



## How to Cisco external web authentication

Bo Nielsen, CCIE #53075 (Sec)

Oktober 2016, V1.00

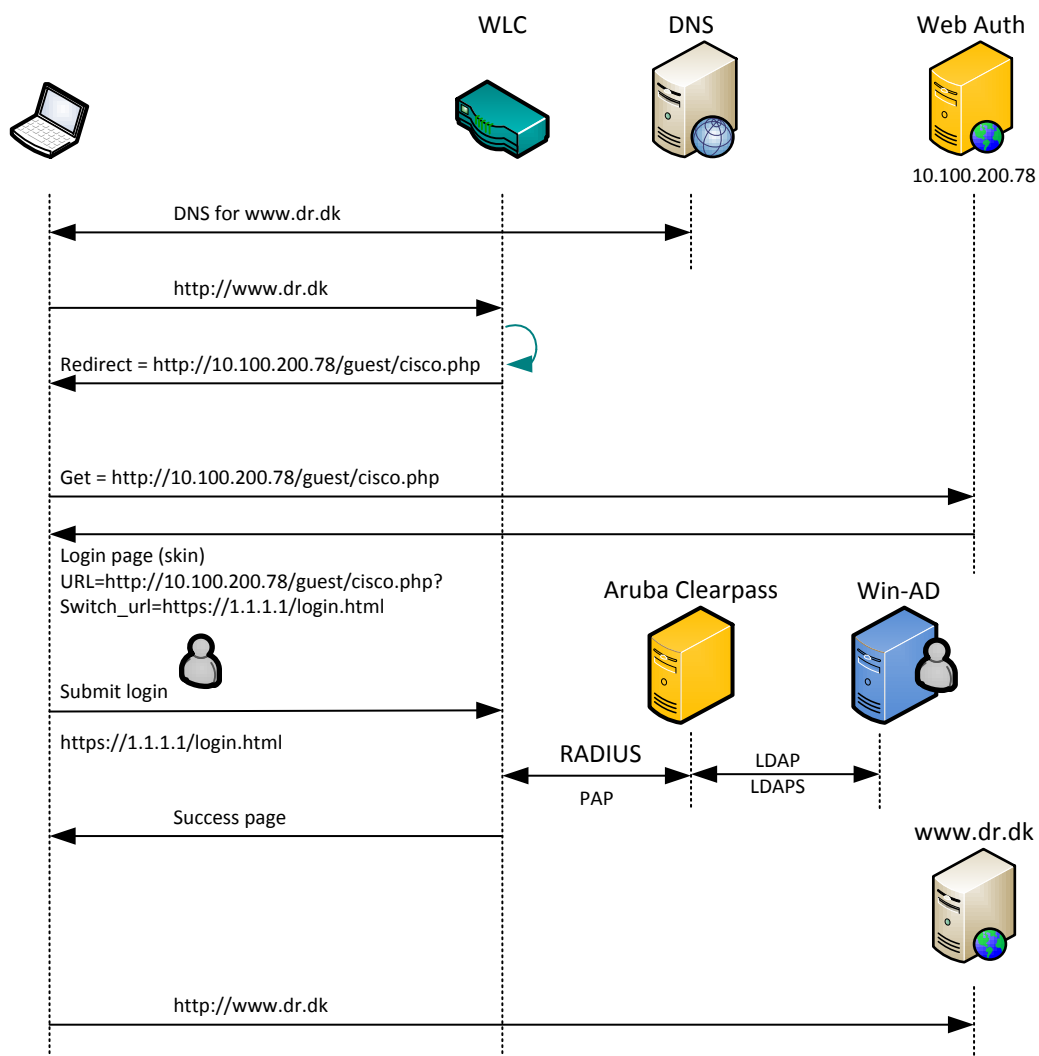
## Overview

The principle is that the user connects to a wireless network, and the network must be open. An open network with captive portal always starts with providing access to the network with an IP address, and in this phase DNS implicitly allowed. The principle is to make an http-redirect at the first http-request, and here the WLC will spoof the original destination IP address, and the browser think that it communicates with the requested web page.

Redirect http on Cisco WLC is either to a local web page or to an external web page.

In both cases the web page must guide the user's web browser to send the login credentials to the virtual interface (1.1.1.1). When login is delivered as https and the authentication may be made locally from WLC itself or via a RADIUS. With RADIUS the login can be approved by Windows AD.

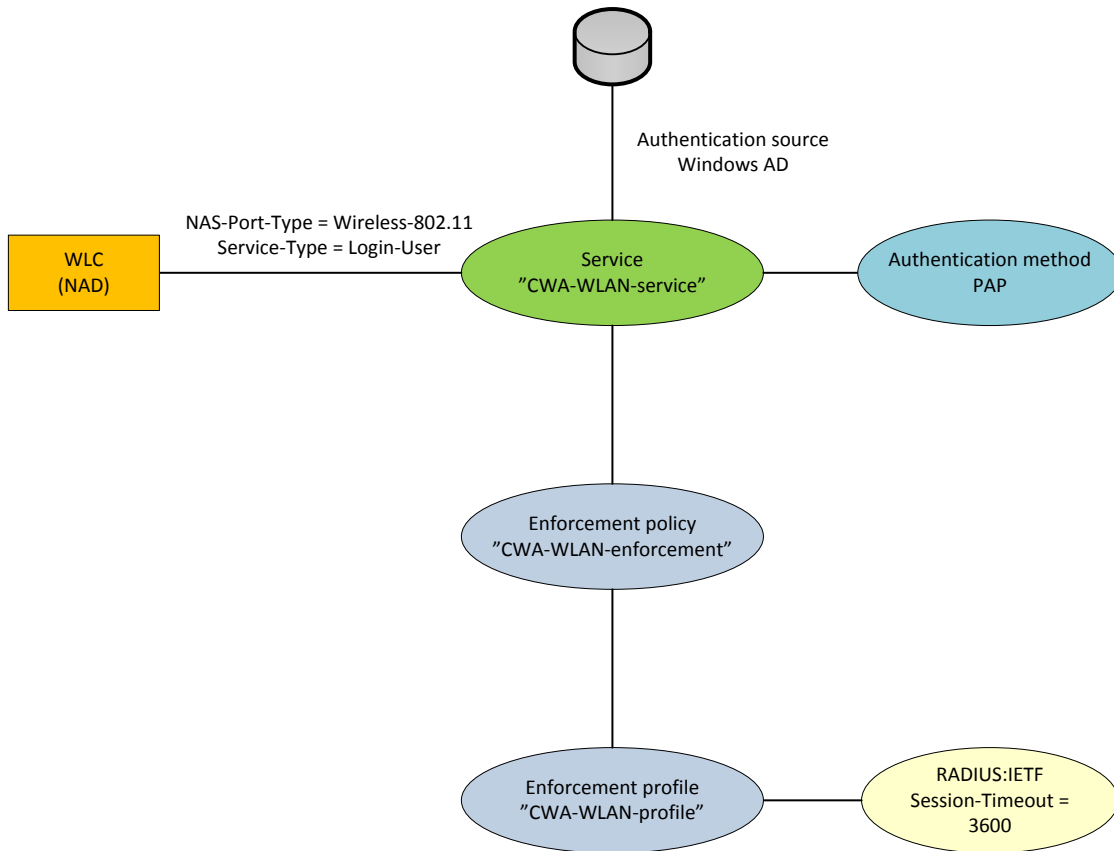
The process of external web authentication is illustrated here:



For authentication via RADIUS the Cisco WLC by default uses PAP and can be set to either PAP, CHAP or MD5-CHAP under *Security -> General*.

## Aruba Clearpass

An overview of the service rule, enforcement policy and enforcement profile is:



The enforcement profile uses the attribute *Session-Timeout* to set the timer for the session.

The session time is stored on the Cisco WLC after successful authentication.

In this example the session-timeout is set to 1 hour (3600s), and the user is approved for 1 hour. When reaching 1 hour the captive portal is displayed again, and the user must re-enter their login.

In practice the session timeout can be set to a higher value than 1 hour.

On Aruba Clearpass the configuration tasks are:

1. Authentication source from Windows AD.
2. Enforcement profile
3. Enforcement policy to set the session timeout
4. Service rule with authentication source, authentication method and enforcement policy

## Enforcement profile

Configuration -> Enforcement -> Profiles

### Enforcement Profiles - CWA-WLAN-profile

Summary	Profile	Attributes
<b>Profile:</b>		
Name:	CWA-WLAN-profile	
Description:	Timeout = 3600	
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	
<b>Attributes:</b>		
Type	Name	Value
1. Radius:IETF	Session-Timeout	= 3600

## Enforcement policy

Configuration -> Enforcement -> Policies

### Enforcement Policies - CWA-WLAN-enforcement


Summary	Enforcement	Rules
<b>Enforcement:</b>		
Name:	CWA-WLAN-enforcement	
Description:		
Enforcement Type:	RADIUS	
Default Profile:	[Deny Access Profile]	
<b>Rules:</b>		
Rules Evaluation Algorithm:	Evaluate all	
Conditions	Actions	
1. (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday)	CWA-WLAN-profile	

How to Cisco external web authentication

Service rule

Configuration -> Services

Services - CWA-WLAN-service

Summary	Service	Authentication	Roles	Enforcement
<b>Service:</b>				
Name:	CWA-WLAN-service			
Description:	Central Web Authentication service			
Type:	802.1X Wireless - Identity Only			
Status:	Enabled			
Monitor Mode:	Disabled			
More Options:	-			
<b>Service Rule</b>				
Match ALL of the following conditions:				
Type	Name	Operator	Value	
1. Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)	
2. Radius:IETF	Service-Type	EQUALS	Login-User (1)	
<b>Authentication:</b>				
Authentication Methods:	[PAP]			
Authentication Sources:	SARS-AD  Your external source			
Strip Username Rules:	-			

Services - CWA-WLAN-service

Summary	Service	Authentication	Roles	Enforcement
Use Cached Results:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions			
Enforcement Policy:	CWA-WLAN-enforcement			<a href="#">Add new Enforcement</a>
<b>Enforcement Policy Details</b>				
Description:				
Default Profile:	[Deny Access Profile]			
Rules Evaluation Algorithm:	evaluate-all			
Conditions	Enforcement Profiles			
1. (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday)	CWA-WLAN-profile			

## External web page on Aruba Clearpass

Configuration -> Pages - Web Logins

The screenshot shows the 'Web Login Editor' interface in Aruba ClearPass Guest. The left sidebar contains a navigation menu with 'Pages' expanded to 'Web Logins'. The main content area is titled 'Web Login (Cisco WLC)' and includes a breadcrumb trail: 'Home » Configuration » Pages » Web Logins'. Below the title, there is a note: 'Use this form to make changes to the Web Login Cisco WLC.' The configuration form has the following fields:

- \* Name:** Cisco WLC
- Page Name:** cisco
- Description:** Cisco external web authentication
- \* Vendor Settings:** Cisco Systems
- Login Method:** Controller-initiated — Guest browser performs HTTP form submit
- \* Address:** 1.1.1.1
- Secure Login:** Use vendor default
- The controller will send the IP to submit credentials

It is very important to select *The controller will send the IP to submit credentials*.

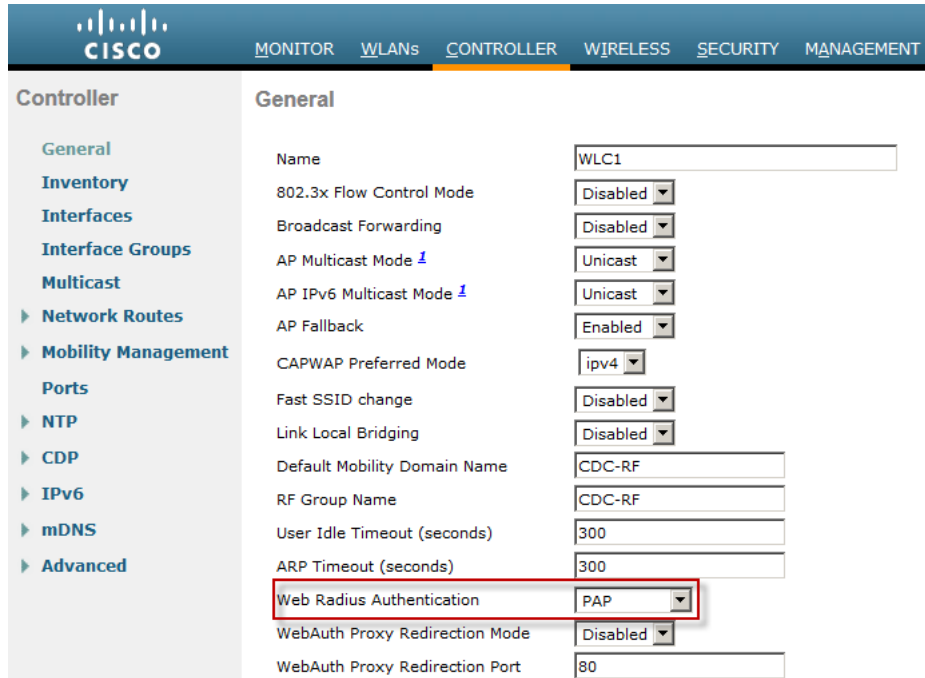
The screenshot shows the 'Login Form' configuration page in Aruba ClearPass Guest. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Login Form' and includes a breadcrumb trail: 'Home » Configuration » Pages » Web Logins'. Below the title, there is a note: 'Options for specifying the behaviour and content of the login form.' The configuration form has the following fields:

- Authentication:** Credentials – Require a username and password
- Prevent CNA:**  Enable bypassing the Apple Captive Network Assistant
- Custom Form:**  Provide a custom login form
- Custom Labels:**  Override the default labels and error messages
- Username Suffix:** (empty field)
- \* Pre-Auth Check:** None — no extra checks will be made
- Terms:**  Require a Terms and Conditions confirmation

## Cisco Wireless LAN Controller

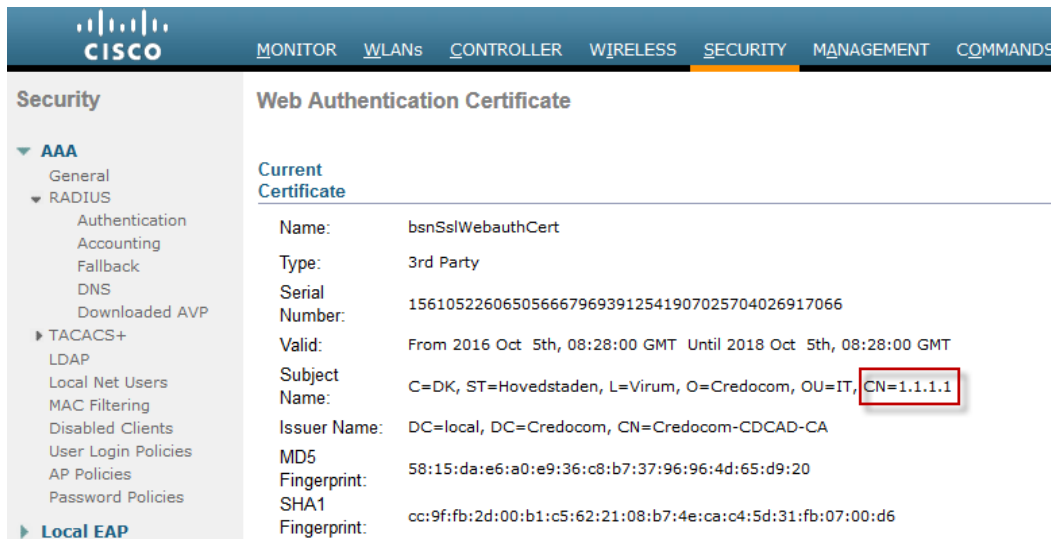
Start by checking that the Cisco WLC uses PAP.

Controller -> General



Next verification is that the installed certificate for Web Auth has the *common name* set to **1.1.1.1** or the certificate has the SAN field set to **1.1.1.1** as an IP address.

Security -> Web Auth -> Certificate

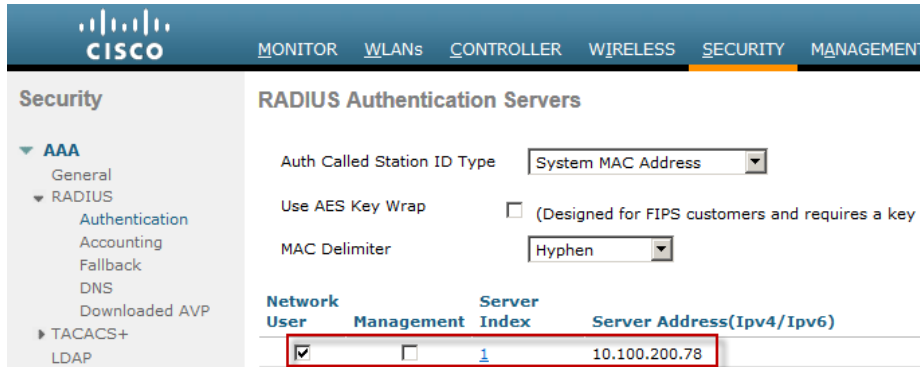


In this example I have used a certificate from an internal PKI, and it can be used for testing purpose only because the external users have not installed the root certificate from the internal PKI. In practice a public certificate should be used for example from Verisign, GoDaddy, DigiCert etc.

How to Cisco external web authentication

**Radius**

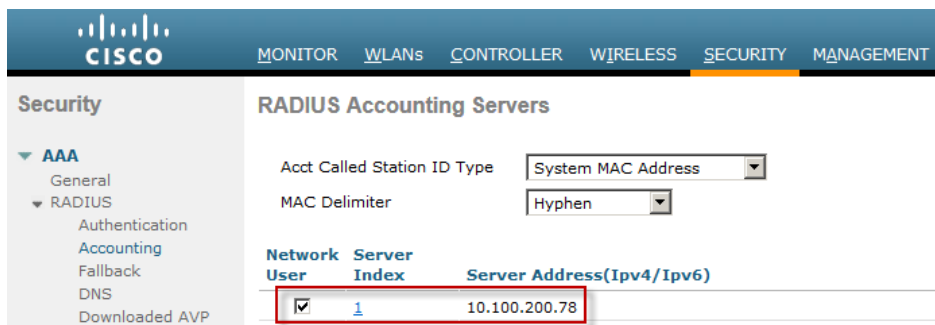
Security -> RADIUS -> Authentication



In this example the Aruba Clearpass is the radius of the IP address 10,100,200.78.

**Note:** The name of the SSID can not be used as a condition for a service rule on Aruba Clearpass, and this is because the Cisco WLC sends the index number of the SSID. If SSID index should be included in a service rule, then *Auth Called Station ID Type* must be changed to a type where the SSID index is included in RADIUS-request.

Security -> RADIUS -> Accounting



**Access Control Lists**

Security -> Access Control Lists - Access Control Lists

**General**

Access List Name: Pre-Auth-External-Web

Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 /	0.0.0.0 /	Any	Any	Any	Any	Outbound
2	Permit	0.0.0.0 /	0.0.0.0 /	UDP	Any	DHCP Server	Any	Inbound
3	Permit	0.0.0.0 /	10.100.200.78 /	TCP	Any	HTTP	Any	Inbound

The ACL gives access to the website on Aruba Clearpass and DHCP. DNS is allowed by the WLC.



## WLAN

In this example it is a setup with the SSID name *Ford*, and the management interface is used for WiFi clients and they obtain their IP address from this interface.

### General

General Security QoS Policy-Mapping Advanced

Profile Name: Ford

Type: WLAN

SSID: Ford

Status:  Enabled

Security Policies: Web-Auth  
(Modifications done under security tab will appear after ...)

Radio Policy: All

Interface/Interface Group(G): management

### Security (open SSID), Layer 2

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security: None

MAC Filtering:

Fast Transition:

### Security (Web Auth), Layer 3

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 3 Security: Web Policy

Authentication

Passthrough

Conditional Web Redirect

Splash Page Web Redirect

On MAC Filter failure<sup>10</sup>

Preauthentication ACL: IPv4: Pre-Auth-External-Web IPv6: None

Sleeping Client:  Enable

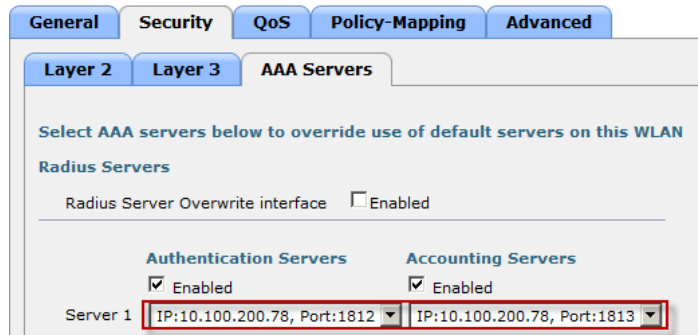
Over-ride Global Config:  Enable

Web Auth type: External(Re-direct to external server)

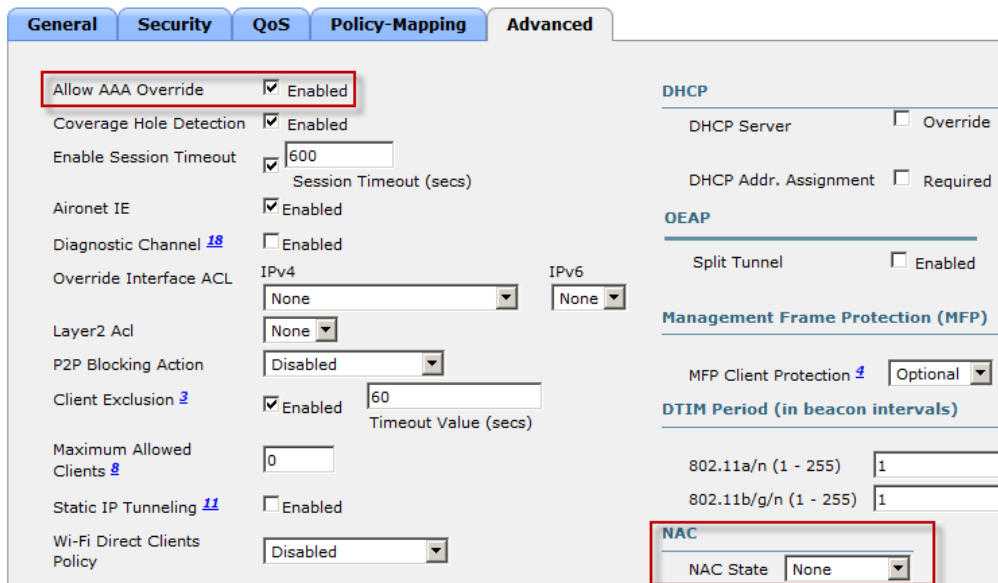
URL: http://10.100.200.78/guest/cisco.php

Pre Authentication ACL restricts traffic to Aruba Clearpass until the user is authenticated.

### Security (Radius), AAA Servers



### Advanced



It is important to select the *Allow AAA Override*. This causes the session-timeout from RADIUS to become the active session timer. If override not selected, the value for *Session Timeout* on the Cisco WLC (here 600) sets the session-timeout. For an open SSID the *NAC State* must be set to *None*.

### Redirect of https

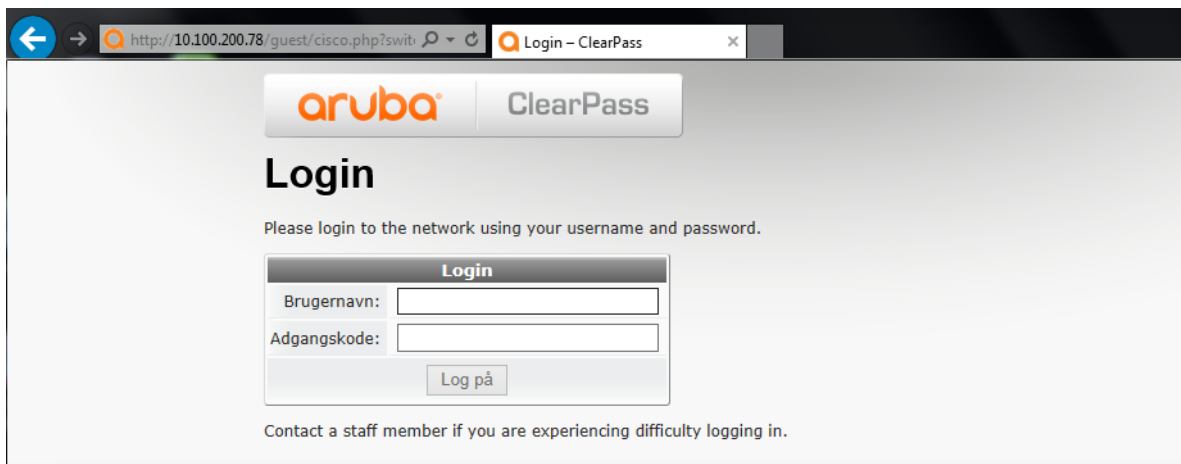
By default on Cisco WLC the redirect for https is disabled. You can enable https redirect with:

```
config network web-auth https-redirect enable
```

If selected there will always be a certificate warning because the DNS name in the URL does not match with the Cisco WLC certificate for Web Auth (default CN = 1.1.1.1).

## Verification

Before approval



Client Properties		AP Properties	
MAC Address	00:13:e8:80:f5:c5	AP Address	1c:6a:7a:89:d4:d0
IPv4 Address	10.100.200.227	AP Name	AP1c6a.7a86.78d4
IPv6 Address		AP Type	802.11g
		AP radio slot Id	0
		WLAN Profile	Ford
		WLAN SSID	Ford
		Data Switching	Central
		Authentication	Central
		Status	Associated
		Association ID	1
		802.11 Authentication	Open System
		Reason Code	1
		Status Code	0
		CF Pollable	Not Implemented
		CF Poll Request	Not Implemented
		Short Preamble	Implemented
		PBCC	Not Implemented
		Channel Agility	Not Implemented
		Timeout	600
		WEP State	WEP Disable
Client Type	Regular		
User Name			
Port Number	1		
Interface	management		
VLAN ID	0		
CCX Version	CCXv4		
E2E Version	E2Ev1		
Mobility Role	Local		
Mobility Peer IP Address	N/A		
Policy Manager State	WEBAUTH_REQD		
Management			

After approval

Client Properties		AP Properties	
MAC Address	00:13:e8:80:f5:c5	AP Address	1c:6a:7a:89:d4:d0
IPv4 Address	10.100.200.227	AP Name	AP1c6a.7a86.78d4
IPv6 Address		AP Type	802.11g
		AP radio slot Id	0
		WLAN Profile	Ford
		WLAN SSID	Ford
		Data Switching	Central
		Authentication	Central
		Status	Associated
		Association ID	1
		802.11 Authentication	Open System
		Reason Code	1
		Status Code	0
Client Type	Regular	CF Pollable	Not Implemented
User Name	bon	CF Poll Request	Not Implemented
Port Number	1	Short Preamble	Implemented
Interface	management	PBCC	Not Implemented
VLAN ID	0	Channel Agility	Not Implemented
CCX Version	CCXv4	Timeout	3600
E2E Version	E2Ev1	WEP State	WEP Disable
Mobility Role	Local		
Mobility Peer IP Address	N/A		
Policy Manager State	RUN		
Management	...		