

Securing Enterprise Networks with Cisco Meraki



ciscopress.com

RYAN CHANEY, CCIE® No. 16666
SIMERJIT SINGH, CCIE® No. 38710

FREE SAMPLE CHAPTER |



Securing Enterprise Networks with Cisco Meraki

Ryan Chaney, CCIE No. 16666
Simerjit Singh, CCIE No. 38710

Securing Enterprise Networks with Cisco Meraki

Ryan Chaney, Simerjit Singh

Copyright© 2025 Cisco Systems, Inc.

Published by:
Cisco Press
Hoboken, New Jersey

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

\$PrintCode

Library of Congress Control Number: 2024943927

ISBN-13: 978-0-13-829818-0

ISBN-10: 0-13-829818-1

Warning and Disclaimer

This book is designed to provide information about securing an enterprise network with Cisco Meraki. 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 authors and are not necessarily those of Cisco Systems, Inc.

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.

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification 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.

Microsoft and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published as part of the services for any purpose. All such documents and related graphics are provided “as is” without warranty of any kind. Microsoft and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement. In no event shall Microsoft and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from the services.

The documents and related graphics contained herein could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Microsoft and/or its respective suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time. Partial screenshots may be viewed in full within the software version specified.

Microsoft® and Windows® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. Screenshots and icons reprinted with permission from the Microsoft Corporation. This book is not sponsored or endorsed by or affiliated with the Microsoft Corporation.

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: Copy Editor: Chuck Hutchinson
Soo Kang

Technical Editors: Akhil Behl, Jeffry Handal

Alliances Manager, Cisco Press: Caroline Antonio

Editorial Assistant: Cindy Teeters

Director, ITP Product Management: Brett Bartow

Cover Designer: Chuti Prasertsith

Managing Editor: Sandra Schroeder

Composition: codeMantra

Development Editor: Christopher Cleveland

Indexer: Timothy Wright

Senior Project Editor: Tonya Simpson

Proofreader: Jennifer Hinchliffe



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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

About the Authors

Ryan Chaney, the lead author on this book, started his Cisco journey in his early 20s, completing his first CCIE (R+S) at the age of 25, before completing his second CCIE (Security) just 2 years later. Before joining Cisco, he worked in a variety of networking roles across the world, including time as a network architect for Visa in London. Ryan spent the first 10 years of his 15 years at Cisco as a systems engineer, educating customers, designing, and building IT solutions. His first experience with Meraki came while volunteering at the Royal Far West Centre for Country Kids, where he designed and built the network for their new headquarters in Manly, Sydney. At the time, no books had been published on Meraki. This experience and wanting to share his learnings with fellow network engineers, like you, became the inspiration for this book. Ryan lives in Bondi Beach, Australia.

Simerjit Singh, the contributing author on this book, is a seasoned Meraki solutions engineer with more than 17 years' tenure at Cisco. From his wealth of experience working with customers in the Enterprise and SMB segments, Simerjit contributes his vast experience of the diverse needs of these customers and relevant Meraki solutions. Simerjit holds highly regarded qualifications in networking and security, including a bachelor of technology in computer science, as well as both CCIE and ISC2 Certified Cloud Security Professional (CCSP) certifications. Committed to continuous learning and professional growth, Simerjit is currently pursuing a master's degree in cybersecurity from the Royal Melbourne Institute (RMIT). Simerjit lives in Melbourne with his mother, wife, and two sons.

About the Technical Reviewers

Akhil Behl is a passionate technologist and business development practitioner. He has more than 19 years of experience in the IT industry working across several leadership, advisory, consultancy, and business development profiles across OEMs, Telcos, and SI organizations. Akhil believes in cultivating an entrepreneurial culture, working across high-performance teams, identifying emerging technology trends, and ongoing innovation. For the last 7+ years he has been working extensively with hyperscalers across industry verticals—FSI, RCPG, transport, public sector, and mining. He is employed at Red Hat and leads the Global System Integrator (GSI) partner alliances for ANZ region across modernization, automation, cloud first Go-To-Market (GTM) motions.

Akhil is a published author. Over the span of past few years, he has authored multiple titles on security and business communication technologies. He has contributed as technical editor for more than a dozen books on security, networking, and information technology. He has published four books with Pearson Education's Cisco Press. He has published several research papers in national and international journals, including IEEE Xplore, and presented at various IEEE conferences, as well as other prominent ICT, security, and telecom events. Writing and mentoring is his passion and a part of his life. This is his fifth book.

Akhil holds CCIE No. 19564 Emeritus (Collaboration and Security), CompTIA Data+, Azure Solutions Architect Expert, Google Professional Cloud Architect, Azure AI Certified Associate, Azure Data Fundamentals, CCSK, CHFI, PMP, ITIL, VCP, TOGAF, CEH, ISM, CCDP, and other industry certifications. He has bachelors in Technology and masters in Business Administration degrees.

Akhil lives in Melbourne, Australia with his better half, Kanika, and two sons, Shivansh (11 years) and Shaurya (9 years). Both of them are passionate gamers and are excellent musicians, sporting guitar and keyboard, respectively.

In his spare time, Akhil likes to play cricket and console games with his sons, watch movies with family, and write articles or blogs.

Jeffrey Handal is a principal solutions engineer at Cisco. He completed his bachelors and masters 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, Jeffrey 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 (TACops, IPv6 Ambassadors, Security Technical Advisory Group, Meraki).

Outside of work, Jeffrey 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, Jeffrey serves the public through his participation in conferences and standards bodies (IETF, IEEE); speaks at local and international events (Internet2, CANS, IPv6 Summits, AI/ML Symposiums, IEEE events, WALC, Cisco Live); contributes to and reviews publications; and appears as a guest in podcasts like *IPv6 Buzz* and *Meraki Unboxed*. He is a big promoter of technological change for the betterment of humanity.

Dedications

First and foremost, I'd like to dedicate this book to my proud parents, Steve and Susanne, who encouraged me to fly high, enjoy life, and dream big. I could never have imagined such a project without their interest and enthusiasm for both reading and technology.

—*Ryan Chaney*

This book goes out to my family. My wife, your faith in my dreams has been my driving force. My sons, who carried on without me when I was working on this book. They always provided me with incredible support, and I simply couldn't achieve my goals without them. And to my brothers, who have given me encouragement, love, and wisdom to shape me into the person I am today. My mother, her unwavering love, patience, and encouragement have carried me through every storm and celebrated every success.

—*Simerjit Singh*

Acknowledgments

We'd like to heartfully acknowledge all those wonderful people, including many new names and faces, who selflessly supported us in our efforts to create this fantastic book.

First, we'd like to start by thanking Rob Soderbery, former SVP at Cisco and current CEO of Western Digital, for taking the time to share his memories of Cisco's acquisition of Meraki.

I (Ryan) would like to thank my contributing author, Simerjit Singh, for his time, knowledge, and professional network, which made this book possible.

We'd like to personally thank Fady Sharobeem, solutions engineer with Meraki and fellow CCIE, for his technical support and enthusiasm for this project. Likewise, Kabeer Noorudeen, CCIE, rock star and solutions engineer at Cisco, for his support.

I (Simerjit) would like to acknowledge Dimitri Polydorou for being an exceptional mentor. Dimitri, you have not only imparted guidance and support but also instilled confidence and inspired me to strive for excellence.

Thanks also to Sheela Kishan, security solutions engineer with Cisco, Duo guru, and fellow CCIE, for her help and support on all things Duo.

Similarly, a big thank you to Shweta Palande, technical marketing engineer at Meraki, for her technical support on ServiceNow.

A shout out and thanks go to Harry Lewins from AlgoSec. We could not have included AlgoSec without your support.

A big thank you to Tim Mallyon, Jacqueline Emery, Pip Crooks, and the whole Royal Far West team. It was working together that provided the inspirational spark for this book.

This book in its final form would not be what it is without the insights and enormous experience of our technical reviewers, Akhil Behl and Jeffry Handal.

Last, but most important, this book would not have been possible without the support of many people in the Cisco Press team. We'd like to thank Brett Bartow, director, IT Professional Product Management at Pearson Education, who was instrumental in sponsoring this book. A big thank you to Chris Cleveland, development editor, for your expertise and keeping us on track. Thanks also to Tonya Simpson, senior project editor, for getting us across the finish line. Finally, many thanks to the many other Pearson folks behind the scenes who made this project possible.

Contents at a Glance

	Introduction	xix
Chapter 1	Meraki's History	1
Chapter 2	Security Frameworks and Industry Best Practices	11
Chapter 3	Meraki Dashboard and Trust	19
Chapter 4	Role-Based Access Control (RBAC)	37
Chapter 5	Securing Administrator Access to Meraki Dashboard	61
Chapter 6	Security Operations	169
Chapter 7	User Authentication	257
Chapter 8	Wired and Wireless LAN Security	353
Chapter 9	Meraki MX and WAN Security	493
Chapter 10	Securing User Traffic	557
Chapter 11	Securing End-User Devices	671
Chapter 12	Physical Security	715
Appendix A	Comparison of Common Security Standards and Framework Requirements	729
	Index	757

Reader Services

Register your copy at www.ciscopress.com/title/9780138298180 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 9780138298180 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.

Contents

	Introduction	xix
Chapter 1	Meraki's History	1
	Roofnet	1
	Start-up	3
	Acquisition by Cisco	4
	The Meraki Museum	7
	Summary	7
	Notes	8
	Further Reading	8
Chapter 2	Security Frameworks and Industry Best Practices	11
	The Cybersecurity Imperative	11
	Adopting Industry Best Practice	13
	Industry Standards	13
	Security as a Team Sport	15
	Key Themes Across Security Standards	15
	Continuous Improvement	16
	Comparison of Common Security Standards and Framework Requirements	16
	Summary	17
	Further Reading	17
Chapter 3	Meraki Dashboard and Trust	19
	Meraki Dashboard	19
	Out-of-Band Management	20
	Meraki Dashboard Hierarchy	20
	Trust	22
	Privacy	23
	<i>Data Retention Policy</i>	24
	Data Security	24
	Data Center Resiliency	26
	Compliance with Information Standards, Regulations, and Industry Best Practices	26
	Hardware Trust Model	28
	<i>Supply Chain Security</i>	28
	<i>Secure Boot</i>	29

	<i>Secure Device Onboarding</i>	29
	Software Trust Model	30
	Cloud Shared Responsibility Model	32
	Summary	32
	Notes	33
	Further Reading	33
Chapter 4	Role-Based Access Control (RBAC)	37
	Meraki Dashboard's Administration Hierarchy	38
	Administrator Access Levels for Dashboard Organizations and Networks	38
	Assigning Permissions Using Network Tags	40
	Port-Level Permissions	42
	Role-Based Access Control for Camera-Only Administrators	49
	Role-Based Access Control for Sensor-Only Administrators	52
	Role-Based Access Control Using Systems Manager Limited Access Roles	53
	Summary	60
	Further Reading	60
Chapter 5	Securing Administrator Access to Meraki Dashboard	61
	Securing Administrative Access to Meraki Dashboard	61
	Meraki Dashboard Local Administrator Access Controls	62
	<i>Creating Meraki Dashboard Local Administrator Accounts</i>	62
	<i>Password Age</i>	68
	<i>Password Reuse</i>	70
	<i>Password Complexity</i>	72
	<i>Account Lockout After Invalid Login Attempts</i>	74
	<i>Idle Timeout</i>	77
	<i>IP Whitelisting</i>	79
	<i>Multifactor Authentication (MFA)</i>	81
	Configuring SAML Single Sign-On (SSO) for Dashboard	98
	The Use Cases for Single Sign-On	98
	SAML Single Sign-On Login Flow	99
	SAML Single Sign-On Design	99
	Configuring Meraki SAML SSO Using Cisco Duo and Microsoft Entra ID	102
	<i>Prerequisites</i>	103
	<i>Adding SP-Initiated SAML SSO</i>	146

Verifying SAML SSO Access to Meraki Dashboard with Cisco Duo and Microsoft Entra (Including Duo Inline Enrollment) 148

Implementing Additional Access Controls Using Cisco Duo and Microsoft Entra ID	159
Password Policies	159
<i>Password Age</i>	160
<i>Password Reuse</i>	160
<i>Password Complexity</i>	160
<i>Account Lockout After Invalid Login Attempts</i>	160
Security Policies	161
<i>IP Whitelisting</i>	161
<i>Restricting Concurrent Logins</i>	162
<i>Automatically Disabling Inactive Accounts</i>	162
<i>Automatically Disabling Accounts After a Predetermined Period of Time Unless Revalidated</i>	163
<i>Automatically Disabling Temporary Accounts</i>	165
Summary	165
Further Reading	166

Chapter 6 Security Operations 169

Centralized Logging Capabilities	170
Login Attempts	172
Change Log	172
Event Log	174
Creating API Keys	175
Finding Your Organization ID	180
Exporting Logs	180
Exporting Logs to Splunk	181
Syslog	190
Exporting Flow Data	192
NetFlow, IPFIX, and Encrypted Traffic Analytics	193
Syslog Flows	196
Compliance Reporting with AlgoSec	197
Prerequisites	197
Integrating AlgoSec with Meraki Dashboard for Compliance Reporting	197

Monitoring and Incident Response	208
Security Center	209
Alerts	210
External Alerting	213
<i>Webbooks</i>	213
<i>SNMP Traps</i>	224
External Polling	227
Meraki Dashboard API	228
SNMP	234
Automated Incident Response with ServiceNow	240
Security Management	246
Inventory	247
<i>Hardware</i>	247
<i>Software</i>	248
<i>Configuration</i>	249
<i>Client Devices</i>	251
Topology	252
Summary	253
Notes	253
Further Reading	254
Chapter 7	User Authentication 257
Configuring Meraki Cloud Authentication	260
Configuring SAML with Cisco Duo and Microsoft Entra	264
Confirming Functionality of SAML Configuration Using AnyConnect VPN	273
Configuring RADIUS Using Cisco ISE, Cisco Duo, and Microsoft Active Directory	276
Prerequisites	277
Configuring Users and Groups in Microsoft Active Directory	280
<i>Configuring Group(s) in Active Directory</i>	280
<i>Configuring User(s) in Active Directory</i>	281
Configuring Cisco Identity Services Engine (ISE)	285
<i>Adding Network Access Devices (NADs) to Cisco ISE</i>	285
RADIUS Configuration for Wired and Wireless 802.1X	295
<i>Configuring Organization-Wide RADIUS in Meraki Dashboard</i>	295
<i>Creating a Policy Set for Wired and Wireless 802.1X in Cisco ISE</i>	300

<i>Configuring an Authentication Policy in Cisco ISE</i>	304
<i>Configuring an Authorization Policy in Cisco ISE</i>	305
<i>Confirming Functionality of RADIUS Authentication on Wireless</i>	308
<i>Confirming Functionality of RADIUS Authentication for Wired 802.1X</i>	312
RADIUS Configuration for AnyConnect VPN with Duo MFA	315
<i>Configuring Duo Authentication Proxy</i>	317
<i>Configuring AD Sync in Duo Admin Panel</i>	319
<i>Encrypting Passwords in Duo Authentication Proxy</i>	330
<i>Enrolling Users with Cisco Duo</i>	330
<i>Configuring Cisco Duo as an External RADIUS Server in Cisco ISE</i>	335
<i>Creating the Policy Set for AnyConnect VPN in Cisco ISE</i>	337
Meraki Dashboard Using Active Directory Authentication for AnyConnect VPN	342
Prerequisites	342
Configuring Active Directory Authentication	346
Confirming Functionality of Active Directory Configuration	348
Summary	350
Further Reading	350
Chapter 8	Wired and Wireless LAN Security 353
Access Control Lists and Firewalls	354
Access Control Lists (Meraki MS)	354
Meraki MR Firewall	357
<i>Layer 3 Firewall</i>	358
<i>Layer 7 Firewall (Including NBAR Content Filtering)</i>	360
Ethernet Port Security Features (Meraki MS)	362
MAC Allow Lists	362
Sticky MAC Allow Lists	366
Port Isolation	368
SecurePort	370
Dynamic ARP Inspection	373
Rogue DHCP Server Detection (Meraki MS)	376
Hardening Meraki MR and MS Devices (Local Status Page)	379
Zero Trust (Wired and Wireless Dot1x)	382
802.1X with Protected EAP (PEAP) on Wired and Wireless Networks	383

<i>Configuring Wireless 802.1X with Protected EAP (PEAP)</i>	383
<i>Configuring Wired 802.1X with Protected EAP (PEAP)</i>	388
Configuring 802.1X Using EAP-TLS on Wired and Wireless Networks	394
<i>Configuring the Identity Source Sequence in Cisco ISE</i>	396
<i>Configuring the Policy Set in Cisco ISE</i>	398
<i>Generating a Client Certificate Using Cisco ISE</i>	404
<i>Exporting the Cisco ISE Certificate Authority Certificate</i>	408
<i>Testing Wireless 802.1X with EAP-TLS</i>	411
<i>Testing Wired 802.1X with EAP-TLS</i>	413
Sentry-Based 802.1X with EAP-TLS on Wired and Wireless Networks	416
Sentry Wi-Fi	416
Sentry LAN	419
Configuring MAC Authentication Bypass (MAB)	426
<i>Configuring an Endpoint Identity Group in Cisco ISE</i>	426
<i>Creating a Policy Set in Cisco ISE for MAC Authentication Bypass</i>	430
<i>Configuring Wireless MAC Authentication Bypass in Meraki Dashboard</i>	436
<i>Configuring Wired MAC Authentication Bypass in Meraki Dashboard</i>	439
Group Policies	443
Creating a Group Policy	443
Applying Group Policies	446
<i>Applying Group Policies to a Client Manually</i>	446
<i>Applying Group Policies Using a Sentry Policy</i>	449
<i>Applying Group Policies Using RADIUS Attributes and Cisco ISE</i>	452
Adaptive Policy and Security Group Tags (SGTs)	459
Enabling Adaptive Policy	460
Configuring Security Group Tag Propagation	461
<i>Enabling SGT Propagation on Meraki MS Switches</i>	461
<i>Enabling SGT Propagation on Meraki MX Security Appliances</i>	463
Creating Security Group Tags	466
<i>Creating Adaptive Policy Groups in Meraki Dashboard</i>	466
<i>Creating Security Group Tags in Cisco ISE</i>	469
Assigning Security Group Tags	472

<i>Statically Assigning Security Group Tags to SSIDs</i>	472
<i>Statically Assigning Security Group Tags to Switch Ports</i>	473
<i>Assigning Security Group Tags Using Cisco ISE</i>	475
Creating an Adaptive Policy	476
Testing Adaptive Policy	479
<i>Client Laptop</i>	480
<i>POS Terminal</i>	480
<i>POS Server</i>	483
<i>Testing</i>	483
Wireless Security	487
Summary	489
Notes	489
Further Reading	490

Chapter 9 Meraki MX and WAN Security 493

Meraki MX Introduction	493
Site-to-Site VPN (Auto VPN)	494
Site-to-Site VPN with Non-Meraki Devices	499
ThousandEyes	505
Remote-Access VPN	507
Client VPN	508
Sentry VPN	514
AnyConnect VPN	519
<i>Confirming Functionality of AnyConnect VPN Access</i>	524
Restricting Client VPN Traffic	529
Virtual MX (vMX)	531
Sizing a Virtual MX	531
Understanding Feature Parity with Meraki MX	532
Deploying Virtual MX in Amazon Web Services (AWS)	533
<i>Creating a New vMX Network in Meraki Dashboard</i>	533
<i>Configuring the Default VPC in AWS</i>	536
<i>Deploying vMX in AWS</i>	541
<i>Viewing the New vMX in Meraki Dashboard</i>	552
Summary	553
Notes	554
Further Reading	554

Chapter 10 Securing User Traffic 557

Comparison of Meraki's Native Security Capabilities and Cisco Secure Connect	558
Native Meraki MX Capabilities	559
Layer 3 Firewall	559
Layer 7 Firewall	563
Geo-IP Firewall	566
<i>Enabling Detailed Traffic Analysis</i>	566
<i>Configuring Geo-IP Firewall</i>	567
Content Filtering	570
<i>URL Filtering</i>	570
<i>Category Blocking with Cisco Talos Intelligence</i>	572
Threat Protection	576
<i>Advanced Malware Protection (AMP)</i>	576
<i>Intrusion Detection and Prevention (IDS/IPS)</i>	580
Cisco Secure Connect	582
Setting Up Secure Connect	584
<i>Initial Setup and Integration with Cisco Umbrella</i>	586
<i>Adding Meraki SD-WAN Sites to Secure Connect</i>	597
<i>Configuring DHCP to Assign Umbrella's DNS Servers</i>	601
<i>Installing Umbrella's Root CA Certificate on Clients</i>	602
<i>Enabling Intelligent Proxy and SSL Decryption in Cisco Umbrella</i>	603
DNS Security	606
Cloud Firewall	608
<i>Layer 3/4 Firewall</i>	608
<i>Application Blocking</i>	614
<i>Intrusion Detection and Prevention (IDS/IPS)</i>	620
Secure Web Gateway (SWG)	622
<i>URL Filtering (Destination Lists)</i>	622
<i>Content Filtering (Content Categories)</i>	631
<i>File Inspection and Advanced Sandboxing</i>	636
<i>File Type Control</i>	645
Cloud Access Security Broker (CASB)	649
Data Loss Prevention (DLP)	657
Summary	667
Notes	667
Further Reading	667

Chapter 11 Securing End-User Devices 671

- Integrating with Vender Mobile Device Enrollment Programs 672
- Enrolling Devices with Systems Manager 676
- Checking Compliance with Security Policy (Systems Manager Policies) 677
- Creating a Systems Manager Profile 681
- Configuring End-User Devices for Network Connectivity 684
 - Certificate Settings Payload 684
 - Wi-Fi Settings Payload 686
 - VPN Settings Payload 693
- Applying Security Policy to Devices (Systems Manager Profiles) 697
 - Passcode Policy (Includes Screen Lock) 697
 - Disk Encryption 700
 - Preventing the Installation of Banned Apps 700
- Deploying Applications to Devices 704
- Pushing Operating System Updates to Devices 711
- Summary 712
- Notes 713
- Further Reading 713

Chapter 12 Physical Security 715

- Meraki MV Security Cameras 716
 - Privacy 716
 - Monitoring Video 717
 - Motion Alerts 719
 - Motion Search 721
- Sensor Sight (Meraki Smart Camera and Sensor Integration) 724
- Summary 727
- Further Reading 727

Appendix A Comparison of Common Security Standards and Framework Requirements 729

Index 757

Introduction

Despite Meraki's huge success and wide adoption, at the time we started this project, no one had written a book about Cisco's Meraki product lines. After helping organizations to deploy Meraki, we realized that it was time for this to change. As a result, we sought to create a book that enables more organizations to adopt cloud-managed infrastructure and build better, more modern, and more secure networks.

Our goal is to show you that Meraki can be used, not just to build secure networks, but as the foundation for a more secure enterprise as a whole. By researching as many of the common IT security standards and frameworks as we could find, we gathered together over a hundred common security requirements that we believe you can solve with a Meraki solution. With this goal in mind, we show how Cisco Meraki, either on its own or when easily integrated with complementary products, can be deployed to meet the requirements of the most common IT security standards.

Guided by the requirements of industry best practices, the topics in this book stretch beyond what might be considered traditional networking roles, perhaps with a view to secure networking roles of the future. As such, the target audience includes roles covering IT security, networking, and systems, such as:

- All new Meraki customers
- Experienced networking engineers looking to upskill on cloud-managed networking
- The next generation of networking and IT professionals who may be just starting their careers and have basic CCNA-level networking knowledge
- Multidisciplined, lean IT teams
- IT managers looking to streamline and modernize operations

The book is organized as follows:

- **Chapter 1, Meraki's History:** This chapter recounts the history of Meraki from its beginnings as a research project at the Massachusetts Institute of Technology (MIT). It charts the intersection of the explosive growth in Wi-Fi devices and broadband Internet, with the launch of Meraki as a start-up. The chapter concludes with the story of Meraki's acquisition by Cisco, including an interview with Rob Soderbery, then SVP of Cisco's Enterprise Networking Group.
- **Chapter 2, Security Frameworks and Industry Best Practices:** This chapter opens by highlighting the consequences of IT security failures. Common IT standards and frameworks are introduced as the conversation shifts to how to minimize IT risk and industry best practices. Finally, this chapter identifies the nine key themes that you must consider when designing and implementing Meraki solutions.

- **Chapter 3, Meraki Dashboard and Trust:** This chapter introduces the Meraki management portal, Meraki Dashboard, before addressing the common considerations when adopting cloud-managed infrastructure. This includes discussions around privacy, data security, resiliency, compliance, hardware, and software trust. With a full understanding of these topics and the steps Cisco has taken to address them, organizations should feel confident in adopting Cisco Meraki solutions.
- **Chapter 4, Role-Based Access Control (RBAC):** RBAC is one of the nine key themes identified from industry best practices. Being central to the principle of least privilege, RBAC receives its own dedicated chapter. This chapter introduces and demonstrates the RBAC capabilities available in Meraki Dashboard.
- **Chapter 5, Securing Administrator Access to Meraki Dashboard:** This chapter discusses the need for strong authentication and multifactor authentication (MFA) in relation to administrator access to Meraki Dashboard. Here, we guide you through the configuration of Meraki Dashboard's native controls. This chapter also demonstrates the enhanced capabilities available when using SAML single sign-on (SSO). This includes a full step-by-step guide, showing how to implement SAML SSO with MFA using Meraki, Cisco Duo, and Microsoft Entra.
- **Chapter 6, Security Operations:** This chapter covers the native Meraki toolset to support a security operations center. Also covered is the implementation of external solutions providing compliance reporting, centralized logging including Cisco Splunk, polling, the Meraki Dashboard API, alerting, and incident response.
- **Chapter 7, User Authentication:** User access authentication is an essential part of an enterprise's zero trust architecture. This chapter covers the configuration of the authentication infrastructure in support of authenticating user access via wired, wireless, and VPN. This includes implementing Meraki Cloud Authentication, SAML, and RADIUS (with and without MFA). This chapter covers RADIUS extensively, including the full configuration steps for Cisco Identity Services Engine (ISE) and Cisco Duo. This chapter is a prerequisite for Chapter 8.
- **Chapter 8, Wired and Wireless LAN Security:** This chapter covers two main topics—first, how to implement authentication for wired and wireless users. This includes step-by-step guided configuration of 802.1X, Sentry-based access, and MAC Authentication Bypass (MAB). The second major topic discusses those network-based security features available on Meraki MS and MR devices. This includes the implementation of firewalling, Layer 2 switching features such as port isolation, as well as group policies and adaptive policies.
- **Chapter 9, Meraki MX and WAN Security:** Encryption is vital for protecting the confidentiality and integrity of data over public networks. This chapter shows how various VPN types—client VPN, Sentry VPN, AnyConnect VPN, and site-to-site VPN (Auto VPN)—can be implemented using Meraki MX. This chapter also introduces Meraki virtual MX (vMX), stepping through how to extend your secure Meraki SD-WAN into public cloud. This includes a step-by-step guide to setting up Meraki vMX in Amazon Web Services (AWS).

- **Chapter 10, Securing User Traffic:** This chapter discusses the various ways administrators can secure Internet traffic both natively and using the recently released Secure Connect. This includes such features as URL filtering, IDS/IPS, content filtering, Advanced Malware Protection (AMP), and much more. Secure Connect is a must-have solution bringing advanced functionality that will be new for a lot of readers. Of particular interest are the Cloud Access Security Broker (CASB) and Data Loss Prevention (DLP) capabilities. This chapter shows how, using these capabilities, administrators can reduce the risk of sensitive data leaving their organization via webmail, email attachments, file uploads, and via generative AI platforms like ChatGPT.
- **Chapter 11, Securing End-User Devices:** Meraki Systems Manager, Meraki's own mobile device management (MDM) solution, helps organizations manage corporate devices in line with industry best practices. This chapter shows how Systems Manager provides an important role through enabling organizations to take advantage of Sentry-based policies for 802.1X on wired and wireless. You also learn how to apply your own profiles to managed devices, simplifying the deployment of wireless and VPN access.
- **Chapter 12, Physical Security:** This chapter focuses on the capabilities of Meraki's MV smart camera solution, covering all the topics relevant for monitoring the physical environment, such as a data center. This chapter addresses important topics like privacy, before delving into video walls, motion alerts, motion search, and other capabilities required by today's security operation centers.
- **Appendix A, Comparison of Common Security Standards and Framework Requirements:** This book has been created to help you understand today's IT security requirements and how to meet them using Cisco Meraki. This appendix shows the mapping between IT security requirements, security standards, and where each topic is addressed in this book. This helpful resource enables you to visualize the breadth, commonality, and key themes across industry best practices.

Figure Credits

Cover Page: PeopleImages.com - Yuri A/Shutterstock.

Figures 1-1, 1-2: Sanjit Biswas

Figure 1-3: Rob Soderbery

Figures 2-1, 10-115, 10-117, 10-126d, 10-140, 10-142, 10-143: Google

Figures 5-73–5-92, 5-95–5-97, 5-105–5-113, 5-116–5-145, 5-161–5-163, 5-174, 5-175, 5-180, 5-183–5-185, 7-15–7-20, 7-27–7-38, 7-112, 7-133, 7-135, 7-136, 10-126c: Microsoft

Figure 6-35: Solarwinds

Figures 6-40–6-56: AlgoSec

Figures 6-62–6-71,6-78: PagerDuty

Figures 6-86, 7-89, 7-90, 8-6, 8-24, 8-48–8-50, 8-77, 8-78, 8-80, 8-81, 8-85, 8-127, 8-179, 8-180, 9-21, 9-22, 9-27–9-30, 9-42, 9-43, 10-3, 10-7, 10-13, 10-14, 10-17, 10-23, 10-28, 10-72, 10-73, 10-80, 10-126a, 11-3, 11-4, 11-25, 11-26, 11-34, 11-41–11-43: Apple Inc.

Figures 6-87–6-93: JetBrains

Figures 6-103–6-111: ServiceNow

Figures 7-134, 8-181, 8-182: Wireshark

Figures 9-47–9-73, 10-126b: Amazon Web Services, Inc.

Figure 10-27: EICAR

Figures 10-145, 10-146: Open AI

Role-Based Access Control (RBAC)

In this chapter, you learn the following:

- The organizational hierarchy and the built-in access levels available in Meraki Dashboard
- The various roles available in Meraki Dashboard
- How to configure role-based access control (RBAC) within Meraki Dashboard to adhere to the principle of least privilege

The principle of least privilege and role-based access control (RBAC) are key themes across industry best practices. RBAC is an essential feature that enables you to assign appropriate access rights to users based on their roles and responsibilities. Practical use cases for differentiated administrative roles include the following:

- Providing help-desk staff with limited access to Dashboard to be able to collect vital troubleshooting information, thereby enabling incidents to be resolved faster.
- Providing CCTV operators with the access they need to view and edit footage, while limiting access to network settings.
- Assigning limited read-write access for junior administrators. Having fewer admins with full access at the organizational level reduces the likelihood of mistakes that can have a wide-ranging impact.

Meraki Dashboard incorporates RBAC, providing a built-in way to precisely control administrative access to specific parts of the Meraki organization. In addition to the built-in roles, you can create distinct and granular roles if required.

Meraki Dashboard's Administration Hierarchy

Meraki Dashboard administrator privileges are controlled at the organization and network levels:

- Organization administrators have visibility of the organization and all its networks. Organizational admins do not necessarily have the highest permissions. Access can be restricted; for example, it is possible to have an organizational administrator with only read-only access.
- Network administrators have visibility of individual networks. Network administrators can have complete or limited control over these networks but do not have access to organization-level information (licensing, device inventory, and so on) unless granted such access at the organization level.

The privileges grant control over what a user can see and do in Meraki Dashboard. Permissions granted at the organization level cannot be reduced at the network level. If required, a user can have access to multiple networks and multiple organizations. We cover how to assign access to multiple networks later in the section titled “Assigning Permissions Using Network Tags.”

For more information on the Meraki Dashboard's hierarchical structure, see https://documentation.meraki.com/General_Administration/Organizations_and_Networks/Meraki_Dashboard_Organizational_Structure.

Administrator Access Levels for Dashboard Organizations and Networks

Three levels of administrative access are available at the organization level:

- **None:** Users will have no access to the organization, meaning they cannot perform any actions or view any configurations at the organization level. They may, however, still have privileges assigned at the network level.
- **Read-Only:** Users with read-only access can view the Dashboard configurations for the organization but cannot make any changes. This includes the ability to view video footage if the organization has cameras. Be aware that administrators may still have privileges assigned at the network level.
- **Full:** Users with full access have access to all parts of Dashboard (including cameras), can make configuration changes, and can even delete the organization. This access level should be limited to suitably qualified and trusted personnel.

Four additional levels of access are available when configuring privileges at the network level:

- **Full:** This level grants full access to the target network, including the ability to view all of the Dashboard and change any configuration settings (see Figure 4-1).

The screenshot shows a web form titled "Update administrator" with a close button (X) in the top right corner. The form contains the following fields and sections:

- Name:** A text input field containing "John Smith".
- Email:** A text input field containing a partially visible email address.
- Organization access:** A dropdown menu set to "None".
- Target:** A dropdown menu set to "Bondi Beach".
- Access:** A dropdown menu set to "Full".
- + Add access privileges:** A green link below the Target dropdown.
- Update camera and sensor permissions:** A section header.
- Camera and sensor permissions must be edited on each Network's admin page. Refresh this page to view your changes.** A text instruction.
- Bondi Beach:** A dropdown menu.
- Navigate:** A green link next to the dropdown.
- privacy:** A link at the bottom left.
- Close:** A button at the bottom center.
- Update admin:** A blue button at the bottom right.

Figure 4-1 An Example of an Administrator Configured as a Network-Only Admin

- **Read-Only:** With this level, users can view all configurations in the target network but are restricted from making any modifications.
- **Monitor-Only:** Administrators with this access level can view a dedicated monitor page in the Dashboard but cannot make any changes. Users with this access level can monitor and analyze network performance metrics, troubleshoot issues, and gain insights into the network's health and performance.
- **Guest Ambassador:** This level of access is intended for managing user access to Wi-Fi or client VPN access. The most common use case for this role is a hotel receptionist or lobby ambassador needing to provide temporary (time-bound) Wi-Fi access for guests and visitors. Staff with this access level can manage guest users, granting or revoking access as needed. When logging in, the Guest Ambassador user is presented with a purpose-built user management portal. It allows them to efficiently manage guest user accounts without having access to other parts of the Dashboard.

Note You cannot assign full access to a user at the organization level and then assign only read-only permissions at the network level. Dashboard will give you a warning if you try to do this. If you want to create some network-focused admin users, you can grant read-only or no access (none) at the organization level and then the desired access at the network level.

Tip For more information on managing Dashboard administrators and permissions, check out https://documentation.meraki.com/General_Administration/Managing_Dashboard_Access/Managing_Dashboard_Administrators_and_Permissions. Alternatively, search for “Managing Dashboard Administrators and Permissions” using Search Dashboard in the top right of Meraki Dashboard.

Assigning Permissions Using Network Tags

If you’re not using configuration templates, then here’s a handy little tip that will save you a ton of time when it comes to administering admin users. Because you will have a network for every location, grouping them together in a logical way will make assigning administrative rights far easier. In Dashboard, group networks by assigning them a common tag. Then, when granting access to administrators, select only the tag name rather than all the individual network names. Tagged networks appear with the prefix *Tag:* in the **Target** list on the **Organization Administrators** page.

Follow these steps to tag your networks and assign administrator access using them:

- Step 1.** Log in to Meraki Dashboard (<https://dashboard.meraki.com>).
- Step 2.** Navigate to **Organization > Overview** (under Monitor), as demonstrated in Figure 4-2.

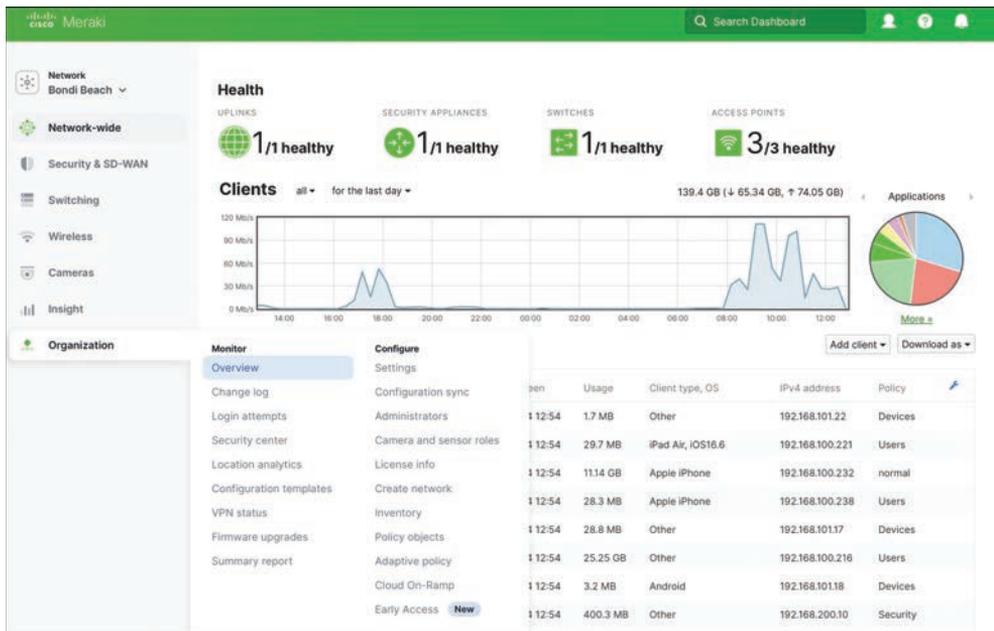


Figure 4-2 Navigating to the Organization Overview Page

Step 3. Select the check box or boxes next to the network(s) you want to tag, as demonstrated in Figure 4-3.



Figure 4-3 *The Organization Overview Page*

Step 4. Click **Tag** and then enter the tag name you would like to create. In the case illustrated in Figure 4-4, we used the tag **Stores**. Click **Add**. The Add button will change to Updating, then quickly turn green, then change to Updated, before changing back to Add.

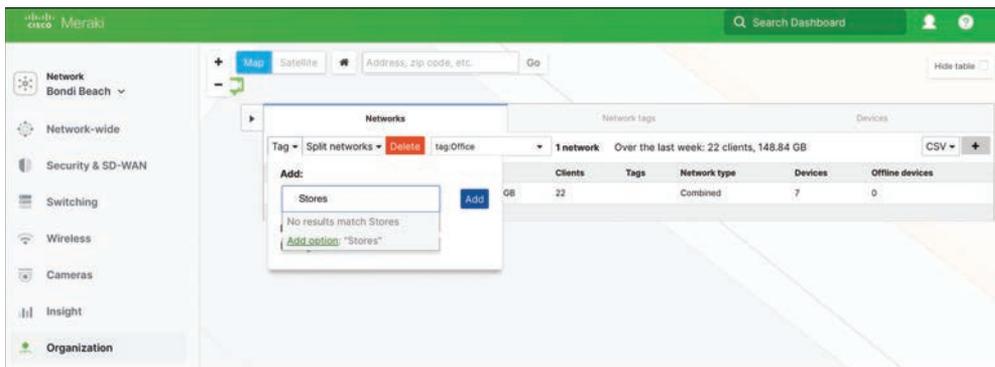


Figure 4-4 *Creating New Network Tags*

You can now see the tag next to the network name selected previously, confirming that the changes have been applied, as demonstrated in Figure 4-5.

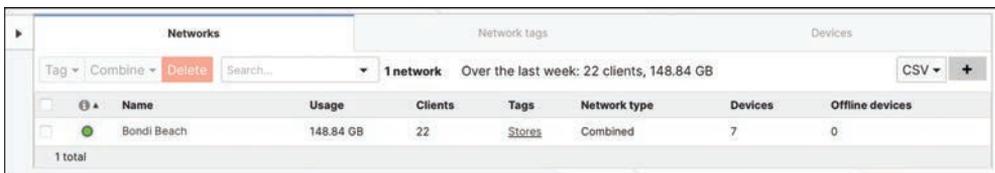


Figure 4-5 *Confirming Networks Are Now Tagged*

Step 5. When updating organization administrator privileges (**Organization > Administrators**), you can now see the Stores group created with the prefix

Tag: in the **Target** list, as demonstrated in Figure 4-6. From here, just assign access the same way you would to a regular network, by choosing the access level from the **Access** drop-down menu and clicking **Update Admin**.

The screenshot shows a web interface titled "Update administrator". It contains the following elements:

- Name:** John Smith
- Email:** [Redacted]
- Organization access:** Read-only
- Target:** A search box with a magnifying glass icon. Below it is a list of tags:
 - Tag: Stores (highlighted in blue)
 - Bondi Beach
 - All cameras in this organization
- Access:** Full
- Target Selection:** Bondi Beach (selected in a dropdown menu)
- Buttons:** Close, Update admin, and a green "Navigate" button.
- Footer:** A "privacy" link.

Figure 4-6 Assigning Administrator Access to a Group Using Tags

Port-Level Permissions

In Meraki Dashboard it is possible to provision read-only administrator accounts with read-write access to selected switchports. In traditional networks, doing this wasn't easy, so we avoided it. However, now that the capability exists, some immediate use cases come to mind:

- Labs, teaching environments, dormitories, and the like. If you have any such environments in your network, you can now provide limited admin access to staff or students without having to provide them with admin access to the rest of the network. With the access locked down, if required, you could continue to serve regular users off the remaining ports.
- Multitenanted environments like airports or shopping centers. In a multitenanted environment where you're responsible for providing network connectivity to businesses inside your premises, you could provide tenants with admin access to the ports serving just their premises. Because the control is down to the port level, potentially you could now share switches between tenants where you previously had provided a switch per tenant, reducing costs.

Follow these steps to tag your ports and configure roles with port-level permissions:

- Step 1.** Log in to Meraki Dashboard (<https://dashboard.meraki.com>).
- Step 2.** Navigate to **Switching > Switch Ports** (under Monitor), as demonstrated in Figure 4-7.

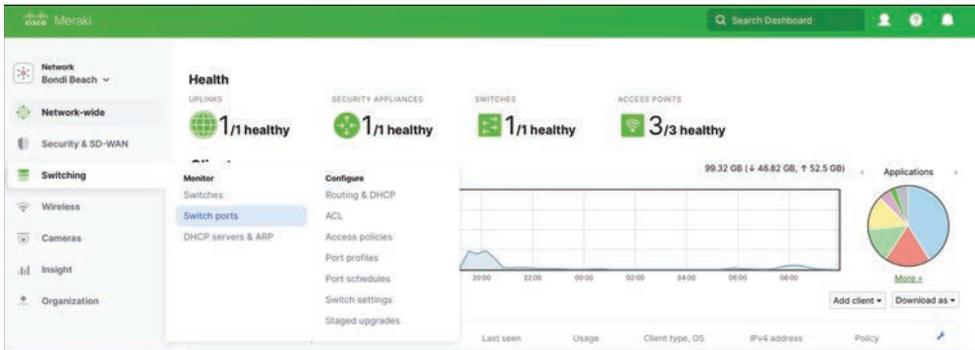


Figure 4-7 Navigating to the Switch Ports Page

- Step 3.** Select the ports that you want to tag using the check box next to their name, as demonstrated in Figure 4-8.

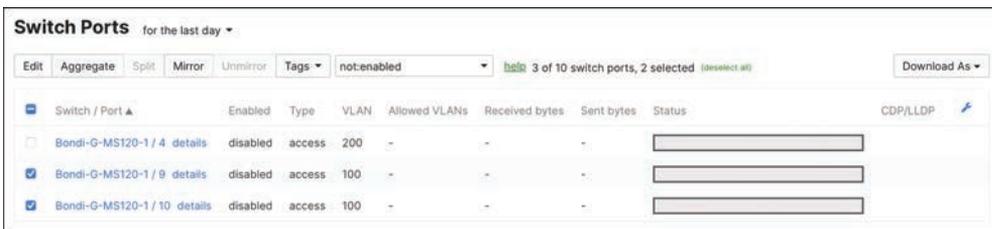


Figure 4-8 Selecting Ports to Tag

- Step 4.** Click the **Tags** drop-down menu and enter the name for a new tag or select an existing tag. In the example in Figure 4-9, we added the tag **Lab**. Click **Add** to confirm the changes.

If you have the Tags column enabled (click the spanner symbol on the far-right column name to customize the columns displayed), you see the new tag associated with these ports, as demonstrated in Figure 4-10.

- Step 5.** Navigate to **Network-wide > Administration** to open the Network administration page, as demonstrated in Figure 4-11.
- Step 6.** Scroll down to the **Port Management Privileges** section and click **Add a Port Management Privilege**.

The privilege name is displayed in the **Access** drop-down menu when this role is assigned to administrators, as demonstrated in Figure 4-12. Enter a privilege name that makes sense for your use case; then select the port tags that apply.

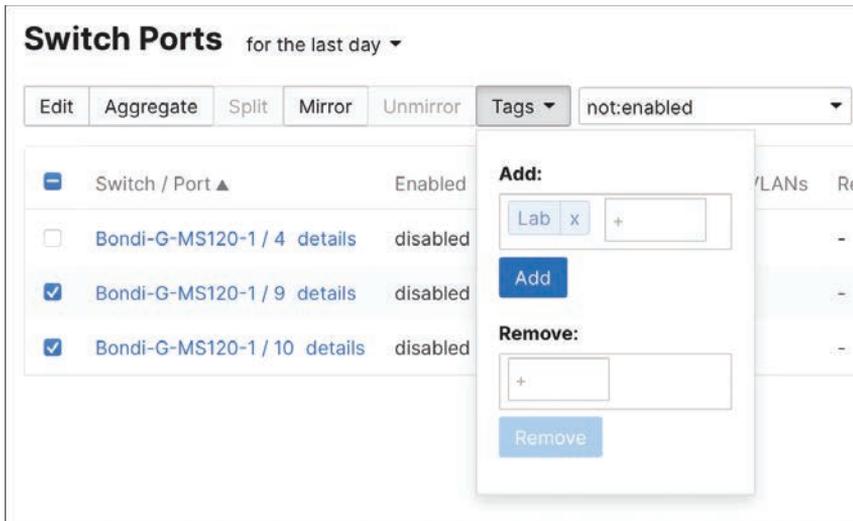


Figure 4-9 Creating Port Tags

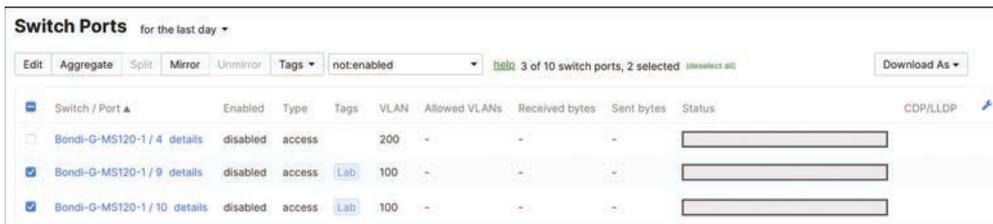


Figure 4-10 Showing Port Tags on the Switch Port Page

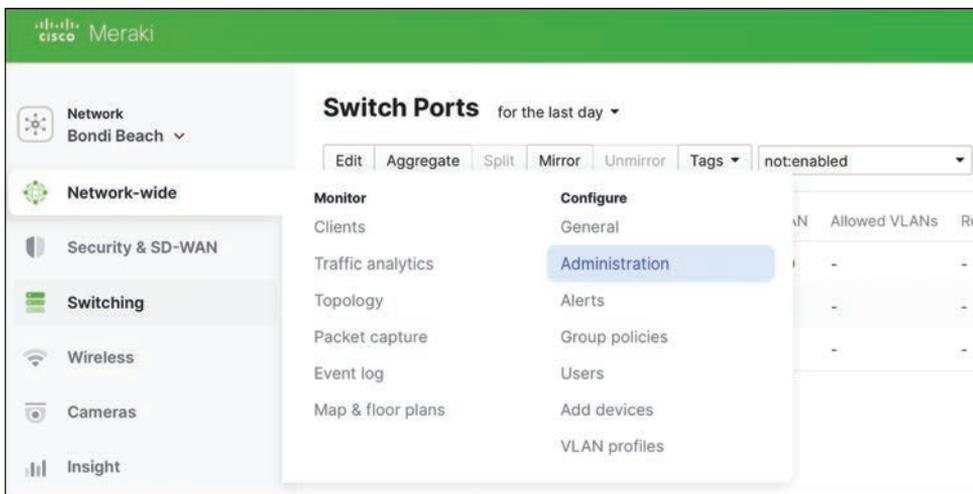


Figure 4-11 Navigating to the Network Administration Page



Figure 4-12 *Creating a Port Management Role*

Step 7. Decide whether this role should be able to do packet captures on these ports (the default is Allowed), as demonstrated in Figure 4-13, and then click Save in the bottom-right corner. A message at the top of the screen confirms that the changes have been saved.



Figure 4-13 *Selecting Packet Capture Permissions*

Step 8. Navigate to **Organization > Administrators** to open the Organization administrators page, as demonstrated in Figure 4-14.

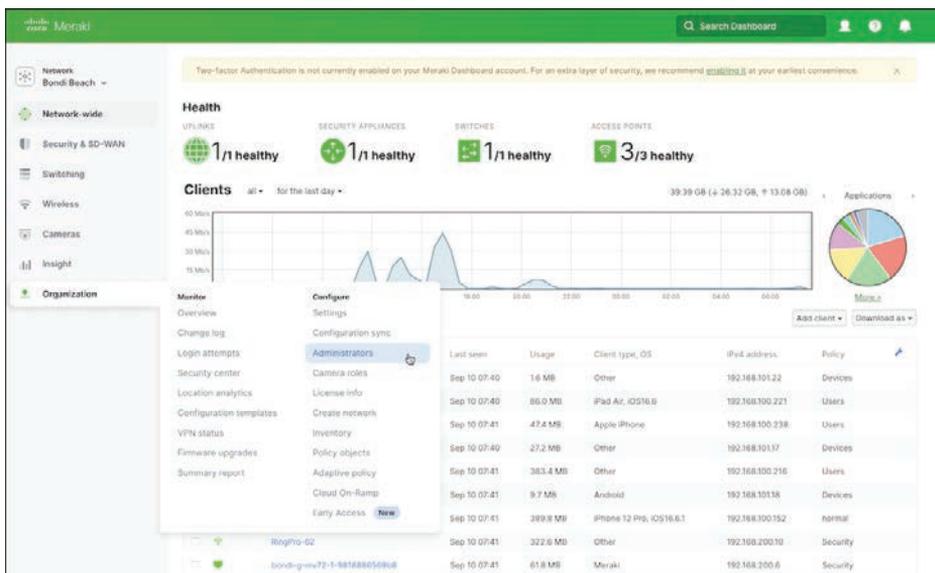


Figure 4-14 *Navigating to the Organization Administrators Page*

- Step 9.** Click the name or email address of an existing administrator that you want to modify (or create a new one), as demonstrated in Figure 4-15.

<input type="checkbox"/>	Name ^	Email address	Privilege ⓘ	Account status ⓘ	Authentication method	Two-factor authentication	Has API key	Last active
<input type="checkbox"/>	John Smith		Organization (Read)	Ok	Email	Off	No	17 Sep 2023 at AEST

-1 total

Figure 4-15 *The Organization Administrators Page (Port-Based Permissions)*

- Step 10.** Set the Organization access to **Read-only** or **None** and then select the target network. At the time of writing, the target network cannot be a tagged group of networks—that is, one starting with *Tag:*. In Figure 4-16, you can now select the Lab admins role created in the Access drop-down menu.

Update administrator ✕

Name:

Email:

Organization access: **Read-only** ⓘ

Target

Access

- ✓ Full ⓘ
- Read-only
- Monitor-only
- Lab admins**
- Guest Ambassador

Update camera and sensor permissions

Camera and sensor permissions must be edited on each Network's admin page. Refresh this page to view your changes.

[privacy](#)

Figure 4-16 *Assigning Port-Level Permissions on the Organization Administrators Page*

- Step 11.** Click **Update Admin** to save the changes.

Perform the following steps to verify that these changes are now in effect:

- Step 1.** Log in to Meraki Dashboard as the user that was just configured. In the example in Figure 4-17, this is the user John Smith. You can see on the network-wide administrators page (**Network-wide > Administrators**) that this user is configured with the Lab admins privileges. Note how the X is missing under the Actions column, confirming the user has read-only access.



Figure 4-17 A Network Admin with Lab Admin Privileges

- Step 2.** Navigate to the switch ports page (**Switching > Switch Ports**). Here, the Tags column is enabled to make it clear which ports you have access to. Select those port(s) with the tag to which this user has read-write permissions; then click **Edit**. In this example, the lab admin has selected port 1/9, as shown in Figure 4-18.

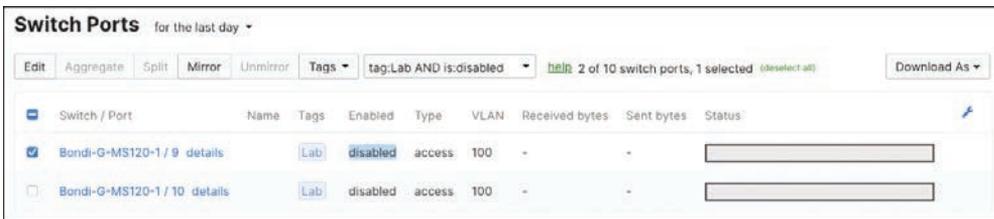


Figure 4-18 A Lab Admin Selecting Switch Ports to Modify

- Step 3.** On the update port page, as shown in Figure 4-19, change the port status to **Enabled** and click **Update**.

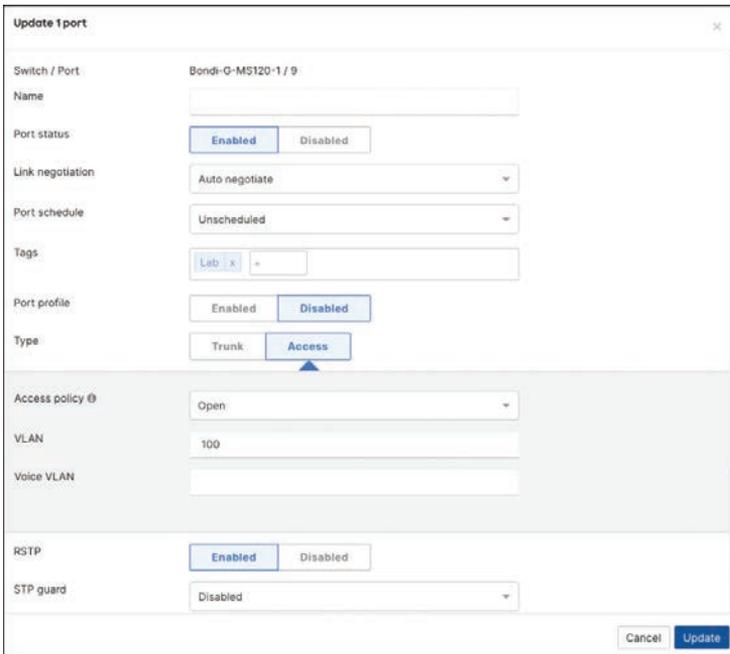
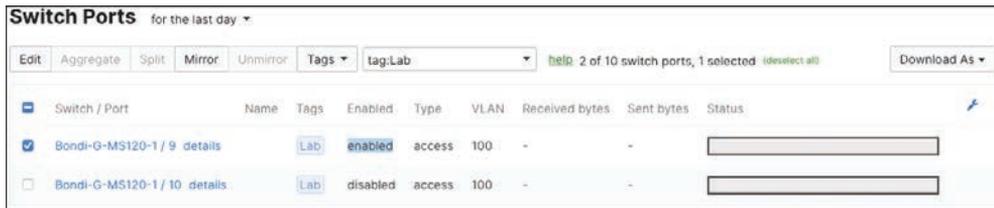


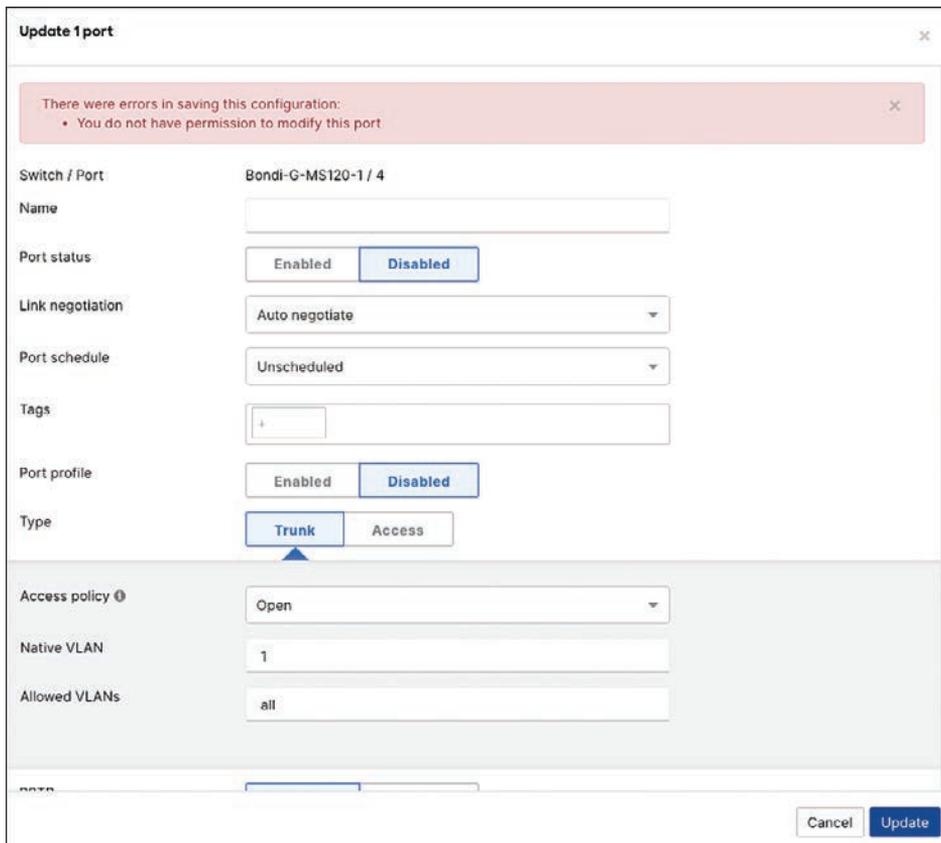
Figure 4-19 A Lab Admin Enabling a Disabled Port

Thanks to port-level permissions, you have successfully enabled this port, despite only having read-only access to the rest of the network (see Figure 4-20). If you try to make changes to another port that is not tagged correctly, you will receive an error, as demonstrated in Figure 4-21.



Switch / Port	Name	Tags	Enabled	Type	VLAN	Received bytes	Sent bytes	Status
<input checked="" type="checkbox"/>	Bondi-G-MS120-1 / 9 details	Lab	enabled	access	100	-	-	<input type="text"/>
<input type="checkbox"/>	Bondi-G-MS120-1 / 10 details	Lab	disabled	access	100	-	-	<input type="text"/>

Figure 4-20 *Verifying That the Lab Admin Was Able to Enable a Port*



Update 1 port

There were errors in saving this configuration:

- You do not have permission to modify this port

Switch / Port: Bondi-G-MS120-1 / 4

Name:

Port status:

Link negotiation:

Port schedule:

Tags:

Port profile:

Type:

Access policy:

Native VLAN:

Allowed VLANs:

Figure 4-21 *Verifying That the Lab Admin Is Not Able to Edit Other Ports*

Role-Based Access Control for Camera-Only Administrators

The Meraki platform features multiple product lines including smart cameras (the MV series) and sensors (the MT series), creating a need for additional admin roles beyond the traditional network admins.

Camera-only roles are intentionally limited to camera-related functions. When correctly configured, local camera-only administrators can log in to both Meraki Dashboard and Meraki Vision. The Meraki Vision portal is a purpose-built CCTV portal designed for staff who need to monitor CCTV footage. Meraki Vision portal has none of the other features of Meraki Dashboard. In Meraki Dashboard, camera-only administrator access is limited to read-only access to the cameras page (other menu items are hidden), as demonstrated in Figure 4-22.

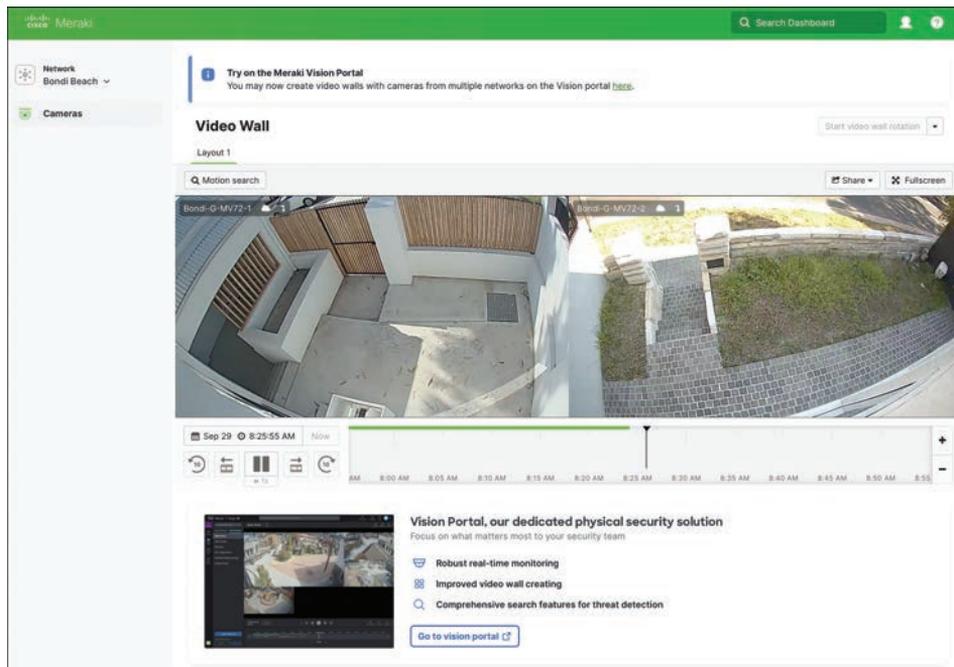


Figure 4-22 A Camera-Only Admin's Limited View of Meraki Dashboard

In either portal, camera-only admins cannot make changes to camera settings such as focus, zoom, or aperture, nor can they create video walls or access the network tab of cameras. A camera-only admin's access is therefore limited to performing only what is allowed by the following camera roles (see Figure 4-23):

- **No Access:** These admins do not have access to any cameras.
- **View Live Footage:** Admins with this level of access can watch live footage on a single camera or video wall.

- **View Any Footage:** Admins with this level of access can watch live and historical footage on a single camera or video wall.
- **View and Export Any Footage:** Admins with this level of access can watch all footage and manage video exports.

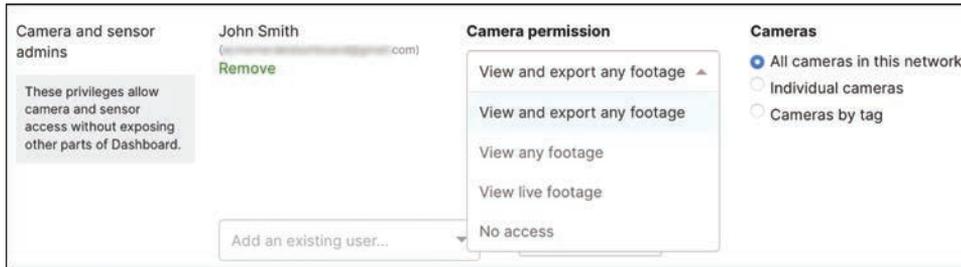


Figure 4-23 Camera Roles for Local Administrators at the Network Level

Local camera-only administrators can be configured at the organization or network level. Organization-wide camera admins are configured on the Organization administrators page (**Organization > Administration**). Privileges at the organization level must be set to None; otherwise, these privileges will override the camera privileges, giving users more access than intended.

Camera-only users should be configured in a purposeful way to limit their scope to what is required. You can configure the local camera-only users as outlined in Table 4-1 and Figure 4-24 to suit their job requirements.

Table 4-1 How to Configure Camera-Only Users to Suit Their Access Requirements

Access Required	How to Configure
The same level of access to all cameras in the organization	Configure the user's administrator access as follows: <ul style="list-style-type: none"> ■ Organization Access to None. ■ Target to All Cameras in This Organization. ■ Access to the highest necessary, such as View and export all footage.
Differentiated levels of access to cameras in the organization	Configure the user's administrator access as follows: <ul style="list-style-type: none"> ■ Organization Access to None. ■ Target to All Cameras in This Organization. ■ Access to the lowest access the user requires, such as View live footage. ■ On the network-wide administrators page (Network-wide > Administration), specify those cameras to which this user needs a higher level of access. For camera-only networks, you will also find this page under Cameras > General (under Configure) > Camera and Sensor Only Admins).

Access Required	How to Configure
Access to only certain cameras	<p>The best way to restrict access within the same organization is to group the cameras into different networks. For example, create a camera-only network for common area devices and another for cameras in restricted or sensitive areas. Then configure the administrator's access as follows:</p> <ul style="list-style-type: none"> ■ Organization Access to None. ■ Target to the appropriate network containing the cameras you want to allow access to. ■ Access to the lowest access the user requires, such as View live footage.
No access to any cameras while retaining access to Dashboard	<p>The best way to configure this access would be to have all the cameras in their own organization, with another organization for all other devices, such as switches and access points. Only camera administrators would be given access to the camera organization. In this case, you would have two completely standalone instances of Meraki Dashboard, with neither team having any visibility of the other environment.</p>

Update administrator [X]

Name:

Email:

Organization access: None [v]

Target All cameras in this organization [v]

Access View and export all [v] [X]

[+ Add access privileges](#)

Update camera and sensor permissions

Camera and sensor permissions must be edited on each Network's admin page. Refresh this page to view your changes.

Bondi Beach [v] Navigate

[privacy](#) Close Update admin

Figure 4-24 An Example of an Administrator Configured as a Camera-Only Admin

We cover more details on this topic in Chapter 12, “Physical Security.”

Role-Based Access Control for Sensor-Only Administrators

Sensor-only administrators are admin accounts that have access to sensor devices and nothing else in Dashboard. Three additional roles apply to sensor-only admins, as illustrated in Figure 4-25:

- **No Access:** These users do not have access to any sensors.
- **Read-Only Sensor Access:** Admins with this level of access can read sensor readings and configurations but not make any changes.
- **Full Sensor Access:** Admins with this level of access can both monitor and edit sensor readings and configurations.

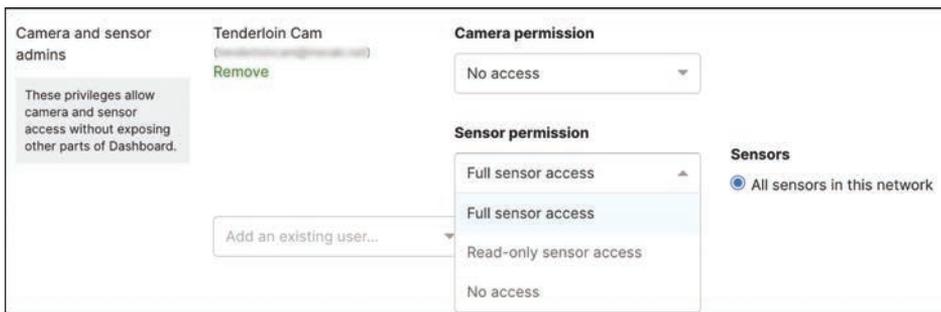


Figure 4-25 *Sensor Roles for Local Administrators at the Network Level*

At the time of writing, access control for sensors is still undergoing heavy development. It is important to note the following:

- Sensors connect via a gateway; both the gateway and the sensor need to be in the same network. This means you can't have a true sensor-only network.
- There is no equivalent to All Cameras in This Organization for sensors. This would be an elegant solution, so do not be surprised to see it added in the future.
- It is not possible to select a subset of sensors on the network-wide administration page.

It is important to remember that sensors are used to collect data such as temperature, air quality, and moisture readings, none of which is personally identifiable information. Nevertheless, to create a local sensor-only user (this user will have the same level of access for all sensors in the organization), configure their administrator profile as follows (**Organization > Administration**):

- **Organization Access to None**
- **Target** to the network containing the sensors and their gateways
- **Access** to the highest access the user requires, such as full access

When single sign-on is configured, permissions for camera and sensor admins can also be assigned using Security Assertion Markup Language (SAML). The organization-wide roles used by single sign-on can be defined in Dashboard by navigating to **Organization > Camera and Sensor Roles**. The permissions mapping is done at time of login, and the admin user is mapped to one of these locally configured roles. It is recommended to use single sign-on for medium to large organizations or where administrators require differentiated access. Configuring single sign-on using SAML is explained in detail in Chapter 5, “Securing Administrator Access to Meraki Dashboard.”

For more information on role-based access for cameras and sensors using SAML, see [https://documentation.meraki.com/MT/MT_General_Articles/Camera_and_sensor-only_admin_\(IoT_Admin\)](https://documentation.meraki.com/MT/MT_General_Articles/Camera_and_sensor-only_admin_(IoT_Admin)).

Role-Based Access Control Using Systems Manager Limited Access Roles

There are additional roles known as *limited access roles* when using Meraki Systems Manager for mobile device management (MDM). Limited access roles allow you to create roles that have defined privileges, for a defined scope of Systems Manager devices. These roles apply only to System Manager commands such as rebooting devices, requesting device check-in, and pushing out notifications. These commands are targeted at managed end-user devices such as phones, tablets, and computers. Here are some examples of use cases where this functionality could come in handy:

- A trainer wants to reboot all classroom devices at the end of a lesson.
- A store manager wants all devices in the store to check in at the start of the day (to verify they are functioning and that none have gone missing).
- You may have administrators responsible for end-user technology whom you want to give limited access to Meraki Dashboard. You could create a role that provides full access to Systems Manager, while limiting their access to the rest of Dashboard.

Limited access roles remain hidden in Meraki Dashboard until all three of these prerequisites are met:

- At least one Systems Manager Agent license has been added.
- A Systems Manager Network has been created.
- At least one device has been enrolled.

Once the prerequisites are in place, follow these steps to tag your Systems Manager devices and configure limited access roles:

- Step 1.** Log in to Meraki Dashboard (<https://dashboard.meraki.com>).
- Step 2.** If you want to use the built-in tags such as IOS devices or Android devices, you can go straight to Step 5. To use custom tags, navigate to **Systems Manager > Devices**, as demonstrated in Figure 4-26.

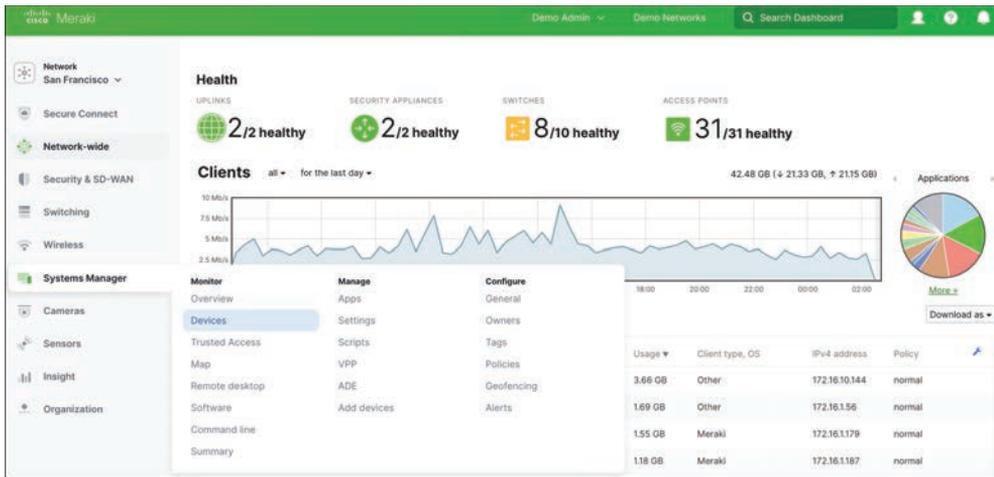


Figure 4-26 Navigating to the Systems Manager Devices Page

- Step 3.** Select the devices you want to tag, as shown in Figure 4-27, and then click the Tag drop-down menu.

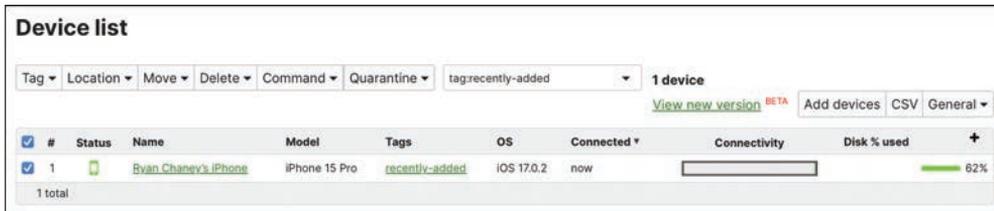


Figure 4-27 Selecting Systems Manager Devices to Tag

- Step 4.** Input the tag name in the Add: text input box and click Add. In the example in Figure 4-28, we created a tag called Store_device to identify all the devices that are used in retail store locations.

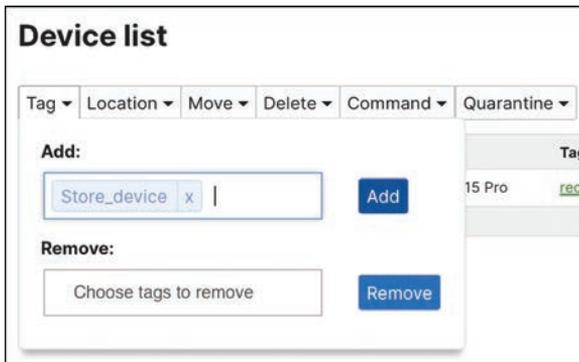


Figure 4-28 Creating a System Manager Tag and Adding It to Our Device(s)

Step 5. Now create the limited access role by first navigating to **Systems Manager > General** (under Configure) for a standalone Systems Manager (SM) network or **Network-wide > Administration** (under Configure) in a combined network. Scroll down to Limited Access Roles (see Figure 4-29).

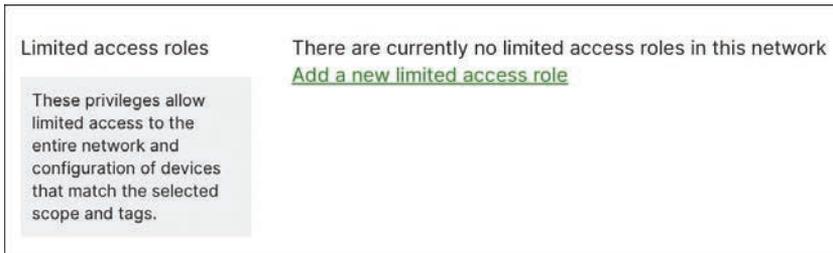


Figure 4-29 Limited Access Roles on the Network-Wide Administration Page

Step 6. Click Add a New Limited Access Role.

Enter a name for this role in the text input box under **Role Name**. Then set the appropriate scope. In the example shown in Figure 4-30, we created a role for a store manager with a scope of **With ANY of the Following Tags**.



Figure 4-30 Entering Name and Scope to Create a Limited Access Role

Step 7. Select the tags that identify the devices that this admin should have access to. In the example in Figure 4-31, we selected the **Store_device** tag. Click **Save** in the bottom-right corner.

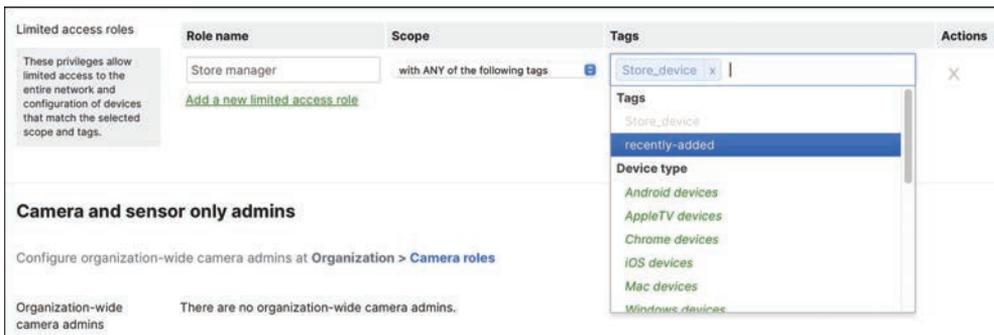


Figure 4-31 Selecting the Tag(s) to Create a Limited Access Role

The **Limited Access Roles** section should now look like the screen in Figure 4-32. A banner at the top of the page confirms that the changes have been saved (not shown here).



Figure 4-32 *A Completed Limited Access Role*

Step 8. Navigate to the Organization administrators page (**Organization > Administrators**), as demonstrated in Figure 4-33.

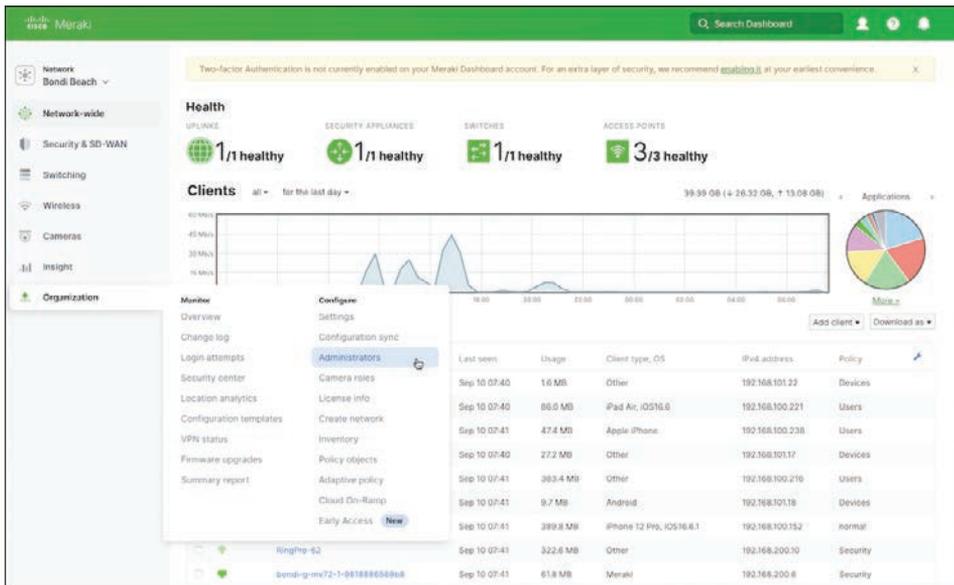


Figure 4-33 *Navigating to the Organization Administrators Page*

Step 9. From page shown in Figure 4-34, click the name or email address of an existing administrator that you want to modify (or create a new one).

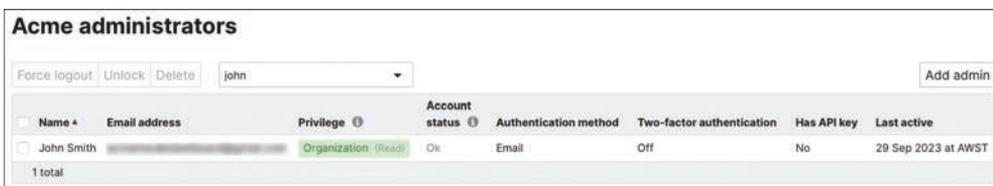


Figure 4-34 *The Organization Administrators Page*

Step 10. In the dialog box shown in Figure 4-35, set the Organization access to **None**. Set the **Target** to the network containing the Systems Manager devices, and under **Access**, choose the name of the role you have just created. Here, we chose the **Store Manager** role. Finish by clicking **Update Admin**.

The screenshot shows a dialog box titled "Update administrator" with a close button (X) in the top right corner. The dialog contains the following elements:

- Name:** A text input field containing "John Smith".
- Email:** A text input field with a blurred email address.
- Organization access:** A dropdown menu set to "None".
- Target:** A dropdown menu set to "Bondi Beach".
- Access:** A dropdown menu set to "Store manager".
- + Add access privileges:** A green link below the Access dropdown.
- Update camera and sensor permissions:** A section with a heading and a paragraph: "Camera and sensor permissions must be edited on each Network's admin page. Refresh this page to view your changes." Below this is a dropdown menu set to "Bondi Beach" and a green "Navigate" button.
- Footer:** A "privacy" link on the left, a "Close" button, and an "Update admin" button on the right.

Figure 4-35 An Example of an Administrator Configured in a Limited Access Role

Step 11. You now return to the Organization administrators page. Click **Save Changes** for the changes to be applied.

Perform the following steps to verify that the changes are in effect:

Step 1. Log in as the user with the limited access role. Navigate to **Systems Manager > Devices**. Note the limited view of Dashboard that this user has, as demonstrated in Figure 4-36.

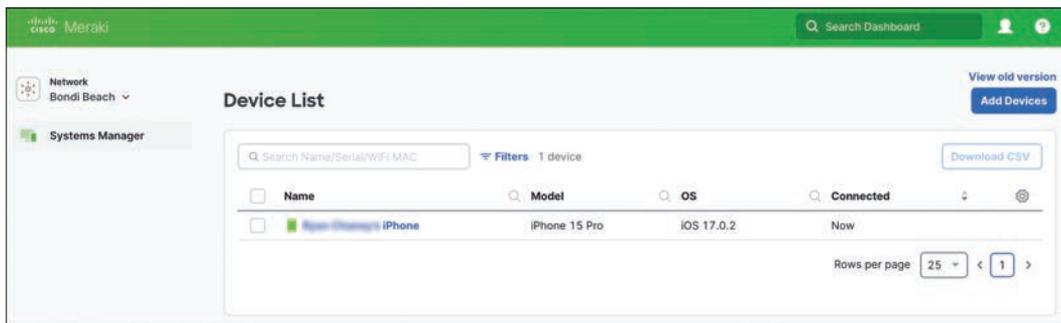


Figure 4-36 Navigating to the Systems Manager Devices Page (Limited Access Role)

- Step 2.** Test that the privileges for this new limited access role are working as intended by requesting a device check-in. Before starting, to make it possible to determine the check-in time, enable the columns for **Tags** and **Last Check-in (MDM)** by clicking the settings (or sprocket) icon on the far right. Once this is done, the **Device List** page should look like Figure 4-37 with the additional columns showing. In this example, you can see that the last check-in time for this device was 7:37 a.m.

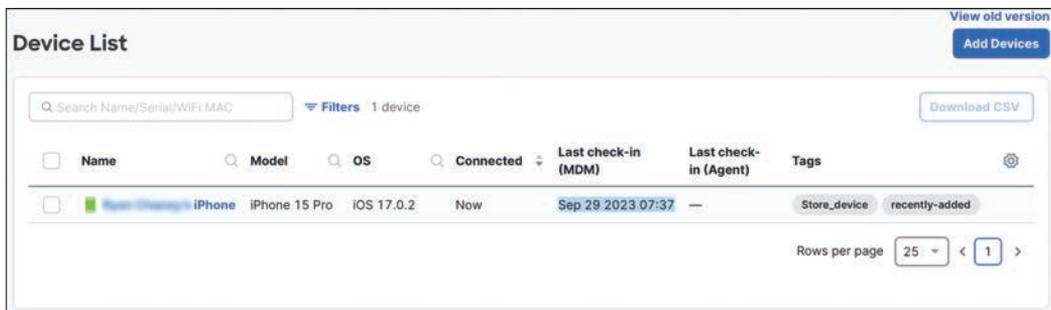


Figure 4-37 Confirming the Most Recent Check-In Date/Time

- Step 3.** Check the box on the row for the device(s) you want to check in and select **Request Check-in** from the **Command** drop-down menu, as demonstrated in Figure 4-38.
- Step 4.** Click **Confirm** on the pop-up window, as shown in Figure 4-39. You see the **Devices List** page again with confirmation that the check-in request has been sent, as demonstrated in Figure 4-40.

You can now see that this device has successfully completed check-in, with a new check-in time of 7:54 a.m., as demonstrated in Figure 4-41.

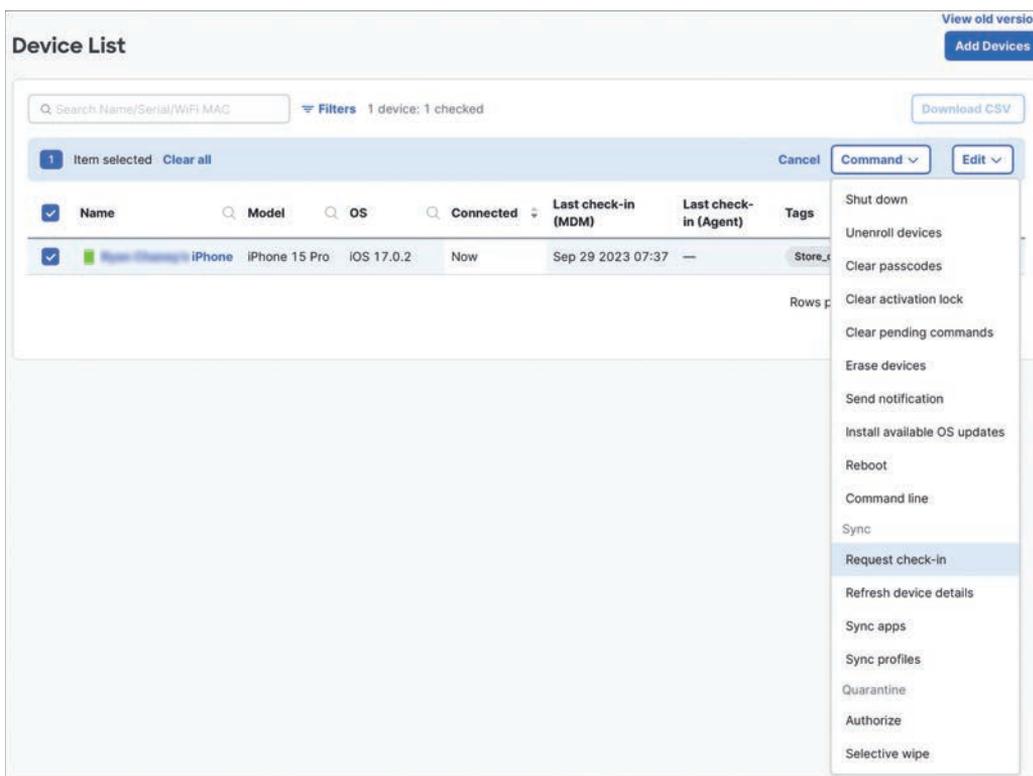


Figure 4-38 Requesting a Device Check-In with Systems Manager

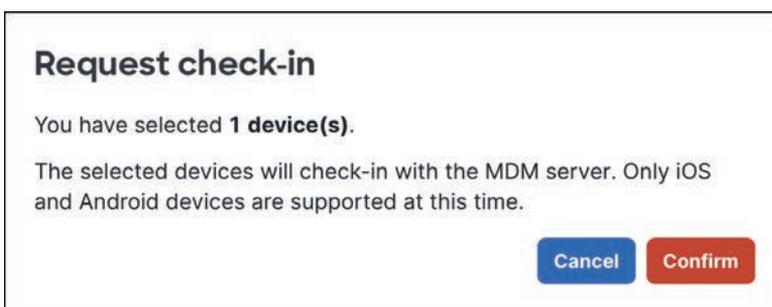


Figure 4-39 Confirming the Check-In Request

If you would like to know more about limited access roles, please check out https://documentation.meraki.com/SM/Other_Topics/Limited_Access_Roles. For more information on Meraki Systems Manager, refer to Chapter 11, “Securing End-User Devices.”



Figure 4-40 *Systems Manager Devices Page After Check-In Request Sent*

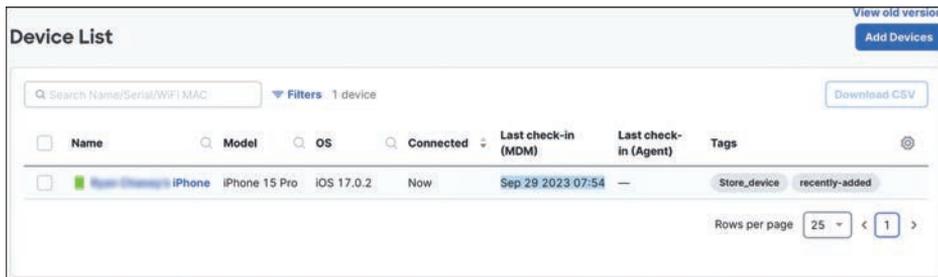


Figure 4-41 *Successful Check-In with Updated Time*

Summary

Role-based access control (RBAC) is a key requirement of modern security standards. In this chapter, we detailed the steps to configure RBAC to adhere to the principle of least privilege. This included learning how to configure user access at the organization and network levels within the Dashboard hierarchy. We also explained how special roles can be created for specific use cases. This included creating roles with control over specific ports, camera-only and sensor-only admins, as well as the creation of limited access roles for Systems Manager admins.

Further Reading

- Cisco Meraki. (2023, June 8). Limited Access Roles. https://documentation.meraki.com/SM/Other_Topics/Limited_Access_Roles
- Cisco Meraki. (2023, August 22). Meraki Dashboard Organizational Structure. https://documentation.meraki.com/General_Administration/Organizations_and_Networks/Meraki_Dashboard_Organizational_Structure
- Cisco Meraki. (2023, November 1). Managing Dashboard Administrators and Permissions. https://documentation.meraki.com/General_Administration/Managing_Dashboard_Access/Managing_Dashboard_Administrators_and_Permissions

This page intentionally left blank

Index

Numerics

- 2FA (two-factor authentication), 81–82
 - configuring using Cisco Duo, 82–91
 - configuring using SMS, 91–95
 - enabling at the organization level, 91–95
- 802.1X, 295, 382. *See also* RADIUS
 - configuring using EAP-TLS, 394–396
 - configuring the identity source sequence in Cisco ISE, 396–398*
 - configuring the policy set in Cisco ISE, 398–403*
 - exporting the CA certificate from Cisco ISE, 408–411*
 - generating a client certificate using Cisco ISE, 404–408*
 - creating a policy set, 300–304
 - verifying wired functionality, 312–315
 - wired, configuring with PEAP, 388–394

- wireless
 - configuring with PEAP, 383–388*
 - testing with EAP-TLS, 411–415*

A

- access points, 1, 4. *See also* Meraki MR access points
- account lockout, 74–77, 97–98, 160–161
- ACLs (access control lists), configuring on Meraki MS switches, 354–357
- AD Sync, configuring in Duo Admin Panel, 317–320
- adaptive policy, 460
 - creating, 476–478
 - groups, 466–468
 - testing, 479, 483–485
- add-on, Splunk, configuring, 182–187
- ADE (Automated Device Enrollment), 676, 700
- administrative access. *See also* privileges

- authentication solutions, 100–102
 - camera-only, 49–51
 - IP whitelisting, 79–81
 - limited access roles, 53–59
 - network tags, 40–42
 - network-level, 38–39
 - organization-level, 38
 - port-level permissions, 42–48
 - sensor-only, 52–53
- administrator account**
 - creating inside a new Meraki organization, 62
 - creating inside an existing Meraki organization, 63–68
- advanced sandboxing, 636–645**
- Air Marshal, 488**
- alerts, 210–213, 679–681**
 - dismissing, 212
 - filtering, 210–211
 - motion, 719–721
 - sensor, 724
 - SNMP traps, 224–227
 - webhooks, 213–222
- AlgoSec, integrating with Dashboard, 197–207**
- AMP (Advanced Malware Protection), 576–577**
 - configuring on Meraki MX security appliances, 577–578
 - verifying functionality, 578–580
- Android, device owner mode, 676**
- AnyConnect VPN, 519–520**
 - configuring, 520–524
 - configuring RADIUS, 315–317
 - policy set, creating in Cisco ISE, 337–342
 - SAML-based authentication, configuring, 265–273
 - verifying functionality, 524–529
- API**
 - key, creating, 175–180
 - Meraki Dashboard, 181, 228–233
 - Python script, 232–233
- Apple push certificate, installing on Meraki Dashboard, 672–676**
- application integration**
 - API key, creating, 175–180
 - organization ID, 180
- applications, pushing to devices, 704–711**
- applying group policies, 446**
 - manually, 446–449
 - using a Sentry policy, 446–449
 - using RADIUS attributes and Cisco ISE, 452–459
- ARP (Address Resolution Protocol), 373**
- assigning SGTs**
 - client laptop, 480–481
 - POS server, 483
 - POS terminal, 480–482
 - to SSIDs, 472
 - to switch ports, 473–475
 - using Cisco ISE, 475–476
- authentication, 61, 257–259. *See also password***
 - 802.1X, 295, 382
 - creating a policy set, 300–304*
 - organization-wide, 295–300*
 - wired, configuring with PEAP, 388–394*
 - wireless, configuring with PEAP, 383–388*
 - EAP, 382
 - Meraki Cloud, 260–264

- Microsoft Active Directory. *See* Microsoft Active Directory
 - multifactor, 81–82
 - configure using Cisco Duo*, 82–91
 - configure using SMS*, 91–95
 - enabling at the organization level*, 91–95
 - policy, 304–305
 - RADIUS
 - configuring for AnyConnect VPN with Duo MFA*, 315–317
 - configuring for wired and wireless 802.1X*, 295
 - configuring using Cisco ISE, Cisco Duo, and Microsoft Active Directory*, 276–277, 277–279
 - confirming functionality for wired 802.1X*, 312–315
 - confirming functionality on wireless*, 308–312
 - organization-wide*, 295–300
 - SAML SSO, 98
 - configure using Cisco Duo and Microsoft Entra ID*, 102–140
 - design*, 99–102
 - IdP-initiated*, 140–145, 148–155
 - login flow*, 99–100
 - SP-initiated*, 146–148, 154–159
 - use cases*, 98
 - SAML-based, 264–273
 - authorization, policy, 305–308
 - Auto VPN, 494–495
 - Meraki MX security appliances, 495–496
 - using non-Meraki devices, 499–505
 - verifying functionality, 496–499
 - AWS (Amazon Web Services), vMX deployment, 533
 - configuring the default VPC in AWS, 536–541
 - creating a new vMX network in Meraki Dashboard, 533–535
 - deploying vMX from the AWS Marketplace, 541–552
 - viewing the new vMX in Meraki Dashboard, 552
- ## B
-
- Biket, John, 3
 - Biswas, Sanjit, 3, 4–5
 - blocking Internet advertisements
 - using content categories, 631–636
 - broadband, 1
 - brute-force attacks, 72
 - BYOD (bring your own device), 676
- ## C
-
- camera-only administrators, role-based access control, 49–51
 - CASB (Cloud Access Security Broker), 649–657
 - category blocking, configuring on Meraki MX security appliances, 572–576
 - chain of trust, 29
 - change log, 172–173
 - change management, 68
 - Cisco Duo
 - AD Sync, configuring in Duo Admin Panel, 317–320
 - Authentication Proxy, 317–320, 330
 - configuring RADIUS, 276–279

- enrolling users, 330–337
- MFA (multifactor authentication), 82–91
- SAML SSO (single sign-on), 102, 112–140, 259
 - directory sync with Microsoft Entra ID*, 112–123
 - IdP-initiated SAML SSO*, 140–145
 - prerequisites*, 103–112
- SAML-based authentication, 264–273
- Cisco ISE (Identity Services Engine), 260**
 - adding Active Directory as an external identity source, 288–295
 - adding NADs (network access devices), 285
 - Meraki MS switches and MR access points*, 285
 - Meraki MX security appliances*, 285–288
 - applying group policies, 452–459
 - assigning SGTs, 475–476
 - configuring an authentication policy, 304–305
 - configuring an authorization policy, 305–308
 - configuring an endpoint group, 426–430
 - configuring RADIUS, 276–279
 - configuring the identity source sequence, 396–398
 - configuring the policy set, 398–403
 - creating a policy set
 - for AnyConnect VPN*, 337–342
 - for wired and wireless 802.1X*, 300–304
 - creating SGTs, 469–472
 - exporting the CA certificate, 408–411
 - generating a client certificate, 404–408
- Cisco Secure Connect, 557, 582–584.**
 - See also Cisco Umbrella*
 - adding Meraki SD-WAN sites, 597–601
 - Cloud Firewall, 608
 - adding Layer 3/4 firewall rule*, 608–611
 - application blocking*, 614–620
 - IDS/IPS (intrusion detection and prevention)*, 620–622
 - verifying functionality*, 611–614
 - DLP (Data Loss Prevention), 657–665
 - initial setup and integration with Cisco Umbrella, 586–597
 - security feature comparison with Meraki MR and Meraki MX, 558–559
 - setting up, 584–585
- Cisco SolutionsPlus partners, 197**
- Cisco Talos, 572**
- Cisco Umbrella**
 - configuring DHCP to assign DNS servers, 601–602
 - content categories, 631–636
 - DNS security, 606–608
 - downloading the Root CA certificate, 603
 - enabling intelligent proxy and SSL decryption, 603–604
 - File Inspection, 638
 - file type control, 645–649
 - installing Root CA certificate on clients, 602

- integrating with Cisco Secure Connect, 586–597
 - Cisco XDR, 193**
 - client certificate, generating, 404–408
 - client devices, 251
 - Client VPN, 508**
 - configuring, 508–510
 - restricting traffic, 529–531
 - testing, 510–514
 - Cloud Firewall, 608**
 - adding Layer 3/4 firewall rule, 608–611
 - application blocking, 614–620
 - IDS/IPS (intrusion detection and prevention), 620–622
 - verifying functionality, 611–614
 - content categories, 631–636**
 - content filtering, 570**
 - category blocking, configuring on Meraki MX security appliances, 572–576
 - URL filtering
 - configuring on Meraki MX security appliances, 570–571*
 - destination lists, 622–629*
 - continuous improvement, 16**
 - controls, security, 16**
 - creating**
 - Active Directory user account, 281–285
 - adaptive policies, 476–478
 - administrator account
 - inside a new Meraki organization, 62*
 - inside an existing Meraki organization, 63–68*
 - API key, 175–180
 - group policies, 443–446
 - SGTs (security group tags), 466
 - Systems Manager profile, 681–683
 - CSF (cybersecurity framework), 13, 14, 169, 493–494, 508**
 - CTB (Cisco Telemetry Broker), 195–196**
 - CVE (common vulnerabilities and exposures), 209**
 - cyber insurance, 12
 - cyber kill chain, 192–193
 - cybercrime, 11–12
-
- ## D
-
- Dashboard API, 716**
 - dashboard/s. *See also* Meraki Dashboard**
 - Security Center, 209–210
 - ThousandEyes, 505–506
 - data center, 24**
 - locations, 25
 - resiliency, 26
 - vulnerability scans, 27
 - data retention policy, 24**
 - data security, 24–26**
 - destination lists, 622–629**
 - device/s**
 - check-in, 58
 - client, 251
 - compliance, 677, 678–680
 - enrolling with Meraki Systems Manager, 676–677
 - inventory, 247
 - owner mode, 676
 - pushing operating system updates to, 711

- supervised, 700
- tags, 53–59
- DHCP, rogue server detection, 376–379
- diagram, topology, 252–253
- disk encryption, 700–701
- dismissing alerts, 212
- DLP (Data Loss Prevention), 657–665
- door sensor, 725
- Dynamic ARP Inspection, 373–376

E

- EAP (Extensible Authentication Protocol), 382. *See also* PEAP (Protected EAP)
- EAP-TLS, 394–396
 - configuring 802.1X, 394–396
 - configuring the identity source sequence in Cisco ISE, 396–398*
 - configuring the policy set in Cisco ISE, 398–403*
 - exporting the CA certificate from Cisco ISE, 408–411*
 - generating a client certificate using Cisco ISE, 404–408*
 - testing wired 802.1X, 413–415
 - testing wireless 802.1X, 411–413
- EasyNet, 715
- encryption, 493–494
 - AES256, 24
 - disk, 700–701
- endpoint group, configuring in Cisco ISE, 426–430
- enrolling devices with Meraki Systems Manager, 676–677
- Essential Eight, 573, 631, 636, 645

- Essential Eight framework, 13
- European Union, GDPR (General Data Protection Regulation), 14
- event log, 174–175
- expiration, password, 68–70
- exporting
 - CA certificate from Cisco ISE, 408–411
 - logs, 180
 - to Splunk, 181–189*
 - using syslog, 190–192*
 - NetFlow data, 196
- extensibility, MV smart camera, 716
- external alerts
 - SNMP traps, 224–227
 - webhooks, 213–222
- external polling, 227

F

- feature support, vMX (Virtual MX), 532–533
- File Inspection
 - enabling, 636–639
 - verifying functionality, 639–645
- file type control, 645–649
- filtering. *See also* content filtering
 - event log, 174–175
 - Security Center page, 209–210
 - Splunk results, 189
- FIPS 200, 240, 715
- firewall. *See also* Cloud Firewall
 - configuring on Meraki MR access points, 357–358
 - flows, 196
 - geo-IP based, 566
 - configuring, 567–569*

verifying functionality, 569
Layer 3, 559–560

*configuring on Meraki MR
access points*, 358–360

*configuring on Meraki MX
security appliances*,
560–562

ping test, 562–563

Layer 7, 563

*configuring on Meraki MR
access points*, 360–361

*configuring on Meraki MX
security appliances*, 564–
565

rules, 504, 559

firmware, Meraki device, 30

flows, syslog, 196

frameworks, 13, 16

information security, 27

NIST Cybersecurity, 169

full access, 38, 39

G

gateway, sensor, 52

**GDPR (General Data Protection
Regulation)**, 14, 23

geo-IP based firewall, 566

configuring, 567–569

verifying functionality, 569

Google, 3

group policy, 443

applying, 446

manually, 446–449

using a Sentry policy, 446–449

*using RADIUS attributes and
Cisco ISE*, 452–459

applying to AnyConnect VPN users,
529–530

creating, 443–446

**groups, configuring in Microsoft
Active Directory**, 279–280

guest ambassador access, 39

H

**hardening, Meraki MR and MS
devices**, 379–382

hardware, inventory, 247–248

hardware trust model, 28

secure boot, 29

secure device onboarding, 29–30

supply chain security, 28–29

TAM (trust anchor module), 29

**HIPAA (Health Insurance Portability
and Accountability Act)**, 14

hub and spoke, site-to-site VPN, 495

I

**IAM (identity and access
management)**, 260

Idle timeout, Dashboard, 77–79

IdP (identity provider), 99

IdP-initiated SAML SSO, 140–145,
148–155

**IDS/IPS (intrusion detection and
prevention)**, 580–581

Cloud Firewall, 620–622

configuring on Meraki MX security
appliances, 581–582

verifying functionality, 581–582

**inactive user account, automatic
disable**, 162–163

incident response, 208, 240, 241–245

industry standards and best practices,
13–14, 16, 26–27. *See also* CSF
(cybersecurity framework); NIST
(National Institute of Standards
and Technology); standards

customer data, 14

data center, 26

healthcare, 14

key themes, 15–16

NIST SP 800–53, 13, 241, 257, 362,
488–489, 514–515, 573, 715

NIST SP 800–207, 353, 382

payment, 14

privacy, 23

information security, 26–27

installing, Apple push certificate,
672–676

intelligent proxy, 603–604

Internet

blocking advertisements using
content categories, 631–636

visibility, 505

Internet Outages page,
ThousandEyes, 505–506

inventory, 247

client devices, 251

configuration, 249–251

hardware, 247–248

software, 248–249

IP whitelisting, 79–81, 161–162

ISPs (internet service providers), 1

J-K-L

Lad, Mohit, 505

last mile, 1

Layer 3 firewall, 559–560

configuring on Meraki MR access
points, 358–360

configuring on Meraki MX security
appliances, 560–562

ping test, 562–563

Layer 7 firewall, 563, 564–566

configuring on Meraki MR access
points, 360–361

configuring on Meraki MX security
appliances, 564–565

limited access roles, 53–59

login attempts, logging, 172

logs/logging, 169, 170

AlgoSec, 197–207

audit controls, 170

change, 172–173

event, 174–175

exporting, 180

to Splunk, 181–189

using syslog, 190–192

login attempts, 172

NetFlow data, 193–196

storage retention period, 171–172

syslog flows, 196

timestamps, 171

M

MAB (MAC Authentication Bypass),
426

configuring

endpoint group in Cisco ISE,
426–430

creating a policy set, 430–436

wired access control policy,
439–443

wireless access control policy,
436–439

- MAC allow lists, 362, 366–368
- man-in-the-middle attack, 373
- Meraki, acquisition by Cisco, 4–6
- Meraki Cloud, 20–21
 - authentication, 260–264
 - shared responsibility model, 32
- Meraki Cloud Controller, 4
- Meraki Dashboard, 4, 19–20, 246–247
 - accessing, 22
 - account lockout, 74–77, 97–98
 - Active Directory authentication for AnyConnect VPN, 342
 - configuring*, 346–348
 - confirming functionality*, 348–350
 - prerequisites*, 342–346
 - administration hierarchy, 38
 - administrative access
 - camera-only*, 49–51
 - limited access roles*, 53–59
 - sensor-only*, 52–53
 - administrator account
 - creating inside a new Meraki organization*, 62
 - creating inside an existing Meraki organization*, 63–68
- Alerts page, 210–212
- AlgoSec integration, 197–207
- API, 228–233
- API key, creating, 175–180
- creating a vMX network, 533–535
- data retention policy, 24
- hierarchy, 20–21
- Idle timeout, 77–79
- installing Apple Push Notification certificate, 672–676
- inventory, 247
 - client devices*, 251
 - configuration*, 249–251
 - hardware*, 247–248
 - software*, 248–249
- IP whitelisting, 79–81, 161–162
- logs, 170. *See also* logs/logging
 - change*, 172–173
 - event*, 174–175
 - exporting*, 180
 - exporting to Splunk*, 181–189
 - login attempts*, 172
 - NetFlow*, 193–196
 - syslog*, 190–192
 - timestamps*, 171
- MFA (multifactor authentication), 81–82
 - configure using Cisco Duo*, 82–91
 - configure using SMS*, 91–95
 - enabling at the organization level*, 91–95
- network tags, 40–42
- organizational structure, 21–22
- organization-wide RADIUS, configuring, 295–300
- out-of-band management, 23
- password/s
 - expiration*, 68–70
 - reuse*, 70–72
 - strong*, 72–74
- raising incidents in ServiceNow, 241–245
- RBAC (role-based access control), 37
- SAML SSO, 98
 - configure using Cisco Duo and Microsoft Entra ID*, 102–140

design, 99–102

IdP-initiated, 140–145,
148–155

login flow, 99–100

SP-initiated, 146–148, 154–159

use cases, 98

Security Center, 209–210

SNMP

configuring, 235–236

traps, 224–227

topology diagrams, 252–253

Traffic Analytics Page, 566–567

user IDs, 62

viewing vMX in, 552

webhooks, 213–222

Meraki Developer Hub, 232

Meraki MR access points

Air Marshal, 488

firewall, 357–358

Layer 3, 358–360

Layer 7, 360–361

hardening, 379–382

security feature comparison with
Meraki MX and Cisco Secure
Connect, 558–559

WPA3, 487

Meraki MS switches

ACLs (access control lists), 354–357

Dynamic ARP Inspection, 373–376

hardening, 379–382

MAC allow lists, 362–366

port isolation, 368–370

rogue DHCP server detection,
376–379

SecurePort, 370–373

SGT propagation, 461–463

sticky MAC allow lists, 362–366

Meraki MT sensor, 724

Meraki Museum, 7

Meraki MX security appliances

AMP (Advanced Malware
Protection), 576–577

configuring, 577–578

verifying functionality,
578–580

category blocking, 572–576

Client VPN

configuring, 508–510

testing, 510–514

configuring DHCP to assign
Umbrella's DNS servers, 601–602

content filtering, 570

encryption, 493–494

IDS/IPS (intrusion detection and pre-
vention), *configuring*, 581–582

Layer 3 firewall, 559–560

configuring, 560–562

ping test, 562–563

Layer 7 firewall, 563

configuring, 564–565

verifying configuration,
564–566

security feature comparison with
Meraki MR and Cisco Secure
Connect, 558–559

SGT propagation, 463–465

site-to-site VPN, 494–495

configuring, 495–496

verifying functionality,
496–499

Snort engine, 581

URL filtering, *configuring*, 570–571

verifying functionality, 581–582

vMX (Virtual MX), 493, 531. *See*
also vMX (Virtual MX)

- deploying in AWS*, 533–552
 - feature support*, 532–533
 - sizing*, 531–532
- Z series, 493
- Meraki MX50**, 4
- Meraki MX70**, 4
- Meraki Python library**, 228
- Meraki Systems Manager**, 671, 672
 - alerting and reporting, 679–681
 - checking device compliance, 678–680
 - configuring end-user devices for network connectivity, 684
 - enrolling devices, 676–677
 - limited access roles, 53–59
 - operating system updates, pushing to devices, 711
 - policies, 677, 678–679
 - profile
 - certificate settings payload*, 684–686
 - creating*, 681–683
 - passcode policy*, 697–700
 - Restrictions policy*, 700–702
 - VPN settings payload*, 693–696
 - Wi-Fi settings payload*, 686–693
 - pushing applications to devices, 704–711
- Meraki Vision portal**, 49, 717
- MFA (multifactor authentication)**, 81–82
 - configure using Cisco Duo, 82–91
 - configure using SMS, 91–95
 - enabling at the organization level, 95–97
- Microsoft Active Directory**
 - adding to Cisco ISE as an external identity source, 288–295
 - configuring groups, 279–280
 - configuring on Meraki Dashboard, 342, 346–348
 - confirming functionality*, 348–350
 - prerequisites*, 342–346
 - configuring RADIUS, 276–279
 - configuring users, 281–285
- Microsoft Entra ID**
 - access review feature, 162–163
 - directory sync with Cisco Duo, 112–123
 - SAML SSO, 123–140
 - SAML-based authentication, 264–273
- MIT (Massachusetts Institute of Technology), Roofnet**, 1–3
- monitoring**, 169, 208. *See also* alerts
 - external polling, 227
 - video
 - using Meraki Display app*, 717
 - via the Meraki Dashboard*, 717
 - via the Meraki Vision Portal*, 717
- monitor-only access**, 39
- motion alerts**, 719–721
- motion search**, 721–724
- MR58**, 4
- MSP (managed service provider)**, 21–22, 98
- multitenant environment**, 42
- MV smart cameras**
 - extensibility, 716
 - video-specific privacy controls, 716

N

NADs (network access devices), adding to Cisco ISE, 285

Meraki MS switches and MR access points, 285

Meraki MX security appliances, 285–288

NBAR (Network-Based Application Recognition), 360

NetFlow, 193–196

network/s, 21

port-level permissions, 42–48

privileges, 38–39

tags, 40–42

topology diagrams, 252–253

NIST (National Institute of Standards and Technology)

CSF (cybersecurity framework), 13, 14, 169, 493–494, 508

SP 800–53, 13, 241, 257, 362, 488–489, 514–515, 573, 715

SP 800–207, 353, 382

O

Oliveira, Ricardo, 505

operating system updates, pushing to devices, 711

order number, 29–30

organization, 20, 21–22

2FA (two-factor authentication), configuring, 95–97

administrator account, creating, 62–68

device inventory, 247

privileges, 38

-wide RADIUS, 295–300

organization ID, 180

outbound firewall rules, 504

out-of-band management, 20–21, 23

P

PagerDuty, 214–222

passcode policy, 697–700

password

age, 68–70, 160

complexity, 72–74, 160

policy, 16

reuse, 70–72, 160

on-path attack, 373

PCI DSS 4.0, 16, 68, 72, 315, 487, 493–494, 573, 715

PCI DSS 4.0 (Payment Card Industry Data Security Standard v4.0), 14

PEAP (Protected EAP)

wired 802.1X, 388–394

wireless 802.1X, 383–388

penetration test, 16, 27

permissions, 38, 42–48

plug-and-play, 2

policy/ies

account lockout, 74–77, 97–98

adaptive, 460, 466–468

creating, 476–478

testing, 479, 483–485

AlgoSec compliance reporting, 197–207

authentication, 304–305

authorization, configuring in Cisco ISE, 305–308

data retention, 24

DLP (Data Loss Prevention), 658–665

- DNS, 606
 - group, 443
 - applying*, 446
 - applying manually*, 446–449
 - applying to AnyConnect VPN users*, 529–530
 - applying using a Sentry policy*, 449–452
 - applying using RADIUS attributes and Cisco ISE*, 452–459
 - creating*, 443–446
 - information security, 27
 - Layer 7 firewall, 361–362
 - passcode, 697–700
 - password, 16
 - age*, 68–70, 160
 - reuse*, 70–72, 160
 - strong*, 72–74, 160
 - Restrictions, 700–702
 - security
 - IP whitelisting*, 161–162
 - restricting concurrent logins*, 162
 - Sentry, 446–449
 - set, 398–403, 430–436
 - creating for AnyConnect VPN in Cisco ISE*, 337–342
 - creating for wired and wireless 802.1X in Cisco ISE*, 300–304
 - Systems Manager, 677, 678–679
 - web, 631, 638–639, 655–656
 - wired access control, 439–443
 - wireless access control, 436–439
 - polling, 227, 234, 235, 236–240
 - port isolation, 368–370
 - port security, 362
 - Dynamic ARP Inspection, 373–376
 - MAC allow lists, 362
 - port isolation, 368–370
 - SecurePort, 370–373
 - sticky MAC allow lists, 366–368
 - port-level permissions**, 42–48
 - principle of least privilege**, 15, 37, 60
 - privacy**, 23
 - privileges**
 - network-level, 38–39
 - organization-level, 38
 - PyCharm, setup**, 228–233
 - Python, script**, 232–233
- ## Q-R
-
- RADIUS**
 - attributes, 452–459
 - configuring for AnyConnect VPN with Duo MFA, 315–317
 - configuring for wired and wireless 802.1X, 295
 - configuring using Cisco ISE, Cisco Duo, and Microsoft Active Directory, 276–277, 277–279
 - confirming functionality for wired 802.1X, 312–315
 - confirming functionality on wireless, 308–312
 - organization-wide, 295–300
 - RBAC (role-based access control)**, 37, 60
 - camera-only administrators, 49–51
 - limited access roles, 53–59
 - sensor-only administrators, 52–53
 - read-only access**, 38, 39
 - Real-Time Rules**, 657–662. *See also* DLP (Data Loss Prevention)

recovering from account lockout,
97–98

registry, VPN, 494

remote-access VPN, 507

AnyConnect, 519–520

configuring, 520–524

verifying functionality,
524–529

Client VPN, 508

configuring, 508–510

restricting traffic, 529–531

testing, 510–514

Sentry VPN, 514–515

configuring, 515–517

verifying functionality,
517–519

reports, 679–681

resiliency, data center, 26

Restrictions policy, 700–702

right to be forgotten, 23

Robertson, Hans, 3

rogue DHCP server detection,
376–379

Romanski, Hilton, 5

Roofnet, 1–3

routing protocol, SrcRR, 2–3

RTSP (Real-Time Streaming Protocol),
716

rules, firewall, 504, 559, 560–562.
See also Layer 3 firewall; Layer 7
firewall

S

SaaS (Software as a Service), 505

SAML SSO (single sign-on), 53, 98.
See also SSO (single sign-on)

configure using Cisco Duo and
Microsoft Entra ID, 102,
123–140

directory sync, 112–123

prerequisites, 103–112

design, 99–102

IdP-initiated, 140–145, 148–155

login flow, 99–100

SP-initiated, 146–148, 154–159

use cases, 98

SAML-based authentication

configuring, 264–273

verifying configuration, 273–276

SASE (Secure Access Service Edge),
557

script, Python, 232–233

SDL (Secure Development Lifecycle),
27, 30

secure boot, 29

SecurePort, 370–373

security, 13. *See also* authentication

ACLs (access control lists), config-
uring on Meraki MS switches,
354–357

administrative access

network-level, 38–39

organization-level, 38

alerts, 210–212, 679–681

dismissing, 212

webhooks, 213–222

authentication, 257–259

Meraki Cloud, 260–264

multifactor, 81–97

SAML-based, 264–273

controls, 16

data, 24–26

data center, 26

- DLP (Data Loss Prevention), 657–665
- DNS, 606–608
- encryption, 493–494
 - AES256*, 24
 - disk*, 700–701
- firewall. *See* firewall
- hardening Meraki MR and MS devices, 379–382
- industry standards, 13–14
- information, 26–27
- IP whitelisting, 79–81, 161–162
- privacy, 23
- reports, 681
- restricting concurrent logins, 162
- rogue DHCP server detection, 376–379
- shared responsibility model, 32
- supply chain, 28–29
- switch port, 362
 - Dynamic ARP Inspection*, 373–376
 - MAC allow lists*, 362
 - port isolation*, 368–370
 - SecurePort*, 370–373
 - sticky MAC allow lists*, 366–368
- as a team sport, 15
- trust, 22–23
- WPA3, 487
- Zero Trust, 15, 257, 382
- Security Center, 209–210**
- self-installation kits, Roofnet, 2**
- sensor**
 - alerts, 724
 - door, 725
 - gateway, 52
 - only administrators, role-based access control, 52–53
- Sensor Sight, 724–727**
- Sentry LAN, 419**
 - configuring, 419–423
 - verifying functionality, 422–426
- Sentry policy, 446–449**
- Sentry VPN, 514–515**
 - configuring, 515–517
 - verifying functionality, 517–519
- Sentry Wi-Fi**
 - configuring, 416–417
 - verifying functionality, 417–419
- separation of user and traffic management, 20–21**
- Sequoia Capital, 3**
- server**
 - DHCP, rogue, 376–379
 - POS, 483
- Service Graph Connector, 241**
- ServiceNow, 241–245**
- session timeout, Dashboard, 77–79**
- setup, PyCharm, 228–233**
- SGTs (security group tags), 459–460**
 - assigning
 - client laptop*, 480–481
 - POS server*, 483
 - POS terminal*, 480–482
 - to SSIDs*, 472
 - to switch ports*, 473–475
 - using Cisco ISE*, 475–476
 - creating, 466
 - creating in Cisco ISE, 469–472
 - propagation, 461
 - on Meraki MS switches*, 461–463

- on Meraki MX security appliances, 463–465*
- shared responsibility model, 32
- single sign-on, 53
- site-to-site VPN, 494–495
 - hub and spoke, 495
 - Meraki MX security appliances, 495–496
 - using non-Meraki devices, 499–505
 - verifying functionality, 496–499
- sizing, vMX (Virtual MX), 531–532
- SMS, MFA (multifactor authentication), configuring, 91–95
- SNMP, 235–236
 - polling, 234, 235, 236–240
 - traps, 224–227, 234
 - versions, 234
- snmpget command, 237
- snmpwalk tool, 239–240
- SnortML, 581
- Soderbery, Rob, 4–5, 6
- software, inventory, 248–249
- software trust model, 30–31. *See also* hardware trust model
- SP-initiated SAML SSO, 146–148, 154–159
- split tunneling, 523
- Splunk
 - add-on, configuring, 182–187
 - logs, importing, 181–189
 - verifying integration, 188–189
- SrcRR, 2–3
- SSL decryption, 604
- standards, 13–14, 16
 - customer data, 14
 - data center, 26
 - healthcare, 14

- key themes, 15–16
- payment, 14
- privacy, 23
- sticky MAC allow lists, 366–368
- storage, log, 171–172
- strong passwords, 72–74, 160
- SUDI (Secure Unique Device Identifier), 29
- supervised devices, 700
- supply chain security, 28–29
- SWG (Secure Web Gateway), 622–629
- switches, 4
- synthetic tests, 505–506
- syslog, 190–192, 196

T

- tags
 - network, 40–42
 - port, 42–48
 - Systems Manager device, 53–59
- TAM (trust anchor module), 29
- templates, configuration, 249–251
- temporary accounts, automatically disabling, 165
- test/ing
 - adaptive policy, 483–485
 - Client VPN, 510–514
 - penetration, 16, 27
 - ping, 562–563
 - software release, 30–31
 - synthetic, 505–506
 - wireless 802.1X with EAP-TLS, 411–415
- third-party service providers, 25
- ThousandEyes, 505

- dashboard, 505–506
- Internet Insights, 505–506
- Internet Outages page, 505–506
- synthetic tests, 505–506

threat protection

- AMP (Advanced Malware Protection)

- configuring on Meraki MX security appliances, 577–578*
 - verifying functionality, 578–580*

- IDS/IPS, 580–581

- timestamps, log, 171

- tools, snmpwalk, 239–240

- topology diagrams, 252–253

- TPAT Tier III accreditation, 28–29

- Traffic Analytics Page, 566–567

- trust, 22–23

U

- unique user IDs, 62

updates

- Meraki device, 30
- operating system, pushing to devices, 711

- upgrades, software, 31

URL filtering

- configuring on Meraki MX security appliances, 570–571
- destination lists, 622–629

user account

- API key, creating, 175–180
- automatic disable, 163–165
- creating in Active Directory, 281–285
- inactive, automatic disable, 162–163
- lockout, 74–77, 97–98

- restricting concurrent logins, 162
- temporary, automatic disable, 165

- user IDs, 62

V

video

- monitoring
 - using Meraki Display app, 717*
 - via the Meraki Dashboard, 717*
 - via the Meraki Vision Portal, 717*

- motion search, 721–724

- specific privacy controls, 716

- walls, 717, 718

- visibility, Internet, 505. *See also* ThousandEyes

- vMX (Virtual MX), 493, 531

- deploying in AWS, 533
 - configuring the default VPC in AWS, 536–541*
 - creating a new vMX network in Meraki Dashboard, 533–535*
 - deploying vMX from the AWS Marketplace, 541–552*
 - viewing the new vMX in Meraki Dashboard, 552*

- feature support, 532–533

- sizing, 531–532

VPN

- registry, 494

- remote-access, 507

- AnyConnect, 519–529*

- Client VPN, 508–514, 529–531*

- Sentry VPN, 514–519*

- site-to-site, 494–495

- hub and spoke, 495*

Meraki MX security appliances, 495–496
using non-Meraki devices, 499–505
verifying functionality, 496–499

vulnerability scan, 27, 30

W

web policy, 631, 638–639, 655–656
webhooks, 213–222
Wi-Fi, 3. *See also* Sentry Wi-Fi
wireless
802.1X

configuring with PEAP, 383–388
testing with EAP-TLS, 411–415

access point, 1

best path, 2–3

workplace safety, 715–716

WPA3, 487

X-Y-Z

XDR (extended detection and response), 192–193

Z series teleworker gateways, 493

Zero Trust, 15, 257, 353, 382