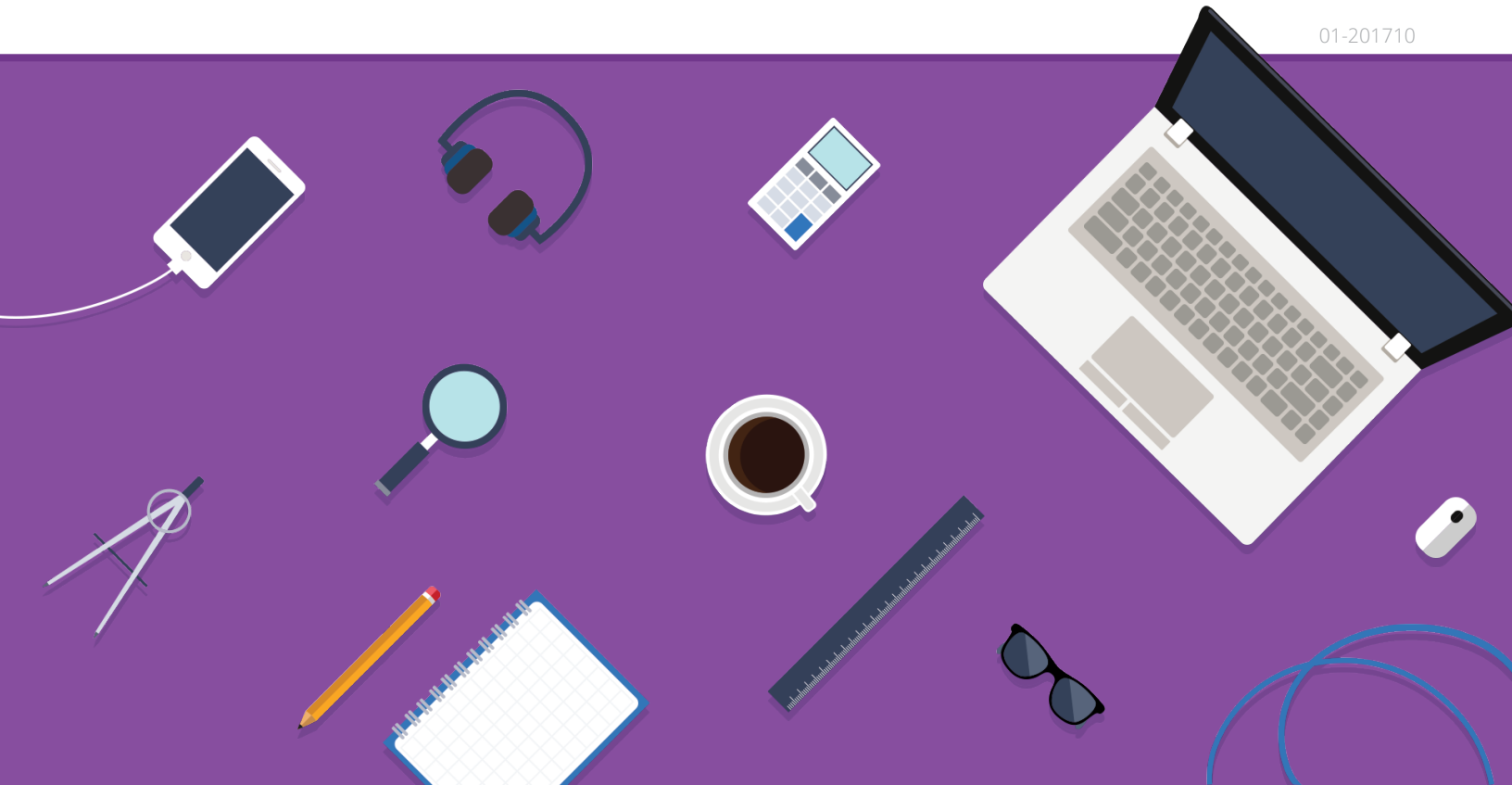
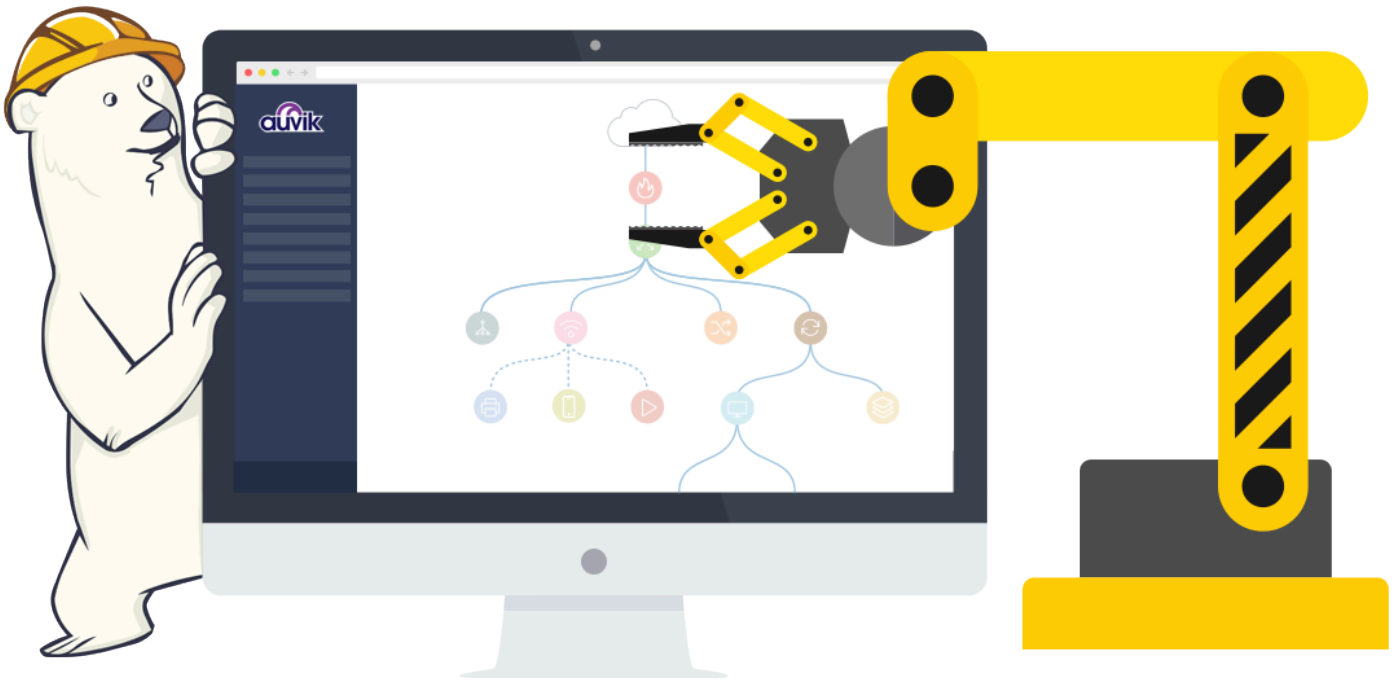
Auvik
Technical Review

01-201710



Contents



BASIC TECHNICAL REVIEW

UNDERSTANDING THE DISCOVERY PROCESS

Auvik's discovery process is a quick and easy way for MSPs and their clients to get a complete network topology map and manage all network infrastructure.

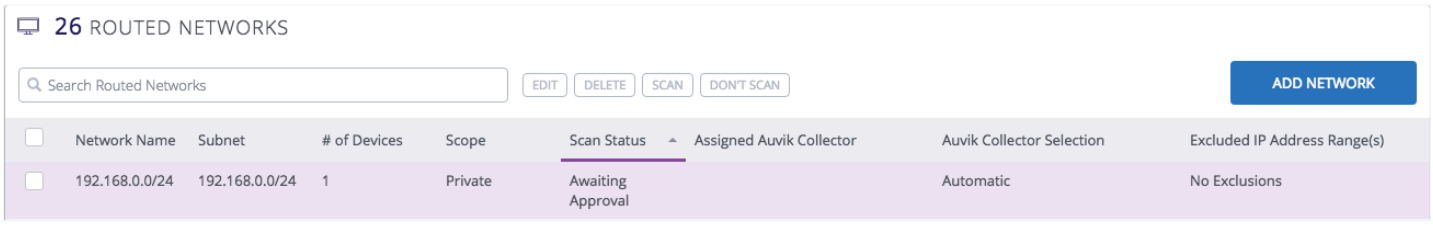
When you deploy Auvik out to a network, the initial discovery process begins. Discovery is not a one-time event but an ongoing process that continues to find new devices as they come online.

Auvik uses a number of discovery protocols to understand the network. At the core is a basic ping scan of the managed subnets.

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 starts 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.

- Do you see a /16 or a /8 network under `Discovery > Manage Networks`? 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.

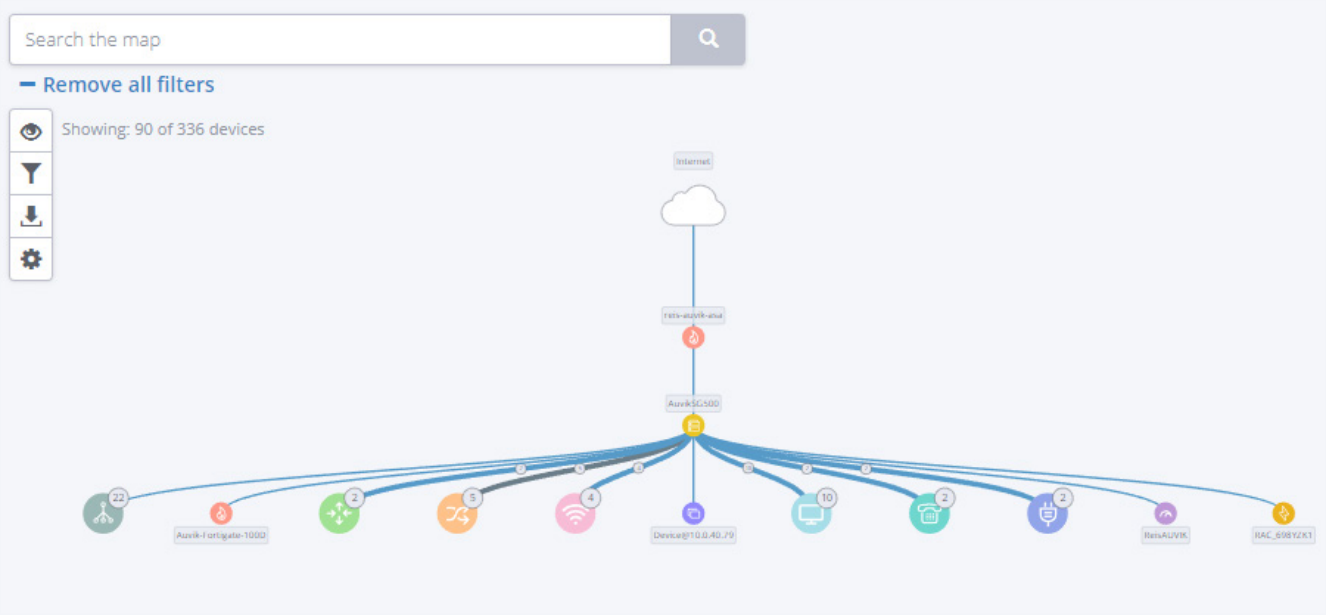


In addition to the ping scan that Auvik uses for basic asset discovery, Auvik also uses protocols such as:

- SNMP, SSH, and Telnet to dive deep into managed devices
- FTP and TFTP to back up and restore device configurations
- Discovery protocols such as multicast DNS (MDNS), Microsoft SMB, and UPnP to identify various endpoint devices

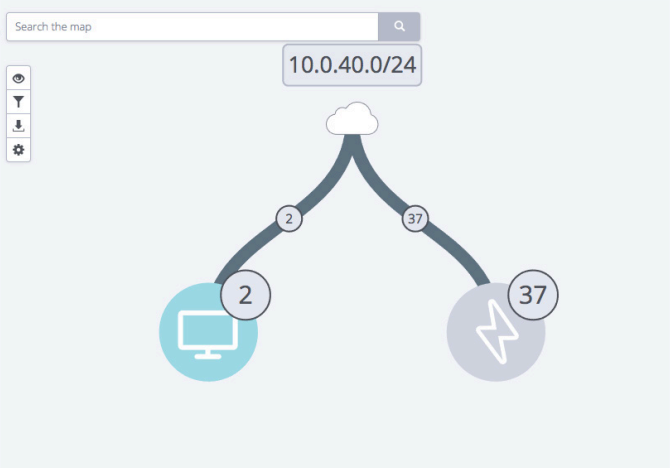
You'll find more detail on Auvik's discovery protocols here:
https://support.auvik.com/hc/en-us/articles/204304894

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).

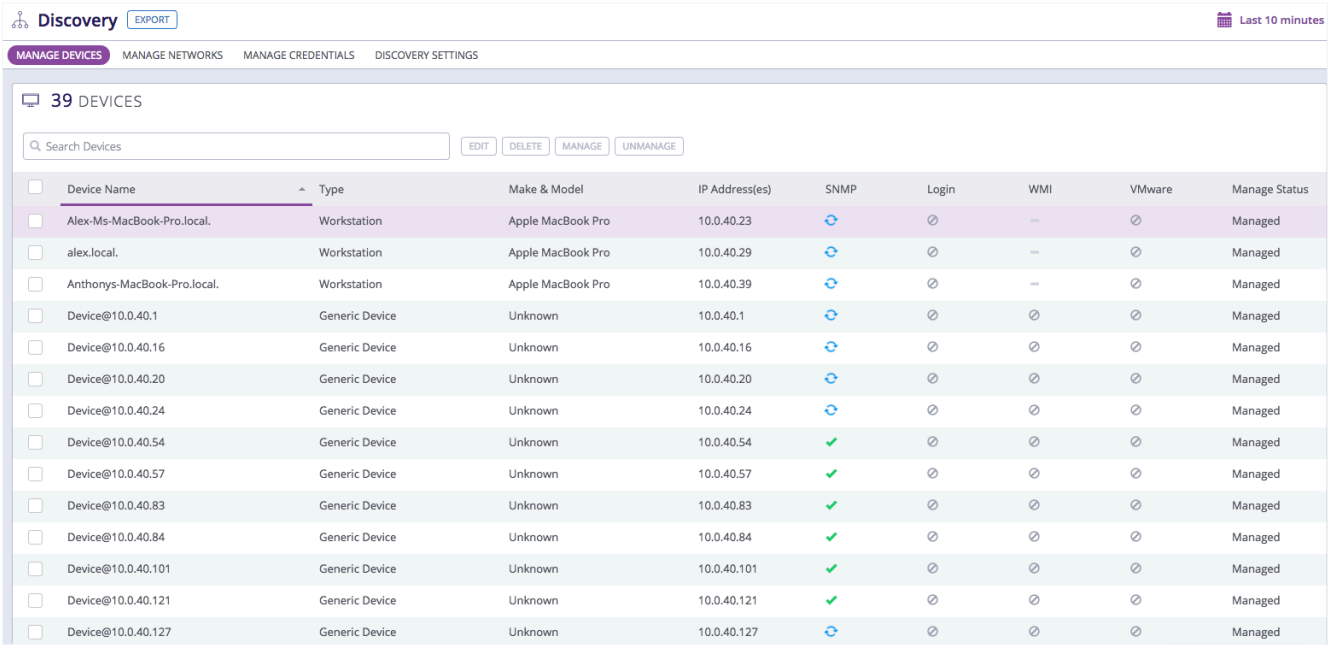


AUVIK COLLECTOR CONNECTS AND BEGINS INITIAL DISCOVERY.

As we start to discover that first subnet, you'll start to see devices appear on the map. At first, it will probably look something like the map below. 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.



Go to `Discover > Manage Devices.`



Device Name	Type	Make & Model	IP Address(es)	SNMP	Login	WMI	VMware	Manage Status
Alex-Ms-MacBook-Pro.local.	Workstation	Apple MacBook Pro	10.0.40.23					Managed
alex.local.	Workstation	Apple MacBook Pro	10.0.40.29					Managed
Anthonys-MacBook-Pro.local.	Workstation	Apple MacBook Pro	10.0.40.39					Managed
Device@10.0.40.1	Generic Device	Unknown	10.0.40.1					Managed
Device@10.0.40.16	Generic Device	Unknown	10.0.40.16					Managed
Device@10.0.40.20	Generic Device	Unknown	10.0.40.20					Managed
Device@10.0.40.24	Generic Device	Unknown	10.0.40.24					Managed
Device@10.0.40.54	Generic Device	Unknown	10.0.40.54					Managed
Device@10.0.40.57	Generic Device	Unknown	10.0.40.57					Managed
Device@10.0.40.83	Generic Device	Unknown	10.0.40.83					Managed
Device@10.0.40.84	Generic Device	Unknown	10.0.40.84					Managed
Device@10.0.40.101	Generic Device	Unknown	10.0.40.101					Managed
Device@10.0.40.121	Generic Device	Unknown	10.0.40.121					Managed
Device@10.0.40.127	Generic Device	Unknown	10.0.40.127					Managed

Consider the Manage Devices grid your tech review home page. This is where you'll refine Auvik's network discovery. The grid shows you where Auvik is trying discovery protocols such as SNMP, login credentials like SSH and Telnet, and WMI. You can quickly see where you need to invest some time in adding credentials.

What the symbols mean:

- **Blue spinner**: Auvik is currently trying that credential.
- **Yellow key**: The service is enabled but the credentials aren't working.
- **Yellow triangle with exclamation mark**: Auvik doesn't recognize the CLI, which means you'll probably need to contact our support team.
- **Green checkmark**: Yay! All is good.
- **Grey bar**: The service isn't running or Auvik can't access it.

USE THE BANNERS TO IDENTIFY REQUIRED CREDENTIALS.

If you're lucky, the default SNMP and login credentials just work. If not, that's OK. Auvik pops up blue banners across the top of your screen. The banners mean Auvik has found one or more devices that need credentials.

TIP!

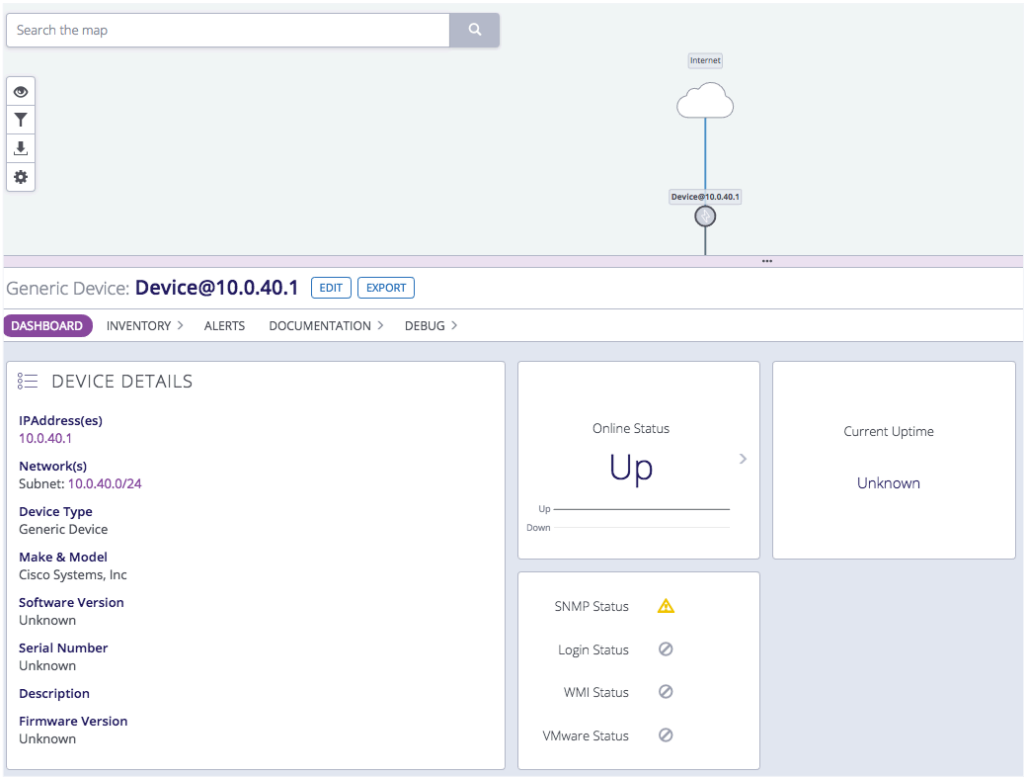
Don't try to manage everything right away. Focus on core devices first: firewalls, switches, routers, access points, and Wi-Fi controllers.

Add SNMP, login, and WMI credentials using the Manage Credentials button. As you add credentials, the map evolves. Sometimes it takes a few minutes for Auvik to process all the data after we get a green checkmark on a device. Give it a bit of time—say, 5 to 15 minutes.

Keep in mind these banners only show devices where we see a particular service enabled. For example, if SNMP isn't enabled on a switch, then we won't display a banner asking for SNMP credentials. You'll need to do a little more digging to find that switch.

FIND CLUES ON THE MAP ABOUT ABOUT WHERE CREDENTIALS ARE NEEDED.

Not seeing many discovery banners? Expecting more network devices but don't see SNMP anywhere? The map may present clues. For example, Auvik will anchor the device we identify as the default gateway at the top of the map if we get a "route" that points to that IP.



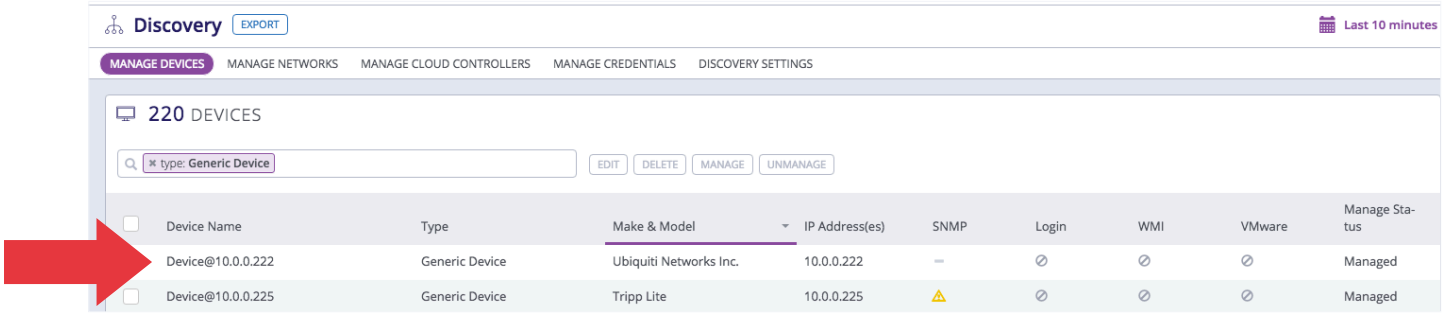
Next, you'll have to look for other devices that might be network devices. Remember that Manage Devices grid? Use that to help with the search.

Look for some of the following IPs:

1. Devices at .1 or .254 are often routers, firewalls, or switches.
2. Other network devices tend to hold special IPs as well, sometimes in the lower range (.2 to .10) or higher range (.250 to .253).

There are other clues within the Manage Devices grid as well. Using the search bar in the top left of the Manage Devices window, search for Device Type: Generic Devices.

Now that you're seeing only generic devices, look at the vendor column. You'll likely see lots of unknown devices but there may be clues. Look for common network vendors like Cisco, Netgear, Ubiquiti, and Meraki. You'll likely see a grey dash beside those devices—enable SNMP on those.



TIP!

Refer to the Auvik Knowledge Base if you need to enable SNMP and you're not sure how.

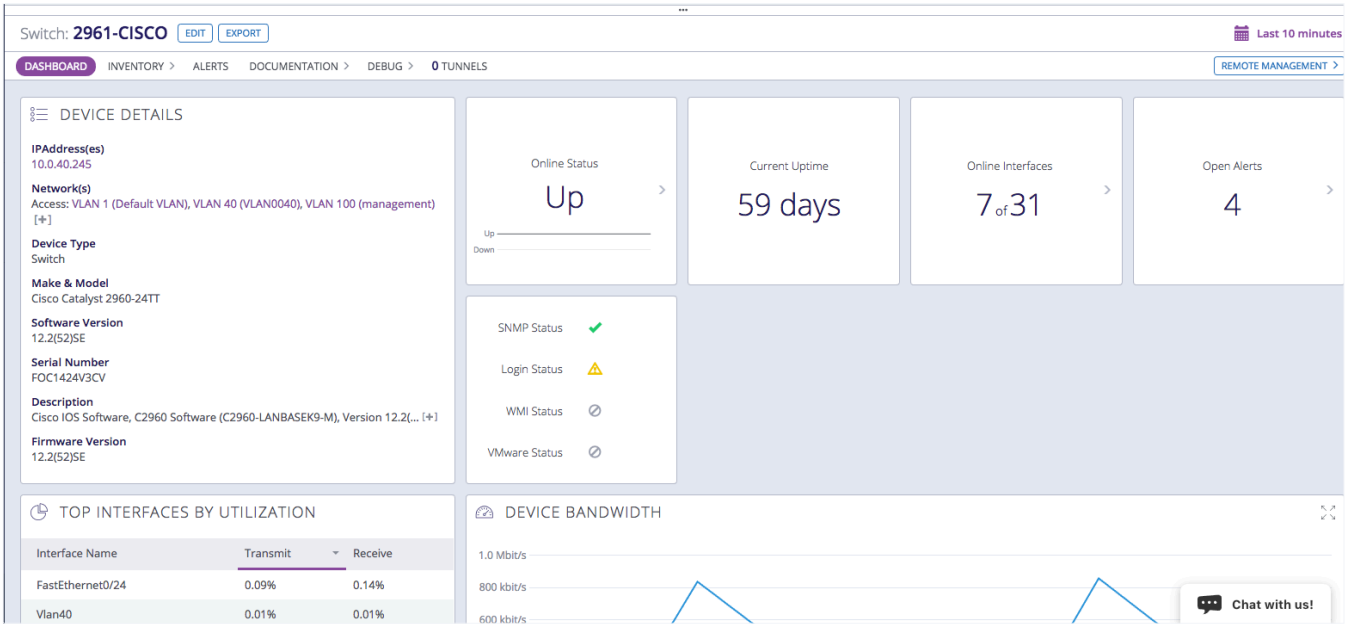
If you're not sure whether a device is a network device or not, go to the device's dashboard by clicking on the device name. Once on the device dashboard, you'll see a Remote Management button in the top right. Hover over it. If you see Remote Terminal or Remote Browser available, click on it. The device's terminal or browser will often give away what it is.

You can also use that remote terminal and remote browser to log into the network device and enable SNMP.

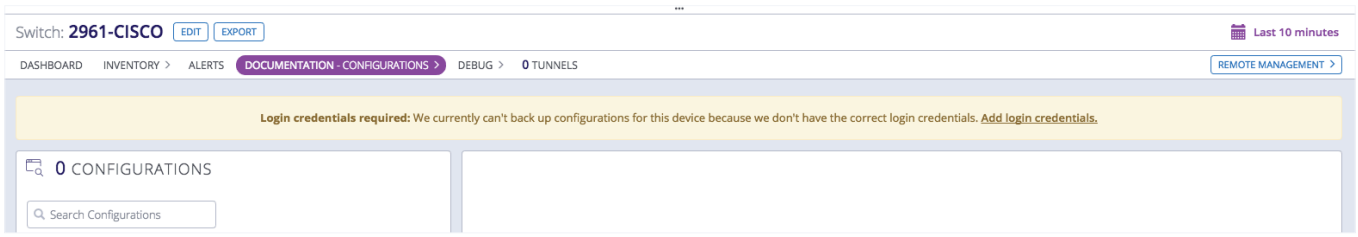
Remember, as you enable SNMP on network devices, make sure you add the device credentials to Auvik.

MAKE SURE LOGIN CREDENTIALS ARE ADDED.

If SNMP is enabled but login credentials haven't been added, you'll have lots of data being displayed and plenty of detail on your device dashboard.



But you won't be able to use a couple of key features, such as configuration backups. Add in those login credentials.



If credentials were added but they don't work, go to **`Discovery > Troubleshooting`** on the Device Profile page. On the Troubleshooting grid, you'll see every step Auvik works through to try the credentials, with links to related Knowledge Base articles. If you're still having trouble, reach out to support@auvik.com.

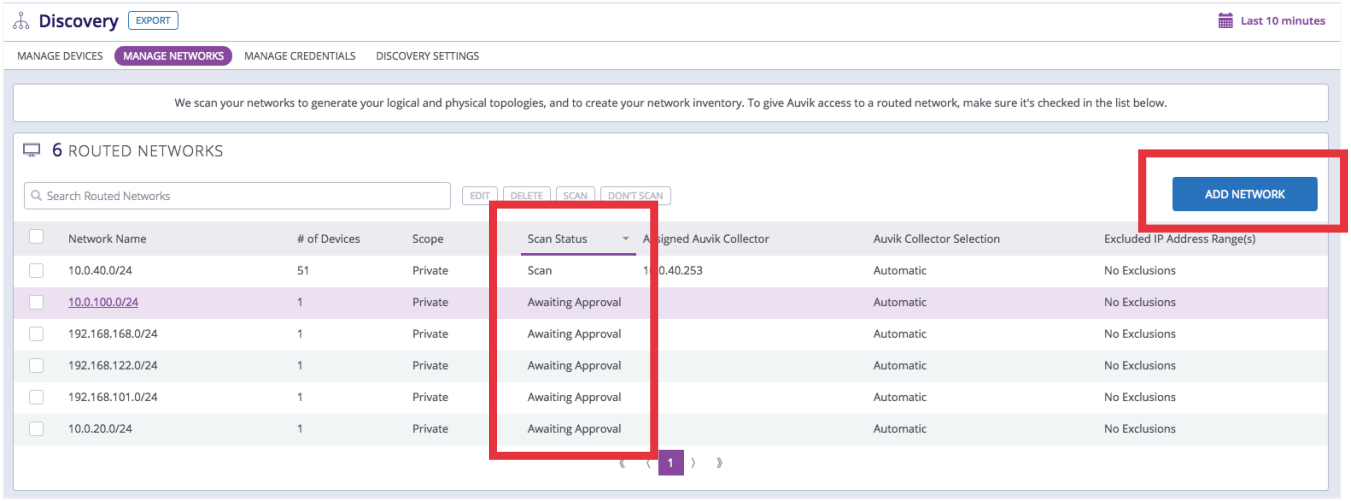
TIP!

Before diving too deep into troubleshooting login credentials, make sure SNMP on that device has a green check mark.

APPROVE ADDITIONAL SUBNETS.

Are there more internal subnets? By default, Auvik scans only the first subnet. The rest require your action.

Check the `Discovery > Manage Networks` grid. If you've added SNMP credentials, we've likely already found more subnets. Select the networks you want to discover, click **Scan**, and Auvik continues the iterative discovery process.



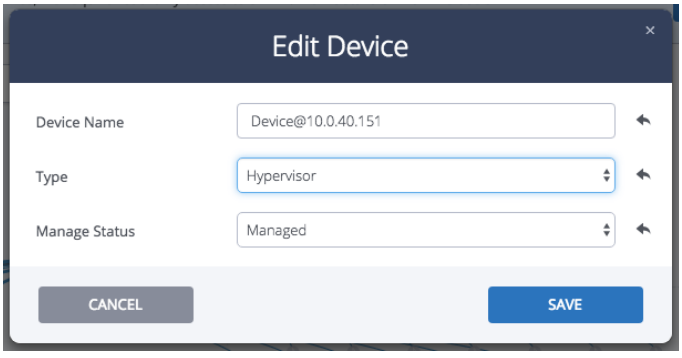
If you know of a subnet that's missing, or if there are no subnets listed, you can manually add networks to be scanned by clicking the blue **Add Network** button.

Shared collectors don't scan any subnets by default. You need to manually add the first subnet to scan using the **Add Network** button. Public subnets are also not scanned by default and won't show up. So if you're using a non-RFC-1918 subnet you'll need to manually add it.

MANAGE DISCOVERY OF VMWARE HYPERVISORS.

If you're lucky, SNMP is enabled on the hypervisors and they're already correctly classified. Most often, SNMP isn't enabled so your hypervisors will still be showing as generic devices.

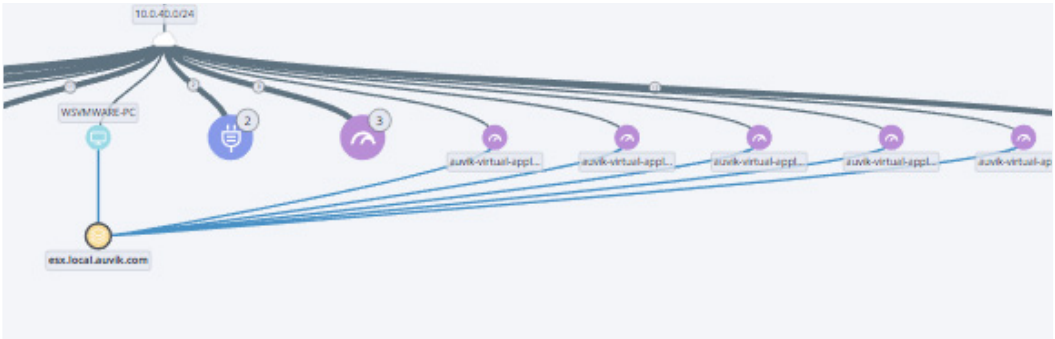
Don't worry. Rather than enabling SNMP on the VMware host, you can simply change the device type. (You'll find instructions on how to change the device type here.) As soon as that's done, Auvik starts trying the VMware API and prompts you for credentials.



Keep in mind that to query the API, Auvik requires the device's root credentials.

KEEP GOING WITH DEVICES AND CREDENTIALS.

When you start getting good data from your network devices, the black wires on your network map turn to blue. Be patient: The map does get messier before it gets better.



Discovery is not a one-time thing. Continue to refine the map and refine discovery by finding more devices and adding more credentials. The more Auvik has to work with, the better your map will be.

MOVE ON TO ADVANCED TROUBLESHOOTING IF NEEDED.

So far, Auvik has collected a lot of data and mapped out a good portion of the network. Plus we've started monitoring the performance of network devices, initiated configuration backups, and turned on alerting.

If the map still doesn't look great, though, move onto the section on advanced troubleshooting. You might also want to open up a support ticket for help with missing pieces.

ADVANCED TROUBLESHOOTING

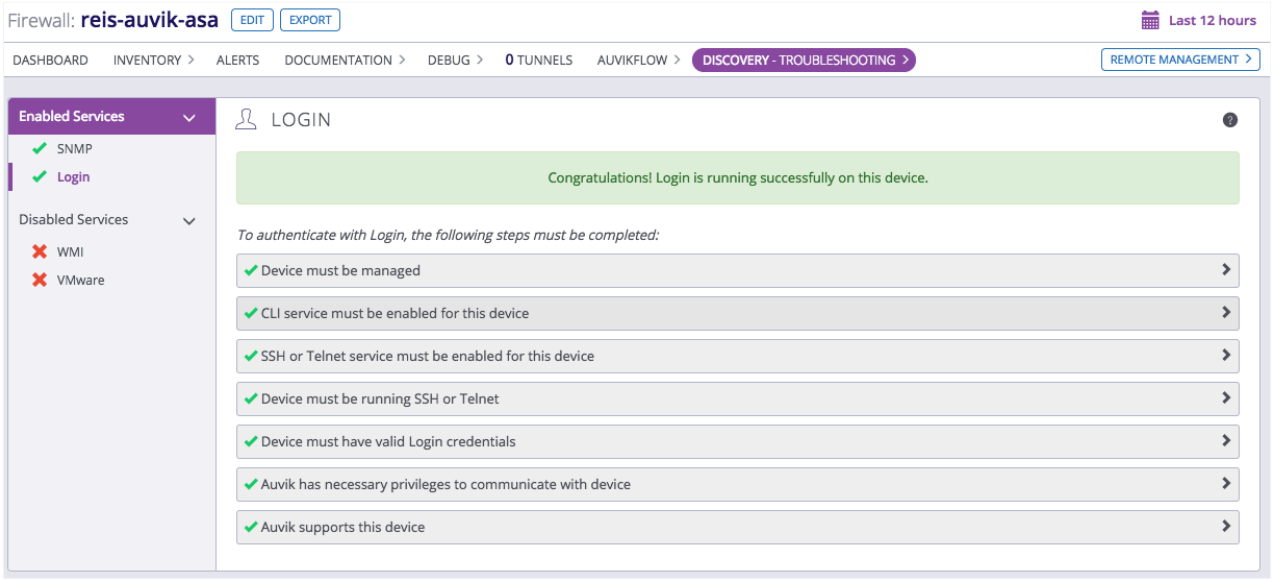
CLEAN UP DISCOVERY BANNERS.

This section assumes all login credentials and SNMP credentials have been added in the basic troubleshooting steps. Make sure you've dealt with all of the blue discovery banners that popped up.

DEBUG ADVANCED CREDENTIALS.

You've added credentials but Auvik still shows a yellow key, meaning the credentials aren't working. What next?

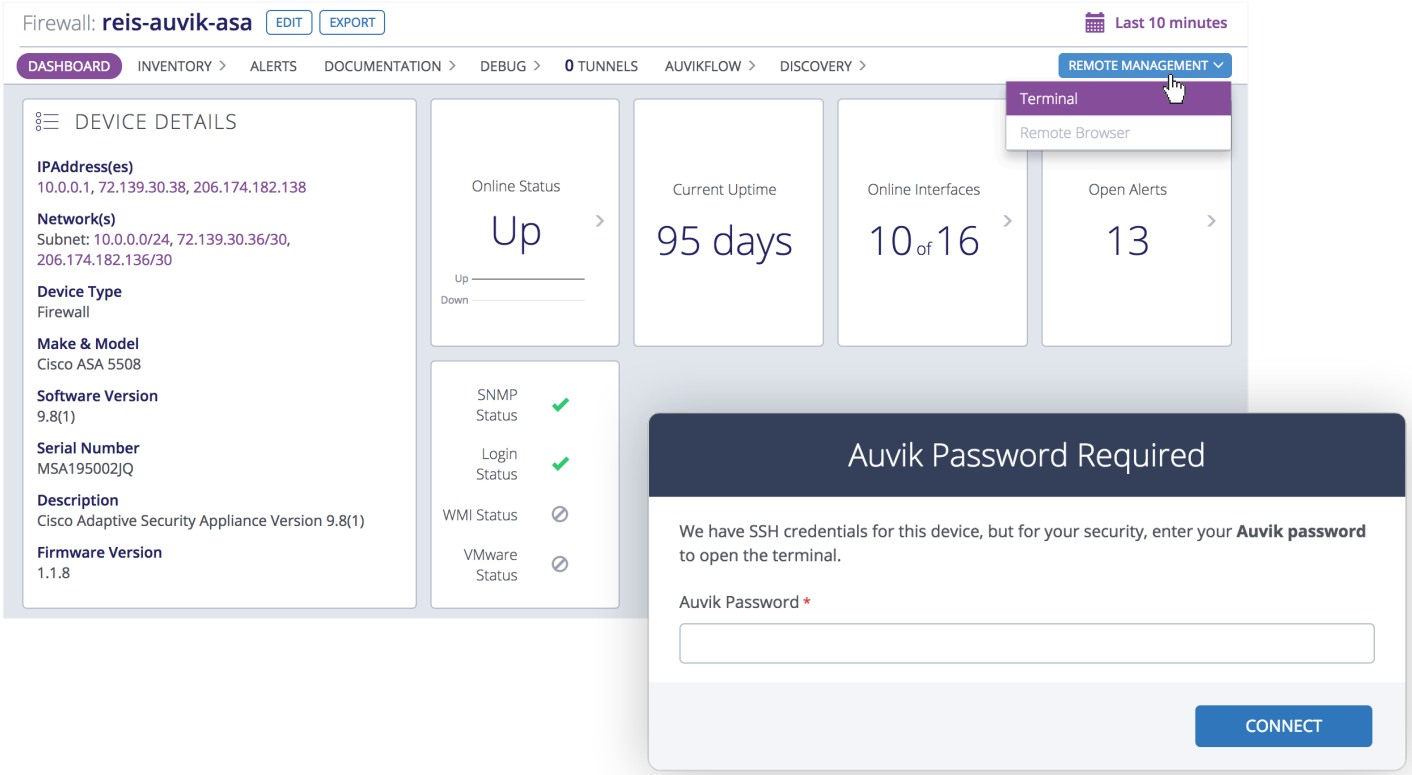
From the device dashboard, go to `Discovery > Troubleshooting` to see exactly where the credential is failing. Auvik gives you some tips and hints at each debug step.



You've added credentials *and* followed the steps in **`Discovery > Troubleshooting`** but you're still getting the yellow key. Now what?

Check to see if the credentials work to actually log into the device. Since the credentials are stored within Auvik, you can simply launch the terminal from under the Remote Management button and we'll attempt to use those to SSH or Telnet into the device.

If we prompt you for your Auvik password, SSH is working so the device credentials are good. If it prompts you instead for device credentials, then the credentials themselves are wrong.



If you've successfully logged into the device using the terminal, you can check the enable password you entered. Is it correct?

As a last resort, go to **`Discovery > Manage Credentials`**, delete the credential, and add it back in from scratch. (Don't edit it. Select Delete, then Add.)

If the credentials still don't work after trying all that, open a support ticket and include the device name and client URL.

FIND ADDITIONAL NETWORK ELEMENTS.

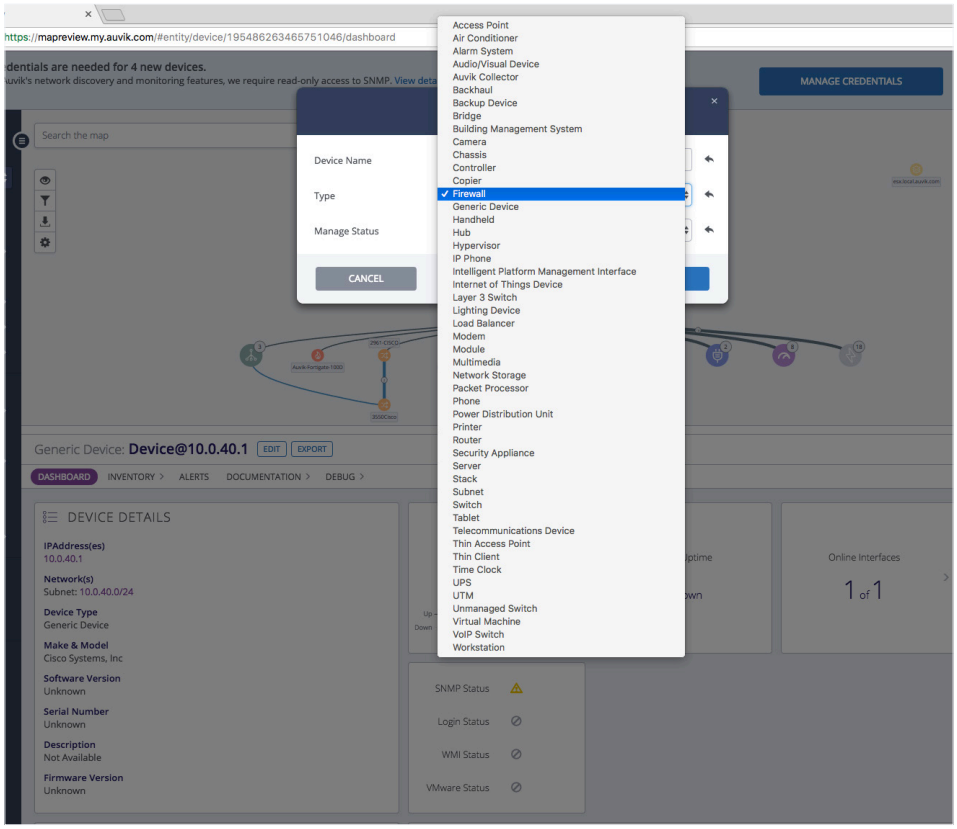
As discussed previously, firewalls, switches, and other devices may not have SNMP enabled. Use the **`Discovery > Manage Devices`** grid to look for common vendors still classified as generic devices.

If you've reviewed that devices grid and are still missing devices, you can look for devices that have a web interface available. Most network devices do have a web management interface, and if the device still has a generic device name (e.g., device@10.0.0.1) then it could be a network device.

Navigate to **`Inventory > All Services > HTTP or HTTPs service`**. All devices listed are those running a web service. You can pick a few devices and try the Remote Browser feature on them—the login screen may give away the device type. If you're able to log in, make sure you navigate to the SNMP settings and enable SNMP.

Unfortunately, there are devices out in the wild that don't support SNMP. In that case, try manually setting the device type to firewall, switch, or router. Auvik will automatically try Telnet or SSH.

You may see a little less information than with SNMP, but providing login credentials at least lets you use the remote management function. You may be able to back up the device configuration as well.



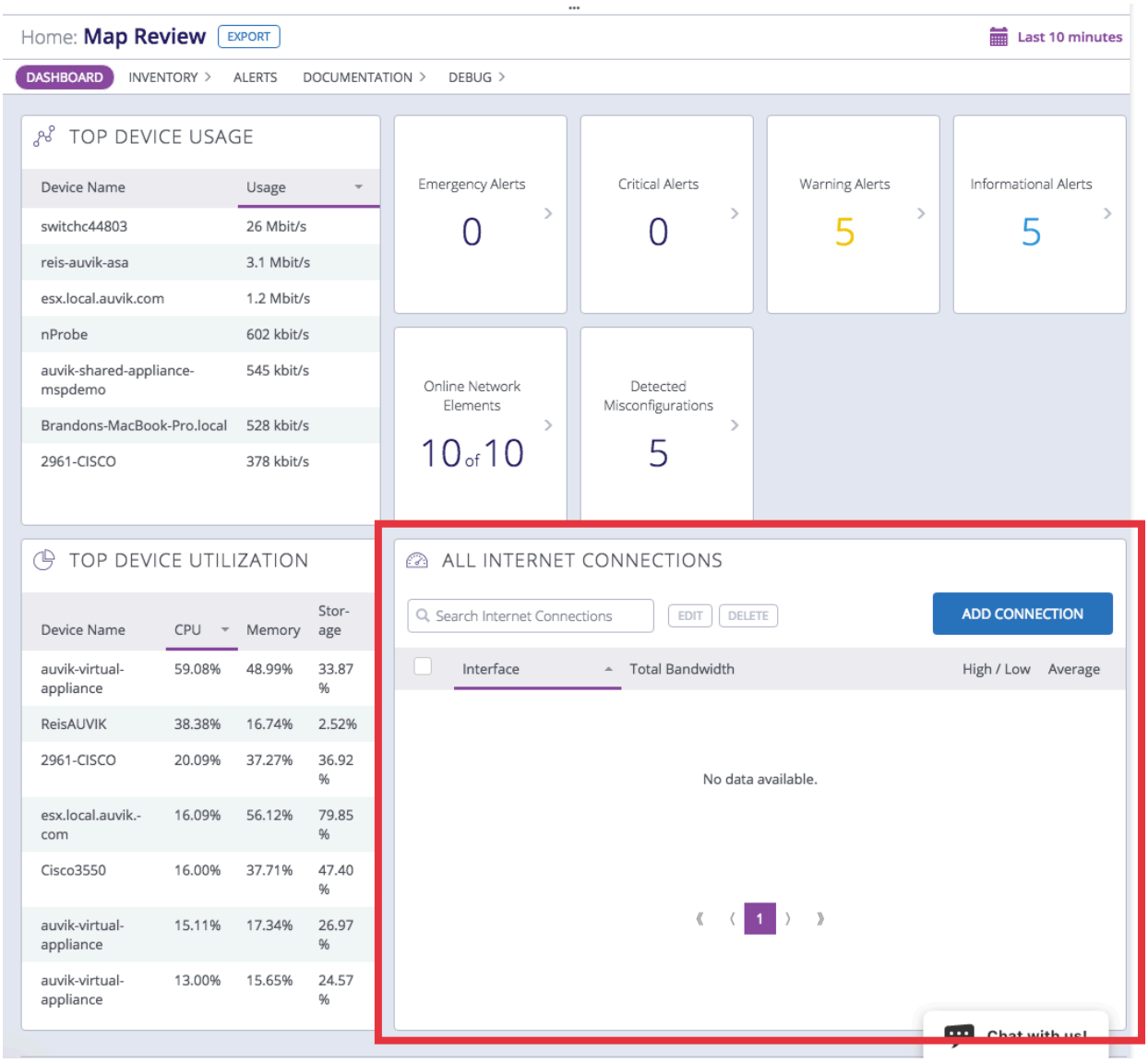
IDENTIFY POTENTIAL NETWORK ELEMENTS WITH THE TERMINAL.

If the remote browser feature isn't helping you track down network devices, check for other remote management options. If the terminal is available, try logging in using default credentials (such as admin/admin) or credentials you know. If successful, you can enable SNMP (or reset the community).

CLEAN UP THE INTERNET CLOUD.

There are a few common questions around the internet cloud: Why don't I see an internet cloud? Why are there devices connected to the internet cloud that shouldn't be?

If there's no internet cloud, go to the home dashboard and look under All Internet Connections. Is there anything listed there?



If yes, you'll want to make sure it's showing the correct outside interface. You can view the interface name to confirm (or click on the interface name to see more details). If it's not showing the correct outside interface, update it. Click **Edit** and select the right interface.

If no connections are showing, click **Add Connection** to add a new internet connection. Select the outside interface on the firewall or perimeter router. There may be more than one internet connection.

Despite our best efforts, sometimes devices report that they're connected to the public internet when they're actually not. In those cases, Auvik may make too many internet connections. To clean up the map, you can delete internet connections that have been wrongly discovered.

VERIFY INTERNET CONNECTION HEALTH.

Did you know that Auvik monitors the outside interface of the firewall for performance, and to ensure the internet connection stays alive?

To make the internet connection health check work, Auvik needs to ping the correct IP. Make sure the correct outside interface is configured and that Auvik has discovered the public IP address of that interface. Look under All Internet Connections for these details.

Also, the firewall needs to allow ICMP from public IPs. Auvik's ICMP comes from one specific IP in the cloud. See the Auvik Knowledge Base for tips on troubleshooting the internet connection health check.

TIP!

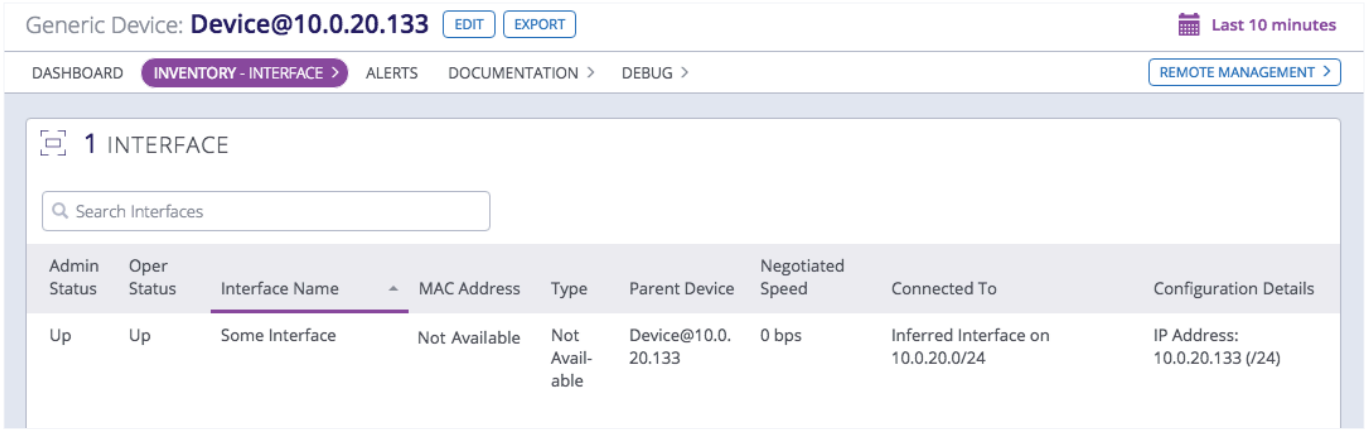
Not all devices provide a public IP address to Auvik. If you've set up the outside interface through All Internet Connections and still aren't seeing the internet connection health check as active, open a ticket with support.

WIRE IN THE FLOATING OR BLACK WIRE DEVICES.

By now your map is likely 90% complete. That's great! Remember the days when you had to trace wires and parse through the CLI to figure this out?

For that last 10%, there may still be a couple of devices "floating" on the map or black wires. We'll clean those up now.

If you select a generic device with a black wire, you'll probably find it has an interface with an IP address but no MAC address. We can't map the device without a MAC address. That means you need ARP table data, which usually comes from a firewall or a router, not a switch.



So you need to find the firewall or router and make sure both SNMP and login credentials have green check marks. If they don't have green check marks, go back to the section on credential debugging and work through the tips.

If they *do* have green check marks, go to the dashboard for the router or firewall. Select ARP/FDB from under the Debug menu. If there are no ARP entries, open a support ticket and include the device ID, client URL, and a screenshot of the device's dashboard showing the lack of ARP information.

If network devices do have green check marks and there are some entries in the ARP table, then we may be missing just *some* of the ARP entries. That means we're missing a few network elements. Head back to the section on finding additional network elements and work through those steps.

CAN'T FIND AN IP?

If you're expecting to see a device on the map but Auvik hasn't found it yet, there are a few things to consider:

Is Auvik scanning the subnet the device is on? Check to make sure the subnet is listed under the `Discovery > Manage Networks` page. Pay attention to the subnet mask.

Is there an ACL on the device or the path from the Auvik collector to the device we're not finding? One quick way to test this is to ping it from the server hosting the collector (for the Windows service) or from the virtual collector itself. If you can't ping the IP address you're expecting to find, then the collector is being blocked.

To find a device, Auvik needs ICMP to be enabled on the device. Double check the device to make sure it is.

Is there a host-level firewall on the Auvik collector, other than the default Windows firewall? Other host firewalls may block some of the Auvik service requests, since they operate on a per-application basis. Try disabling the host firewall. You can also test ping directly from the Auvik collector itself, following the debug directions in our Knowledge Base.

ENHANCE WORKSTATION MAP AND STATS.

Most often, Auvik maps all of the workstations to the correct switch or access point based on the evidence we've already collected from the network devices.

If you want more detail on the workstations, Auvik can collect some stats from Microsoft Windows workstations and servers using WMI. This may also help improve the mapping if there are still some grey wires.

Case 1: ALL of your Windows devices are on the same domain.

Verify that a manual WMI query against the machine works using the winrm identify command, found here. If the query doesn't work, configure a WinRM group policy.

Case 2: A domain doesn't exist.

You'll need to enable WMI manually on each device. With some scripting savvy, you may be able to script it through ConnectWise Automate or PowerShell.

For help troubleshooting WMI, see the Auvik Knowledge Base.

INTEGRATIONS

One key benefit of Auvik is how well we fit into your existing MSP tool stack. We currently integrate with the following systems:

- **PSA**: ConnectWise Manage, Autotask, Freshdesk
- **RMM**: Connectwise Automate, Continuum
- **Messaging**: Slack, Microsoft Teams

The most bang for your buck comes from the PSA integration so focus on enabling that one first. Integration with Connectwise Manage takes 10-15 minutes, for example—that's it! If you're using Autotask, it's just as quick. The links in the list above take you to detailed instructions for setting up each integration.

PSA INTEGRATION TIPS FOR CONNECTWISE MANAGE AND AUTOTASK:

- Make sure you're on the MSP dashboard. You won't see the integration on the client dashboard.
- When doing the client mapping for the first time, map only one client, then enable inventory sync for that client. That way, if there's any weirdness with the inventory sync, we can catch it quickly.
- Getting alerts flowing is a multi-step process:
  - Make sure you do a status mapping for each service board that alerts will be posted on.
  - Create a new notification channel for each service board that alerts will be posted on. Do this at the MSP level so the notification channels are available for all clients.
  - Set some alerts to use the notification channel. You can use Associate With Alerts from the notification channels page to quickly update multiple alerts.

RMM INTEGRATION TIPS:

- The integrations are generally done from the RMM tool, not Auvik.

For best results, make sure you're using the latest version of the Auvik plugin and the latest version of the RMM software.

MESSAGING INTEGRATION TIPS:

- Getting alerts flowing is a multi-step process. Once you've completed the initial integration:
  - Create a notification channel for that messaging app.
  - Associate alerts with the new notification channel.

VENDOR-SPECIFIC TROUBLESHOOTING

Aerohive

Aerohive access points come shipped with a public IP, so you'll see lots of them identified as internet connections. You can clean those up by editing All Internet Connections.

Cisco SG-Series switches

For the Cisco SG series line of switches, you'll notice that we don't log into those devices. Here's why. If you'd like to enable login for those devices to get configuration backups, open a support ticket and we can show you how.

HP 1900 series switches

The HP 1910, 1920, and 1950 series switches have a secret command line mode that Auvik uses to get full access to the devices. If you've walked through the device troubleshooting steps, you probably see that we're stuck without enough permissions. You can give Auvik the secret CLI-enable password to get the green check mark. Don't know what the secret password is? Try these ones.

Meraki

Meraki has two implementations of SNMP: a local implementation and a cloud-based implementation. Use the local implementation. You'll find it under `Network Wide > General`. Don't forget to enable the cloud controller integration as well.

Sophos Firewalls

Sophos firewalls, like most others, are based on a Linux kernel. Auvik discovers these devices as a generic device since they just don't give us enough information right off the bat. To enable configuration backups, follow the directions in our Knowledge Base.

SonicWALL

If you're not getting configuration backups or are having other issues with SonicWALLs, check the device's firmware version. Auvik works best with 5.9 and up. If you have 5.8.x or earlier, it's time to upgrade.

Watchguard

SSH on Watchguard uses a non-standard port—4118. Go to `Discovery > Discovery Services` to add port 4118 for SSH and CLI. If you use WatchGuard on multiple clients, make the change at the MSP dashboard to push the change across clients at once.

AH! I'VE READ THROUGH THIS WHOLE GUIDE AND AM STILL HAVING TROUBLE!

If you're still having trouble after all that, don't worry—we're here for you.

There are many support options:

- Use the chat box in the bottom right corner of the Auvik window.
- The Auvik Knowledge Base has a ton of articles to help with common issues. Click Knowledge Base in the bottom left corner of the toolbar in your Auvik window.
- To create a ticket, email support@auvik.com. Someone from the support team will get back to you shortly.
- Call support at 519-804-4700. Hit 2 at the main prompt.

Make sure you collect a couple of screenshots showing the errors or issues you're facing, and include information such as the client URL and the device name so we can help solve your issue quickly.