# Securing Enterprise Networks with Cisco Meraki

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

ciscopress.com

# Securing Enterprise Networks with Cisco Meraki

Ryan Chaney, CCIE No. 16666

Simerjit Singh, CCIE No. 38710

Cisco Press

# Securing Enterprise Networks with Cisco Meraki

Ryan Chaney, Simerjit Singh

Published by:
Cisco Press
Hoboken, New Jersey

$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:** Soo Kang

**Alliances Manager, Cisco Press:** Caroline Antonio

**Director, ITP Product Management:** Brett Bartow

**Managing Editor:** Sandra Schroeder

**Development Editor:** Christopher Cleveland

**Senior Project Editor:** Tonya Simpson

**Copy Editor:** Chuck Hutchinson

**Technical Editors:** Akhil Behl, Jeffry Handal

**Editorial Assistant:** Cindy Teeters

**Cover Designer:** Chuti Prasertsith

**Composition:** codeMantra

**Indexer:** Timothy Wright

**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.**

## 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.

**Jeffry 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, Jeffry was a very active customer, always pushing the envelope designing and maintaining networks with new technologies, testing new protocols, and providing Cisco and others a large-scale testbed for new products, features, and functionality. Currently, he plays an active role in several Cisco groups (TACops, IPv6 Ambassadors, Security Technical Advisory Group, Meraki).

Outside of work, Jeffry is an active volunteer in organizations ranging from search and rescue operations with the Air Force to humanitarian technology groups such as NetHope. He sits on several boards within IEEE, actively promotes IPv6 adoption via different task forces, volunteers to teach networking classes in third-world countries, and promotes STEM for women and minorities. In addition, Jeffry serves the public through his participation in conferences and standards bodies (IETF, IEEE); 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

# 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

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

Chapter 4

# 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.

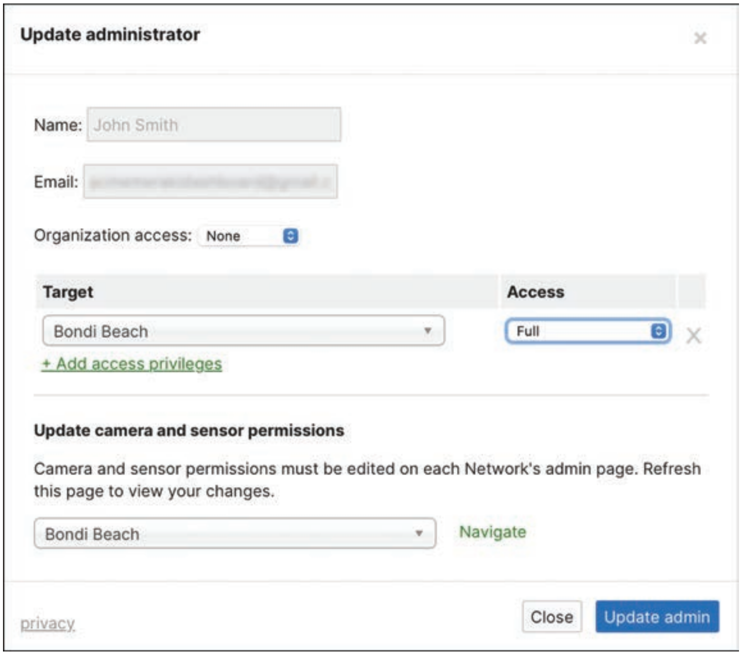
## Administrator Access Levels for Dashboard Organizations and Networks

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).



Update administrator

Name: John Smith

Email: [redacted]

Organization access: None

| Target | Access |
|---|---|
| Bondi Beach | Full |

+ 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

**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.

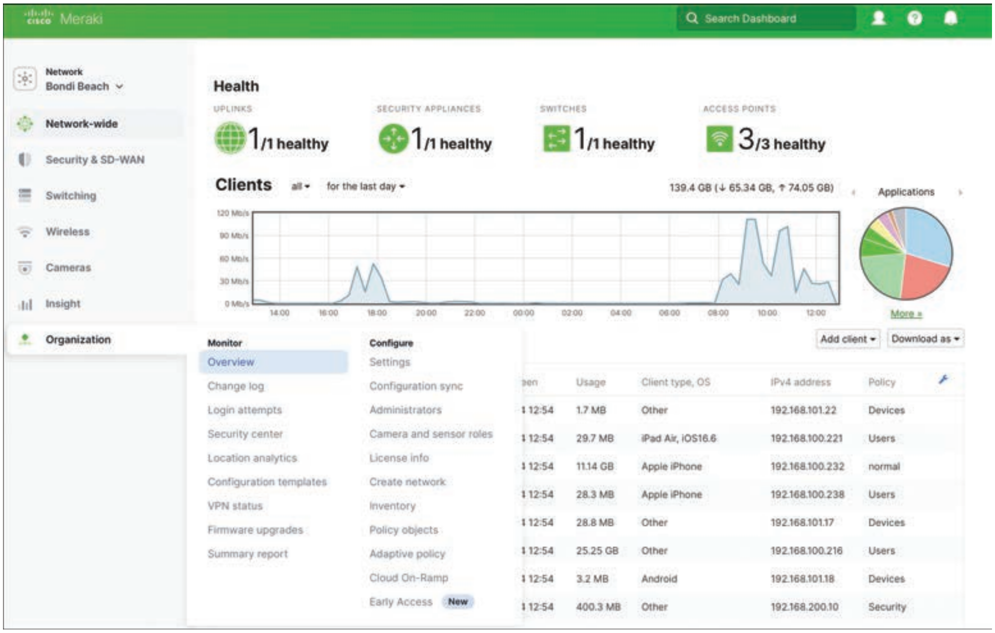
## Assigning Permissions Using Network Tags

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).

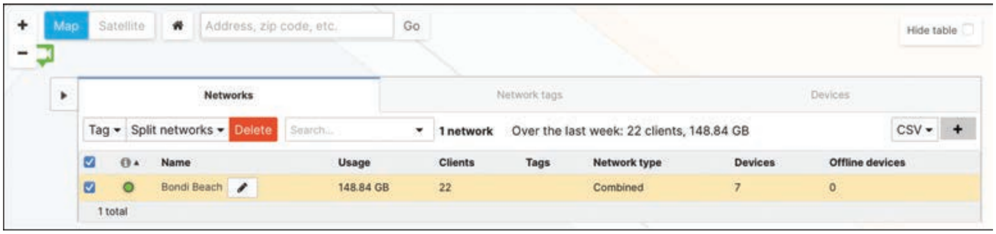
**Step 2.** Navigate to **Organization** > **Overview** (under Monitor), as demonstrated in Figure 4-2.



| een | Usage | Client type, OS | IPv4 address | Policy |
|---|---|---|---|---|
| 12:54 | 1.7 MB | Other | 192.168.101.22 | Devices |
| 12:54 | 29.7 MB | iPad Air, iOS16.6 | 192.168.100.221 | Users |
| 12:54 | 11.14 GB | Apple iPhone | 192.168.100.232 | normal |
| 12:54 | 28.3 MB | Apple iPhone | 192.168.100.238 | Users |
| 12:54 | 28.8 MB | Other | 192.168.101.17 | Devices |
| 12:54 | 25.25 GB | Other | 192.168.100.216 | Users |
| 12:54 | 3.2 MB | Android | 192.168.101.18 | Devices |
| 12:54 | 400.3 MB | Other | 192.168.200.10 | Security |

**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.



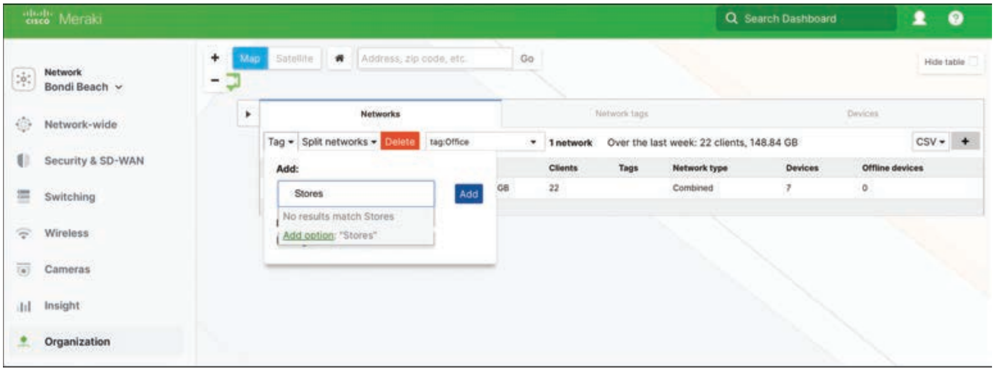
1 network Over the last week: 22 clients, 148.84 GB

| ☑ | | Name | Usage | Clients | Tags | Network type | Devices | Offline devices |
|---|---|---|---|---|---|---|---|---|
| ☑ | ● | Bondi Beach | 148.84 GB | 22 | | Combined | 7 | 0 |

1 total

**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.



Stores

No results match Stores

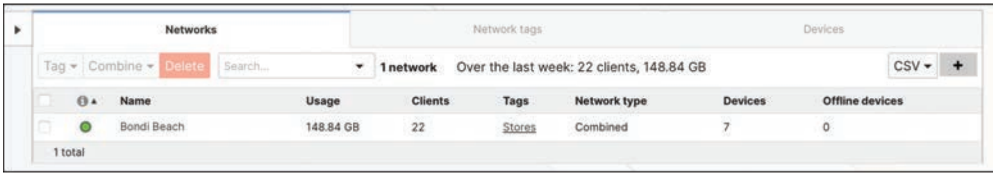
Add option: "Stores"

1 network Over the last week: 22 clients, 148.84 GB

| | Clients | Tags | Network type | Devices | Offline devices |
|---|---|---|---|---|---|
| GB | 22 | | Combined | 7 | 0 |

**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.



1 network Over the last week: 22 clients, 148.84 GB

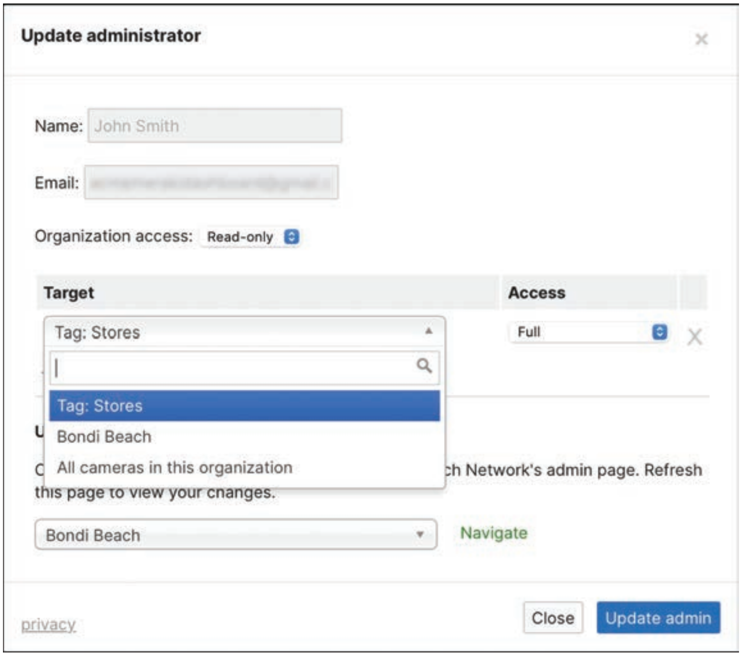
| □ | | Name | Usage | Clients | Tags | Network type | Devices | Offline devices |
|---|---|---|---|---|---|---|---|---|
| □ | ● | Bondi Beach | 148.84 GB | 22 | Stores | Combined | 7 | 0 |

1 total

**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**.



Update administrator

Name: John Smith

Email: [redacted]

Organization access: Read-only

| Target | Access |
|---|---|
| Tag: Stores | Full |

U

C ch Network's admin page. Refresh this page to view your changes.

Bondi Beach

**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.

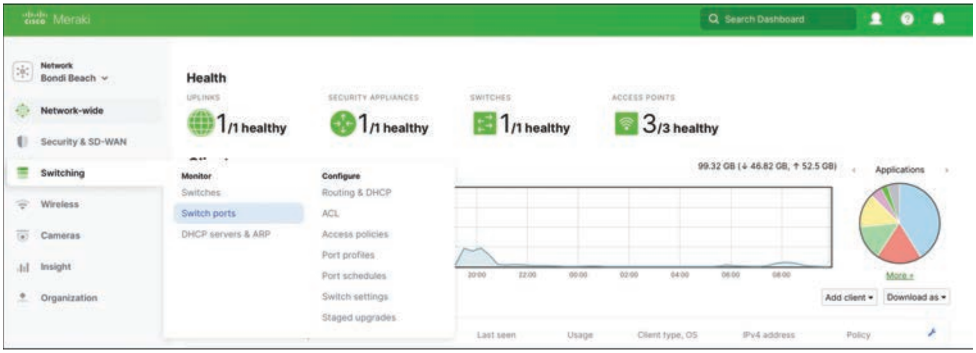
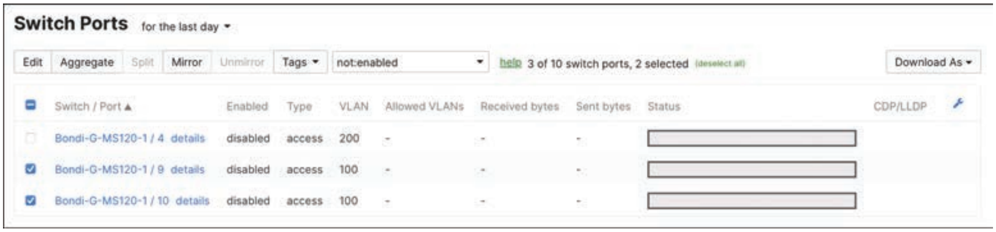


**Figure 4-7** *Navigating to the Switch Ports Page*

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



Switch Ports for the last day ▾

Edit | Aggregate | Split | Mirror | Unmirror | Tags ▾ | not:enabled ▾ | help 3 of 10 switch ports, 2 selected (deselect all) | Download As ▾

| ☐ | Switch / Port ▲ | Enabled | Type | VLAN | Allowed VLANs | Received bytes | Sent bytes | Status | CDP/LLDP |
|---|---|---|---|---|---|---|---|---|---|
| ☐ | Bondi-G-MS120-1 / 4 details | disabled | access | 200 | - | - | - | | |
| ☑ | Bondi-G-MS120-1 / 9 details | disabled | access | 100 | - | - | - | | |
| ☑ | Bondi-G-MS120-1 / 10 details | disabled | access | 100 | - | - | - | | |

**Figure 4-8** *Selecting Ports to Tag*

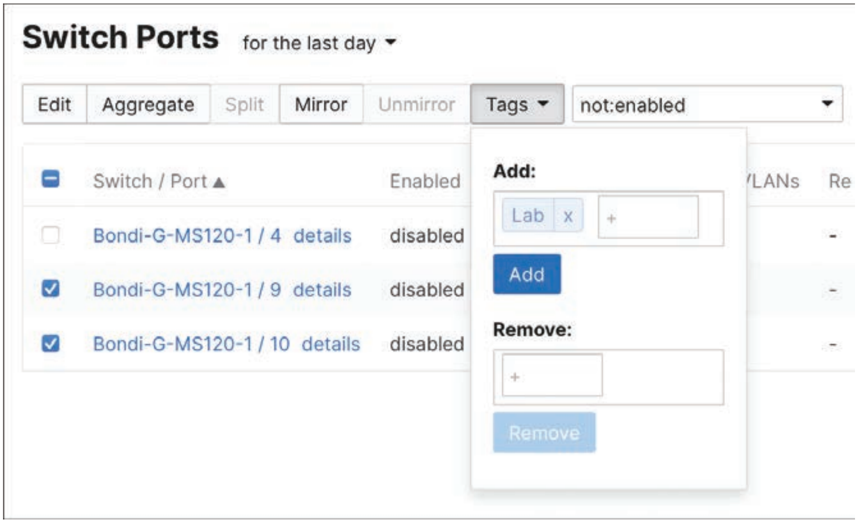
**Step 4.** Click the **Tags** drop-down menu and enter the name for a new tag or select an existing tag. In the example in Figure 4-9, we added the tag **Lab**. Click **Add** to confirm the changes.

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.

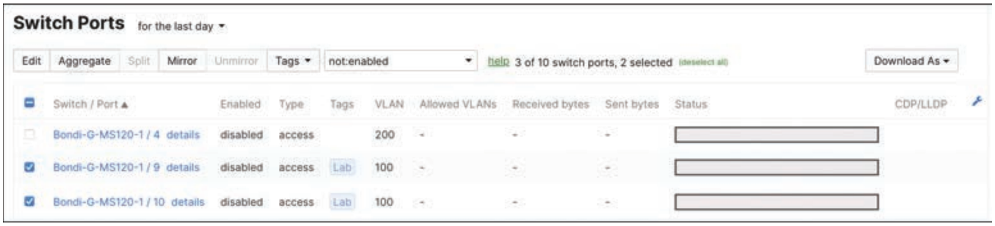
**Step 6.** Scroll down to the **Port Management Privileges** section and click **Add a Port Management Privilege.**

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.



| ☐ | Switch / Port ▲ | Enabled | VLANs | Re |
|---|---|---|---|---|
| ☐ | Bondi-G-MS120-1 / 4 details | disabled | | - |
| ☑ | Bondi-G-MS120-1 / 9 details | disabled | | - |
| ☑ | Bondi-G-MS120-1 / 10 details | disabled | | - |

**Figure 4-9** *Creating Port Tags*



3 of 10 switch ports, 2 selected (deselect all)

| ☐ | Switch / Port ▲ | Enabled | Type | Tags | VLAN | Allowed VLANs | Received bytes | Sent bytes | Status | CDP/LLDP |
|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | Bondi-G-MS120-1 / 4 details | disabled | access | | 200 | - | - | - | | |
| ☑ | Bondi-G-MS120-1 / 9 details | disabled | access | Lab | 100 | - | - | - | | |
| ☑ | Bondi-G-MS120-1 / 10 details | disabled | access | Lab | 100 | - | - | - | | |

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

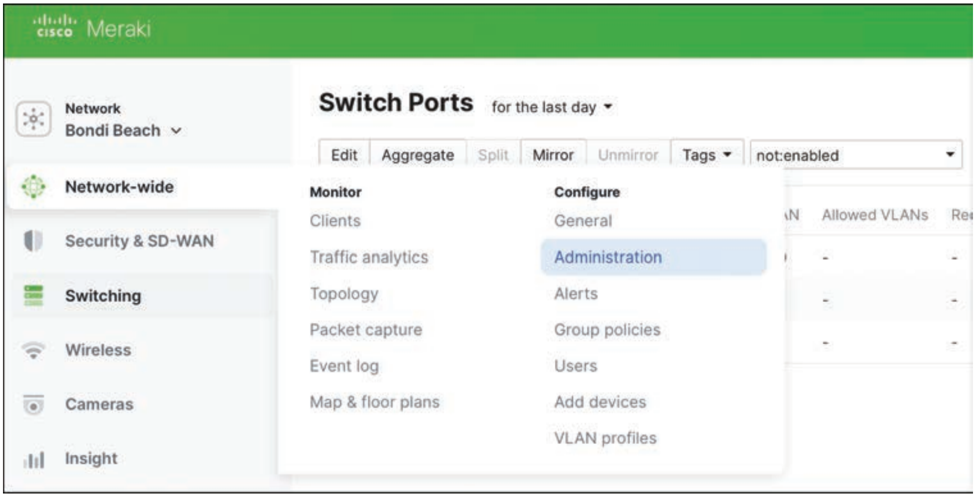
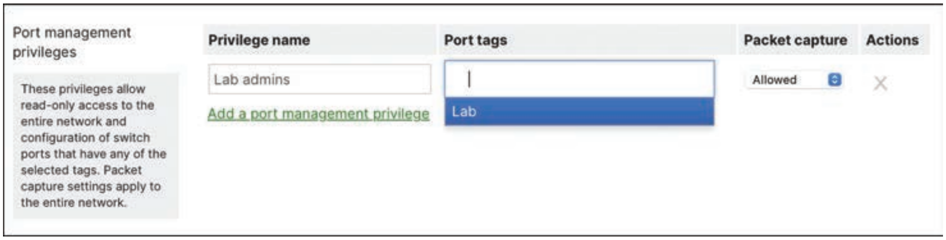


**Figure 4-11** *Navigating to the Network Administration Page*



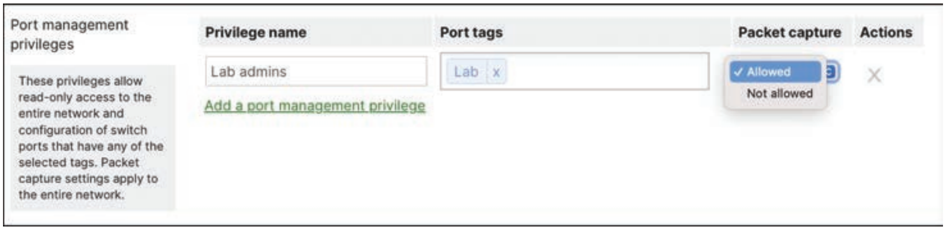
Port management privileges

These privileges allow read-only access to the entire network and configuration of switch ports that have any of the selected tags. Packet capture settings apply to the entire network.

| Privilege name | Port tags | Packet capture | Actions |
|---|---|---|---|
| Lab admins | Lab | Allowed | × |

**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.



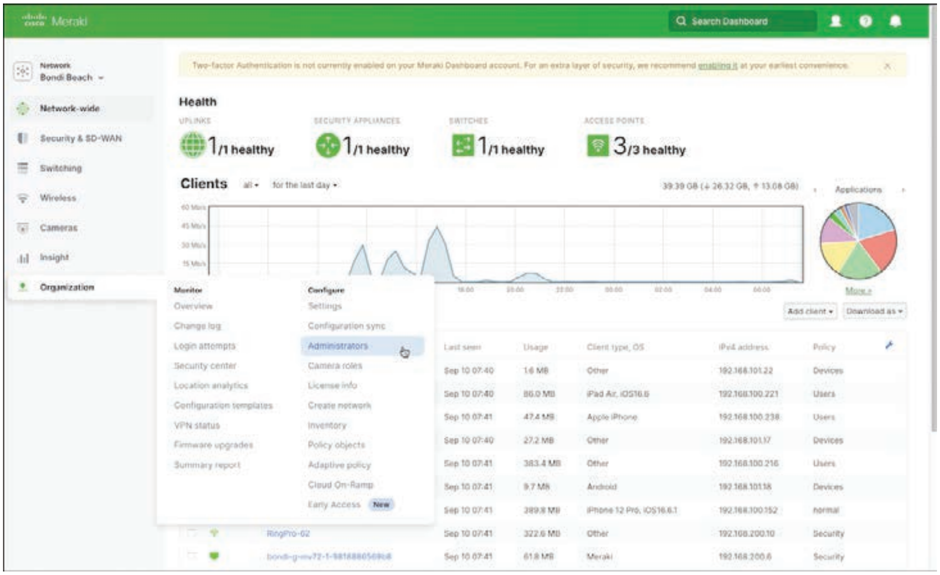
Port management privileges

These privileges allow read-only access to the entire network and configuration of switch ports that have any of the selected tags. Packet capture settings apply to the entire network.

| Privilege name | Port tags | Packet capture | Actions |
|---|---|---|---|
| Lab admins | Lab x | ✓ Allowed<br>Not allowed | × |

**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.



Two-factor Authentication is not currently enabled on your Meraki Dashboard account. For an extra layer of security, we recommend enabling it at your earliest convenience.

Health

UPLINKS 1/1 healthy

SECURITY APPLIANCES 1/1 healthy

SWITCHES 1/1 healthy

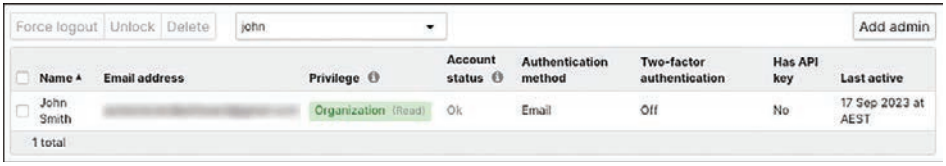
ACCESS POINTS 3/3 healthy

Clients all for the last day 39.39 GB (↓ 26.32 GB, ↑ 13.08 GB)

| | Last seen | Usage | Client type, OS | IPv4 address | Policy |
|---|---|---|---|---|---|
| | Sep 10 07:40 | 1.6 MB | Other | 192.168.101.22 | Devices |
| | Sep 10 07:40 | 86.0 MB | iPad Air, iOS16.6 | 192.168.100.221 | Users |
| | Sep 10 07:41 | 47.4 MB | Apple iPhone | 192.168.100.238 | Users |
| | Sep 10 07:40 | 27.2 MB | Other | 192.168.101.17 | Devices |
| | Sep 10 07:41 | 383.4 MB | Other | 192.168.100.216 | Users |
| | Sep 10 07:41 | 9.7 MB | Android | 192.168.101.18 | Devices |
| | Sep 10 07:41 | 389.8 MB | iPhone 12 Pro, iOS16.6.1 | 192.168.100.152 | normal |
| RingPro-02 | Sep 10 07:41 | 322.6 MB | Other | 192.168.200.10 | Security |
| bondi-g-mv72-1-9818880569c8 | Sep 10 07:41 | 61.8 MB | Meraki | 192.168.200.6 | Security |

**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.

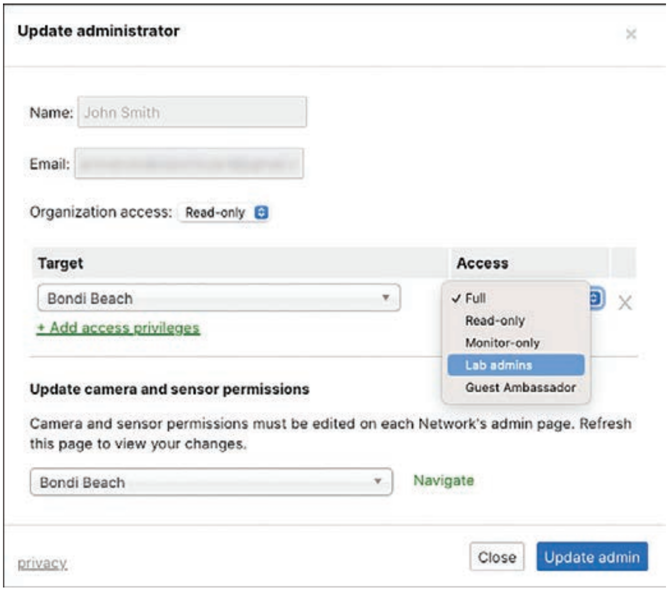


| ☐ | Name ▴ | Email address | Privilege ⓘ | Account status ⓘ | Authentication method | Two-factor authentication | Has API key | Last active |
|---|---|---|---|---|---|---|---|---|
| ☐ | John Smith | [redacted] | Organization (Read) | Ok | Email | Off | No | 17 Sep 2023 at AEST |

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: John Smith

Email: [redacted]

Organization access: Read-only

| Target | Access |
|---|---|
| Bondi Beach | ✓ Full |

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.

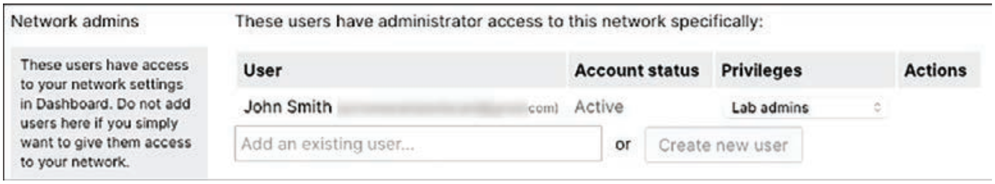
Bondi Beach

**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.



Network admins

These users have access to your network settings in Dashboard. Do not add users here if you simply want to give them access to your network.

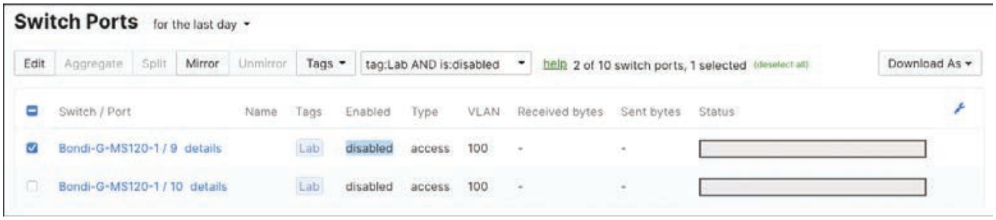
These users have administrator access to this network specifically:

| User | Account status | Privileges | Actions |
|---|---|---|---|
| John Smith [redacted]com) | Active | Lab admins | |

Add an existing user... or Create new user

**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.



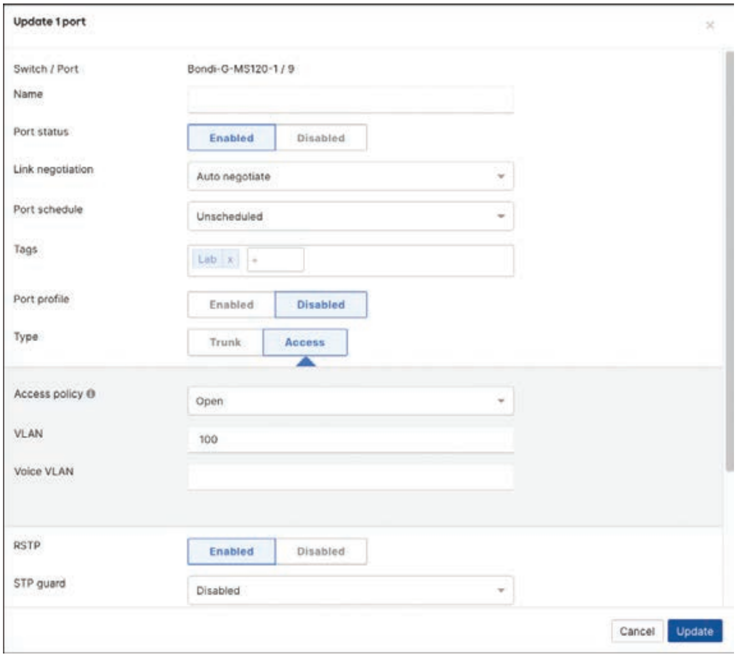
Switch Ports for the last day

Edit | Aggregate | Split | Mirror | Unmirror | Tags | tag:Lab AND is:disabled | help 2 of 10 switch ports, 1 selected (deselect all) | Download As

| | Switch / Port | Name | Tags | Enabled | Type | VLAN | Received bytes | Sent bytes | Status |
|---|---|---|---|---|---|---|---|---|---|
| ☑ | Bondi-G-MS120-1 / 9 details | | Lab | disabled | access | 100 | - | - | |
| ☐ | Bondi-G-MS120-1 / 10 details | | Lab | disabled | access | 100 | - | - | |

**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**.



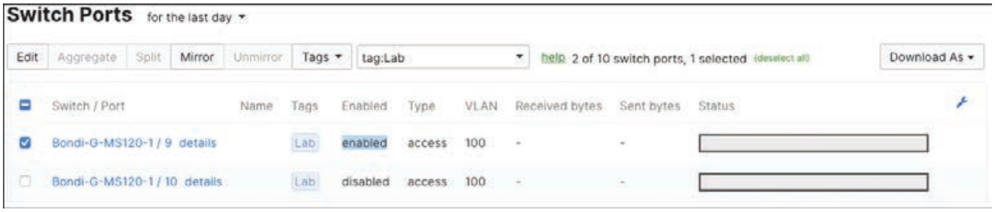
Update 1 port

| | |
|---|---|
| Switch / Port | Bondi-G-MS120-1 / 9 |
| Name | |
| Port status | [✓ Enabled] Disabled |
| Link negotiation | Auto negotiate |
| Port schedule | Unscheduled |
| Tags | Lab x |
| Port profile | Enabled [✓ Disabled] |
| Type | Trunk [✓ Access] |
| Access policy | Open |
| VLAN | 100 |
| Voice VLAN | |
| RSTP | [✓ Enabled] Disabled |
| STP guard | Disabled |

Cancel 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.



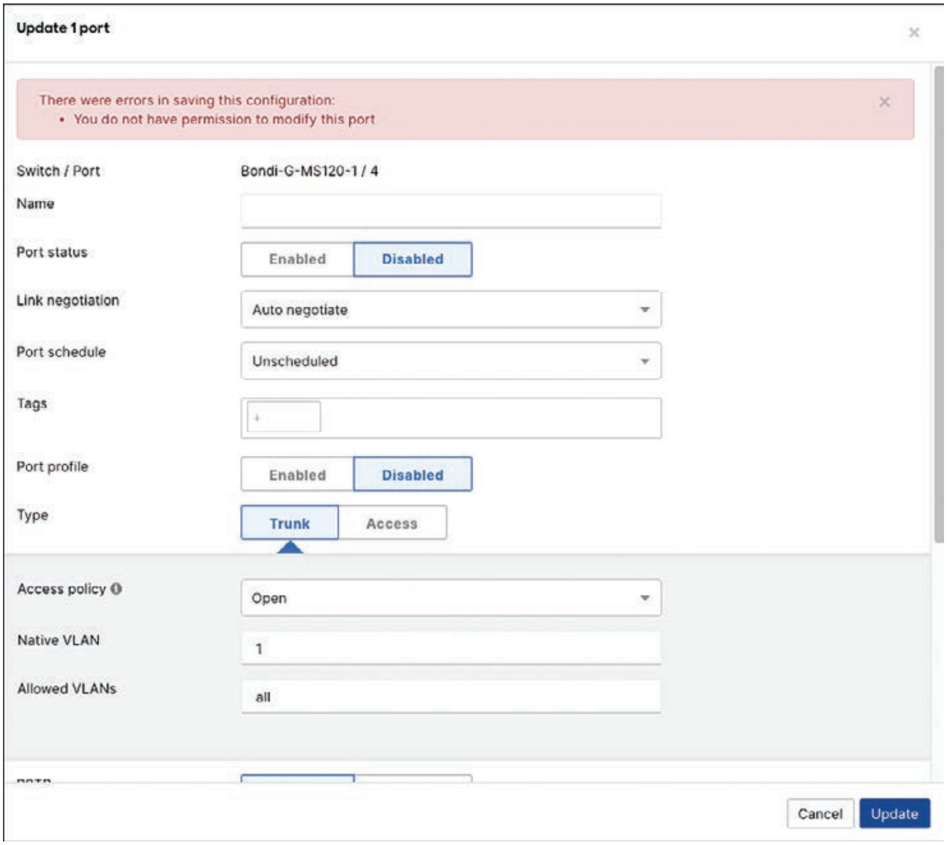
Switch Ports for the last day

tag:Lab

help 2 of 10 switch ports, 1 selected (deselect all)

| | Switch / Port | Name | Tags | Enabled | Type | VLAN | Received bytes | Sent bytes | Status |
|---|---|---|---|---|---|---|---|---|---|
| ☑ | Bondi-G-MS120-1 / 9 details | | Lab | enabled | access | 100 | - | - | |
| □ | Bondi-G-MS120-1 / 10 details | | Lab | disabled | access | 100 | - | - | |

**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

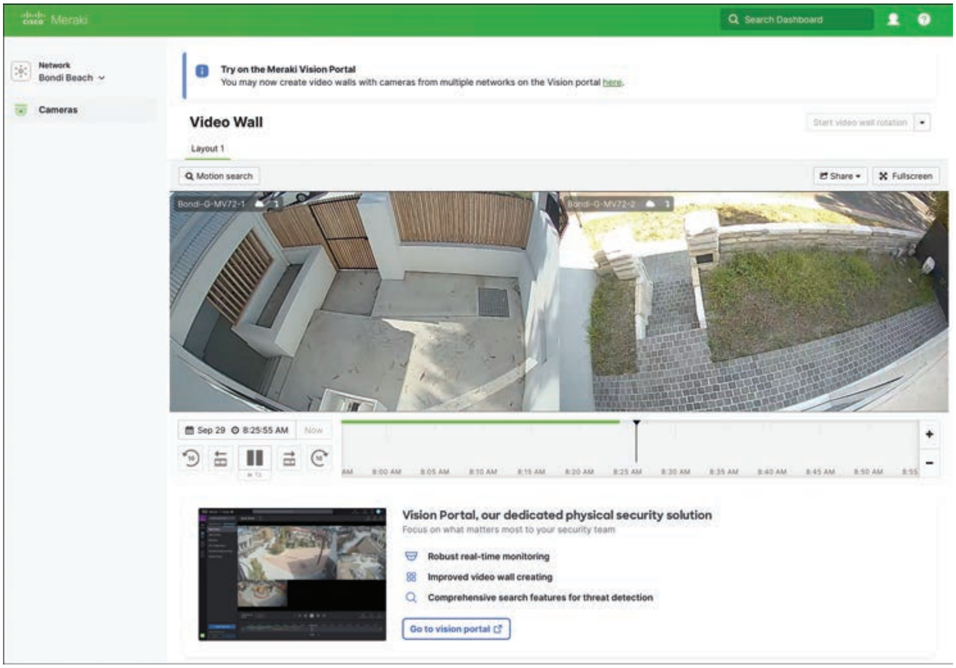
| | |
|---|---|
| Switch / Port | Bondi-G-MS120-1 / 4 |
| Name | |
| Port status | Enabled [✓ Disabled] |
| Link negotiation | Auto negotiate |
| Port schedule | Unscheduled |
| Tags | |
| Port profile | Enabled [✓ Disabled] |
| Type | [✓ Trunk] Access |
| Access policy | Open |
| Native VLAN | 1 |
| Allowed VLANs | all |

**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.



Try on the Meraki Vision Portal
You may now create video walls with cameras from multiple networks on the Vision portal here.

Video Wall

Vision Portal, our dedicated physical security solution
Focus on what matters most to your security team

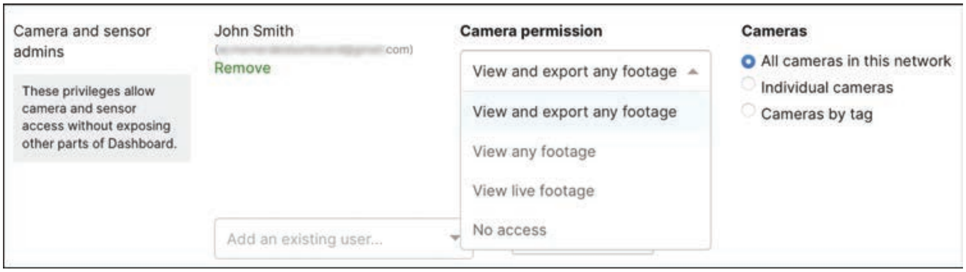
- Robust real-time monitoring
- Improved video wall creating
- Comprehensive search features for threat detection

**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.



Camera and sensor admins

These privileges allow camera and sensor access without exposing other parts of Dashboard.

John Smith

([redacted]com)

Remove

Add an existing user...

**Camera permission**

View and export any footage

- View and export any footage
- View any footage
- View live footage
- No access

**Cameras**

● All cameras in this network

○ Individual cameras

○ Cameras by tag

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

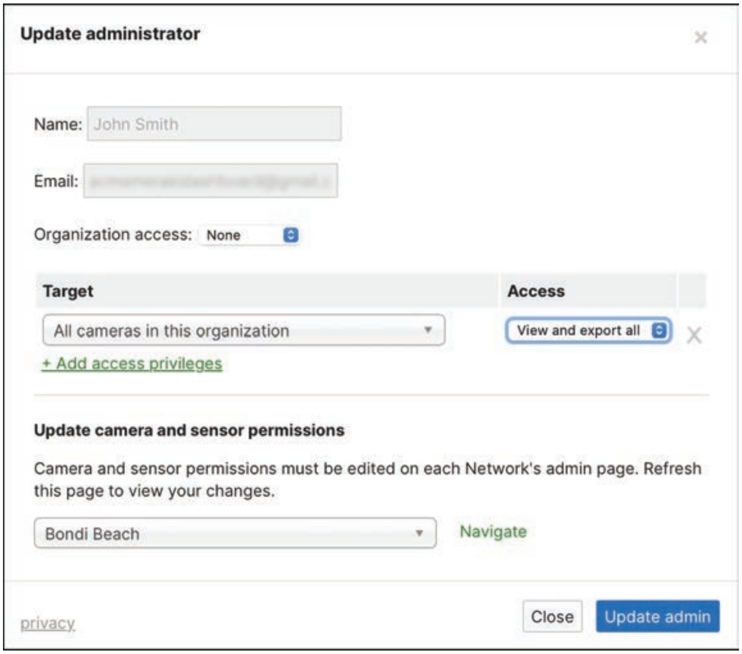
Local camera-only administrators can be configured at the organization or network level. Organization-wide camera admins are configured on the Organization administrators page (**Organization** > **Administration**). Privileges at the organization level must be set to None; otherwise, these privileges 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:<br>■ **Organization Access** to **None.**<br>■ **Target** to **All Cameras in This Organization.**<br>■ **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:<br>■ **Organization Access** to **None.**<br>■ **Target** to **All Cameras in This Organization.**<br>■ **Access** to the lowest access the user requires, such as **View live footage.**<br>■ 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 | 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:<br>■ **Organization Access** to **None**.<br>■ **Target** to the appropriate network containing the cameras you want to allow access to.<br>■ **Access** to the lowest access the user requires, such as View live footage. |
| No access to any cameras while retaining access to Dashboard | 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. |



**Update administrator**

Name: John Smith

Email: [redacted]

Organization access: None

| Target | Access |
|---|---|
| All cameras in this organization | View and export all |

**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

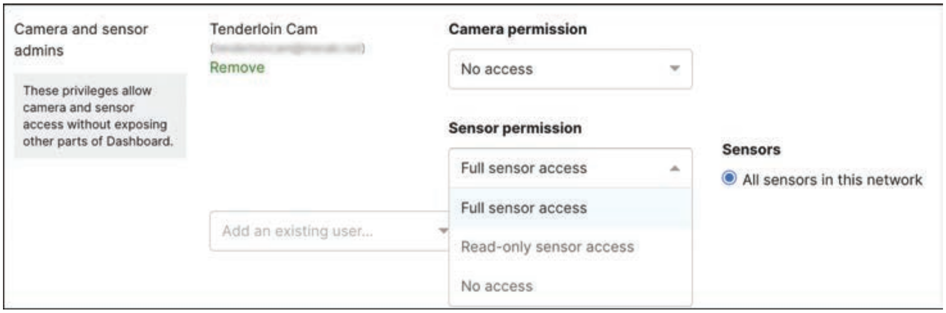
**Figure 4-24** *An Example of an Administrator Configured as a Camera-Only Admin*

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.



Camera and sensor admins

These privileges allow camera and sensor access without exposing other parts of Dashboard.

Tenderloin Cam
([redacted])
Remove

Add an existing user...

Camera permission: No access

Sensor permission: Full sensor access

Sensors: ● All sensors in this network

**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).

## 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.

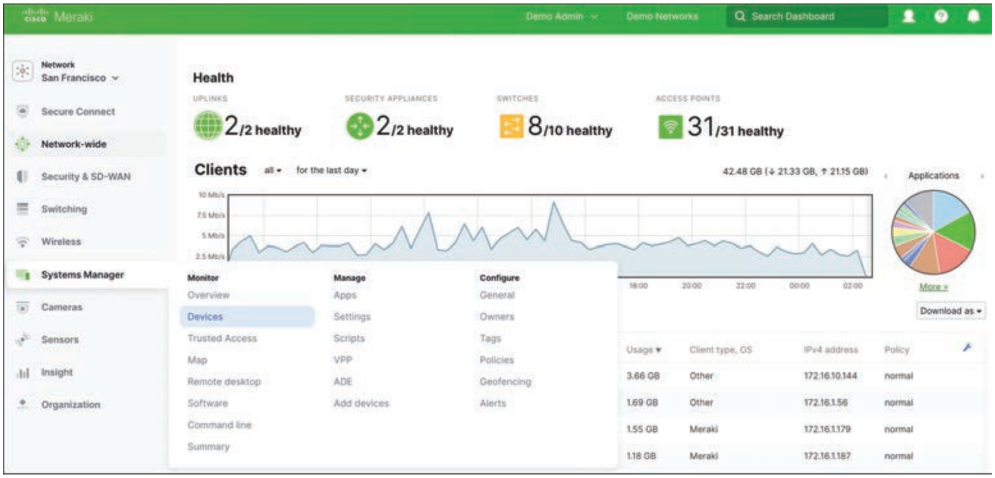
Limited access roles remain hidden in Meraki Dashboard until all three of these prerequisites are met:

- 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).

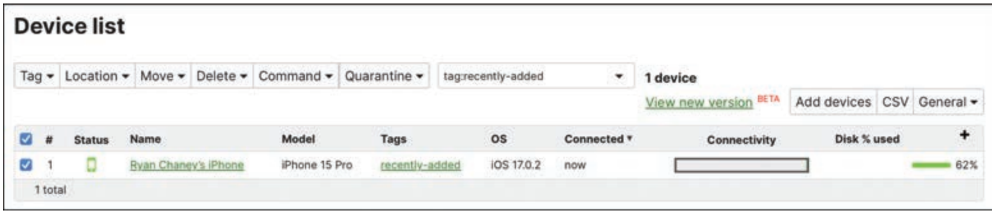
**Step 2.** If you want to use the built-in tags such as IOS devices or Android devices, you can go straight to Step 5. To use custom tags, navigate to **Systems Manager** > **Devices**, as demonstrated in Figure 4-26.



| Usage ▾ | Client type, OS | IPv4 address | Policy |
|---|---|---|---|
| 3.66 GB | Other | 172.16.10.144 | normal |
| 1.69 GB | Other | 172.16.1.56 | normal |
| 1.55 GB | Meraki | 172.16.1.179 | normal |
| 1.18 GB | Meraki | 172.16.1.187 | normal |

**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.

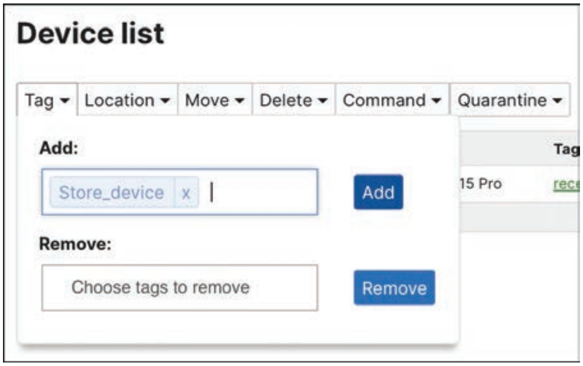

Device list

| ☑ | # | Status | Name | Model | Tags | OS | Connected ▾ | Connectivity | Disk % used |
|---|---|---|---|---|---|---|---|---|---|
| ☑ | 1 | | Ryan Chaney's iPhone | iPhone 15 Pro | recently-added | iOS 17.0.2 | now | | 62% |

1 total

**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.


Device list

Add:

Store_device x

Add

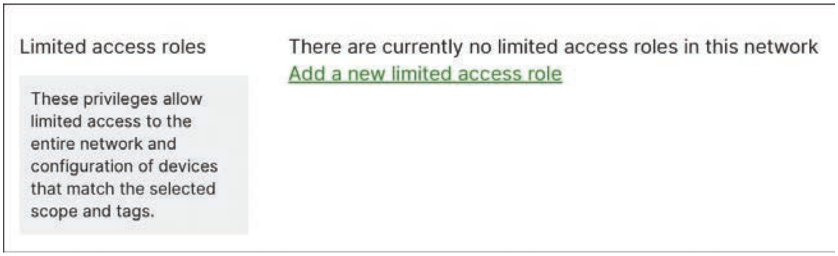
Remove:

Choose tags to remove

Remove

**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).



Limited access roles

These privileges allow limited access to the entire network and configuration of devices that match the selected scope and tags.

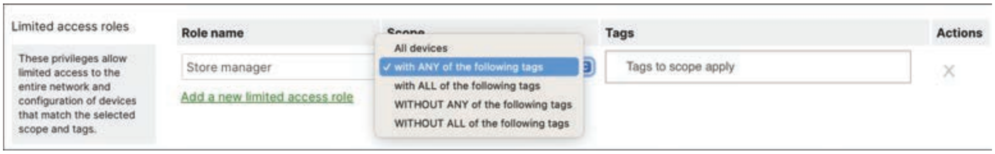
There are currently no limited access roles in this network

Add a new limited access role

**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.**



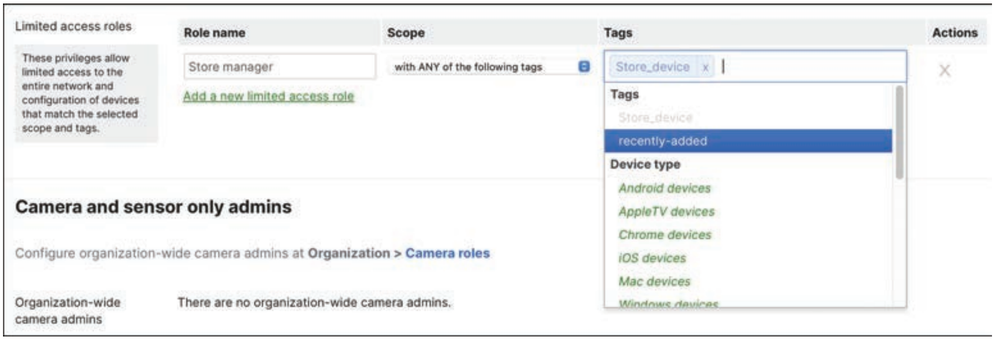
Limited access roles

These privileges allow limited access to the entire network and configuration of devices that match the selected scope and tags.

| Role name | Scope | Tags | Actions |
|---|---|---|---|
| Store manager | All devices<br>✓ with ANY of the following tags<br>with ALL of the following tags<br>WITHOUT ANY of the following tags<br>WITHOUT ALL of the following tags | Tags to scope apply | × |
| Add a new limited access role | | | |

**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.



Limited access roles

These privileges allow limited access to the entire network and configuration of devices that match the selected scope and tags.

| Role name | Scope | Tags | Actions |
|---|---|---|---|
| Store manager | with ANY of the following tags | Store_device × | × |
| Add a new limited access role | | | |

Tags: Store_device, recently-added

Device type: Android devices, AppleTV devices, Chrome devices, iOS devices, Mac devices, Windows devices

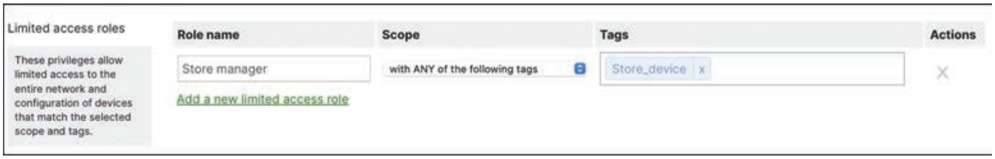
**Camera and sensor only admins**

Configure organization-wide camera admins at **Organization > Camera roles**

Organization-wide camera admins: There are no organization-wide camera admins.

**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).



Limited access roles

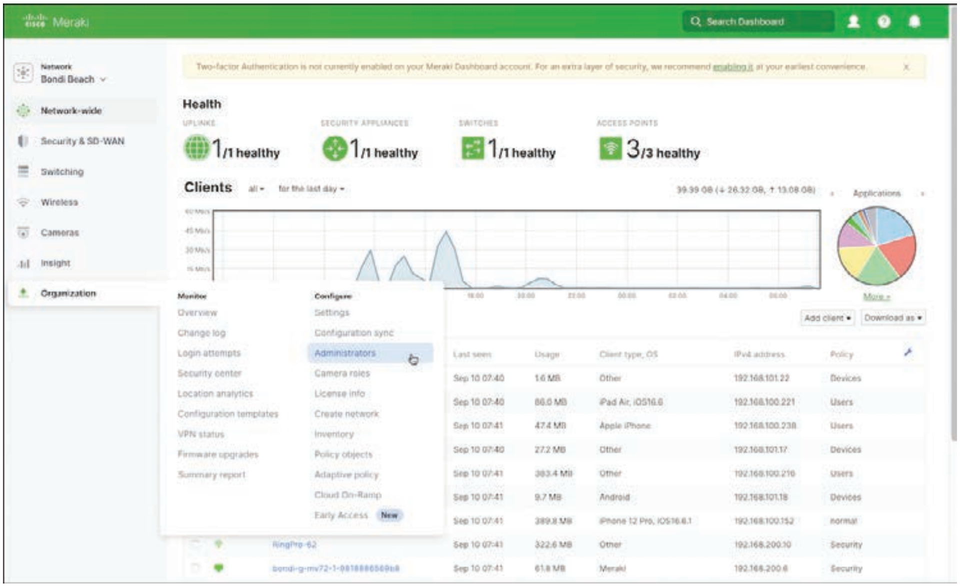
These privileges allow limited access to the entire network and configuration of devices that match the selected scope and tags.

| Role name | Scope | Tags | Actions |
|---|---|---|---|
| Store manager | with ANY of the following tags | Store_device x | × |

Add a new limited access role

**Figure 4-32** *A Completed Limited Access Role*

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

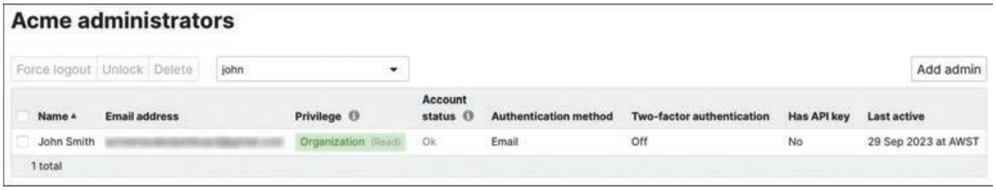


Two-factor Authentication is not currently enabled on your Meraki Dashboard account. For an extra layer of security, we recommend enabling it at your earliest convenience.

| | Last seen | Usage | Client type, OS | IPv4 address | Policy |
|---|---|---|---|---|---|
| | Sep 10 07:40 | 1.6 MB | Other | 192.168.101.22 | Devices |
| | Sep 10 07:40 | 86.0 MB | iPad Air, iOS16.6 | 192.168.100.221 | Users |
| | Sep 10 07:41 | 47.4 MB | Apple iPhone | 192.168.100.238 | Users |
| | Sep 10 07:40 | 27.2 MB | Other | 192.168.101.17 | Devices |
| | Sep 10 07:41 | 383.4 MB | Other | 192.168.100.216 | Users |
| | Sep 10 07:41 | 9.7 MB | Android | 192.168.101.18 | Devices |
| | Sep 10 07:41 | 389.8 MB | iPhone 12 Pro, iOS16.6.1 | 192.168.100.152 | normal |
| RingPro-62 | Sep 10 07:41 | 322.6 MB | Other | 192.168.200.10 | Security |
| bondi-g-mv72-1-9818886569b8 | Sep 10 07:41 | 61.8 MB | Meraki | 192.168.200.6 | Security |

**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).



Acme administrators

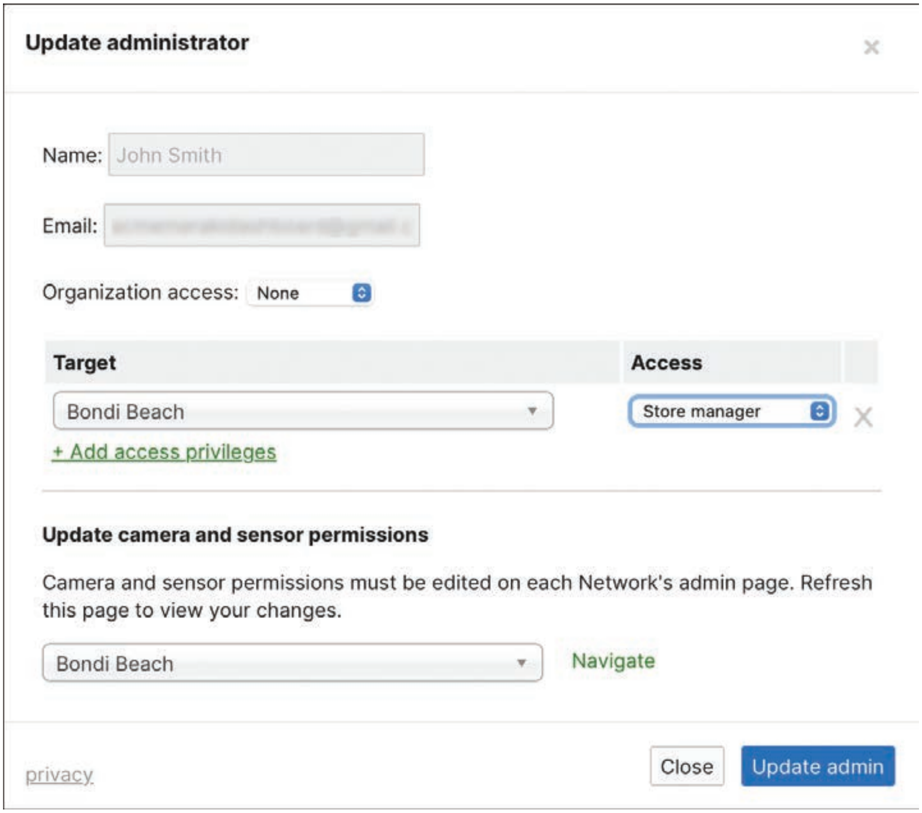
Force logout | Unlock | Delete    john    Add admin

| | Name ▲ | Email address | Privilege | Account status | Authentication method | Two-factor authentication | Has API key | Last active |
|---|---|---|---|---|---|---|---|---|
| □ | John Smith | [redacted] | Organization (Read) | Ok | Email | Off | No | 29 Sep 2023 at AWST |

1 total

**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.**



**Update administrator**

Name: John Smith

Email: [redacted]

Organization access: None

| Target | Access |
|---|---|
| Bondi Beach | Store manager |

**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.

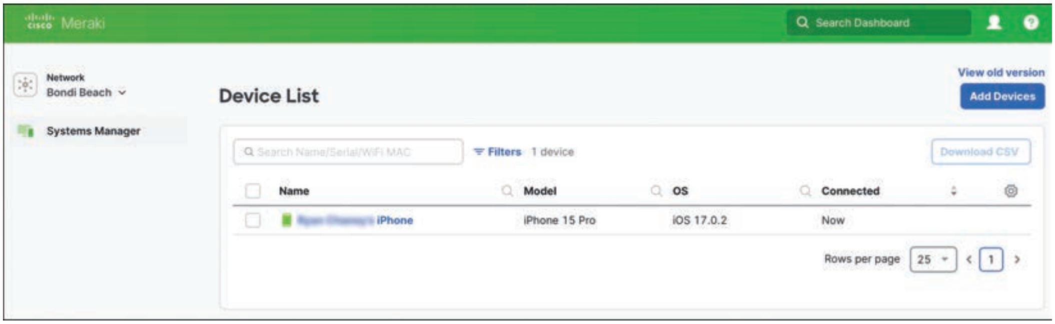
Bondi Beach

**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:

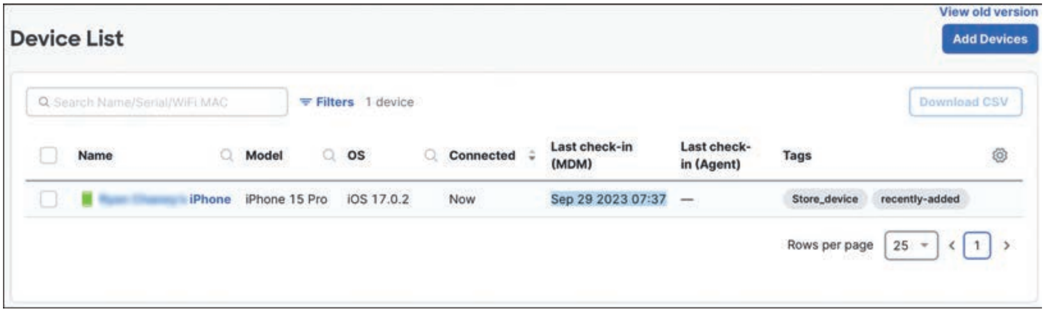
**Step 1.** Log in as the user with the limited access role. Navigate to **Systems Manager > Devices.** Note the limited view of Dashboard that this user has, as demonstrated in Figure 4-36.



| Name | Model | OS | Connected |
|---|---|---|---|
| [redacted] iPhone | iPhone 15 Pro | iOS 17.0.2 | Now |

**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.



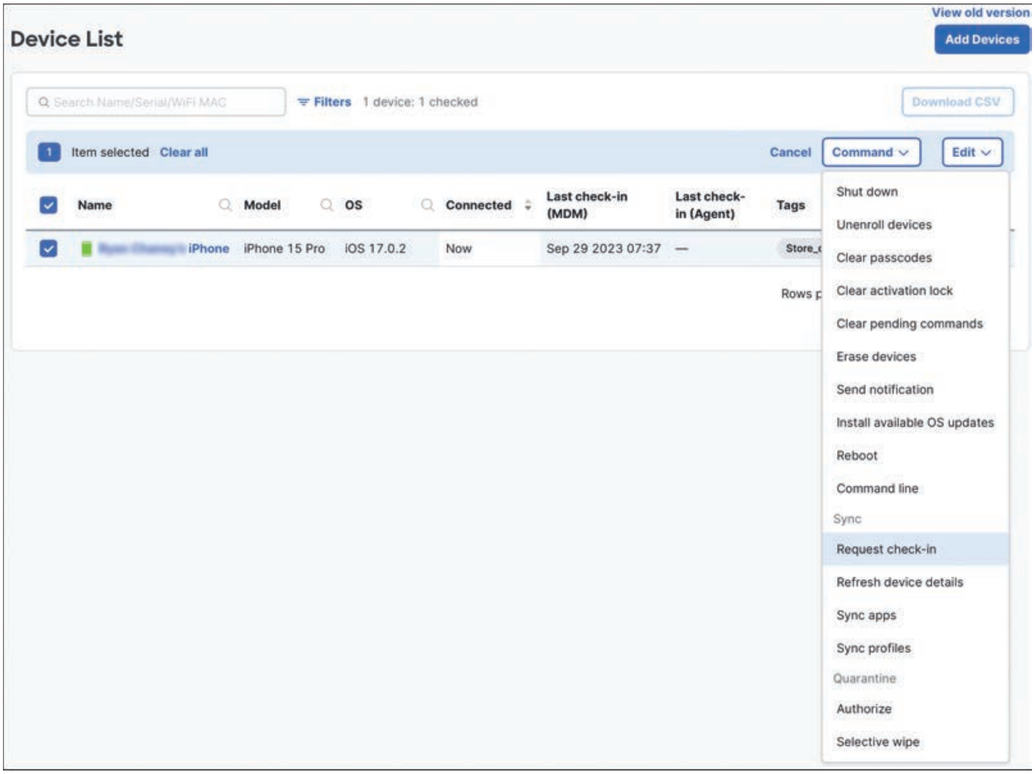
| Name | Model | OS | Connected | Last check-in (MDM) | Last check-in (Agent) | Tags |
|---|---|---|---|---|---|---|
| [redacted] iPhone | iPhone 15 Pro | iOS 17.0.2 | Now | Sep 29 2023 07:37 | — | Store_device<br>recently-added |

**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.



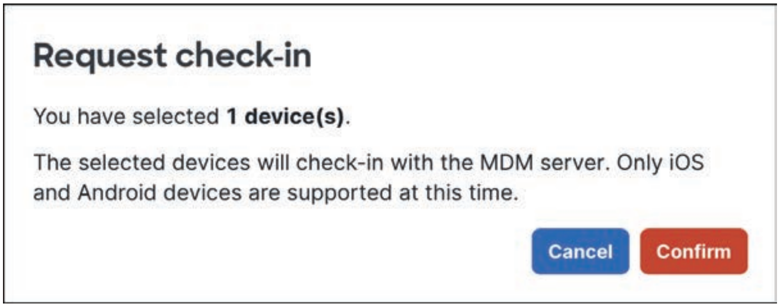
Device List

1 device: 1 checked

1 Item selected Clear all

| ☑ | Name | Model | OS | Connected | Last check-in (MDM) | Last check-in (Agent) | Tags |
|---|---|---|---|---|---|---|---|
| ☑ | [redacted] iPhone | iPhone 15 Pro | iOS 17.0.2 | Now | Sep 29 2023 07:37 | — | Store_( |

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



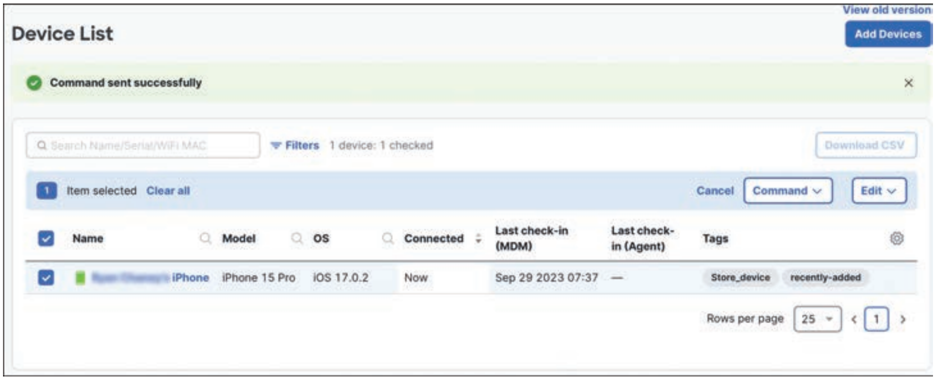
Request check-in

You have selected **1 device(s)**.

The selected devices will check-in with the MDM server. Only iOS and Android devices are supported at this time.

**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.”



Device List

Command sent successfully

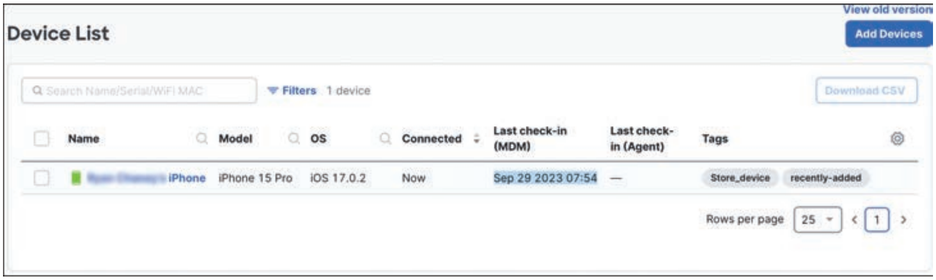
Search Name/Serial/WiFi MAC

1 device: 1 checked

1 Item selected

| ☑ | Name | Model | OS | Connected | Last check-in (MDM) | Last check-in (Agent) | Tags |
|---|---|---|---|---|---|---|---|
| ☑ | [redacted] iPhone | iPhone 15 Pro | iOS 17.0.2 | Now | Sep 29 2023 07:37 | — | Store_device recently-added |

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



Device List

Search Name/Serial/WiFi MAC

1 device

| □ | Name | Model | OS | Connected | Last check-in (MDM) | Last check-in (Agent) | Tags |
|---|---|---|---|---|---|---|---|
| □ | [redacted] iPhone | iPhone 15 Pro | iOS 17.0.2 | Now | Sep 29 2023 07:54 | — | Store_device recently-added |

**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