Troubleshooting the Splash Page Appearance

Cisco Meraki MR access points and MX security appliances support the use of Splash pages to restrict users access to network resources prior to authentication. The Splash page is enabled on Wireless/Security appliance > Configure > Access control and the frequency at which it appears is configured on Wireless/Security appliance > Configure > Splash page.

Note: If Active Directory is integrated onto the MX, the Splash page and Access control tabs will disappear, as AD integration is incompatible with an MX-hosted Splash page.

In some cases, a configured splash page may appear more or less frequently than intended on client devices, or not at all. This article describes what occurs when a user passes through a Splash page, the possible reasons why a Splash page is appearing at a frequency that is different than what is configured on the Dashboard, and how to resolve these problems.

What is the Splash Page Authentication Process?

When Sign-on Splash page is configured as the Network sign-on method, a user is authenticated by opening their web browser and submitting user credentials to the splash page. 'Signing-on' opens up full network access provided no additional Layer 3 or Layer 7 firewall rules exist. Users are authenticated by the Cisco Meraki Cloud Controller through the gateway AP.

If a Click-through Splash page is configured a user gains full network access after agreeing to the terms presented on the splash page.

After passing the splash page, three actions occur:

1. An access control list (ACL) entry for the client device is placed on the gateway AP.
2. An access control list (ACL) entry for the client device is placed on the Cloud Controller.
3. A session cookie is placed in the user’s web browser cache.

Troubleshooting Appearance Frequency

The following sections outline how to troubleshoot a splash page that isn't appearing with the appropriate frequency.
The Splash Page Appears More Frequently than Expected

For the best splash page experience, users should have their web browsers configured to accept cookies. Failure to do so may result in the user seeing the splash page on a more frequent basis than is required by Dashboard configuration. For example, a user who clears their web cache or has their browser configured to not accept cookies they will only see the Splash page at the configured interval as long as the gateway AP is not rebooted. If the gateway AP reboots, they will be required to authenticate again or present the cookie to the splash server.

When Captive portal strength is set to Allow non-HTTP traffic prior to sign-on a user will not notice any loss of network access except HTTP (TCP port 80). When the user attempts browse to a new HTTP web page in their web browser, they will be redirected to the splash page. If the browser cookie is present in their web browser cache, the user will be authenticated in the background - they will not see the splash page because the cookie identifies them as authenticated.

If Captive portal strength is set to Block all network access the user will lose network connectivity until they authenticate again, by opening a web browser.

The Splash Page Appears Less Frequently than Expected

This is caused by increasing the Splash frequency on Dashboard after a client is authorized by the splash page. For example, if a network is configured to present a Splash Page weekly and a client is authorized under this setting, they will not have to pass through the Splash page for another week even if the setting is changed to daily. The only way to force the client to pass through the Splash page earlier than that is by revoking that clients authentication. To revoke a client's authentication:

1. Locate the Client by going to Network-wide > Monitor > Clients and selecting the specific client.
2. Select Edit details at the top of the client details page.
3. Select revoke authorization under Splash Authorization and save the changes.

Web Browser Times Out Instead of Loading the Splash Page

There are some circumstances where an unauthorized user will open up a web browser with the intention of hitting the Splash page to authenticate, but the web browser times out or fails to load the page. This will commonly occur when the user was attempting to access a web site via HTTPS.

When the AP or security appliance sees an HTTP GET request from a non-authenticated user, it will redirect that request to its configured Splash page. If the user's initial request is using HTTPS, however, their request is encrypted and therefore cannot be redirected. As such, the request will time out.

To troubleshoot this issue, the user should clear their browser cache and try to access any website using HTTP (at this time, bing.com supports the use of unencrypted HTTP). If the issue persists, ensure that the client has a valid IP configuration, and troubleshoot for other possible network issues.
Blank Page Loads Instead of Splash Page

Since Splash pages rely on cookies to function, a blank page will appear if cookies are not enabled on the user's web browser. This is most common on mobile devices, but can be configured on any modern browser.

To resolve this issue, ensure that cookies are enabled in the web browser. Please refer to browser-specific documentation for details:

- Internet Explorer 9
- Mozilla Firefox
- Google Chrome
- Safari for iOS

Splash Page Loads but Post-Splash URL Doesn't On Android

On Android devices running OS version 5.0 or later, the URL set on "Where should users go after the splash page" in Dashboard will fail to load successfully. This is an expected behavior of Android OS 5.0+

Additional Resources

For more information about troubleshooting Splash pages or Splash in general, please refer to the following documentation:

- MX and MR Splash Pages
- Troubleshooting Users' Network Access with Splash Page Enabled
- Integrating and Troubleshooting Active Directory with Splash Page
- Customizing the Splash Page