



White Paper

Captive Portal Configuration Guide

JUNE 2014

This document describes the protocol flow, configuration process and example use-cases for self-hosted captive portal (splash page) access, which is relevant for Wi-Fi hotspot provision by retailers, hospitality owners and service providers.

Table of Contents

1	What is a Captive Portal?	3
2	Using Meraki's Built-in Splash Tools	4
3	Configuring an External Captive Portal (EXCAP)	6
	A. EXCAP Overview - Click-Through Splash	
	B. EXCAP Overview - Sign-on Splash	
4	Example Implementations	14
	A. Customers	
	B. Service Providers	
	C. Advanced EXCAP Use-Cases	
5	Conclusion	18

Copyright

© 2014 Cisco Systems, Inc. All rights reserved

Trademarks

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

1 What is a Captive Portal?

A captive portal (also known as a “splash page”) is what a user sees when they first associate with a Wi-Fi SSID and open a web browser to surf the Internet. When a captive portal is configured, all Internet traffic will be re-directed to a particular URL and a user is required to take specific actions before their traffic is able to pass through to the Internet. In this fashion, a service provider controls the initial Internet experience for their end customer can request the customer take a variety of actions such as: (1) fill out a survey, (2) purchase a billing plan, (3) view an advertisement, or (4) accept a set of terms and conditions before being allowed onto the Internet. A captive portal facilitates direct audience engagement at a critical point during a user’s Internet experience, and is therefore a powerful medium that can be used for a flexible range of use cases.



Figure 1. Example captive portal page

Cisco Meraki’s cloud management platform includes built-in captive portal functionality with features like credit card billing, prepaid codes, and pre-built templates for free click-through access. In addition, the Meraki solution also provides a powerful external captive portal API known as EXCAP, which can allow customers and partners to deploy and leverage their own captive portal and billing systems, enabling a limitless range of applications such as specialized coupons and user analytics. More information on deploying and configuring these capabilities is described in the subsequent chapters.

2 Using Built-in Splash Tools

The Meraki dashboard cloud management platform has a number of built-in captive portal tools that can be used to get a powerful splash page up and running within minutes. This platform includes some of the following features:

Splash page setup

- Custom messaging/terms of access
- Custom logo/branding
- Customizing specific elements on the splash page

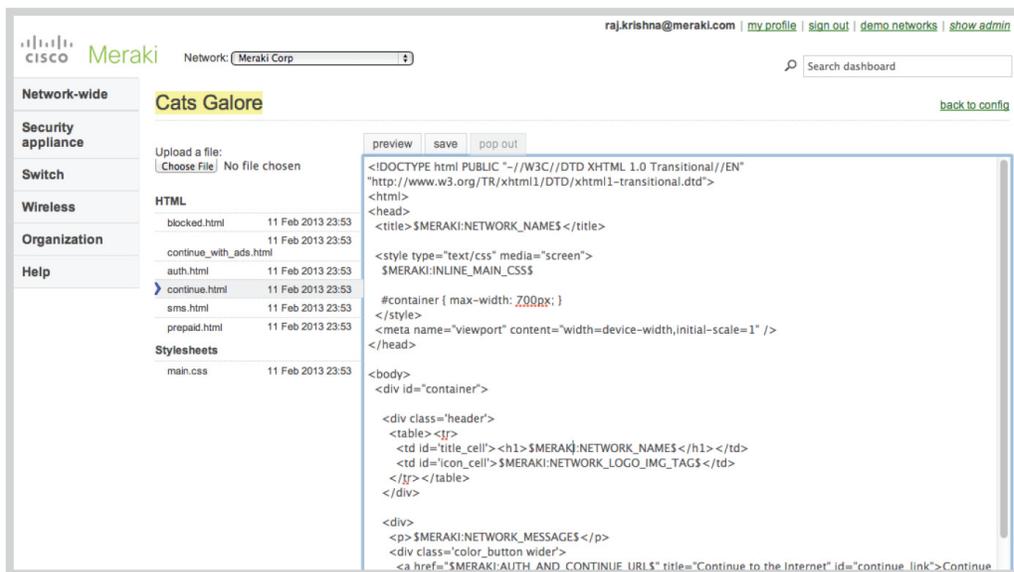


Figure 2. Meraki cloud-hosted custom splash editing tool

Splash page authentication

- Click-through sign-on
- New user-sign up with guest ambassador authorization
- Username/password sign-on with Meraki RADIUS
- Username/password sign-on with own RADIUS/LDAP server (see Meraki whitepaper “Active Directory Integration”)
- Facebook sign-on

Splash page billing options

- Free tiered access
- Setting up credit card billing plans
- Using prepaid codes generated by Meraki

Information on the Meraki built-in splash and captive portal capabilities, as well as instructions on how these settings can be configured, are available within Meraki online documentation at <https://docs.meraki.com/display/MR/splash+pages>.

3 Configuring an External Captive Portal (EXCAP)

This section explains how an administrator can use the Meraki external captive portal (EXCAP) API to configure a splash page that is hosted on their own server. This includes an overview of the two major captive portal sign-on methodologies – ‘Click-Through Splash’, where the user is redirected to a captive portal and clicks on a link to be granted access to the Internet, and ‘Sign-on Splash’, where the user is redirected to a splash page and must either sign up or enter pre-defined user credentials to be granted access after validation against a user database (using RADIUS).

A. EXCAP Overview - Click-Through Splash

The Meraki Wi-Fi EXCAP architecture allows for a user to be re-directed to an external captive portal where the hotspot provider can show a custom web page, targeted advertising, etc. The user can then click on a link to be granted web access. The process is shown below, including the scripting theory behind the behavior as well as the steps to configure the Meraki cloud interface.

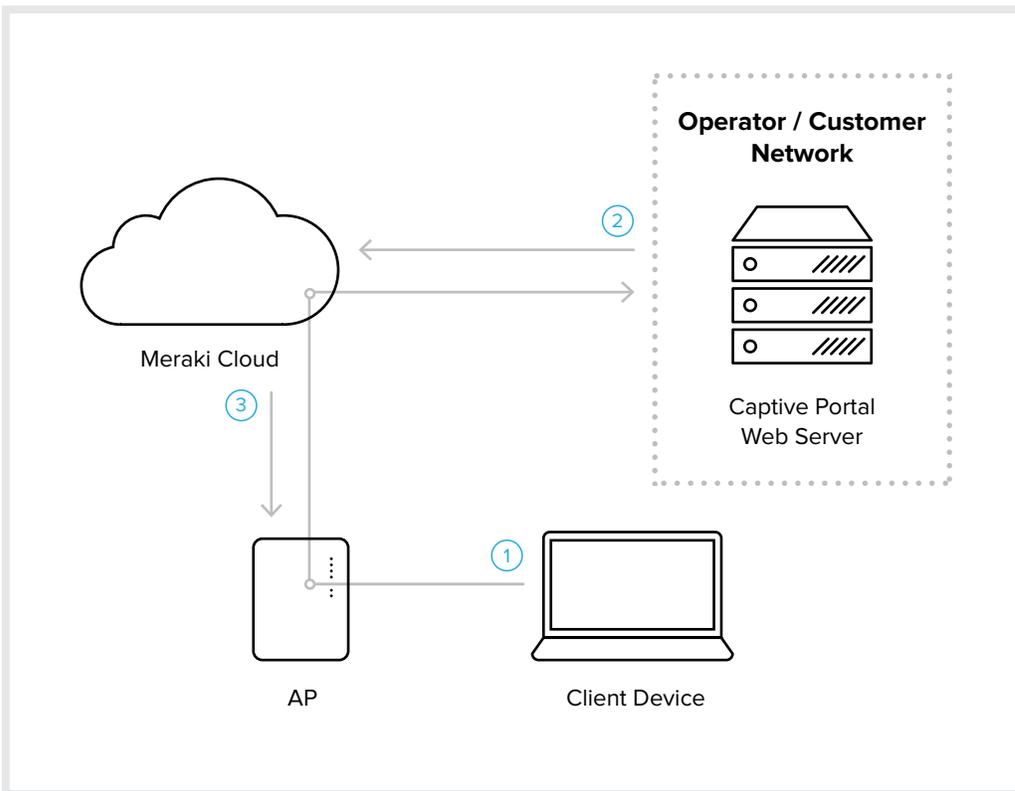


Figure 3. Click-Through EXCAP Architecture

The methodology by which a user is re-directed and ultimately granted access is as follows:

PHP Scripting – Explanation and Theory

- 1 When a client connects to your network a web browser is opened with an HTTP-based request (ie. <http://google.com>). After you have successfully completed the steps described in the configuration section below, the AP in your network will intercept this request and redirect the user through the Meraki cloud platform to the custom URL you specified. The user should be directed to a URL similar to the following string:

```
http://yourwebsite.com/clickthrough.php?base_grant_
url=https%00%00%00n00.meraki.com%2Fsplash%2Fgrant&user_continue_
url=http%3A%2F%2Fgoogle.com%2F&node_mac=00:18:0a:xx:xx:xx&client_
ip=10.128.128.120&client_mac=xx:xx:xx:xx:xx:xx
```

You can use the `node_mac`, `client_ip`, and `client_mac` parameters to mine information about the user and hotspot usage.

After you have correctly added the web server's IP to the walled garden, the user will be viewing the splash page (note that if you wish to whitelist by domain name instead of a list of IPs, you can contact Meraki Support to enable this feature). Note the extra parameters appended to the URL. It is critical that your web server detects and makes use of these parameters, as they indicate how to grant access. You might choose to store these parameters in a session or otherwise save them for later use.

At this point you can interact with the user however you wish. You might require them to agree to your terms of service, complete a form, or watch an advertisement. It is important to note that the user can fetch any web content within your walled garden.

- 2 Once you are prepared to grant access to the user, you must forward certain parameters you can gather from the URL in step 2 above. Specifically, you must forward the user to the following URL:

```
GET['base_grant_url'] + "?continue_url=" + GET['user_continue_url']
```

Where the following parameters are extracted from the user's original query or specified by you:

```
base_grant_url = https://n#.meraki.com/splash/grant
user_continue_url = http://google.com
```

In the case of the example above the assembled URL would be:

```
https://n#.meraki.com/splash/grant?continue_url=http://google.com
```

Note: Your URL may be different than the above example. It is dynamic and you should therefore never hard-code the grant URL.

- 3 The Meraki cloud platform grants access on the AP and redirects the user to continue to the URL (ie. <http://www.google.com>).

Network operators can optionally specify the length of the session they are granting. To do so include an extra GET parameter with name "duration"

For example:

```
GET['base_grant_url'] + "?continue_url=" + GET['user_continue_url'] + "&duration=3600" (to grant access for one hour).
```

You can obtain a pre-made sample PHP script at the following link: <http://bit.ly/Mu9XRv>.

Configuration steps to set up click-through EXCAP on the Meraki dashboard are as follows:

Access Control Configuration

- 1 Login to Dashboard and navigate to Configure -> "Access control."
- 2 Select the SSID you want to configure from the SSID drop-down.
- 3 Under "Network access" -> "Association requirements," choose "Open," "WPA2," or "WEP."
- 4 Under "Network access" -> "Network sign-on method," choose "Click-through splash page"
- 5 Enable walled garden (located under "Network access" -> "Walled garden") and enter the IP address of your web server.
- 6 Click "Save Changes."

Enabling Custom Splash

- 1 Navigate to Configure -> Splash page
- 2 Select the SSID you want to configure from the SSID drop-down.
- 3 Under Custom splash URL select the radio button 'Or provide a URL where users will be redirected' (see Figure 3 below).
- 4 Type the URL of your custom splash page (ie. <http://yourwebsite.com/yourphpscript.php>).
- 5 Click "Save Changes".

B. EXCAP Overview - Sign-on Splash

The end-to-end flow with sign-on splash is similar to the use case with click-through splash, except there is an additional exchange between the Meraki cloud platform and a RADIUS server after a user submits their credentials on a splash page. This could be their existing login credentials from a supplementary service, or new credentials issued after they have made a payment. The process is shown below, including the scripting theory behind the behavior as well as the steps to configure the Meraki cloud interface.

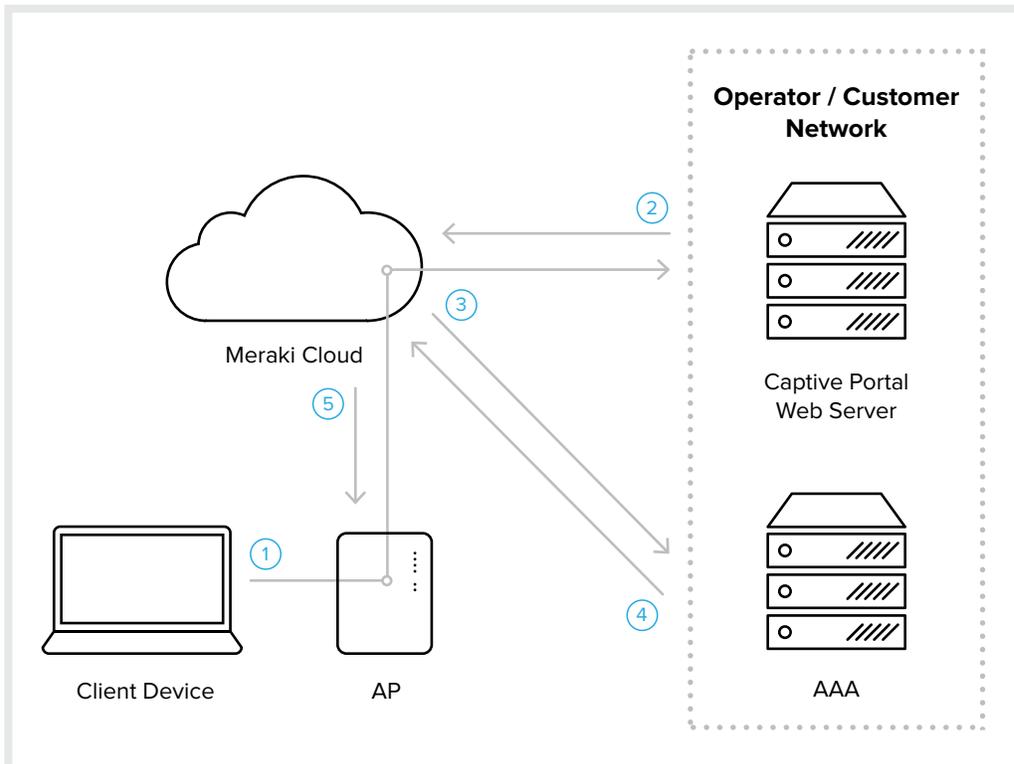


Figure 4. Sign-on EXCAP Architecture

The methodology by which a user is re-directed and ultimately granted access is as follows:

Scripting – Explanation and Theory

- 1 When a client connects to your network a web browser is opened with an HTTP-based request (ie. `http://google.com`). Assuming you have successfully completed the steps described in the configuration section below, the AP in your network will intercept this request and redirect the user through the Meraki cloud platform to the custom URL you specified. The user should be directed to a URL similar to the following string:

```
http://yourwebsite.com/clickthrough.php?continue_
url=http%3A%2F%2Fgoogle.com&login_url=https%3A%2F%2Fexample.
meraki.com%2Fsplash%2Flogin%2F%3Fmauth%3DABCDEF123456&ap_
mac=00:18:0a:00:01:02&ap_name=ap1&ap_tags=cafe
```

You can use the `ap_mac`, `ap_name`, and `ap_tags` parameters to mine information about this hotspot's usage.

Assuming you have correctly added the web server's IP to the walled garden, the user will be viewing the splash page. Note the extra parameters appended to the URL. It is critical that your web server detects and makes use of these parameters, as they indicate how to grant access. You might choose to store these parameters in a session or otherwise save them for later use.

At this point you can interact with the user however you wish. You might require them to sign up for a billing plan, fill in their existing subscriber information, or force them to navigate within a walled garden only. It is important to note that the user can fetch any web content within your walled garden.

- 2 Once you are prepared to grant access to the user, the username and password must be sent via POST to the `login_url`. There are several ways of achieving this:

1. Provide the user with a form where they can enter their credentials and click submit.
2. Use javascript to trigger the form submit automatically on the users behalf. This allows the form to be prefilled and hidden from view.

A sample web form is as follows:

```
<html>
<head><title>Internet Access Login</title></head>
<body>
  <h2>Internet Access Login</h2>
  <form method=POST action="https://example.meraki.com/splash/
login/?mauth=ABCDEF123456">
    <input type="hidden" name="success_url" value="http://www.
example.com/success/" />
    Username: <input type="text" name="username" />
    Password: <input type="text" name="password" />
    <input type="submit" value="Login" />
  </form>
</body>
</html>
```

- 3 The Meraki cloud platform sends a RADIUS ACCESS-REQUEST to the customer's RADIUS server.
- 4 The Meraki cloud platform receives an ACCESS-REJECT or ACCESS-ACCEPT response. The response may include one or more RADIUS parameters that Meraki supports, e.g., bandwidth limits and VLAN tags. If a valid response is received along with values for certain credentials, these will then be pushed to the AP which will in turn apply these values as settings to a client that is trying to connect. A complete list of RADIUS parameters that Meraki supports is included in Table 1.
- 5 When the user's credentials are sent via POST and the user is redirected back to the success_url, we also append the logout_url to the success_url; this can be used to construct a window where a user can click to have their session terminated (e.g. to conserve remaining time in the case of billed access). For the example above, the user would be redirected to the following URL after successfully authenticating:

```
http://www.example.com/success?logout_url=https%3A%2F%2Fexample.meraki.com%2Fsplash%2Flogout%2F%3Fmauth%3DABCDEFG123456
```

This success page is on your splash server, and the code on the success page can take this parameter and unescape it, which yields the following URL for logout:

```
https://example.meraki.com/splash/logout/?mauth=ABCDEFG123456
```

Access Request	Description
User-Name	
User-Password	
Called-Station-ID	(1) the MAC address of the Meraki access point and (2) the SSID on which the client is connecting. Example: "AA-BB-CC-DD-EE-FF:SSID_NAME"
Calling-Station-ID	Contains the MAC address of the wireless device (all caps, octets separated by hyphens). Example: "AA-BB-CC-DD-EE-FF".
Acct-Session-ID	Unique session ID per login
Framed-IP-Address	
NAS-Identifier	
NAS-Port-ID	
NAS-Port-Type	
Service-Type	
Access-Accept / Access-Reject	Description
Session-Timeout	This is the maximum time in seconds that the given user's session will last. After that time, the user will need to log in (authenticate) again using their username and password. Only used in Access-Accept packets.
Idle-Timeout	This is the idle timeout in seconds. If the user does not transfer any data on the network for this amount of time, the user's session will end and they will need to log in (authenticate) again using their username and password. Only used in Access-Accept packets. This attribute is ignored if RADIUS accounting is not enabled on the network.
Maximum-Data-Rate-Upstream/ Maximum-Data-Rate-Downstream	These are used to impose bandwidth limits, only used in Access-Accept packets. The values are the maximum rate in bits/second. See RFC 4679: vendor-specific (set Vendor-Id 3561). If these values are not present, Dashboard will use the Bandwidth limits that the user set on the Dashboard configuration page as a default.
Reply-Message	This is a message for the user that will be displayed inline on the splash page. It is allowed in Access-Accept and Access-Reject messages, but will only be shown to the user in the case of Access-Reject messages.
Filter-ID	This is a policy attribute that can be assigned to a user in order for them to adopt a corresponding Meraki 'group policy' configured in the Meraki Dashboard. A Meraki group policy can define a set of layer 3 and layer 7 firewall rules, in addition to a number of other traffic and QoS policies (e.g. blocking URL visibility). The Filter-ID attribute returned must match the group policy defined in the Dashboard in order for the user to adopt this policy.

Table 1. RADIUS Parameters and Descriptions

Once the user has successfully authenticated using RADIUS, the Meraki cloud platform will send an Accounting Start message with certain parameters that the RADIUS server can use to track and gauge user behavior. Similarly, a RADIUS Accounting Stop message is sent when a user's session is terminated, again filled with a list of statistics that a hotspot provider can use to form the basis for user analytics and policy decision making. A list of Accounting Start and Stop attributes are listed in Table 2.

Accounting Start	Description
Acct-Delay-Time	
Acct-Session-ID	Unique accounting ID meant to simplify matching of start and stop records in a log file.
Acct-Status-Type	
Calling-Station-ID	Contains the MAC address of the wireless device (all caps, octets separated by hyphens). Example: "AA-BB-CC-DD-EE-FF".
Event-Timestamp	Universal timestamp
Framed-IP-Address	
NAS-Identifier	Unique accounting ID meant to simplify matching of start and stop records in a log file.
NAS-IP-Address	
NAS-Port	Contains the MAC address of the wireless device (all caps, octets separated by hyphens). Example: "AA-BB-CC-DD-EE-FF".
Accounting Stop	Description
Acct-Session-Time	
Acct-Input-Packets	Unique accounting ID meant to simplify matching of start and stop records in a log file.
Acct-Output-Packets	
Acct-Input-Octets	Contains the MAC address of the wireless device (all caps, octets separated by hyphens). Example: "AA-BB-CC-DD-EE-FF".
Acct-Output-Octets	Universal timestamp
Acct-Input-Gigawords	

Table 1. RADIUS Parameters and Descriptions

4 Example Implementations

A number of Meraki customers and partners have created advanced captive portal implementations that demonstrate the ease of integration with the Meraki EXCAP API. Examples include:

A. Customers

Forever New

This popular fashion retailer uses Meraki for guest and corporate WiFi at several locations across Australia. They have integrated with EXCAP to build a custom splash page where they collect end-user e-mail addresses in exchange for complimentary access.

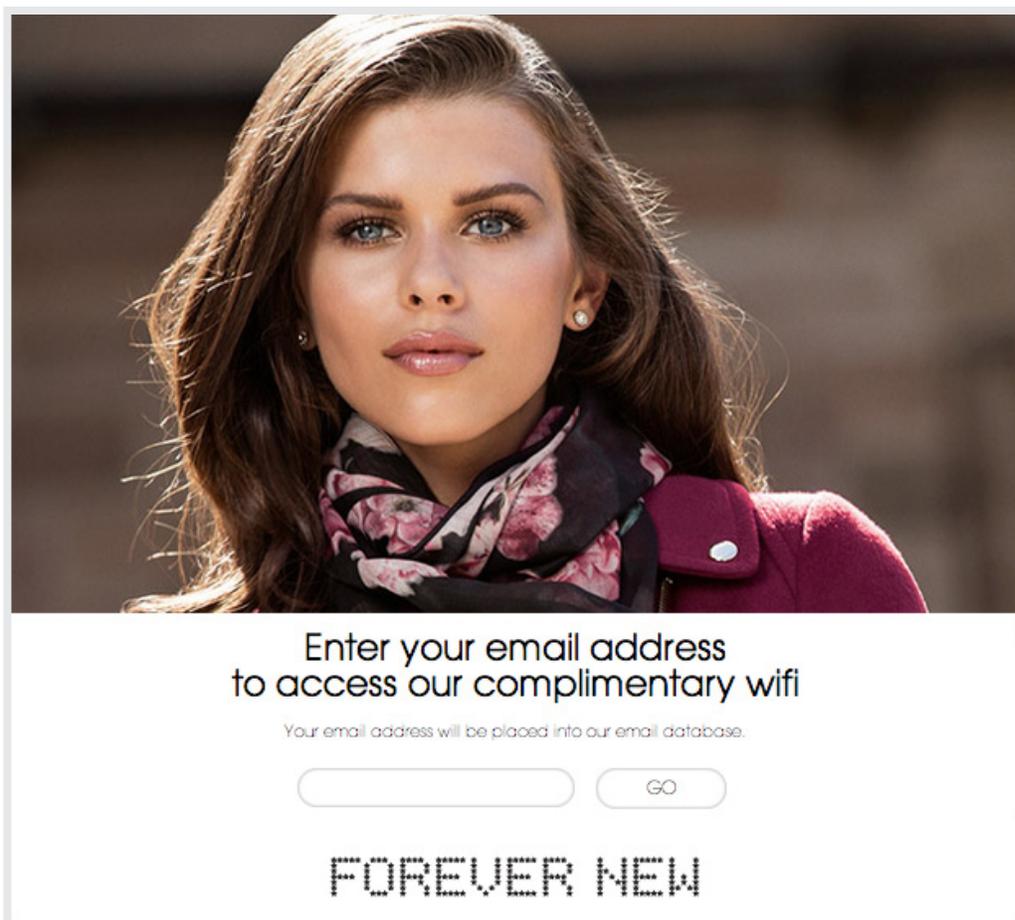


Figure 5. Captive portal at fashion retailer Forever New

A&W Restaurants

A&W uses Meraki to provide free wireless for guests at hundreds of locations across Canada. They have a custom-hosted splash page setup with their terms and conditions displayed for a customer to accept before gaining Internet access.

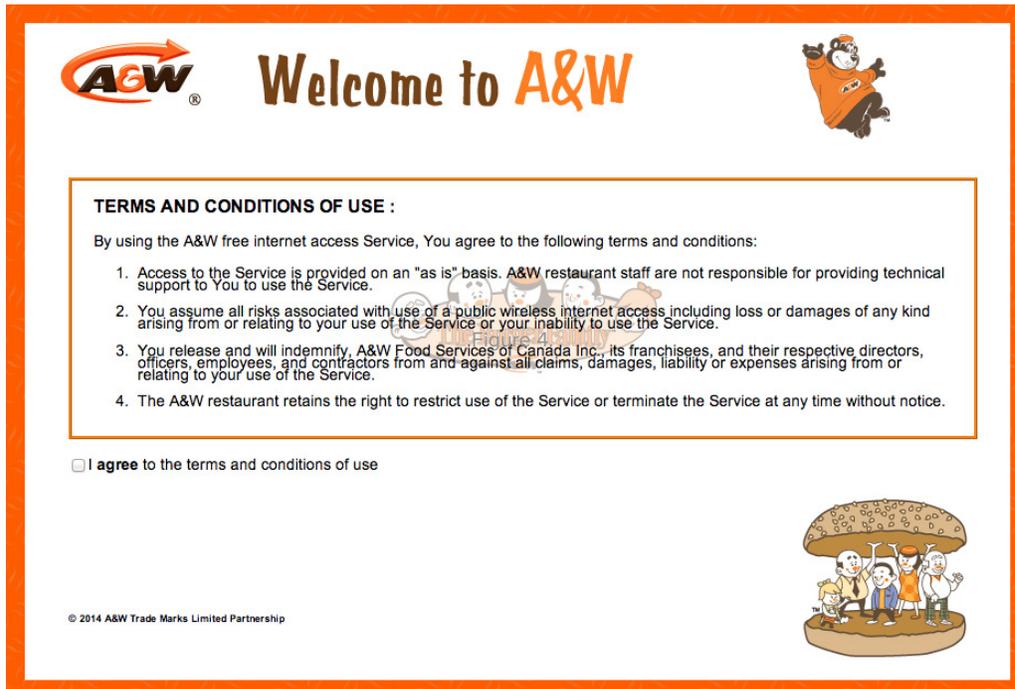


Figure 6. Captive portal at A&W Restaurants

B. Service Providers

Telmex

Telmex integrated their own custom hosted splash pages with back-end subscriber databases so that when a user accesses one of their 10,000+ hotspots in Mexico, they can get free Wi-Fi access if they are an existing Telmex subscriber. The flow is that a user accesses Wi-Fi, sees the [Telmex splash landing page](#), and enters their existing Telmex subscriber details. Telmex performs a look-up in their customer databases; they then grant free access if the person is an existing home broadband subscriber. If they aren't, the user has the option to purchase a plan, at which point Telmex creates a new RADIUS record for the user.



Figure 7. Captive portal at Telmex hotspots in Mexico

Splash Access

[Splash Access](#), a UK-based Meraki partner used EXCAP to create a platform that retailers can use to build custom splash pages and then collect e-mail addresses and other customer info. If email addresses are collected, e-mail marketing campaigns can then be run using MailChimp.

Wi-Tech

Italian Meraki partner provides a managed service for public hotspot provision with a cloud hotspot management platform called [Cloud4WiFi](#). EXCAP is used to allow for customizable splash pages. Wi-Tech offers a layer of customer engagement applications that can be overlaid on top of the splash pages, including geo-targeted ads using rotating banners, 'spot news' for the latest news stories, 'whats around you' for proximity-based recommendations on nearby points of interest such as bars and hotels, couponing, and the creation of online surveys.

C. Advanced EXCAP Use-Cases

The Meraki EXCAP architecture can also be used in tandem with Meraki's CMX API (described in the [Meraki CMX Analytics whitepaper](#)) in order to design a system where shopper's identities are tied to their devices upon their first visit, facilitating real-time shopper engagement without a captive portal on subsequent visits.

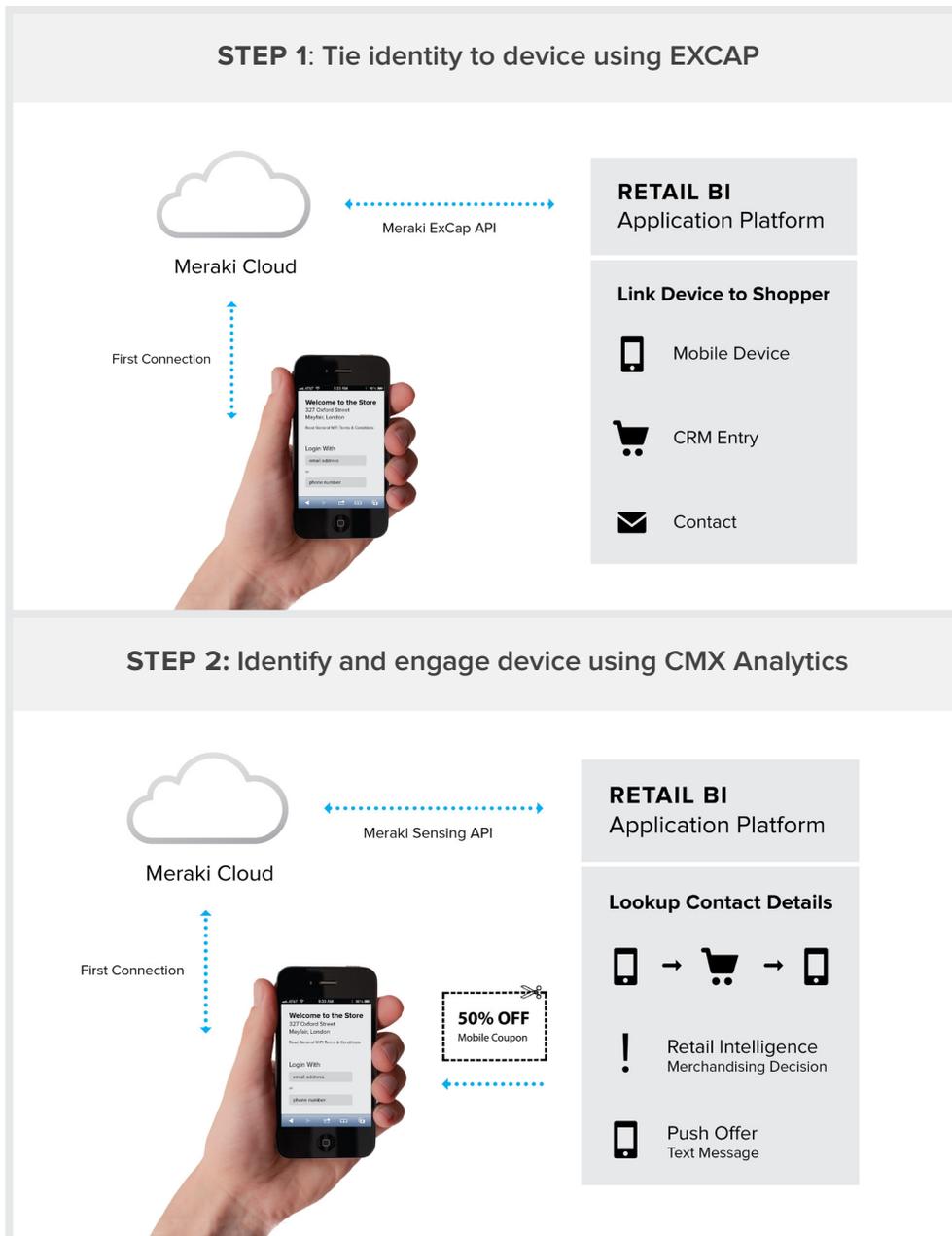


Figure 8. Shopper Engagement Flow

5 Conclusion

Wi-Fi Internet access is increasingly being provided as an amenity to customers across a range of vertical markets. Examples include the provision of Wi-Fi hotspot access for guest access in enterprise, in retail outlets such as shopping complexes and cafes, and in hospitality environments such as hotels and resorts. As the expectation for ubiquitous Wi-Fi access becomes prevalent, Wi-Fi service providers are seeking ways in which they can leverage their hotspot infrastructure to provide unique services such as location-based advertising and customer loyalty programs. Captive portals can facilitate these types of applications by allowing the service provider to provide a customized 'experience' to the customer as a part of their Internet sign-on process.

More information is available from Meraki's knowledge base at <https://meraki.cisco.com/support>, and Meraki Support (support@meraki.com) can be contacted for more detailed information, use cases, and troubleshooting support.