External Captive Web Portal Guide

For ExtremeCloud IQ

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

Published: November 2023

Extreme Networks, Inc.

Phone / +1 408.579.2800

Toll-free / +1 888.257.3000

www.extremenetworks.com

P/N 9037987-00 – Rev AB

Contents

Prerequisites

Before implementing External Captive Web Portal (CWP) authentication methods, the following prerequisites must be in place to ensure a smooth and secure network access experience.

Prerequisites	Description
Network Infrastructure	A functional network infrastructure with configured Access Points (AP) and Remote Authentication Dial-In User Service (RADIUS) servers for RADIUS-based authentication.
External Authentication Server	An external authentication server is essential for External CWP with External RADIUS Authentication and External CWP with External Authentication. Configured the external authentication server to process and authenticate user credentials.
Captive Web Portal Setup	Must be configured to ensure that it can interface with the external authentication server.
User Credential Database	An accessible database of user credentials, maintained by the external server for authenticating users.
HTTP Support	As External CWP with External RADIUS Authentication and External CWP with External Authentication involve Hypertext Transfer Protocol (HTTP) POST requests, ensure that the network environment supports HTTP communication.
Security Policies	Defined security policies that govern the access control rules, data encryption, and security measures for the network.
Understanding Authentication Protocols	Familiarity with the following authentication protocols is crucial for configuring and troubleshooting the authentication process: • RADIUS • Password Authentication Protocol (PAP) • Challenge Handshake Authentication Protocol (CHAP) • Microsoft Challenge Handshake Authentication protocol Version 2 (MSCHAPv2) • HTTP Used with an Open Service Set Identifier (SSID) and provides access based on user credentials.

Introduction

External CWP is a vital component in the network security and access control ecosystem. CWP portals are gateways to network resources and are the first point of contact for users seeking access to Wi-Fi networks.

To fortify user network access, Extreme Networks uses various authentication methods, depending on security and user experience requirements.

The following methods offer distinct approaches to verifying user credentials and ensuring network security:

- External CWP with External RADIUS Authentication
- External CWP with External Authentication.

In this guide, we delve into the intricacies of these authentication methods, shedding light on how they operate and their respective advantages. By understanding these authentication processes, organizations can make informed decisions on the most suitable approach for their specific network environments, enhancing both security and user convenience.

Join us on this journey to uncover the inner workings of these authentication methods and their applications in today's network security landscape.

Note

For specific integration projects, contact the Extreme Professional Services Team at https://www.extremenetworks.com/services

Authentication Options

The following work flow describes how an External (CWP) is used along with External RADIUS Authentication.

These two methods of external captive web portal authentication provide flexibility in how user credentials are collected and verified. Organizations can choose the method that best aligns with their security and user experience requirements.

External CWP with External RADIUS Authentication

- The external server displays a login form: When a user attempts to access a network, an external server provides a login form. The login form prompts the user to input their credentials, typically a username and password.

- User credentials sent to AP with HTTP POST: When the user submits their credentials, the AP transmits the details from the external server to the AP using the HTTP POST method. The AP, in this context, acts as a RADIUS client.

- AP as a RADIUS client (PAP/CHAP/MSCHAPv2): The AP deploys the following authentication protocols to verify the user's identity:

    - PAP
    - CHAP
    - MSCHAPv2

The RADIUS client checks user credentials against the RADIUS server for authentication.

The authentication process is different for an External CWP with External Authentication.

External CWP with External Authentication (**)

- The external server displays a login page: An external server provides a login page for users who wish to access the network. The login page requests the user's credentials.

- User credentials sent back to the external web server: After the user enters their credentials, the server sends back the user credentials to the external web server. AP does not handle the user authentication process. The server processes user authentication externally.

- User authentication is processed on an external server: The external server is responsible for processing and verifying the user's authentication details. The external server checks user credentials against its database or authentication mechanisms to determine if the user is authorized to access the network.

- External server passes back success or failure code with HTTP POST: When user credentials are authenticated, the external server communicates the result back to the user's device and the AP using the HTTP POST method. The server sends a success or failure code based on the authentication outcome.

(**) Requires a command that only be set from the client.

Considerations

Walled Garden

When implementing a Walled Garden, to ensure a seamless and secure user experience, keep the following crucial factors in mind:

- Allows access to specific sites before authentication: A Walled Garden setup permits users to access predetermined websites before they complete the authentication process. The Walled Garden feature is particularly useful for presenting essential information or terms of use to users when they first connect.
- Up to 64 IP addresses per SSID: To accommodate various user devices and facilitate network access, a Walled Garden accommodates up to 64 IP addresses per Service Set Identifier (SSID), allowing multiple devices to connect simultaneously.

Encryption

Ensuring data security and privacy is of paramount importance. Here are encryption considerations for a robust network:

- Use HTTPS for all communication between the client, AP and the external web server: Employing Hypertext Transfer Protocol Secure (HTTPS) for all data exchange between the client device, AP, and external web server is fundamental. This encryption protocol safeguards data during transmission, providing protection against eavesdropping and data manipulation.
- User credentials are passed in an HTTP POST: When transmitting user credentials, it is essential to use an HTTP POST method. An HTTP POST method enhances the security of data transmission, preventing credentials from being exposed in the URL.
- Success and failure codes are passed in an HTTP POST: To maintain data integrity, transmit success and failure codes, indicating the outcome of the authentication process, through an HTTP POST.
- Universal Access Method (UAM) for passwords is available if HTTPS is not desired: For cases where HTTPS is not the preferred option, use UAM as an alternative for handling passwords. However, HTTPS is generally recommended for stronger security.

Login Success and Failure Pages

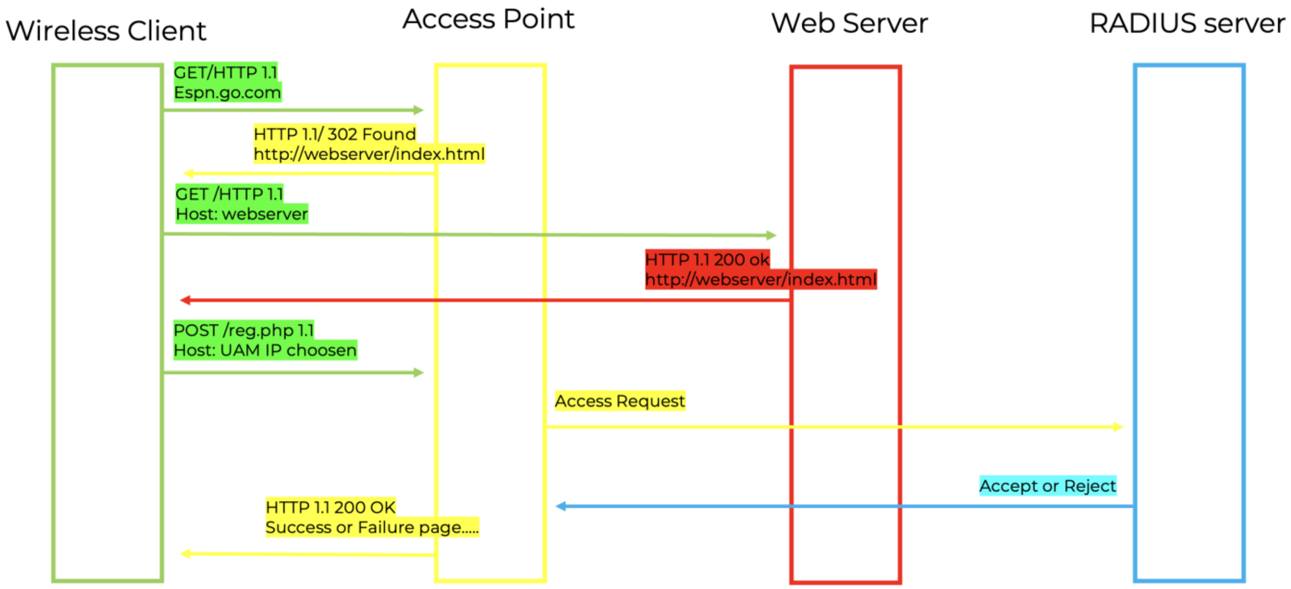
Login success and failure messages are a crucial part of the user experience, and flexibility is key.

Login success and failure pages can be hosted locally on the AP or externally: Hosting login success and failure pages locally allows for quick responses and customizability, while external hosting may be preferred for centralized management and consistent branding.

External CWP with External RADIUS Authentication

External Captive Web Portals play a vital role in securing network access and ensuring that only authorized users can connect to a network. When combined with External RADIUS Authentication, the authentication process gains an additional layer of security and flexibility.

This diagram illustrates a step-by-step process of how an External CWP with External RADIUS Authentication ensures secure network access for users.



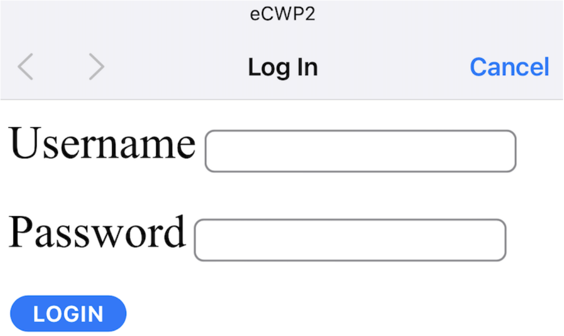
Web Form Example to Web Server

In this example, we create a simple contact form using HTML to illustrate the process of capturing user input and sending it to a web server.

This script demonstrates the essential steps involved in handling data from a web form.

```
<body>

<form name="weblogin" action="http://x.x.x.x/reg.php" id="logon" method="post">

<input type="hidden" name="url" value="any-value-here"/> <p>

<label for="username">Username</label>

<input class="input" type="text" id="username" name="username" /> </p>

<p>

<label for="password">Password</label>

<input class="input" type="text" id="password" name="password" />

</p>

<input type="submit" value="LOGIN" />

</form>

</body>
```

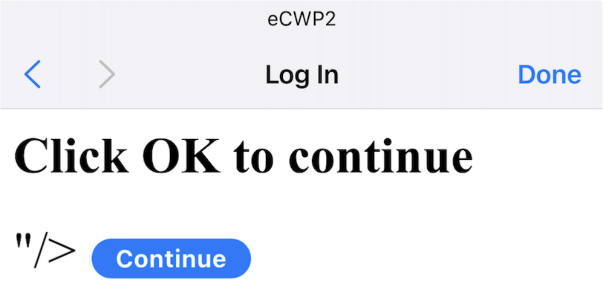
#NOTE: IP address used to UAM anyone(http://x.x.x.x/reg.php), for example, 10.10.10.1



Success or Failure Page Example

This script designs a web form using HTML to collect user information. After the user submits the form, the script determines whether the submission was successful or unsuccessful and redirects the user to the corresponding page.

```
<body>

<p><b>

<?php

    if ($_GET["autherr"] == “0")

        echo "Login Successful! ";

    else echo "Login Failed! "; ?>

Click OK to continue</b></p>

<form name="weblogin" action="http://x.x.x.x/reg.php" id="logon‟ method="post">

<input type="hidden" name="autherr" value="‟

    <?php   if ($_GET["autherr"] == “0")

        echo “0";  else  echo “1"; ?>    "/>

<input type="hidden" name="url" value="‟any-value-here"/>

<input type="submit" value="Continue" />

</form>

</body>
```

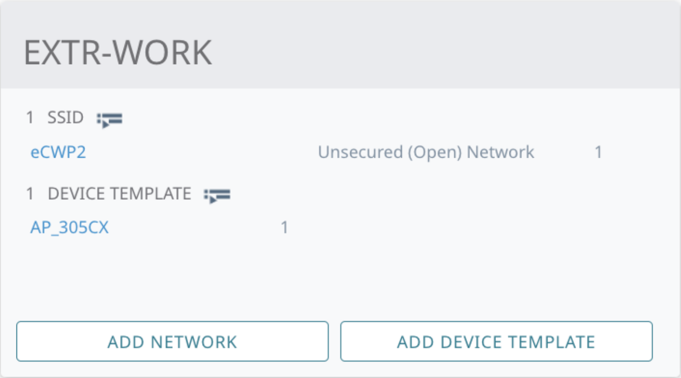


Click OK to continue

"/>

ExtremeCloudIQ Configuration – Enable Open SSID and Captive Portal

These images showcase ExtremeCloud IQ configuration options for enabling an Open SSID and customizing a CWP. Providing a powerful solution for managing network access and security.



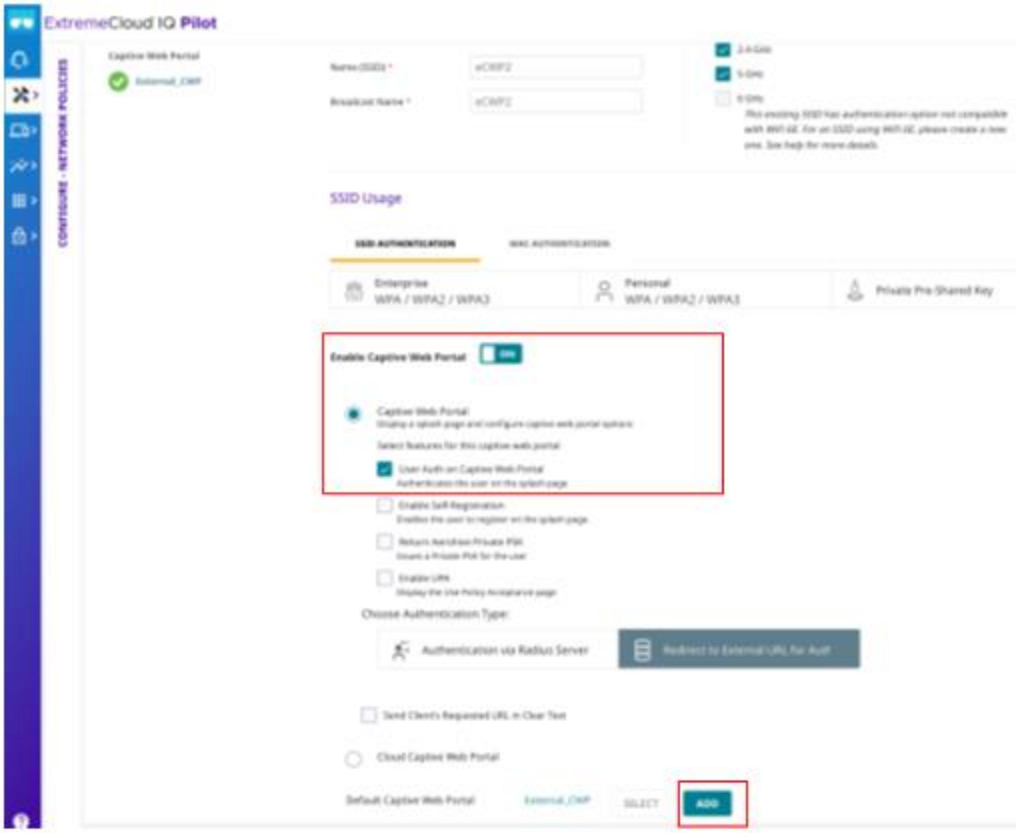
EXTR-WORK

1 SSID

eCWP2	Unsecured (Open) Network	1

1 DEVICE TEMPLATE

AP_305CX	1



ExtremeCloud IQ Pilot

CONFIGURE - NETWORK POLICIES

Captive Web Portal: External_CWP

Name (SSID) *: eCWP2

Broadcast Name *: eCWP2

☑ 2.4 GHz
☑ 5 GHz
□ 6 GHz

This existing SSID has authentication option not compatible with WiFi 6E. For an SSID using WiFi 6E, please create a new one. See help for more details.

SSID Usage

SSID AUTHENTICATION | MAC AUTHENTICATION

Enterprise WPA / WPA2 / WPA3 | Personal WPA / WPA2 / WPA3 | Private Pre-Shared Key

Enable Captive Web Portal: ON

● Captive Web Portal
Display a splash page and configure captive web portal options

Select features for this captive web portal

☑ User Auth on Captive Web Portal
Authenticates the user on the splash page

□ Enable Self-Registration
Enables the user to register on the splash page

□ Return Aerohive Private PSK
Issues a Private PSK for the user

□ Enable UPA
Display the Use Policy Acceptance page

Choose Authentication Type:

Authentication via Radius Server | Redirect to External URL for Auth

□ Send Client's Requested URL in Clear Text

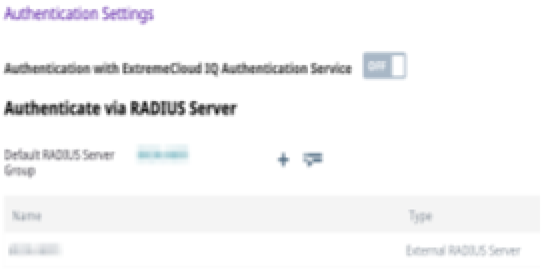
○ Cloud Captive Web Portal

Default Captive Web Portal: External_CWP

ExtremeCloudIQ Configuration – Define Radius Server

This image provides an insight into the ExtremeCloudIQ configuration interface, specifically focusing on the crucial step of defining a RADIUS server.

RADIUS servers play a pivotal role in network security and access control by centralizing user authentication and authorization processes.



Authentication Settings

Authentication with ExtremeCloud IQ Authentication Service OFF

Authenticate via RADIUS Server

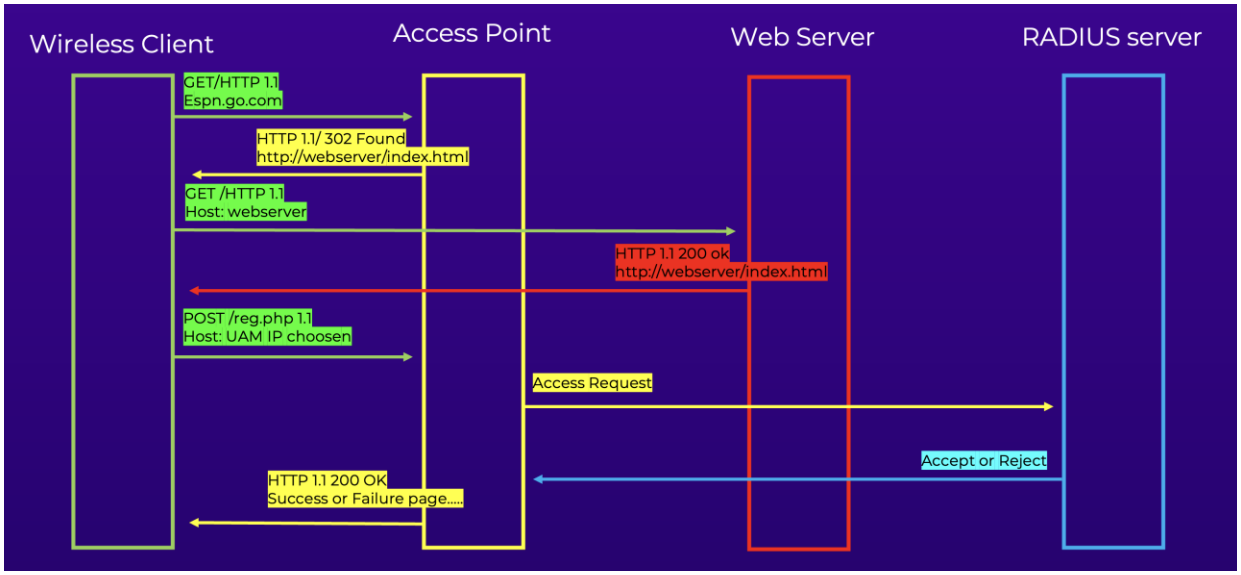
Default RADIUS Server Group [redacted]

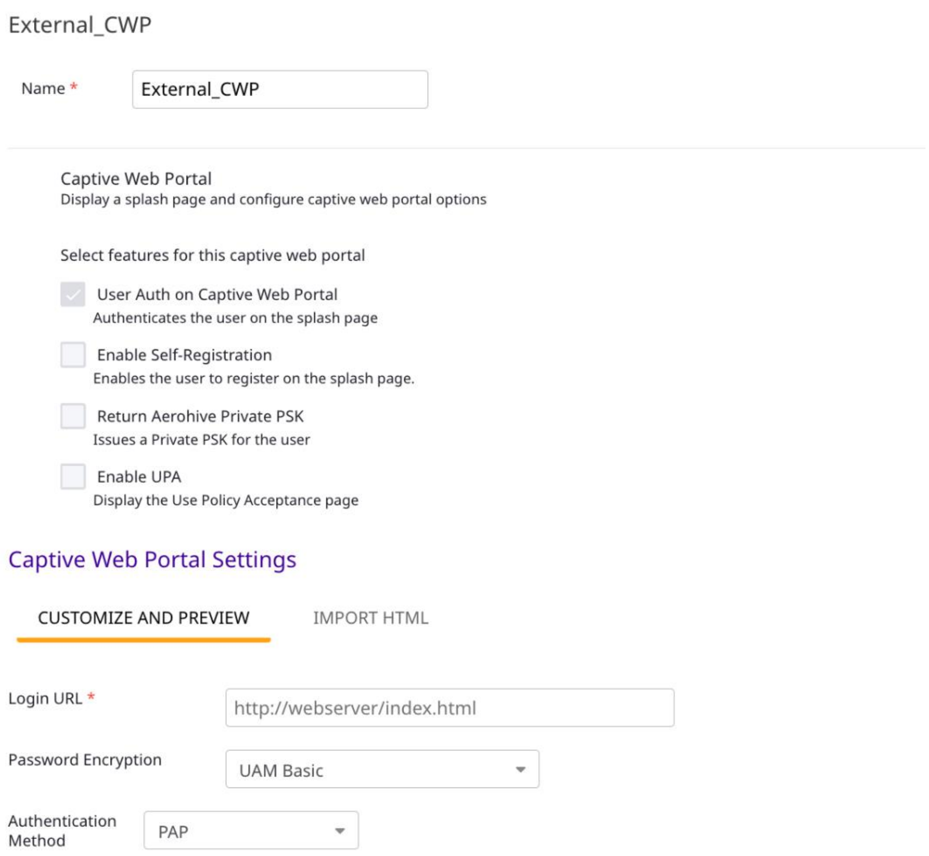
Name	Type
[redacted]	External RADIUS Server

Captive Web Portal Configuration

This image offers a comprehensive overview of CWP configuration within ExtremeCloud IQ. Captive web portals are essential tools for controlling network access, engaging users, and safeguarding network security.

This image highlights key aspects of configuring a CWP in ExtremeCloud IQ.





External_CWP

Name * External_CWP

Captive Web Portal
Display a splash page and configure captive web portal options

Select features for this captive web portal

☑ User Auth on Captive Web Portal
Authenticates the user on the splash page

□ Enable Self-Registration
Enables the user to register on the splash page.

□ Return Aerohive Private PSK
Issues a Private PSK for the user

□ Enable UPA
Display the Use Policy Acceptance page

Captive Web Portal Settings

CUSTOMIZE AND PREVIEW | IMPORT HTML

Login URL * http://webserver/index.html

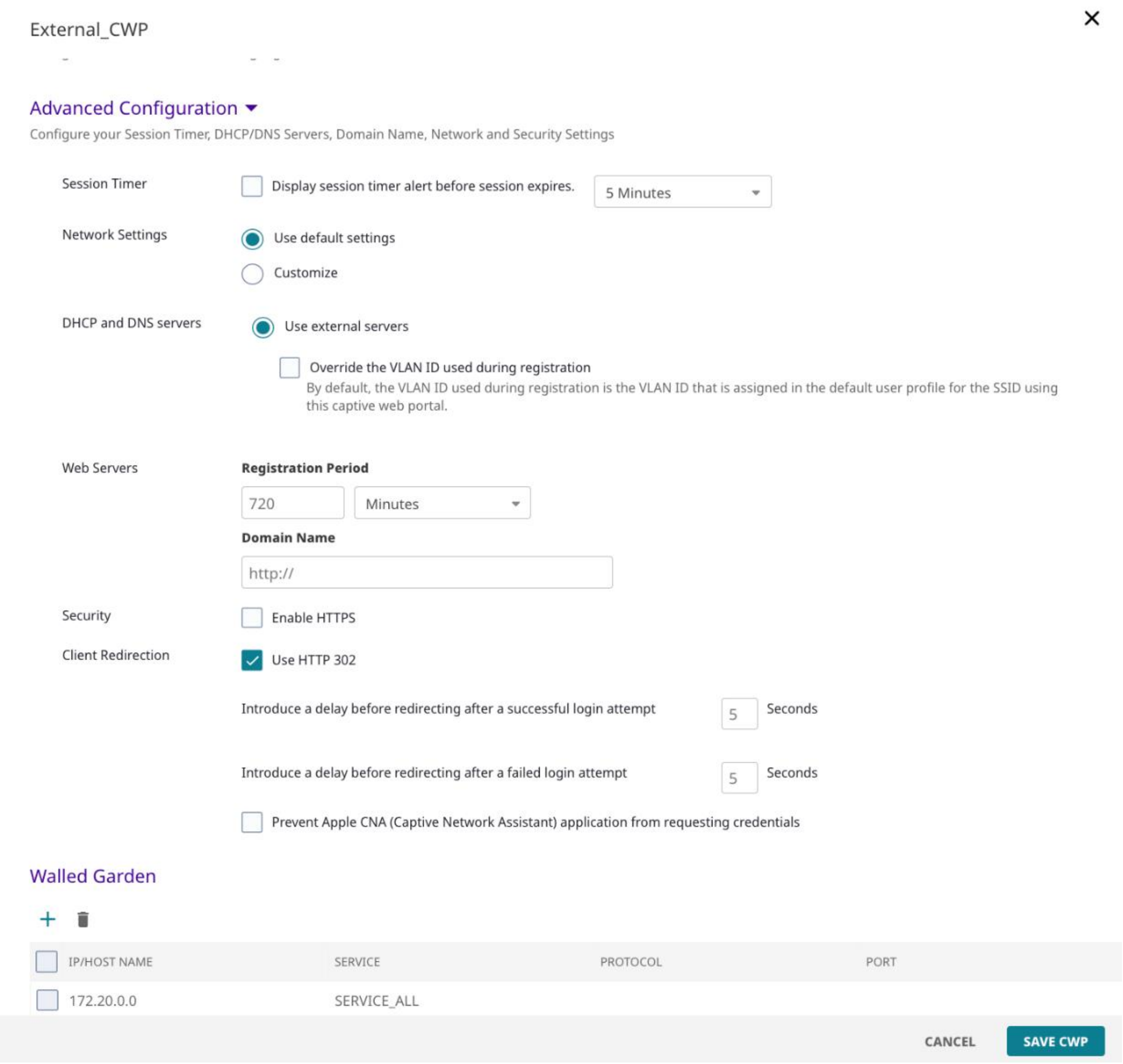
Password Encryption: UAM Basic

Authentication Method: PAP

Advanced Configuration and Walled Garden

This image provides insights into the Advanced Configuration and Walled Garden features in the ExtremeCloud IQ platform. Advanced Configuration options and Walled Garden settings are essential components for optimizing network control and enhancing user experience.

This image highlights key elements of configuring advanced network features in ExtremeCloud IQ.



External_CWP

Advanced Configuration

Configure your Session Timer, DHCP/DNS Servers, Domain Name, Network and Security Settings

Session Timer: □ Display session timer alert before session expires. 5 Minutes

Network Settings: ● Use default settings ○ Customize

DHCP and DNS servers: ● Use external servers

□ Override the VLAN ID used during registration

By default, the VLAN ID used during registration is the VLAN ID that is assigned in the default user profile for the SSID using this captive web portal.

Web Servers:

Registration Period 720 Minutes

Domain Name http://

Security: □ Enable HTTPS

Client Redirection: ☑ Use HTTP 302

Introduce a delay before redirecting after a successful login attempt 5 Seconds

Introduce a delay before redirecting after a failed login attempt 5 Seconds

□ Prevent Apple CNA (Captive Network Assistant) application from requesting credentials

Walled Garden

IP/HOST NAME	SERVICE	PROTOCOL	PORT
172.20.0.0	SERVICE_ALL		

Note

Pay attention to the Client Domain Name System(DNS), Dynamic Host Configuration Protocol (DHCP) and CWP connectivity.

UAM Basic

UAM Basic refers to User Authentication Management Basic. UAM Basic signifies a fundamental authentication mechanism commonly used in CWP setups and public Wi-Fi networks.

This is an example of a captured webserver.

```
"GET/index.html?url=E2B8F3578D88E9B12396E14E98920F99D23B13921837C9FDC99F85D14F238887A7
A8E253D2C4B2FC2A92F84B8&ssid=eCWP2&mac=663967462243&autherr=0&challenge=3579DD1819624
DA8CF210D0D75C7B171&Called-Station-Id=bcf3100069e4&NAS-IP-Address=198.18.32.1&RADIUS-NAS-
IP=172.20.0.127&Calling-Station-Id=663967462243&STA-IP=172.20.0.121&NAS-ID=AP305CX-
ALP&MGT-MAC-Address=bcf3100069c0 HTTP/1.1" 200 585 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS
17_0_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148"
```

Systems Version

Accurately tracking and managing software versions across various components is of paramount importance. Whether in ExtremeCloud IQ, APs, or wireless clients, staying up-to-date with the latest software versions is crucial for optimizing performance, security, and functionality.

This is the version used in this lab.

For Example,

ExtremeCloud IQ

Build ID: 2023-10-04-20.13.40
Build Version: 23.6.0.48

Access Point

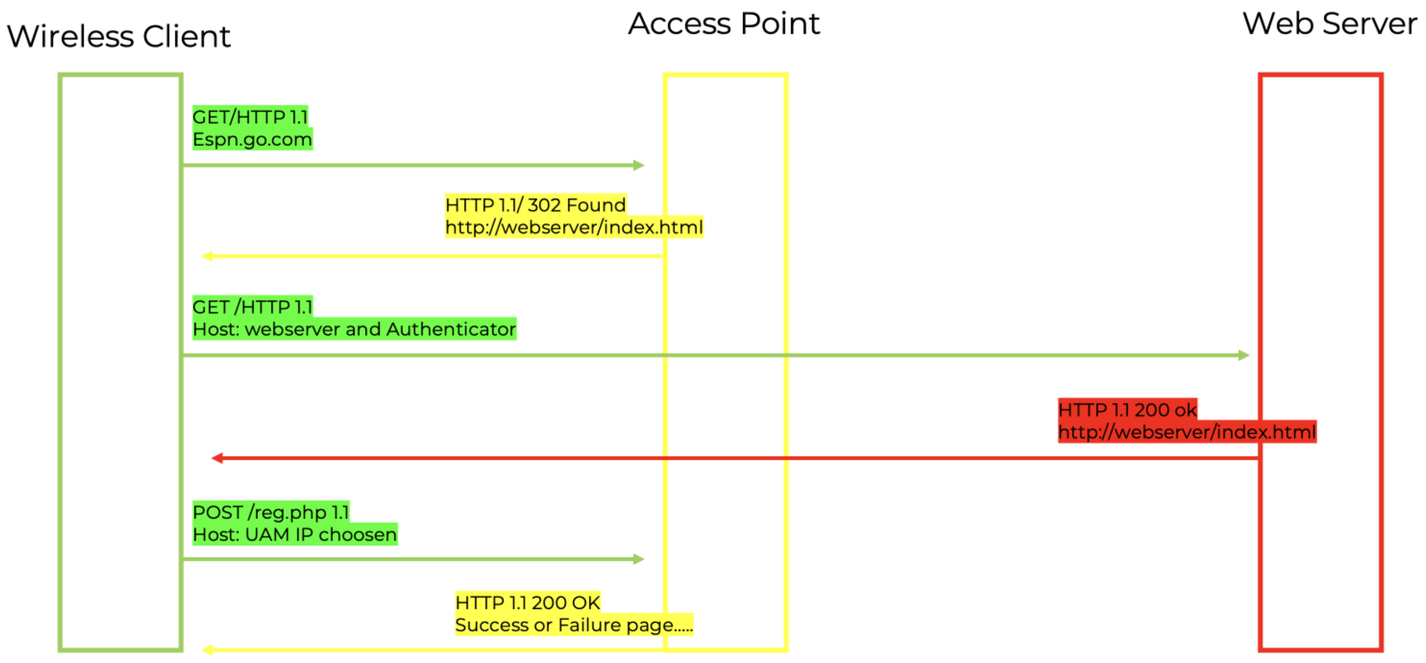
IQ Engine 10.6.1.0

Wireless clients

iOS 17.0.3
Android 13 Knox 3.9
MAC OS Sonoma 14.0

External CWP with External Authentication

The diagram shows the External CWP with the External Authentication process, a configuration commonly used in network setups to ensure secure user authentication and controlled access to network resources.



Requires a command that can only be set from the Command-line Interface (CLI), normally used in the Supplemental CLI:

security-object <SSID-Name> security additional-auth-method captive-web-portal external-server primary no-radius-auth

In this configuration, an external web server hosts the CWP, allowing users to enter their credentials for authentication. The external web server handles the authentication process and communicates the result to the CWP, which then determines whether to grant access. This setup offers flexibility in the choice of authentication methods and allows for a customized user experience. External authentication is a common choice where user data is managed externally, and network access control is crucial for security and compliance.