Cisco Meraki Fundamentals

Cloud-Managed Operations

ARUN PAUL
MIKE WOOLLEY
MEDI JAAFARI
JEFFRY HANDAL

ciscopress.com

Contents

Chapter 3

The Meraki Admin Experience

Over the years, the Meraki platform has expanded beyond just traditional networking and is getting closer to the utopia we all seek—a platform that can be used to manage all digital operations in one, single integration. This chapter explores the design intent and layout of the Meraki Dashboard to help you visualize your cloud-managed operations. This chapter also provides some insight into the ways that Meraki is working to enhance the administrative experience across the board. As you'll see, the Dashboard utilizes the power of Meraki's cloud-enabled platform to provide detailed summary and overview information to help administrators monitor and proactively address potential issues in their day-to-day workflow before those issues begin to cause larger impacts across the organization.

Note Refer to Chapter 2, "Building the Dashboard," for more information on how to set up your Meraki account, create a Dashboard organization, and perform initial setup actions such as creating administrators, assigning privileges, or claiming licenses and hardware.

The Organization Overview page, shown in Figure 3-1, is the first page displayed after logging in or selecting an organization to work within. You also can navigate to it directly from the navigation pane on the left by selecting **Organization > Overview**.

Once you are logged in to your Dashboard organization, you can verify the region where your current organization is hosted. View current session information by checking the footer of any page in the Dashboard, as shown in Figure 3-2.

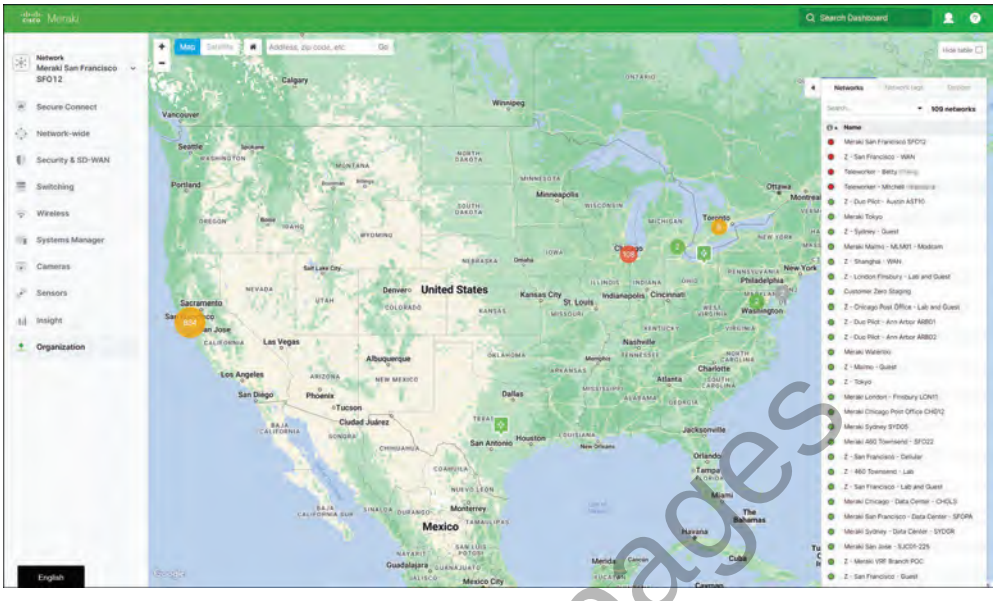

Figure 3-1 *The Organization Overview Page for the Cisco Meraki Organization Showing the Map Alongside the Network List in Collapsed Form*

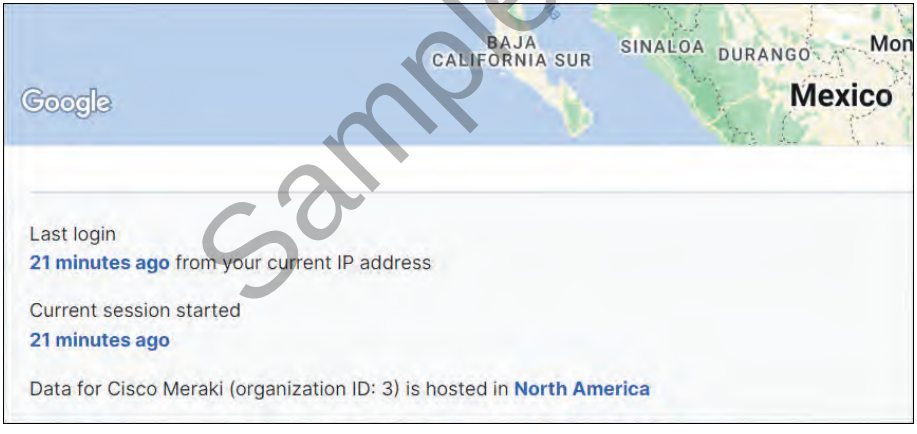

Figure 3-2 *The Current Session and Organization Hosting Details for an Example Organization*

Org-wide Health

The Organization Overview page in your Meraki Dashboard provides a high-level overview of each of the networks contained within the current organization. Its purpose is to elevate data to help you find the "needle in the haystack." You can expand the network list view by selecting the left-facing arrow at the top left of the network list on the

right of the page, and add additional columns to get more overview information, such as Firmware Status or Network Health, for each of the listed networks by clicking the **+** button in the top-right corner of the table and selecting the column or columns to add, as shown in Figure 3-3.

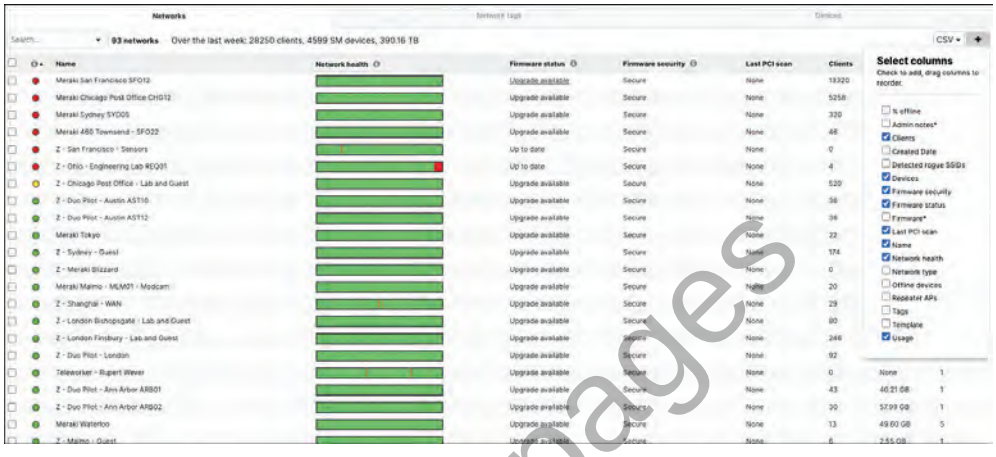

Figure 3-3 *The Organization Overview Page Showing the Expanded Network List for the Cisco Meraki Organization*

For example, to view firmware-related statuses for each network in the organization, click the **+** sign and select the **Firmware Security** and **Firmware Status** options to add the corresponding columns to the table.

Pro Tip Most tables in the Meraki Dashboard can display additional columns of related information.

Firmware Status

Meraki manages device firmware statuses on a per-network basis and will notify administrators when an optional firmware upgrade is available for a given network with the Upgrade Available status in the Firmware Status column, as shown in Figure 3-4. A status of Upgrade Scheduled indicates a firmware upgrade has actively been scheduled for the specified network.

The Firmware Security column reports whether any critical security patches are missing for specific devices in a given network outside the general firmware availability. If a status of Custom is displayed in the Firmware Status column, that indicates that a specific firmware has been statically configured to run on one or more devices in the network by Meraki Support, in which case you will need to engage Meraki Support to remove the static mapping before any additional changes can be made to the firmware for that network.

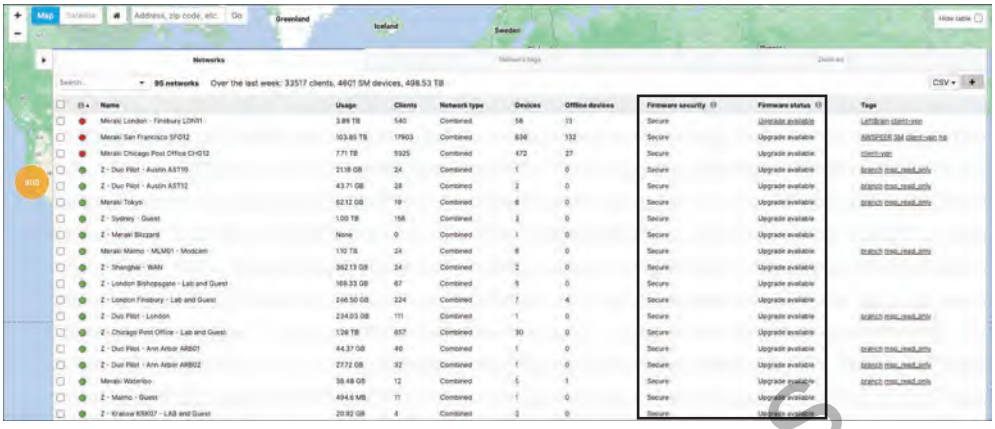

Figure 3-4 *The Organization Overview Page Showing the Current Firmware Security and Status of Each Network*

The Organization Overview page provides quick, organization-wide visibility and easily accessible notifications related to firmware security and current upgrade status for each network within the organization.

For more information on firmware updates and best practices, see the "Cisco Meraki Firmware FAQ" article at https://documentation.meraki.com.

Note The "Additional Reading" section at the end of this chapter provides the full URL for every article that is cross-referenced in this chapter. Alternatively, you can search for the article title at https://documentation.meraki.com to locate it.

Detailed Firmware Status and Security

You can find more detailed visibility regarding firmware security and status across the organization by navigating to **Organization > Firmware Upgrades** and clicking the **All Networks** tab, shown in Figure 3-5. This page provides a detailed overview of every network within the organization and its current firmware-related statuses.

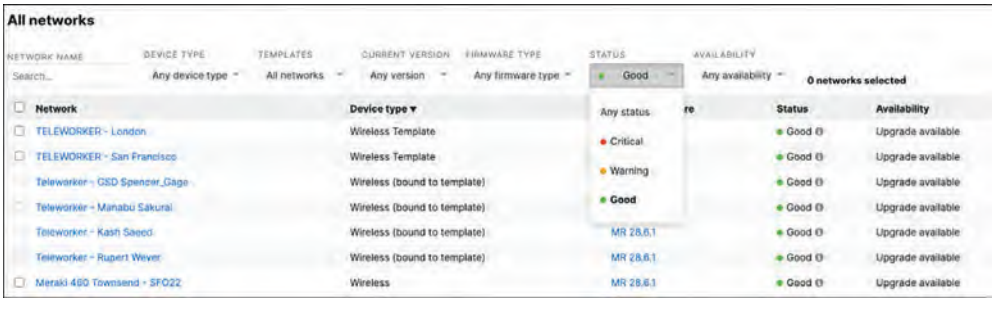

Figure 3-5 *The All Networks View of the Firmware Upgrades Page for the Cisco Meraki Organization*

As shown in Figure 3-5, you can open the **Status** drop-down menu to quickly highlight networks with their current firmware in Critical or Warning states, like in Figures 3-6 and 3-7, respectively. Networks have a Warning status when their currently running firmware has an end-of-support date set within the next 6 months, and networks have a Critical status when the running firmware is past the end-of-support date. This option is one way to quickly see what sites are potentially in a time-sensitive situation that needs quick attention.

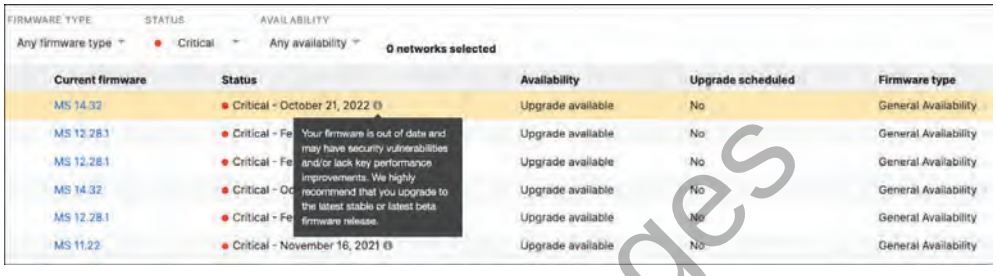

Figure 3-6 *Networks in the Cisco Meraki Organization That Have Critical-Level Firmware Alerts*

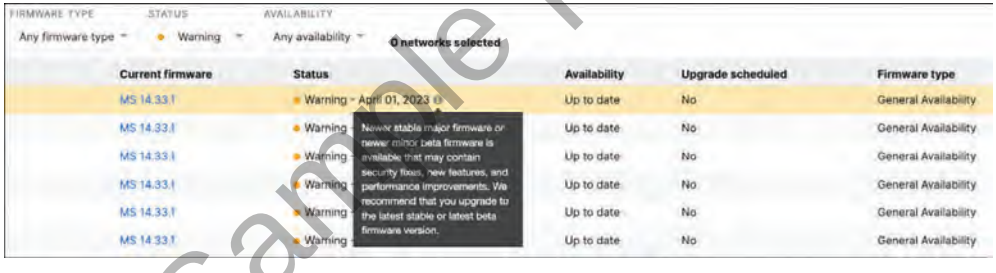

Figure 3-7 *Networks in the Cisco Meraki Organization That Have Warning-Level Firmware Alerts*

Getting to know the current status of all your networks and prioritizing sites that require security patches helps to ensure that your networks are up to date on security posture, compliance, and availability.

Proactive Replacements

Because Cisco Meraki strives for the highest-quality hardware and user experience possible, much of the Meraki hardware comes with a lifetime replacement warranty. However, no mass-manufacturing process is perfect, and sometimes a problematic component might not be discovered until long after the equipment has been manufactured and sold. In the unlikely event there is an unforeseen product defect that Meraki is unable to address before distributing the equipment to customers, the Meraki platform is capable of handling the complex task of tracking known hardware or product defects and

proactively alerting administrators who manage potentially affected devices so that they can replace those devices before they fail or cause a significant impact to operations. An excellent example of a defect that produced an industry-wide impact is the Intel clock component failures that occurred around 2018.

While Meraki will actively alert any customer who may be operating an affected device in which a defect is discovered, organization administrators can always check at any time to see if any devices in their organization are eligible for a proactive replacement program. To do so, open the **Help** menu at the top of any Dashboard page and click the **Hardware Replacements** link.

Pro Tip The proactive replacement program is different from the proactive RMA process available for devices that have failed outside of a known mass defect.

For more information regarding Meraki Return Materials Authorization (RMA) and end-of-life (EOL) policies, refer to the "Returns (RMAs), Warranties and End-of-Life Information" article at https://documentation.meraki.com.

Dashboard Early Access Program

Meraki is continuously working to enhance the design of the Dashboard to improve performance and usability for its customers. This effort includes developing new features and pages to improve the Dashboard experience. You can explore the latest features and pages opting in to the Dashboard Early Access program.

Pro Tip You can find detailed, up-to-date information about new features and firmware support for all Meraki products on Meraki's "Firmware Features" documentation page at https://documentation.meraki.com/Firmware_Features.

To opt in to specific Early Access Dashboard features, go to the **Organization > Early Access Program** page, shown in Figure 3-8, and use the toggle switches to enable or disable new features in the Dashboard, such as new pages, UI designs, or new features, before they are pushed to the wider Dashboard audience. To give you an idea of what types of enhancements are available through the Early Access Program, the following subsections briefly introduce a few of the currently available options (marked 1 through 4 in Figure 3-8) that are particularly relevant to the day-to-day administrator experience. Keep in mind that new features are always being developed, so this is just a snapshot of the future of the Meraki Dashboard at the time of writing.

Magnetic Design System

Use this toggle to enable the newest iteration of the Dashboard UI, known as Magnetic, which not only overhauls the visual appearance of the Dashboard while maintaining a

familiar layout but also enables the options for many more related features and pages within the new UI. This new design also acts as a building block of the new, next-generation unified Cisco UI design coming to modern Cisco dashboards.

Figure 3-8 *The Meraki Early Access Program Page, Allowing You to Opt In or Out of New Dashboard Features*

New Landing Page

Use this toggle to enable the Organization Summary page, shown in Figures 3-9 and 3-10, which provides an updated and clearer high-level overview of the health of devices across all the networks in your organization. You can view this page after enabling the feature by navigating to **Organization > Summary**.

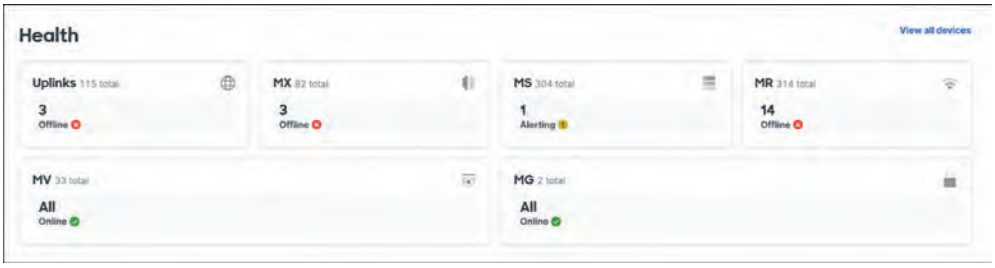

Figure 3-9 *The Health Section of the New Organization Summary Page Available in the New Landing Page*

Figure 3-10 *The Networks Section of the New Organization Summary Page for Networks Within the Cisco Meraki Organization*

The Networks section of this page reports a more detailed device health summary for each network, allowing you to quickly assess the status and health of each network across the organization more easily than ever before.

New Organization Alert Page & Alert Hub Enhancement

Use this toggle to enable the Organization Alerts page, shown in Figure 3-11, as well as the network-level Alert Hub. The Organization Alerts page provides a consolidated view of alerts for all platforms deployed across the organization. To access this page, navigate to **Organization > Alerts** from any Dashboard page.

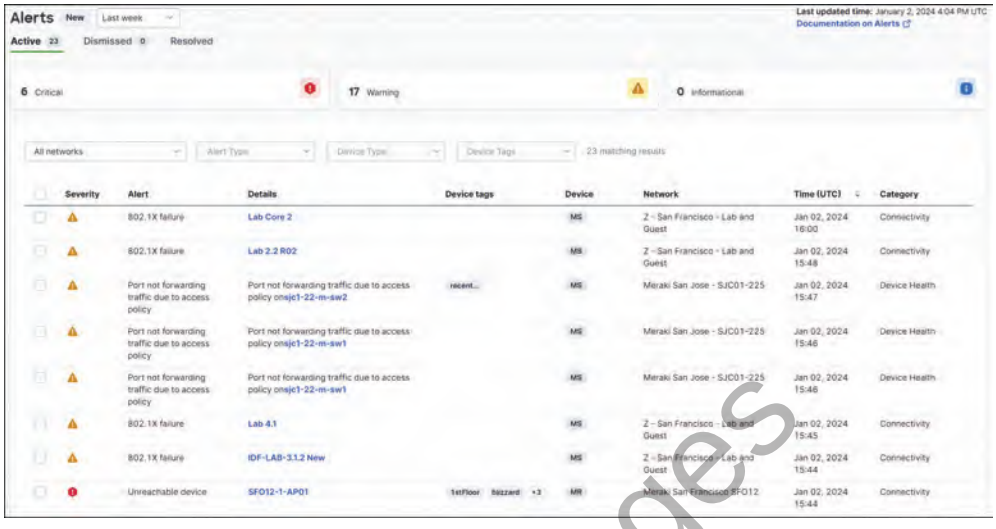

Figure 3-11 *The New Organization Alerts Page*

The Organization Alerts view provides an easy to check report of device statuses across all networks in an organization and can be filtered to narrow the displayed results based on severity, alert type, network, or device type. This provides an excellent top-down view of any alerts present across an organization regardless of organization size or deployment distribution, which results in a shorter time to identify issues, leading to a quicker time to resolution.

When working on any page within an individual network, the network-level Alert Hub notification icon appears in the upper-right corner of the window, as shown in Figure 3-12. This feature provides an easy to access view that consolidates all alerts for the current network into a single panel, as shown in Figure 3-13. These are the same alerts that you can view from the Organization Alerts page but filtered to show only alerts for the currently selected network. From this panel, you can quickly navigate to a problematic device or easily triage a series of alerts for a given network to make addressing the inevitable issue a less stress-inducing task.

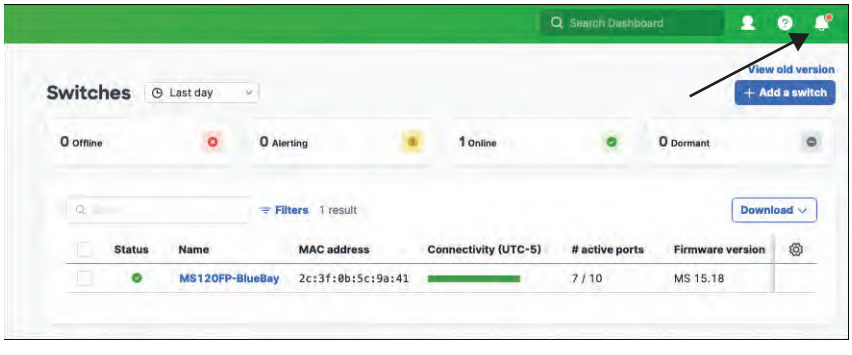

Figure 3-12 *The Alert Hub Notification Icon*

For more information on the new Organization Alerts page and Alert Hub, visit https://documentation.meraki.com and view the "Alerts" article.

Switching Overview

Use this toggle to access the new Switching Overview feature, which consolidates key performance indicators and provides crucial planning information related to switches in a given network. Details like port utilization, PoE budget, and more help Dashboard users to have clearer visibility when reviewing device provisioning and statuses, thereby assisting in planning for future network needs.

You can access the Switching Overview panel after enabling the feature by going to the **Network-wide > Clients** page of any network and selecting the **Switches** modal of the Health section, as demonstrated in Figure 3-14.

More information on the new Switching Overview feature is available at documentation.meraki.com in the "Switching Overview – MS Health" document.

Figure 3-13 *The Alert Hub Notification Panel for the Cisco Meraki San Francisco Campus Network*

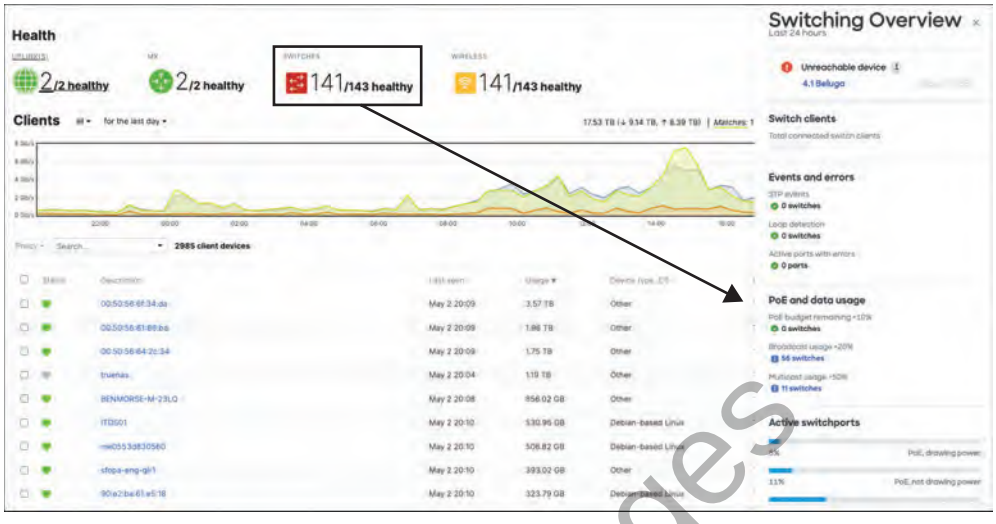

Figure 3-14 *The New Switching Overview Feature*

Global Overview

For administrators who need to manage multiple organizations within the Meraki Dashboard, the Global Overview page, shown in Figure 3-15, provides a summarized overview of the health of all networks and devices an administrator has access to across all organizations. This page also introduces a few additional key features to help manage multiple organizations, like visibility into Meraki support tickets across each organization, license statuses (including unused licenses and expiry dates), and quick reference of device health within each organization.

Figure 3-15 *The Global Overview Page Showing Three Different Organizations*

The Global Overview page is designed to simplify the interaction across organizations for administrators who need to maintain and monitor multiple Dashboard organizations by providing the most useful information for each organization in an easily accessible summary.

You can find more information on the Global Overview feature at https://documentation.meraki.com in the "Global Overview" document.

Network-wide Health Views

After reviewing the high-level summaries at the organization level, it's time to drill down into some of the network-specific pages and views to get a more detailed picture of the health and overall status of a network and its clients.

Network-wide and Uplink Health

To get to the detailed reports and data for a given network in an organization, click the network name from the Organization Summary or Organization Overview page, or select the network from the Networks panel on the left.

After navigating to a specific network, you are presented with the Network-wide > Clients page. The Health section, shown in Figure 3-16, provides a quick reference report for the uplink status (if available) and the device statuses of any Meraki hardware currently added to the network. From this section of the page, you can click each icon to view the product details page for each hardware platform available.

Figure 3-16 *The Network Health Summary on the Network-wide > Clients Page*

Below the Health section is the Clients section, which includes a list of all recently seen clients on the network, a summary of traffic and client usage, and a more detailed traffic analysis of client traffic, which you can view by selecting the **Show** link under the Applications pie chart to the right of the usage summary. An example of the fully expanded Application Details view is shown in Figure 3-17.

The Application Details section is powered by Cisco Network-Based Application Recognition (NBAR), which provides visibility into more than 1500 of the most popular applications. NBAR-enabled platforms are able to better analyze and identify client traffic to enforce more granular Layer 7 firewall rules and policies, configurable from the Security & SD-WAN > Firewall page (see Figure 3-18) or within a Network-wide > Group Policy (see Figure 3-19), allowing for tighter policing of user traffic with less effort than ever before.

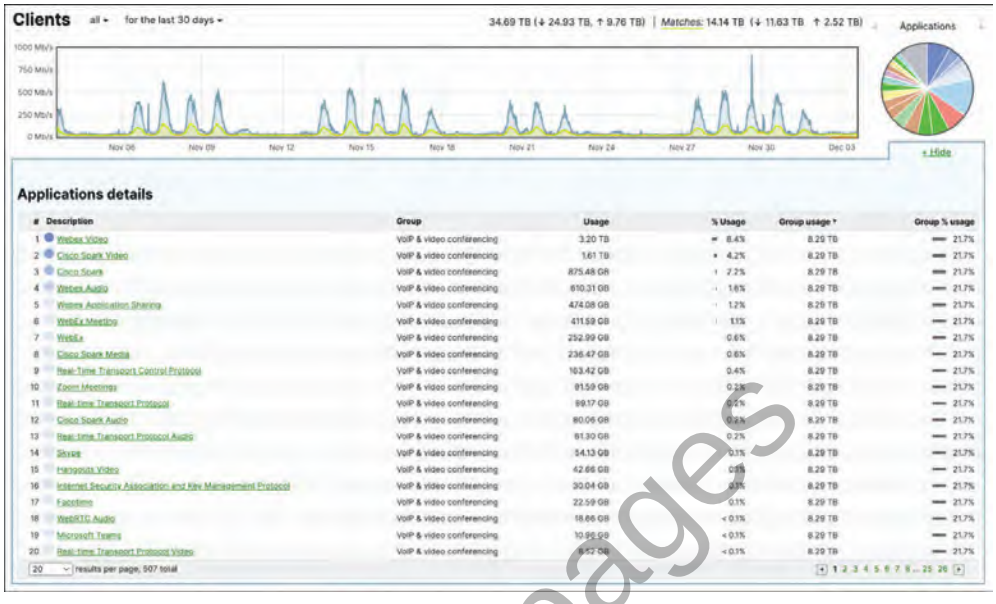

Figure 3-17 *Application Visibility on the Network-wide > Clients Page*

Pro Tip Application Visibility and Control (AVC) details are available on the Clients page, with quick sort options and additional details regarding client usage for each application by selecting the application from the list.

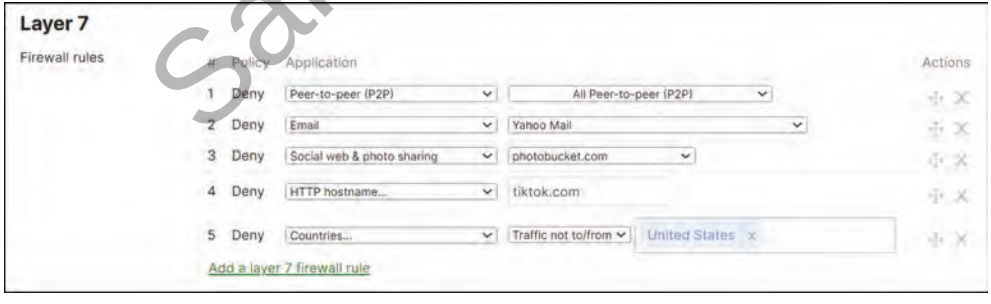

Figure 3-18 *An Example Set of Layer 7 Firewall Rules Utilizing Several NBAR-Based Application Rulesets*

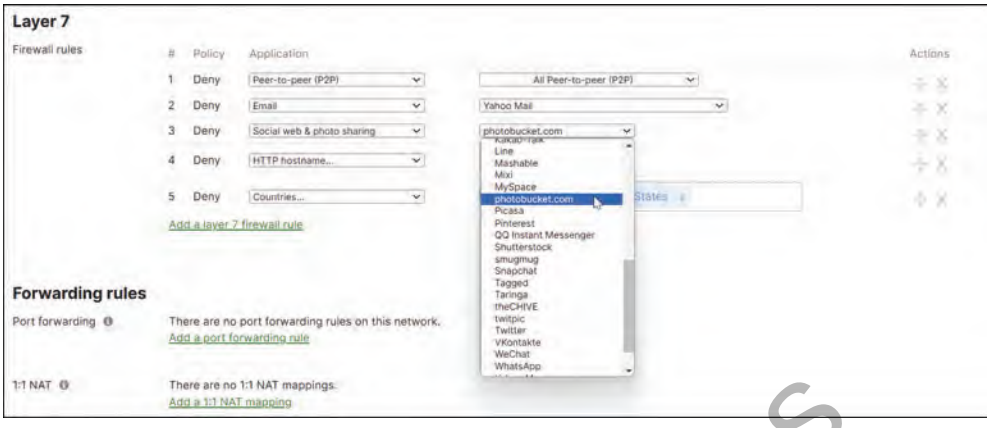

Figure 3-19 *An Example of the Detailed Application-Level Granularity Available for Devices Using NBAR*

To confirm the minimum supported firmware versions for Meraki MX, MS, and MR platforms to allow enabling of NBAR functionality, visit https://documentation.meraki.com and view the article 'Next-gen Traffic Analytics – Network-Based Application Recognition (NBAR) Integration.' You can find more information about NBAR classifications in the same article and by viewing Cisco's NBAR-related documentation at www.cisco.com (search for the keyword NBAR).

Wireless Network Health

Wireless networks sometimes are prone to issues, whether they be deployment related, client related, or even just environmental. Fortunately, the Meraki platform has again embraced the power of the cloud to actively monitor and report on the health and performance of any Meraki wireless networks.

The Wireless Health feature of the Meraki Dashboard offers some significant advantages when trying to troubleshoot issues such as client connectivity or authentication failures. As an example, Figure 3-20 shows the health overview for a wireless network on a Cisco Meraki campus. From this page, it's clear that the network and its clients are functioning smoothly overall and without issue.

Now if you compare that with the view in Figure 3-21 from a different network, the value of the Wireless Health feature and its ability to clearly demonstrate client-impacting issues becomes immediately obvious, as you can quickly and easily see at a glance that there is an authentication-related issue for several devices, unlike the previous network shown in Figure 3-20.

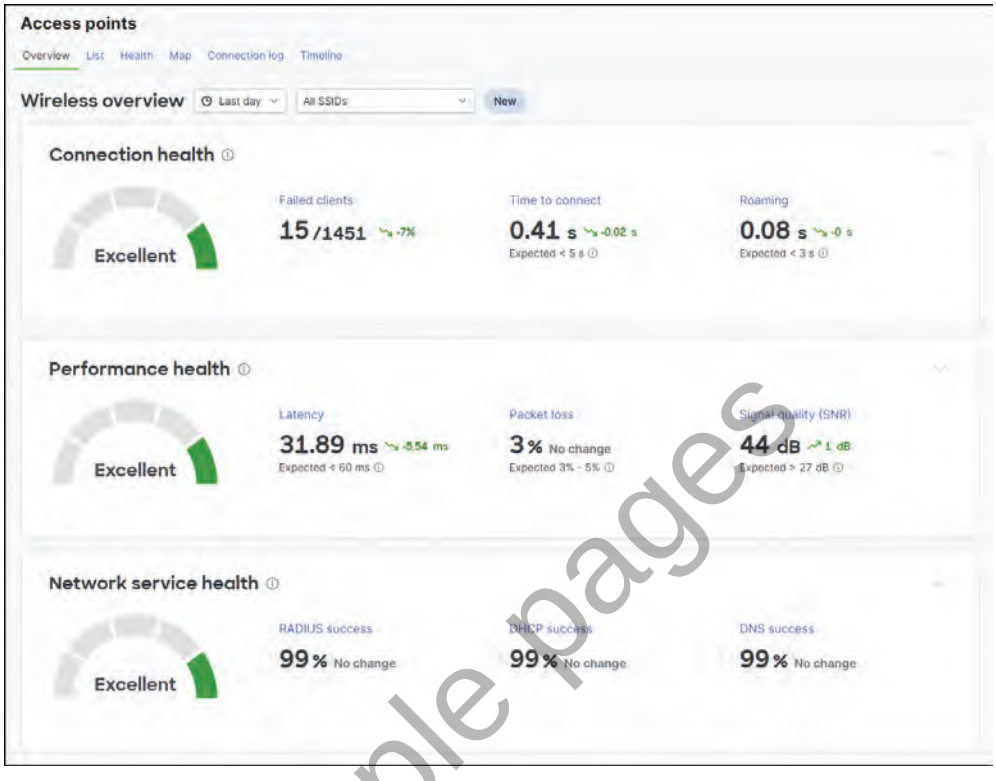

Figure 3-20 *The Wireless Overview for a Cisco Meraki Campus, Showing a Well-Functioning Wireless Network with No Notable Issues*

From this point, you can review the rest of the report to get more details about where the issue may lie. The rest of the Wireless Health page reports several other helpful perspectives, such as issues by SSID, AP, individual client, and even by device type, to help scope and further narrow down potentially impacting issues. This makes it easy to determine if a specific SSID is improperly configured, if a specific AP is connected to an incorrect port, or if a specific client or client type is having issues that are otherwise not present for other clients or client types.

As Figure 3-22 shows for a simple home network, the Wireless Health feature can provide extremely valuable information when you're trying to determine the potential scope and impact of a reported behavior.

As just demonstrated, Meraki's Wireless Health feature helps to take the guesswork out of attempting to triage a wireless issue by providing important details that help to determine the scope and impact of a behavior from a quickly accessible and easy to interpret report. This helps to save time and refocus troubleshooting efforts in appropriate directions, leading to a faster time to resolution for many issues than a more traditional troubleshooting approach.

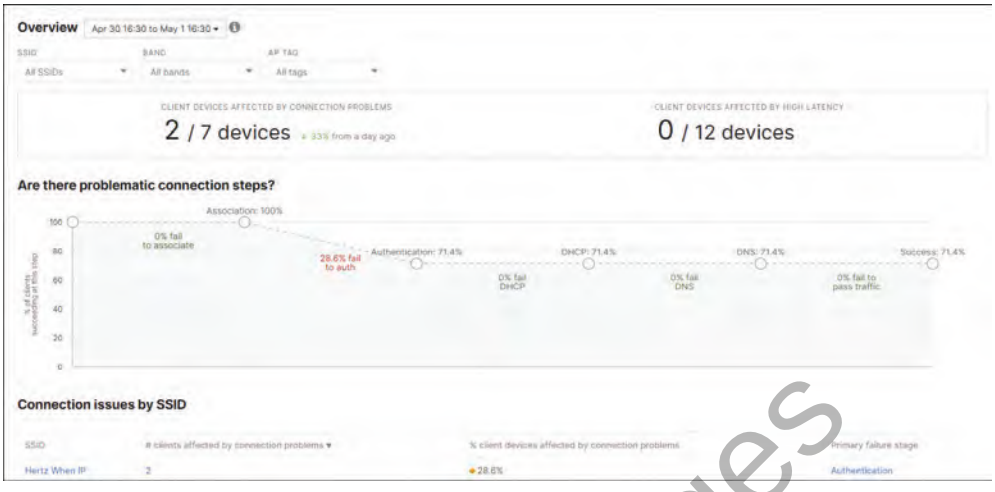

Figure 3-21 *The Wireless Health Report for an Example Network, Showing Failures Relating to Authentication for Two Clients*

The Wireless Health feature is discussed in much further detail in Chapter 8, "Introduction to Meraki MR Access Points."

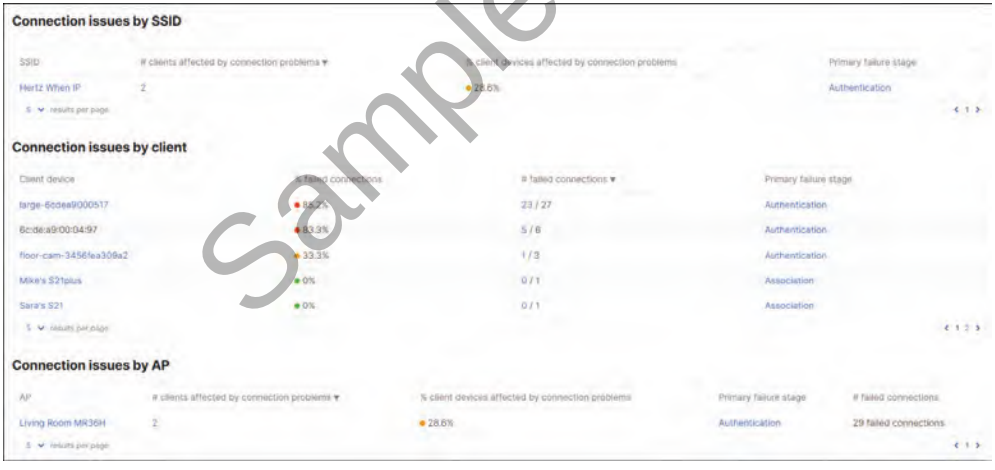

Figure 3-22 *Additional Details of the Wireless Health Report for the Network Showing Client Authentication Issues*