Contents

Introduction

This document describes the configuration about the web authentication redirection over HTTPS. This is a feature introduced in Cisco Unified Wireless Network (CUWN) release 8.0.

Prerequisites

Requirements

Cisco recommends you have knowledge of these topics:

- Basic Knowledge of Wireless LAN Controller (WLC) Web-authentication
- How to configure the WLC for Web-authentication.

Components Used

The information in this document is based on Cisco 5500 Series WLC that runs CUWN firmware version 8.0.

> **Note**: The configuration and web-auth explanation provided in this document is applicable to all WLC models and any CUWN image equal to or later than 8.0.100.0.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

Web authentication is a Layer 3 security feature. It blocks all the IP/data traffic, except DHCP-related packets/ DNS-related packets, from a particular client until a wireless client has supplied a valid username and password.Web authentication is typically used by customers who want to deploy a guest-access network.Web authentication starts when the controller intercepts the first

TCP HTTP (port 80) GET packet from the client.

In order for the client's web browser to get this far, the client must first obtain an IP address, and do a translation of the URL to IP address (DNS resolution) for the web browser. This lets the web browser know which IP address to send the HTTP GET. When the client sends the first HTTP GET to TCP port 80, the controller redirects the client to https:<virtual IP>/login.html for processing. This process eventually brings up the login web page.

Prior to releases earlier than CUWN 8.0 (i.e up to 7.6), if the wireless client presents an HTTPS page (TCP 443), the page is not redirected to the web-authentication portal. As more and more websites begin to use HTTPS, this feature is included in releases CUWN 8.0 and later. With this feature in place, if a wireless client tries https://<website>, it is redirected to the web-auth login page. Also this feature is very useful for the devices that send https requests with an application (but not with a browser).

Certificate Error

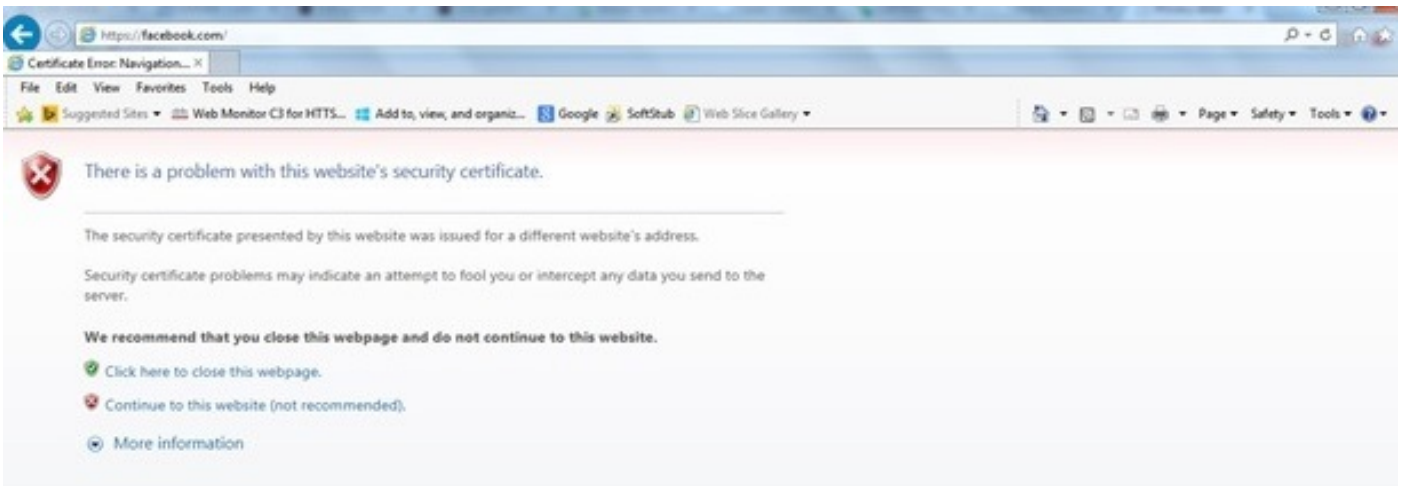
The warning message "certificate is not issued by a trusted certificate authority." appears on the browser after you configure the https-redirect feature. This is seen even if you have a valid root or chained certificate on the controller as shown in Figure 1 and Figure 2. The reason is that the certficiate you installed on the controller is issued to your virtual IP address.

> **Note**: If you try an HTTP-redirect and have this certifcate on the WLC, you do not get this certificate warning error. However in the case of HTTPS-redirect, this error appears.

When the client tries HTTPS://<web-site> , the browser expects the certificate issued to the IP address of the site resolved by the DNS. However, what they receive is the certificate that was issued to the internal web server of the WLC (virtual IP address) which causes the browser to issue the warning. This is purely because of the way HTTPS works and always happens if you try to intercept the HTTPS session in order for web-auth redirection to work.

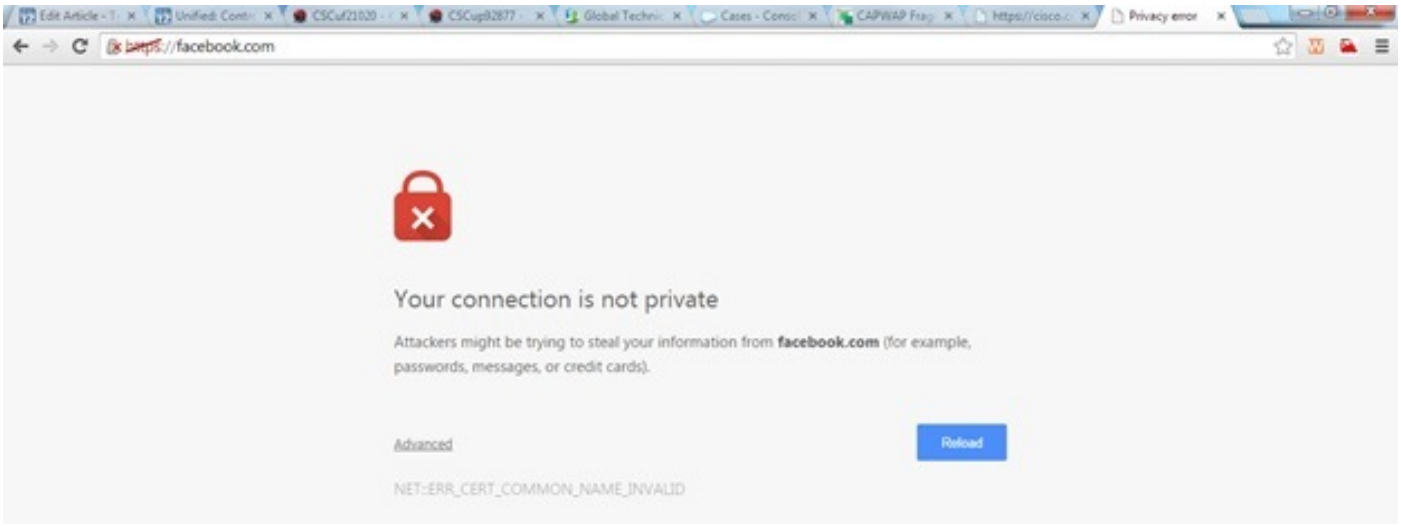
You might see different certificate error messages in different browsers but all relate to the same problem as previously described.

Figure 1



This is an example of how the error can appear in Chrome:

Figure 2



Configure

Configure the WLC for HTTPS-Redirection

This configuration assumes that the Wireless LAN (WLAN) is alraedy configured for the Layer 3 Web authentciation security. In order to enable or disable HTTPS redirect on this Web-auth WLAN:

```
(WLC)>config wlan security web-auth enable 10
(WLC)>config network web-auth https-redirect enable
WARNING! - You have chosen to enable https-redirect.
This might impact performance significantly
```

As the example configuration shows, this might impact throughput for an HTTPS redirection but not HTTP redirection

For more information and a configuration of the web authentication WLANs, see Web Authentication on WLAN Controller.

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) supports certain **show** commands. Use the Output Interpreter Tool in order to view an analysis of **show** command output.

```
(WLC)>show network summary

Web Auth Secure Web ..................... Enable
Web Auth Secure Redirection ............. Enable
```

1. Enable these debugs: `(WLC) debug client <MAC address>`

   `(WLC)> debug web-auth redirect enable`
2. Verify the debugs: `(WLC) >show debug`

```
MAC Addr 1.............................. 24:77:03:52:56:80

Debug Flags Enabled:
webauth redirect enabled.
```

3. Associate the client to the web-auth enabled SSID.
4. Look for these debugs:
```
*webauthRedirect: Jan 16 03:35:35.678: 24:77:3:52:56:80- received
connection.
client socket = 9
*webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- trying to read on socket 95
*webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- calling parser with bytes = 204
*webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- bytes parsed = 204
*webauthRedirect: Jan 16 03:35:35.679: captive-bypass detection enabled,
checking for wispr in HTTP GET, client mac=24:77:3:52:56:80
*webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Preparing redirect
URL according to configured Web-Auth type
*webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- got the hostName
for virtual IP(wirelessguest.test.com)
*webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Checking custom-web
config for WLAN ID:10
*webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Global status is
enabled, checking on web-auth type
*webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Web-auth type Customized,
using URL:https://wirelessguest.test.com/fs/customwebauth/login.html
```
Note: Ensure that either Secure web (config network secureweb enable/disable) or web-auth secure (config network web-auth secureweb enable/disable) are enabled in order to make the HTTPS redirect work. Also note that there might be a slight reduction in the throughput when redirection over HTTPS is used.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.