

Cisco Meraki Fundamentals

Cloud-Managed Operations



Sample paper



Contents

Foreword xxii

Introduction xxiv

Part I Knowledge Is Power: Understanding the Cloud Architecture

Chapter 1 Cisco Meraki Cloud Architecture Basics 1

Dashboard Architecture 1

Cloud/Back-end Architecture 3

Device to Cloud Communication 4

Data Security and Retention 6

Firmware Management and Lifecycle 7

Summary 9

Additional Reading 10

Chapter 2 Building the Dashboard 11

Creating an Organization 12

Creating a Network 14

Claiming and Adding Devices 15

Defining Administrators and Privileges 17

 Special Access Roles 18

 SAML Roles 20

 Maintaining Control of the Dashboard 21

Tagging to Scope 22

 Intro to Tags 22

 Tagging for Administrative Privileges 22

 Network and Device Configurations 23

Configuring SSID Availability on MR Access Points 23

*Configuring Non-Meraki VPN Peer Availability for MX and Z Series
 Devices 24*

 Meraki Systems Manager 25

Dashboard Alerting and Reporting 25

 Dashboard Email Alerts 26

 Webhooks 27

 Syslog 28

 SNMP and SNMP Traps 29

 Automated Summary Reports 29

 Meraki Insight Alerts 31

 Alert Hubs 33

	Global Overview	34
	Summary	35
	Additional Reading	35
Part II	Building a Scalable Foundation with Dashboard	
Chapter 3	The Meraki Admin Experience	37
	Org-wide Health	38
	Firmware Status	39
	Detailed Firmware Status and Security	40
	Proactive Replacements	41
	Dashboard Early Access Program	42
	Magnetic Design System	42
	New Landing Page	43
	New Organization Alert Page & Alert Hub Enhancement	44
	Switching Overview	46
	Global Overview	47
	Network-wide Health Views	48
	Network-wide and Uplink Health	48
	Wireless Network Health	50
	Automated Topology Views	53
	Network-wide Layer 2 Topology	53
	Network-wide Layer 3 Topology	55
	Network-wide Multicast Topology	55
	Summary	57
	Additional Reading	57
Chapter 4	Automating the Dashboard	59
	Configuration Templates	59
	How Do Templates Work?	59
	Local Overrides	61
	Template Caveats and Limitations	62
	Template Best Practice Considerations	64
	Using Webhooks, Syslog, and SNMP to Trigger Outside Automation	65
	Webhooks	66
	Syslog	67
	SNMP	68
	Dashboard API	70

What Is the Dashboard API and How Is It Used?	70
API Tips and Tricks	71
Dashboard API Examples	72
<i>Automated API-based Organization Status</i>	73
<i>Automated MR Naming Based on Upstream Switch</i>	75
MT Automation	78
Dashboard-Based Automation	78
Summary	82
Additional Reading	82

Part III The MX—The Cloud-Managed Swiss Army Knife

Chapter 5 MX and MG Best Practices 83

MX Scaling	84
Deployment Modes	84
Routed Mode	84
Passthrough or VPN Concentrator Mode	85
Security	85
L3/L7 Firewall	86
HTTP Content Filtering (TALOS)	87
Cisco AMP	87
IDS/IPS	88
Cisco Umbrella	89
Dashboard Group Policy	90
Adaptive Policy (SGT)	91
VPN	92
Meraki Auto VPN	92
Client VPN	93
Cisco AnyConnect	94
Non-Meraki VPN	94
Routing	95
Route Priority	95
Static Routes	95
OSPF	96
BGP	97
Deploying Meraki Auto VPN	97
Configuring Auto VPN	98
<i>Hub Versus Spoke</i>	100

<i>NAT Traversal</i>	100
Hub and Spoke Recommendations	101
<i>Sizing It Right</i>	101
<i>Hub Prioritization</i>	102
<i>Full Tunnel Versus Split Tunnel</i>	102
<i>Advanced Configurations</i>	103
Monitoring Your Deployment	104
Meraki Insight	104
<i>Web Application Health</i>	105
<i>WAN Health</i>	108
<i>VoIP Health</i>	108
<i>Insight Alerts</i>	109
<i>ThousandEyes Integration</i>	110
Monitoring VPN	110
Reviewing Dashboard Alerts	112
<i>Alert Hub</i>	112
<i>Organization Alerts</i>	113
Threat Assessment on Meraki Dashboard	114
Security Center	115
<i>Most Prevalent Threats</i>	115
<i>Most Affected Clients</i>	116
Introduction to MG Cellular	117
4G LTE Versus 5G	117
5G NSA Versus 5G SA	118
Dashboard Monitoring for MG	118
MG Deployment Considerations	119
Cellular—Primary or Backup?	120
5G Line of Sight	120
CGNAT and You	121
Prestaging for Deployment	121
Troubleshooting Meraki Devices	122
Local Status Page	122
Safe Mode	124
Support Data Bundle (SDB) Logging	124
Integrated DM Logging	124
Summary	124
Additional Reading	125

Chapter 6 MX SD-WAN Best Practices 127

Introduction to Meraki SD-WAN	127
The Science of Transport Performance	128
The Anatomy of SD-WAN Policies	129
SD-WAN Uplink Policies	130
Custom SD-WAN Performance Classes	131
Traffic Analysis and Identification	133
Dynamic Path Selection Policies	134
<i>Global Preference Policy</i>	135
<i>Basic Load Balancing Policy</i>	136
<i>Basic Policy-Based Routing</i>	137
<i>Performance-Based DPS</i>	137
<i>Policy Routing with Performance-Based DPS</i>	138
SD-WAN over Cellular	138
SD-Internet	140
Integrating MPLS	141
MPLS on the LAN: Failover to Meraki Auto VPN	141
MPLS on the WAN: Meraki Auto VPN Overlay	142
Summary	144
Additional Reading	144

Part IV The Ultimate Cloud-Managed Access Layer

Chapter 7 Meraki Switching Design and Recommendations 145

Introduction to Meraki Switches	145
Meraki Switching Design	145
Designing a Wired Enterprise Network	149
Planning Your Deployment	149
Selecting the Right Switch Product Mix	150
Planning Hybrid Campus LAN Architectures with Cloud Management	152
Designing the Access Layer	154
<i>VLAN Deployment</i>	154
<i>Using Native VLAN 1</i>	155
<i>Planning QoS</i>	156
<i>Fine-Tuning STP in a Hybrid Environment</i>	156
<i>Tags to Optimize Deployment</i>	157
<i>MTU Recommendation</i>	158
<i>Connecting Trunk Ports</i>	158

<i>Connecting MR Access Points</i>	158
Layer 3 Best Practices	159
<i>OSPF Best Practices</i>	159
<i>Multicast Best Practices</i>	160
Securing Layer 2 Operations	160
Infrastructure Security	160
<i>DHCP Snooping</i>	161
<i>Storm Control</i>	161
<i>Dynamic ARP Inspection</i>	162
SecurePort	163
Port Profiles	164
VLAN Profile	164
Network Security	165
Sticky MAC	165
Port Isolation	166
802.1X Authentication	166
MAC Authentication Bypass	169
Change of Authorization with ISE Integration	169
End Point Security	172
Micro-Segmentation with MS (Adaptive Policy)	173
Identity Classification and Propagation	174
Security Policy Definition	174
Policy Enforcement	174
SGT Assignment Methods	175
Caveats in Setting Up Adaptive Policy	176
Operating and Optimizing Meraki Switches	176
Virtual Stacking	177
Firmware Upgrade Consideration on MS	178
Configuration Validations	179
Config-Safe Mechanism	179
Auto-Rollback on Bad Uplink	179
MS PoE Budget	180
MS Power Overview	181
Sustainability Using MS	182
Cloud-Monitored Catalyst	183
Troubleshooting Your Meraki Deployment	184

	Dashboard Reporting	184
	Dashboard Live Tools	187
	<i>Ping</i>	187
	<i>Packet Capture</i>	188
	<i>MTR</i>	189
	<i>MAC Forwarding Table</i>	190
	<i>Cable Testing</i>	190
	<i>Cycle Port</i>	191
	<i>Wake-on-LAN</i>	191
	Summary	192
	Additional Reading	192
Chapter 8	Meraki Wireless Best Practices and Design	195
	Scoping and Scaling the Dashboard	196
	Physical WLAN Design	197
	Location-Aware Wireless Network	197
	Wi-Fi 6E and Dual 5-GHz Mode	198
	6-GHz RF Propagation	199
	AP Mounting Recommendations	199
	AP Adjacency and Overlap	201
	Configuring Meraki Wireless	201
	RF Profile Best Practices and Recommendations	203
	Band Selection: Per SSID Versus All SSIDs	204
	Client Balancing	205
	Minimum Bitrate	206
	Channel Planning Best Practices	209
	Frequency Bands	209
	Channel Width	209
	Channel Selection: DFS Channels	210
	Meraki Auto RF	211
	Other Design Considerations for Meraki Wireless	213
	Why Distributed Networks?	213
	Authentication and Encryption	214
	VLAN Considerations	215
	AP Tag Use Cases	216
	Setting Up Enterprise-Grade Meraki Wireless	217
	Defining Roaming	218

	Defining Domains	219
	<i>Roaming Domains</i>	219
	<i>Layer 2 Domains</i>	220
	<i>Layer 3 Domains</i>	221
	Defining DHCP Scope	221
	Security Features and Wireless Security Best Practices	222
	<i>Air Marshal</i>	222
	<i>Traffic Segregation and Access Control</i>	223
	Operating the Network	225
	Site-Level Wi-Fi Overview	225
	Wireless Health and Overview	227
	Anomaly Detection (Smart Thresholds)	228
	Server RCA	231
	Device Monitoring and Reporting	232
	<i>Roaming Analytics</i>	232
	<i>Client Overview</i>	232
	<i>Client Details</i>	234
	<i>Client Timeline</i>	234
	<i>Access Point Timeline</i>	235
	Summary	236
	Additional Reading	236
Part V	The Environment: The Next Frontier	
Chapter 9	MV Security and MT (IoT) Design	239
	Redefining Surveillance: The Meraki Difference	239
	Meraki Camera Architecture	239
	<i>MV Video Architecture</i>	240
	<i>Ensuring Security</i>	241
	Built-in Analytics	241
	Designing with Purpose: Building an Effective Surveillance System	242
	Planning Camera Mounting Options and Accessories	243
	Technology Considerations	244
	<i>Lens Types</i>	244
	<i>Field of View</i>	244
	<i>Resolution</i>	245
	Other Deployment Needs	245
	Cisco Meraki MV52: An Example of MV Camera Offerings	245

Choosing the Right Storage	246
Planning for Power Requirements	246
Planning Camera Connectivity: Wired and Wireless	247
<i>General Network Considerations</i>	247
<i>Considerations for Wired Connections</i>	248
<i>Considerations for Wireless Connections</i>	248
Building an Optimized Camera System	249
Defining Camera Names and Tags	249
Defining Camera Administrators	249
<i>Dashboard-Defined Camera-only Administrators</i>	250
<i>Role-Based Camera Permissions for SAML/SSO</i>	251
Accessing Footage: Meraki MV Camera Views	251
Meraki Dashboard	252
Meraki Vision Portal	253
Meraki Display App	255
Meraki Mobile App	255
Configuring and Optimizing MV Cameras	257
Listing Camera Details	257
Configuring Camera Profiles	258
<i>Assigning Camera Profiles</i>	261
Manual Camera Configurations	261
<i>Recording in Low Light</i>	262
Camera Motion Alerts	263
<i>Fine-Tuning Camera Alerts</i>	264
Configuring Privacy Windows	267
Setting Up RTSP Integration	267
Configuring Video Walls	267
Operating Meraki MV Cameras	268
Navigating the Video Timeline	269
Built-in Analytics	269
Audio Detection	271
Motion Search and Motion Recap	271
Sharing Video	275
<i>Exporting Video</i>	276
<i>Working with Cloud Archive</i>	278
<i>Accessing Video Event Logs</i>	278

Meraki MV Sense	279
Troubleshooting Meraki MV Cameras	280
Enabling Firewall Ports for Meraki Cloud	280
Providing Camera Access to Meraki Support	281
Strengthening Security: Implementing Meraki IoT with MV	281
Building Smarter Spaces with Meraki MT Sensors	281
Designing Smart Spaces with Meraki MT Sensors	281
Ensuring Sustainability	282
Understanding MT Security Architecture	283
Protecting Business Assets Using MT Sensors	285
Environmental	285
Physical	286
Exploring MT Sensors	286
Physical Infrastructure Monitoring	287
<i>MT12—Water/Leak Sensor</i>	287
<i>MT20—Door Sensor</i>	288
<i>MT40—Smart Power Controller</i>	289
Environmental Monitoring	289
<i>MT11—Cold Storage Sensor</i>	289
<i>Temperature, Humidity, and Air Quality Sensors</i>	291
<i>MT30—Smart Automation Button</i>	293
<i>Smart Button Automation</i>	293
Deploying Meraki MT Sensors	294
Basic Configuration and Setup	294
Understanding Meraki IoT Gateways	295
Accounting for Distance to Sensors	295
Power Considerations	295
Configuration Considerations	296
Configuring and Monitoring Alerts	296
Setting Alert Types	296
Reviewing Generated Alerts	296
Sensor Sight	298
IoT Operational Best Practices	299
Troubleshooting Meraki MT Sensors	299
Monitoring Sensor Status	300
Viewing Sensor Event Logs	300
Monitoring BLE Signal Strength	300

Summary 301
Additional Reading 301
 MV Camera References 301
 MT Sensor References 302

Appendix A Cisco Meraki Licensing 303

Enterprise Licensing Versus Advanced Licensing 309
External Licensing for Integrations 304
Dashboard Licensing Models 304
 Co-termination Licensing (Classic) 304
 Per-Device Licensing 306
 Meraki Subscription Licensing 307
Summary 307
Additional Reading 308

Index 309

Sample pages

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.

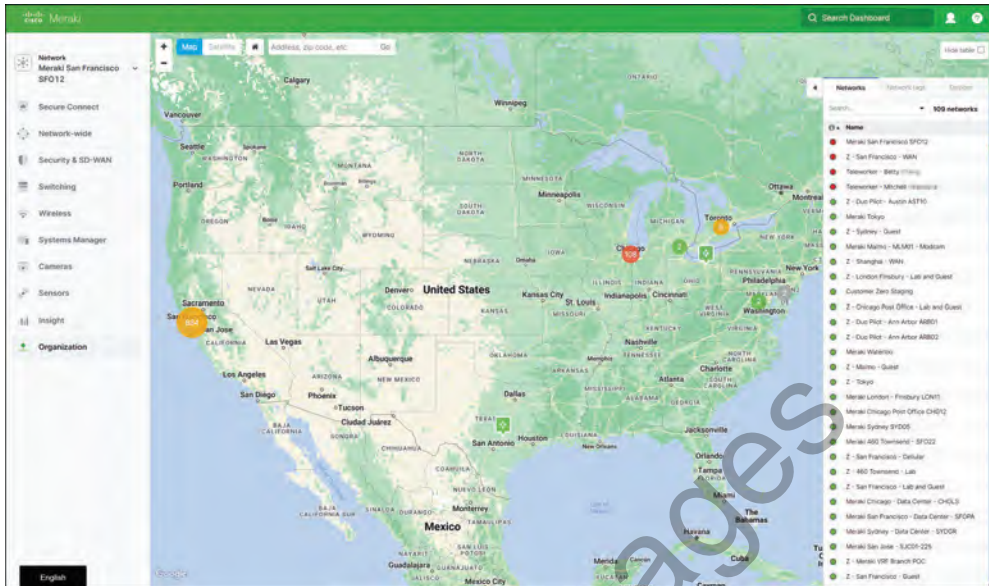


Figure 3-1 *The Organization Overview Page for the Cisco Meraki Organization Showing the Map Alongside the Network List in Collapsed Form*

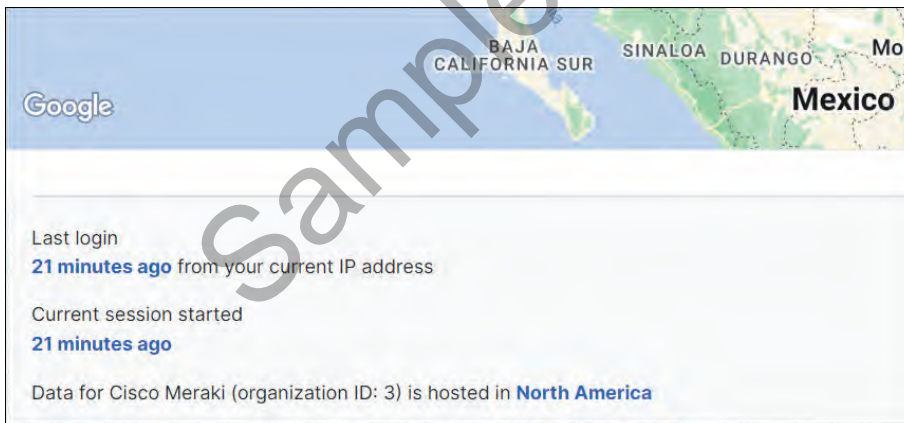


Figure 3-2 *The Current Session and Organization Hosting Details for an Example Organization*

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.

Name	Network health	Firmware status	Firmware security	Last PCI scan	Clients
Meraki San Francisco SFO12	■	Upgrade available	Secure	None	13320
Meraki Chicago Post Office CHG12	■	Upgrade available	Secure	None	5258
Meraki Sydney SYD05	■	Upgrade available	Secure	None	320
Meraki A80 Townsend - SFO22	■	Upgrade available	Secure	None	46
Z - San Francisco - Sensors	■	Up to date	Secure	None	0
Z - Ohio - Engineering Lab REQ31	■	Up to date	Secure	None	4
Z - Chicago Post Office - Lab and Guest	■	Upgrade available	Secure	None	520
Z - Duo Post - Austin AST16	■	Upgrade available	Secure	None	58
Z - Duo Post - Austin AST12	■	Upgrade available	Secure	None	38
Meraki Tokyo	■	Upgrade available	Secure	None	22
Z - Sydney - Guest	■	Upgrade available	Secure	None	174
Z - Meraki Blizzard	■	Upgrade available	Secure	None	0
Meraki Mamo - MSM01 - Moslem	■	Upgrade available	Secure	None	20
Z - Shanghai - WAN	■	Upgrade available	Secure	None	28
Z - London Bishopsgate - Lab and Guest	■	Upgrade available	Secure	None	80
Z - London Finsbury - Lab and Guest	■	Upgrade available	Secure	None	246
Z - Duo Post - London	■	Upgrade available	Secure	None	92
Teleworker - Rupert Winer	■	Upgrade available	Secure	None	0
Z - Duo Post - Ann Arbor AB01	■	Upgrade available	Secure	None	43
Z - Duo Post - Ann Arbor AB02	■	Upgrade available	Secure	None	20
Meraki Waterloo	■	Upgrade available	Secure	None	13
Z - Mamo - Guest	■	Upgrade available	Secure	None	6

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.

Name	Usage	Clients	Network type	Devices	Office devices	Firmware security	Firmware status	Tags
Meraki London - Finbury LO001	3.89 TB	540	Combined	58	13	Secure	Upgrade available	Let's begin client on...
Meraki San Francisco SFO2	103.85 TB	17903	Combined	838	132	Secure	Upgrade available	ANALYSIS ON client on...
Meraki Chicago Post Office CH012	7.71 TB	9325	Combined	472	27	Secure	Upgrade available	Client on...
Z - Dual Flex - Austin AST19	21.9 GB	24	Combined	1	0	Secure	Upgrade available	Search on read only
Z - Dual Flex - Austin AST12	43.71 GB	28	Combined	2	0	Secure	Upgrade available	Search on read only
Meraki Tokyo	62.12 GB	19	Combined	6	0	Secure	Upgrade available	Search on read only
Z - Sydney - Guest	1.00 TB	188	Combined	2	0	Secure	Upgrade available	Search on read only
Z - Meraki Blizzard	None	0	Combined	1	0	Secure	Upgrade available	Search on read only
Meraki Mainz - MLM01 - Modem	1.70 TB	24	Combined	6	0	Secure	Upgrade available	Search on read only
Z - Shanghai - WAN	362.13 GB	24	Combined	2	0	Secure	Upgrade available	Search on read only
Z - London Bishopgate - Lab and Guest	169.33 GB	87	Combined	5	0	Secure	Upgrade available	Search on read only
Z - London Finbury - Lab and Guest	246.50 GB	224	Combined	7	4	Secure	Upgrade available	Search on read only
Z - Dual Flex - London	234.03 GB	111	Combined	1	0	Secure	Upgrade available	Search on read only
Z - Chicago Post Office - Lab and Guest	126 TB	857	Combined	30	0	Secure	Upgrade available	Search on read only
Z - Dual Flex - Ann Arbor AR001	44.37 GB	40	Combined	1	0	Secure	Upgrade available	Search on read only
Z - Dual Flex - Ann Arbor AR002	27.72 GB	32	Combined	1	0	Secure	Upgrade available	Search on read only
Meraki Waterloo	58.48 GB	12	Combined	5	1	Secure	Upgrade available	Search on read only
Z - Mainz - Guest	494.6 MB	11	Combined	1	0	Secure	Upgrade available	Search on read only
Z - Krakra KR002 - Lab and Guest	20.92 GB	4	Combined	2	0	Secure	Upgrade available	Search on read only

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.

Network Name	Device Type	Templates	Current Version	Firmware Type	Status	Availability
Network	Any device type	All networks	Any version	Any firmware type	Good	Any availability
TELEWORKER - London	Wireless Template				Any status	re
TELEWORKER - San Francisco	Wireless Template				Critical	Status
Teleworker - GSD Spencer_Gage	Wireless (bound to template)				Warning	Availability
Teleworker - Mahabub Sakural	Wireless (bound to template)				Good	Good
Teleworker - Kash Saeed	Wireless (bound to template)				Good	Good
Teleworker - Rupert Weyer	Wireless (bound to template)				MR 28.6.1	Good
Meraki 400 Townsend - SFO2	Wireless				MR 28.6.1	Good

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.

Current firmware	Status	Availability	Upgrade scheduled	Firmware type
MS 14.32	Critical - October 21, 2022	Upgrade available	No	General Availability
MS 12.28.1	Critical - February 1, 2023	Upgrade available	No	General Availability
MS 12.28.1	Critical - February 1, 2023	Upgrade available	No	General Availability
MS 14.32	Critical - October 21, 2022	Upgrade available	No	General Availability
MS 12.28.1	Critical - February 1, 2023	Upgrade available	No	General Availability
MS 11.22	Critical - November 16, 2021	Upgrade available	No	General Availability

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

Current firmware	Status	Availability	Upgrade scheduled	Firmware type
MS 14.33.1	Warning - April 01, 2023	Up to date	No	General Availability
MS 14.33.1	Warning - April 01, 2023	Up to date	No	General Availability
MS 14.33.1	Warning - April 01, 2023	Up to date	No	General Availability
MS 14.33.1	Warning - April 01, 2023	Up to date	No	General Availability
MS 14.33.1	Warning - April 01, 2023	Up to date	No	General Availability

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**.

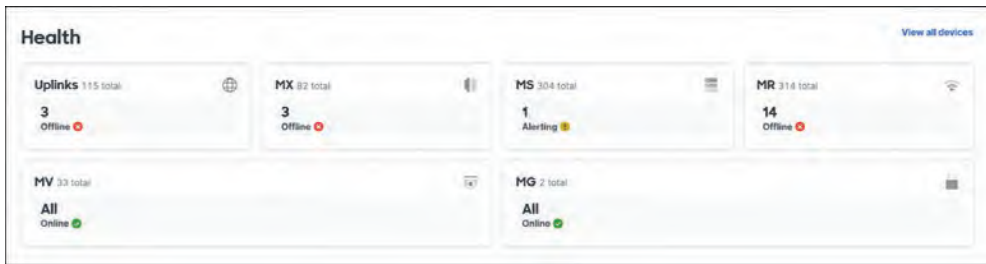


Figure 3-9 The Health Section of the New Organization Summary Page Available in the New Landing Page

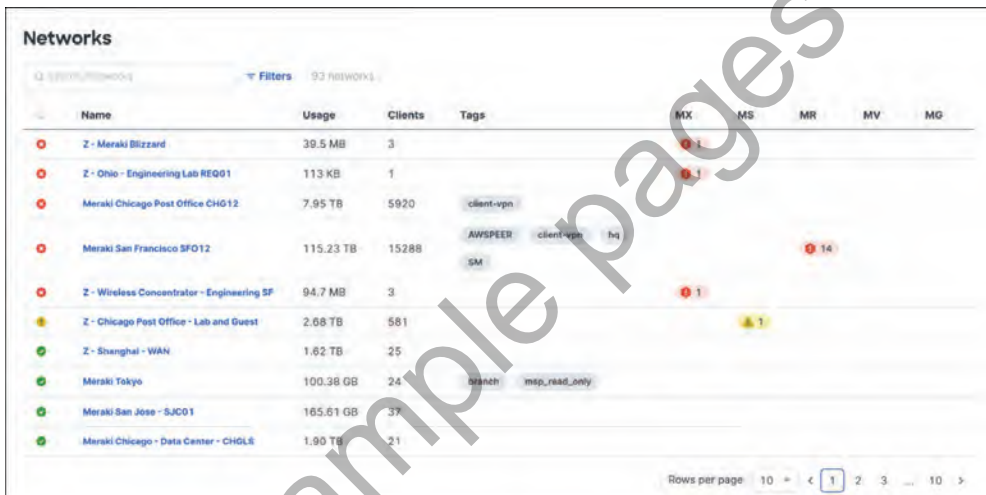


Figure 3-10 The Networks Section of the New Organization Summary Page for Networks Within the Cisco Meraki Organization

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.

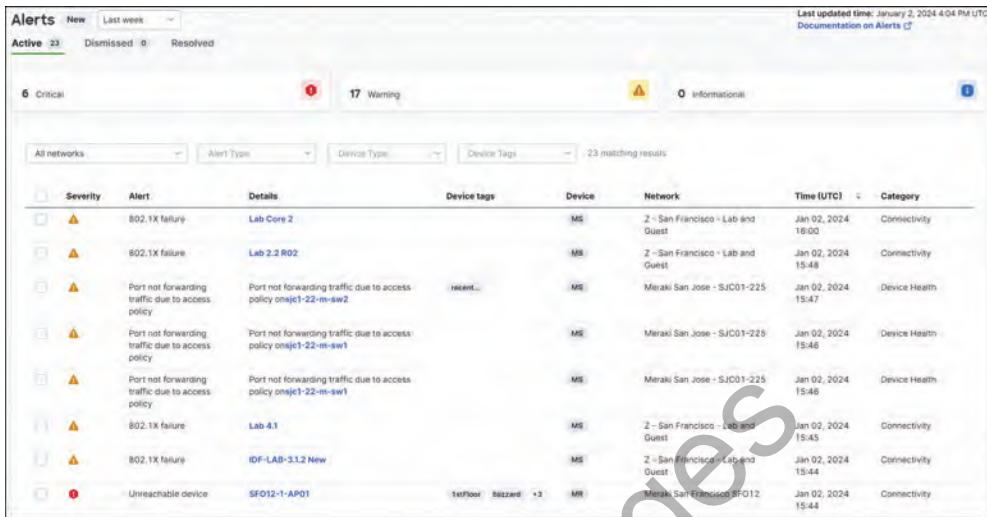


Figure 3-11 The New Organization Alerts Page

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.

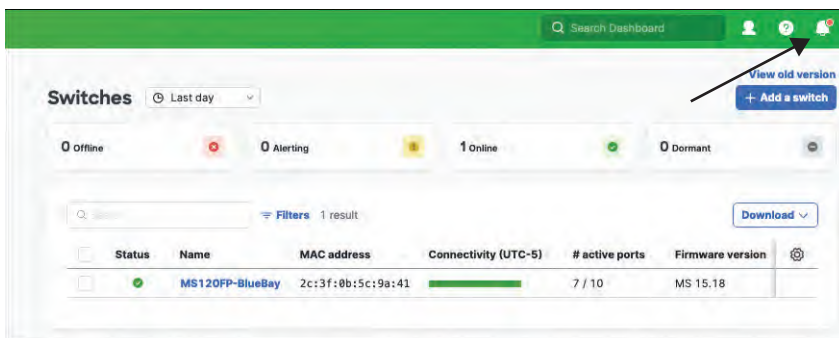


Figure 3-12 The Alert Hub Notification Icon

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.

The screenshot displays the Alerts notification panel for the Meraki San Francisco SF012 network. The panel is organized into several sections:

- Alerts Header:** Shows the network name and a 'Beta' badge.
- Alert Category:** A dropdown menu currently set to 'DEVICE HEALTH'. A 'Troubleshooting Documentation' link is also present.
- Active Alerts:**
 - Power supply offline (4 instances):** Includes details for 'Closet 1.1' (Dec 09 11:02) and 'Closet 4.3' (Dec 08 13:45), with a 'rvch' user and a 'Dec 08 13:45' timestamp. A 'View All' link is provided.
 - CRC errors (1 instance):** Details for 'Switch C / 3 and Switch D3423432' (Dec 08 13:45).
- Dismissal buttons:** A 'Dismissal button' is indicated for the active alerts.
- DISMISSED ALERTS (3):**
 - Two 'Power supply offline' alerts from 'Closet 1.1' (Dec 08 13:45) with 'Restore' buttons.
 - One 'VLAN mismatch' alert for 'Switch C / 3 and Switch D3423432 / 4' (Dec 08 13:45) with a 'Restore' button and a 'Suggested fix' link.
- Dismissed alerts section:** A bracket groups the dismissed alerts section.
- Feedback:** A 'Give feedback on these alerts' link is located at the bottom.

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.

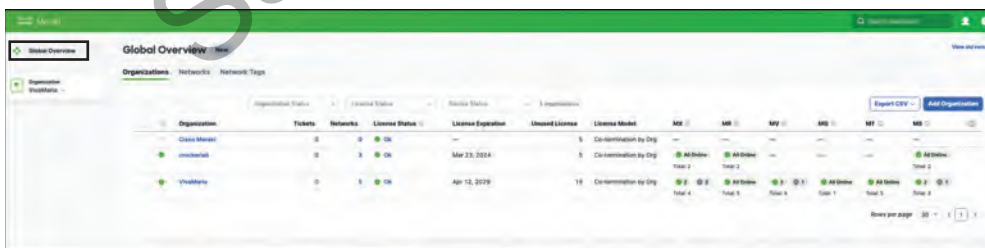


Figure 3-15 The Global Overview Page Showing Three Different Organizations

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.

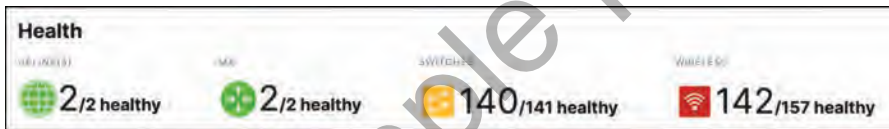


Figure 3-16 *The Network Health Summary on the Network-wide > Clients Page*

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.

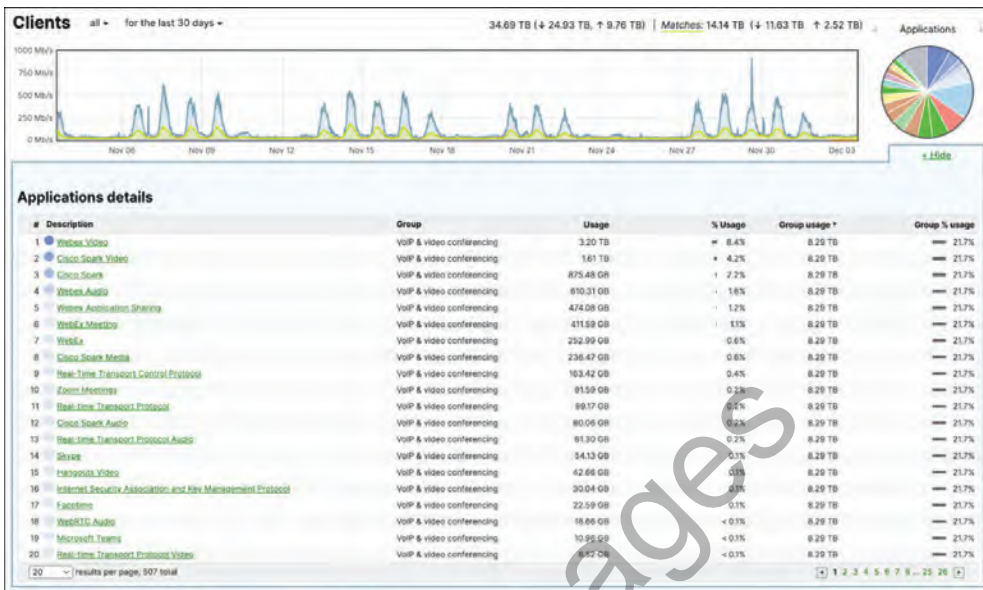


Figure 3-17 Application Visibility on the Network-wide > Clients Page

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.

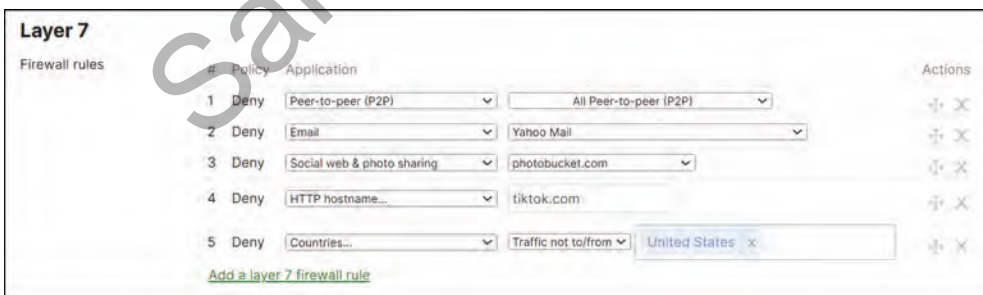


Figure 3-18 An Example Set of Layer 7 Firewall Rules Utilizing Several NBAR-Based Application Rulesets

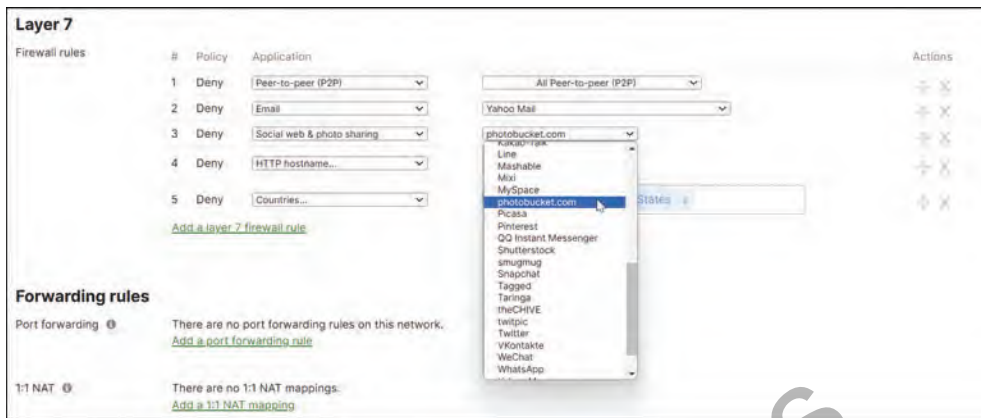


Figure 3-19 An Example of the Detailed Application-Level Granularity Available for Devices Using NBAR

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.

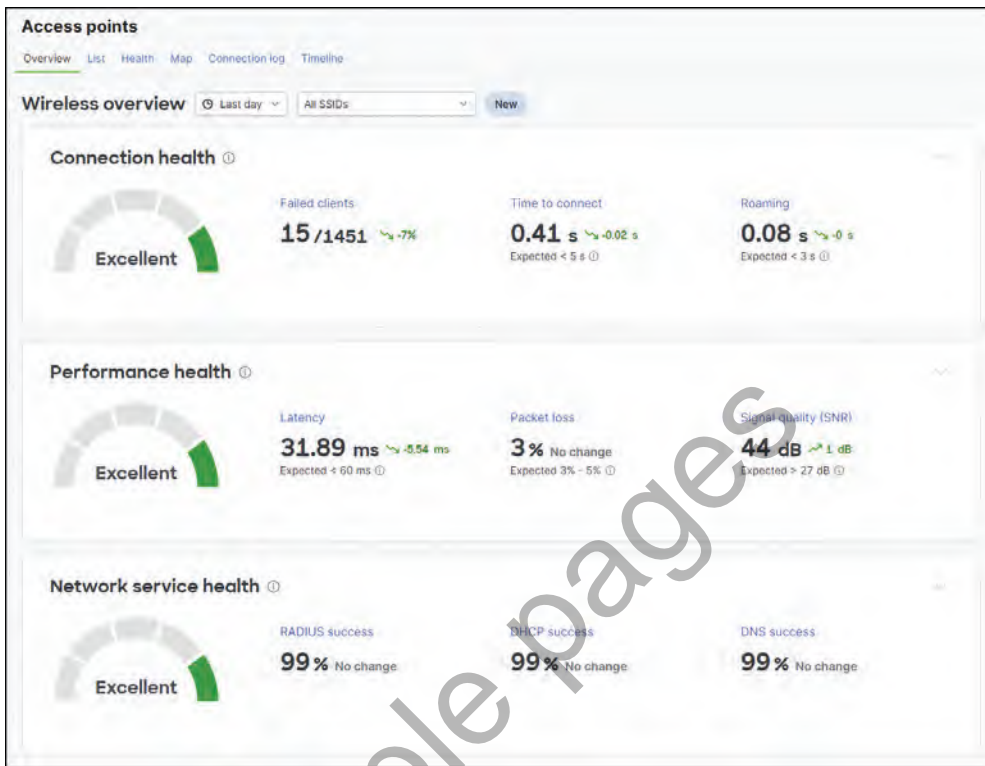


Figure 3-20 *The Wireless Overview for a Cisco Meraki Campus, Showing a Well-Functioning Wireless Network with No Notable Issues*

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.

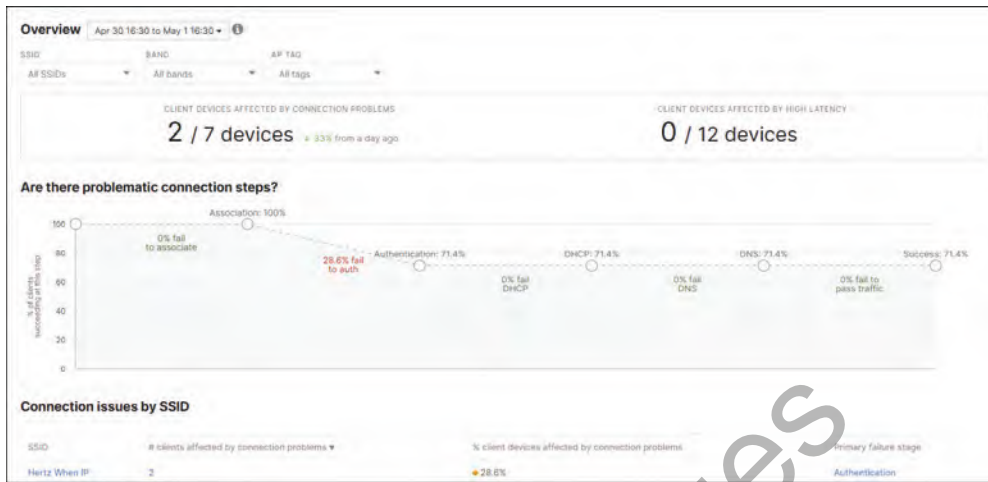


Figure 3-21 *The Wireless Health Report for an Example Network, Showing Failures Relating to Authentication for Two Clients*

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*