Cisco Meraki Fundamentals

Cloud-Managed Operations

ARUN PAUL
MIKE WOOLLEY
MEDI JAAFARI
JEFFRY HANDAL

ciscopress.com

Cisco Meraki Fundamentals

Cloud-Managed Operations

Arun Paul
Mike Woolley
Medi Jaafari
Jeffry Handal

Cisco Press

Cisco Meraki Fundamentals

Cloud-Managed Operations

Arun Paul, Mike Woolley, Medi Jaafari, Jeffry Handal

Published by:
Cisco Press
Hoboken, New Jersey

$PrintCode

Library of Congress Control Number: 2024931249

ISBN-13: 978-0-13-816757-8

ISBN-10: 0-13-816757-5

Warning and Disclaimer

This book is designed to provide information about the Cisco Meraki cloud-managed networking platform and solutions. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Please contact us with concerns about any potential bias at https://www.pearson.com/report-bias.html.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

GM K12, Early Career and Professional Learning: Soo Kang

Alliances Manager, Cisco Press: Caroline Antonio

Director, ITP Product Management: Brett Bartow

Managing Editor: Sandra Schroeder

Development Editor: Ellie C. Bru

Senior Project Editor: Tonya Simpson

Copy Editor: Bill McManus

Technical Editors: Dave Kounas
Ryan Miles
Kyle Murdock

Editorial Assistant: Cindy Teeters

Cover Designer: Chuti Prasertsith

Composition: codeMantra

Indexer: Timothy Wright

Proofreader: Barbara Mack

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

About the Authors

Arun Paul serves as a technical solutions architect at Cisco Meraki, focusing on supporting public sector – SLED customers in the Midwest states. With more than a decade of experience in the technology industry, Arun has held diverse roles ranging from engineering to technical sales.

Arun's tech journey began as a software engineer at the Cisco Catalyst 6500 BU, where he played a pivotal role as a point of contact for Catalyst design recommendations and escalations. Arun showcased his innovative spirit by proposing Cisco innovation ideas and process improvements.

Beyond corporate roles, Arun co-founded a security consulting and training business, gaining valuable entrepreneurial experience. This venture provided insights into customer challenges in the modern technology landscape. Arun holds an MS in Information Security from George Mason University, graduating with a Distinguished Achievement Award.

Arun has consistently demonstrated dedication to excellence, innovation, and customer success throughout his career, earning accolades and awards for his noteworthy contributions to the field.

Mike Woolley is a support product specialist at Cisco Meraki with more than eight years of experience dedicated to supporting Meraki products and solutions. Starting in 2016 after receiving a BT in Network Administration from Alfred State College, Mike began as an intern within Meraki Support in San Francisco and rose through to the highest tiers of the technical support structure. Through this experience Mike has worked directly with customers and deployments of all types and sizes. From independent small businesses to massive international corporations, Mike has developed a tried-and-true approach to working with Cisco Meraki solutions based on these experiences. During this time Mike has also written and contributed to core pieces of Meraki documentation and has since become a leading source of knowledge within his specialization of Meraki's cellular-enabled product lines.

Mike currently lives in western New York with his wife Sara and their dog Noki and enjoys occasional outdoor activities like dirt biking and snowmobiling when not helping on the family farm or playing tabletop games.

Medi Jaafari has more than two decades of industry experience in roles ranging from advanced engineering architectures to director of engineering for a startup ISP colocation specializing in LAN/WAN transport, IoT, SDWAN, SASE, ZTNA, XDR, and observability for multinational, multitenant environments. Medi was an early participant in SDN networking developments working with key tier-one U.S.-based universities while at Cisco and is currently a technical solutions architect for the Cisco Meraki business unit, with more than five years of experience working closely on product design with a focus on SW features, UI, and AI design.

Jeffry Handal is a principal solutions engineer at Cisco. He completed his bachelor's and master's degrees in electrical engineering at Louisiana State University (LSU) and has more than 18 years of experience in the area of information communication technology, with special interest in IPv6, cybersecurity, big data, and experimental networks. Before joining Cisco, Jeffry was a very active customer, always pushing the envelope designing and maintaining networks with new technologies, testing new protocols, and providing Cisco and others a large-scale testbed for new products, features, and functionality. Currently, he plays an active role in several Cisco groups (e.g., TACops, IPv6 Ambassadors, Security Technical Advisory Group, Meraki).

Outside of work, Jeffry is an active volunteer in organizations ranging from search and rescue operations with the Air Force to humanitarian technology groups such as NetHope. He sits on several boards within IEEE, actively promotes IPv6 adoption via different task forces, volunteers to teach networking classes in third-world countries, and promotes STEM for women and minorities. In addition, Jeffry serves the public through his participation in conferences and standards bodies (IETF, IEEE); speaking at local and international events (Internet2, CANS, IPv6 Summits, AI/ML Symposiums, IEEE events, WALC, Cisco Live); contributing to and reviewing publications; and appearing as a guest in podcasts like IPv6 Buzz and Meraki Unboxed. He is a big promoter of technological change for the betterment of humanity.

About the Technical Reviewers

Dave Kounas has more than 26 years of experience in IT, including more than 17 years of networking experience designing and supporting enterprise networks. Dave worked in biotech, Wall Street finance, and manufacturing before joining Cisco in 2016. He joined the Meraki team in 2019 as a technical solutions architect, working closely with public sector and commercial customers to design reliable, high-performance networks.

Ryan Miles has more than 28 years of experience in the networking industry working for the U.S. Air Force, as an IT technical instructor, at a large healthcare provider, and for networking companies Cisco, Brocade, and Mist.

Over the past 15 years at Cisco, Ryan has worked as an enterprise networking consulting systems engineer focused on Cisco's wireless, switching, and security platforms. In 2016 Ryan joined the Meraki team as a senior technical solutions architect. Ryan has designed some of Meraki's largest and most complex global customer deployments. He is also a field advisor for the Meraki IoT product line of cameras and sensors, the Cloud Dashboard Platform, and for Cisco's broader Networking Experiences portfolio.

Kyle Murdock, CCIE R&S No. 2455, is a technical solutions architect for Meraki. During his 27 years at Cisco he has held many roles, including TAC engineer and team lead, service provider advanced services engineer, service provider and commercial systems engineer, and now Meraki technical solutions architect. Kyle is passionate about cloud-managed networking and especially switching. Outside of work, he builds and launches high-power rockets and holds a TRA Level 2 certification.

Dedications

We would like to remember the late Gordon Hughes, a good friend who helped us unlearn and relearn STP in the new world; we miss you.

I want to express my deepest gratitude to those who played a crucial role in bringing this book to life. First and foremost, a heartfelt thank you to my family for their unwavering support throughout the entire two-year writing process. Your encouragement has been my inspiration, and I am grateful for the steadfast belief you've shown in this endeavor.

A special appreciation goes to Mike Woolley and his family, who believed in this project. Thank you for the wonderful partnership and your commitment to deadlines; you have been the harshest critic of our writing standards and have been crucial in keeping us grounded and ensuring the timely delivery of this project.

I extend my thanks to Medi for your invaluable contribution in elevating the quality of the content. Your dedication has truly made a difference.

To Jeffry, your wisdom has played a vital role in defining the overall framework of this book. Thank you for sharing your insights and contributing to the depth of this work.

To all those who have otherwise supported and contributed to this book, thank you. Your belief, partnership, and wisdom have shaped this project, and I am genuinely grateful for each one of you.

—*Arun Paul*

I would like to dedicate this book to all my friends and family who supported us and put up with everything while writing this book.

To my wife Sara, thank you for putting up with the moments of stress and late nights as we navigated the not-as-simple-as-it-seems process of taking an idea and actually making a book out of it while also moving halfway across the country. Your loving support and understanding made immeasurable contributions to our success.

To the rest of my family and friends, I promise I will have more free time now. Thank you all for your support and curiosity about the project; your interest and support helped to fuel the fire and keep driving us to completion.

And to my fellow authors:

Arun, thank you for coming up with the initial idea and inviting me to partner with you early on. You never lost faith in the project and what it could be, even when it felt like it was all falling apart. Your vision accompanied by unending faith and optimism made all the difference.

Medi, thank you for your solutions expertise and wealth of knowledge you allowed us to tap into. Your contributions helped solidify the scope of this book and enable more approachable solutions while saving us a lot of additional research.

Jeffry, your perspective and input provided valuable insight into different approaches and solutions, as well as helping to define the content layout and flow that would evolve into our working template for multiple chapters of content. This book would look very different if it weren't for your input early on.

—*Mike Woolley*

First, I want to recognize our families for putting up with us for being so many times in front of a computer. This is time we will never get back, but their unwavering love and support allowed us to cope. Second, I thank our friends, managers, and leaders for encouraging us to experiment, try something new, and cheering us on.

Next, I want to thank those before us who created the industry of the Internet that has forever transformed the way we live, work, and create. They inspired the generation that we are part of. Now, it is up to us to inspire the next generation by making technology easier to tinker with and use for good.

I am thankful for my fellow co-authors for driving our mission and making it come to reality. Any one of us alone would be able to do it; however, collectively, the ingredients for completing something useful in a timely manner was possible only as a team. Arun was our passion, Woolley our coach, and Medi our vision. I am especially thankful for Arun and Woolley taking our technical depth and putting it into practical words, thereby fulfilling our hopes and dreams to democratize technology for all.

Finally, it is not every day that four people from different walks of life with diverse careers, experiences, and personal backgrounds come together to attempt something outside their comfort zone, i.e., writing. Contributing to writing a book is no easy feat. However, I would not trade the hours spent for anything because of the weekly camaraderie it created among us. Sometimes it served to destress us from our daily routine; other times it forced us to keep the creative muscle active; on many occasions, we solved technical problems we were facing in our day jobs; and other times, it simply allowed for laughs. At the end of the day, it is not about the technology but the human connections it creates. Thank you, Arun, Woolley, and Medi for this journey.

—*Jeffry Handal*

Acknowledgments

Many people helped contribute to this book in one way or another, and our sincere thanks goes out to each and every one of you no matter how large your contribution. Particularly, we acknowledge all of our colleagues at Meraki and Cisco, without whom we wouldn't have had much to write about.

A special thanks to the following people, without whom this book would not have been written:

- **Brett Bartow** and **Ellie Bru:** Your guidance and patience as we navigated the writing process was invaluable, and without you, we certainly never would have made our way to the end.
- **Denise Donohue:** A guiding mentor and the driving force behind the realization of this book. Thank you for pushing us to pursue the idea in the first place and helping wrap our heads around the process that would eventually lead to the completion of the project.
- **Kyle Murdock** and **Benton Heles** (MS Ninjas), **Dave Kounas** (MR Ninja), **Chad Yates** (MX Ninja), **Larry Woods**, and **Ryan Miles** (IoT Ninjas): Your domain expertise and valuable feedback on our writing styles significantly contributed to elevating the quality of our work.
- A special shout-out to **Craig Stork**, Cisco SA, for his guidance and assistance with ISE integration.
- And our official, unofficial consultant, **Varughese Cherian**, who jumped in and wholeheartedly assisted us in our time of need.

Contents at a Glance

Foreword xxii

Introduction xxiv

Part I Knowledge Is Power: Understanding the Cloud Architecture

Chapter 1 Cisco Meraki Cloud Architecture Basics 1

Chapter 2 Building the Dashboard 11

Part II Building a Scalable Foundation with Dashboard

Chapter 3 The Meraki Admin Experience 37

Chapter 4 Automating the Dashboard 59

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

Chapter 5 MX and MG Best Practices 83

Chapter 6 MX SD-WAN Best Practices 127

Part IV The Ultimate Cloud-Managed Access Layer

Chapter 7 Meraki Switching Design and Recommendations 145

Chapter 8 Meraki Wireless Best Practices and Design 195

Part V The Environment: The Next Frontier

Chapter 9 MV Security and MT (IoT) Design 239

Appendix A Cisco Meraki Licensing 303

Index 309

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
Automated API-based Organization Status 73
Automated MR Naming Based on Upstream Switch 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
Hub Versus Spoke 100

NAT Traversal 100

Hub and Spoke Recommendations 101

Sizing It Right 101

Hub Prioritization 102

Full Tunnel Versus Split Tunnel 102

Advanced Configurations 103

Monitoring Your Deployment 104

Meraki Insight 104

Web Application Health 105

WAN Health 108

VoIP Health 108

Insight Alerts 109

ThousandEyes Integration 110

Monitoring VPN 110

Reviewing Dashboard Alerts 112

Alert Hub 112

Organization Alerts 113

Threat Assessment on Meraki Dashboard 114

Security Center 115

Most Prevalent Threats 115

Most Affected Clients 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

Global Preference Policy 135

Basic Load Balancing Policy 136

Basic Policy-Based Routing 137

Performance-Based DPS 137

Policy Routing with Performance-Based DPS 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

VLAN Deployment 154

Using Native VLAN 1 155

Planning QoS 156

Fine-Tuning STP in a Hybrid Environment 156

Tags to Optimize Deployment 157

MTU Recommendation 158

Connecting Trunk Ports 158

Connecting MR Access Points 158

Layer 3 Best Practices 159

OSPF Best Practices 159

Multicast Best Practices 160

Securing Layer 2 Operations 160

Infrastructure Security 160

DHCP Snooping 161

Storm Control 161

Dynamic ARP Inspection 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
Ping 187
Packet Capture 188
MTR 189
MAC Forwarding Table 190
Cable Testing 190
Cycle Port 191
Wake-on-LAN 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

Roaming Domains 219

Layer 2 Domains 220

Layer 3 Domains 221

Defining DHCP Scope 221

Security Features and Wireless Security Best Practices 222

Air Marshal 222

Traffic Segregation and Access Control 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

Roaming Analytics 232

Client Overview 232

Client Details 234

Client Timeline 234

Access Point Timeline 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

MV Video Architecture 240

Ensuring Security 241

Built-in Analytics 241

Designing with Purpose: Building an Effective Surveillance System 242

Planning Camera Mounting Options and Accessories 243

Technology Considerations 244

Lens Types 244

Field of View 244

Resolution 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

General Network Considerations 247

Considerations for Wired Connections 248

Considerations for Wireless Connections 248

Building an Optimized Camera System 249

Defining Camera Names and Tags 249

Defining Camera Administrators 249

Dashboard-Defined Camera-only Administrators 250

Role-Based Camera Permissions for SAML/SSO 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

Assigning Camera Profiles 261

Manual Camera Configurations 261

Recording in Low Light 262

Camera Motion Alerts 263

Fine-Tuning Camera Alerts 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

Exporting Video 276

Working with Cloud Archive 278

Accessing Video Event Logs 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

MT12—Water/Leak Sensor 287

MT20—Door Sensor 288

MT40—Smart Power Controller 289

Environmental Monitoring 289

MT11—Cold Storage Sensor 289

Temperature, Humidity, and Air Quality Sensors 291

MT30—Smart Automation Button 293

Smart Button Automation 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

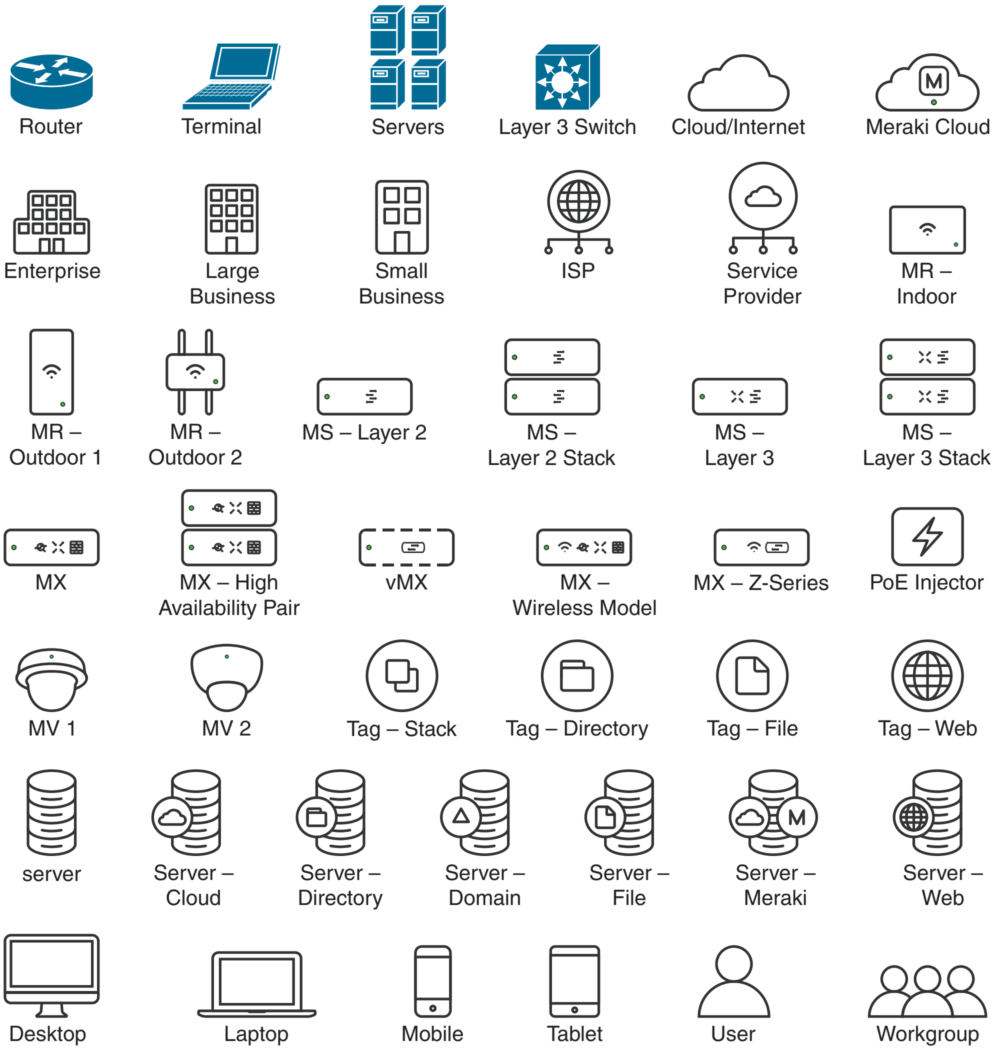
Monitoring BLE Signal Strength 300

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

Icons Used in This Book



Reader Services

Register your copy at www.ciscopress.com/title/9780138167578 for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.ciscopress.com/register and log in or create an account*. Enter the product ISBN 9780138167578 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Foreword

The State of Work

Work is no longer a physical place you go to. While the concept is not new, we knew we would eventually get there in the distant future. However, through a series of world events and accelerated by the pandemic of the 2020s, the adoption curve[1] of work from anywhere went from early adopters to late majority in a span of a few weeks. With the pandemic being over, we have skipped back to the early majority. Despite that "setback," a few things are clear:

- New ways of defining work have emerged.
- Depending on the platforms leveraged, data from these new models of operating has created a baseline.
- The IT world has undergone a transformation in front of our very eyes.

Let's unpack the above observations a little more. What is work? Work, as defined by the physics world, means the transfer of energy from applying a force to create displacement.[2] Putting that in the digital context, work is the means (force) by which we advance business objectives (energy measure) to obtain outcomes (displacement). How we get to those outcomes is not defined by a place. This is only possible because of pervasive, fast connectivity. Despite having a large swath of Earth's population not enjoying this kind of connectivity, the world economies are keeping an eye on this to bridge the gap with the expectation of pushing forward the next economic revolution that will increase human productivity.

The unstated unknown in all this is the central role the information communications technology industry and professionals will play in this transformation. Central to this theme is the digital adaptation to the analog world we had been used to operating. With digital comes data. With data comes new insights, informed decision-making, and expanded visibility into what we can do. How do we manage it all? Do we need a platform?

The Platform Solution

IT engineers are turning into data managers without even knowing it. We would even dare to say this has been the case forever. When we troubleshoot a problem, we are creating data or, viewed differently, gathering data from where it exists, processing it, and then making decisions to get to a resolution in a very manual way. The downsides of the process are that investments have to be made in the tooling required to be effective, and the experience of the person consuming the data matters. At the end of the day, this all translates into a time equation. Fast is not fast enough. Therefore, we need to evolve our approach into a platform-driven methodology for data management.

[1] https://en.wikipedia.org/wiki/Technology_adoption_life_cycle
[2] https://www.britannica.com/science/work-physics

You are about to read a book that will challenge the ways you have done things in networking. Realize you are leaving your comfort zone and pursuing new horizons to improve your "time equation" problem. You seek the utopia we have always wanted, which is end-to-end control, management, and visibility of operations. For that, a platform-thinking mindset must emerge. The difference between today's platforms and those of the not-too-distant future will be more data being gathered with automated processing to make a decision to resolve a problem or enable an outcome. The question is, does the platform you use have the ability to evolve with you into this future?

In this book, the authors plan to show that what Cisco has built with the Meraki platform is an effective tool to "manage" data and get to outcomes quicker—without the complexity. In other words, it is a platform for automation that is growing to include more than just traditional core networking. The Meraki platform is expanding to include physical security and IoT, and that is only the beginning. As we add an IP to more things, it just means it is another data source we can use to enrich our decision-making.

As you peruse these pages, think of the possibilities, the what-ifs you would solve within the confines of your operation. Having a platform challenges you to tackle a problem, build a solution within the constraints of the system to produce a desired outcome. Embrace the design, build, optimize approach that is deeply rooted in the data-rich foundation of the Meraki platform. Embrace the change. That is the Meraki way.

—Jeffry Handal

Introduction

A founding concept of Meraki was the idea of making networking simple. That goal is something Meraki still strives to achieve throughout all its products to this day. This book was conceived with that concept in mind and has been organized into chapters of related sections that begin with explaining the overarching organization and operation of the Cisco Meraki cloud-managed platform and gradually move toward more general design philosophy and use cases for the Meraki cloud platform.

The goal of this book is to help provide a better understanding of cloud-based management with Meraki devices and highlight the operational and administrative differences between a cloud-managed Meraki network and a more traditional network.

Topics covered by this book include the general organization and operation of the Meraki cloud, the basics of administering a network within the Meraki Dashboard, how Meraki can be integrated and automated with non-Meraki tools and services, as well as some Meraki-specific best practices. We will also provide an overview of what a day in the life of an administrator of a Meraki-based platform might look like, including monitoring an existing deployment and how the cloud platform assists in identifying and troubleshooting potential issues more easily.

Whenever referring to a page in the Dashboard, we use a standard convention to indicate the appropriate navigation menu options in the Dashboard to reach the indicated page. For example, if the navigation path is presented as **Security & SD-WAN > SD-WAN & Traffic Shaping > Uplink Selection**, that indicates to hover over the Security & SD-WAN navigation tab on the left, then select the link for **SD-WAN & Traffic Shaping** on the pop-out menu (see Figure 0-1), then scroll to the Uplink Selection section of the SD-WAN & Traffic Shaping page.

If the navigation path is presented as Organization > Change Log, that indicates to hover over the **Organization** tab on the left, then select the link for **Change Log** on the pop-out menu (see Figure 0-2).

All topics covered in this book are explored in more detail and depth in the Meraki official documentation, which you can access by visiting https://documentation.meraki.com. You can also find additional resources by visiting https://meraki.cisco.com or reaching out to one of Meraki's friendly sales representatives.

The Meraki Dashboard is a constantly evolving and changing entity, with new features and updates coming frequently. The information presented in this book is as accurate as possible at the time of writing. Given the required timelines and limitations involved in writing and publishing a book, there will inevitably be changes or updates that are unable to be included in the final copy. We have strived to cover the topics in this book in a way that allows the information presented to be applicable through future developments and evolutions of the Meraki platform as best as possible.

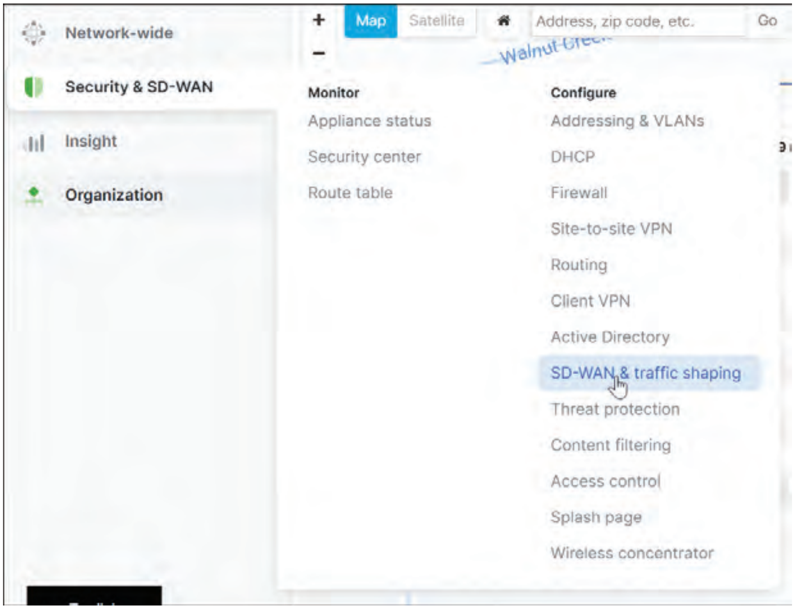


Figure 0-1 *Navigating to the Security & SD-WAN > SD-WAN & Traffic Shaping Page in a Dashboard Network*

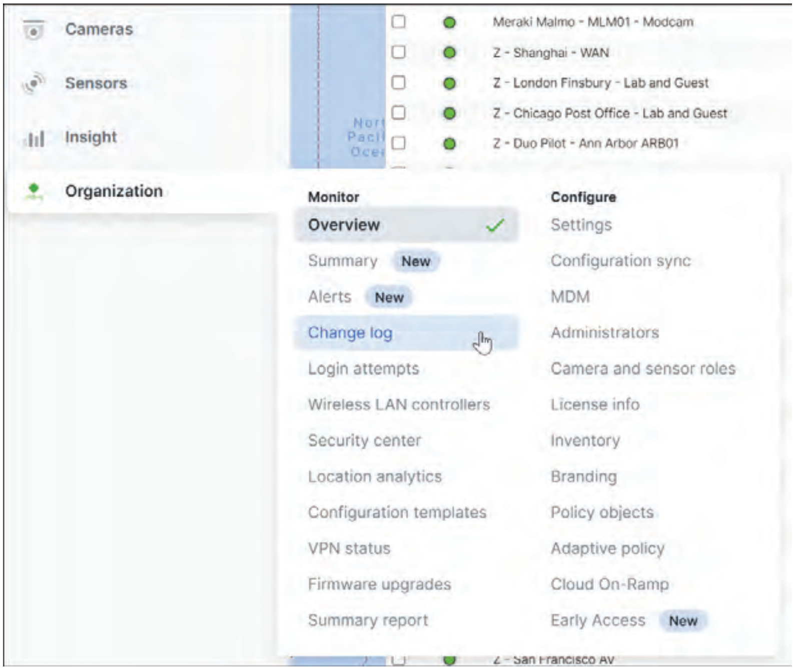


Figure 0-2 *Navigating to the Organization > Change Log Page in a Dashboard Organization*

Why Meraki?

When considering networking solutions, there are a myriad of available options from numerous different companies. In this sea of options, why should Meraki be the solution of choice?

After being acquired by Cisco in 2012, Meraki was quickly acknowledged as one of the fastest growing and most successful business entities within Cisco. It is now leading the way with Cisco's push for cloud-managed solutions through the design of Meraki's full stack of cloud-managed products, designed from the ground up for cloud management. By utilizing the power of the cloud for management, Meraki has been able to build a simple, scalable solution that allows for easy management through a single pane of glass: the Meraki Dashboard.

By utilizing the capabilities of the Dashboard, Meraki has enabled administrators to simplify their "day 1" operational deployments to near zero-touch, where a device can be configured on the cloud long before installation; then, once deployed, automatically come online and apply the configuration by just providing the device with an active Internet connection.

The Dashboard also plays a pivotal role to simplify "day 2" (daily operations) like maintenance and optimization of existing deployments. Capabilities such as cloud-based firmware management for all Meraki devices significantly reduce the amount of time and effort required to keep critical devices up to date with the latest firmware and security patches across platforms. An additional advantage of the cloud-based management design of the Dashboard is the ability to use APIs and web integrations to easily automate almost every feature of network, device, and even client management across the entire organization.

With these options and the focus on cloud management, the Meraki Dashboard also allows for a reduction in OPEX for customers, as the single pane of glass allows a single administrator to more easily monitor, manage, and troubleshoot multiple sites when compared to a more traditional deployment.

Supporting a Different Experience

Included with all Cisco Meraki licensing is access to Meraki's highly rated 24/7 support team. With multiple offices around the globe, Meraki Support is always ready and available to assist any Meraki customer at any time. Meraki Support strives to provide actual solutions to customer problems instead of focusing on ticket closure or call length metrics. In other words, Meraki Support engineers are dedicated to helping you solve your problem no matter how big or small.

A significant advantage of the cloud-based solutions offered by Meraki through the Dashboard is the ability for a Support engineer to work with the same views and data that are displayed to customers, reducing the back-and -forth exchanges traditionally needed to provide data and logging to Support for analysis. In many instances, Meraki Support directly gathers the necessary data directly from the Dashboard. This helps to significantly reduce troubleshooting time and mean time to resolution (MTR) for customer issues.

Meraki Support is also able to quickly diagnose and provide RMAs (return material authorizations) for covered devices, with the advantage of cloud monitoring to allow for early detection of certain issues before a device fails completely. This allows Meraki to alert customers of certain issues, such as a potential hardware failure, and begin the proactive replacement process before the device fails completely and causes a more significant impact.

An example of this ability in action is the clock component failures seen across the industry around 2017. This issue resulted from a faulty clock component commonly installed in devices across the industry that was discovered to fail prematurely after a period of operation, resulting in an inoperable device. Several Meraki hardware products were identified as containing the problematic component and, through the use of the Dashboard, Meraki was able to reach out and initiate a proactive replacement program for all customers using an affected device. This allowed the devices to be identified and proactively replaced before encountering significant issues resulting from the faulty clock component.

All Cisco Meraki RMAs are proactive, meaning that once the RMA is approved, a new device is immediately in the process of being express shipped to the destination to replace the failing or failed device before requiring the failed device to be shipped back. All replacement devices also include a free return shipping label to allow the failed device to be returned to Meraki at no cost.

Meraki devices are strategically placed in Cisco resource depots around the world to allow for advanced 4 hour or less RMAs through the purchase of additional advanced RMA coverage for mission-critical devices. When combined with Meraki's included limited lifetime warranty for most devices, Meraki provides excellent replacement ability to ensure that your networks stay up and running for as long as possible.

For the curious customer looking to get their hands on Meraki equipment to see if the Cisco Meraki platform is the right fit for their deployments, Meraki offers the ability to See/Try/Buy Meraki equipment through its Sales Trial programs. Sales Trials allow customers to work with a Cisco Meraki representative to determine what Meraki products would best fit the requirements of the deployment and allow them to trial real Meraki hardware in their own environment at no cost with the option to purchase the trial hardware or return the hardware back to Meraki at the end of the trial. Trials also include full access to Meraki Support resources to assist in troubleshooting any issues that may arise during the trial. This allows for trials to be leveraged in a more effective way within an actual environment as opposed to reviewing datasheets or observing performance in a controlled lab scenario. Thus, customers can make more informed purchasing decisions and feel confident in how the hardware will perform in their unique environment.

Meraki offers some clear advantages when compared to other, more traditional deployment solutions. If you are curious to learn more about how the topics previously mentioned are accomplished and what it looks like to work with the Meraki Dashboard and manage a Meraki network, read on to Chapter 1, which begins discussing the Meraki cloud architecture, how Meraki handles device-to-cloud communications, and how Meraki safely handles data in the cloud and between sites.

Who Should Read This Book?

This book is intended to provide an overview and general understanding of the experiences, products, and capabilities offered by the Cisco Meraki cloud platform at any scale. This book introduces each of Meraki's multiple cloud-managed solutions—MX appliances, MS switches, MR access points, MV cameras, and more—and provides helpful advice for planning or working with Meraki deployments, including more advanced tips and considerations for administrators who are planning for or working with very large or complex deployments.

While the primary audience for this book is IT professionals who are unfamiliar with Meraki and are looking to either learn more about how a Meraki solution might work in their environment or learn how to better work with an existing Meraki solution recently acquired, the content has been written with the intent of providing new and useful information to both those familiar and unfamiliar with the Meraki platform.

Special care has been taken to highlight numerous "Pro Tips" throughout the text, which are typically lesser known pieces of information or recommendations you won't find in any other documentation. These have been chosen and highlighted specifically based on the experiences of the authors while troubleshooting customer deployments and are intended to provide helpful assistance like pointing out commonly overlooked configuration steps, or alternate approaches or solutions that may not be immediately obvious. With information gathered from multiple decades' worth of combined experience, even the most seasoned network operator will likely find new information or approaches in this book for working with the Cisco Meraki platform.

Book Structure

The book is organized into five parts.

Part I: Knowledge Is Power: Understanding the Cloud Architecture

- **Chapter 1: Cisco Meraki Cloud Architecture Basics:** This chapter provides an introduction and overview of the Meraki cloud architecture, including the core hosting services around the world and how the Meraki organization structure works to enable powerful and secure cloud-managed solutions at any scale.
- **Chapter 2: Building the Dashboard:** This chapter goes into detail on the Meraki cloud organization structure, including covering the basic setup and configuration process of a new organization, such as defining administrators, creating networks, and claiming licenses and devices. It also shows how the Dashboard simplifies the workload of several common administrative tasks, such as creating and reviewing alerts or reports from within the Dashboard.

Part II: Building a Scalable Foundation with Dashboard

- **Chapter 3: The Meraki Admin Experience:** This chapter depicts a day in the life of a Meraki administrator. It explores using the Dashboard to check the overall health of the organization's network and make sure that all Meraki products are working securely. It also describes how to find and use the latest features in Meraki to keep your technology up to date. The chapter also explores ways to connect events from different products and network services to find problems more quickly. It is intended as a practical introductory guide for administrators to manage their network effectively using Meraki solutions.
- **Chapter 4: Automating the Dashboard:** This chapter is focused on using automation both within and outside the Meraki Dashboard to further reduce the management workload for a deployment. Topics range from using built-in Dashboard tools to generate reports and manage configuration at scale, to incorporating external solutions using Meraki's robust API support that enables automated deployment, configuration, and reporting abilities.

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

- **Chapter 5: MX and MG Best Practices:** This chapter introduces the primary functions of Meraki's security/WAN appliance series of devices and covers the basic and advanced security and routing features offered by these devices, including Meraki AutoVPN, AMP, content filtering, and basic traffic shaping. The chapter also touches on the MG line of cellular WAN uplinks offered by Meraki and provides recommendations for their practical deployment and operation.
- **Chapter 6: MX SD-WAN Best Practices:** This chapter is dedicated specifically to Meraki's advanced SD-WAN (software-defined wide area network) solution offered by the MX series of devices. Built over the AutoVPN solution discussed in Chapter 5, this chapter introduces Meraki's SD-WAN solution and guides customers in choosing between a basic policy and more advanced options, including application-specific metrics, to better fine-tune the traffic in their SD-WAN deployments.

Part IV: The Ultimate Cloud-Managed Access Layer

- **Chapter 7: Meraki Switching Design and Recommendations:** This chapter covers Meraki's switching product line and design best practices, including the new cloud-managed Catalyst switches. The chapter explains how the modern hybrid world of on-premises and cloud-managed switches benefits from the best of both worlds, while still achieving interoperability and cross-platform micro-segmentation capabilities. The chapter also covers how the Meraki Dashboard brings visibility into network-wide topology and operational visibility for both cloud-based and monitored Catalyst product lines.
- **Chapter 8: Meraki Wireless Best Practices and Design:** This chapter dives into the key aspects of designing, building, and optimizing with Meraki wireless access points, with a particular focus on converged hardware. It highlights the Wireless

Health features of Meraki, offering insights into how these features assist in identifying the root cause of issues. The chapter also explores the impact of AI-powered automation features in maintaining the wireless infrastructure at peak performance levels. It also covers the design principles behind achieving enterprise-grade roaming using Meraki wireless technology. This chapter provides a concise yet comprehensive guide to implementing best practices for a robust and efficient Meraki wireless network.

Part V: The Environment: The Next Frontier

- **Chapter 9: MV Security and MT (IoT) Design:** This chapter looks at Meraki's IoT technology and its unique architecture, which simplifies camera and IoT integration and operation. It discusses the various modes of access and ease of searching and retrieving footage from Meraki cameras on the Meraki platform as well as how Meraki's MT line of IoT devices can be deployed alongside MV cameras to provide additional monitoring and insights.

Appendix A: Meraki Licensing: This appendix is intended to provide a brief overview of the available Meraki licensing models, including their operation and how the differences between licensing models may impact your planning and operations, to help you ensure you choose the most appropriate licensing model for each deployment.

Figure Credits

Figure 9-10: Google LLC

Chapter 3

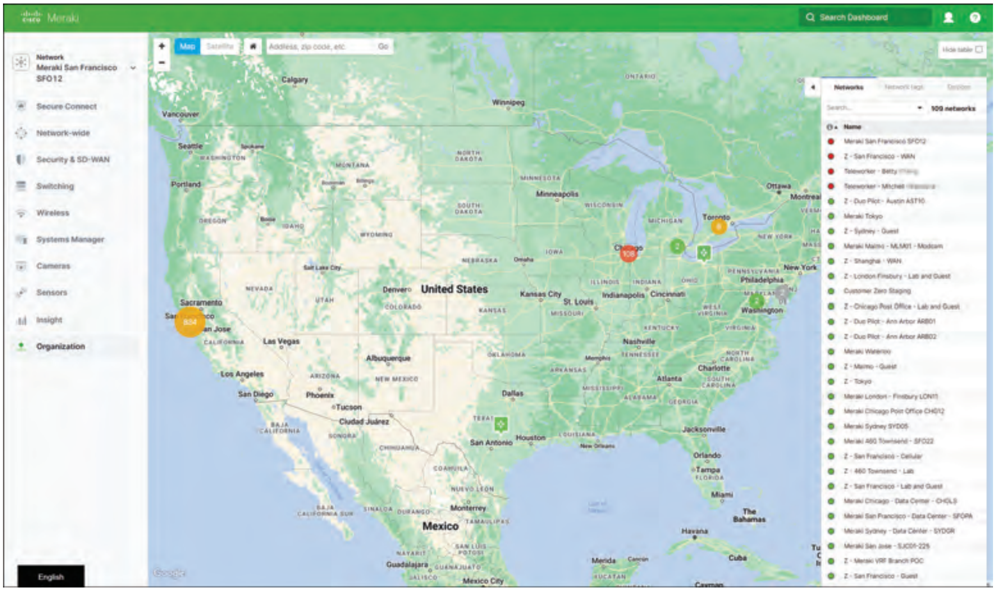
The Meraki Admin Experience

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.

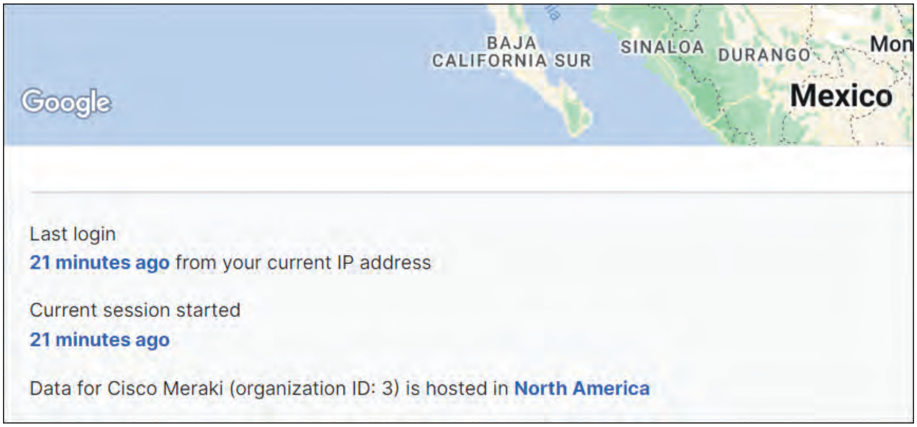
The Organization Overview page, shown in Figure 3-1, is the first page displayed after logging in or selecting an organization to work within. You also can navigate to it directly from the navigation pane on the left by selecting **Organization > Overview**.

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.



	Name
●	Meraki San Francisco SFO12
●	Z - San Francisco - WAN
●	Teleworker - Betty
●	Teleworker - Mitchell
●	Z - Duo Pilot - Austin AST10
●	Meraki Tokyo
●	Z - Sydney - Guest
●	Meraki Malmo - MLM01 - Modcam
●	Z - Shanghai - WAN
●	Z - London Finsbury - Lab and Guest
●	Customer Zero Staging
●	Z - Chicago Post Office - Lab and Guest
●	Z - Duo Pilot - Ann Arbor ARB01
●	Z - Duo Pilot - Ann Arbor ARB02
●	Meraki Waterloo
●	Z - Malmo - Guest
●	Z - Tokyo
●	Meraki London - Finsbury LON11
●	Meraki Chicago Post Office CHO12
●	Meraki Sydney SYD05
●	Meraki 460 Townsend - SFO22
●	Z - San Francisco - Cellular
●	Z - 460 Townsend - Lab
●	Z - San Francisco - Lab and Guest
●	Meraki Chicago - Data Center - CHOLS
●	Meraki San Francisco - Data Center - SFOPA
●	Meraki Sydney - Data Center - SYDGR
●	Meraki San Jose - SJC01-225
●	Z - Meraki VRF Branch POC
●	Z - San Francisco - Guest

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



Last login
21 minutes ago from your current IP address

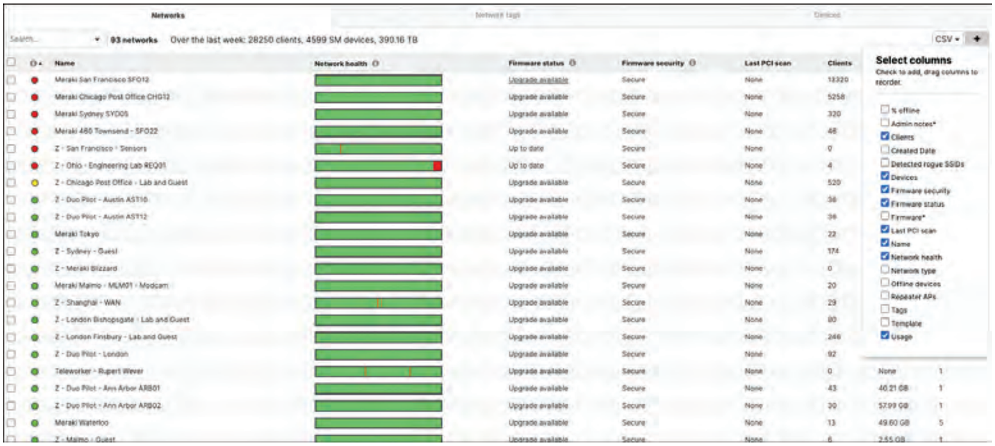
Current session started
21 minutes ago

Data for Cisco Meraki (organization ID: 3) is hosted in North America

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.



Networks | Network tags | Devices

Search... ▾ **93 networks** Over the last week: 28250 clients, 4599 SM devices, 390.16 TB

CSV ▾ **+**

□	●	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 480 Townsend - SFO22		Upgrade available	Secure	None	48		
□	●	Z - San Francisco - Sensors		Up to date	Secure	None	0		
□	●	Z - Ohio - Engineering Lab REQ01		Up to date	Secure	None	4		
□	●	Z - Chicago Post Office - Lab and Guest		Upgrade available	Secure	None	520		
□	●	Z - Duo Pilot - Austin AST10		Upgrade available	Secure	None	38		
□	●	Z - Duo Pilot - Austin AST12		Upgrade available	Secure	None	36		
□	●	Meraki Tokyo		Upgrade available	Secure	None	22		
□	●	Z - Sydney - Guest		Upgrade available	Secure	None	174		
□	●	Z - Meraki Blizzard		Upgrade available	Secure	None	0		
□	●	Meraki Malmo - MLM01 - Modcam		Upgrade available	Secure	None	20		
□	●	Z - Shanghai - WAN		Upgrade available	Secure	None	29		
□	●	Z - London Bishopsgate - Lab and Guest		Upgrade available	Secure	None	80		
□	●	Z - London Finsbury - Lab and Guest		Upgrade available	Secure	None	246		
□	●	Z - Duo Pilot - London		Upgrade available	Secure	None	92		
□	●	Teleworker - Rupert Wever		Upgrade available	Secure	None	0	None	1
□	●	Z - Duo Pilot - Ann Arbor ARB01		Upgrade available	Secure	None	43	40.21 GB	1
□	●	Z - Duo Pilot - Ann Arbor ARB02		Upgrade available	Secure	None	30	57.99 GB	1
□	●	Meraki Waterloo		Upgrade available	Secure	None	13	49.60 GB	5
□	●	Z - Malmo - Guest		Upgrade available	Secure	None	6	2.55 GB	1

Select columns
Check to add, drag columns to reorder.

- □ % offline
- □ Admin notes*
- ☑ Clients
- □ Created Date
- □ Detected rogue SSIDs
- ☑ Devices
- ☑ Firmware security
- ☑ Firmware status
- □ Firmware*
- ☑ Last PCI scan
- ☑ Name
- ☑ Network health
- □ Network type
- □ Offline devices
- □ Repeater APs
- □ Tags
- □ Template
- ☑ Usage

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

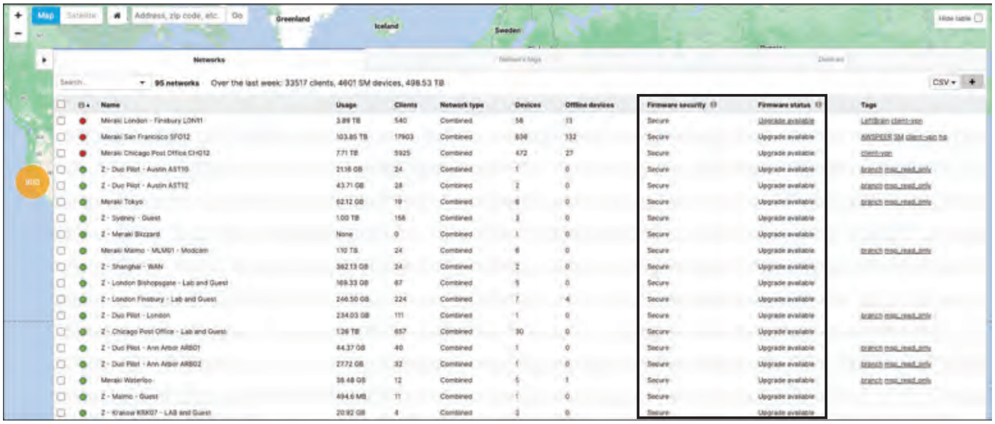
For example, to view firmware-related statuses for each network in the organization, click the **+** sign and select the **Firmware Security** and **Firmware Status** options to add the corresponding columns to the table.

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.



Networks

Search... 95 networks Over the last week: 33517 clients, 4601 SM devices, 498.53 TB

CSV ▾ +

☐		Name	Usage	Clients	Network type	Devices	Offline devices	Firmware security	Firmware status	Tags
☐	●	Meraki London - Finsbury LON11	3.89 TB	540	Combined	58	13	Secure	Upgrade available	LeftBrain client-vpn
☐	●	Meraki San Francisco SFO12	103.85 TB	17903	Combined	836	132	Secure	Upgrade available	AWSPEER SM client-vpn hq
☐	●	Meraki Chicago Post Office CHG12	7.71 TB	5925	Combined	472	27	Secure	Upgrade available	client-vpn
☐	●	Z - Duo Pilot - Austin AST10	21.18 GB	24	Combined	1	0	Secure	Upgrade available	branch msp_read_only
☐	●	Z - Duo Pilot - Austin AST12	43.71 GB	28	Combined	2	0	Secure	Upgrade available	branch msp_read_only
☐	●	Meraki Tokyo	62.12 GB	19	Combined	6	0	Secure	Upgrade available	branch msp_read_only
☐	●	Z - Sydney - Guest	1.00 TB	158	Combined	3	0	Secure	Upgrade available	
☐	●	Z - Meraki Blizzard	None	0	Combined	1	0	Secure	Upgrade available	
☐	●	Meraki Malmo - MLM01 - Modcam	1.10 TB	24	Combined	6	0	Secure	Upgrade available	branch msp_read_only
☐	●	Z - Shanghai - WAN	362.13 GB	24	Combined	2	0	Secure	Upgrade available	
☐	●	Z - London Bishopsgate - Lab and Guest	169.33 GB	67	Combined	5	0	Secure	Upgrade available	
☐	●	Z - London Finsbury - Lab and Guest	246.50 GB	224	Combined	7	4	Secure	Upgrade available	
☐	●	Z - Duo Pilot - London	234.03 GB	111	Combined	1	0	Secure	Upgrade available	branch msp_read_only
☐	●	Z - Chicago Post Office - Lab and Guest	1.26 TB	657	Combined	30	0	Secure	Upgrade available	
☐	●	Z - Duo Pilot - Ann Arbor ARB01	44.37 GB	40	Combined	1	0	Secure	Upgrade available	branch msp_read_only
☐	●	Z - Duo Pilot - Ann Arbor ARB02	27.72 GB	32	Combined	1	0	Secure	Upgrade available	branch msp_read_only
☐	●	Meraki Waterloo	38.48 GB	12	Combined	5	1	Secure	Upgrade available	branch msp_read_only
☐	●	Z - Malmo - Guest	494.6 MB	11	Combined	1	0	Secure	Upgrade available	
☐	●	Z - Krakow KRK07 - LAB and Guest	20.92 GB	4	Combined	3	0	Secure	Upgrade available	

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

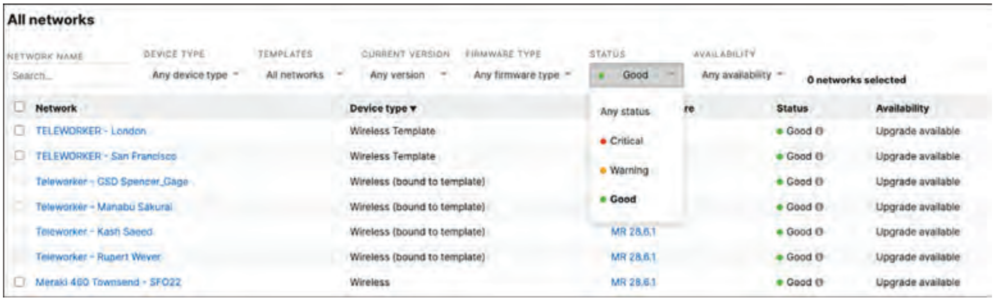
The Organization Overview page provides quick, organization-wide visibility and easily accessible notifications related to firmware security and current upgrade status for each network within the organization.

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.



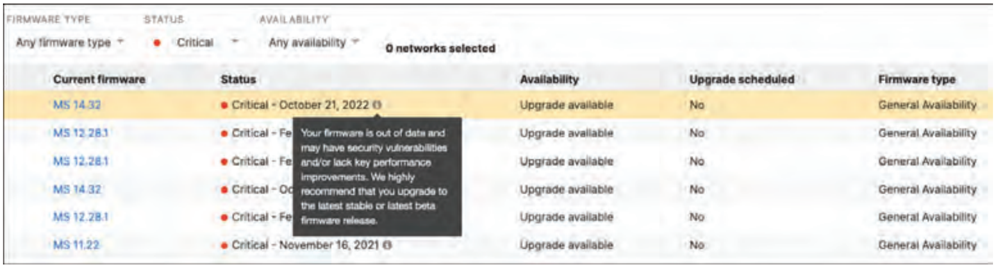
All networks

NETWORK NAME: Search...
DEVICE TYPE: Any device type
TEMPLATES: All networks
CURRENT VERSION: Any version
FIRMWARE TYPE: Any firmware type
STATUS: ● Good
AVAILABILITY: Any availability
0 networks selected

☐	Network	Device type ▾	re	Status	Availability
☐	TELEWORKER - London	Wireless Template		● Good	Upgrade available
☐	TELEWORKER - San Francisco	Wireless Template		● Good	Upgrade available
	Teleworker - CSD Spencer_Gage	Wireless (bound to template)		● Good	Upgrade available
	Teleworker - Manabu Sakurai	Wireless (bound to template)		● Good	Upgrade available
	Teleworker - Kash Saeed	Wireless (bound to template)	MR 28.6.1	● Good	Upgrade available
	Teleworker - Rupert Wever	Wireless (bound to template)	MR 28.6.1	● Good	Upgrade available
☐	Meraki 460 Townsend - SFO22	Wireless	MR 28.6.1	● Good	Upgrade available

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.

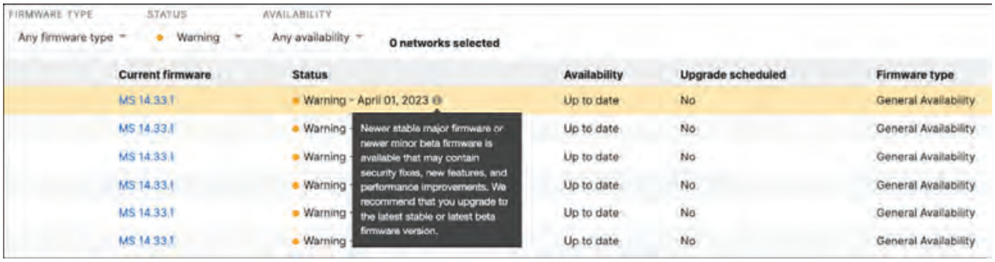


FIRMWARE TYPE: Any firmware type ▾ STATUS: ● Critical ▾ AVAILABILITY: Any availability ▾ **0 networks selected**

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 - Fe	Upgrade available	No	General Availability
MS 12.28.1	● Critical - Fe	Upgrade available	No	General Availability
MS 14.32	● Critical - Oc	Upgrade available	No	General Availability
MS 12.28.1	● Critical - Fe	Upgrade available	No	General Availability
MS 11.22	● Critical - November 16, 2021 ⓘ	Upgrade available	No	General Availability

Your firmware is out of date and may have security vulnerabilities and/or lack key performance improvements. We highly recommend that you upgrade to the latest stable or latest beta firmware release.

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



FIRMWARE TYPE: Any firmware type ▾ STATUS: ● Warning ▾ AVAILABILITY: Any availability ▾ **0 networks selected**

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	Up to date	No	General Availability
MS 14.33.1	● Warning	Up to date	No	General Availability
MS 14.33.1	● Warning	Up to date	No	General Availability
MS 14.33.1	● Warning	Up to date	No	General Availability
MS 14.33.1	● Warning	Up to date	No	General Availability

Newer stable major firmware or newer minor beta firmware is available that may contain security fixes, new features, and performance improvements. We recommend that you upgrade to the latest stable or latest beta firmware version.

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

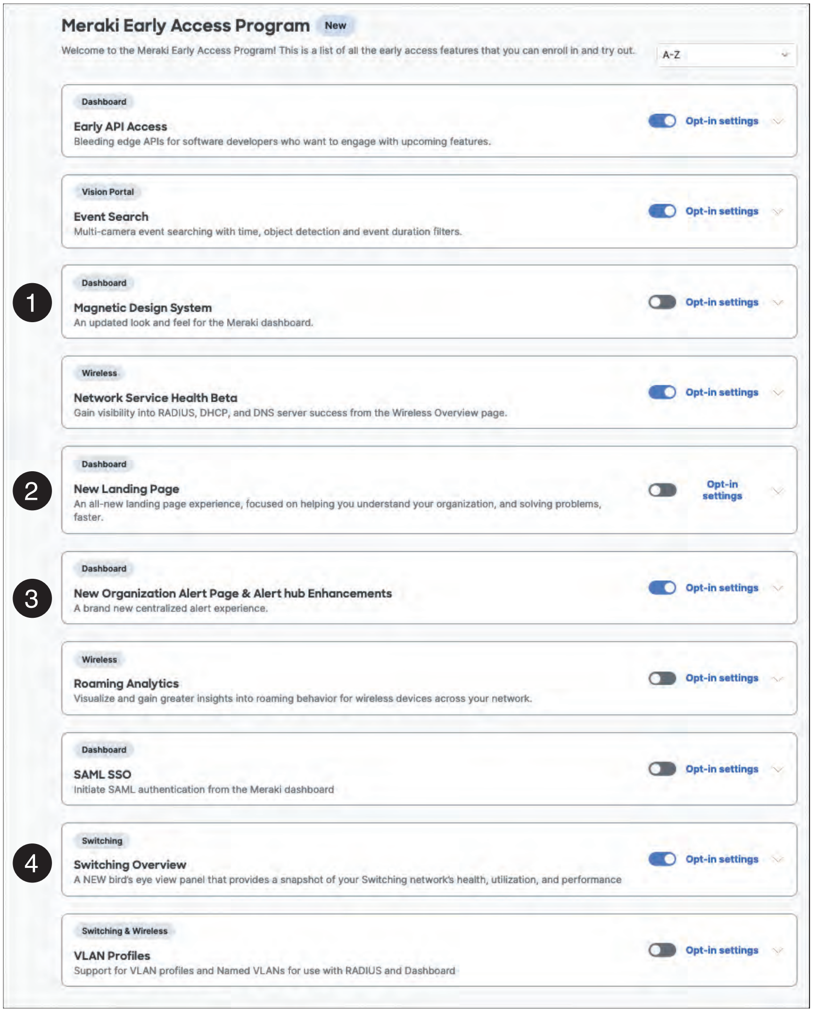
Meraki is continuously working to enhance the design of the Dashboard to improve performance and usability for its customers. This effort includes developing new features and pages to improve the Dashboard experience. You can explore the latest features and pages opting in to the Dashboard Early Access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



Meraki Early Access Program New

Welcome to the Meraki Early Access Program! This is a list of all the early access features that you can enroll in and try out. A-Z

Dashboard
Early API Access
Bleeding edge APIs for software developers who want to engage with upcoming features.
● Opt-in settings

Vision Portal
Event Search
Multi-camera event searching with time, object detection and event duration filters.
● Opt-in settings

Dashboard
Magnetic Design System
An updated look and feel for the Meraki dashboard.
○ Opt-in settings

Wireless
Network Service Health Beta
Gain visibility into RADIUS, DHCP, and DNS server success from the Wireless Overview page.
● Opt-in settings

Dashboard
New Landing Page
An all-new landing page experience, focused on helping you understand your organization, and solving problems, faster.
○ Opt-in settings

Dashboard
New Organization Alert Page & Alert hub Enhancements
A brand new centralized alert experience.
● Opt-in settings

Wireless
Roaming Analytics
Visualize and gain greater insights into roaming behavior for wireless devices across your network.
○ Opt-in settings

Dashboard
SAML SSO
Initiate SAML authentication from the Meraki dashboard
○ Opt-in settings

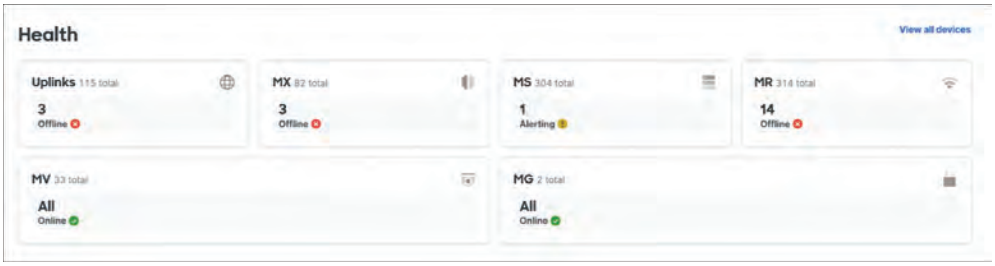
Switching
Switching Overview
A NEW bird's eye view panel that provides a snapshot of your Switching network's health, utilization, and performance
● Opt-in settings

Switching & Wireless
VLAN Profiles
Support for VLAN profiles and Named VLANs for use with RADIUS and Dashboard
○ Opt-in settings

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**.



Health

View all devices

Uplinks 115 total
3
Offline ✕

MX 82 total
3
Offline ✕

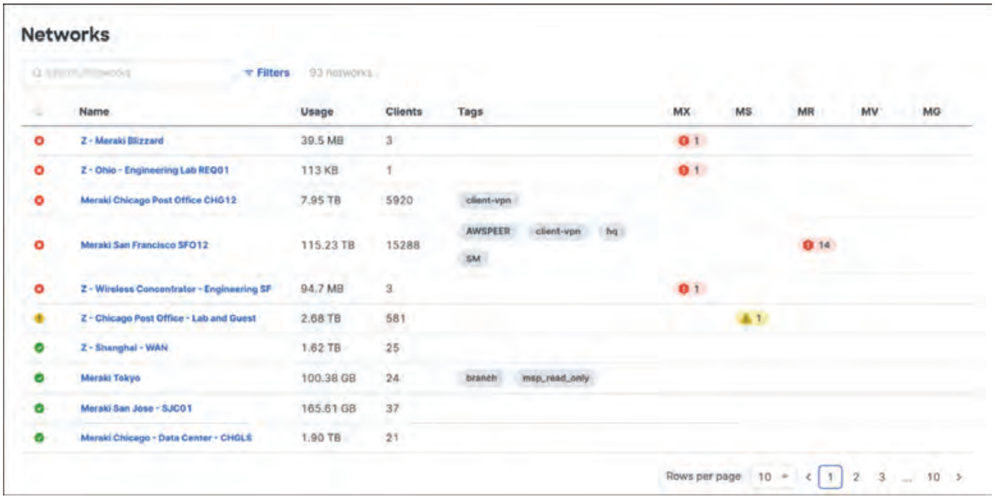
MS 304 total
1
Alerting !

MR 314 total
14
Offline ✕

MV 33 total
All
Online ✓

MG 2 total
All
Online ✓

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



Networks

Filters 93 networks

	Name	Usage	Clients	Tags	MX	MS	MR	MV	MG
✕	Z - Meraki Blizzard	39.5 MB	3		! 1				
✕	Z - Ohio - Engineering Lab REQ01	113 KB	1		! 1				
✕	Meraki Chicago Post Office CHG12	7.95 TB	5920	client-vpn					
✕	Meraki San Francisco SFO12	115.23 TB	15288	AWSPEER client-vpn hq SM			! 14		
✕	Z - Wireless Concentrator - Engineering SF	94.7 MB	3		! 1				
!	Z - Chicago Post Office - Lab and Guest	2.68 TB	581			⚠ 1			
✓	Z - Shanghai - WAN	1.62 TB	25						
✓	Meraki Tokyo	100.38 GB	24	branch msp_read_only					
✓	Meraki San Jose - SJC01	165.61 GB	37						
✓	Meraki Chicago - Data Center - CHGLS	1.90 TB	21						

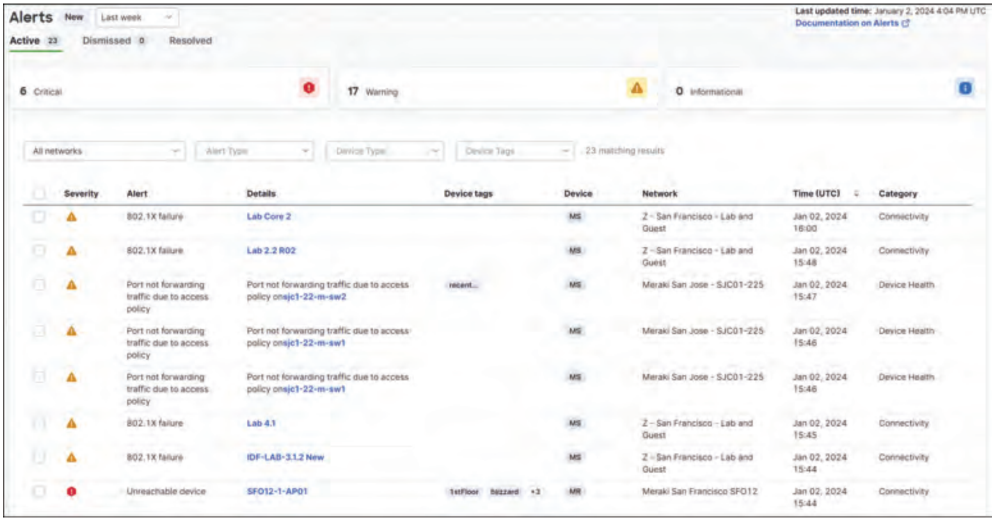
Rows per page 10 ‹ 1 2 3 ... 10 ›

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.



Alerts New Last week

Last updated time: January 2, 2024 4:04 PM UTC
Documentation on Alerts

Active 23 Dismissed 0 Resolved

6 Critical | 17 Warning | 0 Informational

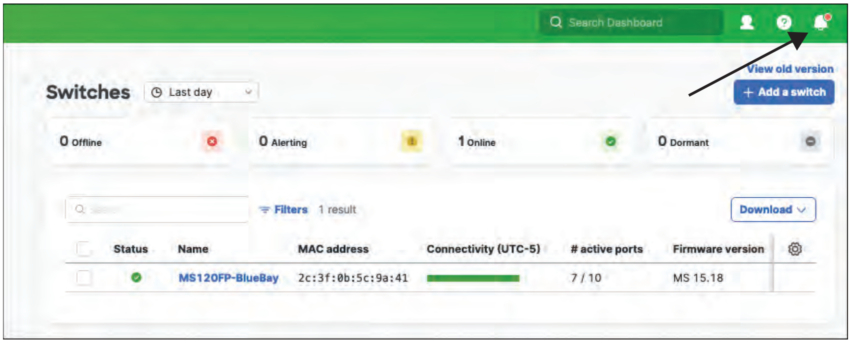
All networks | Alert Type | Device Type | Device Tags | 23 matching results

Severity	Alert	Details	Device tags	Device	Network	Time (UTC)	Category
▲	802.1X failure	Lab Core 2		MS	Z - San Francisco - Lab and Guest	Jan 02, 2024 16:00	Connectivity
▲	802.1X failure	Lab 2.2 R02		MS	Z - San Francisco - Lab and Guest	Jan 02, 2024 15:48	Connectivity
▲	Port not forwarding traffic due to access policy	Port not forwarding traffic due to access policy onsjc1-22-m-sw2	recent...	MS	Meraki San Jose - SJC01-225	Jan 02, 2024 15:47	Device Health
▲	Port not forwarding traffic due to access policy	Port not forwarding traffic due to access policy onsjc1-22-m-sw1		MS	Meraki San Jose - SJC01-225	Jan 02, 2024 15:46	Device Health
▲	Port not forwarding traffic due to access policy	Port not forwarding traffic due to access policy onsjc1-22-m-sw1		MS	Meraki San Jose - SJC01-225	Jan 02, 2024 15:46	Device Health
▲	802.1X failure	Lab 4.1		MS	Z - San Francisco - Lab and Guest	Jan 02, 2024 15:45	Connectivity
▲	802.1X failure	IDF-LAB-3.1.2 New		MS	Z - San Francisco - Lab and Guest	Jan 02, 2024 15:44	Connectivity
●	Unreachable device	SFO12-1-AP01	1stFloor bizzard +3	MR	Meraki San Francisco SFO12	Jan 02, 2024 15:44	Connectivity

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.



Switches Last day

0 Offline | 0 Alerting | 1 Online | 0 Dormant

Filters 1 result

Status	Name	MAC address	Connectivity (UTC-5)	# active ports	Firmware version
●	MS120FP-BlueBay	2c:3f:0b:5c:9a:41		7 / 10	MS 15.18

Figure 3-12 *The Alert Hub Notification Icon*

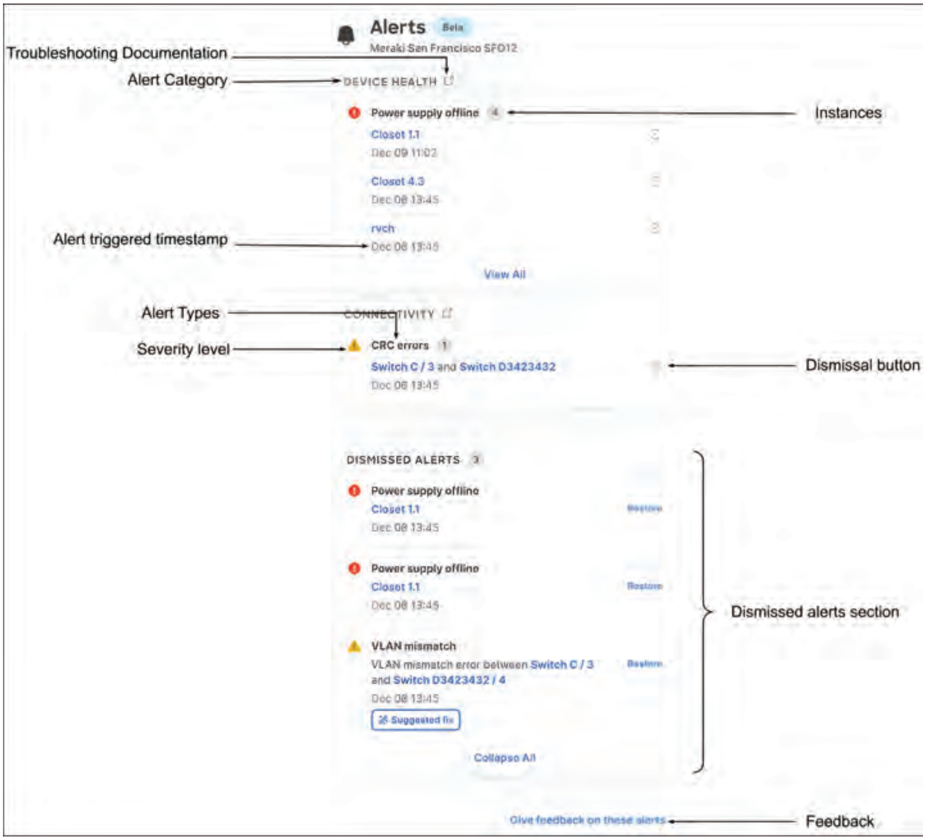
For more information on the new Organization Alerts page and Alert Hub, visit https://documentation.meraki.com and view the “Alerts” article.

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.



Alerts Beta
Meraki San Francisco SFO12

DEVICE HEALTH

Power supply offline 4
Closet 1.1
Dec 09 11:02

Closet 4.3
Dec 08 13:45

rvch
Dec 08 13:45

View All

CONNECTIVITY

CRC errors 1
Switch C / 3 and Switch D3423432
Dec 08 13:45

DISMISSED ALERTS 3

Power supply offline
Closet 1.1
Dec 08 13:45
Restore

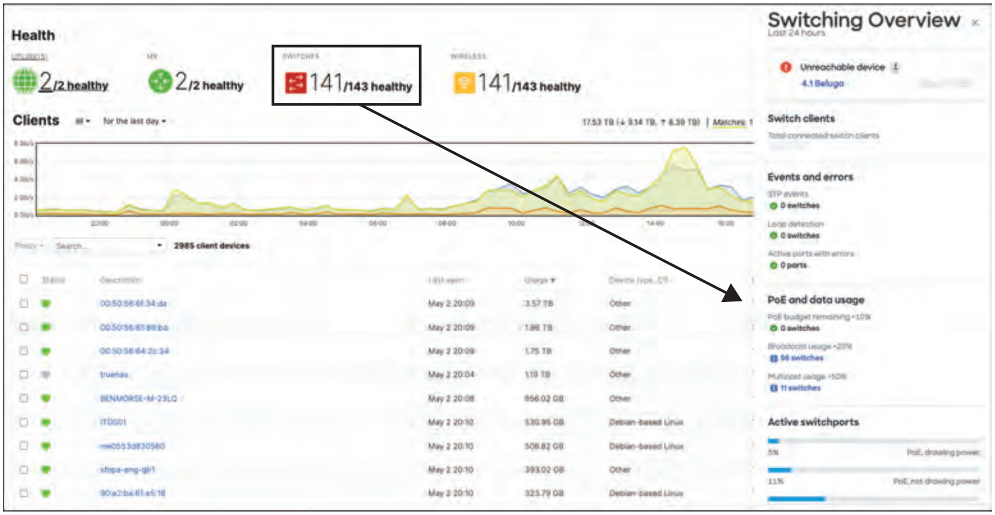
Power supply offline
Closet 1.1
Dec 08 13:45
Restore

VLAN mismatch
VLAN mismatch error between Switch C / 3 and Switch D3423432 / 4
Dec 08 13:45
Suggested fix
Restore

Collapse All

Give feedback on these alerts

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



☐	Status	Description	Last seen	Usage ▼	Device type...OS
☐	●	00:50:56:6f:34:da	May 2 20:09	3.57 TB	Other
☐	●	00:50:56:81:88:ba	May 2 20:09	1.98 TB	Other
☐	●	00:50:56:64:2c:34	May 2 20:09	1.75 TB	Other
☐	●	truenas	May 2 20:04	1.19 TB	Other
☐	●	BENMORSE-M-23LQ	May 2 20:08	856.02 GB	Other
☐	●	ITDS01	May 2 20:10	530.95 GB	Debian-based Linux
☐	●	mw0553d830560	May 2 20:10	506.82 GB	Debian-based Linux
☐	●	sfopa-eng-gl1	May 2 20:10	393.02 GB	Other
☐	●	90:e2:ba:61:e5:18	May 2 20:10	323.79 GB	Debian-based Linux

Switching Overview ×
Last 24 hours

Unreachable device 1
4.1 Beluga

Switch clients
Total connected switch clients

Events and errors
STP events
● 0 switches
Loop detection
● 0 switches
Active ports with errors
● 0 ports

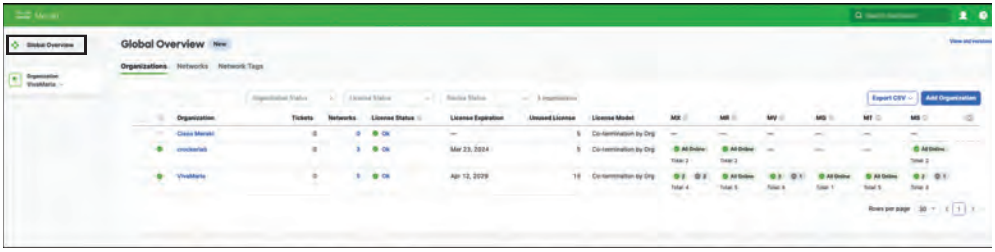
PoE and data usage
PoE budget remaining <10%
● 0 switches
Broadcast usage >20%
56 switches
Multicast usage >50%
11 switches

Active switchports
5% PoE, drawing power
11% PoE, not drawing power

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.



Organization	Tickets	Networks	License Status	License Expiration	Unused License	License Model	MX	MR	MV	MG	MT	MS
Cisco Meraki	0	0	● Ok	—	5	Co-termination by Org	—	—	—	—	—	—
crockerlab	0	3	● Ok	Mar 23, 2024	5	Co-termination by Org	● All Online Total 2	● All Online Total 2	—	—	—	● All Online Total 2
VivaMaria	0	5	● Ok	Apr 12, 2029	18	Co-termination by Org	● 2 ● 2 Total 4	● All Online Total 5	● 3 ● 1 Total 4	● All Online Total 1	● All Online Total 5	● 2 ● 1 Total 3

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.

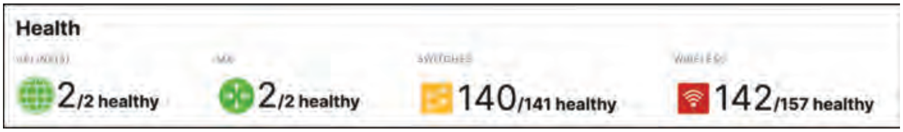
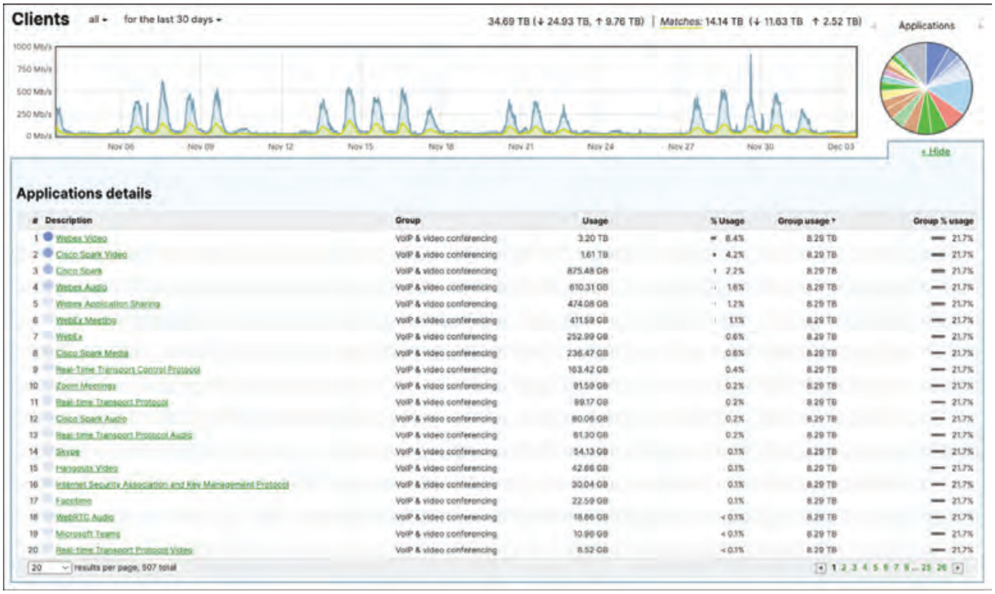


Figure 3-16 *The Network Health Summary on the Network-wide > Clients Page*

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.



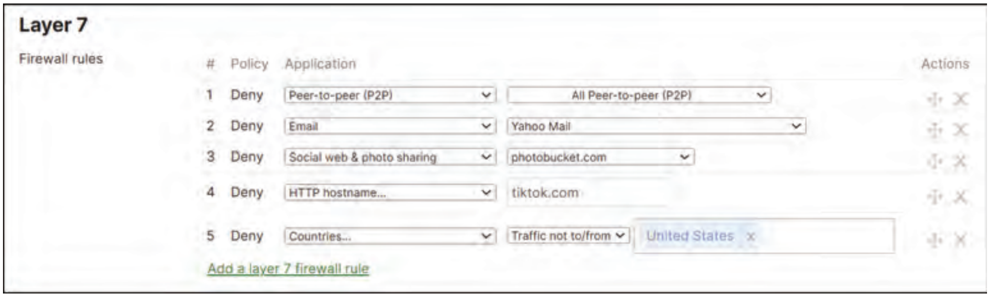
Applications details

#	Description	Group	Usage	% Usage	Group usage ▾	Group % usage
1	Webex Video	VoIP & video conferencing	3.20 TB	8.4%	8.29 TB	21.7%
2	Cisco Spark Video	VoIP & video conferencing	1.61 TB	4.2%	8.29 TB	21.7%
3	Cisco Spark	VoIP & video conferencing	875.48 GB	2.2%	8.29 TB	21.7%
4	Webex Audio	VoIP & video conferencing	610.31 GB	1.6%	8.29 TB	21.7%
5	Webex Application Sharing	VoIP & video conferencing	474.08 GB	1.2%	8.29 TB	21.7%
6	WebEx Meeting	VoIP & video conferencing	411.59 GB	1.1%	8.29 TB	21.7%
7	WebEx	VoIP & video conferencing	252.99 GB	0.6%	8.29 TB	21.7%
8	Cisco Spark Media	VoIP & video conferencing	236.47 GB	0.6%	8.29 TB	21.7%
9	Real-Time Transport Control Protocol	VoIP & video conferencing	163.42 GB	0.4%	8.29 TB	21.7%
10	Zoom Meetings	VoIP & video conferencing	91.59 GB	0.2%	8.29 TB	21.7%
11	Real-time Transport Protocol	VoIP & video conferencing	89.17 GB	0.2%	8.29 TB	21.7%
12	Cisco Spark Audio	VoIP & video conferencing	80.06 GB	0.2%	8.29 TB	21.7%
13	Real-time Transport Protocol Audio	VoIP & video conferencing	61.30 GB	0.2%	8.29 TB	21.7%
14	Skype	VoIP & video conferencing	54.13 GB	0.1%	8.29 TB	21.7%
15	Hangouts Video	VoIP & video conferencing	42.66 GB	0.1%	8.29 TB	21.7%
16	Internet Security Association and Key Management Protocol	VoIP & video conferencing	30.04 GB	0.1%	8.29 TB	21.7%
17	Facetime	VoIP & video conferencing	22.59 GB	0.1%	8.29 TB	21.7%
18	WebRTC Audio	VoIP & video conferencing	18.66 GB	< 0.1%	8.29 TB	21.7%
19	Microsoft Teams	VoIP & video conferencing	10.96 GB	< 0.1%	8.29 TB	21.7%
20	Real-time Transport Protocol Video	VoIP & video conferencing	8.52 GB	< 0.1%	8.29 TB	21.7%

20 results per page, 507 total

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.

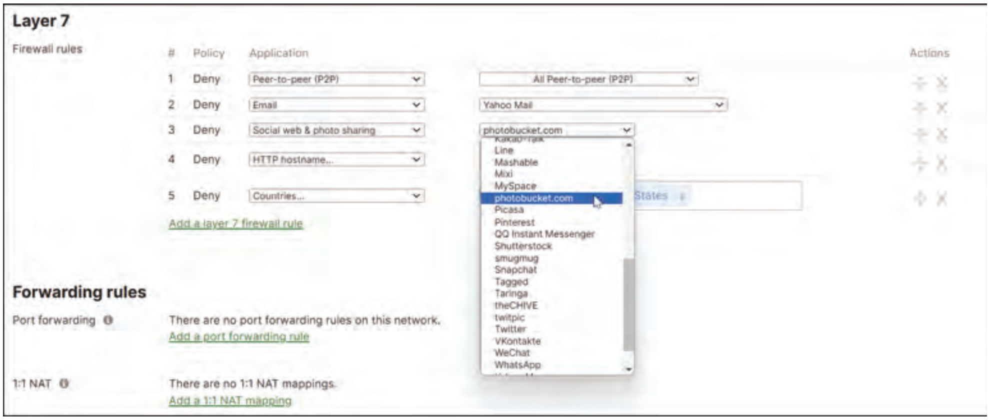

Layer 7

Firewall rules

#	Policy	Application			Actions
1	Deny	Peer-to-peer (P2P)	All Peer-to-peer (P2P)		
2	Deny	Email	Yahoo Mail		
3	Deny	Social web & photo sharing	photobucket.com		
4	Deny	HTTP hostname...	tiktok.com		
5	Deny	Countries...	Traffic not to/from	United States	

Add a layer 7 firewall rule

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



Layer 7

Firewall rules

#	Policy	Application		Actions
1	Deny	Peer-to-peer (P2P)	All Peer-to-peer (P2P)	
2	Deny	Email	Yahoo Mail	
3	Deny	Social web & photo sharing	photobucket.com	
4	Deny	HTTP hostname...		
5	Deny	Countries...	States	

Add a layer 7 firewall rule

Forwarding rules

Port forwarding There are no port forwarding rules on this network.
Add a port forwarding rule

1:1 NAT There are no 1:1 NAT mappings.
Add a 1:1 NAT mapping

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

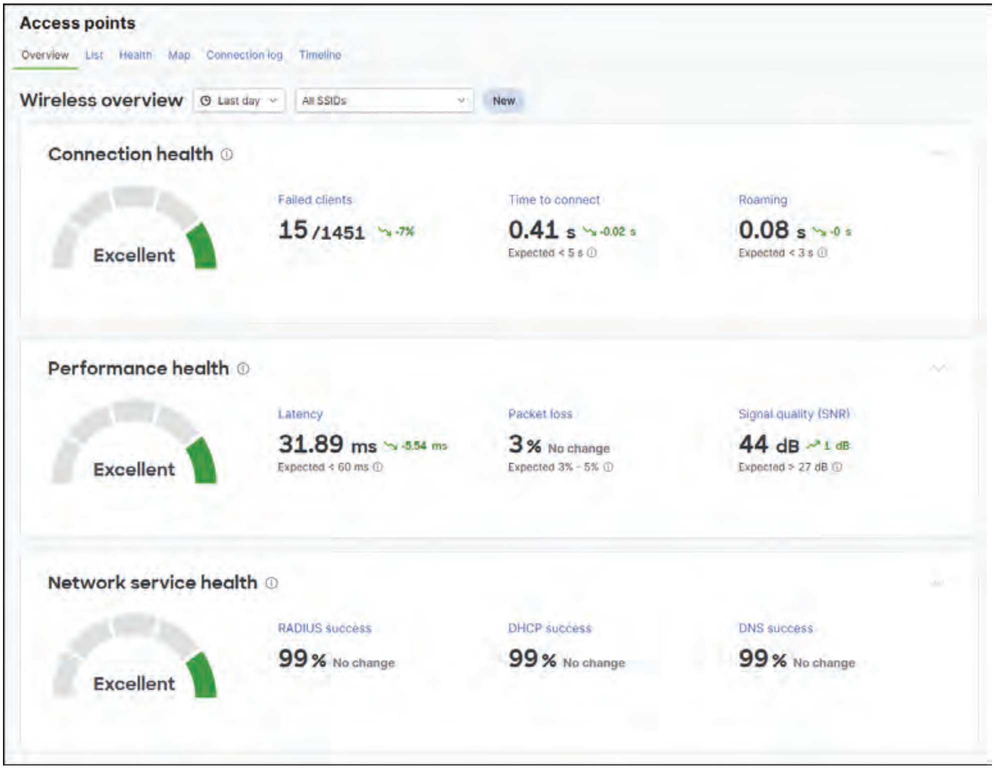
To confirm the minimum supported firmware versions for Meraki MX, MS, and MR platforms to allow enabling of NBAR functionality, visit https://documentation.meraki.com and view the article 'Next-gen Traffic Analytics – Network-Based Application Recognition (NBAR) Integration.' You can find more information 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.



Wireless overview · Last day · All SSIDs

Connection health ⓘ

Excellent

Failed clients
15/1451 -7%

Time to connect
0.41 s -0.02 s
Expected < 5 s ⓘ

Roaming
0.08 s -0 s
Expected < 3 s ⓘ

Performance health ⓘ

Excellent

Latency
31.89 ms -5.54 ms
Expected < 60 ms ⓘ

Packet loss
3% No change
Expected 3% - 5% ⓘ

Signal quality (SNR)
44 dB 1 dB
Expected > 27 dB ⓘ

Network service health ⓘ

Excellent

RADIUS success
99% No change

DHCP success
99% No change

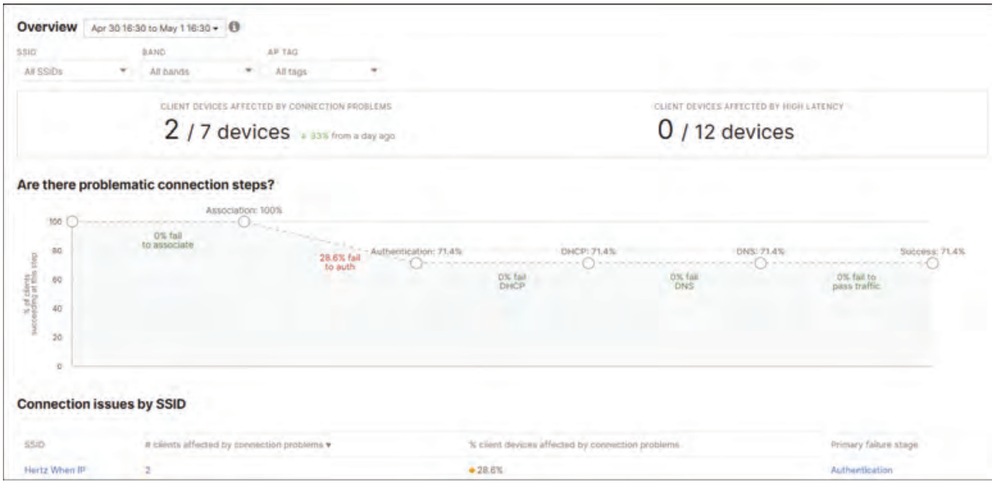
DNS success
99% No change

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.



Overview Apr 30 16:30 to May 1 16:30 ▾

SSID: All SSIDs ▾
BAND: All bands ▾
AP TAG: All tags ▾

CLIENT DEVICES AFFECTED BY CONNECTION PROBLEMS
2 / 7 devices ↓ 33% from a day ago

CLIENT DEVICES AFFECTED BY HIGH LATENCY
0 / 12 devices

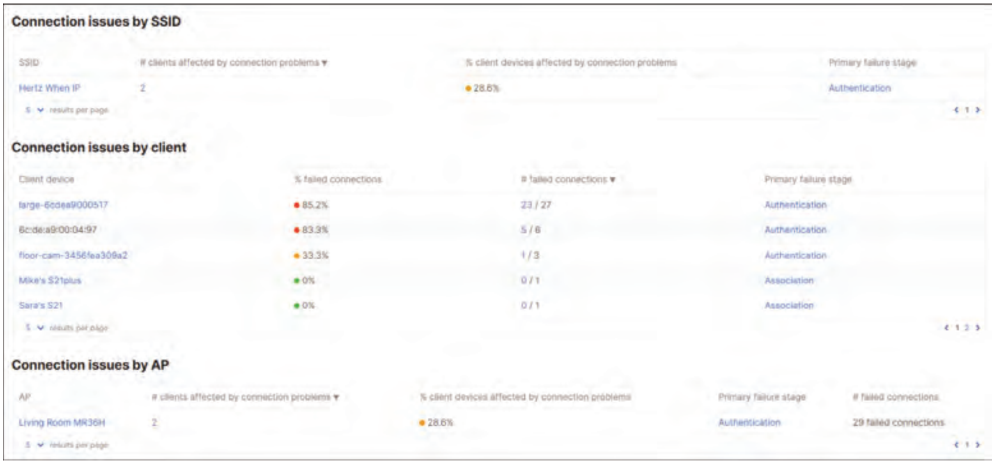
Are there problematic connection steps?

Connection issues by SSID

SSID	# clients affected by connection problems ▾	% client devices affected by connection problems	Primary failure stage
Hertz When IP	2	● 28.6%	Authentication

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."



Connection issues by SSID

SSID	# clients affected by connection problems ▾	% client devices affected by connection problems	Primary failure stage
Hertz When IP	2	● 28.6%	Authentication

5 ▾ results per page ‹ 1 ›

Connection issues by client

Client device	% failed connections	# failed connections ▾	Primary failure stage
large-6cdea9000517	● 85.2%	23 / 27	Authentication
6c:de:a9:00:04:97	● 83.3%	5 / 6	Authentication
floor-cam-3456fea309a2	● 33.3%	1 / 3	Authentication
Mike's S21plus	● 0%	0 / 1	Association
Sara's S21	● 0%	0 / 1	Association

5 ▾ results per page ‹ 1 2 ›

Connection issues by AP

AP	# clients affected by connection problems ▾	% client devices affected by connection problems	Primary failure stage	# failed connections
Living Room MR36H	2	● 28.6%	Authentication	29 failed connections

5 ▾ results per page ‹ 1 ›

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

Automated Topology Views

Stepping down from the organization views into a specific network, Meraki's integrated topology views can provide full-stack visibility for any Dashboard network containing MS switches. Using Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) data reported by the devices in the network, the Meraki Dashboard is able to intelligently construct multiple types of topology maps to allow for a quick and up-to-date reference of the current deployment topology.

This feature is another location where the combined networks discussed in Chapter 2 bring some significant advantages when compared to a standalone network consisting of only a single device type. When working in a combined network, each Meraki device is able to report data back to the Dashboard regarding any network connections between devices, allowing for a more comprehensive view of the topology of the network.

As previously mentioned, the Dashboard is able to build multiple types of topology reports based on the information available for each network, including Layer 2, Layer 3, and multicast routing topologies. You can view all topologies by navigating to the **Network-wide > Topology** page from the related network.

Network-wide Layer 2 Topology

The Layer 2 topology diagram, an example of which is shown in Figure 3-23, is based on advertised LLDP and CDP data that has been learned and reported back to the Dashboard by Meraki devices. Through the use of this information, the Dashboard is able to present an automatically generated, dynamic, and interactive Layer 2 topology map of a network.

Pro Tip Hovering over a device icon or link between devices provides more detailed information about the object and provides a direct link to that client, device, or related port.

This type of automatic and dynamic topology diagram can be immensely useful when attempting to track down a client or device, or when trying to determine the traffic flow/path of a given client. When looking at the Network-wide > Client Details page for any current client on the network, the most recent edge device closest to the client is listed as well as a link to the Layer 2 topology for the network, as shown in Figure 3-24. Clicking that link will automatically highlight the path through the network to the client in question, like the example shown in Figure 3-25.

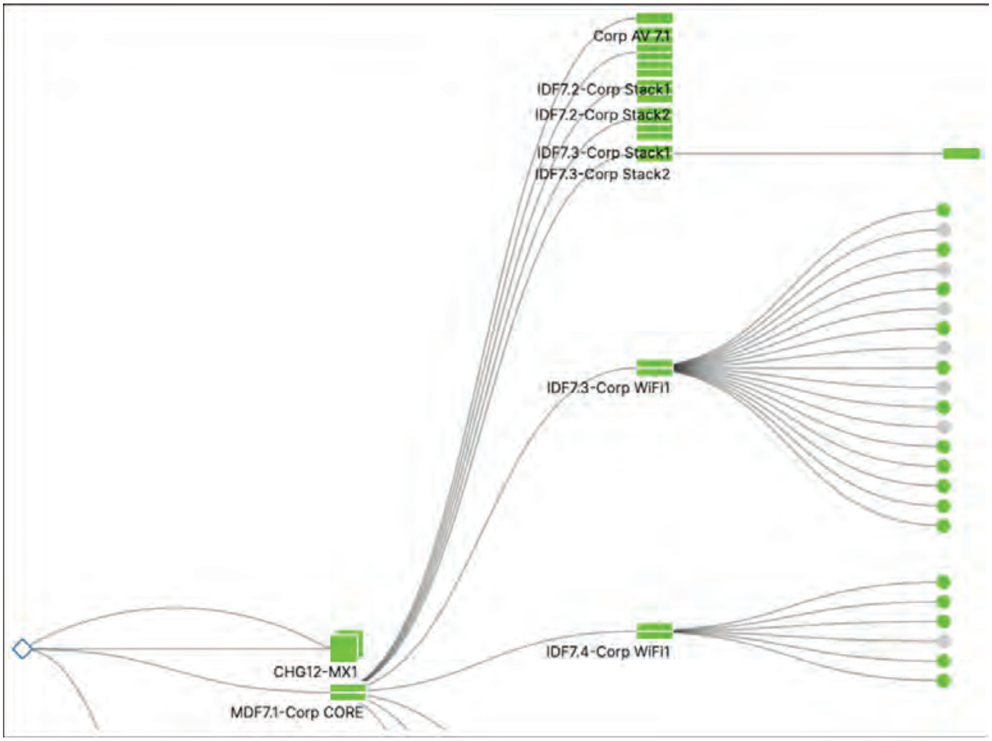
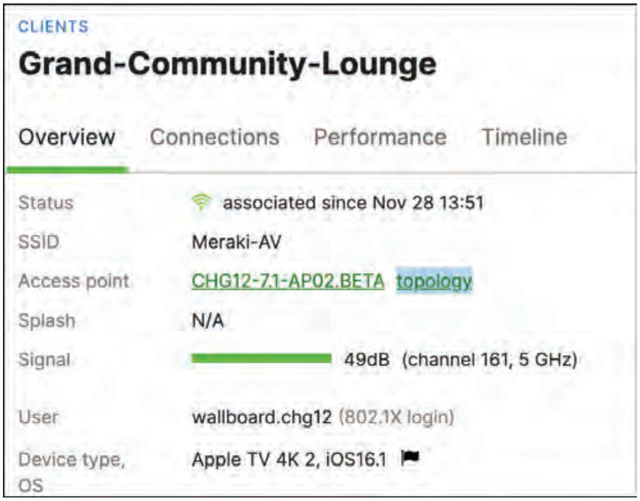


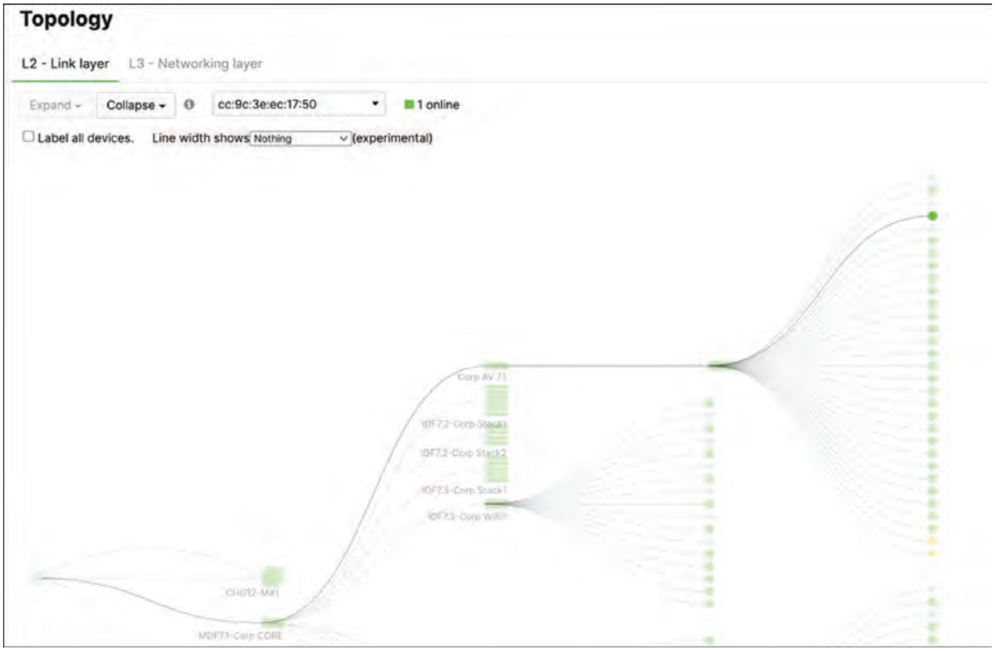
Figure 3-23 *A Partial View of the Layer 2 Topology Diagram for the Meraki Corp Network*


CLIENTS

Grand-Community-Lounge

Status	associated since Nov 28 13:51
SSID	Meraki-AV
Access point	CHG12-7.1-AP02.BETA topology
Splash	N/A
Signal	49dB (channel 161, 5 GHz)
User	wallboard.chg12 (802.1X login)
Device type, OS	Apple TV 4K 2, iOS16.1

Figure 3-24 *The Topology Link for a Client on the Client Details Page*



Topology

L2 - Link layer L3 - Networking layer

Expand ▾ Collapse ▾ cc:9c:3e:ec:17:50 ▾ 🟩 1 online

□ Label all devices. Line width shows Nothing ▾ (experimental)

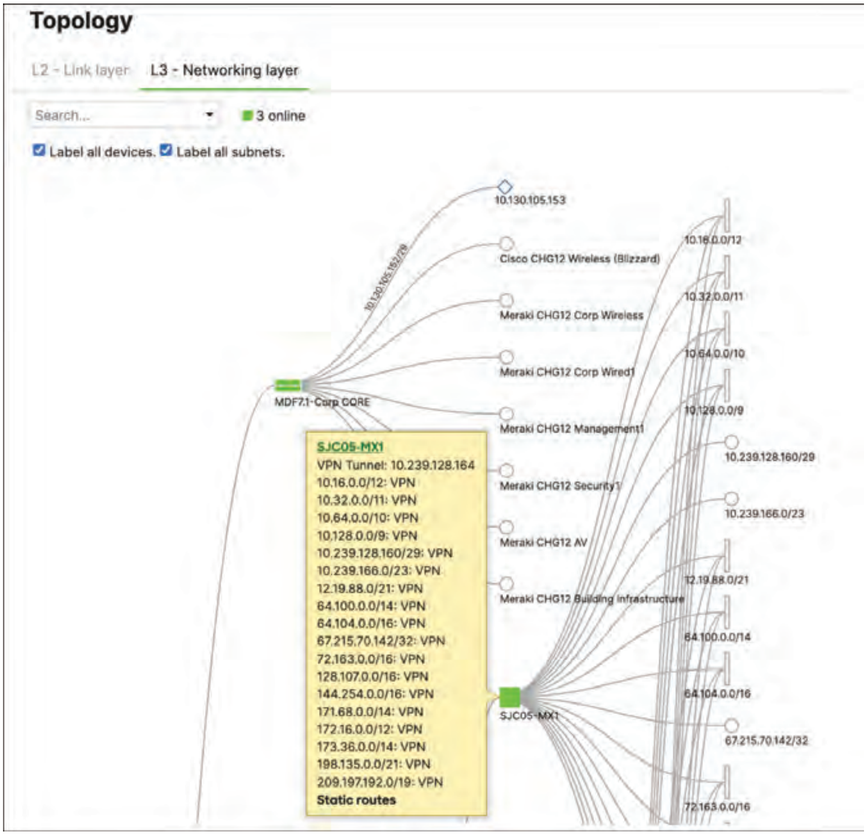
Figure 3-25 *The L2 Topology Page, with the Path to the Previously Selected Client Highlighted*

Network-wide Layer 3 Topology

The Topology page also includes the option to view the Layer 3 topology for the network, as shown in Figure 3-26, by selecting the L3 – Networking Layer tab. This view displays a dynamic layout of the Layer 3 topology of the network based on the current Dashboard configuration for MX and MS devices.

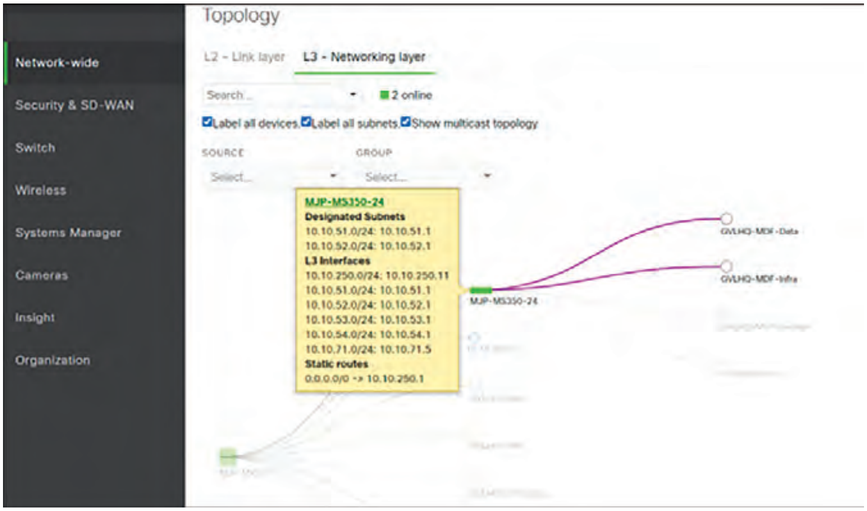
Network-wide Multicast Topology

For networks that have multicast routing enabled, you can configure the Layer 3 Topology page to show the current multicast topology as an overlay on top of the existing Layer 3 topology by checking the **Show Multicast Topology** check box, as shown in Figure 3-27. This provides a highlighted view of the multicast topology specifically.



SJC05-MX1
VPN Tunnel: 10.239.128.164
10.16.0.0/12: VPN
10.32.0.0/11: VPN
10.64.0.0/10: VPN
10.128.0.0/9: VPN
10.239.128.160/29: VPN
10.239.166.0/23: VPN
12.19.88.0/21: VPN
64.100.0.0/14: VPN
64.104.0.0/16: VPN
67.215.70.142/32: VPN
72.163.0.0/16: VPN
128.107.0.0/16: VPN
144.254.0.0/16: VPN
171.68.0.0/14: VPN
172.16.0.0/12: VPN
173.36.0.0/14: VPN
198.135.0.0/21: VPN
209.197.192.0/19: VPN
Static routes

Figure 3-26 *A Portion of the L3 Topology Page for a Cisco Meraki Campus Network*



MJP-MS350-24
Designated Subnets
10.10.51.0/24: 10.10.51.1
10.10.52.0/24: 10.10.52.1
L3 Interfaces
10.10.250.0/24: 10.10.250.11
10.10.51.0/24: 10.10.51.1
10.10.52.0/24: 10.10.52.1
10.10.53.0/24: 10.10.53.1
10.10.54.0/24: 10.10.54.1
10.10.71.0/24: 10.10.71.5
Static routes
0.0.0.0/0 -> 10.10.250.1

Figure 3-27 *An Example Multicast Topology Highlighted on Top of the Layer 3 Topology of a Network*

Summary

As you've seen in this chapter, the Meraki platform utilizes the cloud to help present the Dashboard as a unified interface that is easy to navigate and embraces the power of cloud communication and management. This allows Meraki to offer features like the ability to easily view and manage firmware for an entire organization from a single page or provide detailed topology maps and troubleshooting information based on observed trends and behaviors in a network. These types of enhancements are only possible by aggregating client and device data in ways that were previously not feasible without the cloud. Meraki uses all of this and more to help drive a better administrator experience no matter what task you're trying to accomplish.

Next, Chapter 4 introduces how you can further enhance the power of the Meraki platform through the use of automation, both inside and outside the Dashboard.

Additional Reading

Best Practices for Meraki Firmware: https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Best_Practices_for_Meraki_Firmware

Cisco Meraki Firmware FAQ: https://documentation.meraki.com/General_Administration/Firmware_Upgrades/Cisco_Meraki_Firmware_FAQ

Firmware Features: https://documentation.meraki.com/Firmware_Features

Returns (RMAs), Warranties and End-of-Life Information: https://documentation.meraki.com/General_Administration/Other_Topics/Returns_(RMAs)%2C_Warranties_and_End-of-Life_Information

Alerts: https://documentation.meraki.com/General_Administration/Cross-Platform_Content/Global_Alerts_Widget

Switching Overview – MS_Health: https://documentation.meraki.com/MS/Meraki_MS_Beta/Switching_Overview_-_MS_Health

Global Overview: https://documentation.meraki.com/General_Administration/Cross-Platform_Content/Global_Overview

Next-gen Traffic Analytics – Network-Based Application Recognition (NBAR) Integration: https://documentation.meraki.com/General_Administration/Cross-Platform_Content/Next-gen_Traffic_Analytics_-_Network-Based_Application_Recognition_(NBAR)_Integration

Network Topology: https://documentation.meraki.com/MS/Monitoring_and_Reporting/Network_Topology

This page intentionally left blank

Index

Numbers

4G LTE (Long Term Evolution), 117

5G, 118, 120–121

6-GHz RF propagation, 199

802.1X authentication, 166–168

A

access layer, hybrid campus deployment, 154
- connecting MR access points, 158
- MTU recommendation, 158
- QoS (Quality of Service), 156
- STP (Spanning Tree Protocol), 156–157
- trunk ports, 158
- VLAN deployment, 154–156

active client balancing, 205

Adaptive Policy, 91–92, 173, 224
- caveats and limitations, 176
- enforcement, 174–175
- security policy definition, 174
- SGTs (Security Group Tags), 174, 175

adding, devices to network, 17

adjacency, access point, 201

administrative/administrator
- camera, 249–250
- roles, 17–18
  - *camera-only, 18–19*
  - *Guest Ambassador, 18*
  - *Monitor-only, 19*
  - *SAML, 20*
- scoping privileges and access, 196

Administrator account, Dashboard, 2

Advanced license, 303–304

AI (artificial intelligence), 146–147, 212–213

Air Marshal, 222

Alert Hub, 112–113

alert/s, 25–26, 105–108. *See also* **monitoring and monitoring tools**
- camera
  - *fine-tuning, 264–267*
  - *motion, 263–264*
- device defect, 41–42
- email, 26–27
- hubs, 33

Insight, 31–33, 109–110
Meraki MT sensor, 296
reviewing, 296–297
selecting the type, 296–297
organization, 44–46, 113–114
Smart Thresholds, 228–230
webhooks, 27–28, 66–67
AMI (Alternate Management Interface), 223
analytics, 3
Meraki MV camera, built-in tools, 241
roaming, 232–233
video, 269–271
anomaly detection, 228–230
API, Dashboard, 70–71
examples, 72
reporting organization status, 73–75
tips and tricks, 71–72
updating device name based on network, 73–78
AP/s (access point/s)
adjacency and overlap, 201
channel width, 209
CW916X, 195
DFS (Dynamic Frequency Selection) channels, 210–211
dual 5-GHz mode, 198
external antenna, 200
frequency bands, 209
location-aware, 197–198
Meraki MR, 195–196
minimum bitrate, 206–208
mounting recommendations, 199–200
RF profile, 202–204
Auto RF, 211–213
band selection, 204
client balancing, 205–206
roaming, 206, 218. *See also* roaming
DHCP scope, 221–222
domains, 219–220
Layer 2 domain, 220–221
Layer 3 domain, 221
types of, 218
SNR (signal-to-noise ratio), 201
tags, 216–217
timeline, 235–236
Wi-Fi 6E, 198
architecture
cloud/back-end, 3–4
Dashboard, 1–2
Meraki MV camera, 239–240
Meraki switching platform, 145–146
out-of-band, 4
audio detection, MV camera, 271
authentication
802.1X, 166–168
Cisco XDR Sign-On, 21
wireless network, 214–215
X.509 certificate, 4
Auto RF, 211–213
Auto VPN, 92, 128
automated summary report, 29–31
automated topology report, 53
automation
Dashboard API, 70–71
examples, 72
reporting organization status, 73–75
tips and tricks, 71–72
Dashboard-based, 78–81
MT device, 78
rule, 80–81

smart button, 293–294
SNMP, 68–70
syslog messaging, 67–68
template/s
caveats and limitations, 62–64
configuration, 59, 60–61
creating, 59–60
updating device name based on network, 75–78
webhooks, 66–67
AVC (Application Visibility and Control), 49

B

back-end, architecture, 3–4
backup and restore, customer management data, 4
band steering, 209
best practices
channel planning, 209
IoT, 299
multicast, 160
OSPF, 159
RF profile, 203–204
template, 64–65
beta firmware, 8
BGP, support on MX security appliance line, 97
BLE signal strength, monitoring, 300–301

C

Cable Test feature, 190
camera-only administrator, 18–19
Catalyst switch, 151
cloud monitoring, 183–184
cloud-managed, 154
cloud-monitored, 153–154
caveats and limitations, template, 62–64
CDP (Cisco Discovery Protocol), 53
cellular uplink, 120
5G line of sight, 120–121
CGNAT (Carrier Grade NAT), 121
prestaging for deployment, 121–122
SD-WAN over, 138–140
centralized management, Meraki switching platform, 146
CGNAT (Carrier Grade NAT), 121
channel/s
DFS (Dynamic Frequency Selection), 210–211
planning, 209. *See also* AP/s (access point/s)
width, 209
Cisco AMP, 87–88
Cisco AnyConnect, 94
Cisco ISE, integration with Meraki MS switches, 169–172
Cisco TALOS Intelligence, 87
Cisco Threat Grid, 88
Cisco Umbrella, 89–90
Cisco XDR Sign-On, 21
Claim button, 16
client balancing, 205–206
Client VPN, 93–94
cloud
architecture, 3–4
Catalyst switch monitoring, 183–184
to device communication, 4–5

-managed Catalyst switch, 154

-monitored Catalyst switch, 153–154

Cloud Archive, 278

cold storage sensor, 289–291

combined network, 14–15

combo filter, 177–178

configuration, Meraki Auto VPN, 98–100

configuration template, 59, 60–61

caveats and limitations, 62–64

local overrides, 61–62

MX security appliance, 60, 61, 63

VLAN, 60–61

connectivity

cellular, 120

Meraki MV camera, 247

general network considerations, 247

wired, 248

wireless, 248–249

Co-termination licensing, 304–306

creating

group policies, 90

organizations, 12–13

templates, 59–60

custom performance classes, SD-WAN, 131–132

customer management data, 4

CW916X access point, 195

Cycle Port, 191

D

DAI (Dynamic ARP Inspection), 162–163

Dashboard

accessing MV cameras, 252–253

Administrator account, 2

Alert Hub, 112–113

alert/s, 25–26. *See also* logging; report/ing

email, 26–27

hubs, 33

Insight, 31–33

webhooks, 27–28

API, 70–71

examples, 72

reporting organization status, 73–75

tips and tricks, 71–72

updating device name based on network, 73–78

automated summary report, 29–31

-based automation, 78–81

Content Filtering configuration page, 87

Early Access program, 42–43

Global Overview page, 47

licensing models, 304

Live Tools, 187

Cable Test, 190

Cycle Port, 191

MAC forwarding table, 190

MTR (My TraceRoute), 189

packet capture, 188–189

ping, 187–188

Wake-on-LAN, 191

Magnetic, 42–43

maintaining access and control, 21–22

MG device monitoring, 118–119

Most Prevalent Threats report, 115–116

MS Power Overview, 181–182

network/s, 2
Alert Hub notification icon, 45–46
automated topology report, 53
claiming and adding devices, 15–17
creating, 14–15
detailed firmware status and security, 40–41
health, 48–50
Layer 2 diagram, 53–55
Layer 3 diagram, 55–56
multicast diagram, 55–56
organization/s, 1
administrative roles, 17–18
Alerts page, 113–114
camera-only administrator, 18–19
creating, 12–13
Global Overview page, 34
Guest Ambassador account, 18
Monitor-only administrator, 19
overview page. See organization/s, overview page
SAML, 20
Security Center, 115
summary page, 43–44
reporting, 184–187
RF profile, 202–204
Auto RF, 211–213
band selection, 204
client balancing, 205–206
Switching Overview feature, 46
tags and tagging, 22
for administrative privilege, 22–23
configuring non-Meraki VPN peer availability for MX and Z series devices, 24–25
configuring SSID availability on MR access points, 23–24
device, 25
template, 2
Topology View, 147–149
traffic filters, 133–134
Wireless Health feature, 50–52
Wireless Overview page, 227–228

data centers, 4, 285–286

data retention policy, 6–7

deployment
Meraki Auto VPN, 97–98
Meraki MT sensor, 294
accounting for distance, 295
basic configuration and setup, 294–295
configuration considerations, 296
IoT gateways, 295
power considerations, 295
MG device, 119–120

device/s. ***See also*** **Meraki switching platform; MX security appliance line**
to cloud communication, 4–5
name, updating based on network, 75–78
PoE, 180
proactive replacement, 41–42
tagging, 25

DFS (Dynamic Frequency Selection) channels, 210–211

DHCP
mandatory, 223
scope, 221–222
snooping, 161

diagram, topology
Layer 2, 53–55
Layer 3, 55–56
multicast, 55–56
distributed data plane, 213–214
distributed Layer 3 roaming, 218
DM logging, 124
documentation
Hybrid Campus LAN Design Guide, 152
licensing, 85
door sensor, 288–289
DPS (dynamic path selection), 127, 128–129
performance-based, 137
policies, 134–135
with policy routing, 138
dual 5-GHz mode, 198

E

Early Access program, 42
email, alerts, 26–27
encryption, wireless network, 214–215
endpoint security, 172–173
environmental sensors, 285–286
Enterprise license, 303–304
Event Log, 230
exporting video, 276–278
external antenna, access point, 200
external license, 304

F

fast and secure roaming, 218
filter
combo, 177–178
HTTP content, 87
traffic, 133
firewall
enabling ports for Meraki cloud, 280–281
MX security appliance, 86
firmware
beta, 8
detailed status and security, 40–41
rollout process, 7–8
Stable, 8
status, 39–40
upgrade process, 7, 8–9, 178–179
fisheye lens, 244
fixed lens, 244
floor plan, wireless network, 226
FoV (field of view), camera, 244–245
frequency bands, 209

G

Global Overview page, 34, 47
global preference policy, 135–136
group policy, 90–91, 171, 223
Guest Ambassador account, 18

H

health, monitoring and reporting
network-wide, 48–50
VoIP, 108–109
WAN, 108–109
Web Application, 105–108
wireless, 50–52
HTTP content filtering, 87
hub and spoke topology
Meraki Auto VPN

advanced configurations, 103–104

full tunnel versus split tunnel, 102

hub prioritization, 102

VPN, 100

hybrid campus deployment, 152–154

access layer, 154

QoS (Quality of Service), 156

STP (Spanning Tree Protocol), 156–157

VLAN deployment, 154–156

Hybrid Campus LAN Design Guide, 152

I

icon, Alert Hub notification, 45–46

IdP (identity provider), 20

IDS/IPS feature, MX security appliance, 88–89

infrastructure, 160–161

security

DAI (Dynamic ARP Inspection), 162–163

DHCP snooping, 161

port profiles, 164

SecurePort, 163–164

Storm Control, 161–162

VLAN profile, 164–165

Insight alerts, 31–33

intelligent motion indexing, 241

inventory, organization, 16

IoT. ***See also*** **Meraki MT sensor/s; sensor/s**

best practices, 299

gateway, 295

IPv6, 95, 121, 221

J-K-L

JSON, get request and response, 73–75

L3/L7 firewall, MX security appliance, 86

large network

distributed data plane, 213–214

recommended maximum number of devices, 196

Layer 2

domains, 220–221

endpoint security, 172–173

infrastructure security, 160–161

DAI (Dynamic ARP Inspection), 162–163

DHCP snooping, 161

port profiles, 164

SecurePort, 163–164

Storm Control, 161–162

VLAN profile, 164–165

micro-segmentation, 173–174

network security, 165

802.1X authentication, 166–168

integrating Meraki switching and Cisco ISE, 169–172

MAB (MAC Authentication Bypass), 169

port isolation, 166

Sticky MAC, 165

topology diagram, 53–55

Layer 3

multicast, best practices, 160

OSPF, best practices, 159

lens types, Meraki MV camera, 244

licensing
- Co-termination, 304–306
- documentation, 85
- Enterprise versus Advanced, 303–304
- external, 304
- Meraki subscription, 307
- Per-Device, 16–17, 306
- SD-WAN, 140

Live Tools, 187
- Cable Test, 190
- Cycle Port, 191
- MAC forwarding table, 190
- MTR (My TraceRoute), 189
- packet capture, 188–189
- ping, 187–188
- Wake-on-LAN, 191

LLDP (Link Layer Discovery Protocol), 53

load balancing policy, 131, 136–137

local override, template, 61–62

Local Status page, MG device, 122–124

location-aware wireless network, 197–198

logs and logging
- DM, 124
- SDB (Support Data Bundle), 124
- SNMP, 28
- syslog, 28, 67–68
- video, 278–279
- wireless connection, 230–231

low light recording feature, Meraki MV camera, 262–263

M

MAB (MAC Authentication Bypass), 169

MAC forwarding table, 190

Magnetic, 42–43

mandatory DHCP, 223

manual camera configuration, 261–262

Meraki. ***See also*** **MX security appliance line**
- data centers, 4
- New Account Creation page, 12–13
- regions, 3
- service failover times, 128–129
- sustainability goals, 282

Meraki Auto VPN, 92
- advanced configurations, 103–104
- configuration, 98–100
- deployment, 97–98
- full tunnel versus split tunnel, 102
- hub prioritization, 102
- NAT traversal, 100–101
- scaling, 101–102

Meraki Display App, accessing MV cameras, 255

Meraki Insight, 104–105
- alerts, 31–33, 109–110
- ThousandEyes integration, 110
- VoIP Health page, 108–109
- WAN Health page, 108–109
- Web Application Health page, 105–108

Meraki mobile app, accessing MV cameras, 255–257

Meraki MR access points, 195–196
6-GHz RF propagation, 199
adjacency and overlap, 201
channel width, 209
DFS (Dynamic Frequency Selection) channels, 210–211
dual 5-GHz mode, 198
external antenna, 200
frequency bands, 209
location-aware, 197–198
minimum bitrate, 206–208
mounting recommendations, 199–200
RF profile, 202–204
Auto RF, 211–213
band selection, 204
client balancing, 205–206
roaming, 218. *See also* roaming
DHCP scope, 221–222
domains, 219–220
Layer 2 domain, 220–221
Layer 3 domain, 221
types of, 218
SNR (signal-to-noise ratio), 201
tags, 216–217
VLAN considerations, 215–216
Wi-Fi 6E, 198
Meraki MT sensor/s, 281–285
alert/s, 296
reviewing, 296–297
selecting the type, 296–297
automation, 78
cold storage, 289–291
deployment, 294
accounting for distance, 295
basic configuration and setup, 294–295
configuration considerations, 296
IoT gateways, 295
power considerations, 295
door, 288–289
environmental, 285–286
MT30 Smart Automation Button, 293–294
MT40 smart power controller, 289–290
physical, 286
Sensor Sight, 298
temperature, humidity, and air quality, 291–292
troubleshooting, 299–301
water/leak, 287–288
Meraki MV camera/s. ***See also*** **surveillance system**
accessing
through Meraki Display App, 255
through Meraki mobile app, 255–257
through Meraki Vision Portal, 253–255
through the Dashboard, 252–253
administrator roles, 249–250
alert/s
fine-tuning, 264–267
motion, 263–264
architecture, 239–240
audio detection, 271
built-in analytics, 241, 269–271
Cloud Archive, 278
connectivity, 247
general network considerations, 247
wired, 248
wireless, 248–249

enabling firewall ports for Meraki cloud, 280–281
ensuring security, 241
FoV (field of view), 244–245
intelligent motion indexing, 241
lens types, 244
listing details, 257–258
manual configuration, 261–262
motion search and motion recap, 271–275
mounting options and accessories, 243–244
MV Sense, 279–280
MV52, 245–246
navigating the video timeline, 269
power requirements, 246–247
privacy windows, 267
profiles, 258–261
providing access to support technicians, 281
recording in low light, 262–263
resolution, 245
role-based permissions for SAML/SSO, 251
RTSP (Real Time Streaming Protocol) integration, 267
tags, 249
using with templates, 63–64
video
event logs, 278–279
exporting, 276–278
sharing, 275–276
storage, 246
walls, 267–268

Meraki SD-WAN, 127. ***See also* SD-WAN**
custom performance classes, 131–132
DPS (dynamic path selection), 127, 128–129
performance-based, 137
with policy routing, 138
licensing, 140
MPLS
on the LAN, 141–142
on the WAN, 142–143
over cellular uplink, 138–140
policy/ies, 130–131
-based routing, 137
DPS (dynamic path selection), 134–135
global preference, 135–136
load balancing, 136–137
probe interval, 128
traffic analysis and identification, 133–134

Meraki switching platform, 145
access layer design, 154
connecting MR access points, 158
MTU recommendation, 158
native VLAN, 155–156
QoS (Quality of Service), 156
STP (Spanning Tree Protocol), 156–157
tags, 157
trunk ports, 158
VLAN deployment, 154–155
auto-rollback on bad uplink, 179–180
centralized management, 146
cloud-based architecture, 145–146
config-safe mechanism, 179
designing a wired enterprise network, 149

endpoint security, 172–173

firmware upgrade, 178–179

hybrid campus LAN architectures with cloud management, 152–154, 159–160

infrastructure security, 160–161

DAI (Dynamic ARP Inspection), 162–163

DHCP snooping, 161

port profiles, 164

SecurePort, 163–164

Storm Control, 161–162

VLAN profile, 164–165

Layer 2, 160

Layer 3

multicast, 160

OSPF, 159

micro-segmentation, 173–174

network security, 165

802.1X authentication, 166–168

ISE integration, 169–172

MAB (MAC Authentication Bypass), 169

port isolation, 166

Sticky MAC, 165

network telemetry, 146–147

planning your deployment, 149–150

PoE devices, 180

Port Schedules feature, 182–183

Power Overview, 181–182

seamless integration, 146

selecting the right switch product mix, 150–152

tags and tagging, 157

virtual stacking, 177–178

Meraki Systems Manager, 25

Meraki Vision Portal, accessing MV cameras, 253–255

MG device/s, 117. *See also* cellular uplink

4G LTE (Long Term Evolution), 117

5G, 118, 120–121

CGNAT (Carrier Grade NAT), 121

deployment, 119–120

DM logging, 124

Local Status page, 122–124

monitoring, 118–119

prestaging for deployment, 121–122

Safe Mode, 124

SDB (Support Data Bundle) logging, 124

micro-segmentation, 173–174

minimum bitrate, access point, 206–208

MITM (man-in-the-middle) attack, 162

ML (machine learning), 146–147

monitoring and monitoring tools. *See also* sensor/s

BLE signal strength, 300–301

Catalyst switch, 183–184

Insight, 104–105

Meraki Insight

alerts, 109–110

VoIP Health page, 108–109

WAN Health page, 108–109

Web Application Health page, 105–108

MG device, 118–119

sensor/s

event logs, 300

status, 300

ThousandEyes, 110

transport path performance, 128–129

VPN, 110–112

Monitor-only administrative role, 19

MOS (Mean Operating Score), 128

motion alerts, 263–264

motion search and recap, Meraki MV camera, 271–275

mounting options

access point, 199–200

Meraki MV camera, 243–244

MPLS, integrating with Meraki SD-WAN

on the LAN, 141–142

on the WAN, 142–143

MT30 Smart Automation Button, 293–294

MT40 smart power controller, 289–290

MTR (My TraceRoute), 189

MTU (Maximum Transmission Unit), 158

multicast

best practices, 160

DNS, 224

topology, diagram, 55–56

MX security appliance line, 129–130. *See also* troubleshooting Meraki devices

configuration template, 60, 61, 63

NTP (Network Time Protocol), 128

passthrough or VPN Concentrator mode, 85

routed mode, 84–85

routing, 95

BGP, 97

OSPF support, 96

route priority, 95

static, 95–96

scaling, 84

security. *See also* VPN

Adaptive Policy, 91–92

Cisco AMP, 87–88

Cisco AnyConnect, 94

Cisco Umbrella integration, 89–90

Client VPN, 93–94

group policy, 90–91

HTTP content filtering, 87

IDS/IPS, 88–89

L3/L7 firewall, 86

Meraki Auto VPN, 92

Meraki Auto VPN, configuration, 98–100

Meraki Auto VPN, deploying, 97–98

non-Meraki VPN, 94

VPN, 92

UDP probes, 128

N

NAC (network access control), 148–149

NAT traversal, Meraki Auto VPN, 100–101

NBAR (Network-Based Application Recognition), 48–50

NBAR2, 133

network/s. *See also* organization/s; wireless deployment

administrative roles, 17–18

Alert Hub notification icon, 45–46

alerts

email, 26–27

webhooks, 27–28

claiming and adding devices, 15–17

- combined, 14–15
- Dashboard, 2, 14–15
- distributed, 213–214
- firmware
    - *detailed security, 40–41*
    - *status, 39–40*
- health, 48–50
- hybrid management approach, 150
- large, recommended maximum number of devices, 196
- management, 150
- organization, 1
- security, 165
    - *802.1X authentication, 166–168*
    - *integrating Meraki switching and Cisco ISE, 169–172*
    - *MAB (MAC Authentication Bypass), 169*
    - *port isolation, 166*
    - *Sticky MAC, 165*
- standalone, 14–15
- Switching Overview feature, 46
- syslog reporting, 28
- tagging, 22–23
    - *configuring non-Meraki VPN peer availability for MX and Z series devices, 24–25*
    - *configuring SSID availability on MR access points, 23–24*
- telemetry, 146–147
- topology
    - *Layer 2 diagram, 53–55*
    - *Layer 3 diagram, 55–56*
    - *multicast diagram, 55–56*
    - *report, 53*
- wireless, health reporting, 50–52. *See also* wireless deployment

New Account Creation page, 12–13

New Organization alerts page, 45

No-Nat, 143

non-Meraki VPN, 94

NTP (Network Time Protocol), 128

O

opt in, Early Access program, 42

order number, claiming, 16

organization/s, 1

- accounts, 17
- administrative roles, 17–18
    - *camera-only, 18–19*
    - *Guest Ambassador, 18*
    - *Monitor-only, 19*
- alerts, 44–46
- Alerts page, 113–114
- Dashboard, creating, 12–13
- Global Overview page, 34
- Guest Ambassador account, 18
- inventory, 16
- overview page, 37–38
    - *firmware status, 39–40*
    - *organization-wide health, 38–39*
- SAML, 20–21
- Security Center, 115
- special access roles, 18
- status, reporting, 73–75
- summary page, 43–44

OSPF

- best practices, 159
- support on MX security appliance line, 96

out-of-band architecture, 4

overlap, access point, 201

P

packet capture, 188–189

passive client balancing, 206

passthrough or VPN Concentrator mode, MX security appliance, 85

PDL (Per-Device Licensing) model, 16–17

per-device licensing, 16–17, 306

performance

-based DPS, 137

transport path, 128–129

permissions. *See also* administrative roles

administrator, 17–18

camera, 18–19, 251

Guest Ambassador, 18

physical sensors, 286

ping, 187–188

PoE devices, 180

policy/ies. *See also* Adaptive Policy

access, 170

Adaptive, 91–92, 173, 224

caveats and limitations, 176

enforcement, 174–175

SGTs (Security Group Tags), 174

-based routing, 137, 138

data retention, 6–7

DPS (dynamic path selection), 134–135

group, 90–91, 171, 223

SD-WAN, 129–130

default, 130–131

global preference, 135–136

load balancing, 136–137

security, 174

polling, SNMP, 68–70

port isolation, 166

port profiles, 164

port schedule, 182–183

power requirements, camera system, 246–247

privacy windows, 267

Q-R

QoS (Quality of Service), hybrid campus deployment, 156

RADSec, 224–225

RBAC (role-based access control), 241

RCA (root cause analysis), 147, 231–232

regions, Meraki, 3

replacement, device, 41–42

report/ing. *See also* alerts; logging

automated summary, 29–31

Dashboard, 184–187

health

network-wide, 48–50

wireless, 50–52

Most Prevalent Threats, 115–116

organization status, 73–75

Roaming Analytics, 232–233

SNMP, 29, 68–70

syslog, 28, 67–68

topology, 53

resolution, camera, 245

RF profile

access point, 202–204

Auto RF, 211–213

band selection, 204

client balancing, 205–206

RMA (Return Materials Authorization), 42

roaming, 206, 218
analytics, 232–233
DHCP scope, 221–222
domain/s, 219–220
Layer 2, 220–221
Layer 3, 221
types of, 218
rollout process, firmware, 7–8
routed mode, MX security appliance, 84–85
routing
multicast, best practices, 160
MX security appliance, 95
BGP, 97
OSPF support, 96
route priority, 95
static, 95–96
OSPF, best practices, 159
RTSP (Real Time Streaming Protocol), 267
rule, automation, 80–81

S

Safe Mode, MG device, 124
scaling
Meraki Auto VPN, 101–102
MX security appliance, 84
SDB (Support Data Bundle) logging, 124
SD-Internet, 140
SD-WAN, 127, 129–130
custom performance classes, 131–132
licensing, 140
over cellular uplink, 138–140
policy/ies, 130–131
-based routing, 137
basic load balancing, 136–137
global preference, 135–136
traffic analysis and identification, 133–134
seamless roaming, 218
SecurePort, 163–164, 225
security. ***See also*** **access layer; Layer 3**
data retention policies, 6–7
endpoint, 172–173
infrastructure, 160–161
MX security appliance
Adaptive Policy, 91–92
Cisco AMP, 87–88
Cisco AnyConnect, 94
Cisco Umbrella integration, 89–90
Client VPN, 93–94
group policy, 90–91
HTTP content filtering, 87
IDS/IPS, 88–89
Meraki Auto VPN, 92
Meraki Auto VPN, deploying, 97–98
non-Meraki VPN, 94
VPN, 92
network, 165
802.1X authentication, 166–168
integrating Meraki switching and Cisco ISE, 169–172
MAB (MAC Authentication Bypass), 169
port isolation, 166
Sticky MAC, 165
policy, 174
wired network, 150
wireless
Air Marshal, 222

AMI (Alternate Management Interface), 223

mandatory DHCP, 223

wireless deployment

mDNS support, 224

per-SSID group policy, 223

RADSec, 224–225

SecurePort, 225

Security Center, 115

Sensor Sight, 298

sensor/s. *See also* Meraki MT sensors

cold storage, 289–291

door, 288–289

environmental, 285–286

MT series, 78, 281–283

physical, 286

temperature, humidity, and air quality, 291–292

water/leak, 287–288

Server RCA, 231–232

SGTs (Security Group Tags), 91–92, 173, 174, 175,224

site survey, 242

SLA (service-level agreement), 4

smart button automation, 293–294

Smart Thresholds, 228–230

SNMP, 29

automation, 68–70

traps, 69–70

SNR (signal-to-noise ratio), 201

SSID

configuration, 202

frequency bands, 209

group policy, 223

minimum bitrate, 206–208

roaming, 218. *See also* roaming

domains, 219–220

types of, 218

staged upgrades, 149

standalone network, 14–15

static routing, 95–96

Sticky MAC, 165

storage

data retention policy, 6–7

video, 246

Storm Control, 161–162

STP (Spanning Tree Protocol), hybrid campus deployment, 156–157

subnetting, templates and, 62–63

subscription licensing, 307

surveillance system

design

building analysis, 242

exploring constraints, 243

site survey, 242

stakeholder input, 242

video storage, 246

Switching Overview feature, 46

syslog, 67–68

syslog reporting, 28

T

tags and tagging, 22

for administrative privilege, 22–23

camera name, 249

combining with Meraki access points, 216–217

configuring non-Meraki VPN peer availability for MX and Z series devices, 24–25

configuring SSID availability on MR access points, 23–24

device, 25

switch, 157

TAm (Trust Anchor module), 284

telemetry, network, 146–147

temperature, humidity, and air quality sensor, 291–292

template/s, 2

best practices, 64–65

caveats and limitations, 62–64

configuration, 59, 60–61

MX security appliance, 60, 61, 63

VLAN, 60–61

creating, 59–60

local overrides, 61–62

MV cameras and, 63–64

subnetting and, 62–63

ThousandEyes, 110

threat detection, 115–116

timeline

access point, 235–236

client, 234

video, 269

topology

Layer 2, diagram, 53–55

Layer 3, diagram, 55–56

multicast, diagram, 55–56

reporting, 53

VPN, hub and spoke, 100

Topology View, 147–149

traffic

analysis and identification, 133–134

filters, 133, 134

segregation, 223

transport path, performance, 128–129

trap, SNMP, 29, 69–70

troubleshooting Meraki devices, 122

DM logging, 124

Local Status page, 122–124

MT sensors, 299–301

Safe Mode, 124

SDB (Support Data Bundle) logging, 124

trunk ports, 158

U

UDP probes, 128

updating, device name, 75–78

upgrade

firmware, 7, 8–9, 39–40, 178–179

staged, 149

uplink

auto-rollback on bad, 179–180

cellular, 120

5G line of sight, 120–121

CGNAT (Carrier Grade NAT), 121

prestaging for deployment, 121–122

SD-WAN over, 138–140

selection policy, 135–136

User Management portal, 18

user records, 3, 4

V

varifocal lens, 244

video

accessing

through Meraki Display App, 255

through Meraki mobile app, 255–257

through Meraki Vision Portal, 253–255

through the Dashboard, 252–253

event logs, 278–279

exporting, 276–278

sharing, 275–276

storage, 246

timeline, 269

walls, 267–268

virtual stacking, 177–178

VLAN

configuration template, 60–61

hybrid campus deployment, 154–156

in large wireless deployments, 215–216

profile, 164–165

VoIP Health page, 108–109

VoIP policy, 131

VPN, 92

Cisco AnyConnect, 94

Client, 93–94

exclusions, 143

hub and spoke topology, 100

Meraki Auto, 92

advanced configurations, 103–104

configuration, 98–100

deployment, 97–98

full tunnel versus split tunnel, 102

hub prioritization, 102

NAT traversal, 100–101

scaling, 101–102

monitoring, 110–112

non-Meraki, 94

W

Wake-on-LAN tool, 191

WAN Health page, 108–109

water/leak sensor, 287–288

Web Application Health page, 105–108

webhooks, 27–28, 66–67, 80–81

Wi-Fi 6E, 198

wireless deployment. *See also* **AP/s (access point/s); Meraki MR access points**

authentication, 214–215

channel width, 209

client/s, 232–234

details, 234

timeline, 234

DFS (Dynamic Frequency Selection) channels, 210–211

distributed data plane, 213–214

encryption, 214–215

floor plan, 226

Location Heatmap, 226

location-aware, 197–198

physical WLAN design, 197

RF profile, 202–204

security

AMI (Alternate Management Interface), 223

mandatory DHCP, 223

mDNS support, 224

per-SSID group policy, 223

RADSec, 224–225

SecurePort, 225

SSID configuration, 202

VLAN considerations, 215–216

Wireless Health feature, 50–52

Wireless Overview page, 227–228

X-Y-Z

X.509 certificate authentication, 4