



# Meraki White Paper: Wireless User Authentication

---

---

**Version 2.0, February 2009**

Authentication enables administrators to identify the users connecting to a wireless network. Authentication can be at the device level (blocking or allowing a MAC address) or at the user level (validating a username and password). Compared to user authentication, device authentication is trivial (and insecure, since MAC addresses can be spoofed). This white paper focuses on robust, secure, and easy-to-implement techniques for wireless user authentication.

**Copyright**

© 2009 Meraki, Inc. All rights reserved.

**Trademarks**

Meraki® is a registered trademark of Meraki, Inc.



[www.meraki.com](http://www.meraki.com)

660 Alabama St.  
San Francisco, California 94110

Phone: +1 415 632 5800

Fax: +1 415 632 5899

## Table of Contents

<b>1</b>	<b>Authentication Primer .....</b>	<b>4</b>
1.1	What is a Splash Page Login? .....	4
1.2	What is 802.1x? .....	5
1.3	What is Active Directory? What is RADIUS? .....	6
<b>2</b>	<b>Authentication Considerations.....</b>	<b>7</b>
2.1	Client Devices.....	7
2.2	Client Configuration .....	7
2.3	Client Experience .....	8
2.4	Authentication Per VAP .....	8
2.5	User Database.....	9
2.5.1	AD Configuration for RADIUS.....	9
2.6	Monitoring .....	11
2.7	Management.....	11
<b>3</b>	<b>User Authentication with Meraki.....</b>	<b>13</b>

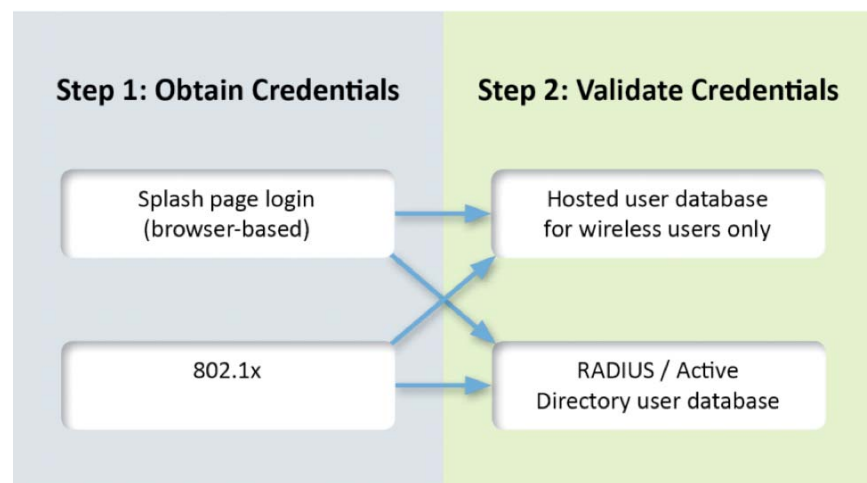
# 1 Authentication Primer

There are two methods for obtaining user credentials from a wireless user:

1. Prompt the user for credentials on a splash page, or
2. Obtain the credentials via 802.1x.

Once the user credentials have been obtained, there are two ways to validate those credentials:


1. Validate the credentials against a built-in user database (only for wireless users), or
2. Validate the credentials against a central user database (e.g., Active Directory or RADIUS).



## 1.1 What is a Splash Page Login?

A splash page login is a web page that prompts a wireless user to enter his credentials. When the user submits his credentials, the web server sends the credentials to the correct source for validation. Splash pages are typically customizable for branding or message. For instance, a splash page may be a company welcome page, or a “home page” for announcements by the IT team and news.

## 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)

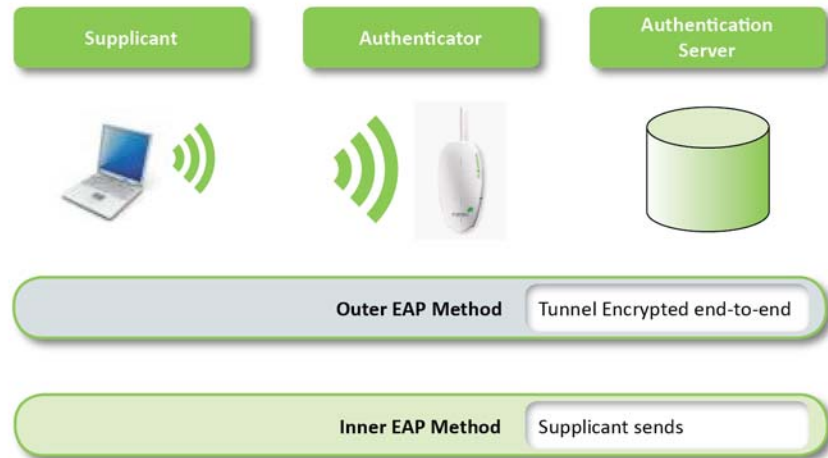
You will need to be on the list of authorized users for this network in order to access the Internet.

### 1.2 What is 802.1x?

802.1x is an IEEE standard for authenticating a user who is trying to associate to a wireless network. The standard utilizes the Extensible Authentication Protocol (EAP), which provides a mechanism for establishing a secure tunnel between participants involved in an authentication exchange. Three roles are defined:

- **Supplicant:** The supplicant is the wireless client that is trying to associate to the wireless network (i.e., the one being authenticated).
- **Authenticator:** The authenticator is the AP with which the wireless client is trying to associate. The AP takes the user credentials from the client and forwards them to someone who can validate them, (i.e., the authentication server).
- **Authentication Server:** The authentication server is the user database that validates the wireless client's credentials.

During an authentication exchange, the supplicant (the wireless client) and the authentication server (e.g., RADIUS) communicate with each other through the authenticator (the AP). The supplicant and the authentication server first establish a protected tunnel (called the outer EAP method). Next, the supplicant sends its credentials to the authentication server (via the inner EAP method).



There are different combinations of EAP methods, cipher suites, and key exchange algorithms that can be used in an 802.1x exchange. For instance, PEAPv0/EAP-MSCHAPv2 is a method that is often deployed in wireless networks. (PEAPv0 is the outer EAP method, and EAP-MSCHAPv2 is the inner EAP method.)

### 1.3 What is Active Directory? What is RADIUS?

Active Directory (AD) is a Microsoft software suite that provides, among other services, a user database. An AD server can validate user credentials using a protocol called RADIUS (Remote Authentication Dial-In User Service). Microsoft's RADIUS module is called Network Policy Server, or NPS (it was formerly called Internet Authentication Service, or IAS.) When NPS runs on the AD server, the authenticator forwards user credentials to the authentication server via RADIUS. The authentication server then accepts or rejects the user's credentials.

An AD server is useful for authenticating users who may connect wired or wirelessly.

## 2 Authentication Considerations

Should users be authenticated via a splash page login or 802.1x? Should user credentials be validated against an AD server or a wireless-only user database? The appropriate combination depends on the requirements and parameters of the wireless network and its users.

### 2.1 Client Devices

Administrators will need to choose an authentication method supported by the devices that will be connecting to the wireless network. For instance, a splash page login will be incompatible with devices that do not have web browsers (e.g., barcode scanners). These same devices may not even be able to perform 802.1x authentication. In this case, access to the wireless network should be controlled using an encryption method, such as a WPA2-Personal pre-shared key (PSK). Because this passphrase is shared, it should be rotated periodically to ensure that unwanted devices that have obtained the passphrase do not retain access to the wireless network.

### 2.2 Client Configuration

Authentication has client-side configuration implications. Splash page login requires the least amount of client-side work because the splash page displays in the client's browser. The splash page should be served securely via HTTPS, so that the credentials are encrypted when sent back to the splash page's web server. For splash page login, administrators should confirm that the splash page displays correctly in the supported browsers, and that the wireless clients are able to validate the server certificate of the splash page's web server. (The wireless client validates the server certificate when it establishes the HTTPS connection.)

In contrast, 802.1x requires a substantial amount of client-side configuration. If administrators control the software inventory of all wireless devices connecting to the network, it may be possible to distribute this client configuration (e.g., using AD). Otherwise, client configuration for 802.1x is non-trivial. For this reason, 802.1x should not be imposed upon visitors seeking guest access.

### 2.3 Client Experience

Authentication affects the user experience when users connect to the wireless network. Splash page login requires the user to enter a username and password in the browser before the browser (or possibly any other applications on the device) can access the Internet. The administrator configures how frequently the splash page is displayed. If this is too frequent, the splash page becomes an annoyance; too rare, and users will forget their credentials the next time they are asked to log in. If done correctly, however, the splash page can not only authenticate wireless users, but also can provide branding, advertising, or announcements to wireless users.

Unlike a splash login, 802.1x authentication can be completely transparent to wireless users. Windows machines can be configured for single sign-on, such that the same credentials a user enters to log into his machine are passed automatically to 802.1x for wireless authentication. The user is never prompted to re-enter his credentials. This transparency is less true for non-Windows devices such as Unix-based systems, however. Again, administrators must consider the device demographics in the network environment when selecting an authentication method.

### 2.4 Authentication Per VAP

A Virtual AP (VAP), also called a Service Set Identifier (SSID), is a logical wireless network that is advertised and supported by wireless access points. In practice, it is the wireless network that a client device “discovers” when it probes for wireless connectivity. When a wireless network supports multiple VAPs simultaneously, wireless users can obtain different services, end user experiences, and policies from the same access points (the physical network), depending on the VAP (the logical network) to which they have connected.

By configuring authentication settings on the correct VAP, administrators ensure that a given authentication method applies to the correct audience. For instance, a guest VAP may have no authentication settings on it, while the employee VAP may be configured to authenticate users via 802.1x against an AD server.

	Guest VAP	Employee SSID	Scanners SSID	Test SSID
<b>Encryption</b>	Open	AES (802.1x)	WPA2-PSK	WPA2-PSK
<b>Obtain credentials via</b>	Splash page login	802.1x	None	None
<b>Validate credentials via</b>	Wireless-only user database	Active Directory server	None	None



## 2.5 User Database

The user database validates user credentials either for the wireless network only, or for both wired and wireless users, depending on its scope and placement in the network. The wireless-only user database is useful for managing wireless users separately from wired users. For instance, a wireless-only user database is able to keep guest accounts separate from employee accounts. In contrast, a single, centralized user database enables employees to connect to the corporate network regardless of whether they are wired or wireless.

### 2.5.1 AD Configuration for RADIUS

An AD server is commonly used as the centralized user database for both wired and wireless user authentication. To handle incoming RADIUS requests for user authentication, the AD server must be configured as follows:

- Install server roles on the AD server (see Figure 1):
  - Network Policy and Access Services
  - Active Directory Certificate Services (AD CS): Only required for 802.1x.
- Under the Network Policy and Access Services role:
  - Install and configure the Network Policy Server (NPS) role service to offer RADIUS service. (See Figure 2.)
  - Within NPS, configure Network Access Protection (NAP) with the IP addresses of the APs that will be contacting the AD server. This is done by creating a policy, then adding the IP addresses of the APs to that policy.
  - Configure the User Groups and Machine Groups with the domain and the EAP method that the server will negotiate with the AP.
- Under the AD CS role (for 802.1x):
  - Install and configure the Certification Authority (CA) role service. (See Figure 3.)
  - Within CA, configure a server certificate that is appropriate for the network (e.g. a self-signed certificate or a domain-issued certificate). The important factor is to ensure that wireless clients are able to validate the server certificate (i.e. no pop-up with a warning about an invalid or unrecognized certificate).

- The wireless network must have connectivity to the RADIUS server. With splash page login, the splash page's web server (which plays the role of the authenticator) must have connectivity to the RADIUS server. With 802.1x, the APs need to be able to route to the RADIUS server.

Figure 1: Install the Network Policy and Access Services server role and (optionally, for 802.1x) the Active Directory Certificate Services (AD CS) role.

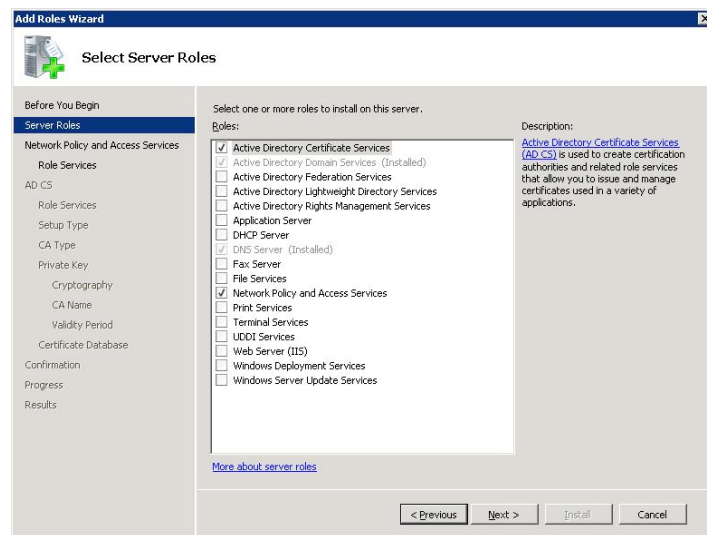


Figure 2: Under the Network Policy and Access Services role, install the Network Policy Server role service.

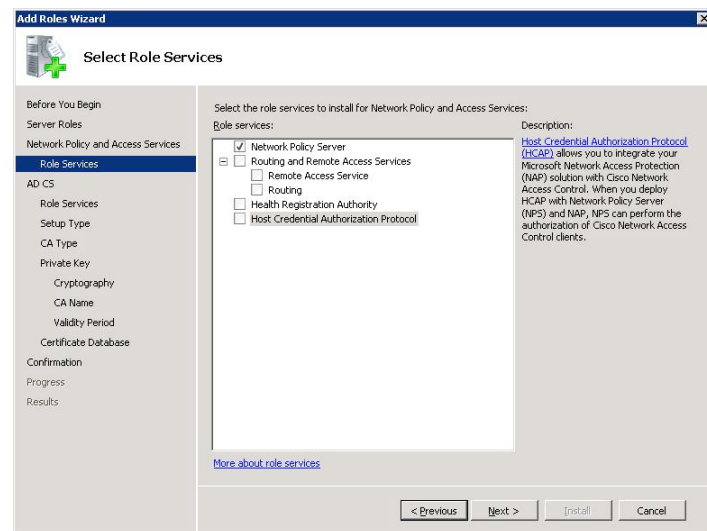
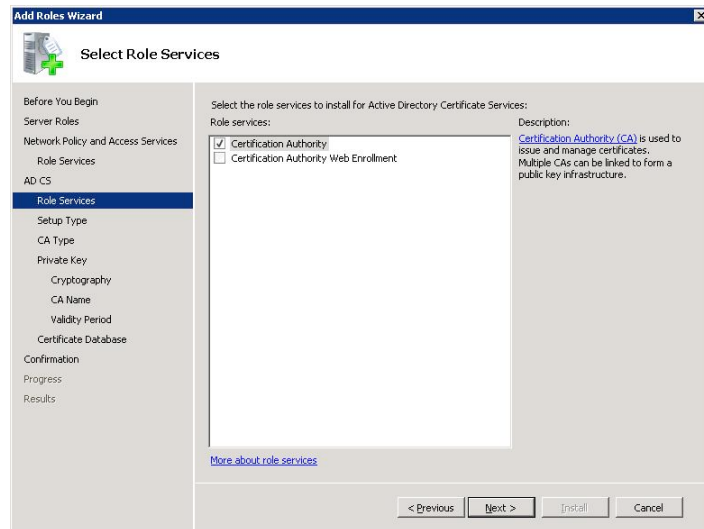


Figure 3: Under the AD CS role, install the Certification Authority role service (for 802.1x).



## 2.6 Monitoring

Administrators should monitor user authentication attempts to see who is trying to access the wireless network. With splash page login, authentication failures can be logged by the splash page's web server and/or the authentication server. With 802.1x, authentication failures can be logged by the AP and/or the backend user database.

## 2.7 Management

Administrators should be able to manage user authentication easily—adding, modifying, and deleting user accounts; troubleshooting wireless users who are unable to authenticate successfully; and troubleshooting the backend infrastructure (e.g., to ensure that the RADIUS server is configured correctly).

Management of the wireless networks also impacts user authentication. If wireless networks have different authentication settings, a single wireless user will require multiple wireless configurations to associate successfully to all of the networks. If, instead, a single authentication configuration were deployed to all of the wireless networks within an organization, a wireless user would then be able to roam seamlessly among the networks. This latter scenario is highly beneficial to organizations with many branch offices, and specifically to employees who roam between the offices. A centralized management solution significantly lowers the challenges associated with distributing and enforcing a single authentication configuration to multiple wireless networks.

The Meraki Cloud Controller is a hosted controller that provides administrators with centralized management and monitoring of multiple wireless networks, without any hardware-based controllers on premises.

### 3 User Authentication with Meraki

Meraki provides all of the user authentication options that administrators require, and more. With Meraki, administrators achieve:

- **Security** by knowing who is accessing the wireless network.
- **Flexibility** that enables different kinds of devices (e.g. laptops, handhelds, etc.) and audiences (e.g. employees, students, guests, etc.) to connect.
- **Ease of deployment** with auto-configuring APs and a hosted controller.

With high-performance hardware and the Meraki Cloud Controller, Meraki offers an affordable, future-proof wireless 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](http://meraki.com).