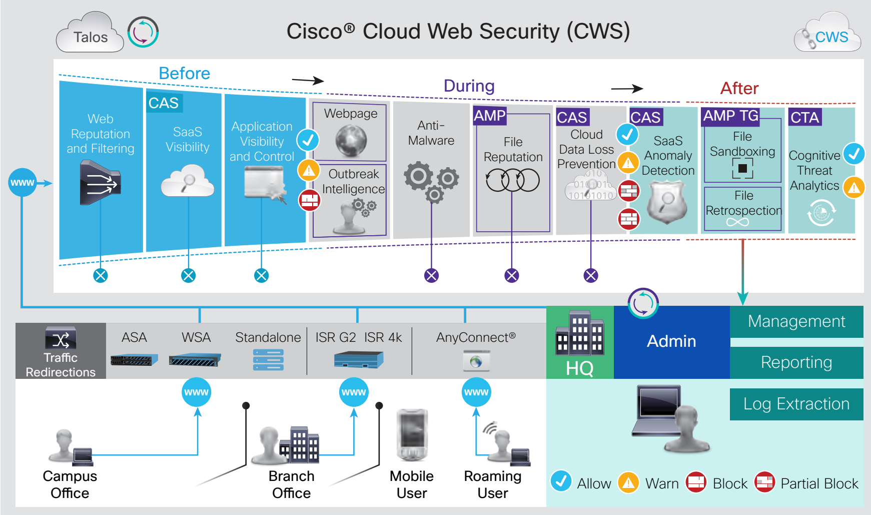
At-a-Glance

Cisco Cloud Web Security

Deliver Security as a Service

Meet a very different security approach from Cisco: comprehensive web security as a cloud service. With the Cisco Cloud Web Security (CWS) solution, Cisco is delivering intelligent cybersecurity for the real world. We provide superb visibility, consistent control, and advanced threat protection before, during, and after an attack.



As a cloud-delivered web security solution, Cisco CWS offers extensive security as a service (SaaS). Deployment is simple and fast. No maintenance or upgrades are required.

With Cisco CWS, administrators can set and enforce specific web use policies across the entire environment. Users can connect Cisco CWS to their existing infrastructure with flexible network integration options. Cisco CWS controls access to websites and specific content in Web pages and applications as well as SaaS applications. Cisco's analysis engines deliver continual industry-leading antimalware and zero-day threat protection against web-based attacks. Our advanced global threat telemetry network continuously updates Cisco CWS against the latest threats.

Cisco Advanced Malware Protection (AMP) protects against advanced malware and tracks file disposition over time to see where malicious files travel. Cognitive Threat Analytics (CTA) scans web traffic for symptoms of an infection and addresses threats that bypass perimeter defenses. Cloud Access Security (CAS) provides protection for the growing risks created by SaaS Apps. And centralized management and reporting provide increased visibility into web usage and threat information.

Benefits

- **Granular web use policies:** Set and enforce across the entire environment for applications, websites and specific webpage content.
- **Easy to integrate:** With flexible network integration options, you can connect Cisco Cloud Web Security (CWS) to your existing infrastructure.
- **Real-time threat intelligence:** Analysis engines deliver industry-leading antimalware and zero-day threat protection from web-based attacks. Our advanced global threat telemetry network continuously updates Cisco CWS to protect against the latest threats.
- **Centralized management and reporting:** Increased visibility into web usage and threat information.

Cloud Web Security Pillars

Comprehensive Defense

Through web filtering and web reputation scoring, Cisco CWS controls access to more than 50 million known websites by applying filters from a list of more than 75 content categories. Our application visibility and control features include SaaS visibility along with acceptable use policy that increases employee productivity and compliance. These controls cover access to web pages, individual web parts, activities within SaaS applications and microapplications so employees can access sites needed for work. Centralized policy management helps you enforce policies and manage the entire solution across all branches and users from a single centralized location that is accessible anywhere, at any time.

Real-time malware protection is based on the identification of unknown, unusual behaviors and zero-hour outbreaks through a heuristics-based, antimalware engine. Outbreak intelligence runs webpage components in a highly secure virtual emulation to determine how each component behaves and blocks any malware. Roaming users are protected with Cisco AnyConnect®, which enforces the same security features available with Cisco CWS in your company's offices. A secure mobile browser provides protection for mobile devices.

Advanced Threat Protection

Cisco AMP and Threat Grid protects your environment across the attack continuum: before, during, and after an attack. The file reputation feature allows Cisco to capture a fingerprint of each file as it traverses the customer network. These fingerprints are sent to AMP's cloud-based intelligence network for a reputation verdict.

After an attack, using file retrospection, you can track a file's disposition over time after it enters your environment. If it is found to be malware, you can discover where the file entered and where it is currently located to mitigate future intrusions.

Our cloud-based CTA feature helps reduce threat identification time to minutes with its continuous efforts. CTA actively identifies symptoms of a malware infection through behavioral analysis, anomaly detection, and machine learning. And with the Cisco Talos Security Intelligence Research Group, among the largest threat detection networks in the world, leading researchers and systems continuously deliver security intelligence to Cisco CWS based on threat tracking across networks, endpoints, mobile devices, virtual systems, the web, and email around the globe.

CAS extends your control to cloud apps, allowing you to set policy that governs how users are permitted to share data with cloud apps. It detects anomalous traffic and allows you to identify root-causes of incidents.

Superior Flexibility

Cisco CWS is backed by a worldwide network and 23 data centers with service-level agreements (SLAs) based on 99.999 percent uptime. You can tailor visibility into your web usage with more than 10,000 customizable reports, updated every 10 minutes, and the ability to categorize traffic by user and application traffic. Web usage data may also be accessed quickly and with a high degree of security by a variety of reporting and analysis tools such as security information and event management (SIEM).

You can also save time and money by redirecting traffic to Cisco CWS through existing Cisco products such as the Cisco Integrated Router G2 and ISR 4000, Cisco Adaptive Security Appliances (ASA and ASAv) next-generation firewalls, Cisco Web Security Appliances (WSA and WSAV), and the Cisco AnyConnect Web Security Module. You can also connect to Cisco CWS in a standalone deployment.

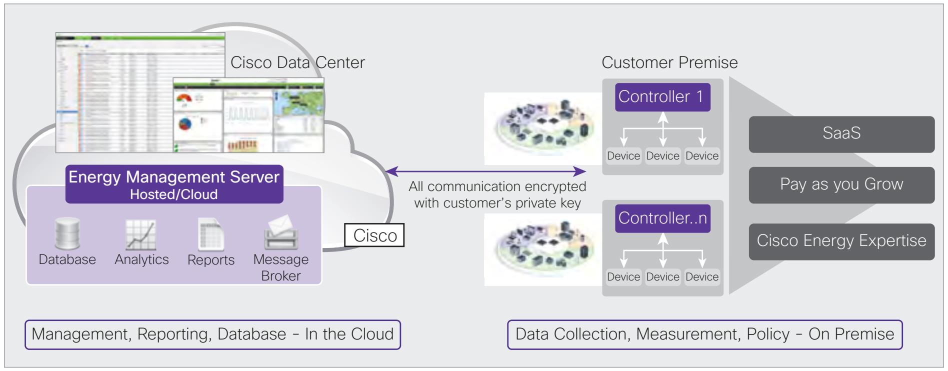
Next Steps

Find out more at http://www.cisco.com/go/cloudwebsecurity.

Cisco Energy Management Cloud

Reduce energy costs and optimize energy consumption in your data center and distributed offices with Cisco® Energy Management® Suite – now enhanced with technology from the recent acquisition of JouleX. See, measure, and manage energy usage of all your IP-connected systems. And now you can manage energy without installing software on your premises, using Cisco Energy Management Cloud, a software-as-a-service (SaaS) application. Gain unprecedented energy usage visibility for every device and system connected to your network. Take advantage of Cisco's energy expertise, greater resiliency, and hassle-free management while paying as you go.

Figure 1. Cisco Energy Management Cloud Model



Begin analyzing and measuring your energy usage quickly without the need for installing a premise-based solution with Cisco Energy Management Cloud. Enjoy robust database, analytics, and reporting from an easy-to-use web interface.

See and Optimize Energy Usage

Rising energy costs increase expenses, so you have less money for critical enterprise projects. You can't invest in additional capacity because of energy constraints. Without a way to see energy use, it is difficult to improve your situation. However, it's costly to purchase, deploy, or manage yet another premise-based solution. You'd rather free your IT team for more important projects that really move the company forward.

Imagine seeing, measuring, and managing all of the energy being used in your company from just one place. When you leave work in the evening and put your computer to sleep, your IT equipment goes to sleep too. That includes your laptops, monitors, IP phones, wireless access points, copiers and printers. You know you're saving money. And you don't have to install hardware to do it.

Cloud-Based for Down-to-Earth Savings

The Cisco Energy Management Cloud delivers powerful, easy-to-use energy management capabilities. This data lets you measure energy usage across your data center and distributed offices.

Manage all of your network-connected devices - including PCs, phones, printers, monitors, virtual servers, and more - not just Cisco devices. And do it through the cloud and an easy-to-use web-based interface. Cisco Energy Management Cloud offers robust database, analytics, and reporting features from a single management pane.

And rest assured that your data is safe. Cisco Energy Management Suite does not collect personal information from devices managed, it collects information about device attributes for the purpose of reporting and analyzing. The data communication between controller and data center is secured using asymmetric encryption. Data stored in databases is also encrypted and is not available to Cisco and its employees.

Choose the Right Level

Choose the right level of service to match your company's needs:

Fast Start trial: Try before you buy with this 45-day trial offer that can be used for up to 500 devices in distributed offices and data centers. Gain comprehensive reporting, unlimited policy management, and immediate visibility into your energy usage. Just download and install the Windows controller software and log into the customer portal.

Foundation: This package is available with 1-5-year subscription plans. Choose the duration that suits you and measure an unlimited number of devices across up to 100 distributed office locations. Get deep visibility into energy usage with more than a dozen reports. Asset connectors and scripting for distributed office devices are included. Foundation customers also receive remote support.

Standard: This package is available with 1-5-year subscription plans. It includes device monitoring and management, a variety of reports and export capabilities, unlimited policies enabled, remote support, asset connectors, and optional single-sign-on.

Advanced: This package includes all of the elements of the standard package, as well as ongoing recommendations, best practices, and remote audit and assurance service from Cisco Energy Management experts.

Cisco Energy Management Cloud Benefits

- **Increase office and data center energy efficiency:** See every device connected to your network at any time along with how they are being used, at what time, where, and how much energy they are using.
- **Reduce IT energy and ownership costs:** You can reduce IT-related energy costs by as much as 35 percent with this innovative energy management suite of tools and services.
- **Cost-effective energy monitoring:** The Cisco Energy Management Cloud service eliminates the need for capital expenditures on servers and other equipment, as well as operations costs associated with on-premises software deployments.
- **Energy expertise:** Energy management experts from Cisco are available to help you create energy policy and implement best practices. Customized device integration assistance is also available.
- **See a difference quickly:** As a cloud-based service, Cisco Energy Management Cloud can be turned up in just a few days. There's no software to install on all of your devices, so it's fast to implement. And the Fast-Start trial takes only minutes to sign up. Start seeing savings in days.
- **Scale as needed:** Because it's a cloud service, Cisco Energy Management Cloud can scale as your needs require.
- **Gain resiliency:** Cisco Energy Management Cloud helps increase solution resiliency. With cloud hosting from Cisco, you get a high-availability service, service level agreements (SLAs), backups, and disaster recovery. You don't have to build a high-availability premise-based system.
- **Improve budget predictability:** Cisco Energy Management Cloud gives you better budget predictability. You'll know your exact cost per month, and gain energy savings at the same time.

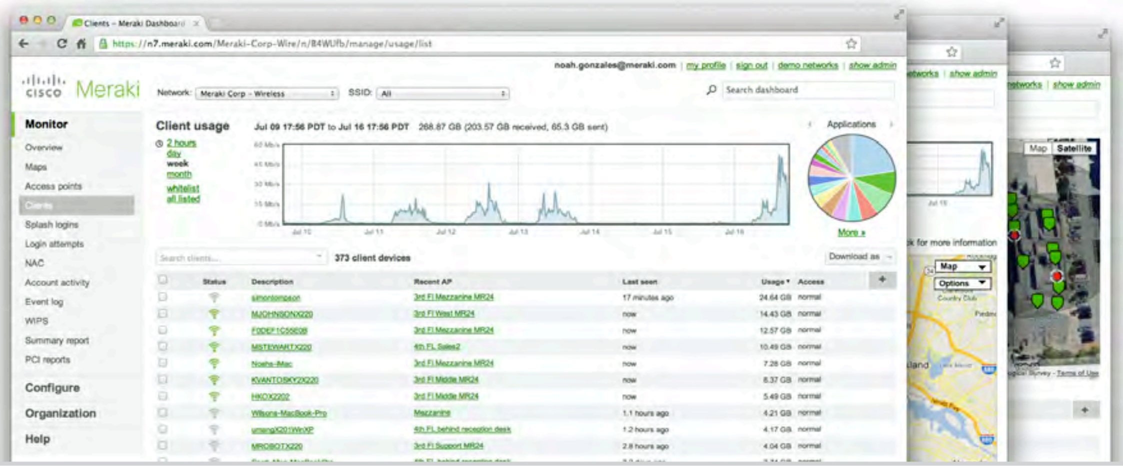
Why Cisco?

We combine the experience of the world's leader in networking with unique, network-based energy management software. Only the Cisco Energy Management Suite uses your existing network infrastructure to save energy and meet your ROI goals.

For More Information

Ask your Cisco representative about the Cisco Energy Management Cloud Fast-Start free trial or the Cisco Energy Management Discovery Service. For more information, visit http://www.cloud.cisco.com/energy. If you are already a customer, please log in here http://www.cloud.cisco.com/energy.

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
	simontompson	3rd Fl Mezzanine MR24	17 minutes ago	24.64 GB	normal
	MJOHNSONX220	3rd Fl West MR24	now	14.43 GB	normal
	F0DEF1C55E08	3rd Fl Mezzanine MR24	now	12.57 GB	normal
	MSTEWARTX220	4th FL Sales2	now	10.49 GB	normal
	Noahs-iMac	3rd Fl Mezzanine MR24	now	7.28 GB	normal
	KVANTOSKYX220	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
	umangX201WinXP	4th FL behind reception desk	1.2 hours ago	4.17 GB	normal
	MROBOTX220	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

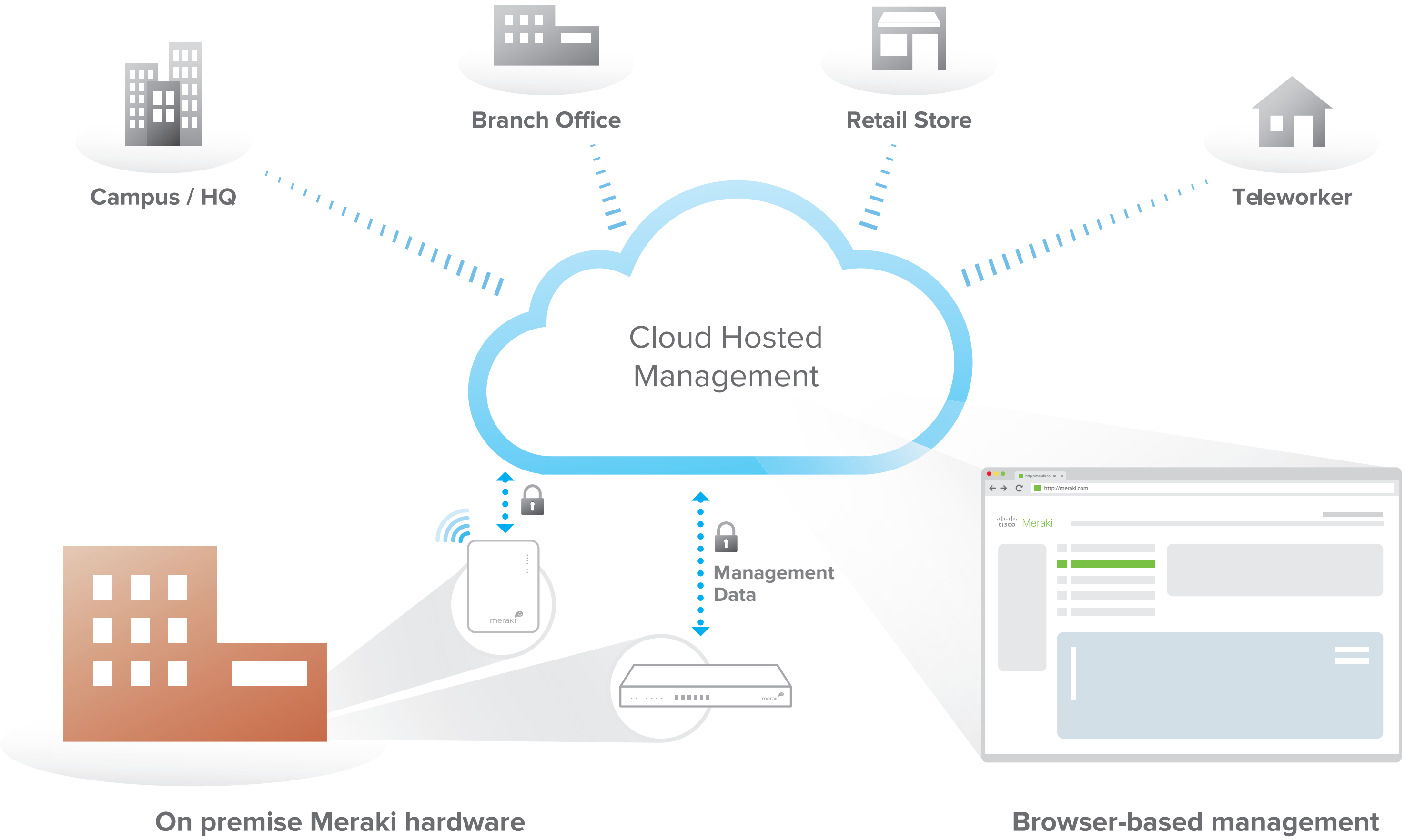
Meraki's architecture provides feature rich network management without on-site management appliances or WiFi controllers.

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.

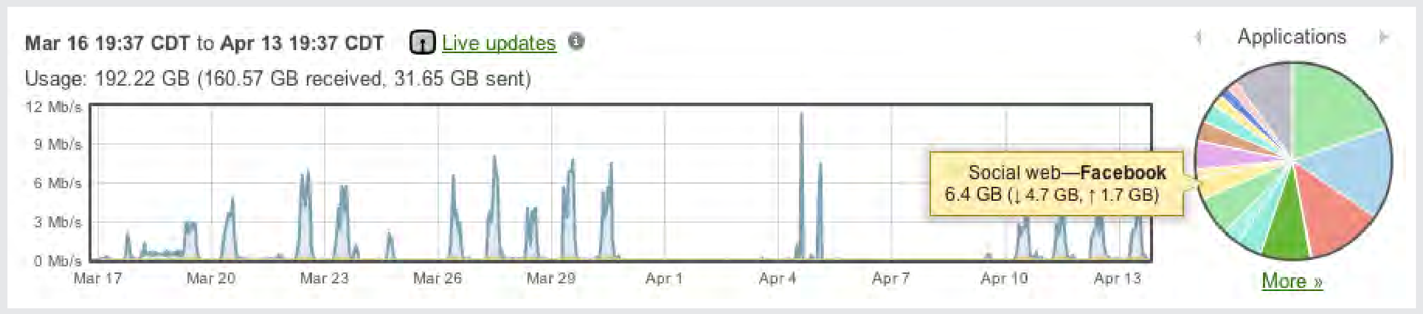
Meraki's cloud platform is designed to spread computation and storage across independent server clusters in geographically isolated datacenters. Any server or datacenter can fail without affecting customers or the rest of the system. Additionally, Meraki's datacenter design is field proven to support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

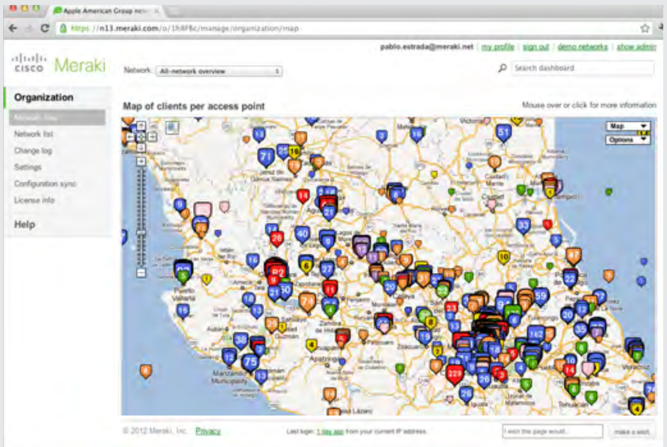


Mar 16 19:37 CDT to Apr 13 19:37 CDT

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

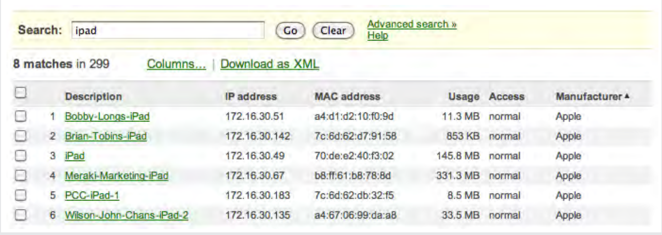
Social web—**Facebook**
6.4 GB (↓ 4.7 GB, ↑ 1.7 GB)

Layer 7 application visibility



Apple American Group
https://n13.meraki.com/o/1h8F8c/manage/organization/map
pablo.estrada@meraki.net | my profile | sign out | demo networks | show admin
cisco Meraki
Network: All-network overview
Search dashboard
Organization
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

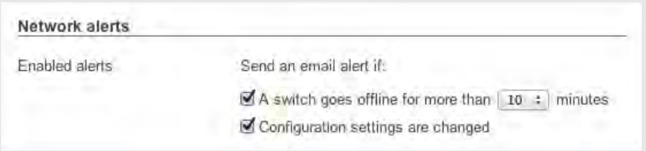


Search: ipad [Go] [Clear] Advanced search » Help

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

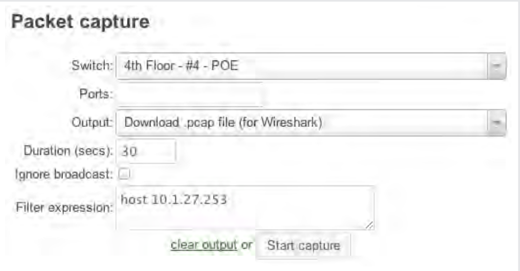
Enabled alerts

Send an email alert if:

☑ A switch goes offline for more than 10 minutes

☑ Configuration settings are changed

Automatic E-mail Alerts



Packet capture

Switch: 4th Floor - #4 - POE

Ports:

Output: Download .pcap file (for Wireshark)

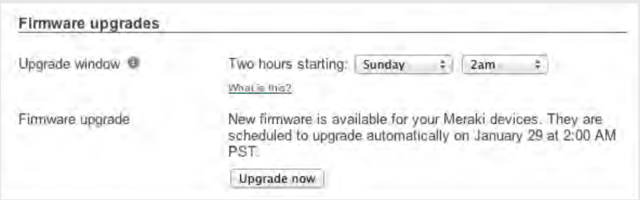
Duration (secs): 30

Ignore broadcast: □

Filter expression: host 10.1.27.253

clear output or [Start capture]

Live Troubleshooting Tools



Firmware upgrades

Upgrade window: Two hours starting: Sunday 2am

What is this?

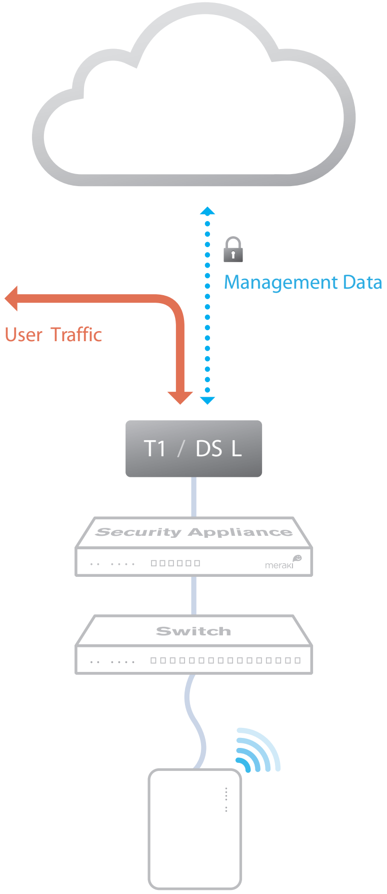
Firmware upgrade: New firmware is available for your Meraki devices. They are scheduled to upgrade automatically on January 29 at 2:00 AM PST.

[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

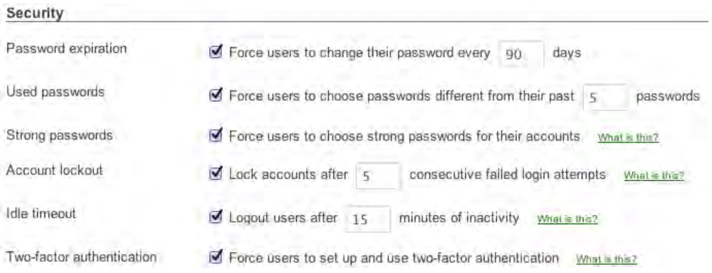
Meraki logs the time, IP, and approximate location (city, state) of logged in administrators. A searchable configuration change log indicates what configuration changes were made, who they were made by, and which part of the organization the change occurred in.

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

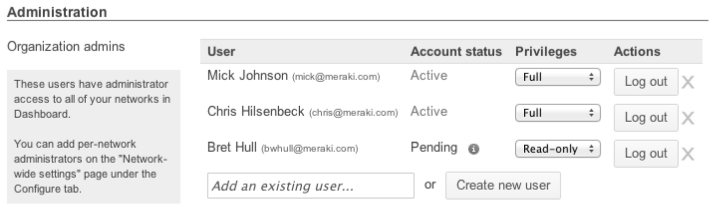
30 seconds before being logged out, users are shown a notice that allows them to extend their session. Once time expires, users are asked to log in again.



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

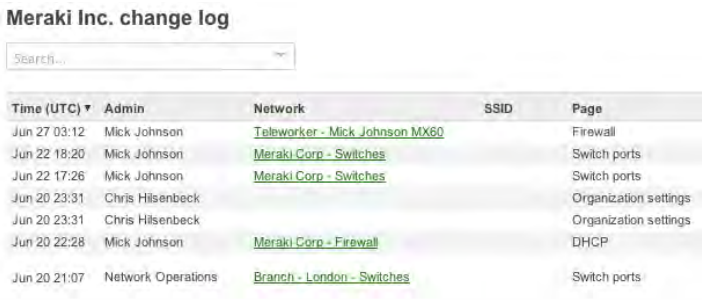
These users have administrator access to all of your networks in Dashboard.

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

Create a Collaborative and Productive Web Meeting Experience

Cisco WebEx Meetings
Product Overview

Cisco WebEx Meetings Highlights:

- Create a richer, more productive web meeting experience with high-definition video, integrated audio, and real-time content sharing
- Make meetings more efficient by sharing documents, agendas, and recordings in a convenient and accessible online meeting space
- Allow team members to collaborate easily using their mobile devices, including two-way video
- Enforce security with strict policy and access controls built into the Cisco WebEx cloud

Cisco WebEx® Meetings accelerates business results by making your web meetings more productive. This people-centric collaboration solution can enable team members to easily share information through any computer or mobile device. WebEx Meetings allows people to attend meetings any time, from anywhere, inside and outside corporate firewalls.

Teams can collaborate more effectively with a virtual meeting incorporating audio, high-definition (HD) video, and real-time content sharing. WebEx Meetings also helps you reduce email clutter and streamline the entire meeting process by providing a highly secure, centralized online space for organizing and sharing all meeting-related activities and information.

WebEx Meetings is a software-as-a-service (SaaS) solution delivered through the Cisco WebEx cloud—a highly available and secure service delivery platform with unmatched performance, integration flexibility, and enterprise-grade security.

A Web Meeting Experience That Facilitates the Best Collaboration

Deliver presentations, discuss ideas, and brainstorm with remote colleagues and virtual project teams. Share content and use integrated audio and HD video to meet online with participants from multiple locations as easily as if you were face-to-face.

Use Meeting Spaces to Streamline Meeting Activities

Managing meeting activities and content is time-consuming and can reduce team efficiency and productivity. WebEx Meetings automatically creates dedicated meeting spaces that help streamline tasks and facilitate easy content sharing. Keep agendas, participant lists, and related documents in one convenient location. Use integrated instant messaging capabilities to reach coworkers and chat. After the meeting ends, using meeting spaces can help sustain momentum and keep information such as recordings and actions synchronized. Use integrated file sharing capabilities to manage documents.

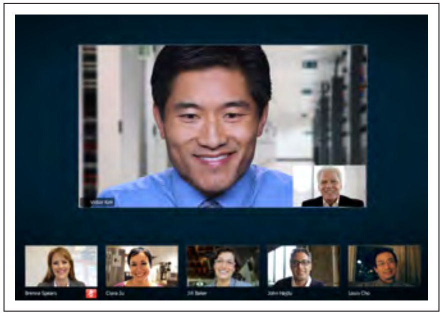
Cisco webex

Conduct Highly Effective Meetings with Powerful Features

Rich, Interactive Meetings

- **File, application, and desktop sharing:** Easily collaborate on any project by sharing content online in real time.
- **Video:** View the exceptionally crisp and clear HD video of the Active Speaker with up to 720p screen resolution. See up to seven simultaneous webcam video feeds with voice-activated switching.

Figure 1. View of full-screen mode

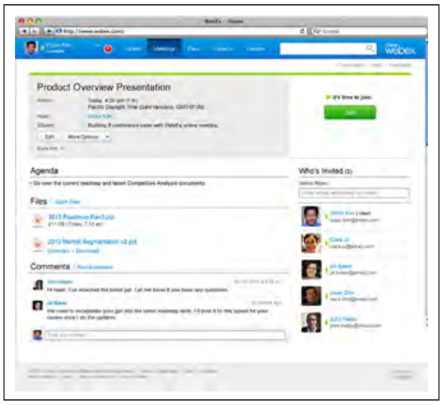


- **Comprehensive multimedia experience:** Share video files in real time and incorporate multimedia into presentations.
- **Integrated voice conferencing:** Choose toll or toll-free with call-in or call-back or voice over IP calling.

Streamline the Entire Meeting Process with Meeting Spaces

- **Persistent, centralized meeting spaces:** Share agendas, documents, meeting notes, action items, and recordings before, during, and after the meeting.
- **Document library and file sharing:** Manage files in folders, with version control, comments, and indexed searches for all content.
- **Access a full array of WebEx collaboration solutions:** Easily link to Cisco WebEx Training Center, Cisco WebEx Event Center®, and Cisco WebEx Support Center.

Figure 2. Meeting Spaces help streamline all meeting activities and facilitate content sharing



Meet Online on Any Device

- **Mobile meetings:** Attend meetings on an iPhone, Android, iPad, and other wireless or 3G and 4G mobile phone and tablet devices.
- **Cross-platform support for Windows, Macintosh, and Linux.**
- **Network-based recording:** Record meetings with session content and audio.

Map to Everyday Processes and Protect Investments

- **Desktop integration:** Initiate meetings instantly from Microsoft Office, Microsoft Outlook, and a variety of integrated instant messaging solutions.
- **Easy to administer and maintain:** Manage users and enforce corporate policy controls with a single identity across services for each user.
- **API integrations:** Easily integrate existing applications with WebEx Meetings using open APIs.

Highly Secure, Reliable Access Anywhere, Anytime

- **Data privacy and security safeguards:** WebEx Meetings offers a variety of security options–from meeting password protection, through Single-sign on (SSO), end-to-end data encryption, and strict network and data center security to ensure the highest levels of privacy and data integrity.
- **Reliability and performance:** Cisco WebEx cloud uses highly secure data centers located strategically near major Internet access points worldwide, routing data, audio, and video on dedicated, high-bandwidth fiber, to eliminate lag time and interruptions.

To learn more about WebEx Meetings and other Cisco WebEx solutions, visit www.cisco.com/go/web-conferencing or www.webex.com. To speak with a solution specialist, call 1.877.GOWebEx (469.3239).

Languages supported in the current version: English, French, German, Brazilian Portuguese, Spanish (Latin American Spanish on all supported platforms and European Spanish on Windows and mobile platforms), Traditional Chinese, Simplified Chinese, Japanese, Korean, Italian, Russian, and Dutch.