for Auvik TrafficInsights](#) in Auvik's Knowledge Base.

## □ ENABLE SYSLOG

Auvik's syslog feature gives you more network context and allows you to get to the root cause of an issue faster by providing centralized access to device logs.

You'll need to configure your network devices to send syslog to the Auvik collector. To find your collector's IP address, click Auvik Collectors from the side navigation bar. If you aren't sure how to enable syslog on a particular device, see [Device configuration for Auvik syslog](#) in Auvik's Knowledge Base.

## □ 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.

SNMP Credentials

Have Credentials 13 > | Need Credentials 1 > | Trying Credentials 25 >

Retry All SNMP Credentials

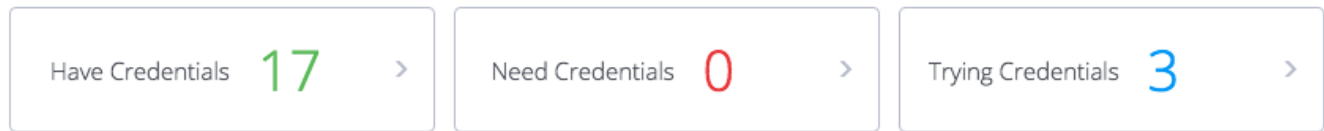
5 SNMP CREDENTIALS

Search SNMP Credentials [EDIT] [DELETE] [RESET] [ADD SNMP CREDENTIALS]

Description	Version	Devices Using These Credentials	Custom
<input type="checkbox"/> Auvik / Dell Switch (Updated)	1/2c	CN0FXP1R282981AD0008A02, CN0FXP1R282981AD0008A02	<input type="checkbox"/>
<input type="checkbox"/> auvik2801	1/2c	Cisco-2801.auvik.local	<input type="checkbox"/>
<input type="checkbox"/> Default Community string - private	1/2c	apcF28CDB, reis-auvik-asa	<input type="checkbox"/>
<input type="checkbox"/> Default Community string - public	1/2c	2961-CISCO, 3550Cisco, apcF28F8B, Auvik-Fortigate-100D, catalyst3750-12-1 [+]	<input type="checkbox"/>
<input type="checkbox"/> ManagedCare	1/2c		<input type="checkbox"/>

< ( 1 ) >

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.

## □ **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. While Auvik will use either SSH or Telnet, we do prefer SSH and will use that whenever possible. Only enable Telnet on older devices where SSH is not available.

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 running-config." 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.



### **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 (like a WatchGuard device that uses port 4118 for SSH), then you need to make some small tweaks.

Details here: [How do I manage discovery services?](#)

4. Auvik needs to be able to detect the service. The service status will show as a grey line instead of circle with a line through it if the device is ready.

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

## □ **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.



### **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.

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.

The screenshot shows a modal window titled "Edit Device" with a close button (X) in the top right corner. It contains three input fields: "Device Name" with the value "Device@10.0.40.151", "Type" with a dropdown menu showing "Hypervisor", and "Manage Status" with a dropdown menu showing "Managed". Each field has a left-pointing arrow icon. At the bottom, there are two buttons: "CANCEL" (grey) and "SAVE" (blue).



### **TIP!**

If you have Hyper-V, we talk to those hosts using WMI. Follow the instructions below 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 API CLOUD CONTROLLERS

Have devices that are managed via a cloud controller such as Meraki or Datto? You'll want to ensure that Auvik can talk to your cloud controller. Go to **Discovery > Manage Credentials > API Credentials** to set up the integration. Detailed instructions here: [How do I edit API credentials?](#)

## □ MANAGE NETWORKS

If there are multiple subnets at this site, Auvik has likely already found them. You can see the networks Auvik found under **Discovery > Manage Networks**. You'll see some of the networks are awaiting approval.

Auvik can scan networks of nearly any size, but we recommend sticking to smaller subnet ranges. If you see networks that are /16 or larger, we recommend breaking the network into smaller /24 ranges to scan—provided that only a portion of the subnet is in use. If you must scan a larger subnet, keep in mind that discovery will take a bit longer, and may result in a map that's a bit overwhelming.



### POWER POINT!

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

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.

Discovery [EXPORT] Last 10 minutes

MANAGE DEVICES MANAGE NETWORKS MANAGE CREDENTIALS DISCOVERY SETTINGS

We scan your networks to generate your logical and physical topologies, and to create your network inventory. To give Auvik access to a routed network, make sure it's checked in the list below.

6 ROUTED NETWORKS

Search Routed Networks [EDIT] [DELETE] [SCAN] [DON'T SCAN] [ADD NETWORK]

<input type="checkbox"/>	Network Name	# of Devices	Scope	Scan Status	Assigned Auvik Collector	Auvik Collector Selection	Excluded IP Address Range(s)
<input type="checkbox"/>	10.0.40.0/24	51	Private	Scan	10.0.40.253	Automatic	No Exclusions
<input type="checkbox"/>	10.0.100.0/24	1	Private	Awaiting Approval		Automatic	No Exclusions
<input type="checkbox"/>	192.168.168.0/24	1	Private	Awaiting Approval		Automatic	No Exclusions
<input type="checkbox"/>	192.168.122.0/24	1	Private	Awaiting Approval		Automatic	No Exclusions
<input type="checkbox"/>	192.168.101.0/24	1	Private	Awaiting Approval		Automatic	No Exclusions
<input type="checkbox"/>	10.0.20.0/24	1	Private	Awaiting Approval		Automatic	No Exclusions

« < 1 > »

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.

## □ 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. Revisit the [collector install steps](#) to configure Auvik to work with a proxy.

Users that have a proxy with 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](mailto:support@auvik.com).

## □ CHECK THE INTERNET CONNECTIONS DASHBOARD

Auvik discovers your internet connections automatically but if our discovery isn't yet complete, you can configure them manually. From the home dashboard, look at the Internet Connections widget to make sure the interfaces listed are in fact associated with your internet-facing WAN connections.

If not, you can edit a connection, delete one entirely, or add a new internet connection 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.

The screenshot shows the Auvik dashboard with the 'ALL INTERNET CONNECTIONS' widget highlighted by a red box. The dashboard includes sections for 'TOP DEVICE USAGE', 'TOP DEVICE UTILIZATION', and various alert counts (Emergency Alerts: 0, Critical Alerts: 0, Warning Alerts: 5, Informational Alerts: 5). The 'ALL INTERNET CONNECTIONS' widget has a search bar, 'EDIT' and 'DELETE' buttons, and an 'ADD CONNECTION' button. Below these are columns for 'Interface', 'Total Bandwidth', and 'High / Low Average'. The widget currently displays 'No data available.' and a pagination indicator showing '1'.

The 'Edit Device' form shows two input fields. The first field is labeled 'Device Name' and contains the text 'Device@10.0.40.151'. The second field is labeled 'Type' and has a dropdown menu with 'Hypervisor' selected. Both fields have back arrows on the right side.



### POWER POINT!

You'll always be the first to know the internet is down at a site. Auvik also helps you narrow down whether performance issues are ISP-related or internal.

## □ 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](#)

## □ 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.



### POWER POINT!

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

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.



# STILL HAVE QUESTIONS?

We're here for you!

**During your free 14 days:** Your Auvik account manager is your primary point of contact. You can email that person directly or send a note to [sales@auvik.com](mailto:sales@auvik.com) to reach the entire sales team.

**As a subscriber:** Your Auvik success manager is your primary point of contact. You can email that person directly or send a note to [success@auvik.com](mailto:success@auvik.com) to reach the entire success team.

And, the Auvik support team is always available to help with all things technical. You can reach them in many 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](mailto:support@auvik.com) to create a ticket.
- Call Auvik toll-free and hit 2 at the main prompt to connect to the support team.
  - 1-866-59-AUVIK (28845) in North America
  - +44 800 368 7578 in the UK
  - 1 800 934 221 in Australia

