Splash Page Details for Meraki MR

A splash page (also known as a ‘captive portal’) can provide a customized branding experience to wireless users in addition to prompting for username/password credentials. For example, the splash page can display a corporate logo and color scheme. The splash page can also show the terms of service, which might include an acceptable use agreement or a privacy statement.

Administrators can set up a separate splash page for each SSID. Splash pages can be hosted by Meraki or by an external host.

None (Direct Access)

With direct access, a wireless client is granted network access as soon as he associates to the SSID. No splash page is presented to the wireless client.

Click-Through Splash Page

When configured, a click-through splash page displays a fully customizable HTML page to the wireless client the first time the client opens a web browser and makes an HTTP request. An administrator can use this splash page to display an acceptable use policy or network announcements. The client is only granted network access after clicking the “Continue” button on the splash page.

The click-through splash page is hosted by the Meraki cloud. As such, the network must have connectivity to the Meraki cloud in order to display the splash page. If the Meraki cloud is unreachable for some reason, the administrator can configure whether new wireless users should be admitted to the wireless network without seeing the splash page. This setting is under the Configure tab on the Access Control page in the “Disconnection behavior” section.

While the click-through splash page requires no client-side configuration, it should only be enabled on an SSID whose clients are all capable of displaying the splash page. When there are clients that are not browser-capable (e.g., gaming consoles, wireless barcode scanners), the splash page should be disabled on the SSID. An administrator can configure whether new wireless clients are able to obtain network access when the click-through splash page cannot be displayed (e.g., if the Internet link goes down and the connection to the Meraki cloud becomes temporarily unavailable).

Sign-On Splash Page

A sign-on splash page provides the functionality of the click-through splash page, but adds the ability to prompt the wireless client for a username and password.

Note: The AP looks for HTTP GET requests on TCP port 80 in order to redirect users to the Splash page. If Block all access until sign-on is complete is enabled for the Captive Portal Strength, and the user attempts to access a web page that uses HTTPS, the AP will be unable to redirect the browser to the Splash page because the web traffic is encrypted. Additionally, if the user attempts the access a web page that uses a different port other than TCP port 80 the connection will also be blocked. In either case, the user’s browser will timeout. If this is occurring, verify users are accessing a web page using HTTP over TCP port 80.
The client is only granted network access after he enters a username and password that are validated against a backend authentication server (either a Meraki-hosted authentication server or a customer-hosted RADIUS, Active Directory or LDAP server).

The sign-on splash page may be hosted by the Meraki cloud or on an external web server. An administrator can configure whether new wireless clients are able to obtain network access when the sign-on splash page cannot be displayed or when the username/password credentials cannot be validated (i.e., the authentication server is unreachable). This setting is under the Configure tab on the Access Control page in the "Disconnection behavior" section.

The sign-on splash page can be configured to allow or disallow multiple simultaneous logins for a single set of user credentials.

Sign-on splash page is an authentication option that requires no client-side configuration. In addition, it is secured by SSL (HTTPS), so that usernames and passwords are sent to the Meraki cloud confidentially. However, when enabled, it requires clients to remember usernames and passwords, which they will need to enter periodically. As with the click-through splash page, clients that are incapable of displaying the splash page need to be considered.

Hosting Your Own Splash Pages

Meraki also supports the ability for you to host splash pages on your own web server. This capability is referred to as “EXCAP” (short for external captive portal) for externally hosted captive portals. Using EXCAP, it is possible to deliver a highly customized user sign-on experience, such as video advertising and credit card billing. For additional information, please see Meraki's Captive Portal Solution Guide.

Billing Splash Page

When configuring an SSID as a wireless hotspot, an administrator can utilize Meraki’s integrated billing features to grant network access only to paying users. Billing is enabled as a network sign-on method. It is configured under the Configure tab on the Access Control page.

Prepaid cards are access codes that can be used to pay for network access on billing SSIDs. Prepaid card pin codes with pre-defined values can be generated in batches by network admins. When creating a batch of cards, the network admin can define face value, quantity, and an optional expiration date. The prepaid pin codes can be downloaded in CSV format and then printed onto cards or labels using programs such as Microsoft Word mail merge.

The administrator can configure the currency for a billed network. Note, however, that once a transaction has occurred on the network, it is not possible to change the currency of the billed network. An administrator can create up to five billing plans (tiers of service). The administrator can specify the fees charged over a particular amount of time with a specific performance limit. For example:

- $5 per month for .5 Mbps of bandwidth
- $10 per month for 1 Mbps of bandwidth

In addition, the administrator can check the “Free access” option, which provides free access for a limited amount of time (and possibly subject to a bandwidth limit). This limited free access can serve as a trial period for wireless users before they purchase a paid plan.

Customization of Billing Splash Pages

Note that it is not possible to customize the splash page when billing is enabled unless the 'Use fast prepaid login page' is selected under the 'Prepaid access' section on the Access control page.

SMS Splash Page

Using the Meraki cloud, it is possible to allow new users to sign on via SMS authentication codes. By utilizing this approach, an administrator can tie each new user to a unique phone number that is displayed on the Clients page in dashboard under the 'Recent User' column. This data can be used to run SMS campaigns and for validation purposes to ensure that a user has provided personal information that can be used to track them, should they abuse the network.
**Configuration**

SMS authentication can be set up under the Access Control page by selecting ‘Sign-on with SMS Authentication’ in the splash page settings.

The splash page that is displayed upon network sign-on can be customized on the Splash page settings; an admin can select a custom logo and write a message that will be displayed. It is also possible for deeper customization of the splash page by creating and editing a new theme, and making changes to the file 'sms.html'.

**Free Trial Period & Billing**

Every Meraki network comes bundled with 25 free SMS text messages. Beyond this limit, the user will be charged on a per-SMS basis and will need to configure billing. Configuring billing is a simple 2 step process:

1) Create Twilio SMS account at www.twilio.com

2) Enter in credit card information to create an account with full privileges, and purchase a phone number with Programmable SMS capabilities.

3) Make a note of the **Account SID** and the **Auth Token** values on the main twilio.com/user/account page.

4) Enter your Twilio Account SID and Auth Token values into the Meraki Dashboard on the Network-wide > General Settings settings page.

You will now be billed on a per-SMS basis via Twilio. Prices can range by country; the typical cost per SMS ranges from 1 cent per SMS for the United States to over 10 cents per SMS for certain carriers in Europe. A complete, up-to-date pricing list is available at [https://www.twilio.com/sms/pricing#outbound-pricing](https://www.twilio.com/sms/pricing#outbound-pricing).

**Splash Sign-on Flow**

The network sign-on method for a new user will be as follows:

1) User accesses SSID with SMS splash authentication enabled.

2) Splash page requesting phone number is displayed.

3) User enters their phone number, an authorization code is sent via the user’s carrier to their phone.

4) User enters the unique authorization code into the splash page and presses the ‘enter’ button, is granted access.

5) The user’s phone number is stored in dashboard, and can be seen by adding the ‘Recent User’ column on the Monitor > Clients page.

**Facebook Login**

Meraki and Facebook provide a social sign-on experience for users logging into Wi-Fi hotspots. Similar to how Meraki splash pages can be used for a customized branding experience, you can now use a specific Facebook page as the sign-on page a user sees when they first log in with Wi-Fi. Users can then check-in with their Facebook credentials, update their status, and ‘like’ the Facebook page.

The [Facebook Wi-Fi FAQ](https://www.facebook.com/help/web/252574832138595) is available on the Facebook website.


**System Manager Sentry enrollment**

The SSID on which Sentry is enabled requires a mobile device to be enrolled in any one of an organization's SM networks before granting the device access to
connect to the SSID. If the device is not enrolled in an existing SM network, the user is prompted with a click to accept message that will enroll the device into the SM network as well as provide any configuration profiles and required apps previously configured.

View the System Manager Sentry enrollment deep dive article for more information including configuration information.

Google Sign-in

Using the oAuth protocol, Meraki MR access points are able to authenticate users via a sign-on splash page for network access control. View the Google Sign-in deep dive article for more information including configuration information.

Wireless User Logins

While the Clients page shows a list of devices, the Logins page shows a list of users. A user can login with multiple devices.

The Logins page shows users who have logged in with one of the following authentication methods:

- Sign-on splash pages with a Meraki-hosted authentication server
- Billing logins

Like the Clients page, the Logins page allows an administrator to filter users by the SSID on which they associated, display different columns of information, sort by different columns, and adjust the zoom level by timeframe.