Meraki

Contents

- 1 Overview
  - 1.1 Security
- 2 Meraki Configuration
- 3 Custom Login Page

Overview

Meraki is a cloud-based managed wi-fi solution. http://www.meraki.com/

This article explains how you can add Swivel Authentication to the wifi authentication process.

The integration is possible because Meraki allows for two features:-

- RADIUS Authenetication
- The ability to direct a user to a specified URL

Security

The wireless connection uses PAP as the authentication method when you are using the Sign-on Splash page feature. With PAP, user credentials are sent in plain text. However, in a Meraki network, user credentials are encrypted in an SSL tunnel when sent from the clients web browser to the Meraki Cloud Controller. The Meraki Cloud Controller acting as the RADIUS client sends the username and password along with other connection specific data in a RADIUS Access-request to the PINsafe RADIUS server you specified in Dashboard. For security, the Meraki Cloud Controller encrypts the password using the RADIUS shared secret and an XOR function. This ensures the users password is never transmitted in plain text.

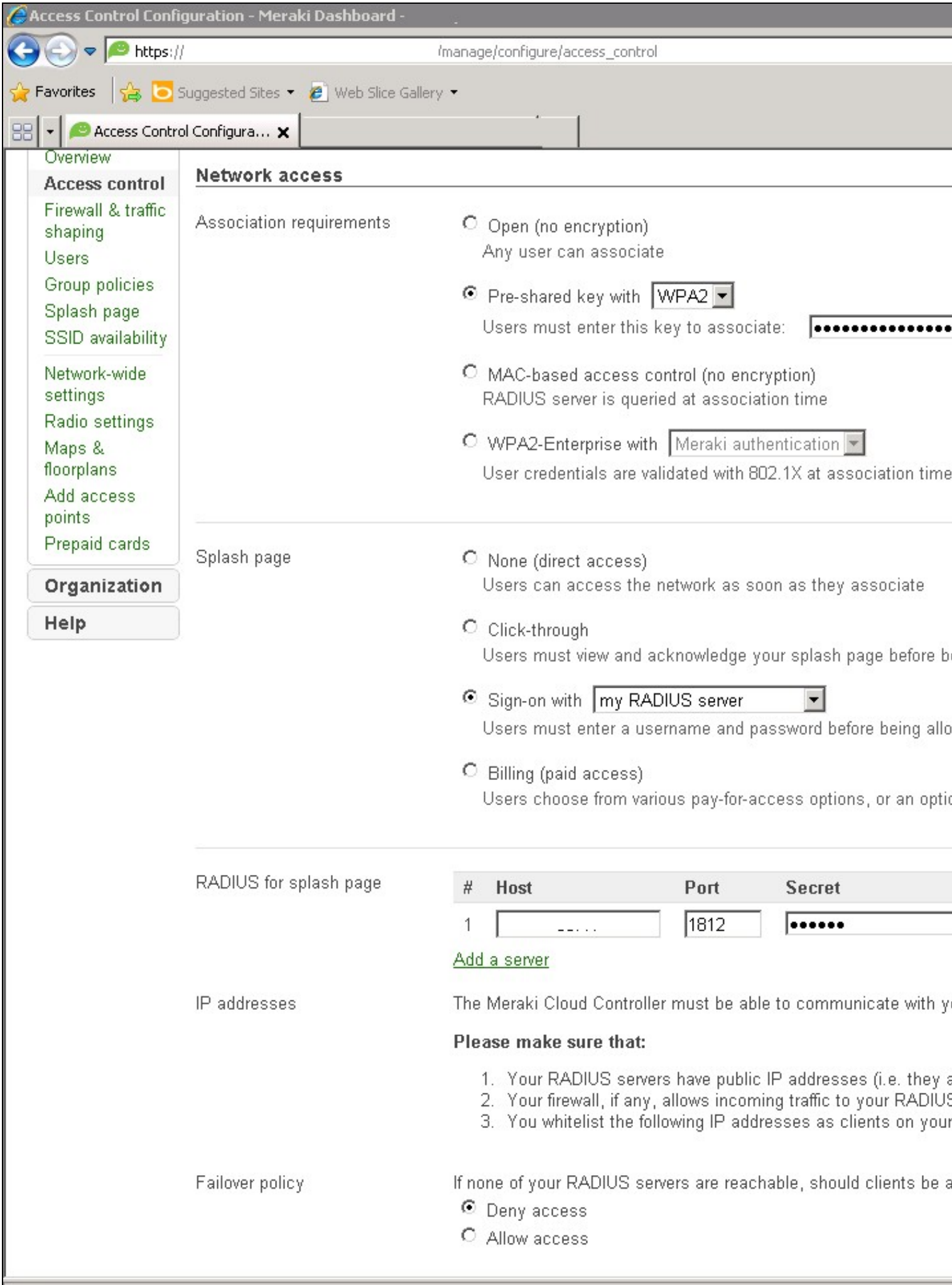
Meraki Configuration

There are two settings specifc to this integation, setting RADIUS for authentication and setting the url of the custom login page.

Firstly on the access control page you need to specify that authentication to this network will be via RADIUS. You need to enter the host name/ip address of the Swivel server and enter a shared secret.

Note that the Swivel server needs to be accessible on the RADIUS port via the internet for the integration to work.

Also you need to create a NAS entry on the Swivel Server that matches that of the Meraki entry. The Meraki config page lists the possible source IP addresses.

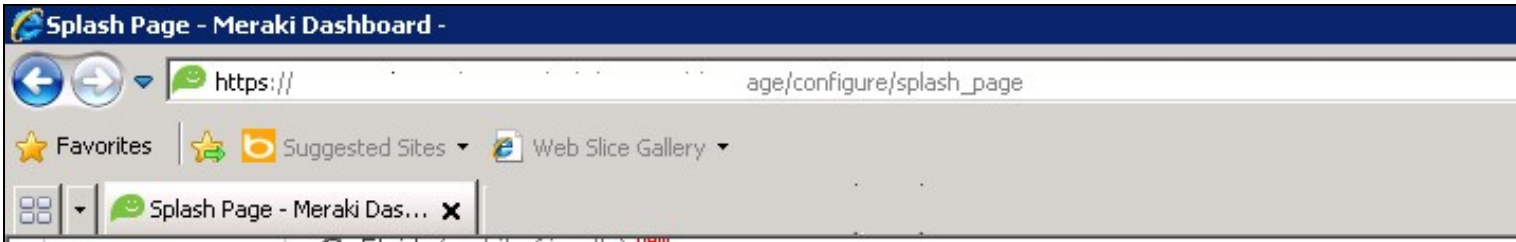

Access Control Configuration - Meraki Dashboard -
https://
/manage/configure/access_control
Favorites
Suggested Sites
Web Slice Gallery
Access Control Configura...
Overview
Access control
Firewall & traffic shaping
Users
Group policies
Splash page
SSID availability
Network-wide settings
Radio settings
Maps & floorplans
Add access points
Prepaid cards
Organization
Help
Network access
Association requirements
Open (no encryption)
Any user can associate
Pre-shared key with WPA2
Users must enter this key to associate:
MAC-based access control (no encryption)
RADIUS server is queried at association time
WPA2-Enterprise with Meraki authentication
User credentials are validated with 802.1X at association time
Splash page
None (direct access)
Users can access the network as soon as they associate
Click-through
Users must view and acknowledge your splash page before b
Sign-on with my RADIUS server
Users must enter a username and password before being allo
Billing (paid access)
Users choose from various pay-for-access options, or an optio
RADIUS for splash page
Host Port Secret
1 1812
Add a server
IP addresses
The Meraki Cloud Controller must be able to communicate with y
Please make sure that:
1. Your RADIUS servers have public IP addresses (i.e. they a
2. Your firewall, if any, allows incoming traffic to your RADIUS
3. You whitelist the following IP addresses as clients on your
Failover policy
If none of your RADIUS servers are reachable, should clients be a
Deny access
Allow access

You can test this setup using the test button on the Meraki configuration page. If this is set-up correctly you should see a authentication failure in the Swivel logs and a the status change or OK on the Meraki configuration screen, as shown in the screen shot above.

Now the redirect to the login page needs to be set up.

The key setting is to set the Custom splash page URL to a web page that can perform the Swivel authentication.

This page can be a page hosted on the Swivel Appliance (e.g. under webapps2) or Swivel Server, but can be any page that can collect the credentials required for the authentication.



Fluid (mobile friendly) new

Classic

Plain

Custom themes

Copy of Classic

Create something new

Custom splash URL

Or provide a URL where users will be redirected:

http:// /login/login-meraki.jsp

What is this?

Customize your page

Message

Splash logo

No logo

Upload a logo

Splash language

English

Splash behavior

Splash frequency

Every half hour

What is this?

Where should users go after the splash page?

The URL they were trying to fetch

A different URL:

Save Changes

© 2012 Meraki, Inc. Privacy

Custom Login Page

When the user attempts to access a URL via the wifi network, they will be re-directed to the custom splash page.

As part of this redirection the following parameters will be passed

- The login_url: The URL to which the login-form needs to be posted
- The continue_url: The url the user was trying to access
- username The users username

The login form must extract these parameters from the request.

Post the username and password (or one-time code) to the login URL, also passing the continue URL.

If a user needs to supply a password and a one-time code, the login form also needs to concatenate the password and one-time code into a single password field.

An example extract of a login page is shown below. The full page is available to download.File:Meraki.zip. Not you will need to supply a suitable header.gif

```
<form method="POST" align="center" onsubmit="combine()" action="<%=grant_url%>">
 <table width="600" align="center">
 <tr>
  <td colspan="2"><image src="./header.gif"></td>
 </tr><tr>
  <td colspan = "2"> <h1>Welcome to Meraki WiFi</h1> </td>
 </tr><tr>
      <th>Username:</th><td><input type ="text" name="username" id="username" onblur="showTuring()" value="<%=username%>" /></td>
      </tr><tr>
      <th>Password:</th><td><input type ="password" id="adpassword" name="adpassword" /></td>
      </tr><tr>
      <th>OTC:</th><td><input type ="password" name="otc" id="otc" /></td>
      </tr><tr>

      <td><input type = "hidden" name="gr" value="<%=grant_url%>"/> </td>
      </tr><tr>
      <td><input type="hidden" name="success_url" value="<%=continue_url%>" /></td>
      </tr><tr>
        <td><input type="hidden" name="password" id="password" /></td>
</tr><tr>
      <td></td><td><input type="submit" value="Login" /><input type="button" onclick="showTuring()" value="New Image" /></td></tr><tr>
          <tr><td colspan="2">Unauthorised access to this network constitutes a breach of the Computer Misuse Act 1990.<br />n</td></tr>

          <% if (grant_url != null) { %>
      <input type="hidden" name="success_url" value="<%=URLEncoder.encode(continue_url)%>" /><%}%></td>
          </tr><tr>

          <th colspan="2"><image id="imgTuring" style="display:none" /></th></tr></table>
    </form>
```