



Solution Guide

# Managing Large-Scale Network Deployments

**NOVEMBER 2013**

This document discusses the Cisco Meraki architecture, and how MSPs and organizations with distributed networks can leverage Meraki to quickly and easily implement networking solutions for their enterprises.

# Table of Contents

<b>Introduction</b>	3
<b>Meraki Dashboard Structure</b>	4
<b>Organizing Network Deployments</b>	6
1. Single Site Network Infrastructure	
2. Multi-Network Infrastructure	
3. Multi-Network Infrastructure Across Standardized Sites	
<b>Dashboard for Managed Service Providers</b>	11
1. Hotspot Infrastructure Model	
2. Single Organization Model	
3. Multiple Organization Model	
4. Hybrid Organization Model	
<b>Conclusion</b>	17

Copyright

© 2013 Cisco Systems, Inc. All rights reserved

Trademarks

Meraki® is a registered trademark of Cisco Systems, Inc.

# Introduction

Without increasing network resources, the strain of scaling network infrastructure requires that lean IT teams be capable of satisfying new network requirements that range from guest wireless access and teleworker connectivity to mission-critical site buildouts, BYOD initiatives, and corporate network fabrics. Successful IT organizations will naturally adopt technologies and practices which enable them to automatically deploy and manage networks that a decade ago wouldn't even have existed. Their adoption of new technologies enable them to thrive by migrating "up the value chain" and providing analytics and business services layered on top of the infrastructure that has dominated the IT management landscape for the past decade.

Managed service providers (MSPs) and telecom carriers have an even larger challenge. Centralized network operations center (NOC) teams must deploy, configure, monitor, and manage a networking estate that spans a globally expanding, distributed customer base. Their success and profitability depends on how their technology platforms scale to meet requirements and demands, and how well they adapt their management procedures to scale alongside that technology.

The Meraki cloud platform provides feature-rich network configuration, monitoring, and management which scales out-of-the-box to seamlessly enable the rollout of small, ten device networks up to massive, multi-customer, cross-vertical, distributed site deployments of global managed service providers with millions of annual network users.

By using the Meraki dashboard to centrally deploy and administer network devices, IT departments, network managers, and service providers can easily monitor and manage multi-tenant, large-scale network deployments that meet current and future network demand.

# Structure of Devices Within the Meraki Dashboard

Meraki network devices are monitored and managed by administrators who organize devices into organizations and networks. Within the dashboard, organizations and networks provide a simple way to organize devices for efficient monitoring and management. As Figure 1 illustrates, organizations contain one or more networks, and networks contain devices (e.g., access points (APs), switches, security appliances).

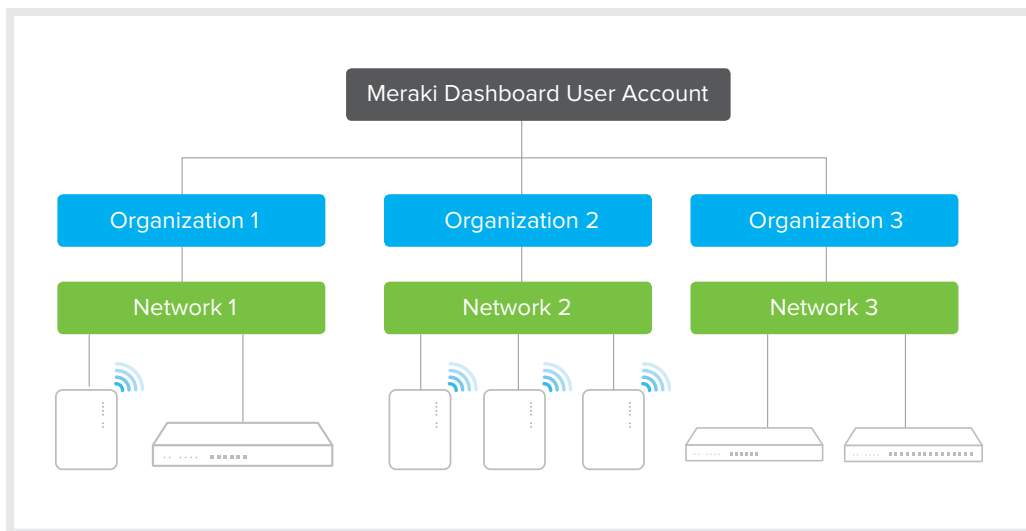


Figure 1 - The Cisco Meraki dashboard organizes devices within organizations, which contain networks

A Meraki dashboard network centralizes common configuration settings that apply across the devices within it, and each network can have administrators specifically assigned to it. Usually, dashboard networks correspond to physical networks or sites (i.e., a retail location, hotel, or office). For example, Figure 2 shows portions of the map and campus views of the single Westmont Santa Barbara College Campus network.

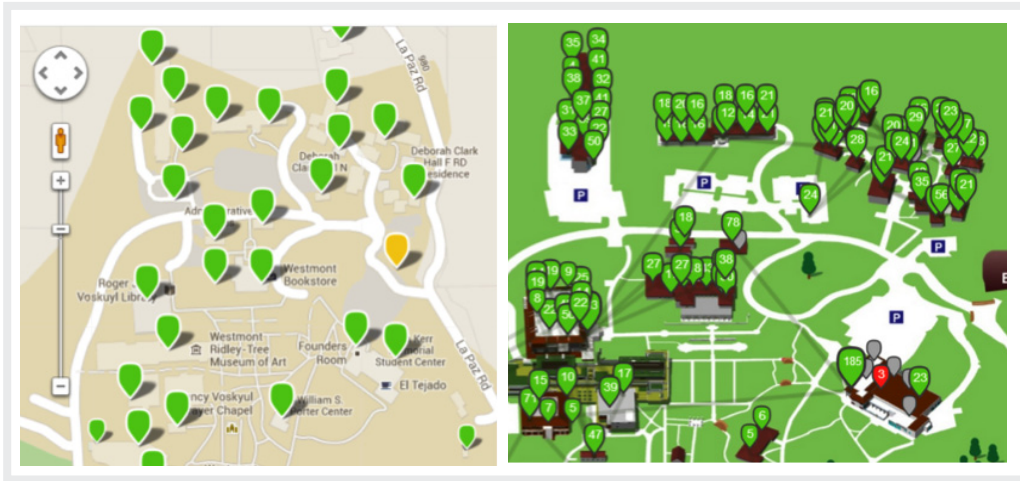


Figure 2 - The Westmont Santa Barbara College Campus network illustrates how individual networks can have multiple map views and/or floorplans configured within the Meraki dashboard

A dashboard organization contains one or more dashboard networks (i.e., networks are children of organizations). Each organization can have administrators and security settings assigned to it that apply to all of the Networks within that organization. For example, Figure 3 shows the Motel 6 organization, which contains 637 individual networks that each correspond to individual hotels across the United States.

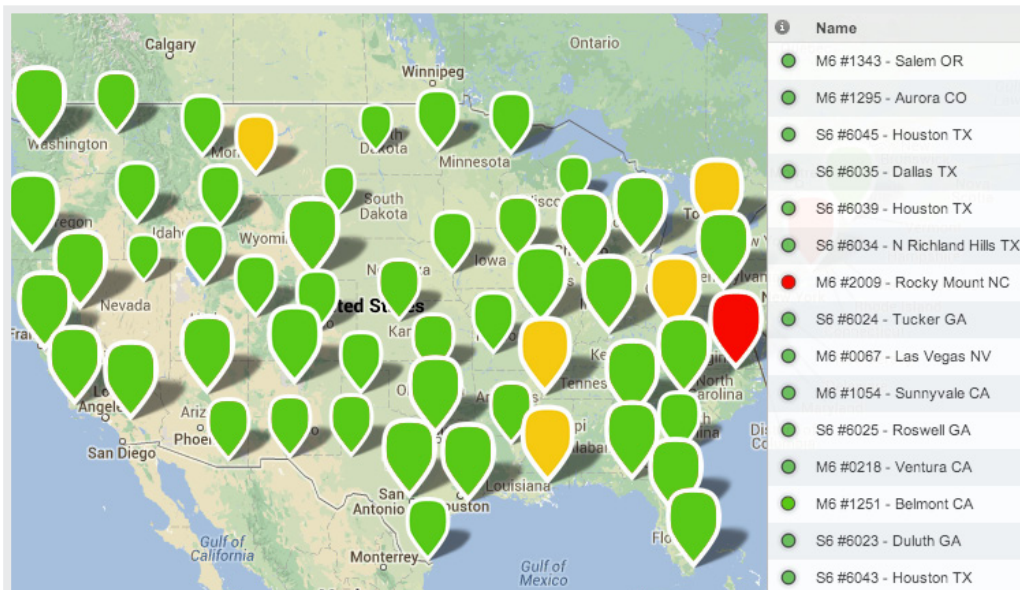


Figure 3 -The Motel 6 Meraki dashboard organization contains hundreds of individual networks, each of which groups APs at an individual hotel.

# Organizing Network Deployments

## 1. Single Site Network Infrastructure

### EXAMPLE DEPLOYMENTS:

- Small office
- Single site healthcare facilities
- Libraries
- Public spaces
- Mall, hotel/inn, event venues

The simplest Meraki deployments involve a single site that may contain any combination of wireless access points, switches, and a single security appliance. In this case, it is natural to organize the Meraki dashboard using one organization containing a single network for the types of devices being used.

The MIT Computer Science and Artificial Intelligence Lab (CSAIL) is an example of a single-site deployment. As Figure 4 shows, within the Meraki dashboard there is an MIT CSAIL organization and a single MIT CSAIL network which contains all of the access points in the building. Within the MIT CSAIL network there are multiple floorplans uploaded, and all of the network's access points are placed onto their relevant floors.

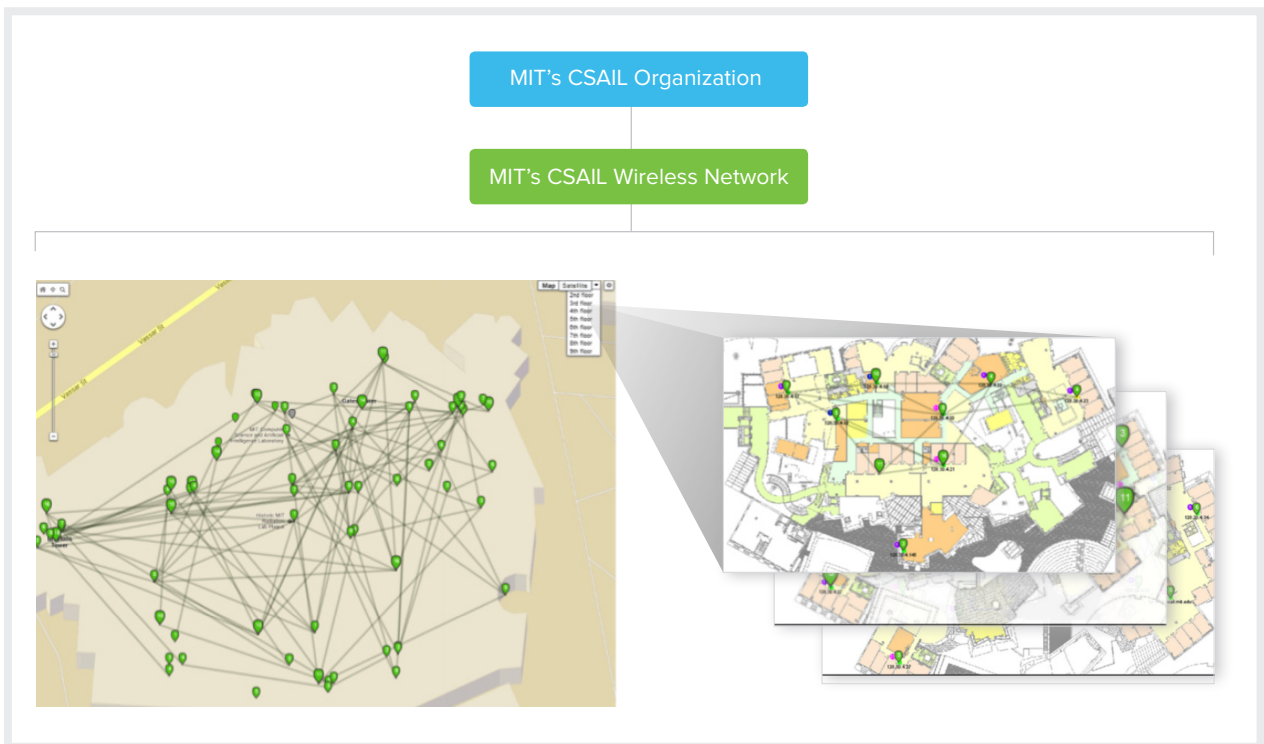


Figure 4 - MIT's CSAIL campus uses a single organization and network to manage its wireless infrastructure

## 2. Multi-Network Infrastructure

### EXAMPLE DEPLOYMENTS

- Multi-site enterprises/office networks (teleworker, HQ, branch offices)
- Large education campuses (e.g., high school, elementary, gym, cafeteria)
- Public city/town deployments (e.g., multiple parks)

As more sites are added to a network, there are multiple options for how to scale your dashboard organization. The easiest of these options is to continue to add devices within a network that already exists. In the prior example, this might involve adding access points elsewhere on campus into the MIT CSAIL Wireless Network. Many Meraki customers scale large network infrastructures this way, with thousands of physical devices controlled centrally from a single dashboard network.

### Scaling with multiple dashboard networks

Within a single network, network-wide settings (e.g., firewall rules and traffic shaping policies) and administrators are the same. If this is not desired for multiple network sites, administrators of a dashboard organization can create multiple networks within that organization, each with its own set of policies, administrators, and settings.

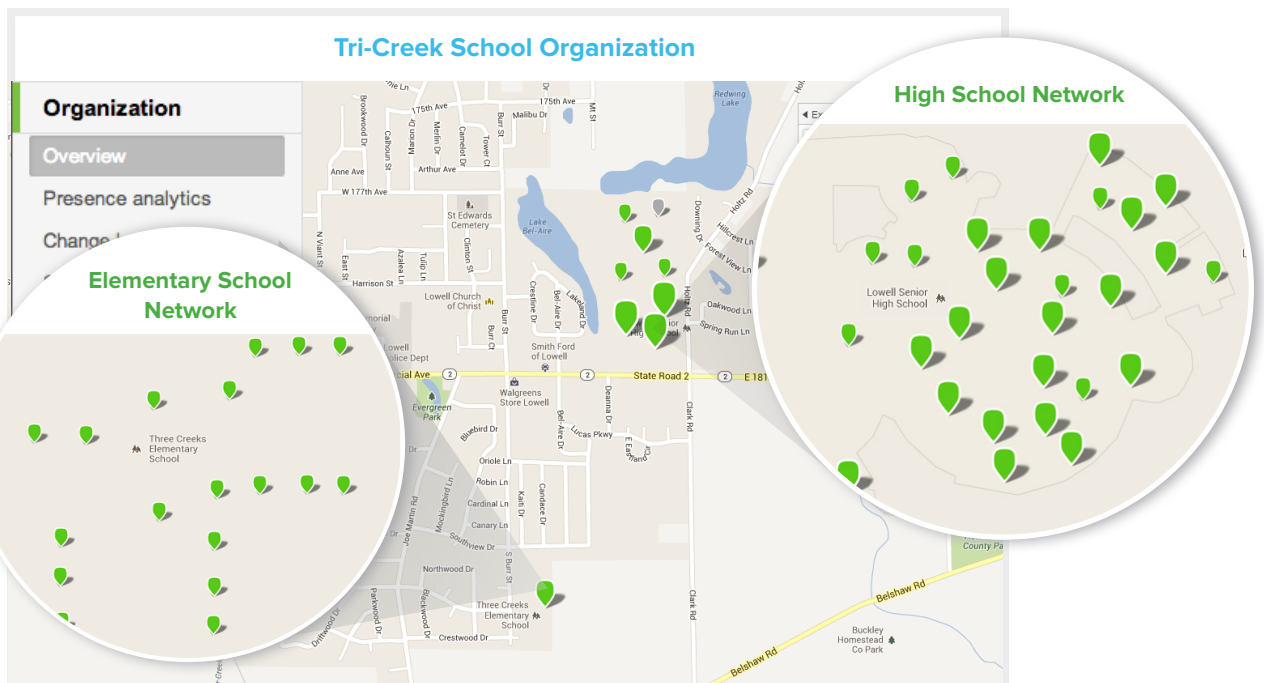


Figure 5 - The Tri-Creek School District separates school deployments across multiple networks within its dashboard organization

Tri-Creek administrators configured distinct dashboard networks with policies and network administrators specific to each of their sites. For example, their HS (High School) network has multiple student SSIDs (HS Tier 1 through HS Tier 4) and an HS Guest SSID, while their MS (Middle School) network has two student SSIDs and a Guest SSID with different bandwidth limits than for the High School. They also created a Systems Manager network in their organization, which uses the Meraki free mobile device management (MDM) platform to track over 3000 student and faculty devices.



### 3. Multi-Network Infrastructure Across Replicated Sites

#### EXAMPLE DEPLOYMENTS

- Distributed Retail Chains (including centralized data centers)
- Distributed Hospitality Enterprises / Brands
- Franchises
- Healthcare Chains

Massive, distributed networks with large-scale replication across many sites present administrators with unique challenges for new site deployments, configuration, and central management. It is common to require, for each site, similar but slightly different policies and administrators. For example, large retail chains may want local store management to manage per-store guest authentication access and regional management to dictate specific 802.1X or WPA2 access policies for guests or employees; similarly, a healthcare provider's IT department might want switches at individual clinics to use different management VLANs or port schedules.

In these cases, dashboard organization administrators configure each site as a new network within their organization as described above, but use the Meraki dashboard's Config Sync toolset to easily stand up new sites and manage common configuration settings across networks. Commonly, organization administrators maintain a "template" network which is used to synchronize default configuration settings across new sites and which can then be modified according to each site's individual requirements.

A&W Food Brands uses Meraki to provide wireless access to over 300 retail locations across Canada in this model.

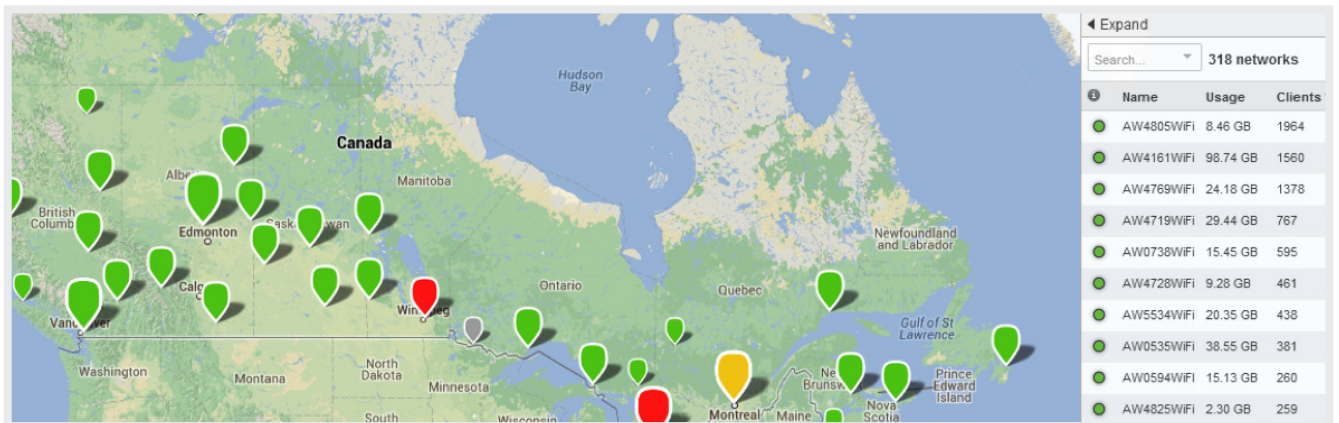


Figure 6 - A&W Food Brands uses the Meraki dashboard's 'Config Sync' and tagging to easily manage common configurations across hundreds of sites



A&W maintains a single account with organization access, and individual store representatives and food providers are assigned read-only access to individual groups of stores.

**A&W Food Services of Canada Inc. administrators**

Search admins... Add admin

Name	Email address	Privilege	Account status	Last login	Actions
AW Admin	admin@aw.ca	Organization	Ok	Fri, Aug 9 2013, at 16:50	Revoke Log out Become
Sonia	sonia@meraki.com	AW1540WFi (Read) AW1307WFi (Read) AW1551WFi (Read) AW1361WFi (Read) AW1554WFi (Read) AW1370WFi (Read) AW1557WFi (Read) AW1349WFi (Read) AW1222WFi (Read) AW1290WFi (Read) AW1495WFi (Read) AW1275WFi (Read) AW1099WFi (Read) AW1095WFi (Read) AW1400WFi (Read) AW1243WFi (Read) AW1550WFi (Read) AW1493WFi (Read)	Ok	Thu, Aug 8 2013, at 17:42	Revoke Log out Become
Thomas	thomas@meraki.com	AW4728WFi AW4825WFi AW4769WFi AW4814WFi AW4356WFi AW4551WFi AW4792WFi AW4372WFi AW4769WFi AW4577WFi AW4811WFi AW4805WFi AW4396WFi	Ok	Fri, Jul 26 2013, at 18:40	Revoke Log out Become
		AW4162WFi (Read) AW4162WFi (Read) AW4589WFi (Read) AW4719WFi (Read) AW4161WFi (Read) AW4369WFi AW4399WFi (Read) AW4107WFi (Read)	Ok	Never	Revoke Log out Become

Figure 7-The dashboard's Administrator management portal enables quick and easy management of dashboard administrators across networks

Using Configuration Sync within dashboard, A&W's organization administrator can easily stand up new sites by selecting those sites and syncing the desired settings, as shown in Figure 8.

**Configuration sync**

Compare your networks, see what settings differ, and maintain consistency when disparity exists.

**Info** Hold down the Ctrl or ⌘ key to select multiple target networks.

Source network: AW0000WiFi Target network: AW0218WiFi x AW0219WiFi x AW4814WiFi x

Category	Source	Target	Comparison	Action
<b>SSID-wide settings</b>	-	-	3 different	
SSID 1	AW0000WiFi	-	3 different	Copy
SSID 2	sample secure wireless LAN	-	2 same, 1 different	Copy
SSID 3	sample billing network	-	3 same	
<b>Network-wide settings</b>	-	-	3 different	
Enabled SSIDs	-	-	2 same, 1 different	Copy
Whitelist & blocked devices	-	-	3 different	Copy
Network Alerts	-	-	3 same	
<b>Other settings</b>	-	-	3 different	Copy

Figure 8-Configuration Sync allows sharing and management of configurations across network sites

For large device deployments within individual networks, devices can be named appropriately (e.g., by floor and location, 4-A2, 5-B1, etc.) and/or tagged (e.g., “lobby”, “cafeteria”) to create quickly searchable and reportable groups of devices.

<input type="checkbox"/>		Name	Usage ▼	Clients	Tags	Network type	Network health
<input type="checkbox"/>		AW6503WIFI	65.13 GB	29	MktgPromo	wireless	
<input type="checkbox"/>		AW5542WIFI	55.74 GB	329	New-DriveThru	wireless	
<input type="checkbox"/>		AW4161WIFI	50.40 GB	1516	Mall	wireless	
<input type="checkbox"/>		AW4719WIFI	37.32 GB	1010	MktgPromo	wireless	
<input type="checkbox"/>		AW0521WIFI	30.31 GB	105	MktgPromo	wireless	
<input type="checkbox"/>		AW0594WIFI	29.72 GB	113	MallCanada	wireless	
<input type="checkbox"/>		AW5332WIFI	27.82 GB	80	New-DriveThru	wireless	

Figure 9-Network tags allow administrators to quickly group, search, and configure distributed network infrastructure

# Meraki Dashboard for Managed Service Providers (MSP)

IT departments are increasingly looking to offload network deployment, monitoring, and management to a trusted partner. Going beyond networking design and installation, managed service providers (MSPs) are delivering networks as a service: ongoing monitoring, configuring, and troubleshooting is handled by the service provider. End customers are able to treat their network as a utility, and MSPs can capitalize on recurring revenue opportunities derived from value-added services.

The Meraki architecture's built-in scalability, centralized management, and zero-touch provisioning makes it an ideal platform for MSPs to increase operational efficiency and profitability by leveraging the cloud to monitor, configure, and troubleshoot remote branch and campus network infrastructure.

Given the uniquely large, distributed, and multi-tenant requirements of MSPs and their network operations centers (NOCs), MSPs can use multiple deployment models when organizing devices and customer networks within the Meraki Dashboard.

1. A distributed hotspot infrastructure
2. A single dashboard organization for all customers
3. A unique dashboard organization per customer
4. A shared dashboard organization for smaller customers, and unique dashboard organizations for larger customers

Which of these models/structures to use will depend on multiple factors, including the licensing and financial business model of an MSP with its end customers, whether Meraki AutoVPN technology is provided by an MSP for site-to-site connectivity, and the expected volume of enterprises in an MSPs target market. Meraki account managers and engineers can assist with the evaluation of these factors during MSP NOC training and pilot customer proof of concept (POC) phases.

## MODEL 1: Service Provider Hotspot Infrastructure

Service providers can use Meraki to provide global, national, or regional wireless hotspot infrastructure. These hotspots can be owned and operated strictly by the provider, or provided by fee to vendor locations like coffee shops, malls, and airports. In either case, Meraki enables easy integration with back end CRM and subscriber systems (for example, to provide existing cable or telephone subscribers with free internet service) and provider billing systems to support pay-for-wireless models (see [Captive Portal Solution Guide](#) for more details).

These deployments are managed by service providers with a single Dashboard organization and multiple networks. When deploying large numbers of access points which all support a common hotspot, granularity of network settings and administrators across individual networks within Dashboard isn't commonly necessary. In these cases, providers use networks to conveniently group access points, but don't create a network for each physical location.

For example, as Figure 10 shows, a hotspot service provider across Mexico manages several thousand access points with about 100 distinct networks created in Dashboard.

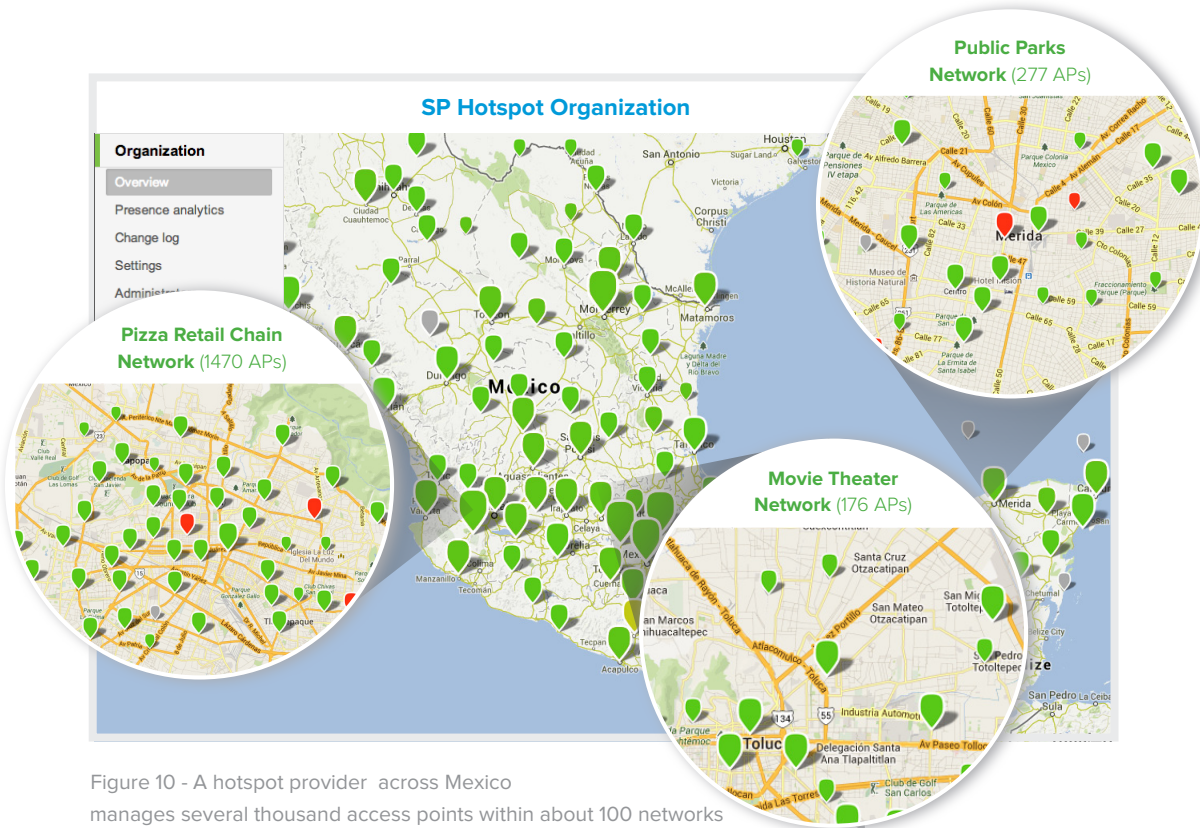


Figure 10 - A hotspot provider across Mexico manages several thousand access points within about 100 networks

Meraki has built a feature set designed to enable Service Providers to quickly and easily deploy massive, distributed networking infrastructure to support public wireless hotspot services. In the above example, the Service Provider's hotspot supports 500,000 individual weekly clients who transfer 30+ TB. And because access points can be easily added into existing or new networks in the SP Dashboard organization, growth of the hotspot footprint does not require skilled engineering labor.

## Model 2: Single Organization

The simplest way for Managed Service Providers to manage the networks of multiple customers using the Meraki dashboard is to use a single organization, and create multiple networks for each end customer network that will be managed. Customer devices may be contained within a single network (see p. 6), or in multiple networks (see p. 8). If customer devices are contained within multiple networks, MSPs should use tags to group those networks together for reporting and searching purposes.

Skool Automatisering (“Skool Automation”) is a Dutch managed service provider that uses Meraki to provide wireless access to schools across western Europe. Headquartered in Holland, Skool installed and manages the network infrastructure for over 1300 school districts in Holland, Germany, and Belgium.

Skool creates each new school or district customer as a new network within their dashboard organization. In this way, their dashboard is structured similarly to A&W Food Brands (see p. 8), though each Dashboard network for Skool is a large school/district deployment rather than a deployment at a single retail store.

Using Config Sync and a template network, Skool can easily deploy sites for new schools by creating a new network and syncing standard network settings to it. Skool organization admins can also assign network administrators for each customer to have read-only access to their own infrastructures.

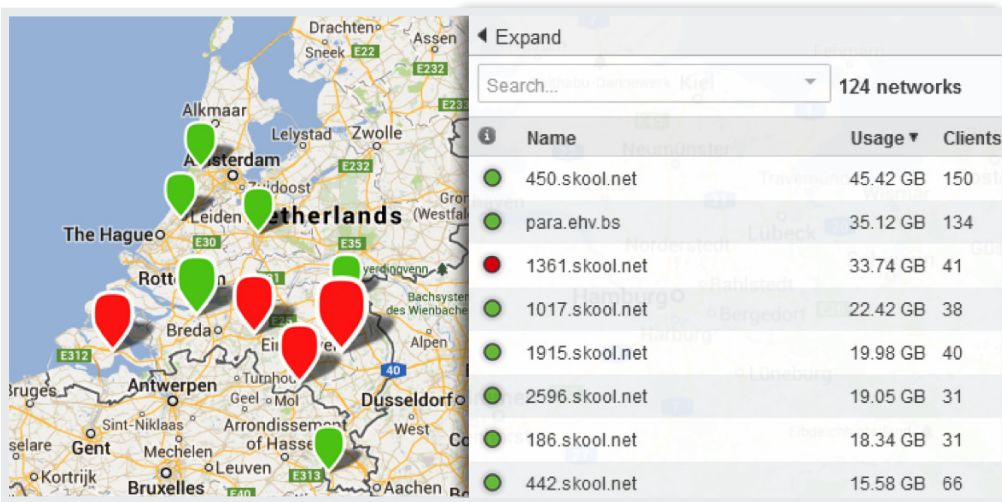


Figure 11 - Using a single dashboard organization, Skool provides managed network services to schools across the Netherlands

### MODEL 3: Multiple Organizations

Meraki has specifically built an MSP Portal that enables MSPs to manage customers with infrastructures separated into distinct Dashboard organizations. This portal provides MSP NOCs with visibility across and quick access into multiple organizations.

Giving each end customer its own Dashboard organization may be desirable for licensing reasons, when the end customer has many networks, or for certain customer site-to-site VPN deployments.

FullyManaged is an MSP that provides IT support, consulting, and managed services to healthcare, education, and SMBs across Canada. They use Meraki security appliances and wireless access points to provide organizations customers with edge gateways, WiFi, threat management, and site-to-site VPN connectivity.

In order to provide customers with individual mesh networks using Meraki's AutoVPN technology, Fully Managed creates a new Dashboard organization for each new customer as shown in Figure 12. For each customer organization, they create a network for each security appliance, and a network for wireless, if they are deploying access points for that customer.

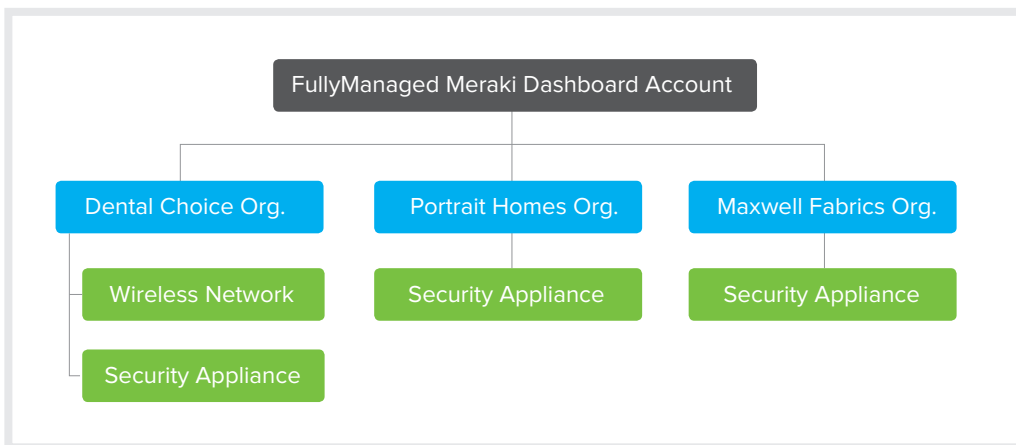


Figure 12 - Fully Managed creates a new dashboard organization for each of its customers

*For MSPs taking over the management of Meraki devices and licenses owned by individual customers, this option — maintaining customer devices and licenses independent and in separate organizations — is likely the best.*



Using Meraki's MSP Portal, Fully Managed's NOC can centrally monitor the status of devices, licenses, and support tickets for each of its customer organizations. In order to deploy new customer networks, Fully Managed can easily create a new Dashboard organization for that customer, add networks and devices to that organization depending on the service that customer purchased, and monitor those customer devices centrally with the MSP Portal.

The MSP Portal (shown in Figure 13) is enabled in Dashboard automatically for any dashboard account with access to multiple organizations. It can be accessed from the Organizations drop-down in the top-left of dashboard.

The screenshot shows the Meraki MSP Portal interface. On the left is a navigation menu with 'Monitor', 'Configure', 'Organization', and 'Help'. The main area is titled 'Organization summaries' and contains a table with columns for Organization, Tickets, License Status, Networks, and Devices. The table lists several organizations, with 'Maxwell Fabrics' highlighted in red due to a 'PROBLEM' license status. Other organizations have 'OK' license statuses. The 'Devices' column shows counts for different device types using colored circles (green, yellow, red).

Organization	Tickets	License Status	Networks	Devices
Dental Choice	0	OK	16	16 (0 Green, 0 Yellow, 0 Red)
Portrait Homes	0	OK	7	15 (0 Green, 0 Yellow, 0 Red)
Maxwell Fabrics	0	PROBLEM	6	10 (0 Green, 0 Yellow, 0 Red)
Urban Home Services LLC	0	OK	5	8 (0 Green, 0 Yellow, 0 Red)
City Harvest	0	OK	4	7 (0 Green, 0 Yellow, 0 Red)
Thompson Brothers Construction LLC	0	OK	4	1 (0 Green, 0 Yellow, 2 Red)
Shoreline Services	0	OK	4	5 (0 Green, 0 Yellow, 0 Red)
Shoreline Golf and Country Club	0	OK	3	5 (0 Green, 0 Yellow, 0 Red)
Frank Architecture	0	OK	3	4 (0 Green, 0 Yellow, 1 Red)

Figure 13 - Using the MSP Portal, Fully Managed can monitor the device, license, and support status for each of its customer organizations



#### Model 4: Hybrid Organization Model

MSPs with many smaller customers (e.g. SMB deployments) can optimize their Dashboard organizations by using a single, shared organization for lots of smaller customers, and create independent organizations only for large accounts that justify independent management of device licensing and Dashboard footprints. By using a shared organization (as in the prior Skool example) for lots of smaller customers and single organizations for larger enterprises, MSPs maintain a manageable number of license renewals and can intuitively separate large customers from mass SMB deployments.

For example, ADP Dealer Services provides integrated technology solutions and services to over 26,500 vehicle dealerships throughout North America. Its GetWireless service uses Cisco Meraki devices to offer auto dealerships WiFi which integrates into their existing networks and additional ADP dealership solutions and services.

To manage their large and small dealership customers, they use a Hybrid Organization Model within Dashboard. For smaller customers who don't want to configure site-to-site VPN, ADP creates networks within a shared organization. For customers who need VPN-connectivity or who had pre-existing Meraki installations which ADP is managing, ADP manages separate Dashboard organizations for each.

Using this separation, ADP can conveniently manage lots of small customers with a single Meraki Dashboard and license co-termination date, but keep its large-scale enterprise customer deployments separate, as Figure 14 shows.

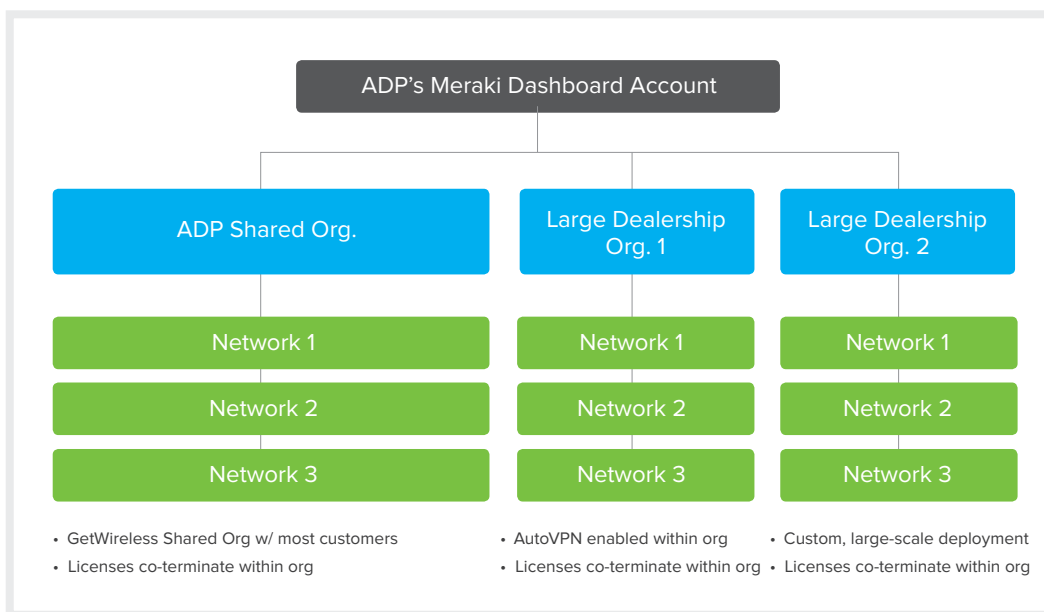


Figure 14 - ADP administrators manage customer networks that are organized within individual dashboard organizations and a shared ADP dashboard organization.

## Conclusion

Service providers, network administrators, and CIOs all face the challenge of managing growing network infrastructure with limited network resources. Managing multi-customer, large-scale network infrastructures is complicated and can be overwhelming without cloud-managed network technology that is designed for centralized administration.

Using the Meraki dashboard, network administrators can achieve unparalleled flexibility for single site, multi-site, and multi-customer network environments. Organizations, networks, and tags allow network operators to centrally monitor and manage tens of thousands of network devices which collectively serve millions of clients. These tools enable low-cost deployment of new devices and ensure that service providers can maximize profitability while IT organizations can deliver results that span technology strategy and business intelligence.

Cisco Meraki is passionate about enabling IT organizations by delivering scalable, simple technology. Consistent development of new features requested by our customers allows agility capable of satisfying new, large-scale network management requirements — but ultimately, each business model and architecture is different. Please contact your account manager or Cisco Meraki engineers to discuss the architectural best practices and dashboard configurations which are ideal for your enterprise.