Technical Guide

Captive Portal and HTTPS Redirection

Released: 2017-07-17
Doc Rev No: R1
Introduction

Controller has included two new features to enhance the Wi-Fi experience when dealing with Captive Portals.

- New browser behavior
- WISPr User Agents enhancement for automatic Captive Portal pop-ups
  - iOS support
  - Samsung Android support
  - Android support
- HTTPS Automatic Redirects

Common browsers and their behaviors when redirecting to the Captive Portal from HTTPS websites are outlined and provided in the following document. Furthermore, since the introduction of HSTS, a stricter HTTPS, popular browsers have been improved to detect and provide alternatives to reaching the network’s Captive Portal.

Controller’s Automatic Captive Portal pop-up support has been improved for additional devices using respective WISPr User Agents. These include the latest iOS, Samsung Android and Android devices. This newest update provides wider support the built-in captive portal detections on supported operating systems.

With controller’s HTTPS Automatic Redirects, we provide the option for venues and operators to allow their users to view these security warning. When enabled, users may encounter security alerts depending on what browser is used and which webpage is redirected to the Captive Portal. When disabled, the user’s browser will be prevented from reaching the security alerts page when an HTTPS website is requested. The user will be either shown a blank page or a connection timeout page. When users access a non-secure HTTP webpage, they will be redirected.

These improvements aim to minimize the percentage of security warnings viewed by users connecting to controller’s Captive Portals.
# Table of Contents

1. What is HTTPS? ................................................................. 3
2. When are these security alerts seen? ................................... 4
3. What are the available methods used today? ......................... 8
4. Controller’s Captive Portal Solution ...................................... 9
5. Remarks ............................................................................. 13
Appendix ................................................................................. 14
1. What is HTTPS?

Before answering what is HTTPS, let’s first introduce HTTP, HyperText Transfer Protocol, which is the foundation of how data is transferred across the internet. You may recognize the acronym HTTP in nearly all websites you see today which begins with “http://”.

HTTPS is an acronym for HTTP over SSL (Secure Socket Layer) or HTTP Secure. Online services such as online banking requires the secure connection provided by HTTPS to protect its user’s confidential information.

As more and more companies shift to using HTTPS for increased security in their websites and protecting its users, redirecting from HTTPS websites to Captive Portals in public hotspots are more likely to occur. The method Captive Portals are initiated is by redirecting the user’s internet traffic on their device to the Hotspot’s captive portal. The redirection happens while the browser is trying to connect to the first website requested by the user. If the website is an “http://” website, there will be no issue on any browser. However, if the website is a secure “https://” website, then the browser will display a security warning since the SSL certificate received does not match that of the requested website.

![User Flow and Captive Portal Redirection Diagram](image-url)
2. When are these security alerts seen?

Each user’s experience when accessing the Login Page/Captive Portal of the Wi-Fi Hotspot is different. Their experience is determined by the following factors:

- **Operating System**: iOS, Android, Windows.
- **Browser**: Internet Explorer, Mozilla Firefox, Google Chrome
- **Webpage**: User’s Default Home Page or First Requested Web Page

The combination of the above factors will determine whether the user is presented with a security warning. The first web page that user visits is the main determining factor.

**Operating Systems**

Recent advances in Mobile Operating Systems have taken initiative to overcome the security warnings that comes with Captive Portal redirection.

**Apple’s iOS** devices support a built-in Captive Portal Detection where once the iOS device connects to a Wi-Fi Hotspot, the iOS’s built-in Web Sheet opens [http://captive.apple.com](http://captive.apple.com) as its first request and successfully redirects to the Captive Portal.
**Android Smartphones** may detect the Wi-Fi Hotspot and inform the user to “Sign in to Network” to access the Internet. Clicking on the message will open the device’s default browser. The Android OS tries to reach a specific URL built into its system, [http://connectivitycheck.android.com/generate_204](http://connectivitycheck.android.com/generate_204), to obtain a response. If a HTTP 204 response is obtained, the network connection is determined to be successful. If any other response is obtained, then a captive portal is assumed since the required response for a successful network is not obtained.

![Android OS Captive Portal Detection](image)

**Windows** (Windows 8, Windows 8.1, Windows 10) Operating Systems have a built in captive portal detection. It will try to reach the following URL, [www.msftncsi.com](http://www.msftncsi.com), to determine whether a Captive Portal exists in the connected network. If exists, the OS will notify the user or automatically open the Captive Portal with the default browser.

![Windows OS Captive Portal Detection](image)
Browsers

Browsers have also begun to incorporate automatic Captive Portal detections when connected to a hotspot requiring the user to go through a login page.

**Chrome** browsers will automatically request an HTTP webpage such as `http://<subdomain>.google.com/generate_204` just like the Android and Windows OS to be redirected to the Captive Portal of the network. If the user manually requests an HTTPS website, the security alert in the second image may be encountered.

![Chrome Browser Captive Portal Detection](image)

![Chrome Browser Certificate Security Alert](image)
Firefox has included a built-in captive portal detection when using their browser. A message is shown to the user, “You must log in to this network before you can access the Internet” and a ‘Open Network Login Page’ button is available. Upon clicking, Firefox will request from `http://detectportal.firefox.com/success.txt` prior to redirecting to the Login Page.

Firefox Browser Certificate Security Alert/Captive Portal Detection

Internet Explorer does not have a captive portal detection mechanism as well but allows the windows operating system to perform this action. The user trying to browse a HTTPS website may encounter a certificate security alert like the following. Clicking ‘Continue to this website’ link will allow the redirection to the Captive Portal to occur.
3. What are the available methods used today?

1. **Block HTTPS webpages and allow only HTTP webpages to be redirected to the Captive Portal.**
   
   **Comment:** In the long run, this method will be less and less effective as more websites are transitioning to HTTPS.

   **Behavior:** Only a blank page or a “Connection Timeout” message will appear on the user’s browser. The user will be required to enter a HTTP webpage to gain full access to the internet.

2. **Allow all HTTPS webpages to be accessed prior to authentication.**
   
   **Comment:** Not effective as many popular websites uses HTTPS.

   **Behavior:** Users will be allowed to browse any or most HTTPS websites, in which increasingly popular companies such as Google and Facebook have now transitioned over. Only when the users enter an HTTP website will they be redirected to the Captive Portal.

3. **Purchase valid certificates for all HTTPS sites that the user may visit.**
   
   **Comment:** Not a practical or financially valid method.

   **Behavior:** The venue will require to determine all the web pages their users will visits and then purchase each website’s certificates.

4. **Create fake certificates on the fly.**
   
   **Comment:** User connection and personal information prone to security risks.

   **Behavior:** When fake certificates are generated, the user will be required to install these 3rd party certificates into their devices. When using public Wi-Fi, it is generally not recommended to trust/install or add exceptions for unknown or untrusted sources. Other than requiring in-depth technical expertise of encryption and certification required for all HTTPS websites on each browser, the connection between the user and an HTTPS website will no longer be secure. This situation may pose an even higher security risk due to the false appearance of a secure connection.
4. Controller’s Captive Portal Solution

Controller’s Captive Portal solution focuses on minimizing and preventing the occurrences of the browser’s security warnings concerning HSTS by providing additional support for the automatic detection of captive portals in today’s devices and an additional option of disabling HTTPS redirection.

4.1 Browser’s Latest HSTS Support

When the user is unable to continue to the captive portal due to the browser’s securing warning, it is most likely the website requested uses a stricter protocol, **HSTS** or **HTTP Strict Transport Security**. Both Google and Facebook is already using HSTS and many users have Google set as their default homepage. On browsers like Google Chrome, redirecting from websites that use HSTS will be shown the following security warning and users are not allowed to proceed. **Chrome’s warning now includes the hint of a Wi-Fi sign-in screen.**

Users will be forced to enter a HTTP website manually to be redirected to the Captive Portal successfully.
If the users visit a HTTPS webpage that does not use HSTS, the browser may allow the user to proceed after displaying a security warning.

**Chrome Browser**

![Chrome Browser Certificate Security Alert with non HSTS website.](image)

**Firefox Browser**

![Firefox Browser Captive Portal Detection with HSTS website](image)

Venues providing a Wi-Fi Hotspot will likely encounter the situation where their customer and users come across the various warning messages displayed on their preferred browsers.
Since controlling which browser the customer uses is out of the question, the issue can be resolved by simply informing the user to access an HTTP website.

All that is required to be redirected to the Captive Portal is an HTTP request.

Many hotels and venues offer instructions for their guests to connect to the Wi-Fi service such as the following example.

```
Free Wi-Fi Service

In order to access Wi-Fi, please proceed to the login process by following the 3 instructions below.

1. Connect to the WiFi SSID: Free Wi-Fi.
2. Allow your smartphone or laptop to automatically open up the captive portal. If your device does not automatically open up the captive portal, please manually open your preferred browser and access a HTTP webpage such as http://abcnews.go.com/.
3. Log in through the Captive Portal to gain access to the internet.
```

As advances in mobile devices supporting Captive Portal redirection continue to expand so will technological advances in the way Captive Portals are redirected. Controller will continue to provide the latest solutions to further enhance user’s Wi-Fi experience.
4.2 Automatic Captive Portal Pop-up Support

3.42.00 firmware release new feature - WISPr User Agent Support.

Some devices require a different response from the network to prompt their Captive Portal detection mechanism. Controller has updated its built-in list of user agents specifically to allow legacy devices or devices with a different captive portal detection method to prompt for one automatically.

**User Agents** are information such as the browser and operating system that is passed to the website. Many vendors will use these user agents for captive portal detections when their devices connect to a Wi-Fi network.

CaptiveNetworkSupport – Apple iOS
SamsungBrowser – Samsung Android OS
Dalvik – Android OS

This support can reduce the inconveniences such as false certification security alerts by leveraging the built-in captive portal detection in the device’s Operating System.

The following list of User Agents are included in hotspot gateway controllers.
- ipassconnect
- cdma+wlan
- skype wispr
- boingo client
- CaptiveNetworkSupport
- SamsungBrowser
- Dalvik

Note: The list of user agents is continuously updated to further improve the Wi-Fi experience.
4.3 HTTPS Automatic Redirects

3.42.00 firmware release new feature - HTTPS Automatic Redirects.

Controller’s HTTPS Automatic Redirect User Interface

Enable: Default – Allow HTTPS Traffic to be redirected to the Captive Portal prior to authentication.

Disable: Block all HTTPS traffic prior to authentication.

HTTPS Automatic Redirects provides an option for allowing or denying HTTPS requests when a user first connects to a network. When enabled, HTTPS traffic will be redirected but may prompt a certificate security warning. When HTTPS is disabled, all HTTPS traffic is denied and will be timed-out. This option will effectively prevent all security warnings being shown on the user’s devices. When HTTPS requests are timed-out, some browsers may automatically request a HTTP webpage to redirect to a Captive Portal.

5. Remarks

For more information, please contact our Technical Support team.
Appendix

Ubiquiti
When HTTPS Redirection is Enabled, users browsing with HTTPS may be shown a certificate security alert when browsing before they access the Captive Portal.
When HTTPS Redirection is Disabled, users browsing with HTTPS will be timed-out, meaning their webpage will appear blank since they never reach their destination.

Cisco Meraki
When “Block all access until sign-on is complete” is selected as Cisco Meraki’s Captive portal strength, both HTTP and HTTPS browsing will be redirected to the Captive Portal page. This means that HTTPS requests may be displayed with certificate security alerts.
When “Allow non-HTTP traffic prior to sign-on” is selected, all HTTPS websites are allowed for browsing even though the user have not accepted the disclaimer page or completed the sign-in process on the Captive Portal.