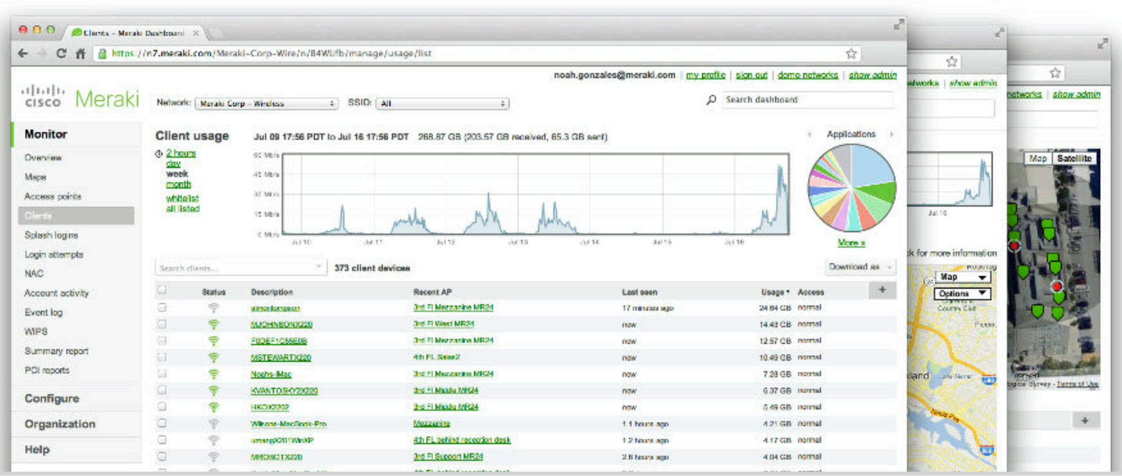
Cloud Management



Client usage

Jul 09 17:56 PDT to Jul 16 17:56 PDT 268.87 GB (203.57 GB received, 65.3 GB sent)

373 client devices

Status	Description	Recent AP	Last seen	Usage ▾	Access
	simonlompaun	3rd Fl Mezzanine MR24	17 minutes ago	24.84 GB	normal
	MJOHNSONX220	3rd Fl West MR24	now	14.43 GB	normal
	F0DEF1C56E0B	3rd Fl Mezzanine MR24	now	12.57 GB	normal
	MSTEWARTX220	4th FL Sales2	now	10.49 GB	normal
	Noahs-Mac	3rd Fl Mezzanine MR24	now	7.28 GB	normal
	KVANTOSKYZX220	3rd Fl Middle MR24	now	6.37 GB	normal
	HKOX2202	3rd Fl Middle MR24	now	5.49 GB	normal
	Wilsons-MacBook-Pro	Mezzanine	1.1 hours ago	4.21 GB	normal
	umanpXP011WinXP	4th FL behind reception desk	1.2 hours ago	4.17 GB	normal
	MMOSC1X220	3rd Fl Support MR24	2.8 hours ago	4.04 GB	normal

Overview

Meraki's cloud based management provides centralized visibility & control over Meraki's wired & wireless networking hardware, without the cost and complexity of wireless controllers or overlay management systems. Integrated with Meraki's entire product portfolio, cloud management provides feature rich, scalable, and intuitive centralized management for networks of any size.

Highlights

- Unified visibility and control of the entire network via a single dashboard: wireless, switching, and security appliances
- Streamlines large networks with tens of thousands of endpoints
- Zero-touch provisioning for rapid deployment
- Built-in multi site network management tools
- Automated network monitoring and alerts
- Intuitive interface eliminates costly training or added staff
- Network tagging engine - search and sync settings by tag
- Role-based administration and auditable change logs
- Continuous feature updates delivered from the cloud
- Highly available and secure (PCI / HIPAA compliant)

Cloud Managed Networks

Meraki's hardware products are built from the ground up for cloud management. As a result, they come out of the box with centralized control, layer 7 device and application visibility, real time web-based diagnostics, monitoring, reporting, and much more.

Meraki networks deploy quickly and easily, without training or dedicated staff. Moreover, Meraki provides a rich feature set that provides complete control over devices, users, and applications, allowing for flexible access policies and rich security without added cost or complexity.

Meraki's cloud management provides the features, security, and scalability for networks of any size. Meraki scales from small sites to campuses, and even distributed networks with thousands of sites. Meraki devices, which self-provision via the cloud, can be deployed in branches without IT. Firmware and security signature updates are delivered seamlessly, over the web. With the cloud, branches can automatically establish secure VPN tunnels between one another with a single click.

With a secure, PCI and HIPAA compliant architecture and fault tolerant design that preserves local network functionality during WAN outages, Meraki is field proven in high security and mission critical network applications.

Cloud Management Architecture

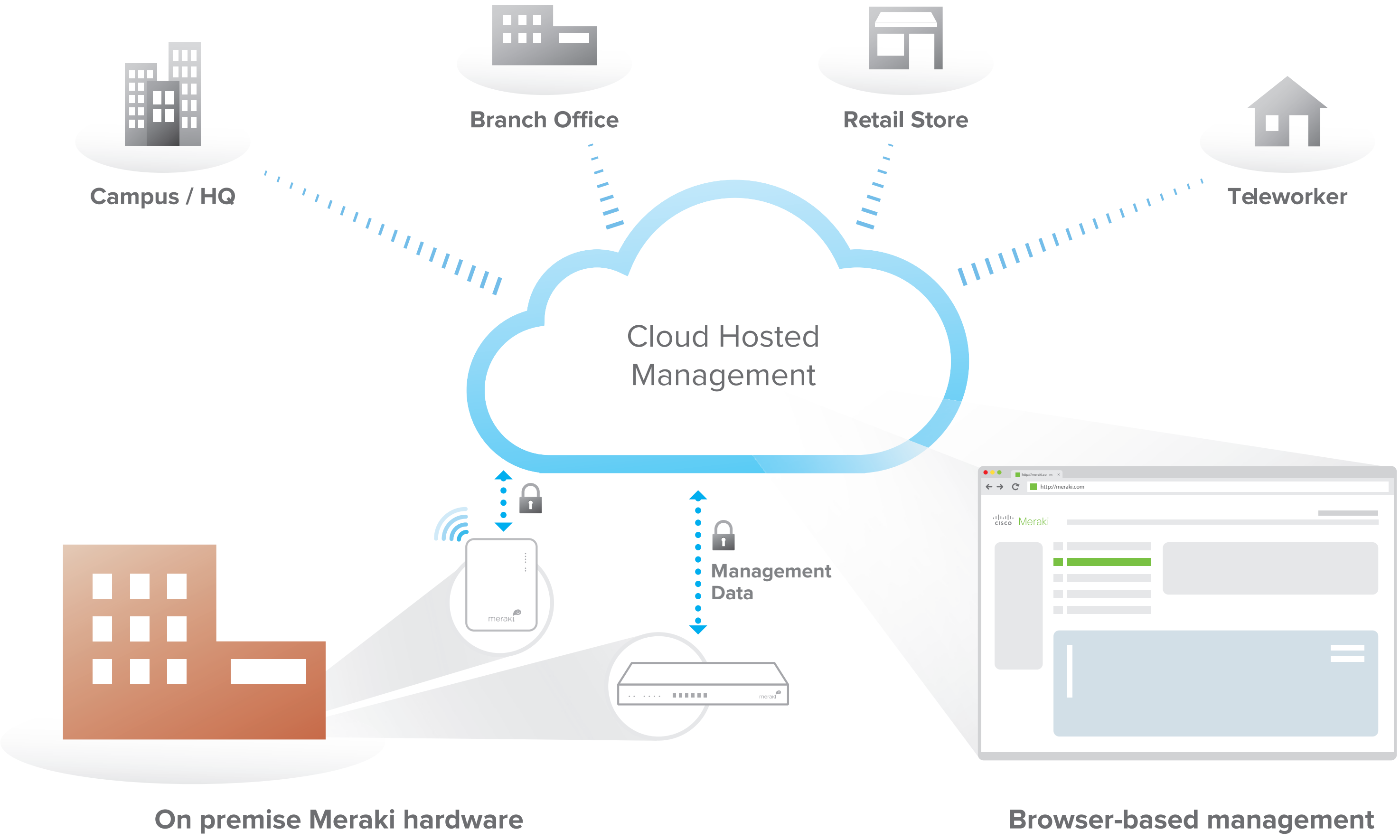
Meraki's architecture provides feature rich network management without on-site management appliances or WiFi controllers.

Every Meraki device - including wirelesss access points, Ethernet switches, and security appliances - connects over the Internet to Meraki's datacenters, which run Meraki's cloud management platform. These connections, secured via SSL, utilize a patented protocol that provides real time visibility and control, yet uses minimal bandwidth overhead (typically 1 kbps or less.)

In place of traditional command-line based network configuration, Meraki provides a rich web based dashboard, providing visibility and control over up to tens of thousands of Meraki devices, anywhere in the world. Tools, designed to scale to large and distributed networks, make policy changes, firmware updates, deploying new branches, etc. simple and expedient, regardless of size or location. Meraki's real time protocols combine the immediacy of on-premise management applications with the simplicity and centralized control of a cloud application.

Every Meraki device is engineered for cloud management. Specifically, this means that Meraki devices are designed with memory and CPU resources to perform packet processing, QoS, layer 3-7 security, encryption, etc. at the network edge. As a result, no network traffic passes through the cloud, with the cloud providing management functionality out of the data path. This architecture enables networks to scale horizontally, adding capacity simply by adding more endpoints, without concern for centralized bottlenecks or chokepoints. Equally important, since all packet processing is performed on premise, end-user functionality is not compromised if the network's connection to the cloud is interrupted.

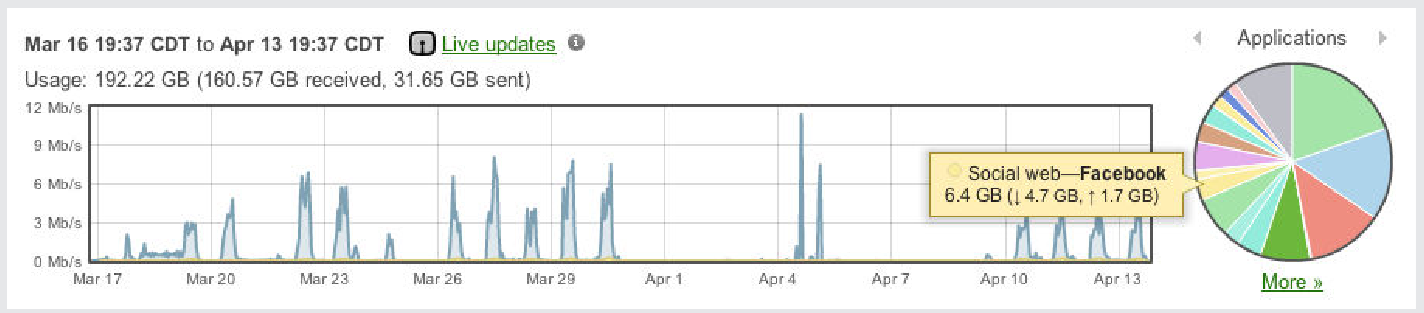
Meraki's cloud platform is designed to spread computation and storage across independent server clusters in geographically isolated datacenters. Any server or datacenter can fail without affecting customers or the rest of the system. Additionally, Meraki's datacenter design is field proven to support tens of thousands of endpoints.



Powerful Insight and Troubleshooting Tools

Meraki's cloud architecture delivers powerful insight and includes live tools integrated directly into the dashboard, giving instant analysis of performance, connectivity, and more. Using live tools, network administrators no longer need to go on site to perform routine troubleshooting tests. Visibility into devices, users, and applications gives administrators the information needed to enforce security policies and enable the performance needed in today's demanding network environments.

Troubleshooting tools such as ping, traceroute, throughput, and even live packet captures are integrated directly into the Meraki dashboard, dramatically reducing resolution times and enabling troubleshooting at remote locations without on-site IT staff.

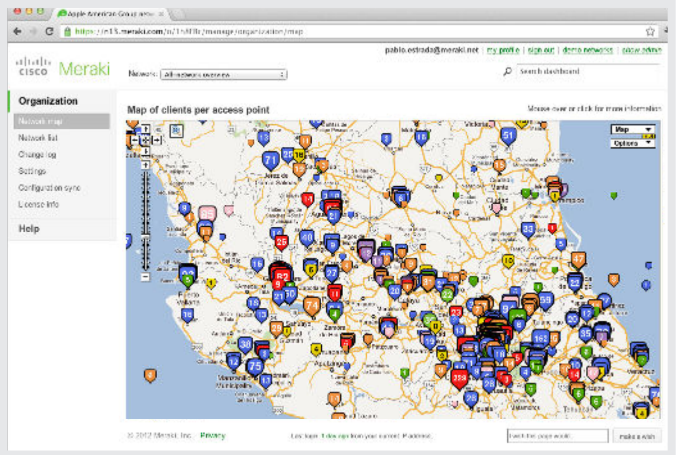


Mar 16 19:37 CDT to **Apr 13 19:37 CDT** Live updates

Usage: 192.22 GB (160.57 GB received, 31.65 GB sent)

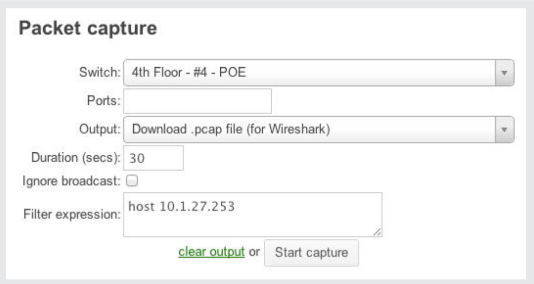
Social web—**Facebook**
6.4 GB (↓ 4.7 GB, ↑ 1.7 GB)

Layer 7 application visibility



Meraki
pablo.estrada@meraki.net | my profile | sign out | demo networks | view admin
Network: All network overview
Search dashboard
Organization
Network map
Network list
Change log
Settings
Configuration sync
License info
Help
Map of clients per access point
Mouse over or click for more information
Map
Options
© 2012 Meraki, Inc.
Privacy

Integrated multi-site management

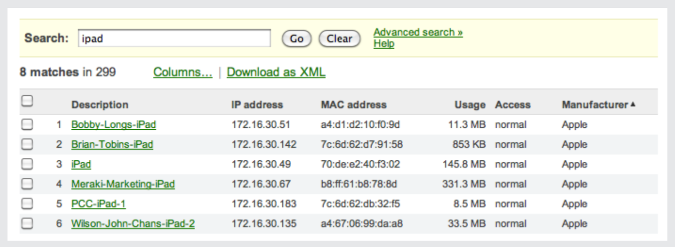


Packet capture

Switch:	4th Floor - #4 - POE
Ports:	
Output:	Download .pcap file (for Wireshark)
Duration (secs):	30
Ignore broadcast:	□
Filter expression:	host 10.1.27.253

clear output or Start capture

Live Troubleshooting Tools

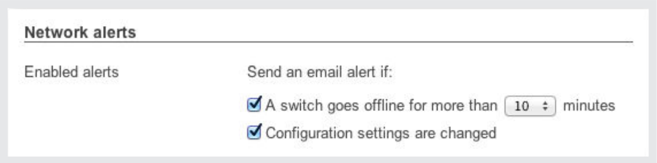


Search: ipad Go Clear Advanced search » Help

8 matches in 299 Columns... | Download as XML

□		Description	IP address	MAC address	Usage	Access	Manufacturer ▲
□	1	Bobby-Longs-iPad	172.16.30.51	a4:d1:d2:10:f0:9d	11.3 MB	normal	Apple
□	2	Brian-Tobins-iPad	172.16.30.142	7c:6d:62:d7:91:58	853 KB	normal	Apple
□	3	iPad	172.16.30.49	70:de:e2:40:f3:02	145.8 MB	normal	Apple
□	4	Meraki-Marketing-iPad	172.16.30.67	b8:ff:61:b8:78:8d	331.3 MB	normal	Apple
□	5	PCC-iPad-1	172.16.30.183	7c:6d:62:db:32:f5	8.5 MB	normal	Apple
□	6	Wilson-John-Chans-iPad-2	172.16.30.135	a4:67:06:99:da:a8	33.5 MB	normal	Apple

User and Device Fingerprints



Network alerts

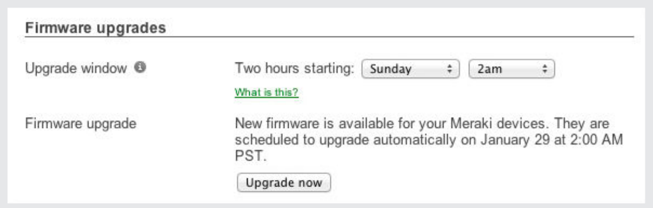
Enabled alerts

Send an email alert if:

☑ A switch goes offline for more than 10 minutes

☑ Configuration settings are changed

Automatic E-mail Alerts



Firmware upgrades

Upgrade window — Two hours starting: Sunday 2am

What is this?

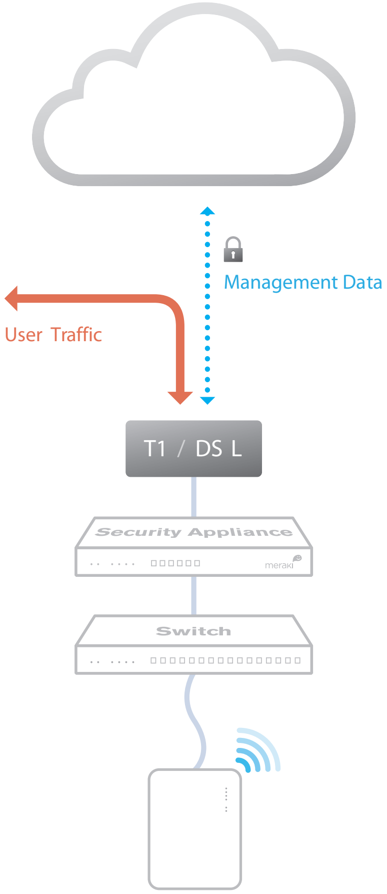
Firmware upgrade — New firmware is available for your Meraki devices. They are scheduled to upgrade automatically on January 29 at 2:00 AM PST.

Upgrade now

Scheduled Firmware Updates

Out-of-Band Control Plane

Meraki's out-of-band control plane separates network management data from user data. Management data (e.g., configuration, statistics, monitoring, etc.) flows from Meraki devices (wireless access points, switches, and security appliances) to Meraki's cloud over a secure Internet connection. User data (web browsing, internal applications, etc.) does not flow through the cloud, instead flowing directly to its destination on the LAN or across the WAN.



Advantages of an out of band control plane:

Scalability

- Unlimited throughput: no centralized controller bottlenecks
- Add devices or sites without MPLS tunnels
- Add switching capacity without stacking limitations

Reliability

- Redundant cloud service provides high availability
- Network functions even if management traffic is interrupted

Security

- No user traffic passes through Meraki's datacenters
- Fully HIPAA / PCI compliant

What happens if a network loses connectivity to the Meraki cloud?

Because of Meraki's out of band architecture, most end users are not affected if Meraki wireless APs, switches, or security appliances cannot communicate with Meraki's cloud services (e.g., because of a temporary WAN failure):

- Users can access the local network (printers, file shares, etc.)
- If WAN connectivity is available, users can access the Internet
- Network policies (firewall rules, QoS, etc.) continue to be enforced
- Users can authenticate via 802.1X/RADIUS and can roam wirelessly between access points
- Users can initiate and renew DHCP leases
- Established VPN tunnels continue to operate
- Local configuration tools are available (e.g., device IP configuration)

While Meraki's cloud is unreachable, management, monitoring, and hosted services are temporarily unavailable:

- Configuration and diagnostic tools are unavailable
- Usage statistics are stored locally until the connection to the cloud is re-established, at which time they are pushed to the cloud
- Splash pages and related functionality are unavailable

Meraki Datacenter Design

Meraki's cloud management service is colocated in tier-1, SAS70 type II certified datacenters. These datacenters feature state of the art physical and cyber security and highly reliable designs. All Meraki services are replicated across multiple independent datacenters, so that customer-facing services fail over rapidly in the event of a catastrophic datacenter failure.

Redundancy

- Five geographically dispersed datacenters
- Every customer's data (network configuration and usage metrics) replicated across three independent datacenters
- Real-time data replication between datacenters (within 60 seconds)
- Nightly archival backups

Availability Monitoring

- 24x7 automated failure detection — all servers are tested every five minutes from multiple locations
- Rapid escalation procedures across multiple operations teams
- Independent outage alert system with 3x redundancy

Disaster Recovery

- Rapid failover to hot spare in event of hardware failure or natural disaster
- Out of band architecture preserves end-user network functionality, even if connectivity to Meraki's cloud services is interrupted
- Failover procedures drilled weekly

Cloud Services Security

- 24x7 automated intrusion detection
- Protected via IP and port-based firewalls
- Access restricted by IP address and verified by public key (RSA)
- Systems are not accessible via password access
- Administrators automatically alerted on configuration changes

Physical Security

- High security card keys and biometric readers control facility access
- All entries, exits, and cabinets are monitored by video surveillance
- Security guards monitor all traffic into and out of the datacenters 24x7, ensuring that entry processes are followed

Out-of-Band Architecture

- Only configuration and usage statistics are stored in the cloud
- End user data does not traverse through the datacenter
- All sensitive data (e.g., passwords) stored in encrypted format

Disaster Preparedness

- Datacenters feature sophisticated sprinkler systems with interlocks to prevent accidental water discharge
- Diesel generators provide backup power in the event of power loss
- UPS systems condition power and ensure orderly shutdown in the event of a full power outage
- Each datacenter has service from at least two top-tier carriers
- Seismic bracing for raised floor, cabinets, and support systems
- In the event of a catastrophic datacenter failure, services fail over to another geographically separate datacenter

Environmental Controls

- Over-provisioned HVAC systems provide cooling and humidity control
- Flooring systems are dedicated for air distribution

Certification

- Meraki datacenters are SAS70 type II certified
- PCI level 1 certified

Service Level Agreement

- Meraki's cloud management is backed by a 99.99% uptime SLA. See www.meraki.com/trust for details.

Security Tools for Administrators

In addition to Meraki's secure out-of-band architecture and hardened datacenters, Meraki provides a number of tools for administrators to maximize the security of their network deployments. These tools provide optimal protection, visibility, and control over your Meraki network.

Two-factor authentication

Two-factor authentication adds an extra layer of security to an organization's network by requiring access to an administrator's phone, in addition to her username and password, in order to log in to Meraki's cloud services. Meraki's two factor authentication implementation uses secure, convenient, and cost effective SMS technology: after entering their username and password, an administrator is sent an a one-time passcode via SMS, which they must enter before authentication is complete. In the event that a hacker guesses or learns an administrator's password, she still will not be able to access the organization's account, as the hacker does not have the administrator's phone. Meraki includes two-factor authentication for all enterprise users at no additional cost.

Password policies

Organization-wide security policies for Meraki accounts help protect access to the Meraki dashboard. These tools allow administrators to:

- Force periodic password changes (e.g., every 90 days)
- Require minimum password length and complexity
- Lock users out after repeated failed login attempts
- Disallow password reuse
- Restrict logins by IP address

Role-based administration

Role-based administration lets supervisors appoint administrators for specific subsets of an organization, and specify whether they have read-only access to reports and troubleshooting tools, administer managed guest access, or can make configuration changes to the network. This minimizes the chance of accidental or malicious misconfiguration, and restricts errors to isolated parts of the network.

Configuration change alerts

The Meraki system can automatically send human-readable email and text message alerts when configuration changes are made, enabling the entire IT organization to stay abreast of new policies. Change alerts are particularly important with large or distributed IT organizations.

Configuration and login audits

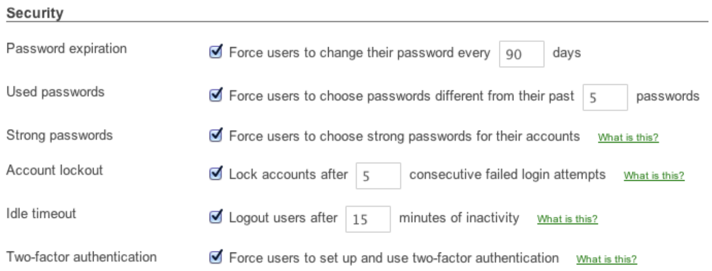
Meraki logs the time, IP, and approximate location (city, state) of logged in administrators. A searchable configuration change log indicates what configuration changes were made, who they were made by, and which part of the organization the change occurred in.

SSL certificates

Meraki accounts can only be accessed via https, ensuring that all communication between an administrator's browser and Meraki's cloud services is encrypted.

Idle Timeout

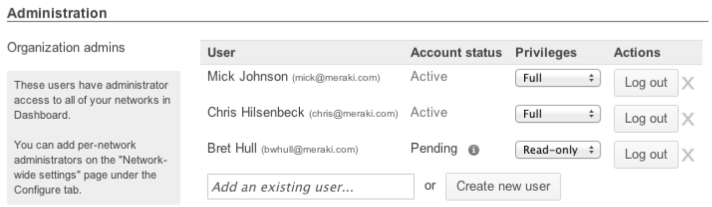
30 seconds before being logged out, users are shown a notice that allows them to extend their session. Once time expires, users are asked to log in again.



Security

Password expiration	☑ Force users to change their password every 90 days
Used passwords	☑ Force users to choose passwords different from their past 5 passwords
Strong passwords	☑ Force users to choose strong passwords for their accounts What is this?
Account lockout	☑ Lock accounts after 5 consecutive failed login attempts What is this?
Idle timeout	☑ Logout users after 15 minutes of inactivity What is this?
Two-factor authentication	☑ Force users to set up and use two-factor authentication What is this?

Password Security Policies



Administration

Organization admins

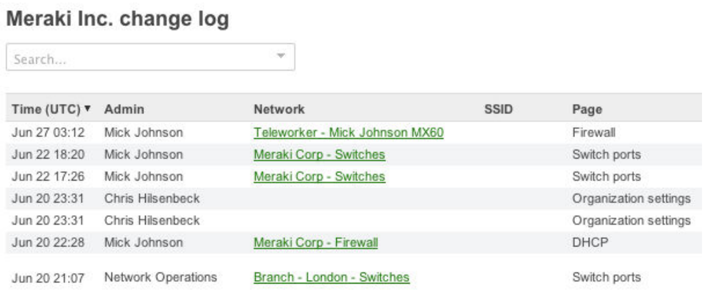
These users have administrator access to all of your networks in Dashboard.

You can add per-network administrators on the "Network-wide settings" page under the Configure tab.

User	Account status	Privileges	Actions
Mick Johnson (mick@meraki.com)	Active	Full	Log out ✕
Chris Hilsenbeck (chris@meraki.com)	Active	Full	Log out ✕
Bret Hull (bwhull@meraki.com)	Pending	Read-only	Log out ✕

Add an existing user... or Create new user

Role-Based Administration



Meraki Inc. change log

Search...

Time (UTC) ▾	Admin	Network	SSID	Page
Jun 27 03:12	Mick Johnson	Teleworker - Mick Johnson MX60		Firewall
Jun 22 18:20	Mick Johnson	Meraki Corp - Switches		Switch ports
Jun 22 17:26	Mick Johnson	Meraki Corp - Switches		Switch ports
Jun 20 23:31	Chris Hilsenbeck			Organization settings
Jun 20 23:31	Chris Hilsenbeck			Organization settings
Jun 20 22:28	Mick Johnson	Meraki Corp - Firewall		DHCP
Jun 20 21:07	Network Operations	Branch - London - Switches		Switch ports

Configuration Change Audits