



Meraki White Paper: Wireless Guest Access at the Office

Version 2.0, March 2009

This document discusses what is required to provide secure and effective wireless guest access in a corporate environment and how Meraki can be used to satisfy these requirements. This publication is for corporate IT administrators who are responsible for the design and implementation of a wireless network. For an overview and manual, please visit the Meraki website.

Copyright

© 2009 Meraki, Inc. All rights reserved.

Trademarks

Meraki® is a registered trademark of Meraki, Inc.



www.meraki.com

660 Alabama St.
San Francisco, California 94110

Phone: +1 415 632 5800

Fax: +1 415 632 5899

Table of Contents

1. Why Guest Access?	4
2. Who Can Access the Guest Network?.....	5
2.1 Open	5
2.2 Pre-Shared Key (PSK)	5
2.3 Username and Password	6
2.4 Hiding the VAP	6
2.5 Whitelisting/Blacklisting by MAC.....	6
2.6 Authentication Options with Meraki	7
3. What Can Guests Access?	8
3.1 Security	8
3.2 Compliance	8
3.3 Splash Pages, Captive Portals, and Walled Gardens	8
4. How Much Bandwidth Do Guests Get?	10
5. How Is Guest Access Managed?	11
5.1 Account Management	11
5.2 Network Management.....	11
6. Providing Guest Access with Meraki	12

1 Why Guest Access?

Internet connectivity has made it to the list of mandatory guest amenities in offices, hotels, and other public spaces. With the growth in the number, importance, and pervasiveness of Internet applications—from hosted services like SalesForce.com, to FaceBook applications that run on iPhones—visitors no longer view Internet connectivity as a luxury; it is now a requirement. Providing wireless Internet access to customers, contractors, and other visitors can help improve customer satisfaction, increase brand loyalty, and enhance business productivity.

Three key issues must be considered when providing wireless guest access:

1. **Admission control** to ensure that only authorized guests are connecting to the wireless network.
2. **User permissions** to constrain the resources that guests can access while connected to the wireless network.
3. **Management** to configure and monitor the guest networks from a centralized interface.



This whitepaper discusses the various options available to address these issues. Careful planning that takes these factors into account will ensure that an organization provides a secure, reliable wireless experience for guests.

2 Who Can Access the Guest Network?

There are four methods for controlling access to a wireless network:

1. Open
2. Pre-shared keys (PSK)
3. Username and password
4. MAC address whitelisting/blacklisting

The subsequent sections discuss the advantages and disadvantages of each method.

2.1 Open

An open wireless network eliminates the need for time-consuming configuration on guest machines. Anyone can connect to an open network. The downside is that unwanted guests (e.g., neighboring businesses) can also connect to the open network freely. To address these concerns, certain features can be enabled to help ensure that only authorized guests can connect to the wireless network.

2.2 Pre-Shared Key (PSK)

A pre-shared key (PSK) is a shared secret that is used to encrypt and decrypt traffic sent between a client device and a wireless access point (AP). Only those users with the correct PSK can send and receive data. The key is “pre-shared” because it is statically configured before the client associates to the wireless network; the key is not negotiated as part of the association process.

Meraki supports two PSK encryption methods: WEP and WPA2-Personal. WEP encryption is an older method that is widely deployed in homes and small offices. WEP is not recommended because the key can become compromised by eavesdropping on a limited amount of wireless traffic. (Meraki offers WEP encryption as a convenience for existing networks with WEP encryption deployed.) WPA2-Personal is the preferred PSK method for Meraki networks.

An organization with only a few guests at any point in time may find that a PSK is sufficient for limiting usage of the guest network. However, as the number of guests on a network increases, it becomes more challenging to configure each guest device with the correct PSK, to ensure that the PSK does not leak out to unwanted users, and to change the PSK if it becomes compromised.

2.3 Username and Password

Individual user authentication provides more secure access control than either an open network (to which anyone can connect) or a PSK-encrypted network (to which anyone with the PSK can connect). User authentication is important if the organization has a shared device, such as a public internet kiosk, that different users might use.

The username and password can be obtained in one of two ways:

1. A splash page login (a web page displayed within the browser), or
2. 802.1x (an authentication protocol that runs when a wireless user attempts to associate).

For guest access, the splash page login is recommended because it requires no client-side configuration. The splash page simply displays within the guest user's browser, and the user is prompted to enter his credentials.

User credentials are then verified against a user database. Two different kinds of user databases can be configured:

1. A user database that is specific to wireless users, or
2. A user database that applies to all users, wired or wireless (e.g. an Active Directory or LDAP server).

2.4 Hiding the VAP

A virtual AP (VAP), also called a Service Set Identifier (SSID), is a logical wireless network that is advertised and supported by a physical AP. In practice, a VAP is the wireless network that a client device "discovers" when the device probes for wireless connectivity. A single physical wireless network can support multiple VAPs. When a VAP is hidden, the AP does not advertise the VAP to clients searching for available wireless networks. Therefore, only those guests that know about the guest VAP in advance can configure their wireless adapters to associate to it. In reality, software tools are available that enable clients to detect hidden VAPs by eavesdropping on the wireless conversations of other clients. Hiding a VAP makes it only slightly more difficult for unwanted guests to associate to the network.

2.5 Whitelisting/Blacklisting by MAC

To manage wireless access at the device level, devices can be whitelisted or blacklisted with the network according to their MAC addresses. However, this method is not recommended because (1) maintaining a list of MAC addresses for guests' devices is logistically difficult, and (2) MAC addresses can be spoofed easily, making MAC blacklisting relatively easy to thwart. Meraki networks permit the use of

MAC whitelisting/blacklisting primarily to allow temporary access. For instance, a client that is having difficulty authenticating to a wireless network can be whitelisted by its MAC address, so that the client can access the Internet while the IT team investigates the issue.

2.6 Authentication Options with Meraki

Meraki offers flexible authentication options, including the following:

- Creation of temporary guest credentials through a web interface
- Guest self-registration with a local web server
- Splash page login with splash page customization
- 802.1x authentication
- Hosted user database (built-in RADIUS)
- RADIUS integration with an on-premise Active Directory or LDAP server
- Hiding a VAP
- Whitelisting/blacklisting by MAC
- Per-VAP authentication settings (e.g., splash page login on the guest VAP, 802.1x on the employees VAP)

3 What Can Guests Access?

After identifying guests, an administrator needs to manage what guests can access with customized security and compliance policies. Splash pages, captive portals, and walled gardens are used to control a guest's initial interaction with the network.

3.1 Security

Guest and corporate data are traversing shared network resources—either through the same wireless APs, or through the same wired routers and switches. How does an administrator ensure that guests cannot access the corporate LAN? Meraki offers two options:

1. **LAN isolation:** When this feature is enabled on a VAP, wireless clients are not allowed to connect to any devices on the LAN to which the APs are connected. Instead, these clients obtain Internet-only access.
2. **VLAN tagging:** Distinguishing guest traffic from corporate traffic over the wired LAN can be achieved by mapping wireless VAPs to different wired VLANs. With this VAP-to-VLAN mapping, guest traffic can be tagged with an identifier, so that an upstream switch will send any traffic with that identifier straight to the firewall. In this manner, guests obtain only Internet access, even though their traffic is traversing the private network.

3.2 Compliance

Guests could violate a company's acceptable use policy if inappropriate content or prohibited applications are accessed over the guest network. To block inappropriate content, a content filtering solution can be used. Meraki offers DNS-based content filtering for wireless users. (However, it is likely that a content filtering solution for both wired and wireless users is required to consistently enforce an acceptable use policy. Moreover, there are techniques to circumvent DNS-based content filtering. Organizations with advanced content filtering requirements should invest in a dedicated content filtering solution.)


To block prohibited applications, the company's firewall should be configured to block all inbound connections (except to the company's public web server), as well as outbound connections on well-known ports that serve prohibited applications (e.g., BitTorrent).

3.3 Splash Pages, Captive Portals, and Walled Gardens

The splash page, the web page that prompts a guest user for credentials, can be used for more than just user authentication. A splash

page can be customized to present a unified branding experience to guests (e.g., the corporate logo and color scheme). The splash page can also be used to show the terms of service, which might include an acceptable use agreement, or a privacy statement.

Welcome to wifi



If you already have an account on this network, sign in here:

email

password

If you don't have an account yet, complete this form:

name

email

email (again)

password

password (again)

You will need to be on the list of authorized users for this network in order to access the Internet.

A splash page is an example of a captive portal, which forces a user to a particular web page until the user successfully authenticates. Whereas a splash page is a one-page captive portal, a walled garden is a multi-page captive portal, allowing an unauthenticated user to access any web pages served from a range of IP addresses. These pages can be used to provide background information about the company or the wireless service. A guest user can peruse the web pages within the walled garden until he is ready to log in; after authenticating, he gains Internet access beyond the walled garden.

Meraki has built-in splash page capabilities that enable administrators to host splash pages through Meraki, eliminating the need to set up local web servers. The network administrator may completely customize the splash page. Meraki also fully supports the walled garden to expand a captive portal with more pages of content.

4 How Much Bandwidth Do Guests Receive?

The final step in designing a guest access network is defining how much bandwidth guests can use. Guests are probably sharing an Internet connection with employees, so administrators need to ensure that guests cannot consume all of the available bandwidth or impede business-related traffic.

To limit bandwidth, administrators should be able to control (1) the number of guest users on the network, and (2) the bandwidth that guest users can obtain. The former is achieved by successful account management, discussed in earlier sections, and the latter by configuring bandwidth limits. An organization's router or firewall may support these bandwidth policies (e.g., for a particular IP subnet or VLAN). If not, the bandwidth policies may be configured directly in the wireless infrastructure.

Meraki offers integrated bandwidth shaping, with upload and download limits that can apply to all guests or to individual users.

5 How Is Guest Access Managed?

Guest access management should not be time-consuming. Meraki provides tools that make it easy to manage guest user accounts and guest networks.

5.1 Account Management

Administrators need to manage guest user accounts to ensure that arriving guests have access, and that departed guests do not.

In a single shared account (e.g., username “guest” and password “companywireless”), the guest account is configured once but used many times. However, like a PSK-encrypted network, it is prone to overuse as the credentials leak out over time. The administrator can rotate the credentials periodically to mitigate this effect.

Alternately, unique guest logins provide network access on a per-user basis. Management overhead for individual guest accounts can be high, especially with larger numbers of guests. Meraki allows administrators to configure guest user accounts that expire after a predefined period of time. This way, guests can be individually provisioned with access, but de-provisioning occurs on its own, when the guest user account expires.

5.2 Network Management

An organization with multiple locations—whether the locations are multiple buildings around a business park, or multiple buildings around the world—should seek a solution that enables administrators to manage guest access centrally and remotely. Having a centralized configuration for guest access reduces both management complexity and end-user complexity.

For centralized management, traditional wireless solutions require multiple wireless LAN controllers (one for each wireless network), which then tie back to a controller at a central office. These controllers are expensive pieces of hardware that must be refreshed every few years. In contrast, the Meraki Cloud Controller provides centralized management without any hardware. The Meraki Cloud Controller enables administrators to provide guests with a consistent guest access experience, regardless of where they are physically located.

6 Providing Guest Access with a Meraki Network

Meraki empowers administrators to provide wireless guest access quickly, easily, and at a disruptively low cost with a comprehensive set of access, security, branding, and management features. Using high-performance hardware and a Cloud Controller, Meraki offers an affordable, future-proof solution that can grow with the organization's needs.

For more information on how to offer wireless guest access with Meraki, please contact Meraki at meraki.com.