You make **possible**

# Be my guest!

## Design and deploy wireless guest access that works

Federico Ziliotto
Technical Solutions Architect
CCIE – 23280 (Wireless, R&S)

BRKEWN-2014

Barcelona | January 27-31, 2020

*(as many things in life)*

*Guest Wi-Fi is about the right choices…*

# Federico → Fede

- 12+ years at Cisco 🎉
  - 4 years as a Customer Support Engineer (CSE)
  - 3 years as a Specialized Systems Engineer
  - 5 years as a Consulting Systems Engineer (CSE)
  - ~1 year as a Technical Solutions Architect (TSA)
- Always focused on Wireless and NAC

FISE
(Family IT Support Engineer)

Very, very amateur photography enthusiast

# What this session covers... and what it doesn't...

- (non-)web authentication techniques;
- controller's web authentication;
- DNA Spaces portals;
- Identity Services Engine (ISE);
- some use cases and caveats;
- mostly IOS-XE, some AireOS.

BRKEWN-2670

BRKEWN-2010

- configuration/customization details;
- version discrepancies;
- roadmap;
- service provider solutions;
- DNA Spaces (other than portals).

BRKEWN-2012

...except when it does.

# For your reference

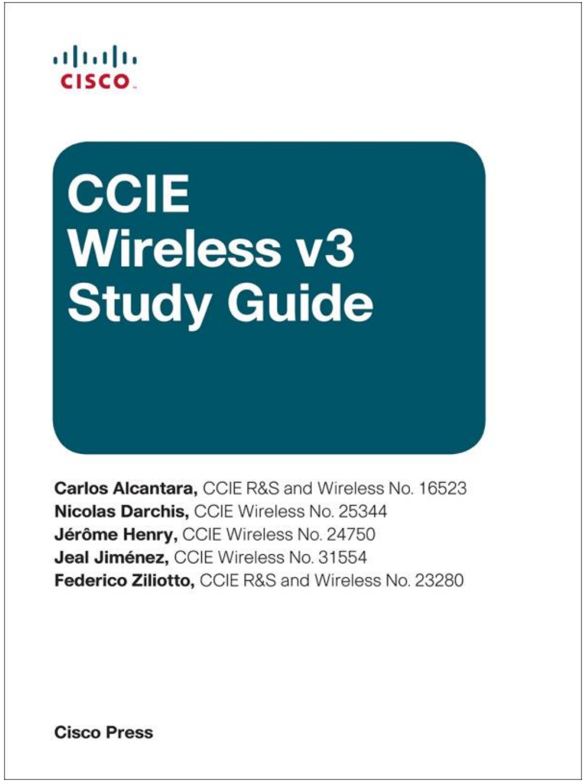
For your reference

- There are slides in your PDF that will not be presented, or quickly presented.
- They are valuable, but included only “For your reference”.

For your reference

# We do everything by the book...

For your reference



cisco

CCIE Wireless v3 Study Guide

**Carlos Alcantara,** CCIE R&S and Wireless No. 16523
**Nicolas Darchis,** CCIE Wireless No. 25344
**Jérôme Henry,** CCIE Wireless No. 24750
**Jeal Jiménez,** CCIE Wireless No. 31554
**Federico Ziliotto,** CCIE R&S and Wireless No. 23280

**Cisco Press**

http://www.ciscopress.com/store/ccie-wireless-v3-study-guide-9781587206207

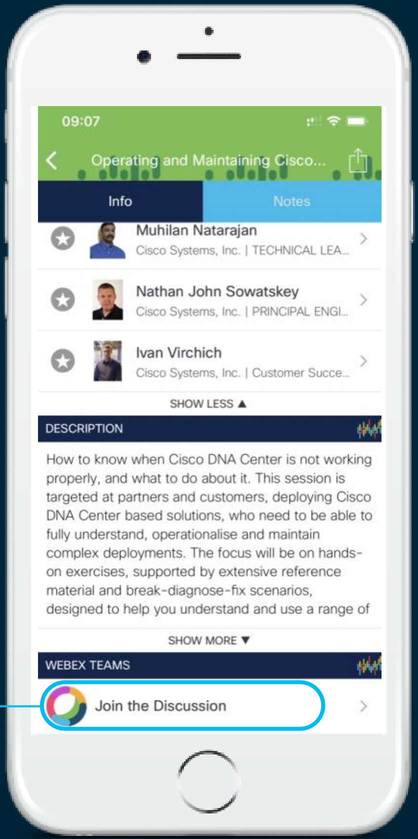
# Cisco Webex Teams

## Questions?

Use Cisco Webex Teams to chat
with the speaker after the session

## How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



Muhilan Natarajan
Cisco Systems, Inc. | TECHNICAL LEA...

Nathan John Sowatskey
Cisco Systems, Inc. | PRINCIPAL ENGI...

Ivan Virchich
Cisco Systems, Inc. | Customer Succe...

DESCRIPTION

How to know when Cisco DNA Center is not working properly, and what to do about it. This session is targeted at partners and customers, deploying Cisco DNA Center based solutions, who need to be able to fully understand, operationalise and maintain complex deployments. The focus will be on hands-on exercises, supported by extensive reference material and break-diagnose-fix scenarios, designed to help you understand and use a range of

WEBEX TEAMS

# Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

# Continue your education

For your reference

Demos in the Cisco Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

# Session Abstract

For your reference

- Guest networks are pervasive nowadays and almost every wireless deployment comes with the requirement for at least one guest SSID.
- Through this session you will learn all about the different Cisco guest solutions, which one to choose according to your needs, and how to successfully implement it. We will also try showing you potential caveats of wireless guest networks, to help you validate your own configuration to proactively anticipate potential issues.
- As some additional topics, we will take a look at other relevant technologies also, such as Open Roaming and WFA's Enhanced Open. Note: this session focuses on IOS-XE and AireOS operating systems, it does not cover Meraki architectures.

# Some things are specific to each scenario

Some common goals:

- Access / provide (free) Wi-Fi.
- Be legally compliant.
- Engage with visitors (e.g., provide maps, applications, advertisements, etc.)

What (not) to ask?

"They need to pay, pay, pay! Make extra money!"

"They will sue you, ask for passports!"

"Don't let them exploit you, block them after the first visit!"

"Let them access it for free, they will be thankful."

"Make it easy, an AUP (acceptable use policy) is all you need."

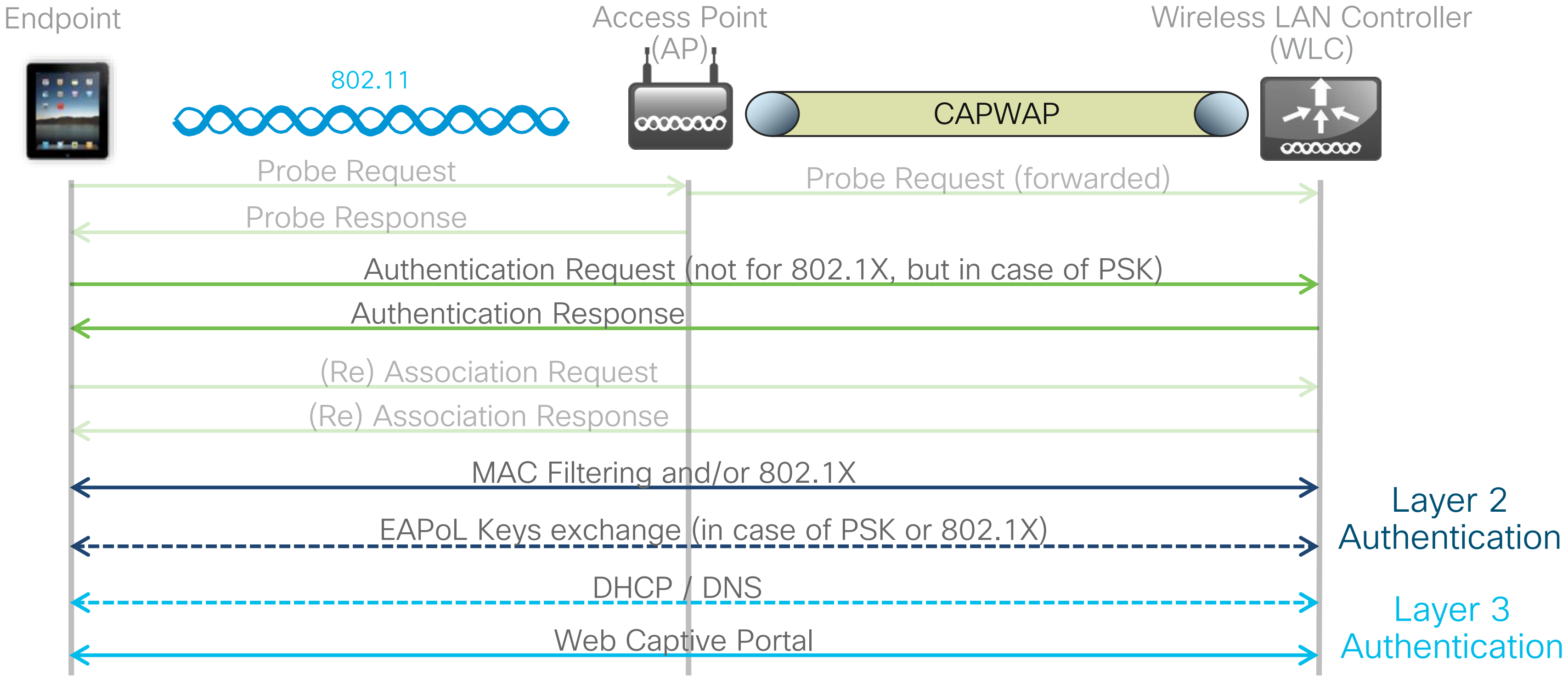
"Encourage them to return."

# Agenda

- How to access a “guest” network
- Guest portal techniques
- The right solution for the right needs
- Tips, tricks and use cases

# How to access a “guest” network

# Wireless connection workflow



Endpoint

Access Point (AP)

Wireless LAN Controller (WLC)

802.11

CAPWAP

Probe Request

Probe Request (forwarded)

Probe Response

Authentication Request (not for 802.1X, but in case of PSK)

Authentication Response

(Re) Association Request

(Re) Association Response

MAC Filtering and/or 802.1X

EAPoL Keys exchange (in case of PSK or 802.1X)

Layer 2 Authentication

DHCP / DNS

Web Captive Portal

Layer 3 Authentication

# Secure or open SSID?

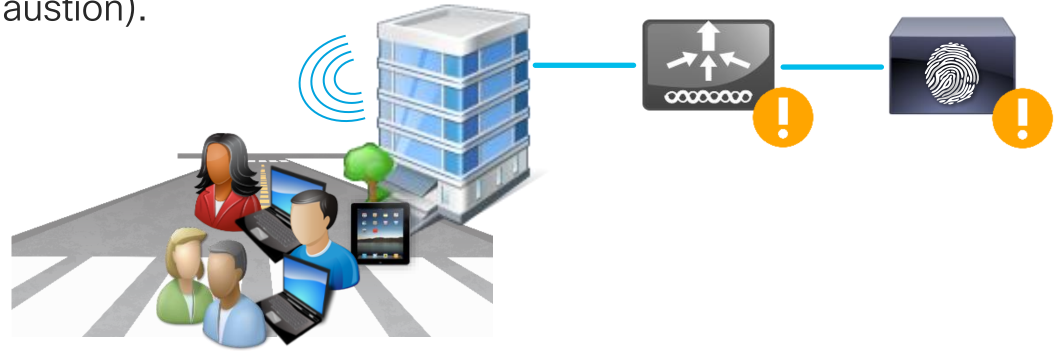
- Secure SSID

- Open SSID

- A secure SSID cannot fall back to open.
  - Example: guests not supporting 802.1X cannot fall back to web portal authentication on the same SSID as corporate users.
- Pre-shared keys (PSK) and keys derived from 802.1X are not supported together.
- We can have a secure SSID (PSK or 802.1X) followed by web portal authentication.

# To PSK or not to PSK?

- Q: Can I deploy PSK on top of web authentication?
  A: Yes…
  - PSK + Local Web Authentication (LWA) has always been supported.
    PSK + Central Web Authentication (CWA) is supported starting from AireOS 8.3 and in IOS-XE.
    Note: with PSK + CWA the WLC disconnects the client, irrespective of the CoA type (CSCvb10807).
  - (WPA2 PSK) It is not much more secure than Open, since all users will share the same key.
  - It may add extra burden, as end users would need to ask for / be given the PSK.
  - It helps avoiding passersby to randomly connect without access to the passphrase (e.g., IP address exhaustion).

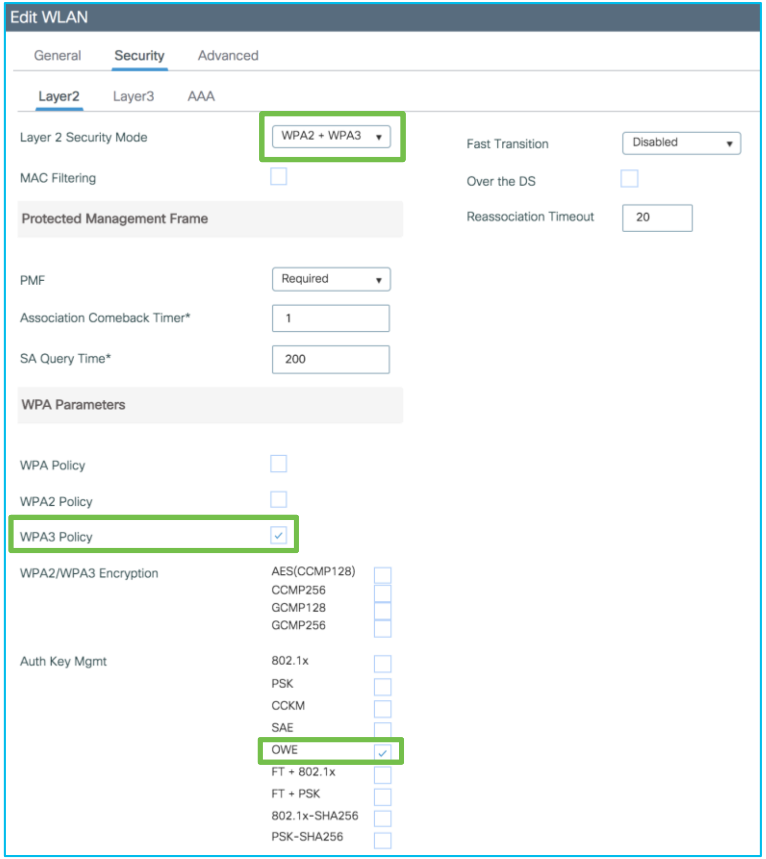


# Enhanced Open for PSK-like security

## Usually supported along with WPA3

- A dedicated Wi-Fi Alliance (WFA) certification, **not part of WPA3**.
- Mostly targeted for hotspots.
- Based on Opportunistic Wireless Encryption (OWE): APs and clients automatically negotiate **encryption without a user-defined PSK**.
- It prevents passive attacks (i.e., traffic visibility).

# Enhanced Open for PSK-like security



Edit WLAN

General | Security | Advanced

Layer2 | Layer3 | AAA

Layer 2 Security Mode: WPA2 + WPA3

MAC Filtering: ☐

**Protected Management Frame**

PMF: Required

Association Comeback Timer*: 1

SA Query Time*: 200

**WPA Parameters**

WPA Policy: ☐

WPA2 Policy: ☐

WPA3 Policy: ☑

WPA2/WPA3 Encryption:
- AES(CCMP128) ☐
- CCMP256 ☐
- GCMP128 ☐
- GCMP256 ☐

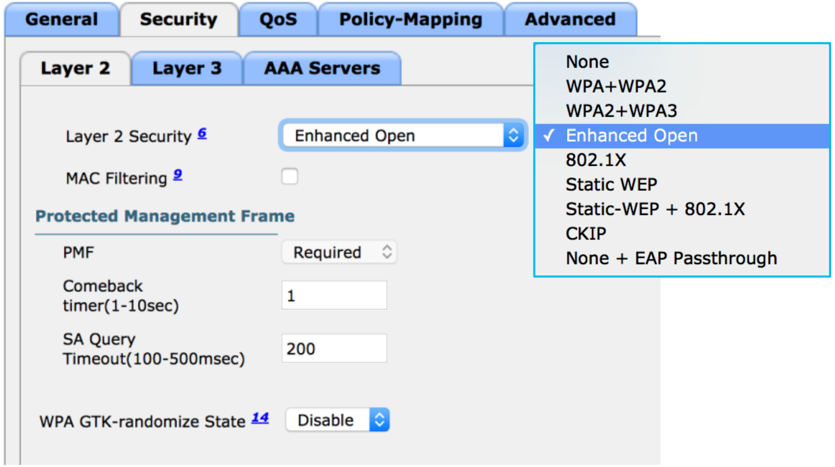
Auth Key Mgmt:
- 802.1x ☐
- PSK ☐
- CCKM ☐
- SAE ☐
- OWE ☑
- FT + 802.1x ☐
- FT + PSK ☐
- 802.1x-SHA256 ☐
- PSK-SHA256 ☐

Fast Transition: Disabled

Over the DS: ☐

Reassociation Timeout: 20

IOS-XE 16.12.1s+



General | Security | QoS | Policy-Mapping | Advanced

Layer 2 | Layer 3 | AAA Servers

Layer 2 Security 6: Enhanced Open

MAC Filtering 9: ☐

**Protected Management Frame**

PMF: Required

Comeback timer(1-10sec): 1

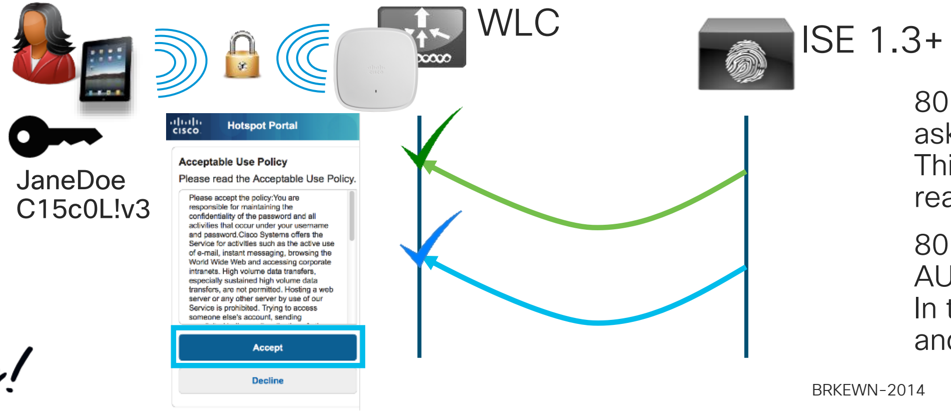
SA Query Timeout(100-500msec): 200

WPA GTK-randomize State 14: Disable

AireOS 8.10+

# To 802.1X or not to 802.1X?

- Q: Can I deploy 802.1X on top of web authentication?
  A: Yes…
  - 802.1X + Local Web Authentication (LWA) is supported since AireOS 7.4.
    802.1X + Central Web Authentication (CWA) is supported since ISE 1.3.
    802.1X + LWA or CWA is supported in IOS-XE.
  - It is more secure than PSK, because keys are dynamic and per user.
  - It may still add extra burden, as end users need to ask for / be given an account to pass 802.1X first, before being redirected to a portal.
  - It helps avoiding passersby to randomly connect without an account.



Acceptable Use Policy

Please read the Acceptable Use Policy.

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending

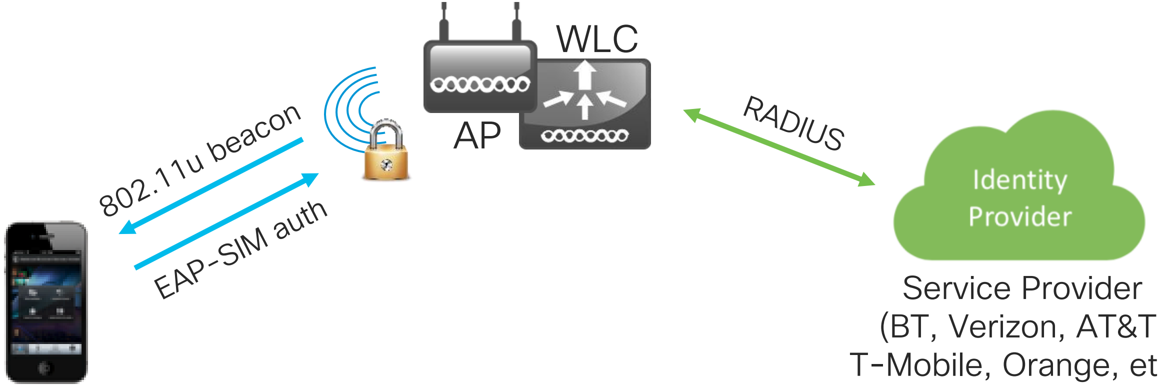
802.1X + LWA is supported only with a web portal asking for login / password.
This means asking twice for authentication (not really for guests).

802.1X + CWA is supported even with a simple AUP page for the web portal.
In this way 802.1X takes care of login / password and CWA of the disclaimer.

# OpenRoaming for 802.1X-like security

## As well as ease of access

- The need: seamless and secure end user’s connectivity to Wi-Fi
- The former answer: 802.11u / Hotspot 2.0 / Passpoint

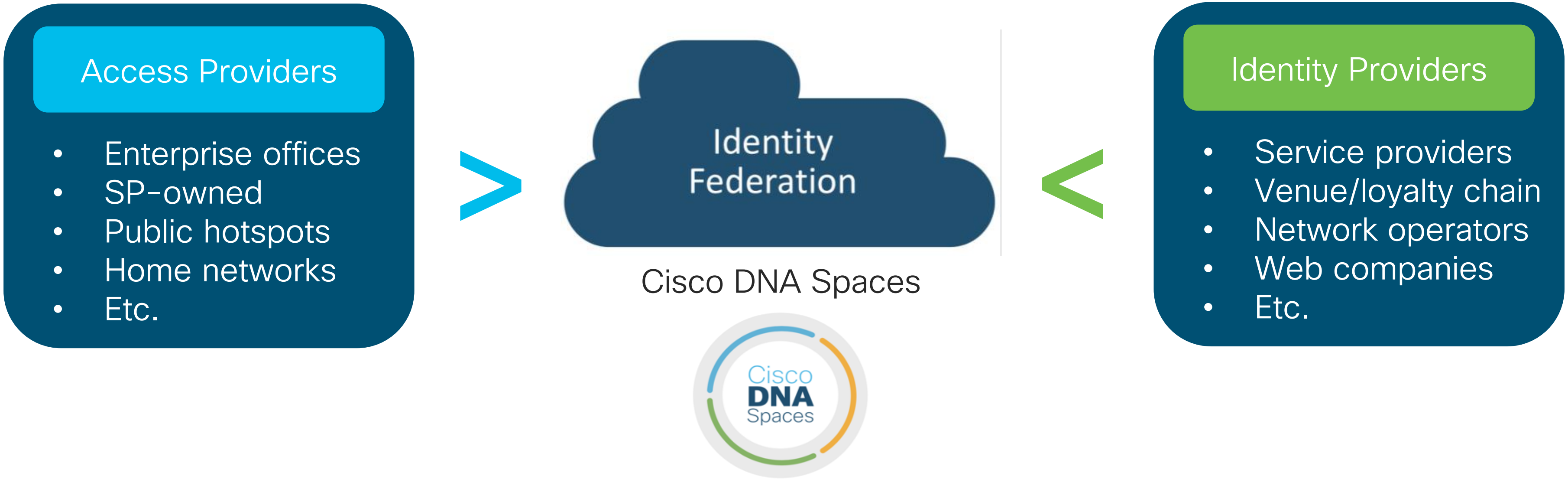


Service Provider
(BT, Verizon, AT&T,
T-Mobile, Orange, etc.)

BUT… it required routing/VPN for secure RADIUS messages, a “clearinghouse” and a AAA proxy for multiple identity providers, it mainly worked with very few service providers, etc.

# OpenRoaming for 802.1X-like security

## As well as ease of access



**Access Providers**

- Enterprise offices
- SP-owned
- Public hotspots
- Home networks
- Etc.

Identity Federation

Cisco DNA Spaces

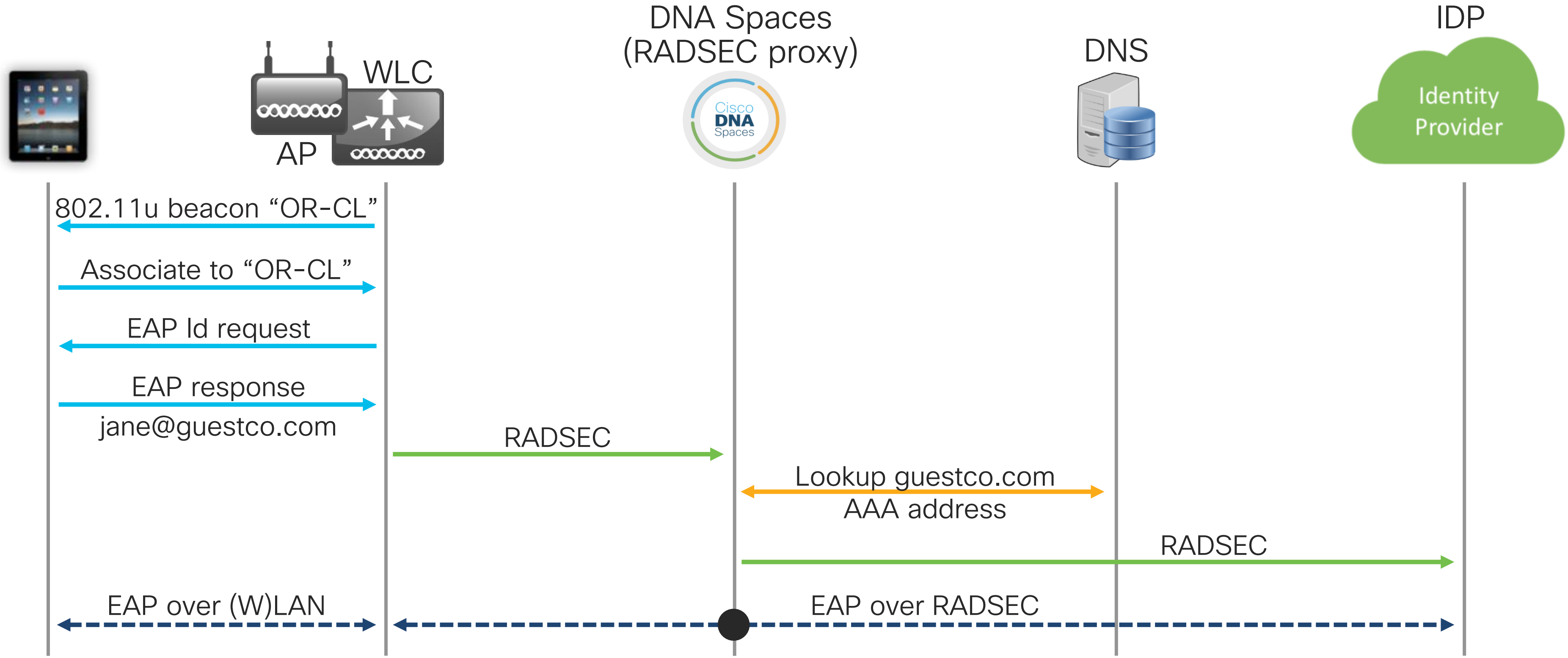
(RADSEC proxy)

**Identity Providers**

- Service providers
- Venue/loyalty chain
- Network operators
- Web companies
- Etc.

# OpenRoaming for 802.1X-like security

## As well as ease of access



# OpenRoaming for 802.1X-like security

## As well as ease of access

Pros:

- It does not need a portal
- Transparent to the end user
- Identity base delegated to well-known providers
- More secure than open/PSK networks

Cons:

- It does not need a portal
- No engagement with the end user
- For additional engagement, we would need to add a portal on top
- Dependent on the endpoint’s support

For more info:
https://www.cisco.com/c/en/us/solutions/enterprise-networks/802-11ax-solution/openroaming.html
https://openroaming.org/

# Why most of them use web authentication?

For your reference

- 802.1X
  - Certificates, AD credentials
  - Good for **managed devices and known users**
- MAC Authentication Bypass (MAB)
  - **Managed devices** with no 802.1X capability or user input
- PSK
  - No individual identity, easily well-known/no rotating keys
- Web Authentication
  - **Supplementary** authentication method vs plain Open netwc
  - **Unmanaged** devices
  - Allows web redirect (AUP/legal)

Employee

Guest

# Why guest portals then?

## A service for the company

For your reference

Customer satisfaction

Analytics

$$$$$$

# Why guest portals then?

## A (legal) service for end users and the company

For your reference

- Depending on the Country, the Wi-Fi operator needs to comply with some rules.
- Disclaimers help Wi-Fi operators (and end users too) to avoid liability.

- Without disclaimers, or according to other specific laws, the Wi-Fi operator might have to guarantee additional, adequate security measures (FW, IPS, etc.).
- Note: lawful intercept (i.e., logs collection) does not always require a user identity in the form of username, given name, family name, etc.
  Often the user identity can simply be translated to the MAC address.

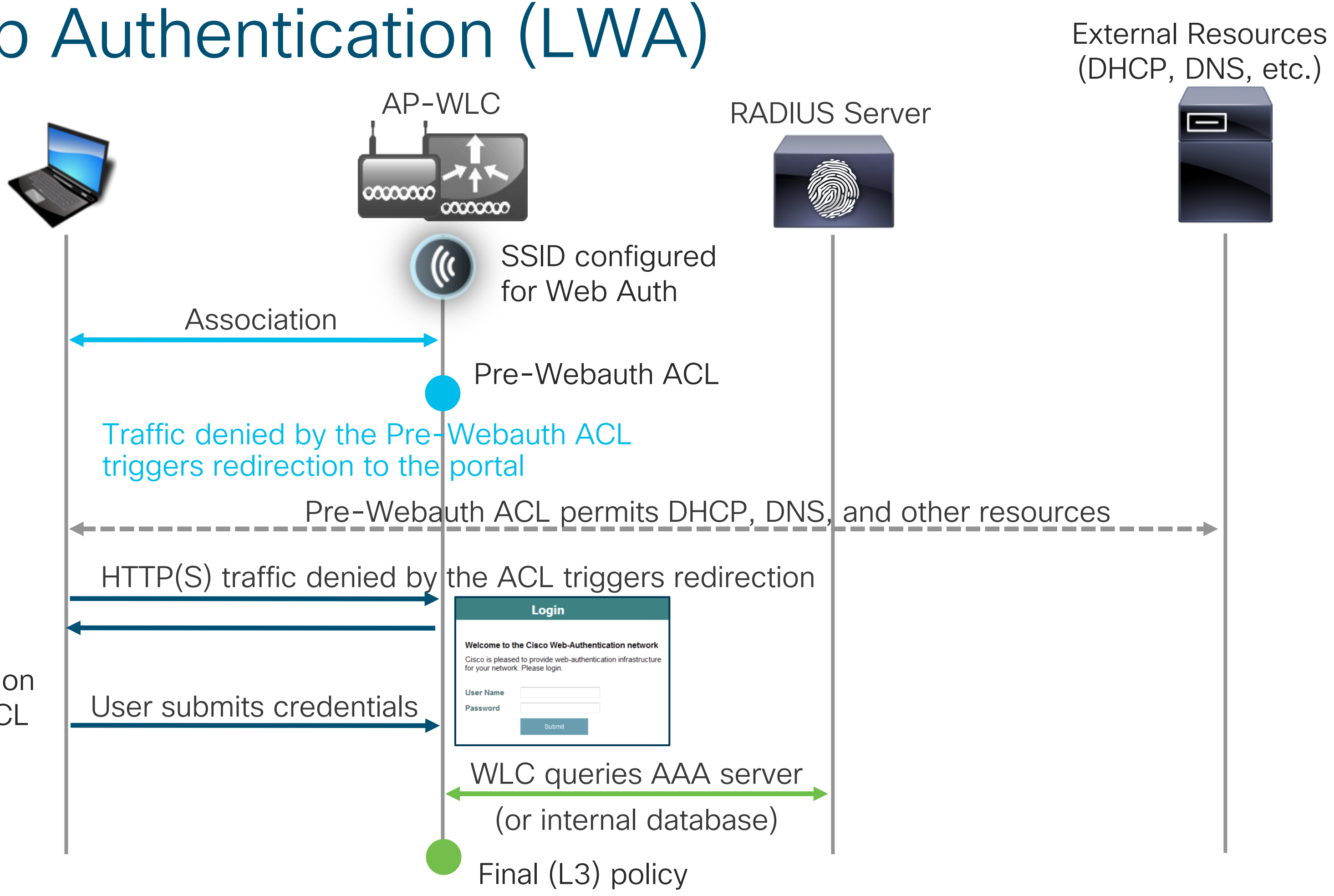
# Guest portal techniques

# Local Web Authentication (LWA)

802.1X / PSK

Local Web Auth

**LOCAL** because the redirection URL and the pre-webauth ACL are **locally** configured on the WLC.


External Resources (DHCP, DNS, etc.)
AP-WLC
RADIUS Server
SSID configured for Web Auth
Association
Pre-Webauth ACL
Traffic denied by the Pre-Webauth ACL triggers redirection to the portal
Pre-Webauth ACL permits DHCP, DNS, and other resources
HTTP(S) traffic denied by the ACL triggers redirection
User submits credentials
WLC queries AAA server
(or internal database)
Final (L3) policy

Login

Welcome to the Cisco Web-Authentication network

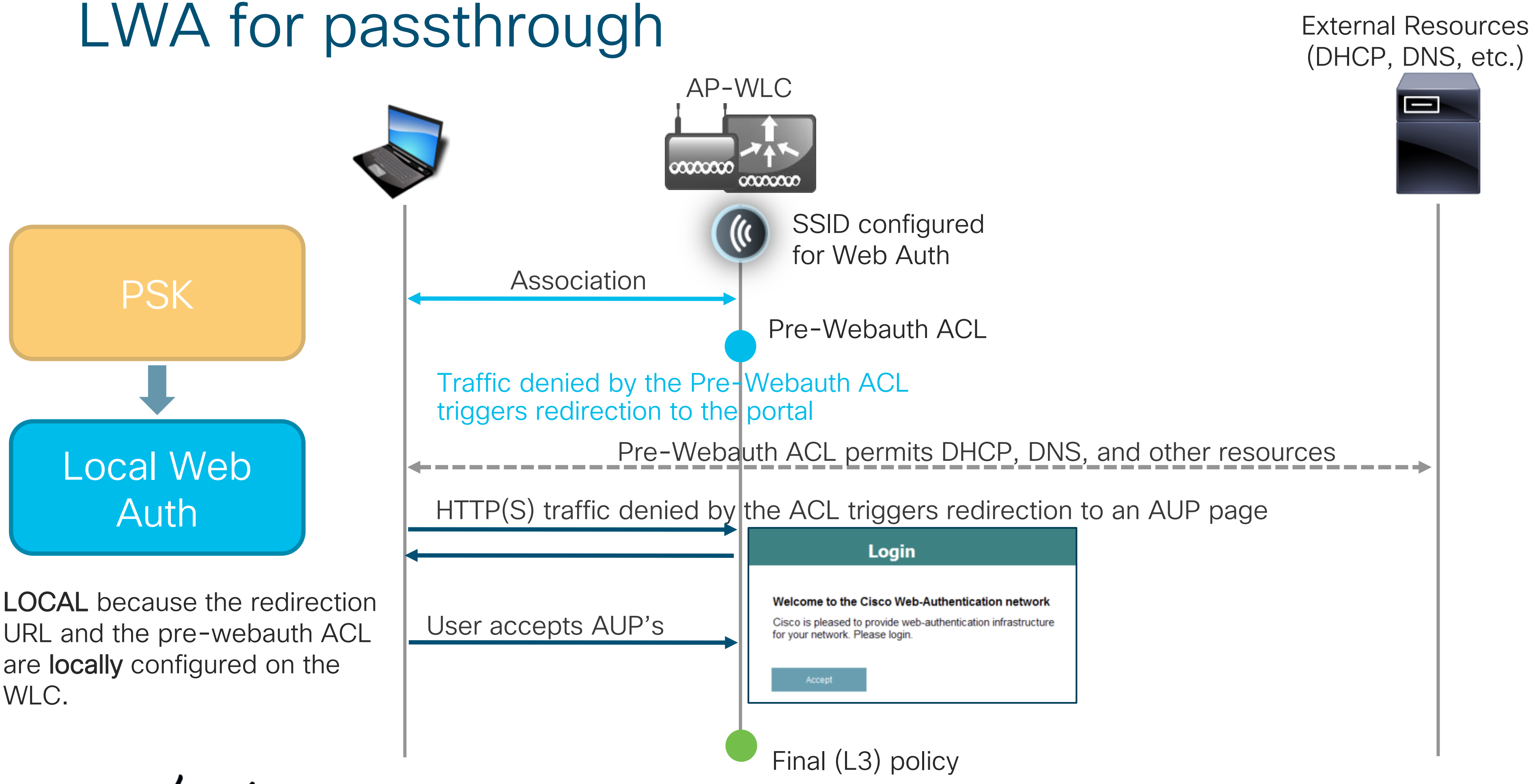
Cisco is pleased to provide web-authentication infrastructure for your network. Please login.

User Name

Password

Submit

# LWA for passthrough



External Resources (DHCP, DNS, etc.)

AP-WLC

PSK

Local Web Auth

SSID configured for Web Auth

Association

Pre-Webauth ACL

Traffic denied by the Pre-Webauth ACL triggers redirection to the portal

Pre-Webauth ACL permits DHCP, DNS, and other resources

HTTP(S) traffic denied by the ACL triggers redirection to an AUP page

User accepts AUP’s

Login

**Welcome to the Cisco Web-Authentication network**

Cisco is pleased to provide web-authentication infrastructure for your network. Please login.

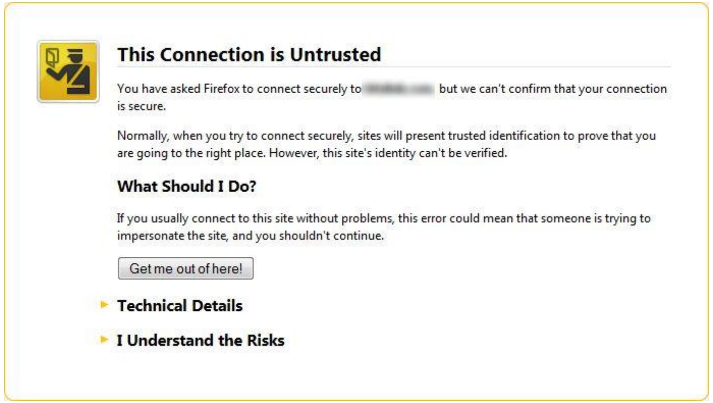
Accept

Final (L3) policy

**LOCAL** because the redirection URL and the pre-webauth ACL are **locally** configured on the WLC.

# LWA and certificates

## WLC's internal portal



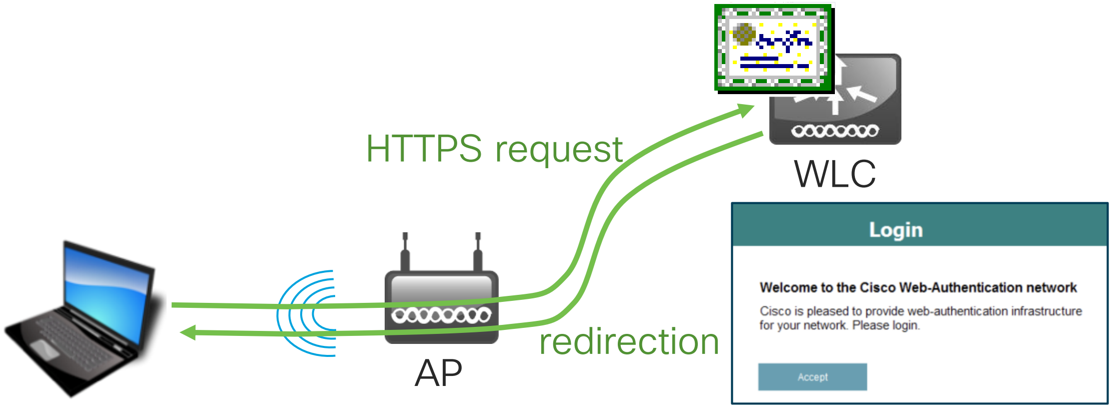
**This Connection is Untrusted**

You have asked Firefox to connect securely to [redacted] but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

**What Should I Do?**

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.



**Welcome to the Cisco Web-Authentication network**

Cisco is pleased to provide web-authentication infrastructure for your network. Please login.

Certificates for the Controller Web Authentication:

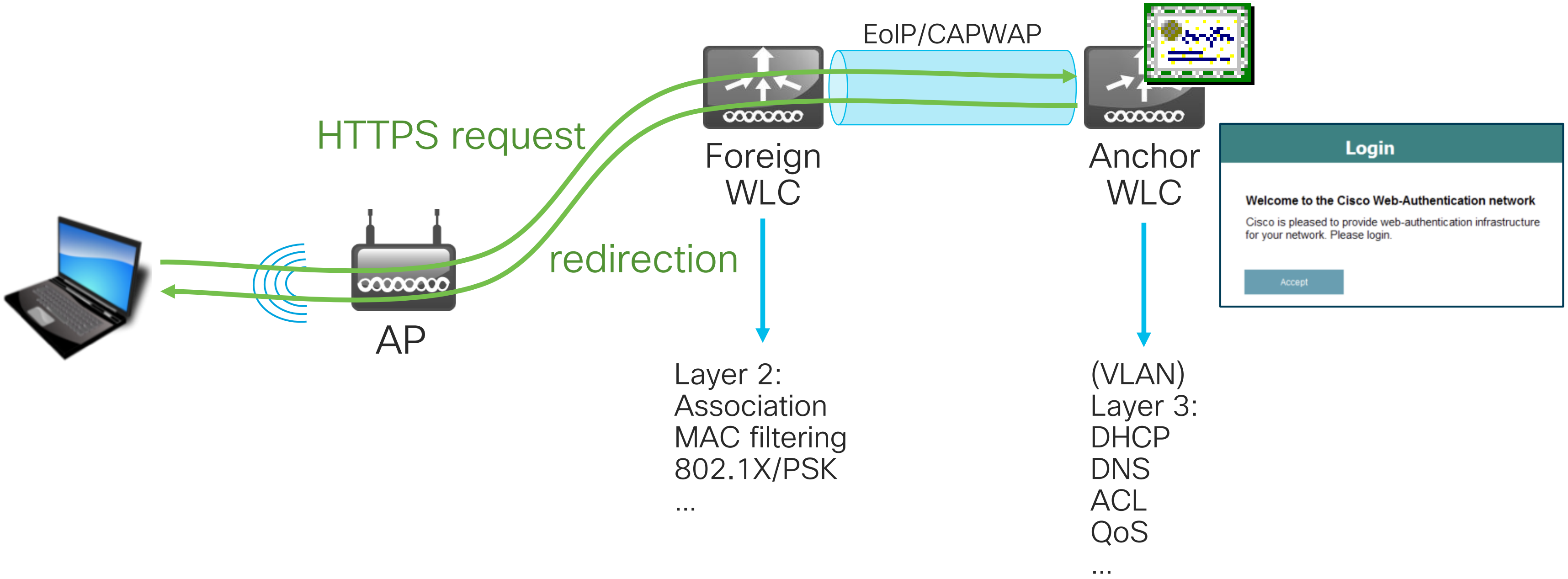
https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213917-generate-csr-for-third-party-certificate.html

http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/115951-web-auth-wlc-guide-00.html#anc20

# LWA with an anchor controller

## WLC’s internal portal

BRKEWN-2010



Layer 2:
Association
MAC filtering
802.1X/PSK
…

(VLAN)
Layer 3:
DHCP
DNS
ACL
QoS
…

**Login**

**Welcome to the Cisco Web-Authentication network**

Cisco is pleased to provide web-authentication infrastructure for your network. Please login.

Accept

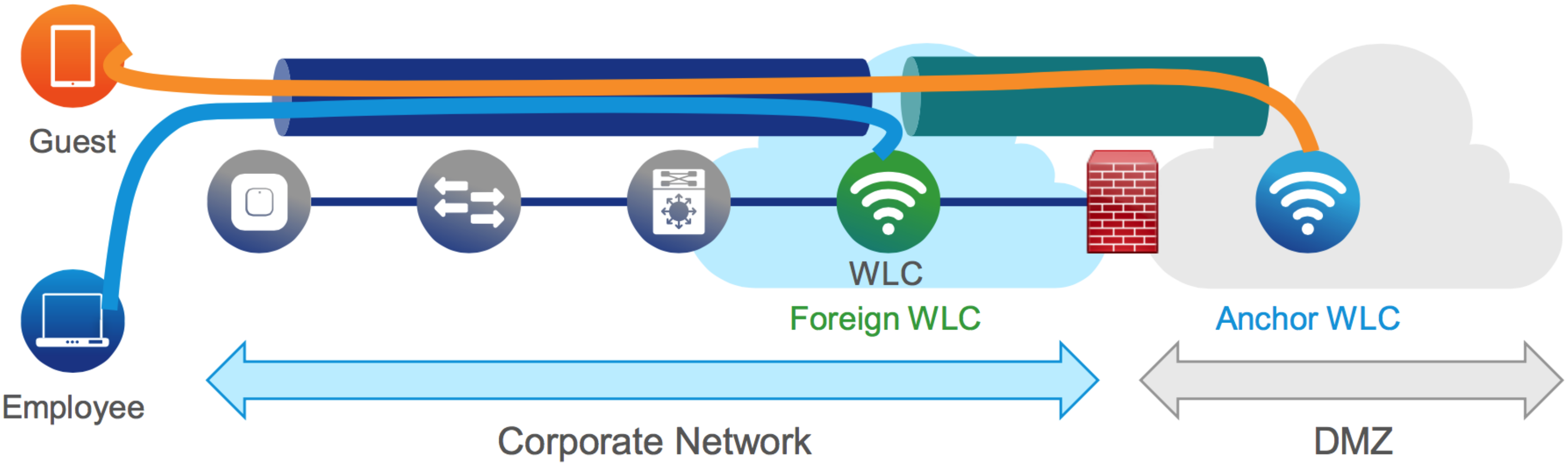
Enterprise Mobility 8.5 Design Guide – Cisco Unified Wireless Network Guest Access Services:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/Enterprise-Mobility-8-5-Design-Guide/Enterprise_Mobility_8-5_Deployment_Guide/WirelessNetwork_GuestAccessService.html

Cisco Catalyst 9800 Wireless Controller – AireOS IRCM Deployment Guide:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_c9800_wireless_controller-aireos_ircm_dg.html

# Guest traffic isolation – build another tunnel

For your reference

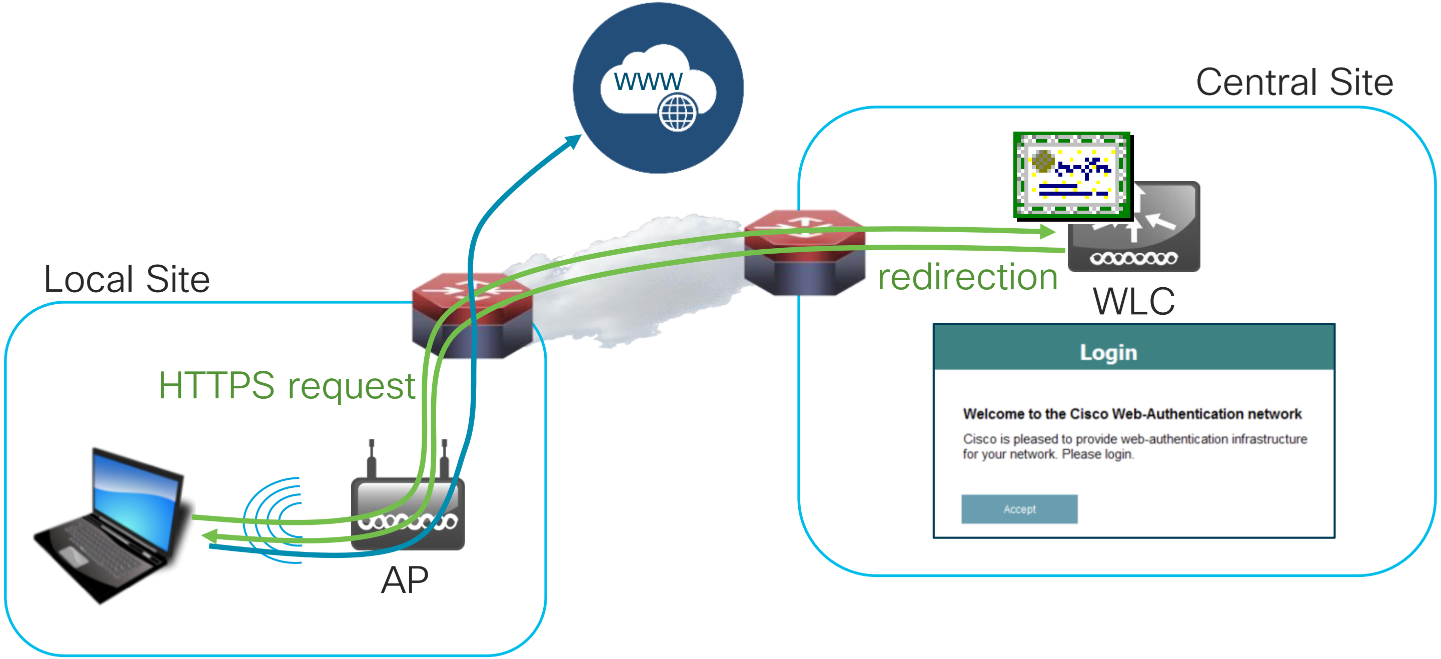
- First hop AP to WLC still via a CAPWAP tunnel
- The "first stop” WLC is now called the Foreign WLC
- Tunnel Guest traffic to an Anchor WLC in the DMZ



# LWA with FlexConnect

## WLC’s internal portal

BRKEWN-2016



**Login**

**Welcome to the Cisco Web-Authentication network**

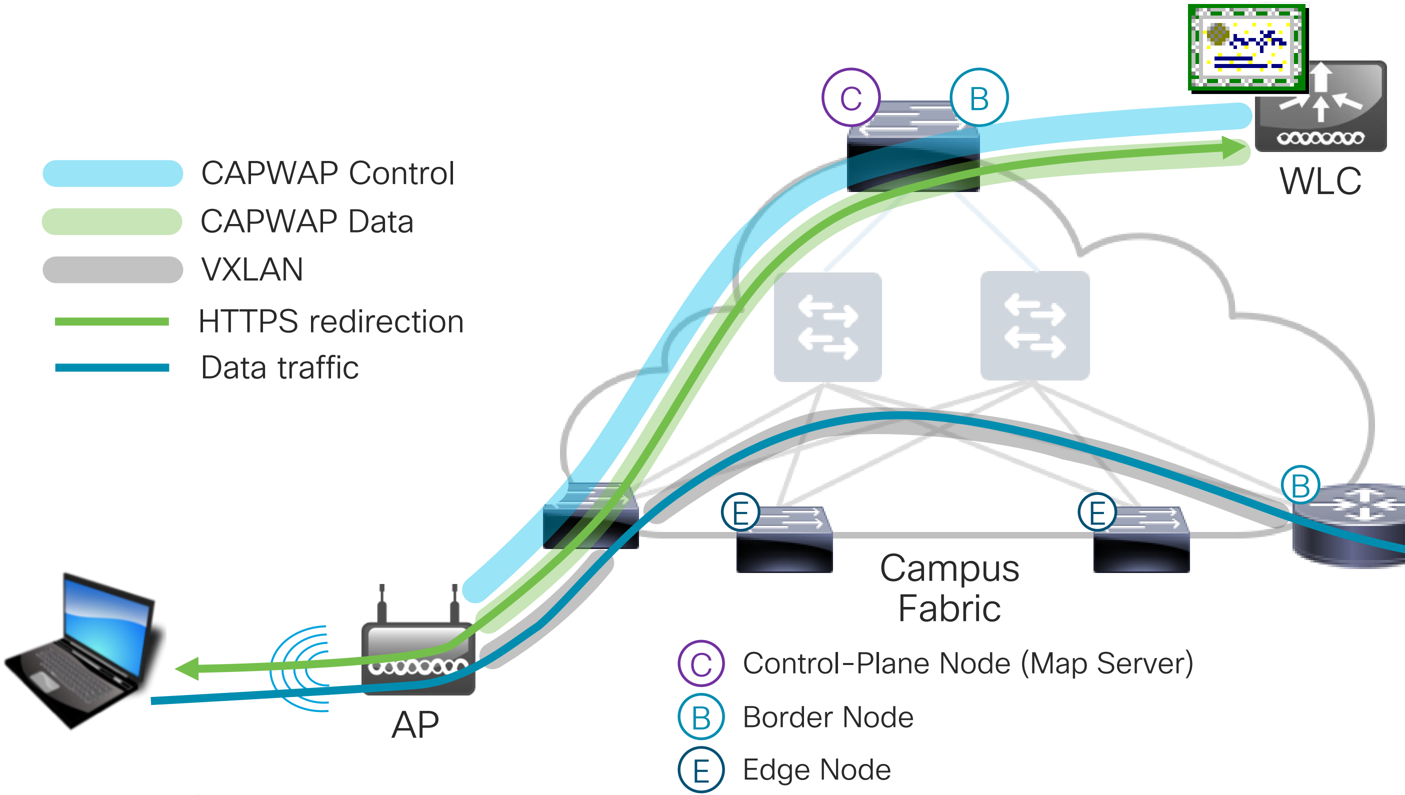
Cisco is pleased to provide web-authentication infrastructure for your network. Please login.

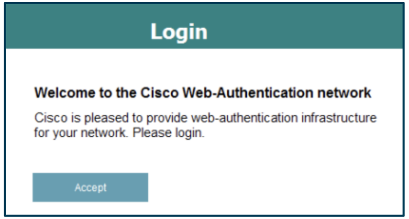
# LWA with Cisco DNA Campus Fabric

## WLC's internal portal

BRKEWN-2020

For your reference





**Login**

**Welcome to the Cisco Web-Authentication network**

Cisco is pleased to provide web-authentication infrastructure for your network. Please login.

| | |
|---|---|
| 🟦 | CAPWAP Control |
| 🟩 | CAPWAP Data |
| ▨ | VXLAN |
| — | HTTPS redirection |
| — | Data traffic |

Ⓒ Control-Plane Node (Map Server)

Ⓑ Border Node

Ⓔ Edge Node

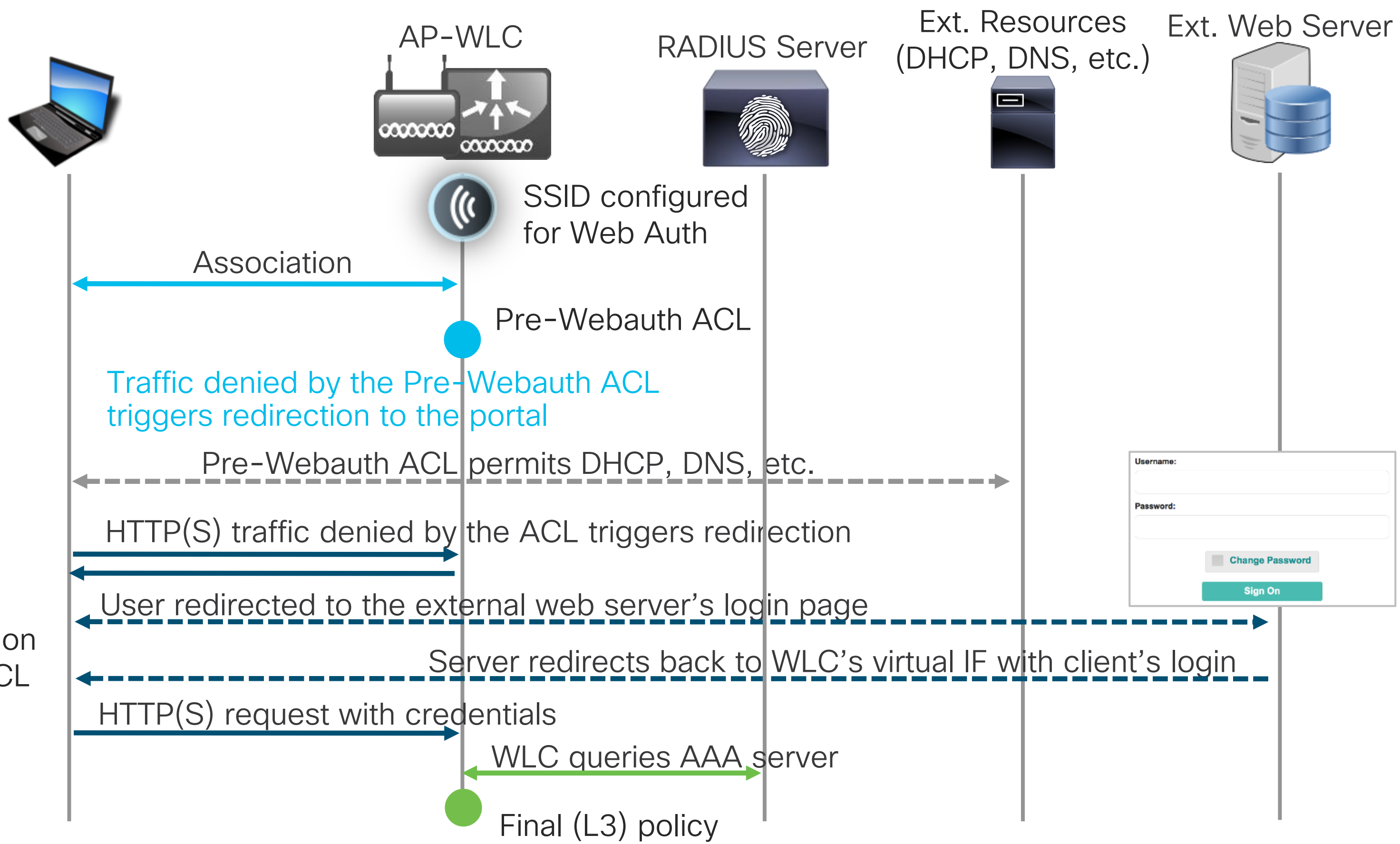
# LWA with external web server redirect

For your reference

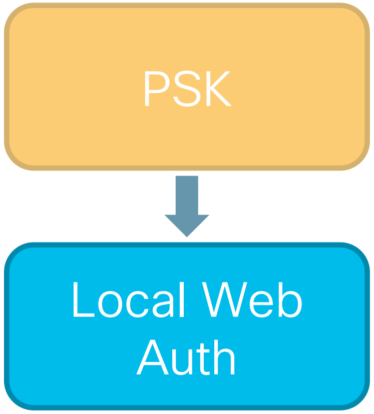
802.1X / PSK

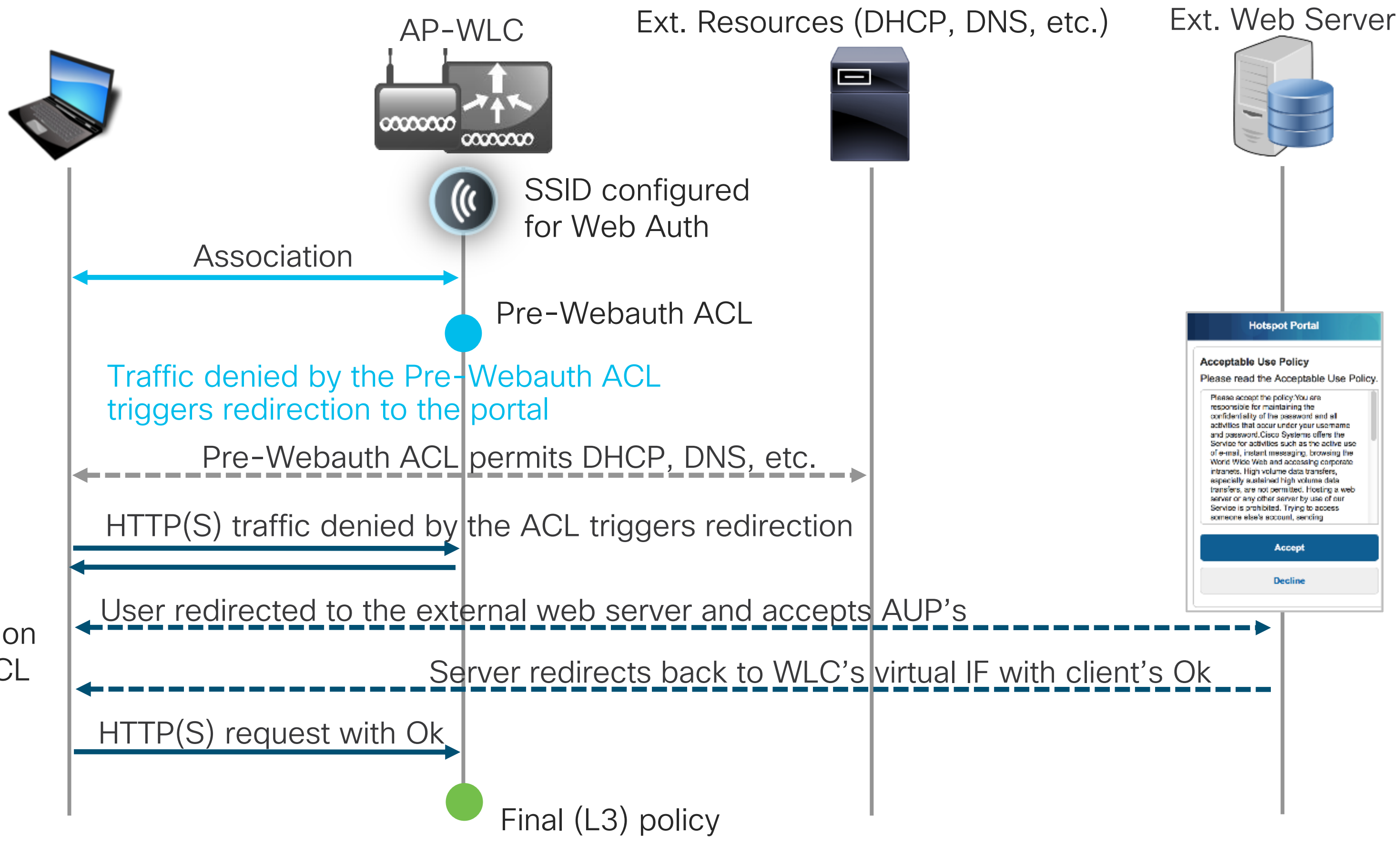
Local Web Auth

**LOCAL** because the redirection URL and the pre-webauth ACL are **locally** configured on the WLC.


AP-WLC
RADIUS Server
Ext. Resources (DHCP, DNS, etc.)
Ext. Web Server
SSID configured for Web Auth
Association
Pre-Webauth ACL
Traffic denied by the Pre-Webauth ACL triggers redirection to the portal
Pre-Webauth ACL permits DHCP, DNS, etc.
HTTP(S) traffic denied by the ACL triggers redirection
User redirected to the external web server's login page
Server redirects back to WLC's virtual IF with client's login
HTTP(S) request with credentials
WLC queries AAA server
Final (L3) policy
Username:
Password:
Change Password
Sign On

# LWA: external web server redirect for passthrough




AP-WLC
Ext. Resources (DHCP, DNS, etc.)
Ext. Web Server
SSID configured for Web Auth
Association
Pre-Webauth ACL
Traffic denied by the Pre-Webauth ACL triggers redirection to the portal
Pre-Webauth ACL permits DHCP, DNS, etc.
HTTP(S) traffic denied by the ACL triggers redirection
User redirected to the external web server and accepts AUP's
Server redirects back to WLC's virtual IF with client's Ok
HTTP(S) request with Ok
Final (L3) policy

Hotspot Portal

**Acceptable Use Policy**

Please read the Acceptable Use Policy.

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending

Accept

Decline

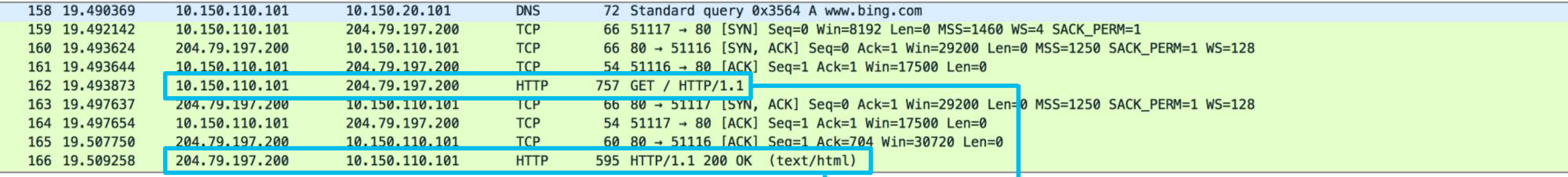
**LOCAL** because the redirection URL and the pre-webauth ACL are **locally** configured on the WLC.

# LWA: external web server redirect for passthrough

## A quick packet capture walkthrough

Wireshark on the endpoint directly, with the following filter (your mileage may vary):

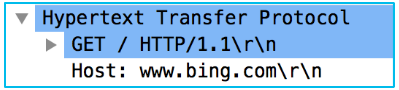
```
eth.addr == 11:22:33:aa:bb:cc && (bootp || dns || tcp.port == 80 || tcp.port == 443)
```



```
158 19.490369   10.150.110.101   10.150.20.101    DNS    72 Standard query 0x3564 A www.bing.com
159 19.492142   10.150.110.101   204.79.197.200   TCP    66 51117 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
160 19.493624   204.79.197.200   10.150.110.101   TCP    66 80 → 51116 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1250 SACK_PERM=1 WS=128
161 19.493644   10.150.110.101   204.79.197.200   TCP    54 51116 → 80 [ACK] Seq=1 Ack=1 Win=17500 Len=0
162 19.493873   10.150.110.101   204.79.197.200   HTTP  757 GET / HTTP/1.1
163 19.497637   204.79.197.200   10.150.110.101   TCP    66 80 → 51117 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1250 SACK_PERM=1 WS=128
164 19.497654   10.150.110.101   204.79.197.200   TCP    54 51117 → 80 [ACK] Seq=1 Ack=1 Win=17500 Len=0
165 19.507750   204.79.197.200   10.150.110.101   TCP    60 80 → 51116 [ACK] Seq=1 Ack=704 Win=30720 Len=0
166 19.509258   204.79.197.200   10.150.110.101   HTTP  595 HTTP/1.1 200 OK  (text/html)
```

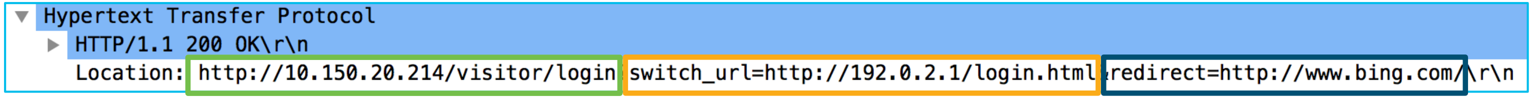
1. The endpoint associates and gets an IP address
2. (optional) The endpoint resolves the FQDN of a specific HTTP(S) web server
3. The endpoint sends and HTTP(S) GET to the web server
4. The WLC spoofs the IP of the web server and redirects the endpoint to the web portal's URL

3



```
▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    Host: www.bing.com\r\n
```

4



```
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Location: http://10.150.20.214/visitor/login?switch_url=http://192.0.2.1/login.html&redirect=http://www.bing.com/\r\n
```

Ext. web portal URL

WLC's web portal URL

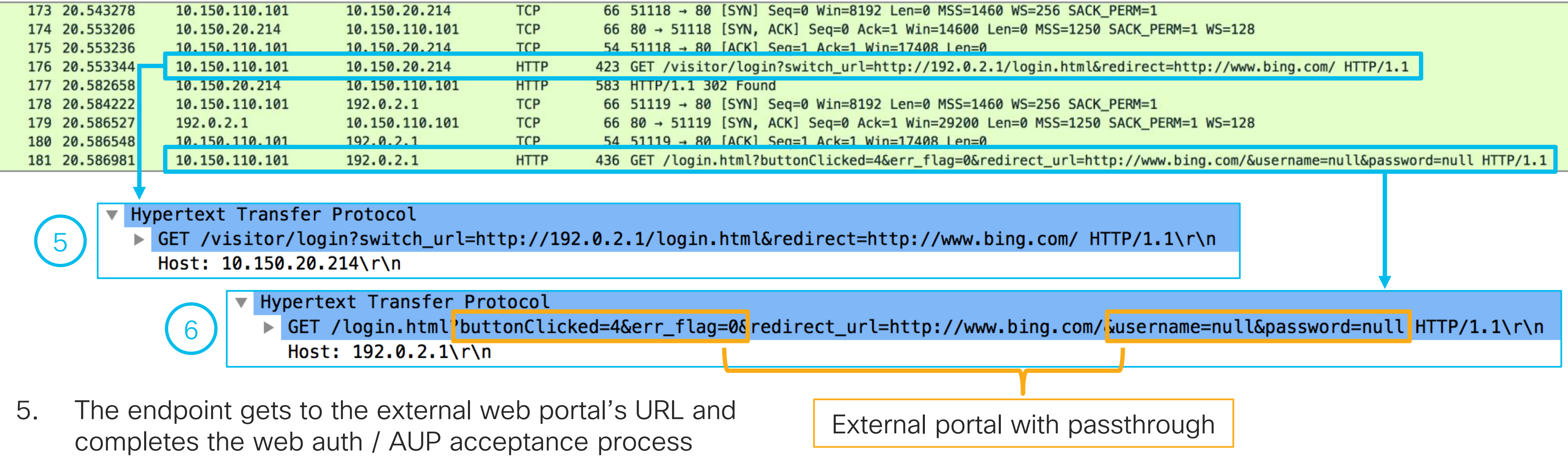
Originally requested URL

# LWA: external web server redirect for passthrough

## A quick packet capture walkthrough

Wireshark on the endpoint directly, with the following filter (your mileage may vary):

```
eth.addr == 11:22:33:aa:bb:cc && (bootp || dns || tcp.port == 80 || tcp.port == 443)
```



```
173 20.543278   10.150.110.101   10.150.20.214    TCP    66  51118 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
174 20.553206   10.150.20.214    10.150.110.101   TCP    66  80 → 51118 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1250 SACK_PERM=1 WS=128
175 20.553236   10.150.110.101   10.150.20.214    TCP    54  51118 → 80 [ACK] Seq=1 Ack=1 Win=17408 Len=0
176 20.553344   10.150.110.101   10.150.20.214    HTTP  423  GET /visitor/login?switch_url=http://192.0.2.1/login.html&redirect=http://www.bing.com/ HTTP/1.1
177 20.582658   10.150.20.214    10.150.110.101   HTTP  583  HTTP/1.1 302 Found
178 20.584222   10.150.110.101   192.0.2.1        TCP    66  51119 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
179 20.586527   192.0.2.1        10.150.110.101   TCP    66  80 → 51119 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1250 SACK_PERM=1 WS=128
180 20.586548   10.150.110.101   192.0.2.1        TCP    54  51119 → 80 [ACK] Seq=1 Ack=1 Win=17408 Len=0
181 20.586981   10.150.110.101   192.0.2.1        HTTP  436  GET /login.html?buttonClicked=4&err_flag=0&redirect_url=http://www.bing.com/&username=null&password=null HTTP/1.1
```

5

```
▼ Hypertext Transfer Protocol
  ▶ GET /visitor/login?switch_url=http://192.0.2.1/login.html&redirect=http://www.bing.com/ HTTP/1.1\r\n
    Host: 10.150.20.214\r\n
```

6

```
▼ Hypertext Transfer Protocol
  ▶ GET /login.html?buttonClicked=4&err_flag=0&redirect_url=http://www.bing.com/&username=null&password=null HTTP/1.1\r\n
    Host: 192.0.2.1\r\n
```

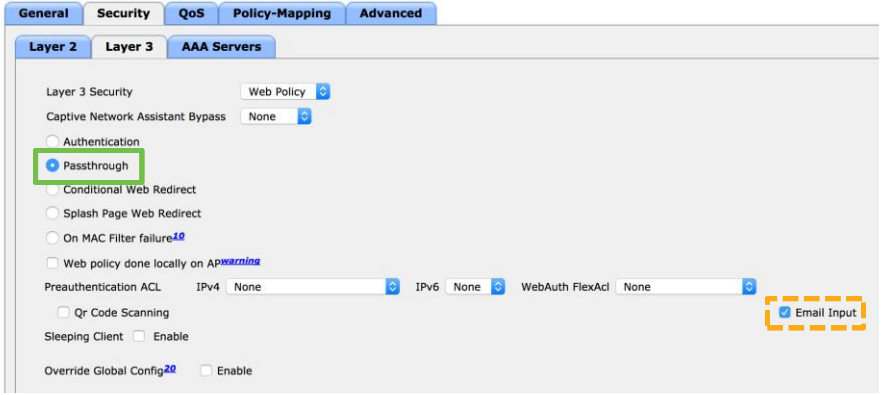
External portal with passthrough

5. The endpoint gets to the external web portal’s URL and completes the web auth / AUP acceptance process
6. The endpoint is redirected back to the WLC’s internal web server (and then optionally to the initially requested URL)

# Web Passthrough on IOS-XE

- "Passthrough" on AireOS
- "Consent" on IOS-XE
- "Hotspot" on ISE

- The user just needs to complete some operation(s) on the web portal.
- There is no form of authentication performed by the WLC (maybe on the web server).



Layer 3 Security: Web Policy

Captive Network Assistant Bypass: None

○ Authentication

● Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

○ On MAC Filter failure10

□ Web policy done locally on APwarning

Preauthentication ACL IPv4 None IPv6 None WebAuth FlexAcl None

□ Qr Code Scanning

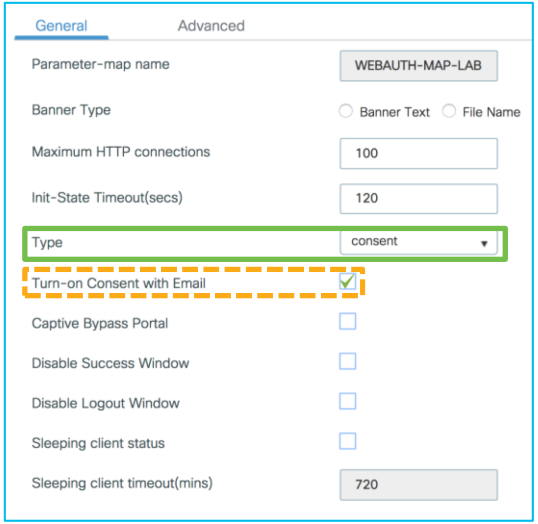
☑ Email Input

Sleeping Client □ Enable

Override Global Config20 □ Enable

AireOS

Configuration > Security > Web Auth > Webauth Parameter Map

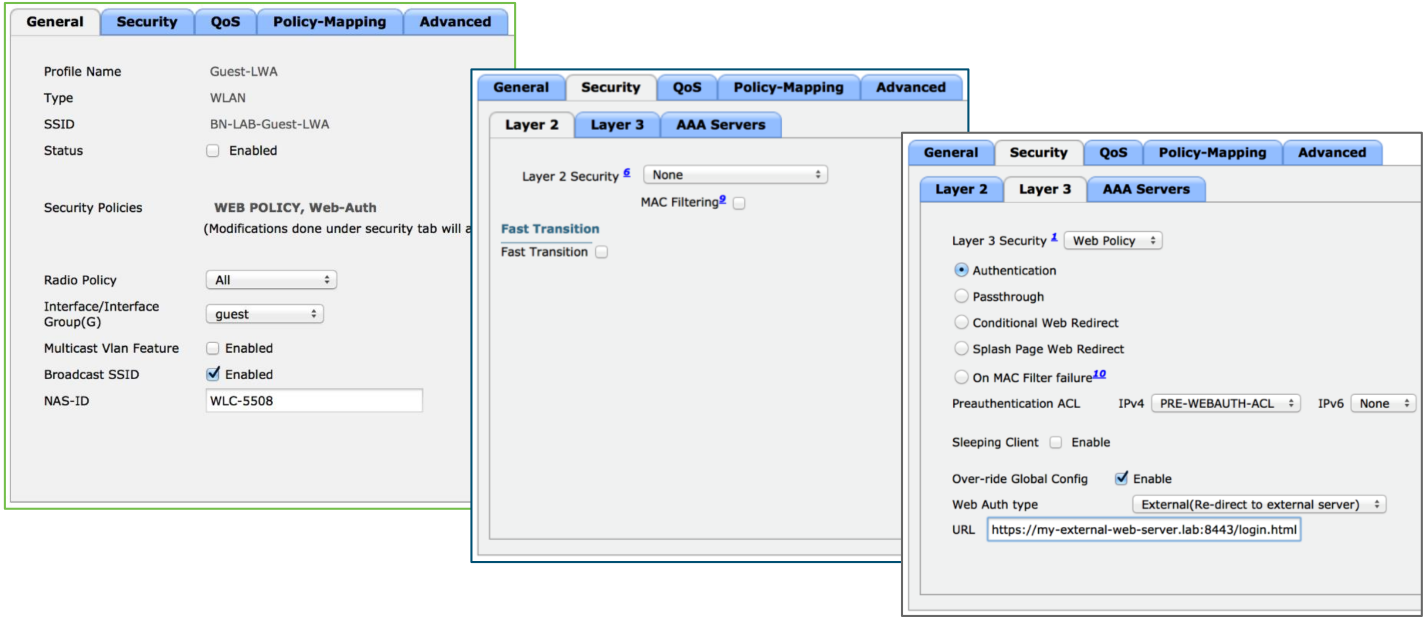


| | |
|---|---|
| Parameter-map name | WEBAUTH-MAP-LAB |
| Banner Type | ○ Banner Text ○ File Name |
| Maximum HTTP connections | 100 |
| Init-State Timeout(secs) | 120 |
| Type | consent |
| Turn-on Consent with Email | ☑ |
| Captive Bypass Portal | □ |
| Disable Success Window | □ |
| Disable Logout Window | □ |
| Sleeping client status | □ |
| Sleeping client timeout(mins) | 720 |

IOS-XE

# LWA – configuration example

For your reference



| | |
|---|---|
| Profile Name | Guest-LWA |
| Type | WLAN |
| SSID | BN-LAB-Guest-LWA |
| Status | □ Enabled |
| Security Policies | WEB POLICY, Web-Auth<br>(Modifications done under security tab will a |
| Radio Policy | All |
| Interface/Interface Group(G) | guest |
| Multicast Vlan Feature | □ Enabled |
| Broadcast SSID | ☑ Enabled |
| NAS-ID | WLC-5508 |

Layer 2 Security 6 None

MAC Filtering9 □

Fast Transition

Fast Transition □

Layer 3 Security 1 Web Policy

● Authentication

○ Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

○ On MAC Filter failure10

Preauthentication ACL IPv4 PRE-WEBAUTH-ACL IPv6 None

Sleeping Client □ Enable

Over-ride Global Config ☑ Enable

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

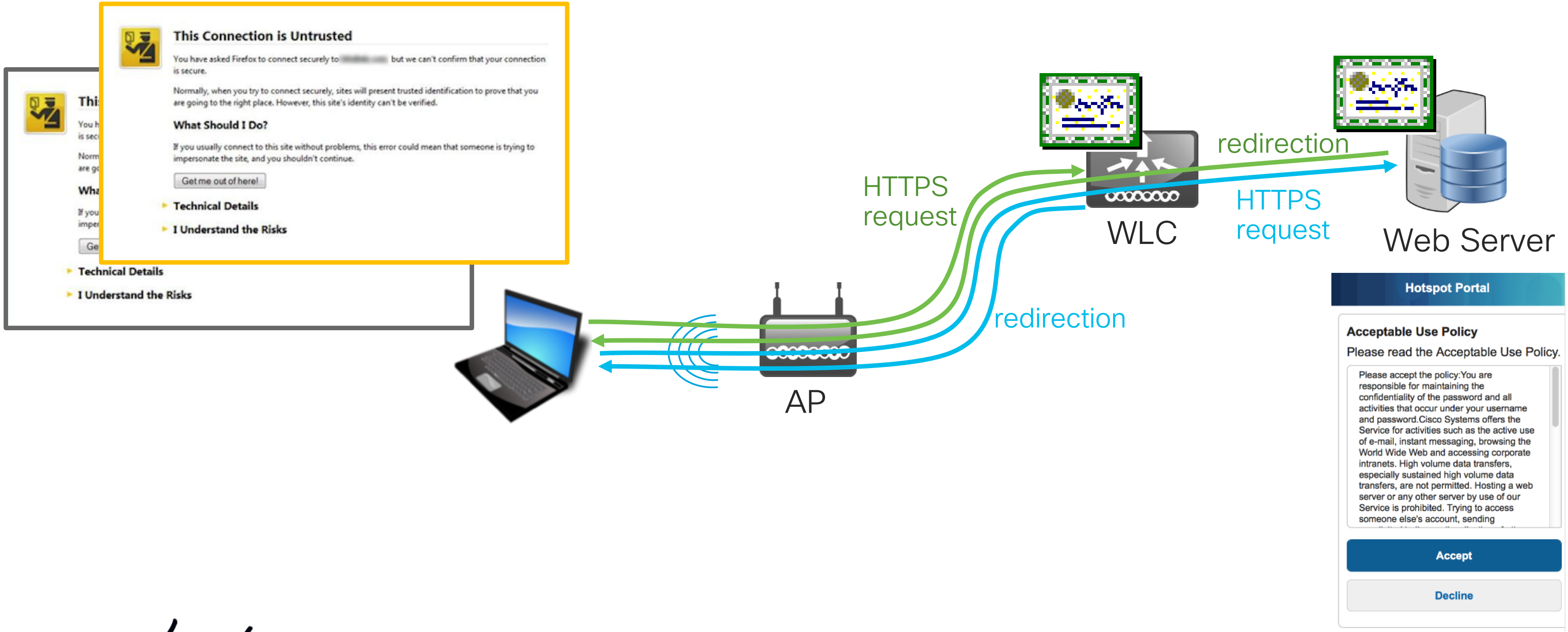
URL https://my-external-web-server.lab:8443/login.html

Web Authentication on WLAN Controller Configuration Example:
http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/115951-web-auth-wlc-guide-00.html

Configure a Web Authentication SSID on Catalyst 9800 Wireless Controllers:
https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213923-configure-a-web-authentication-ssid-on-c.html

# LWA and certificates

## External web portal



**This Connection is Untrusted**

You have asked Firefox to connect securely to [redacted] but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

**What Should I Do?**

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

- Technical Details
- I Understand the Risks

Thi
You h
is sec
Norm
are go
Wha
If you
imper
Ge
Technical Details
I Understand the Risks

**Hotspot Portal**

**Acceptable Use Policy**

Please read the Acceptable Use Policy.

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending

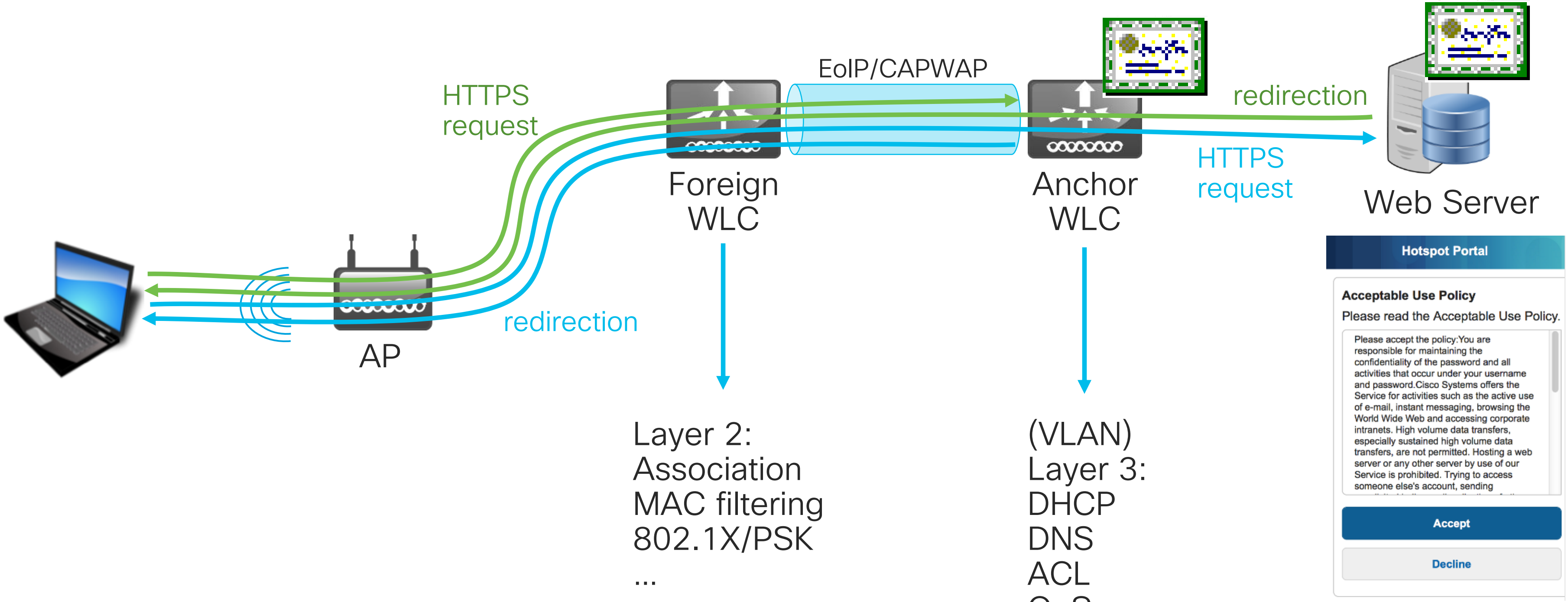
Accept

Decline

# LWA with an anchor controller

## External web portal

For your reference



**Acceptable Use Policy**

Please read the Acceptable Use Policy.

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending

Layer 2:
Association
MAC filtering
802.1X/PSK
...

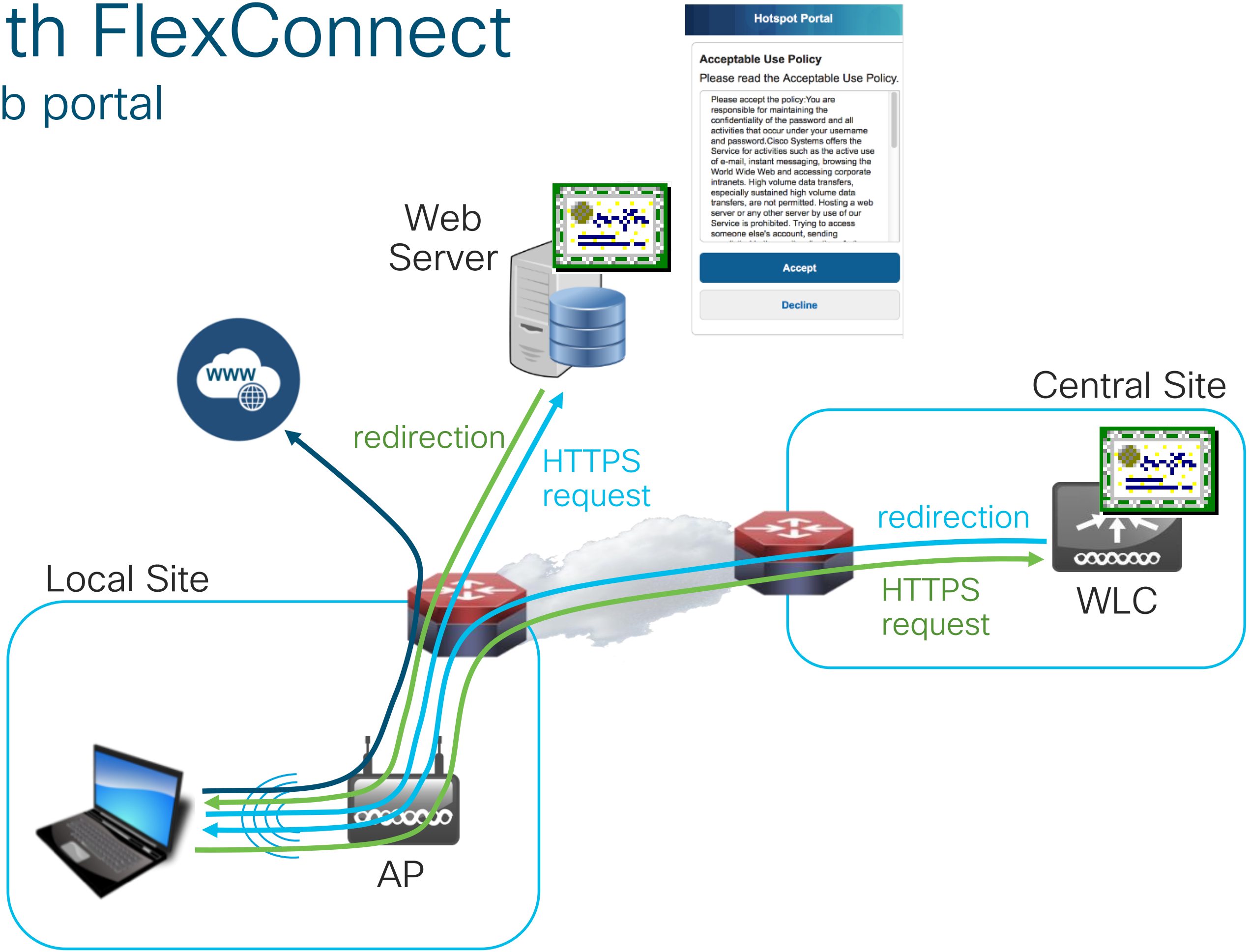
(VLAN)
Layer 3:
DHCP
DNS
ACL
QoS
...

cisco Live!

# LWA with FlexConnect

## External web portal

For your reference



Hotspot Portal

**Acceptable Use Policy**

Please read the Acceptable Use Policy.

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending

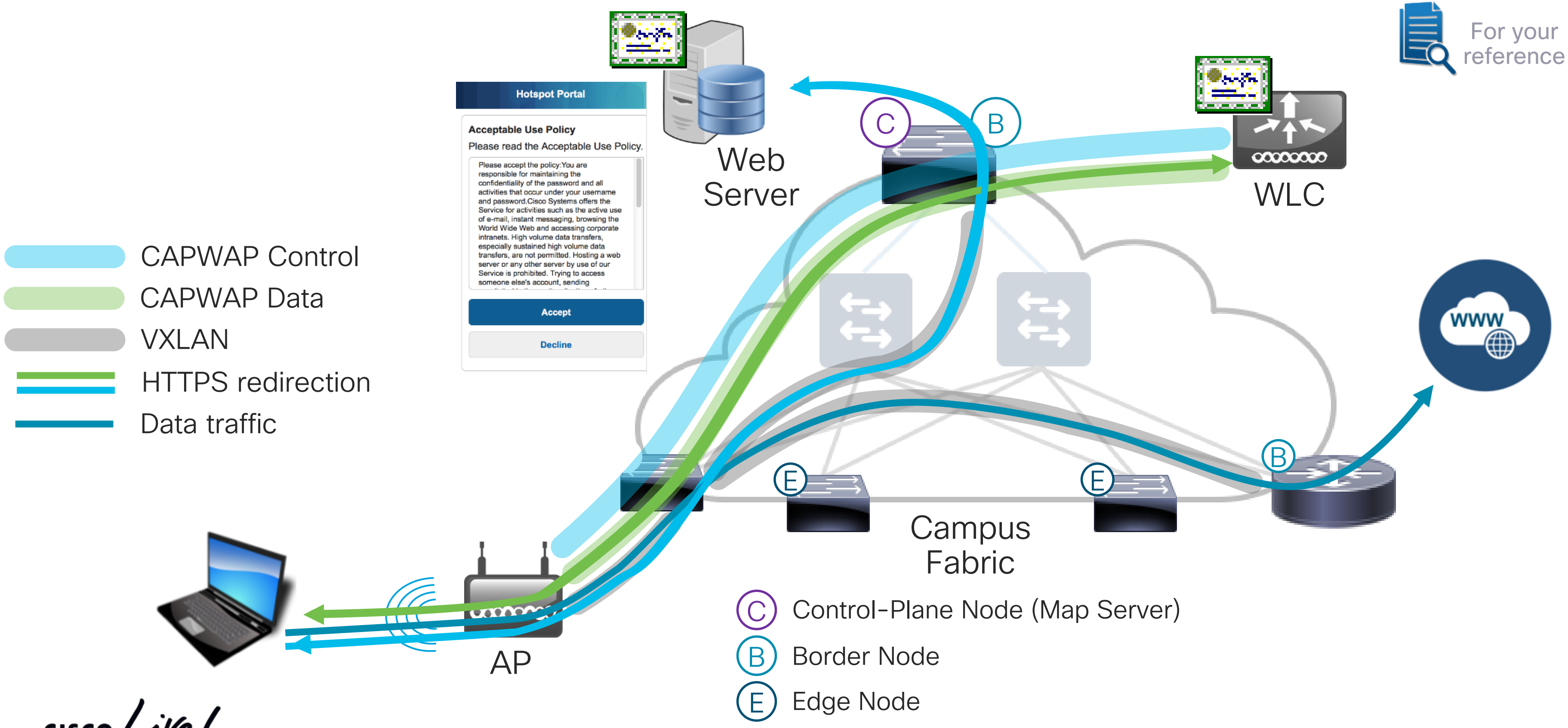
cisco Live!

# LWA with Cisco DNA Campus Fabric

## External web portal

BRKEWN-2020

For your reference



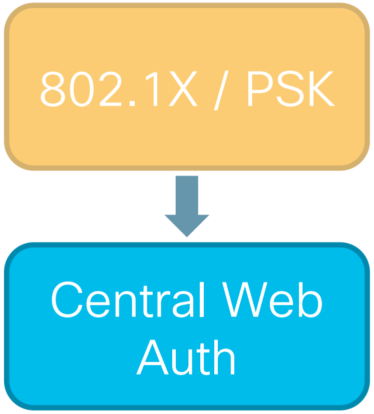
Hotspot Portal

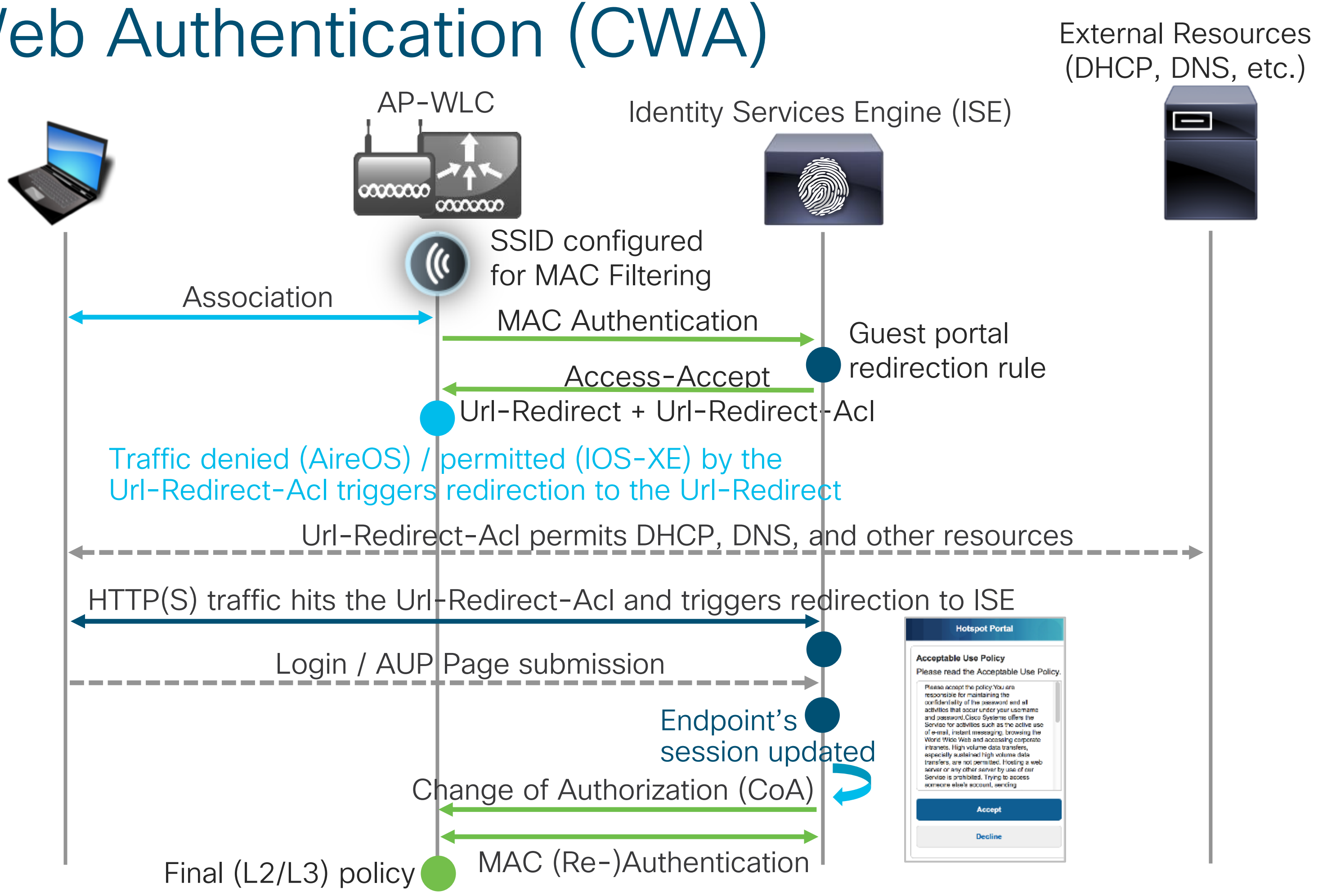
**Acceptable Use Policy**

Please read the Acceptable Use Policy.

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending

# Central Web Authentication (CWA)




External Resources (DHCP, DNS, etc.)
AP-WLC
Identity Services Engine (ISE)
SSID configured for MAC Filtering
Association
MAC Authentication
Guest portal redirection rule
Access-Accept
Url-Redirect + Url-Redirect-Acl
Traffic denied (AireOS) / permitted (IOS-XE) by the Url-Redirect-Acl triggers redirection to the Url-Redirect
Url-Redirect-Acl permits DHCP, DNS, and other resources
HTTP(S) traffic hits the Url-Redirect-Acl and triggers redirection to ISE
Login / AUP Page submission
Endpoint's session updated
Change of Authorization (CoA)
MAC (Re-)Authentication
Final (L2/L3) policy
Hotspot Portal
Accept
Decline

Acceptable Use Policy

Please read the Acceptable Use Policy.

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending

**CENTRAL** because the redirection URL and the pre-webauth ACL are **centrally** configured on ISE and communicated to the WLC via RADIUS.

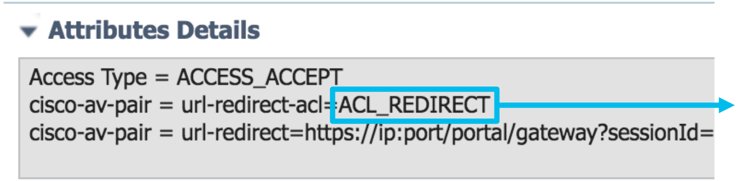
cisco Live!

# URL-Redirect-Acl considerations

## AireOS

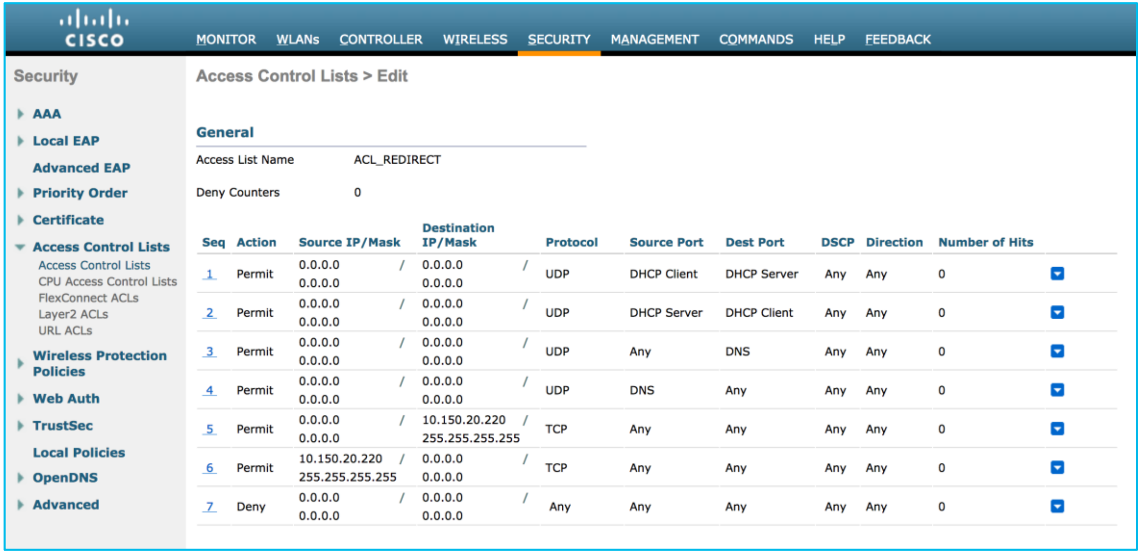
For your reference

For Cisco AireOS based NADs (e.g., 3504, 5520, 8540 WLCs), traffic denied by the Url-Redirect-Acl triggers redirection to the Url-Redirect.
Other traffic permitted by the Url-Redirect-Acl is simply permitted.



**Attributes Details**

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=ACL_REDIRECT
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=
```



Access Control Lists > Edit

**General**

Access List Name ACL_REDIRECT

Deny Counters 0

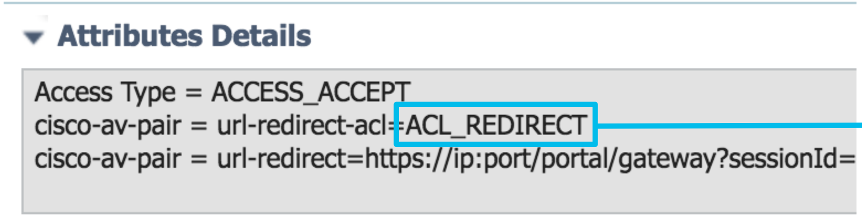
| Seq | Action | Source IP/Mask | Destination IP/Mask | Protocol | Source Port | Dest Port | DSCP | Direction | Number of Hits |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Permit | 0.0.0.0 / 0.0.0.0 | 0.0.0.0 / 0.0.0.0 | UDP | DHCP Client | DHCP Server | Any | Any | 0 |
| 2 | Permit | 0.0.0.0 / 0.0.0.0 | 0.0.0.0 / 0.0.0.0 | UDP | DHCP Server | DHCP Client | Any | Any | 0 |
| 3 | Permit | 0.0.0.0 / 0.0.0.0 | 0.0.0.0 / 0.0.0.0 | UDP | Any | DNS | Any | Any | 0 |
| 4 | Permit | 0.0.0.0 / 0.0.0.0 | 0.0.0.0 / 0.0.0.0 | UDP | DNS | Any | Any | Any | 0 |
| 5 | Permit | 0.0.0.0 / 0.0.0.0 | 10.150.20.220 / 255.255.255.255 | TCP | Any | Any | Any | Any | 0 |
| 6 | Permit | 10.150.20.220 / 255.255.255.255 | 0.0.0.0 / 0.0.0.0 | TCP | Any | Any | Any | Any | 0 |
| 7 | Deny | 0.0.0.0 / 0.0.0.0 | 0.0.0.0 / 0.0.0.0 | Any | Any | Any | Any | Any | 0 |

# URL-Redirect-Acl considerations

## IOS-XE

For your reference

For C9800, traffic permitted by the Url-Redirect-Acl triggers redirection to the Url-Redirect and other traffic denied by the Url-Redirect-Acl is simply permitted.



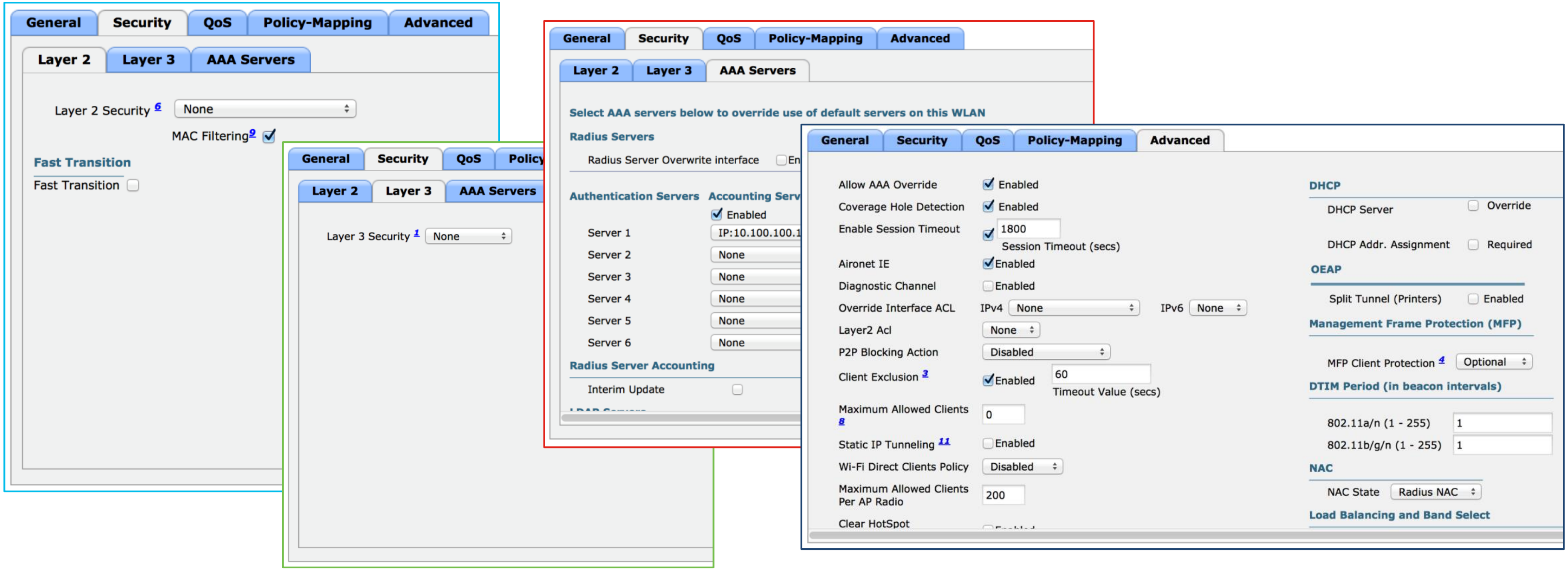
**Attributes Details**

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=ACL_REDIRECT
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=
```

```
ip access-list extended ACL_REDIRECT
 deny udp any eq bootpc any eq bootps
 deny udp any any eq domain
 deny ip any host 10.150.20.220 eq 8443
 permit ip any any
```

# CWA – configuration example

For your reference



Layer 2 Security [6] None

MAC Filtering[9] ☑

**Fast Transition**

Fast Transition □

Layer 3 Security [1] None

**Select AAA servers below to override use of default servers on this WLAN**

**Radius Servers**

Radius Server Overwrite interface □ En

| Authentication Servers | Accounting Serv |
|---|---|
| | ☑ Enabled |
| Server 1 | IP:10.100.100.1 |
| Server 2 | None |
| Server 3 | None |
| Server 4 | None |
| Server 5 | None |
| Server 6 | None |

**Radius Server Accounting**

Interim Update □

| | |
|---|---|
| Allow AAA Override | ☑ Enabled |
| Coverage Hole Detection | ☑ Enabled |
| Enable Session Timeout | ☑ 1800 Session Timeout (secs) |
| Aironet IE | ☑ Enabled |
| Diagnostic Channel | □ Enabled |
| Override Interface ACL | IPv4 None IPv6 None |
| Layer2 Acl | None |
| P2P Blocking Action | Disabled |
| Client Exclusion [3] | ☑ Enabled 60 Timeout Value (secs) |
| Maximum Allowed Clients [8] | 0 |
| Static IP Tunneling [11] | □ Enabled |
| Wi-Fi Direct Clients Policy | Disabled |
| Maximum Allowed Clients Per AP Radio | 200 |
| Clear HotSpot | □ Enabled |

**DHCP**

DHCP Server □ Override

DHCP Addr. Assignment □ Required

**OEAP**

Split Tunnel (Printers) □ Enabled

**Management Frame Protection (MFP)**

MFP Client Protection [4] Optional

**DTIM Period (in beacon intervals)**

802.11a/n (1 - 255) 1

802.11b/g/n (1 - 255) 1

**NAC**

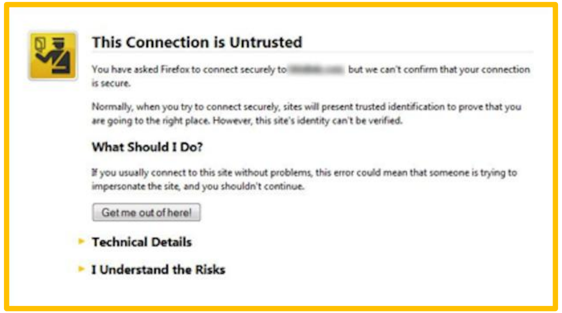
NAC State Radius NAC

**Load Balancing and Band Select**

Central Web Authentication on the WLC and ISE Configuration Example: http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html

# CWA and certificates

2059
BRKSEC-



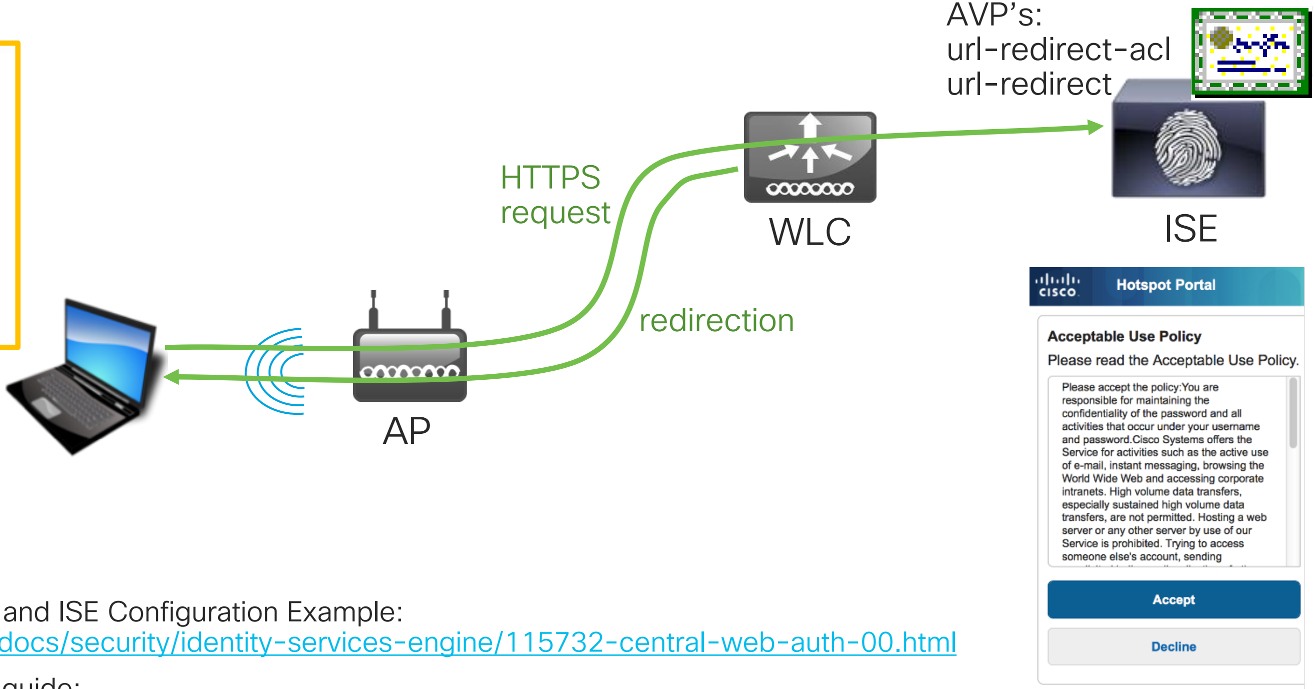
**This Connection is Untrusted**

You have asked Firefox to connect securely to [redacted] but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

**What Should I Do?**

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.



AVP's:
url-redirect-acl
url-redirect

**Acceptable Use Policy**

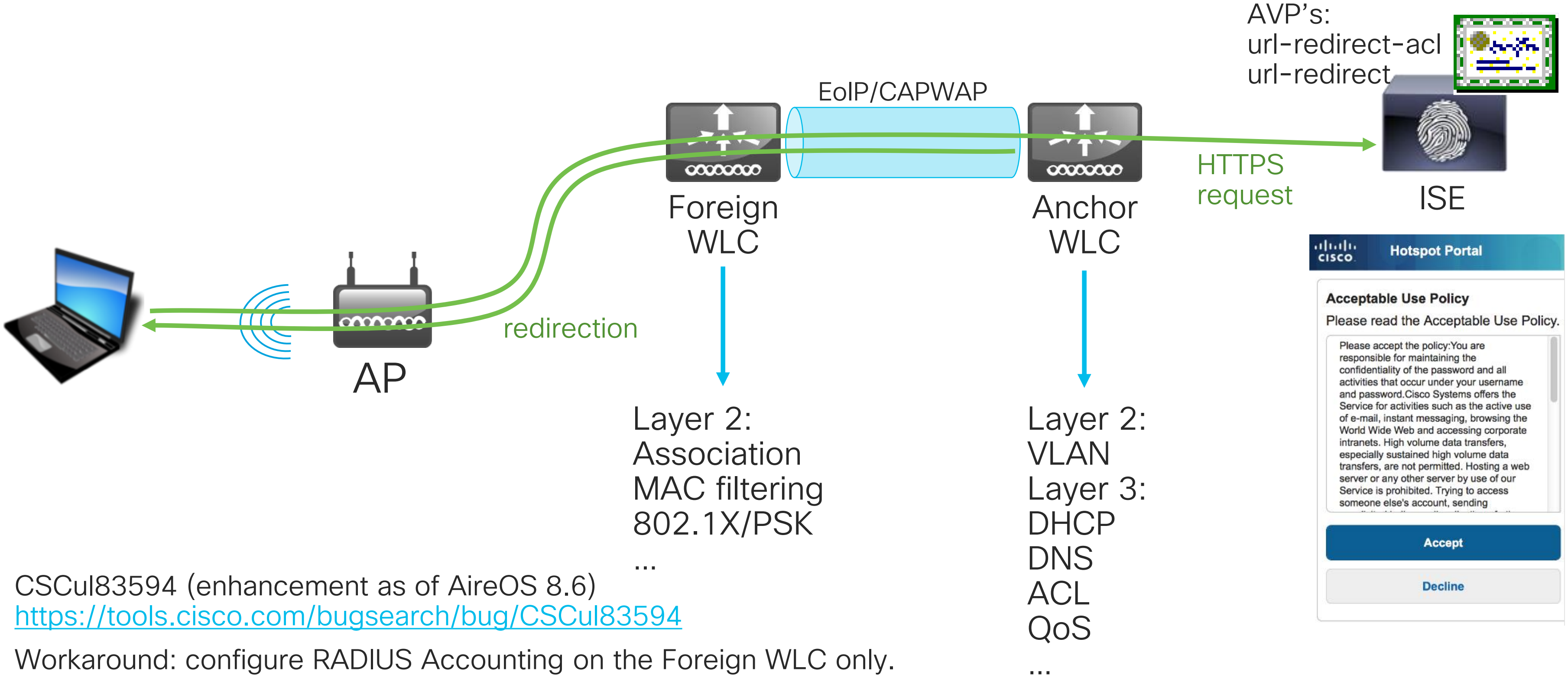
Please read the Acceptable Use Policy.

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending

Central Web Authentication on the WLC and ISE Configuration Example:
http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html

ISE and Catalyst 9800 series integration guide:
https://community.cisco.com/t5/security-documents/ise-and-catalyst-9800-series-integration-guide/ta-p/3753060

# CWA with an anchor controller



Layer 2:
Association
MAC filtering
802.1X/PSK
…

Layer 2:
VLAN
Layer 3:
DHCP
DNS
ACL
QoS
…

**Acceptable Use Policy**

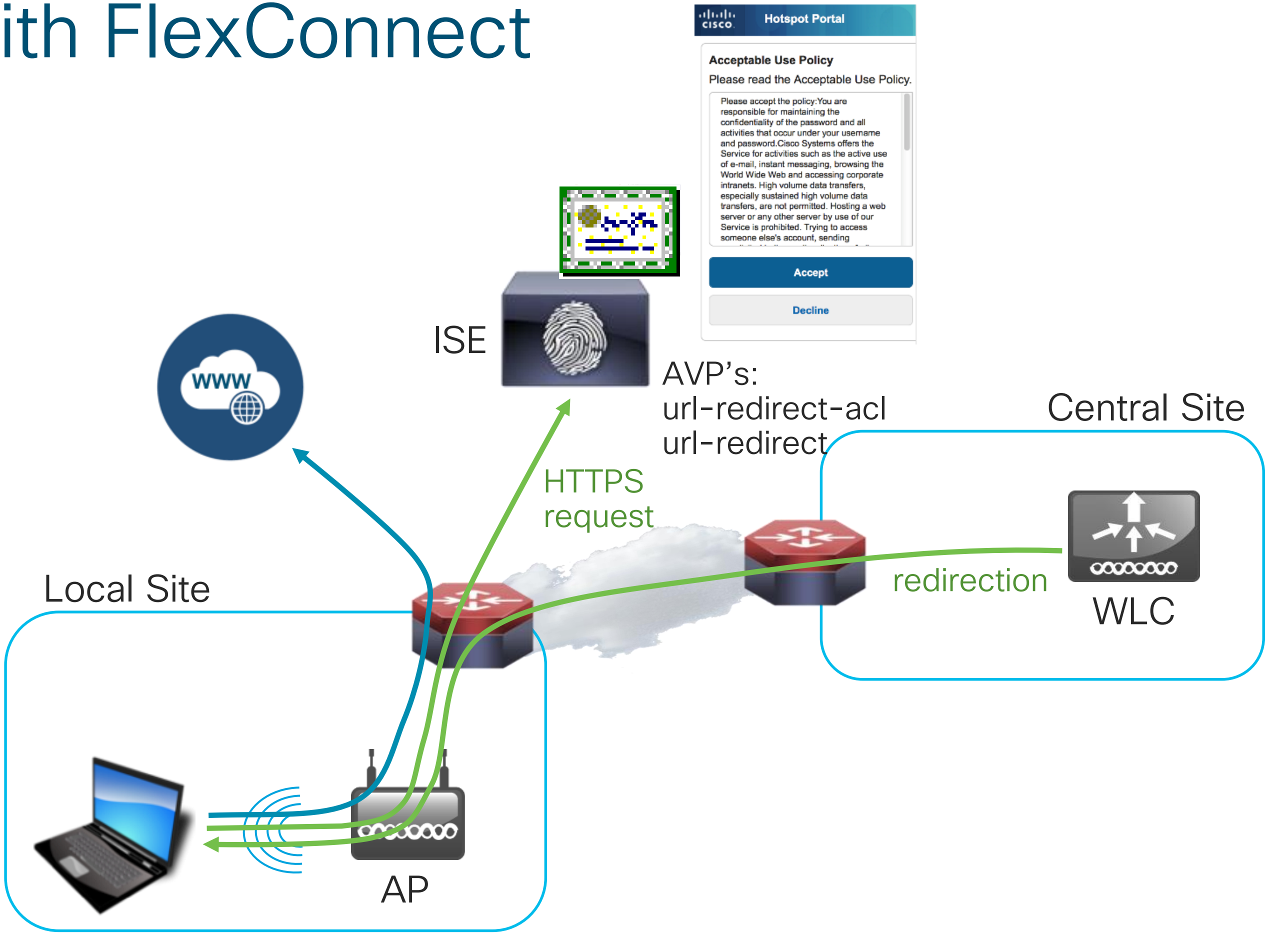
Please read the Acceptable Use Policy.

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending

CSCul83594 (enhancement as of AireOS 8.6)
[https://tools.cisco.com/bugsearch/bug/CSCul83594](https://tools.cisco.com/bugsearch/bug/CSCul83594)

Workaround: configure RADIUS Accounting on the Foreign WLC only.

# CWA with FlexConnect



Hotspot Portal

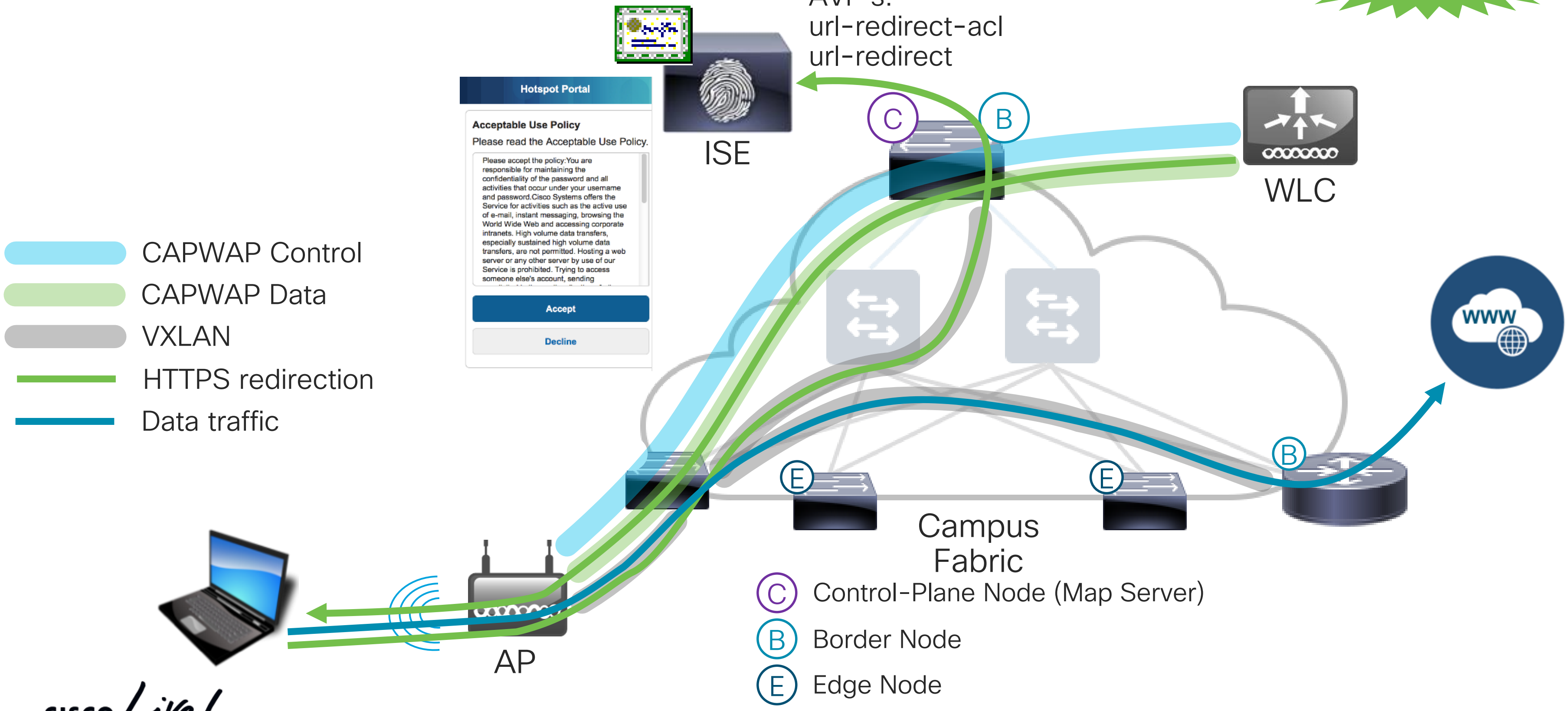
**Acceptable Use Policy**

Please read the Acceptable Use Policy.

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending

# CWA with Software-Defined Access (SDA)

BRKEWN-2020



Hotspot Portal

**Acceptable Use Policy**

Please read the Acceptable Use Policy.

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending

Accept

Decline

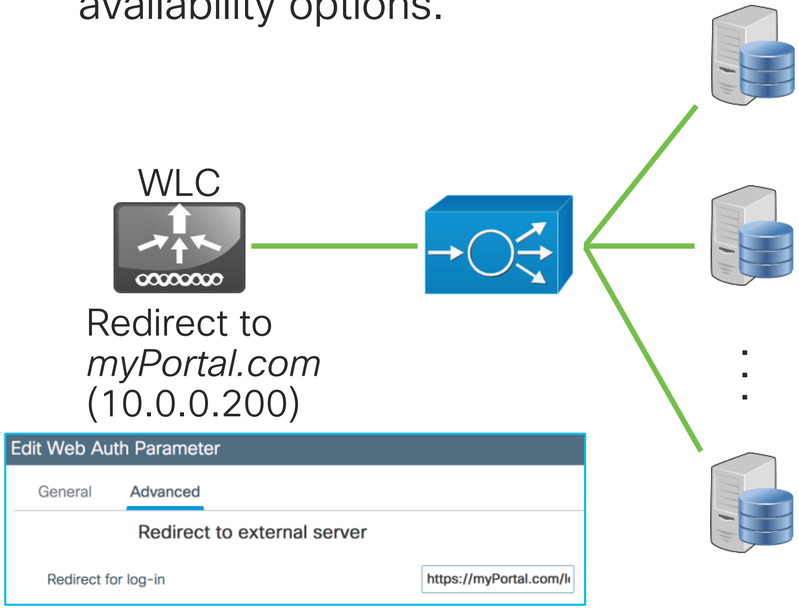
AVP's:
url-redirect-acl
url-redirect

# LWA vs. CWA: main differences

BRKSEC-3432

- LWA happens at L3.
- LWA needs to rely on IP/DNS high availability options.

- CWA happens at L2 and L3.
- CWA can rely on RADIUS / ISE high availability options.



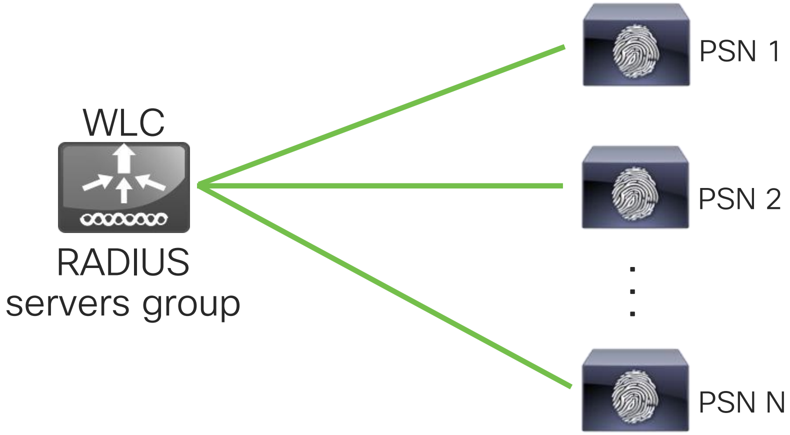
WLC

Redirect to *myPortal.com* (10.0.0.200)

Edit Web Auth Parameter

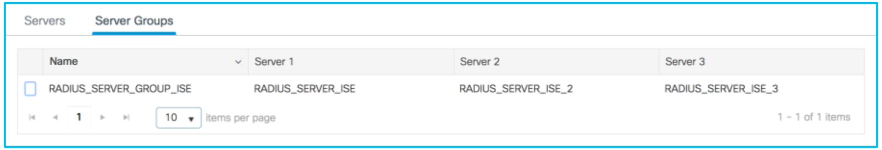
Redirect to external server

Redirect for log-in: https://myPortal.com/l



WLC

RADIUS servers group



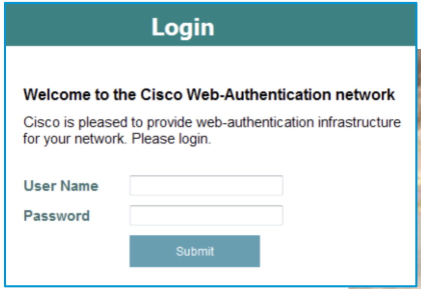
| | Name | Server 1 | Server 2 | Server 3 |
|---|---|---|---|---|
| □ | RADIUS_SERVER_GROUP_ISE | RADIUS_SERVER_ISE | RADIUS_SERVER_ISE_2 | RADIUS_SERVER_ISE_3 |

1 | 10 items per page | 1 - 1 of 1 items

# The right solution for the right needs

# So... which one should I (not) go for?

WLC



**Login**

**Welcome to the Cisco Web-Authentication network**

Cisco is pleased to provide web-authentication infrastructure for your network. Please login.

User Name

Password

Submit

Cisco DNA Spaces

Cisco DNA Spaces

Not us 😬

Cisco Sponsored Guest Portal

Identity Services Engine (ISE)

# WLC’s internal portal

- It’s free ☺
- It supports some customization on a per-web auth parameter map / WLAN basis:

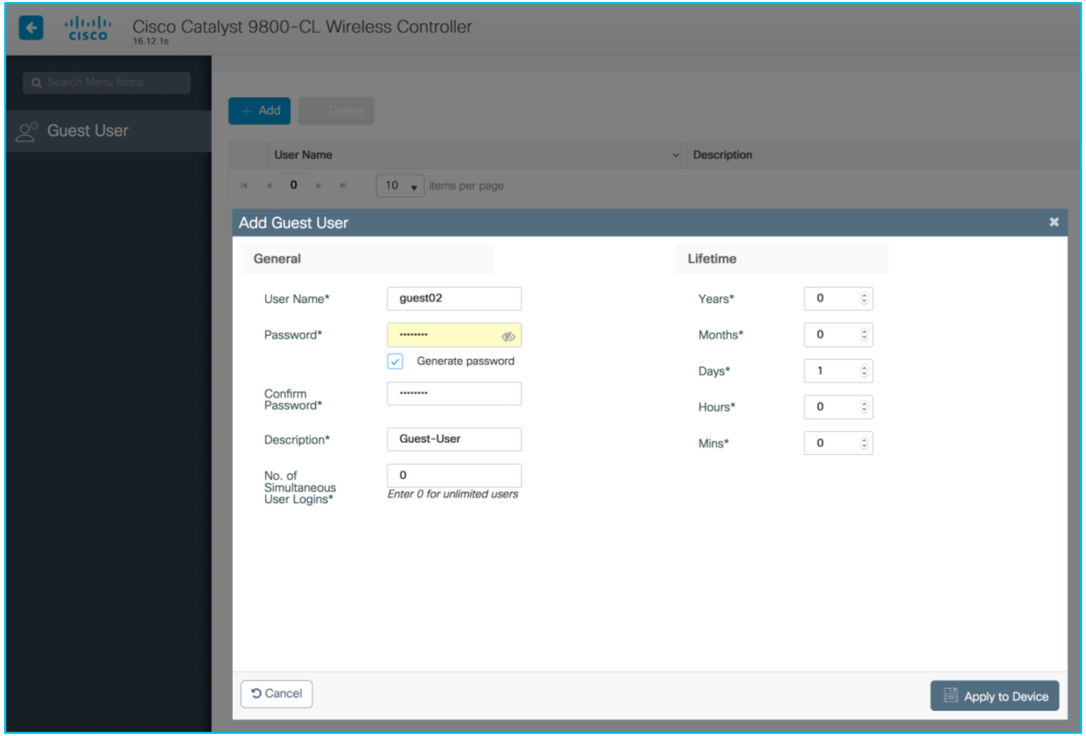
```
C9800-CL-A#dir bootflash:/custom-portals
Directory of bootflash:/custom-portals/

331938  -rw-            4082   Dec 5 2019 15:15:32 +00:00  login.html
331939  -rw-            2574   Dec 5 2019 15:31:18 +00:00  aup.html
331940  -rw-             344   Dec 5 2019 15:31:23 +00:00  failed.html
331941  -rw-             318   Dec 5 2019 15:31:31 +00:00  loginscript.js
331942  -rw-            1116   Dec 5 2019 15:31:37 +00:00  logout.html
331943  -rw-           18432   Dec 5 2019 15:31:43 +00:00  Thumbs.db
331944  -rw-           70123   Dec 5 2019 15:31:48 +00:00  yourlogo.jpg

C9800-CL-A#
C9800-CL-A#conf t
C9800-CL-A(config)#parameter-map type webauth WEBAUTH_PMAP_GUEST
C9800-CL-A(config-params-parameter-map)#custom-page login device bootflash:/custom-portals/login.html
```

Configure a Web Authentication SSID on Catalyst 9800 Wireless Controllers
https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213923-configure-a-web-authentication-ssid-on-c.html

# Creating guest accounts

## Lobby Ambassador

- Some options to create guest accounts on the WLC's internal database (as of IOS-XE 16.12.1s).



Add Guest User

General

| | |
|---|---|
| User Name* | guest02 |
| Password* | •••••••• |
| | ☑ Generate password |
| Confirm Password* | •••••••• |
| Description* | Guest-User |
| No. of Simultaneous User Logins* | 0<br>*Enter 0 for unlimited users* |

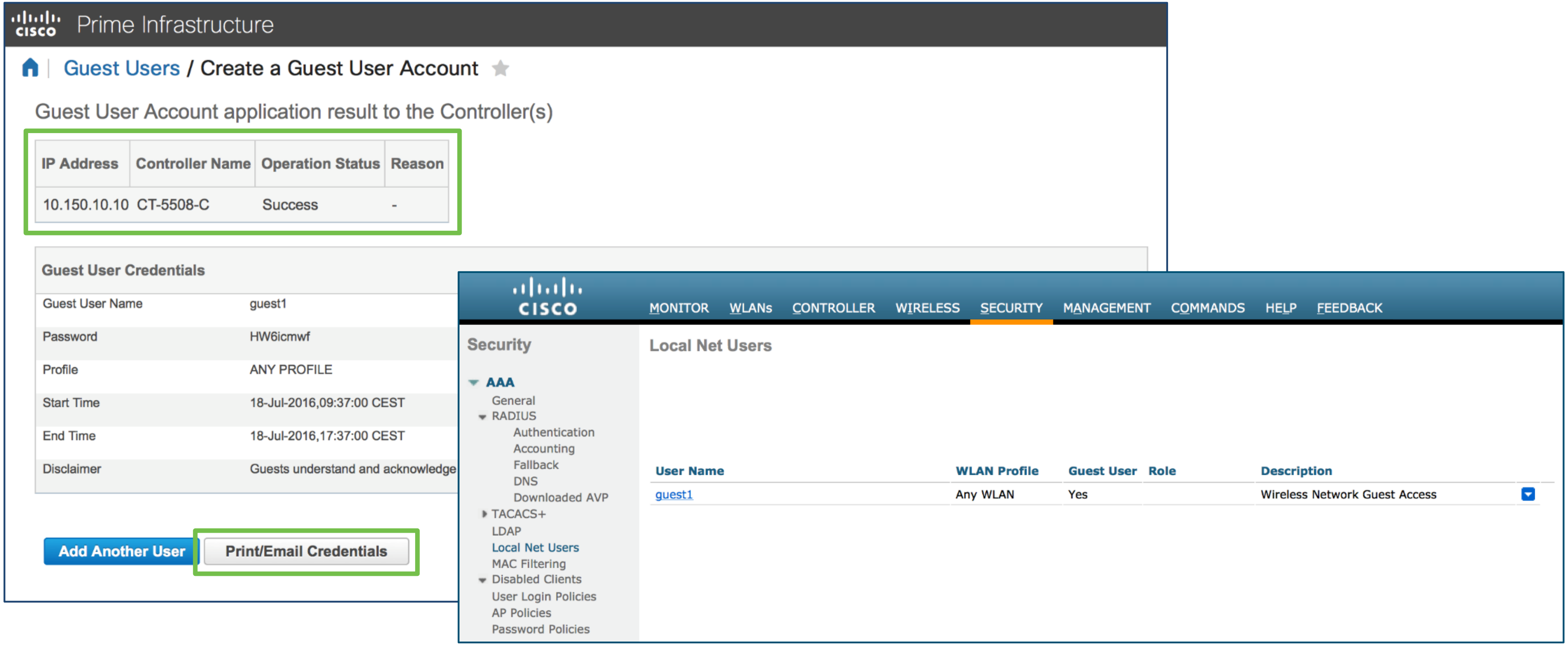
Lifetime

| | |
|---|---|
| Years* | 0 |
| Months* | 0 |
| Days* | 1 |
| Hours* | 0 |
| Mins* | 0 |

# Some more options with Prime

## For AireOS only

For your reference



Prime Infrastructure

Guest Users / Create a Guest User Account

Guest User Account application result to the Controller(s)

| IP Address | Controller Name | Operation Status | Reason |
|---|---|---|---|
| 10.150.10.10 | CT-5508-C | Success | - |

Guest User Credentials

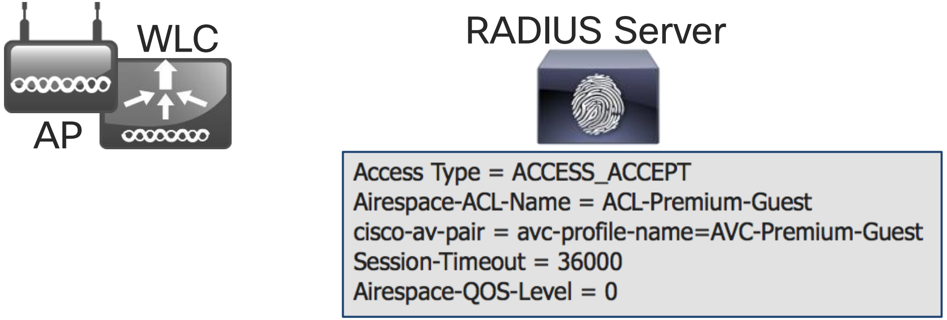
| | |
|---|---|
| Guest User Name | guest1 |
| Password | HW6icmwf |
| Profile | ANY PROFILE |
| Start Time | 18-Jul-2016,09:37:00 CEST |
| End Time | 18-Jul-2016,17:37:00 CEST |
| Disclaimer | Guests understand and acknowledge |

Local Net Users

| User Name | WLAN Profile | Guest User | Role | Description |
|---|---|---|---|---|
| guest1 | Any WLAN | Yes | | Wireless Network Guest Access |

# Authorization options for guest accounts

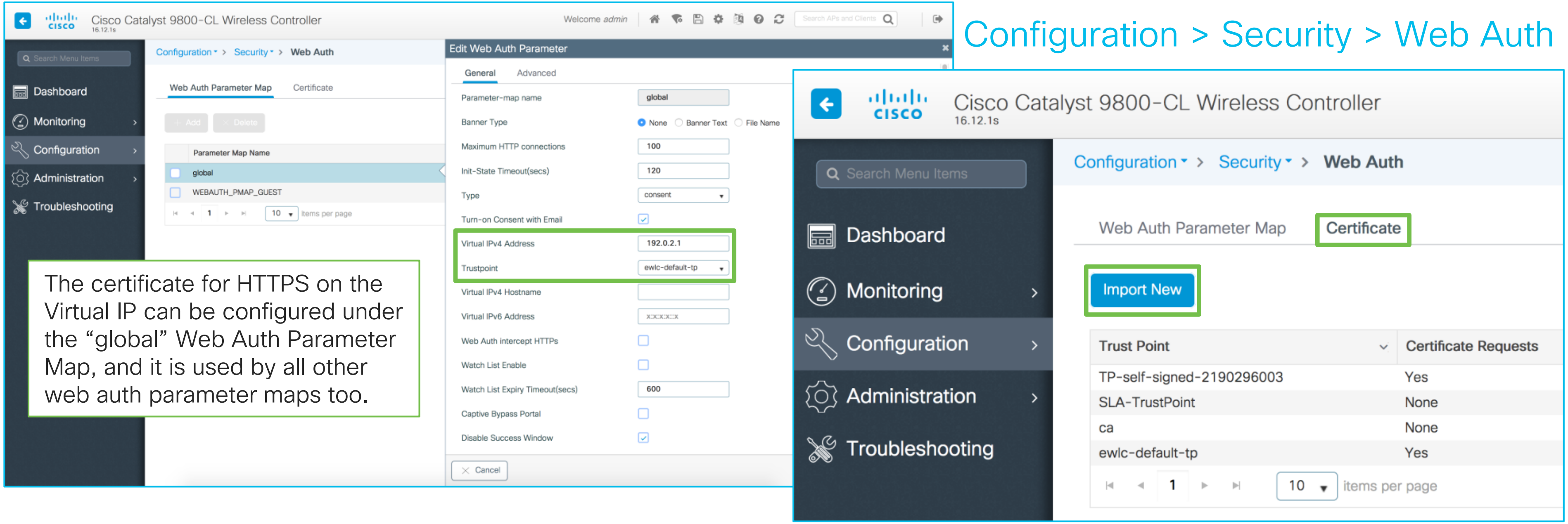
- If using the internal database we can dynamically assign QoS Roles (i.e., bidirectional rate limits) in AireOS.
- If using an external database, we can assign more Layer 3 policies per user:
  - QoS;
  - ACL;
  - AVC Profile (central switching);
  - session timeout;
  - Security Group Tag (SGT);
  - etc.



Access Type = ACCESS_ACCEPT
Airespace-ACL-Name = ACL-Premium-Guest
cisco-av-pair = avc-profile-name=AVC-Premium-Guest
Session-Timeout = 36000
Airespace-QOS-Level = 0

# C9800’s internal portal

## Certificates for the web portal



Configuration > Security > Web Auth

| Parameter Map Name |
|---|
| global |
| WEBAUTH_PMAP_GUEST |

Edit Web Auth Parameter – General

- Parameter-map name: global
- Banner Type: ● None ○ Banner Text ○ File Name
- Maximum HTTP connections: 100
- Init-State Timeout(secs): 120
- Type: consent
- Turn-on Consent with Email: ☑
- Virtual IPv4 Address: 192.0.2.1
- Trustpoint: ewlc-default-tp
- Virtual IPv4 Hostname:
- Virtual IPv6 Address: X:X:X:X::X
- Web Auth intercept HTTPs: □
- Watch List Enable: □
- Watch List Expiry Timeout(secs): 600
- Captive Bypass Portal: □
- Disable Success Window: ☑

The certificate for HTTPS on the Virtual IP can be configured under the “global” Web Auth Parameter Map, and it is used by all other web auth parameter maps too.

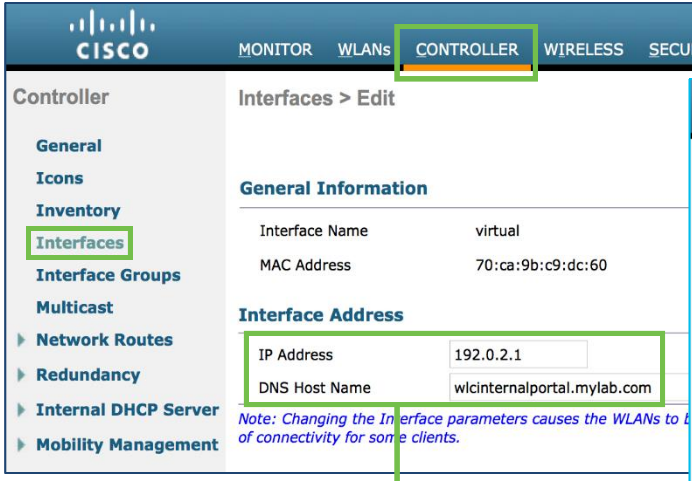
| Trust Point | Certificate Requests |
|---|---|
| TP-self-signed-2190296003 | Yes |
| SLA-TrustPoint | None |
| ca | None |
| ewlc-default-tp | Yes |

Generate CSR for Third-Party Certificates and Download Chained Certificates to Catalyst 9800 Wireless Controllers
https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213917-generate-csr-for-third-party-certificate.html

# WLC’s internal portal

## Certificates for the Virtual Interface’s IP / FQDN

For your reference



Interfaces > Edit

**General Information**

| | |
|---|---|
| Interface Name | virtual |
| MAC Address | 70:ca:9b:c9:dc:60 |

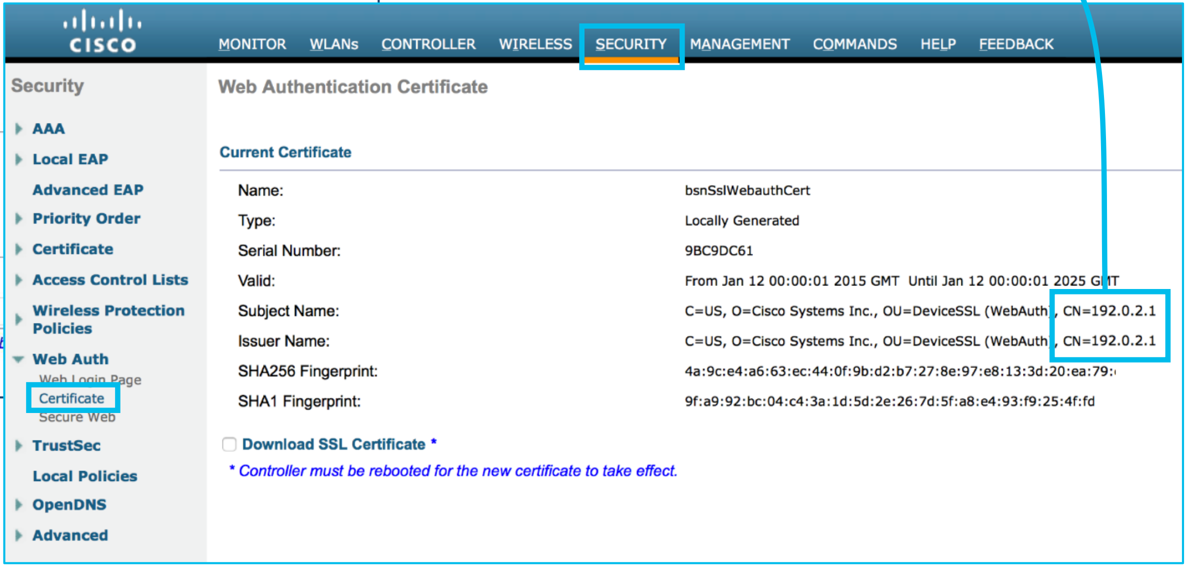
**Interface Address**

| | |
|---|---|
| IP Address | 192.0.2.1 |
| DNS Host Name | wlcinternalportal.mylab.com |

*Note: Changing the In erface parameters causes the WLANs to t of connectivity for som e clients.*

Used in the Common Name (CN) of the certificate.

By default the CN is the Virtual IP, both as Subject and Issuer (self-signed).



Web Authentication Certificate

**Current Certificate**

| | |
|---|---|
| Name: | bsnSslWebauthCert |
| Type: | Locally Generated |
| Serial Number: | 9BC9DC61 |
| Valid: | From Jan 12 00:00:01 2015 GMT Until Jan 12 00:00:01 2025 GMT |
| Subject Name: | C=US, O=Cisco Systems Inc., OU=DeviceSSL (WebAuth), CN=192.0.2.1 |
| Issuer Name: | C=US, O=Cisco Systems Inc., OU=DeviceSSL (WebAuth), CN=192.0.2.1 |
| SHA256 Fingerprint: | 4a:9c:e4:a6:63:ec:44:0f:9b:d2:b7:27:8e:97:e8:13:3d:20:ea:79: |
| SHA1 Fingerprint: | 9f:a9:92:bc:04:c4:3a:1d:5d:2e:26:7d:5f:a8:e4:93:f9:25:4f:fd |

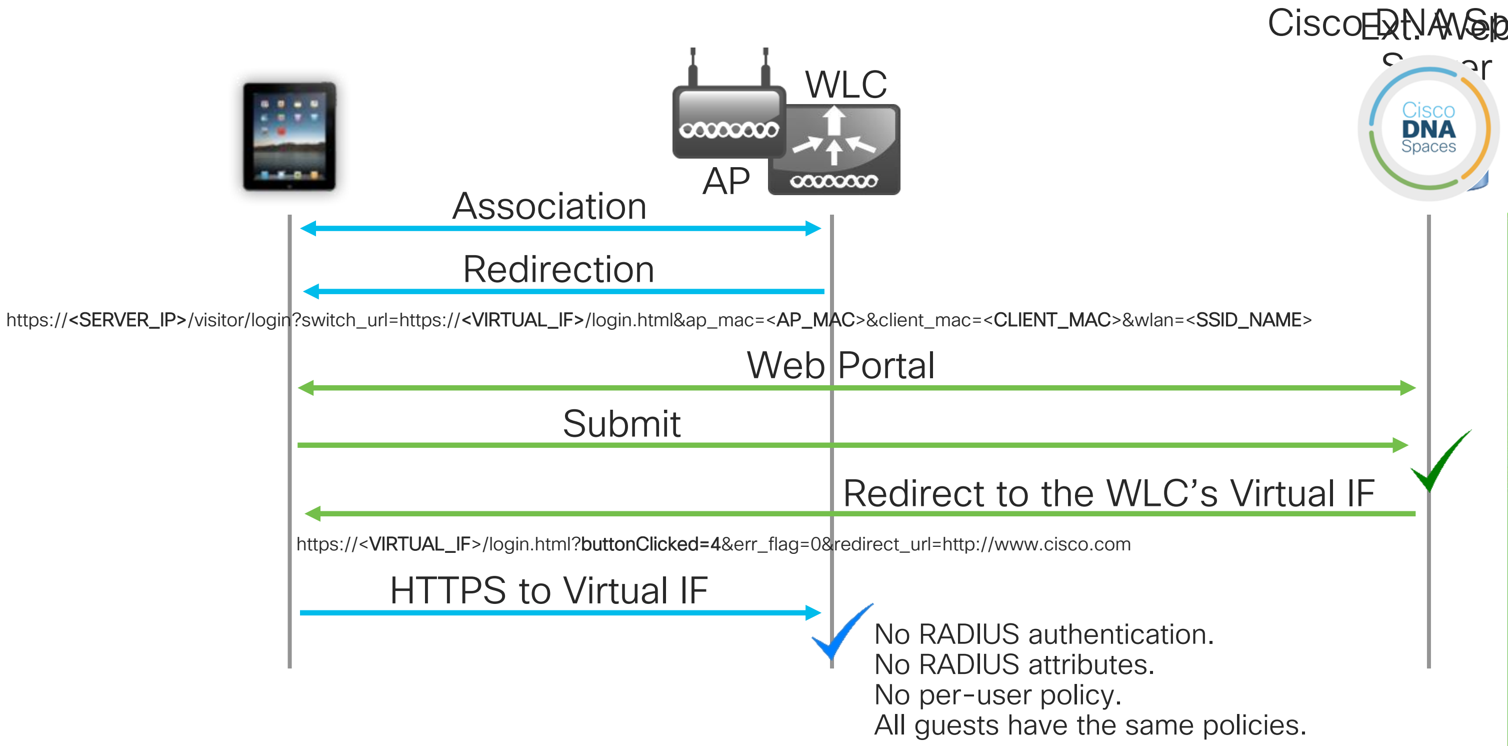
□ Download SSL Certificate *

** Controller must be rebooted for the new certificate to take effect.*

Generate CSR for Third-Party Certificates and Download Chained Certificates to the WLC:
http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/109597-csr-chained-certificates-wlc-00.html

# WLC – LWA passthrough with an external server

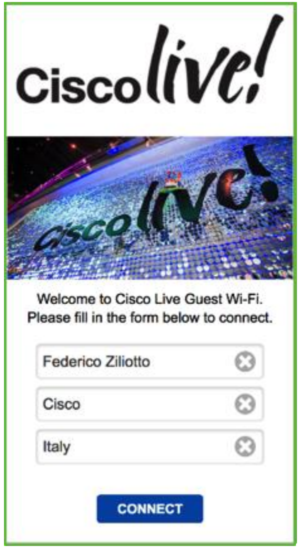
## Delegating to an external web server and differentiating portals by AP / site



https://<SERVER_IP>/visitor/login?switch_url=https://<VIRTUAL_IF>/login.html&ap_mac=<AP_MAC>&client_mac=<CLIENT_MAC>&wlan=<SSID_NAME>

https://<VIRTUAL_IF>/login.html?buttonClicked=4&err_flag=0&redirect_url=http://www.cisco.com

No RADIUS authentication.
No RADIUS attributes.
No per-user policy.
All guests have the same policies.



Welcome to Cisco Live Guest Wi-Fi.
Please fill in the form below to connect.

Federico Ziliotto

Cisco

Italy

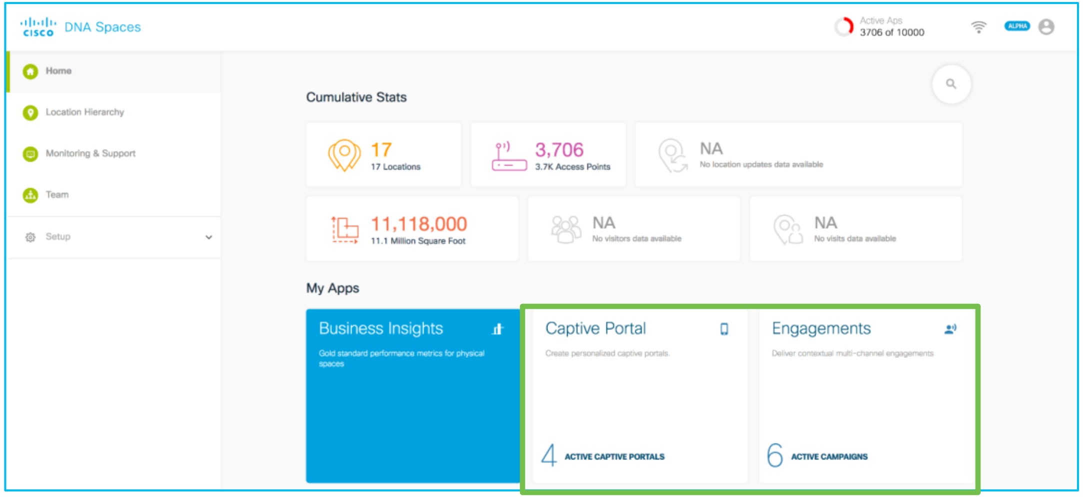
CONNECT

# *Say “CMX” again*

# CMX Connect ➔ CMX Engage ➔ DNA Spaces

BRKEWN-2012

- **CMX Connect**: former on-premise solution
  **CMX Engage**: CMX Connect cloud-based
  **DNA Spaces**: new version of CMX Engage, following from the July Systems acquisition with additional features
- DNA Spaces provides tools for GDPR compliance (database encryption, opt-in/out features, etc.), as that was one of the first goals of CMX Engage, as well as policies for portal's behavior
- CMX Connect for CMX on-premise will be decommissioned as of 10.7



Cumulative Stats

17
17 Locations

3,706
3.7K Access Points

NA
No location updates data available

11,118,000
11.1 Million Square Foot

NA
No visitors data available

NA
No visits data available

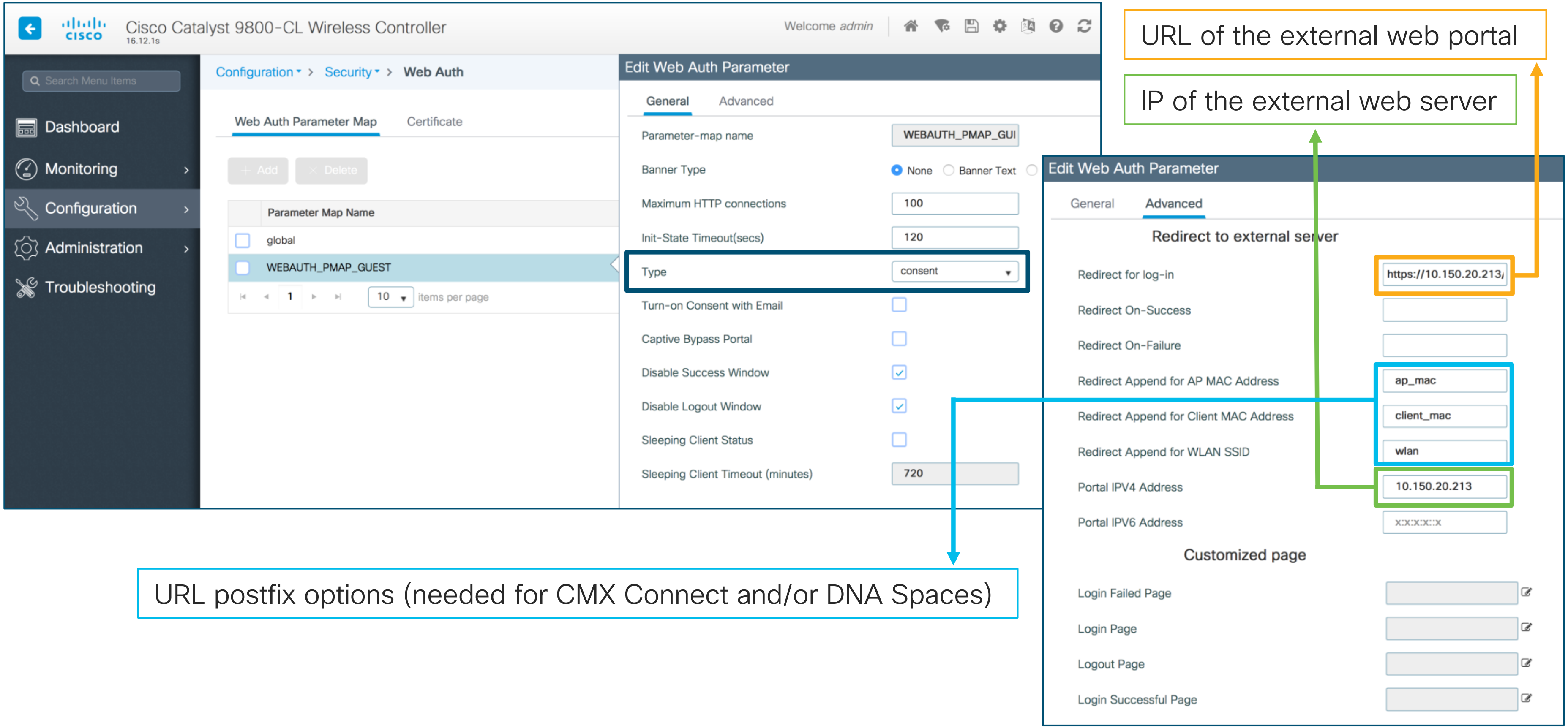
My Apps

Business Insights
Gold standard performance metrics for physical spaces

Captive Portal
Create personalized captive portals.
4 ACTIVE CAPTIVE PORTALS

Engagements
Deliver contextual multi-channel engagements
6 ACTIVE CAMPAIGNS

# Web passthrough/consent on IOS-XE



| | Parameter Map Name |
|---|---|
| □ | global |
| □ | WEBAUTH_PMAP_GUEST |

Edit Web Auth Parameter

General | Advanced

| | |
|---|---|
| Parameter-map name | WEBAUTH_PMAP_GUI |
| Banner Type | ● None ○ Banner Text ○ |
| Maximum HTTP connections | 100 |
| Init-State Timeout(secs) | 120 |
| Type | consent |
| Turn-on Consent with Email | □ |
| Captive Bypass Portal | □ |
| Disable Success Window | ☑ |
| Disable Logout Window | ☑ |
| Sleeping Client Status | □ |
| Sleeping Client Timeout (minutes) | 720 |

Edit Web Auth Parameter

General | Advanced

Redirect to external server

| | |
|---|---|
| Redirect for log-in | https://10.150.20.213/ |
| Redirect On-Success | |
| Redirect On-Failure | |
| Redirect Append for AP MAC Address | ap_mac |
| Redirect Append for Client MAC Address | client_mac |
| Redirect Append for WLAN SSID | wlan |
| Portal IPV4 Address | 10.150.20.213 |
| Portal IPV6 Address | X:X:X:X::X |

Customized page

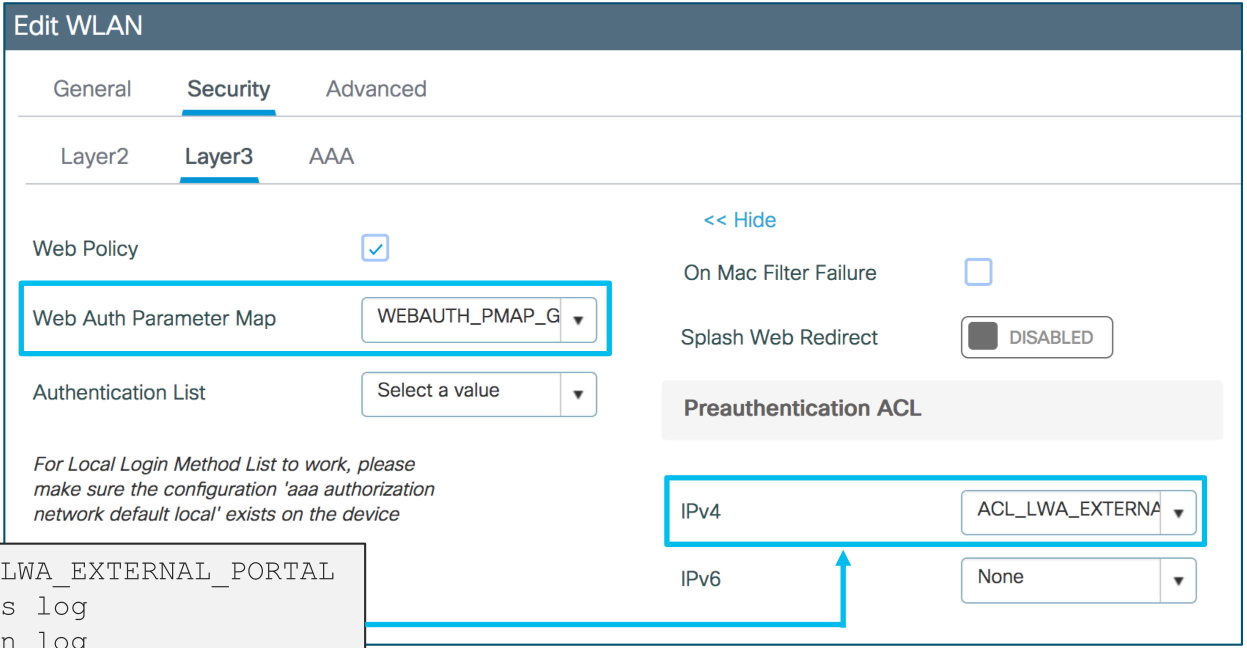
| | |
|---|---|
| Login Failed Page | |
| Login Page | |
| Logout Page | |
| Login Successful Page | |

URL of the external web portal

IP of the external web server

URL postfix options (needed for CMX Connect and/or DNA Spaces)

# Web passthrough/consent on IOS-XE


Edit WLAN

Web Policy ☑

Web Auth Parameter Map: WEBAUTH_PMAP_G

Authentication List: Select a value

*For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device*

On Mac Filter Failure □

Splash Web Redirect: DISABLED

**Preauthentication ACL**

IPv4: ACL_LWA_EXTERNA

IPv6: None

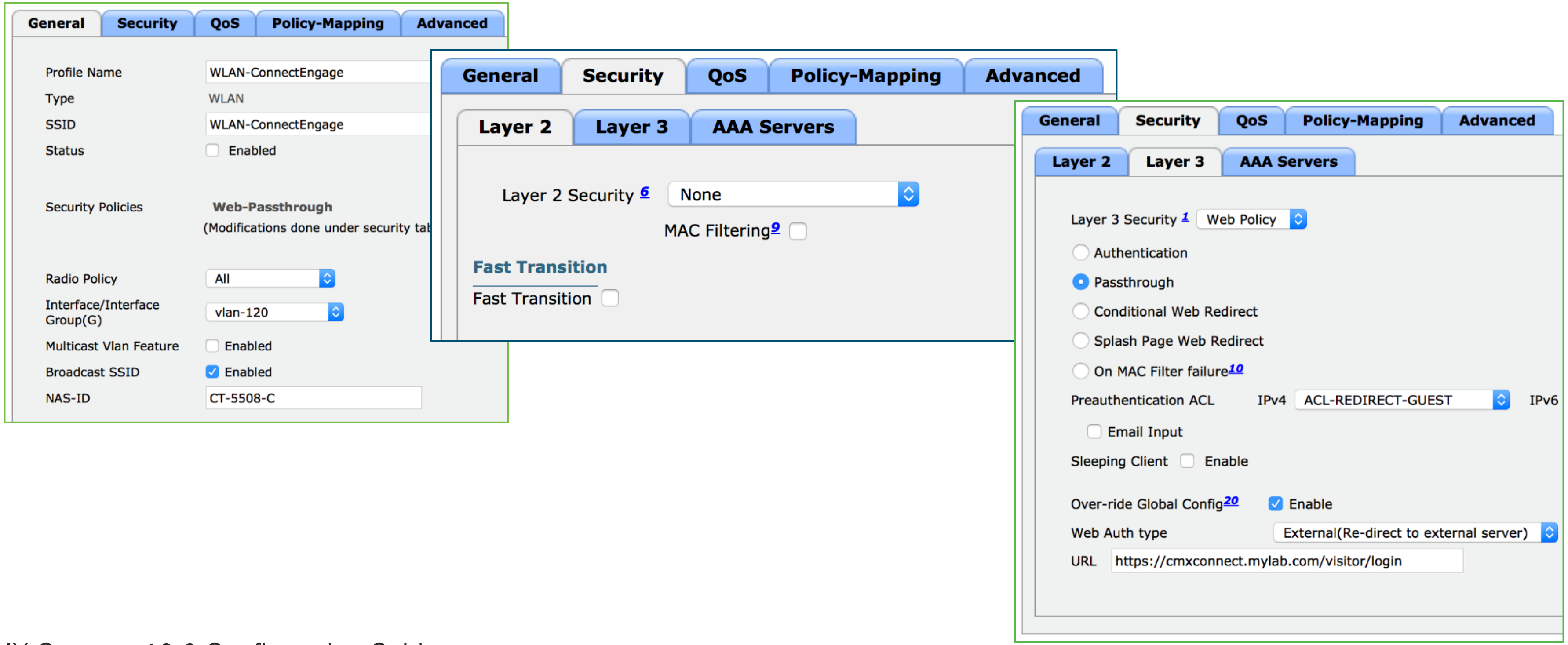
```
ip access-list extended ACL_LWA_EXTERNAL_PORTAL
 permit udp any any eq bootps log
 permit udp any any eq domain log
 permit tcp any host 10.150.20.213 eq 443 log
 deny ip any any log
```

Cisco DNA Spaces Configuration Guide

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/DNA-Spaces/cisco-dna-spaces-config/dnaspaces-configuration-guide/wlc-config.html#task_1402334

# Web passthrough on AireOS

For your reference



| | |
|---|---|
| Profile Name | WLAN-ConnectEngage |
| Type | WLAN |
| SSID | WLAN-ConnectEngage |
| Status | □ Enabled |
| Security Policies | **Web-Passthrough**<br>(Modifications done under security tab |
| Radio Policy | All |
| Interface/Interface Group(G) | vlan-120 |
| Multicast Vlan Feature | □ Enabled |
| Broadcast SSID | ☑ Enabled |
| NAS-ID | CT-5508-C |

| | |
|---|---|
| Layer 2 Security [6] | None |
| MAC Filtering [9] | □ |

**Fast Transition**

Fast Transition □

Layer 3 Security [1] Web Policy

○ Authentication

● Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

○ On MAC Filter failure[10]

Preauthentication ACL IPv4 ACL-REDIRECT-GUEST IPv6

□ Email Input

Sleeping Client □ Enable

Over-ride Global Config[20] ☑ Enable

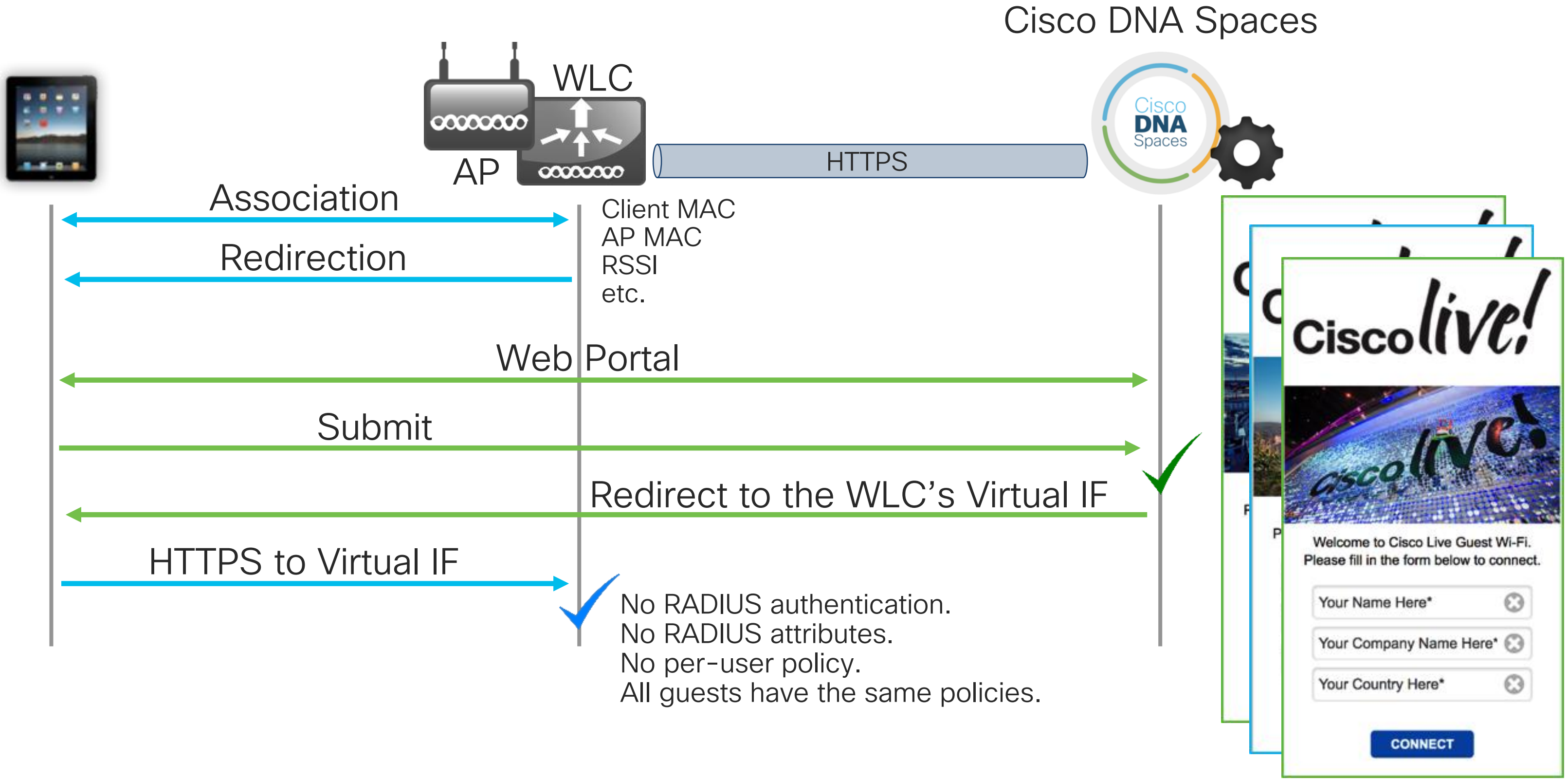
Web Auth type External(Re-direct to external server)

URL https://cmxconnect.mylab.com/visitor/login

CMX Connect 10.6 Configuration Guide:
https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-6/cmx_config/b_cg_cmx106/the_cisco_cmx_connect_and_engage_service.html

# Differentiating portals by site / map

## DNA Spaces



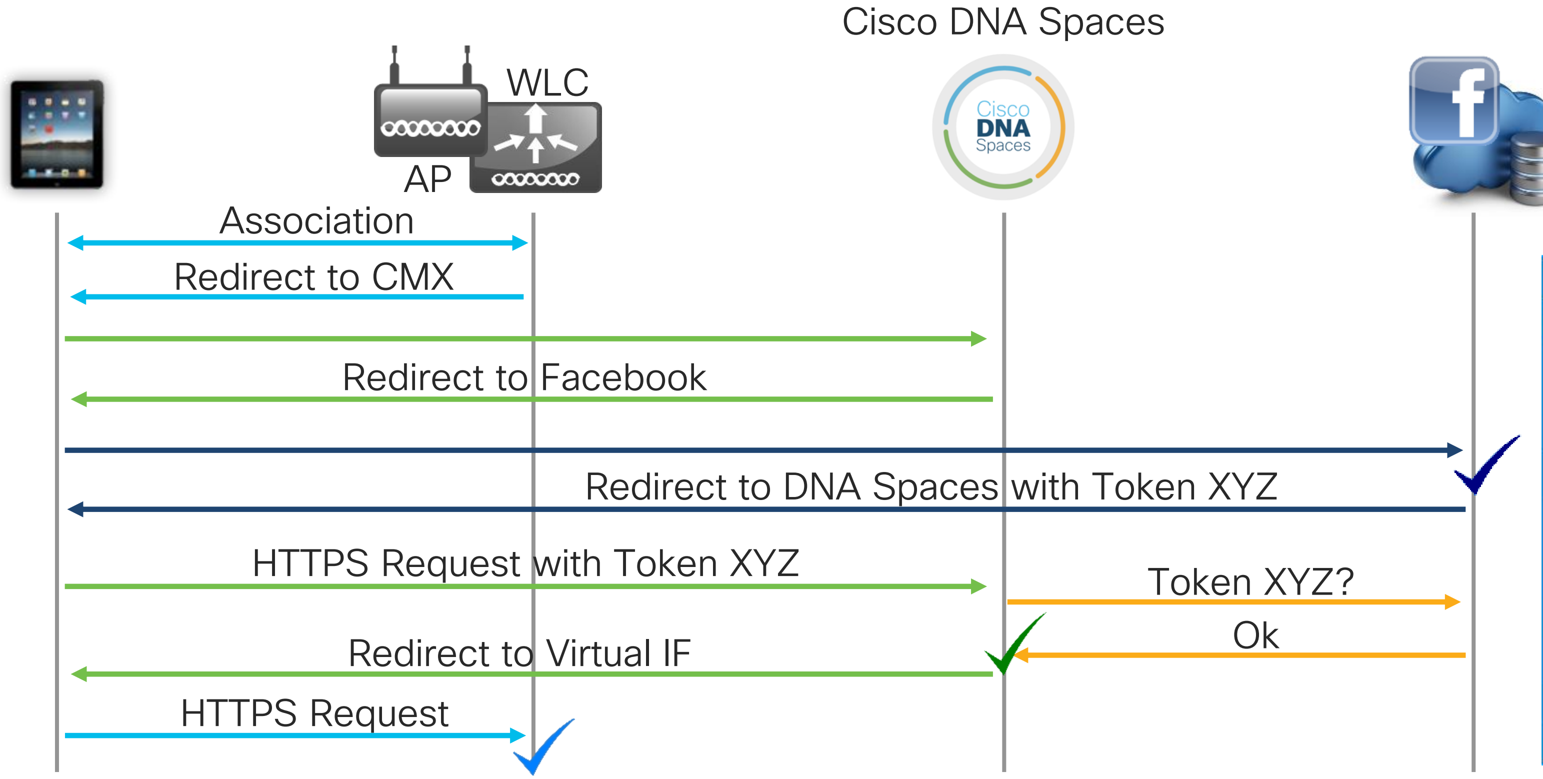
Welcome to Cisco Live Guest Wi-Fi.
Please fill in the form below to connect.

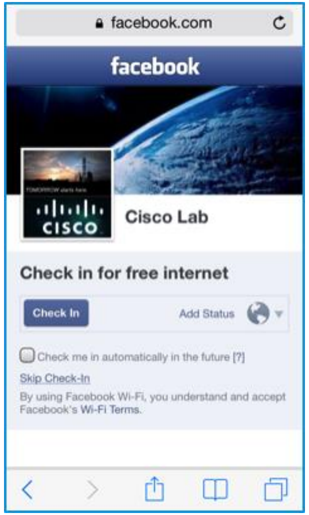
No RADIUS authentication.
No RADIUS attributes.
No per-user policy.
All guests have the same policies.

# Integration with Facebook Wi-Fi

## DNA Spaces

For your reference





facebook.com

facebook

Cisco Lab

Check in for free internet

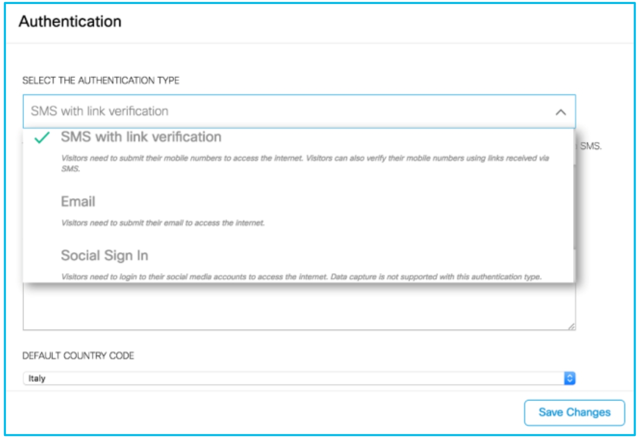
Check In Add Status

□ Check me in automatically in the future [?]

Skip Check-In

By using Facebook Wi-Fi, you understand and accept Facebook's Wi-Fi Terms.

# Cisco DNA Spaces: portal customization and more



Authentication

SELECT THE AUTHENTICATION TYPE

SMS with link verification

✓ SMS with link verification

*Visitors need to submit their mobile numbers to access the internet. Visitors can also verify their mobile numbers using links received via SMS.*

Email

*Visitors need to submit their email to access the internet.*

Social Sign In

*Visitors need to login to their social media accounts to access the internet. Data capture is not supported with this authentication type.*

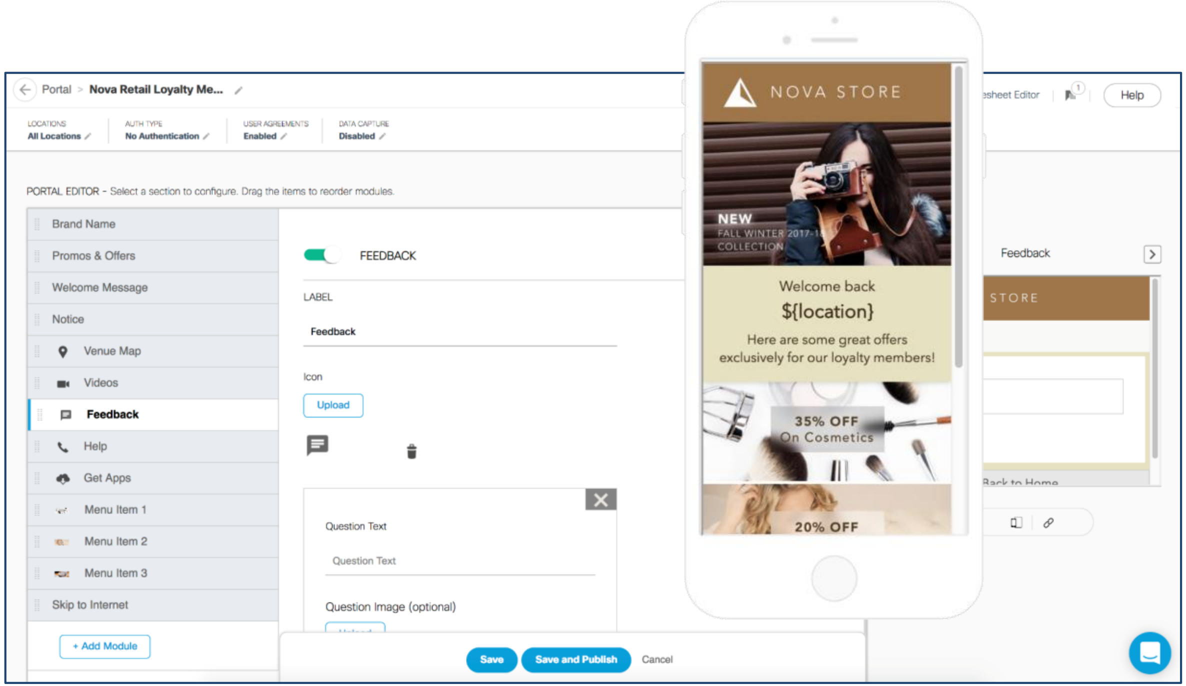
SMS.

DEFAULT COUNTRY CODE

Italy

Save Changes

Additional options for authenticating via SMS, email and social logins



Portal > **Nova Retail Loyalty Me...**

LOCATIONS **All Locations** | AUTH TYPE **No Authentication** | USER AGREEMENTS **Enabled** | DATA CAPTURE **Disabled**

PORTAL EDITOR - Select a section to configure. Drag the items to reorder modules.

- Brand Name
- Promos & Offers
- Welcome Message
- Notice
- Venue Map
- Videos
- **Feedback**
- Help
- Get Apps
- Menu Item 1
- Menu Item 2
- Menu Item 3
- Skip to Internet

+ Add Module

FEEDBACK

LABEL: Feedback

Icon: Upload

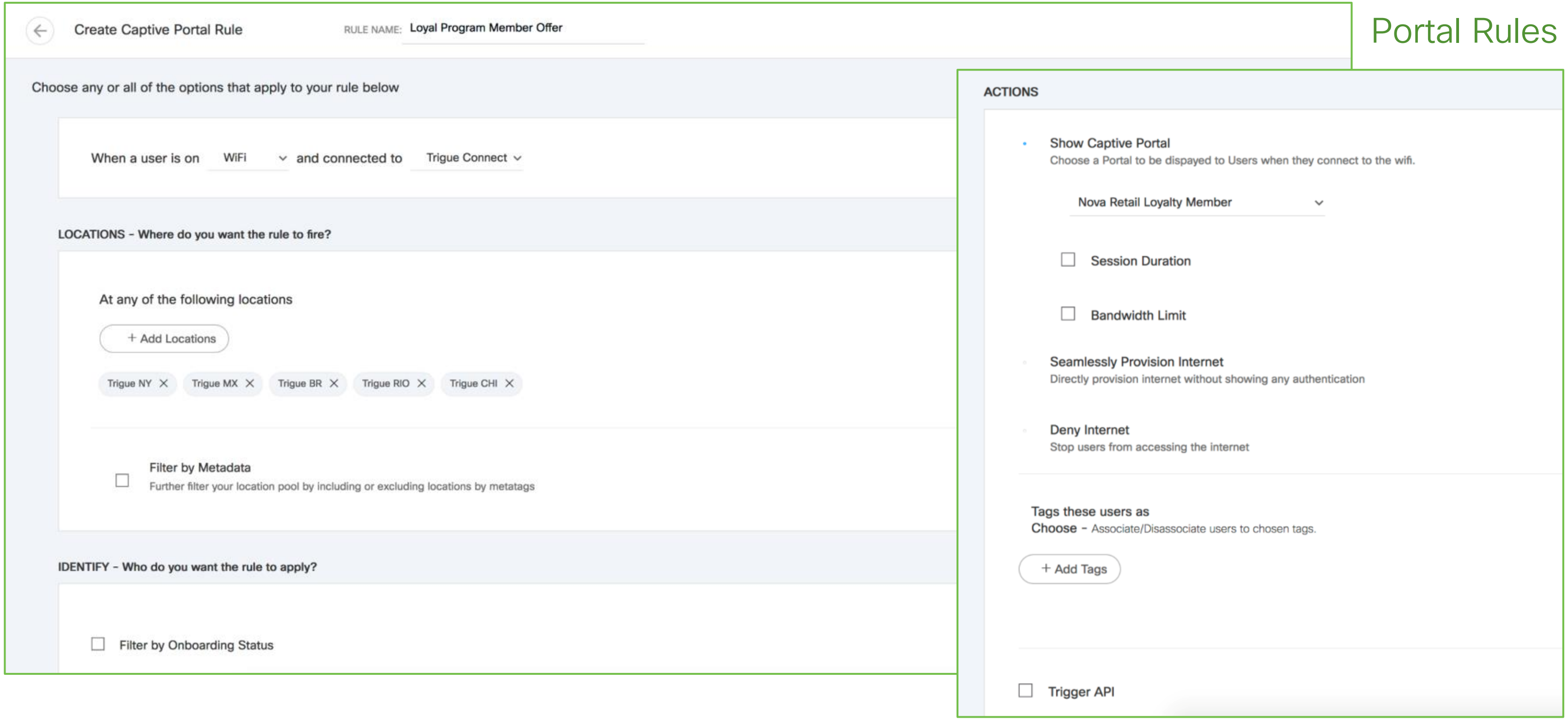
Question Text: Question Text

Question Image (optional)

Save | Save and Publish | Cancel

Hotspot oriented customization

# Cisco DNA Spaces: portal customization and more



Portal Rules

Create Captive Portal Rule    RULE NAME: Loyal Program Member Offer

Choose any or all of the options that apply to your rule below

When a user is on WiFi and connected to Trigue Connect

LOCATIONS - Where do you want the rule to fire?

At any of the following locations

+ Add Locations

Trigue NY ✕  Trigue MX ✕  Trigue BR ✕  Trigue RIO ✕  Trigue CHI ✕

□ Filter by Metadata
Further filter your location pool by including or excluding locations by metatags

IDENTIFY - Who do you want the rule to apply?

□ Filter by Onboarding Status

ACTIONS

● Show Captive Portal
Choose a Portal to be dispayed to Users when they connect to the wifi.

Nova Retail Loyalty Member

□ Session Duration

□ Bandwidth Limit

○ Seamlessly Provision Internet
Directly provision internet without showing any authentication

○ Deny Internet
Stop users from accessing the internet

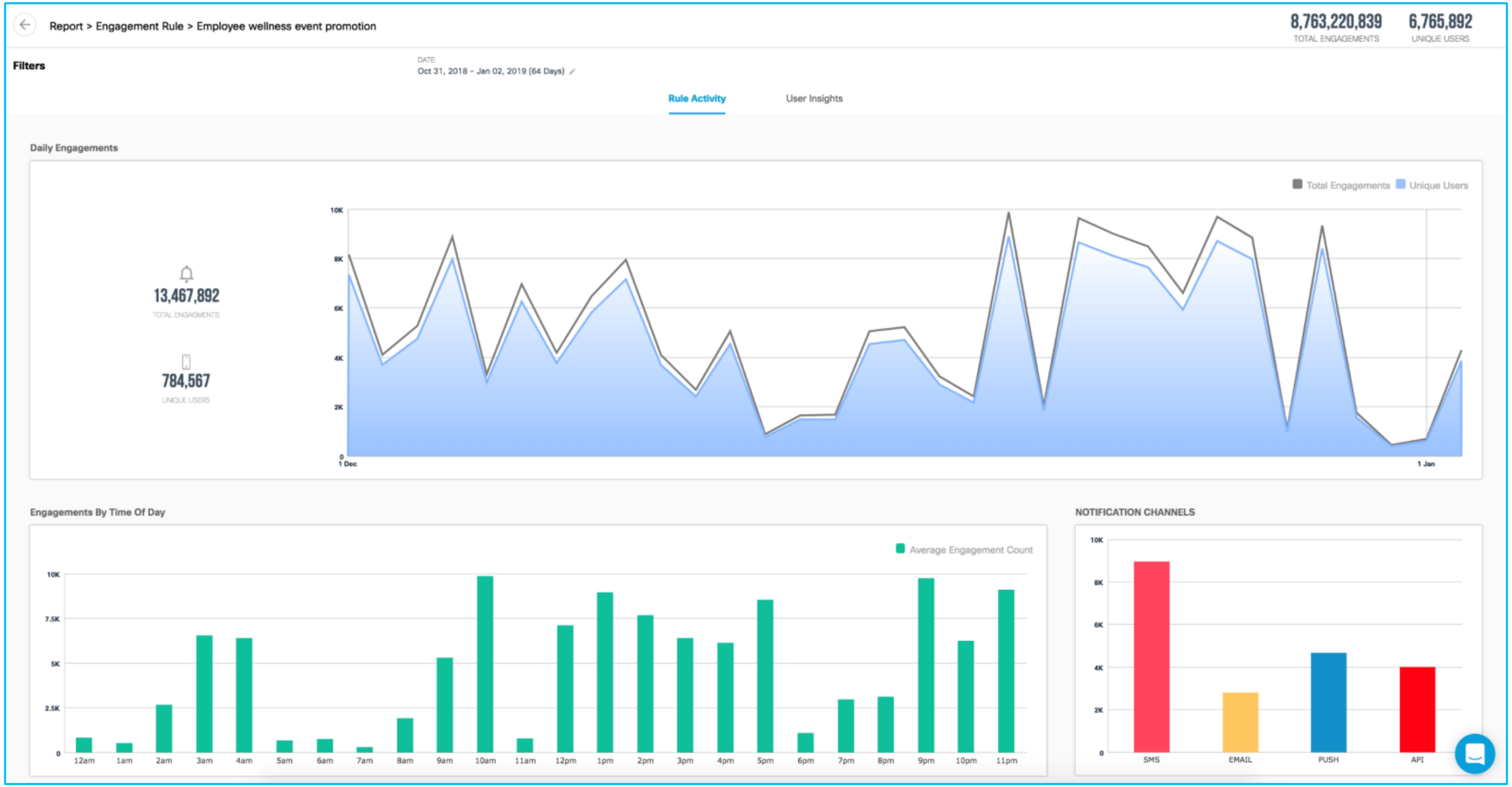
Tags these users as
Choose - Associate/Disassociate users to chosen tags.

+ Add Tags

□ Trigger API

# Cisco DNA Spaces: portal customization and more

For your reference



Report > Engagement Rule > Employee wellness event promotion

8,763,220,839 TOTAL ENGAGEMENTS

6,765,892 UNIQUE USERS

Filters

DATE: Oct 31, 2018 - Jan 02, 2019 (64 Days)

Rule Activity | User Insights

Daily Engagements

13,467,892 TOTAL ENGAGMENTS

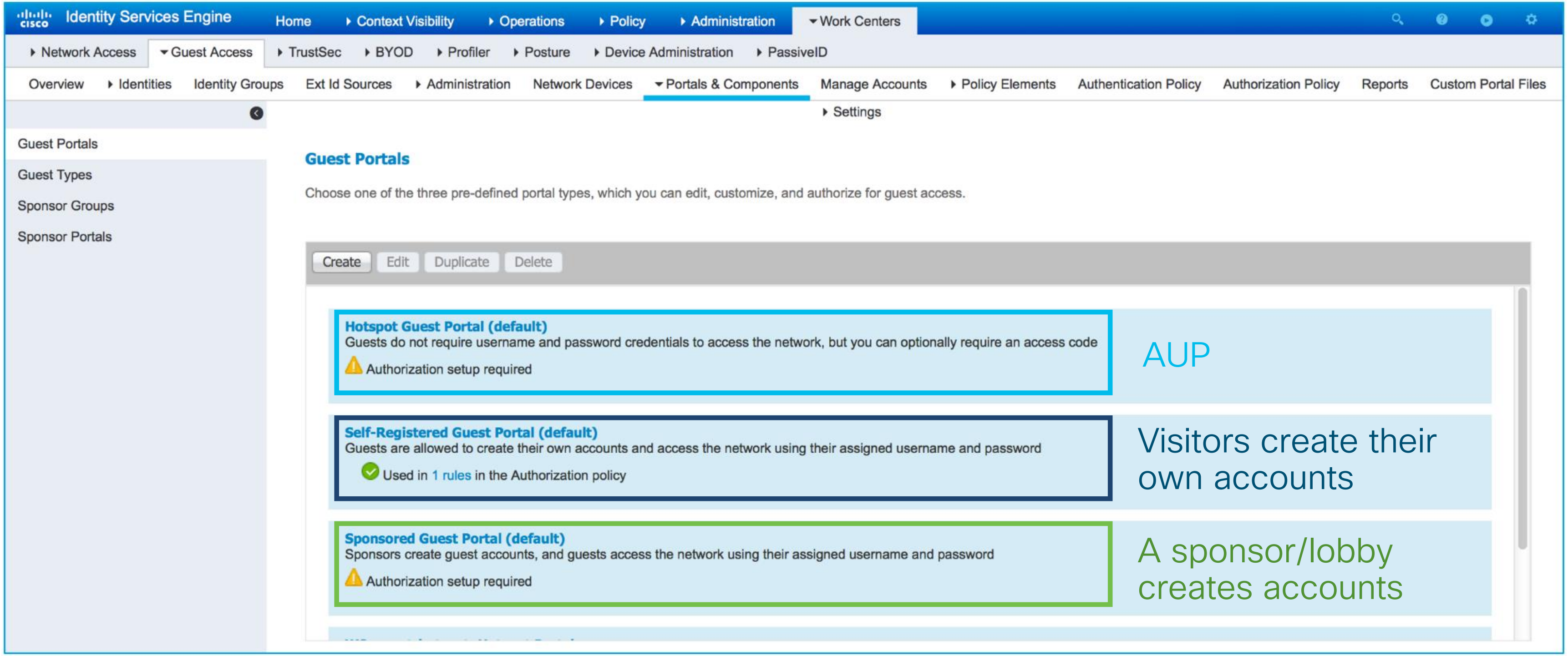
784,567 UNIQUE USERS

Engagements By Time Of Day

NOTIFICATION CHANNELS

# Identity Services Engine (ISE) guest portals

## Even more options for Enterprise Guest Wi-Fi



**Guest Portals**

Choose one of the three pre-defined portal types, which you can edit, customize, and authorize for guest access.

**Hotspot Guest Portal (default)**
Guests do not require username and password credentials to access the network, but you can optionally require an access code
⚠ Authorization setup required

AUP

**Self-Registered Guest Portal (default)**
Guests are allowed to create their own accounts and access the network using their assigned username and password
✓ Used in 1 rules in the Authorization policy

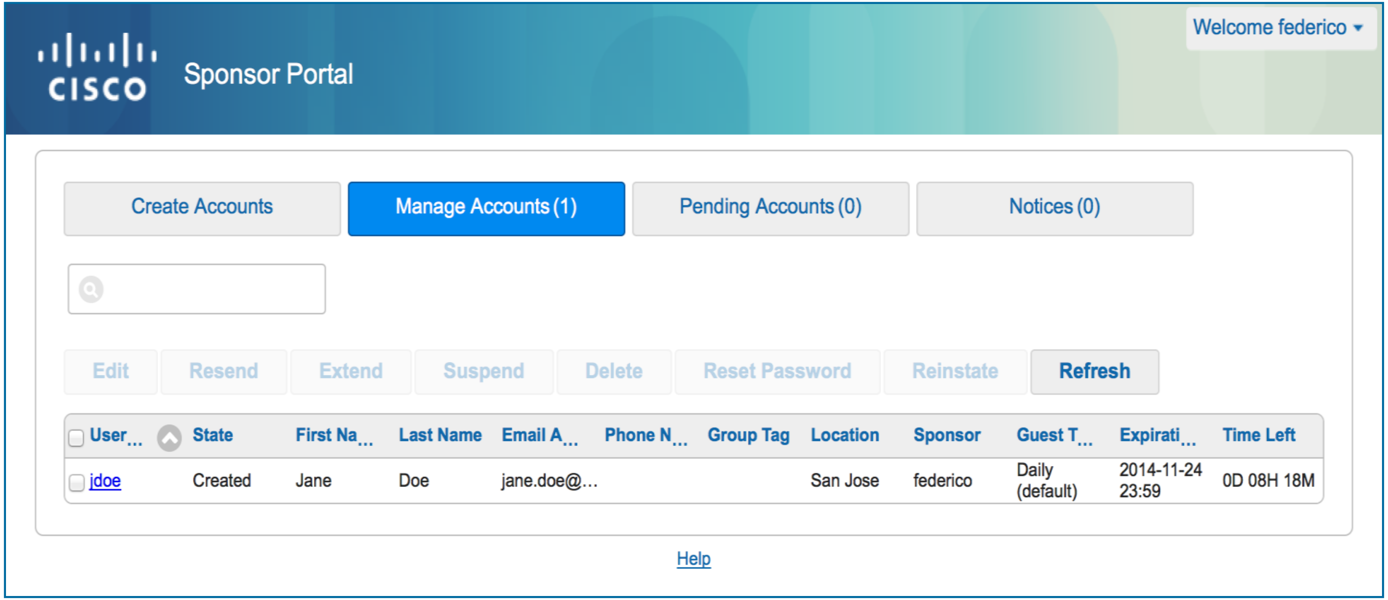
Visitors create their own accounts

**Sponsored Guest Portal (default)**
Sponsors create guest accounts, and guests access the network using their assigned username and password
⚠ Authorization setup required

A sponsor/lobby creates accounts

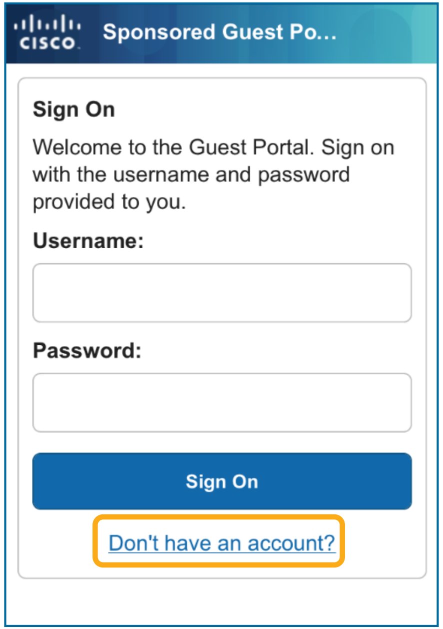
# ISE – Sponsor Portal

- Customizable pages
- Sponsor privileges tied to defined sponsor policy
  - Roles sponsor can create
  - Time profiles can be assigned
  - Management of other guest accounts
  - Single or bulk account creation



| ☐ User... | State | First Na... | Last Name | Email A... | Phone N... | Group Tag | Location | Sponsor | Guest T... | Expirati... | Time Left |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ jdoe | Created | Jane | Doe | jane.doe@... |  |  | San Jose | federico | Daily (default) | 2014-11-24 23:59 | 0D 08H 18M |

# ISE - Guest Self-Service

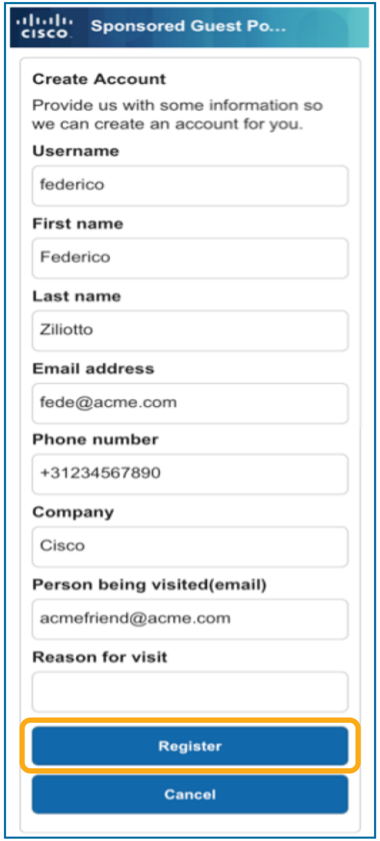


**Sign On**

Welcome to the Guest Portal. Sign on with the username and password provided to you.

**Username:**

**Password:**



**Create Account**

Provide us with some information so we can create an account for you.

**Username**

federico

**First name**

Federico

**Last name**

Ziliotto

**Email address**

fede@acme.com

**Phone number**

+31234567890

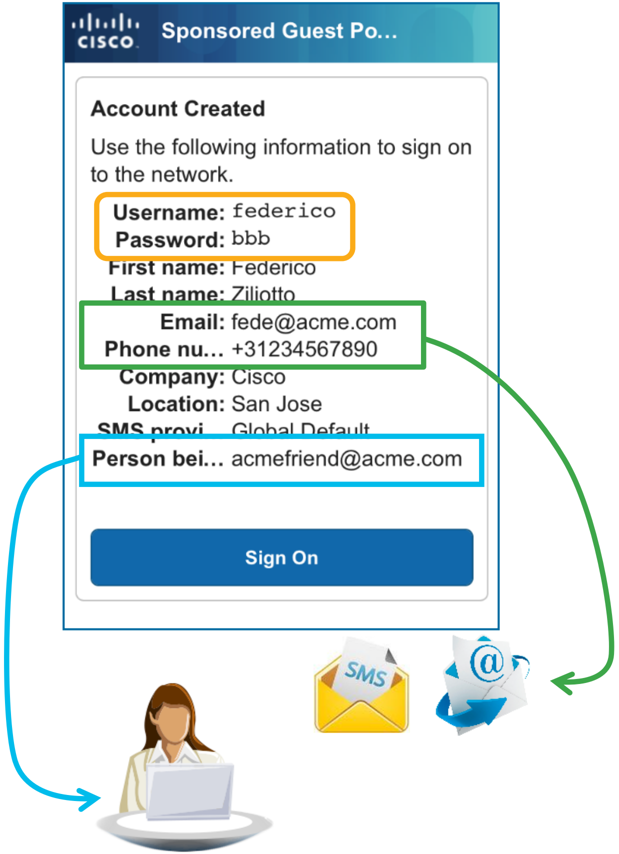
**Company**

Cisco

**Person being visited(email)**

acmefriend@acme.com

**Reason for visit**



**Account Created**

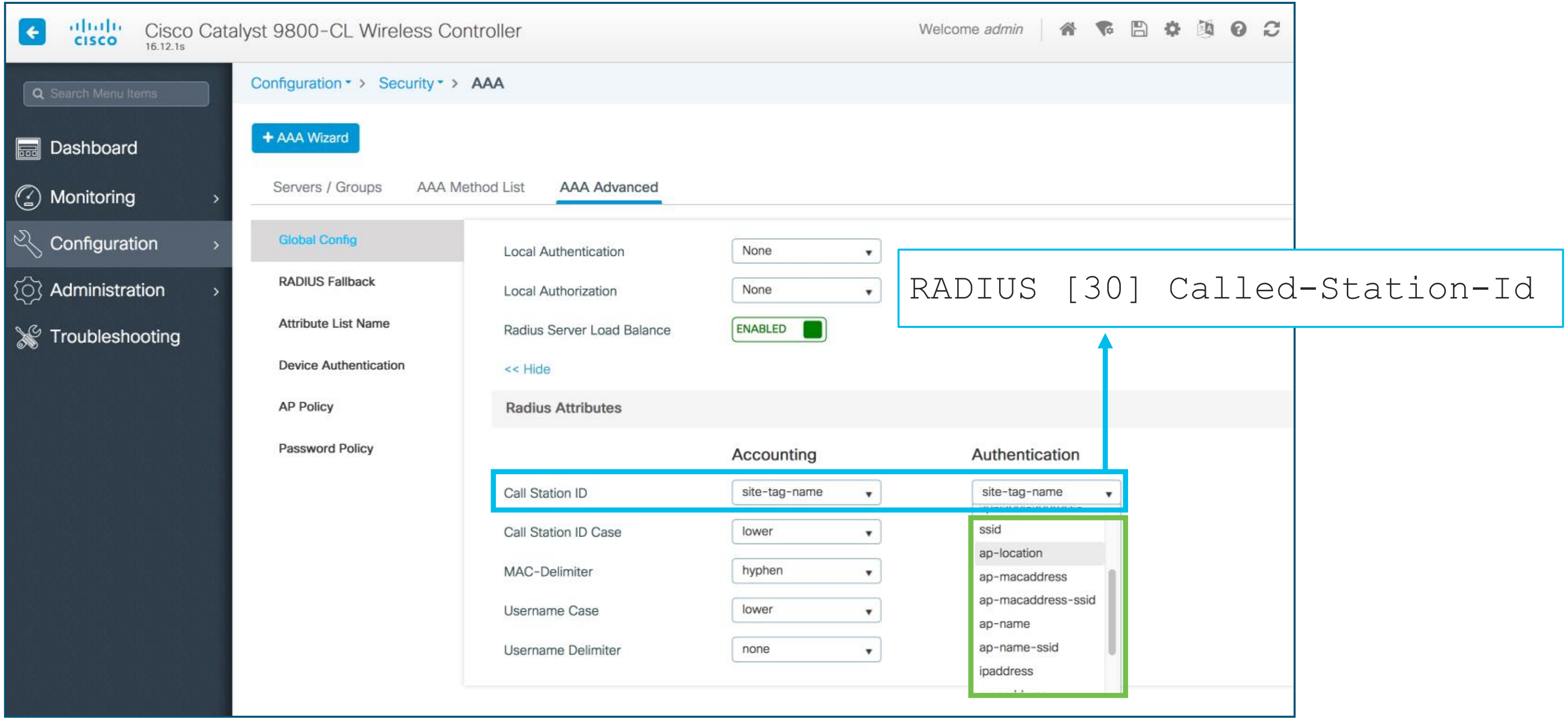
Use the following information to sign on to the network.

**Username:** federico
**Password:** bbb
**First name:** Federico
**Last name:** Ziliotto
**Email:** fede@acme.com
**Phone nu...** +31234567890
**Company:** Cisco
**Location:** San Jose
**SMS provi...** Global Default
**Person bei...** acmefriend@acme.com

# Differentiating Guest Portals

## IOS-XE with RADIUS Called-Station-Id

- How to redirect guests to separate portals based on site tags, AP location, WLAN name, etc.?



Cisco Catalyst 9800-CL Wireless Controller 16.12.1s

Welcome *admin*

Configuration › Security › AAA

+ AAA Wizard

Servers / Groups | AAA Method List | AAA Advanced

Global Config

Local Authentication: None

Local Authorization: None

Radius Server Load Balance: ENABLED

<< Hide

Radius Attributes

| | Accounting | Authentication |
|---|---|---|
| Call Station ID | site-tag-name | site-tag-name |
| Call Station ID Case | lower | |
| MAC-Delimiter | hyphen | |
| Username Case | lower | |
| Username Delimiter | none | |

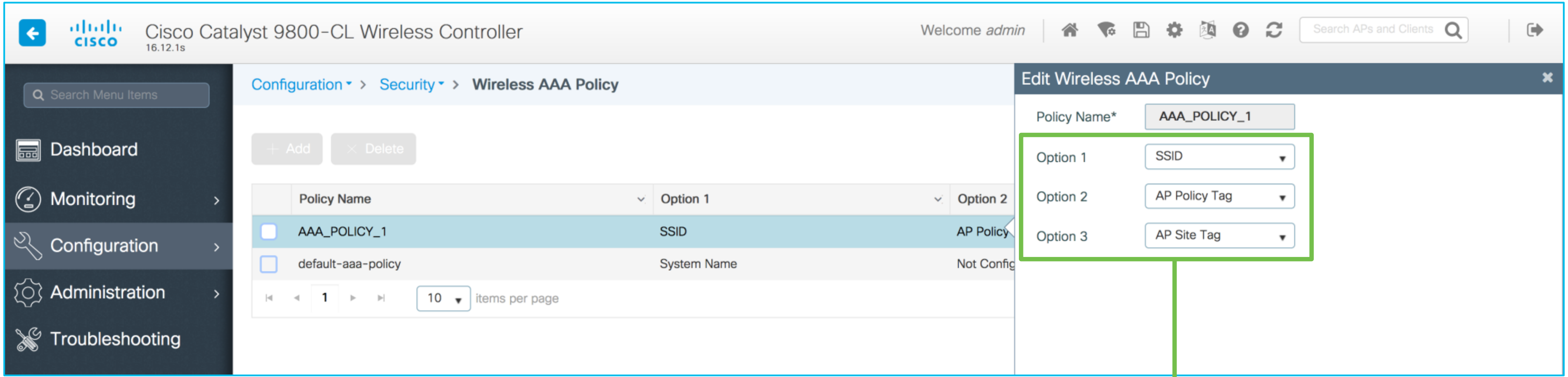
Authentication Call Station ID options: ssid, ap-location, ap-macaddress, ap-macaddress-ssid, ap-name, ap-name-ssid, ipaddress

RADIUS [30] Called-Station-Id

# Differentiating Guest Portals

## IOS-XE with RADIUS NAS-Identifier

- How to redirect guests to separate portals based on site tags, AP location, WLAN name, etc.?



| | Policy Name | Option 1 | Option 2 |
|---|---|---|---|
| □ | AAA_POLICY_1 | SSID | AP Policy |
| □ | default-aaa-policy | System Name | Not Config |

1 · 10 items per page

Policy Name*: AAA_POLICY_1
Option 1: SSID
Option 2: AP Policy Tag
Option 3: AP Site Tag

```
RADIUS [32] NAS-Identifier = Option1:Option2:Option3
```

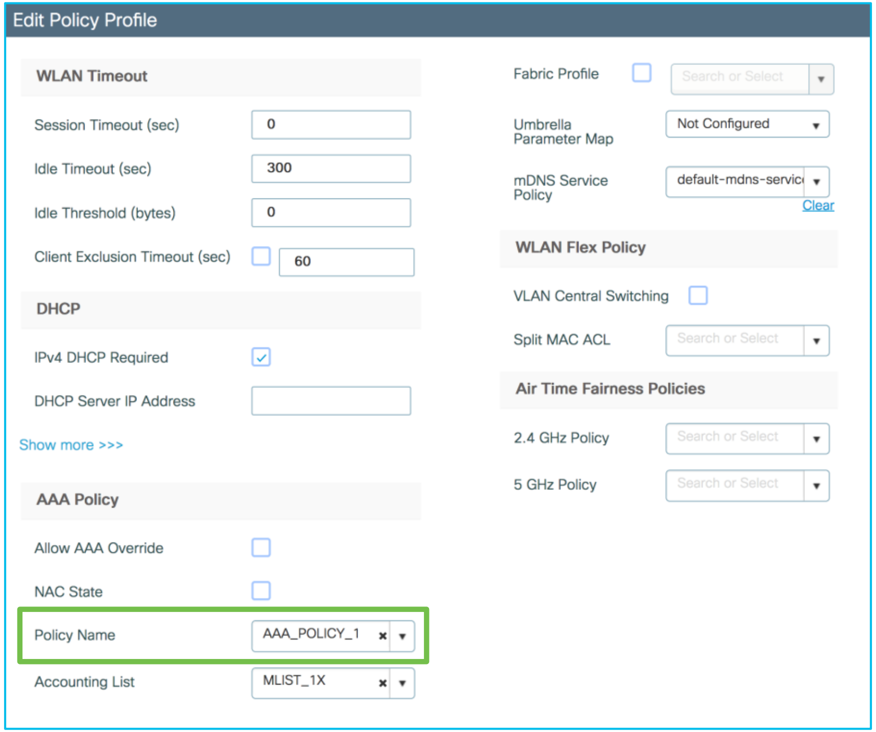
```
▼ AVP: t=NAS-Identifier(32) l=58 val=RackWifi-9800-Guest-07:POLICY_TAG_9800_GUEST:SITE_TAG_CL
    Type: 32
    Length: 58
    NAS-Identifier: RackWifi-9800-Guest-07:POLICY_TAG_9800_GUEST:SITE_TAG_CL
```

# Differentiating Guest Portals

## IOS-XE with RADIUS NAS-Identifier

For your reference

- How to redirect guests to separate portals based on site tags, AP location, WLAN name, etc.?



Edit Policy Profile

**WLAN Timeout**

Session Timeout (sec): 0

Idle Timeout (sec): 300

Idle Threshold (bytes): 0

Client Exclusion Timeout (sec): □ 60

**DHCP**

IPv4 DHCP Required: ☑

DHCP Server IP Address:

Show more >>>

**AAA Policy**

Allow AAA Override: □

NAC State: □

Policy Name: AAA_POLICY_1

Accounting List: MLIST_1X

Fabric Profile: □ Search or Select

Umbrella Parameter Map: Not Configured

mDNS Service Policy: default-mdns-servic

Clear

**WLAN Flex Policy**

VLAN Central Switching: □

Split MAC ACL: Search or Select

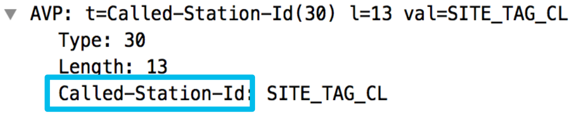
**Air Time Fairness Policies**

2.4 GHz Policy: Search or Select

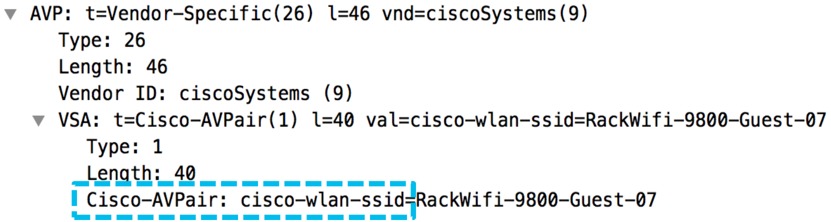
5 GHz Policy: Search or Select

cisco Live!

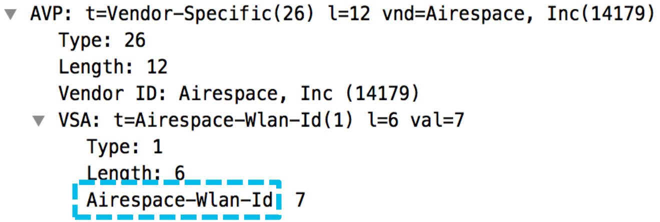
# Location based authorization examples



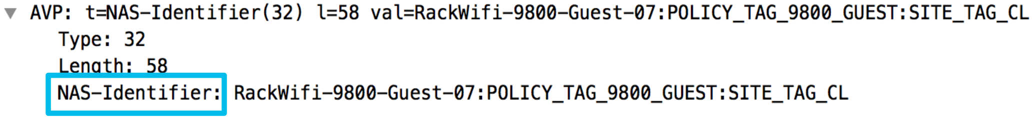
```
▼ AVP: t=Called-Station-Id(30) l=13 val=SITE_TAG_CL
    Type: 30
    Length: 13
    Called-Station-Id: SITE_TAG_CL
```



```
▼ AVP: t=Vendor-Specific(26) l=46 vnd=ciscoSystems(9)
    Type: 26
    Length: 46
    Vendor ID: ciscoSystems (9)
  ▼ VSA: t=Cisco-AVPair(1) l=40 val=cisco-wlan-ssid=RackWifi-9800-Guest-07
      Type: 1
      Length: 40
      Cisco-AVPair: cisco-wlan-ssid=RackWifi-9800-Guest-07
```

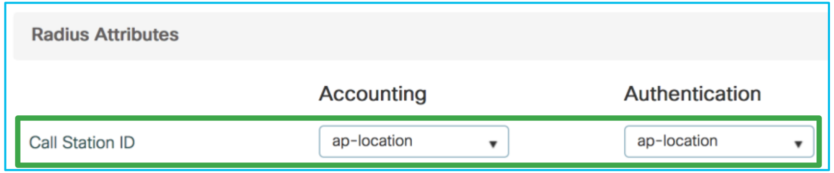


```
▼ AVP: t=Vendor-Specific(26) l=12 vnd=Airespace, Inc(14179)
    Type: 26
    Length: 12
    Vendor ID: Airespace, Inc (14179)
  ▼ VSA: t=Airespace-Wlan-Id(1) l=6 val=7
      Type: 1
      Length: 6
      Airespace-Wlan-Id: 7
```



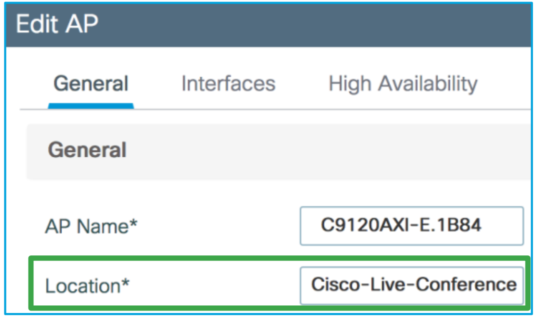
```
▼ AVP: t=NAS-Identifier(32) l=58 val=RackWifi-9800-Guest-07:POLICY_TAG_9800_GUEST:SITE_TAG_CL
    Type: 32
    Length: 58
    NAS-Identifier: RackWifi-9800-Guest-07:POLICY_TAG_9800_GUEST:SITE_TAG_CL
```

Example for Called-Station-Id = AP Location (on the 9800)



**Radius Attributes**

| | Accounting | Authentication |
|---|---|---|
| Call Station ID | ap-location ▾ | ap-location ▾ |



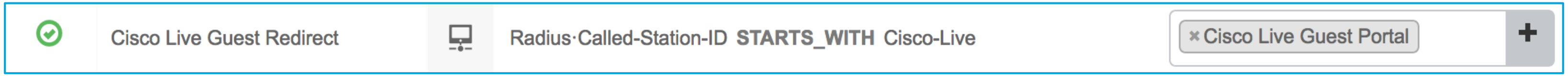
**Edit AP**

**General**

AP Name* C9120AXI-E.1B84

Location* Cisco-Live-Conference

Example on ISE



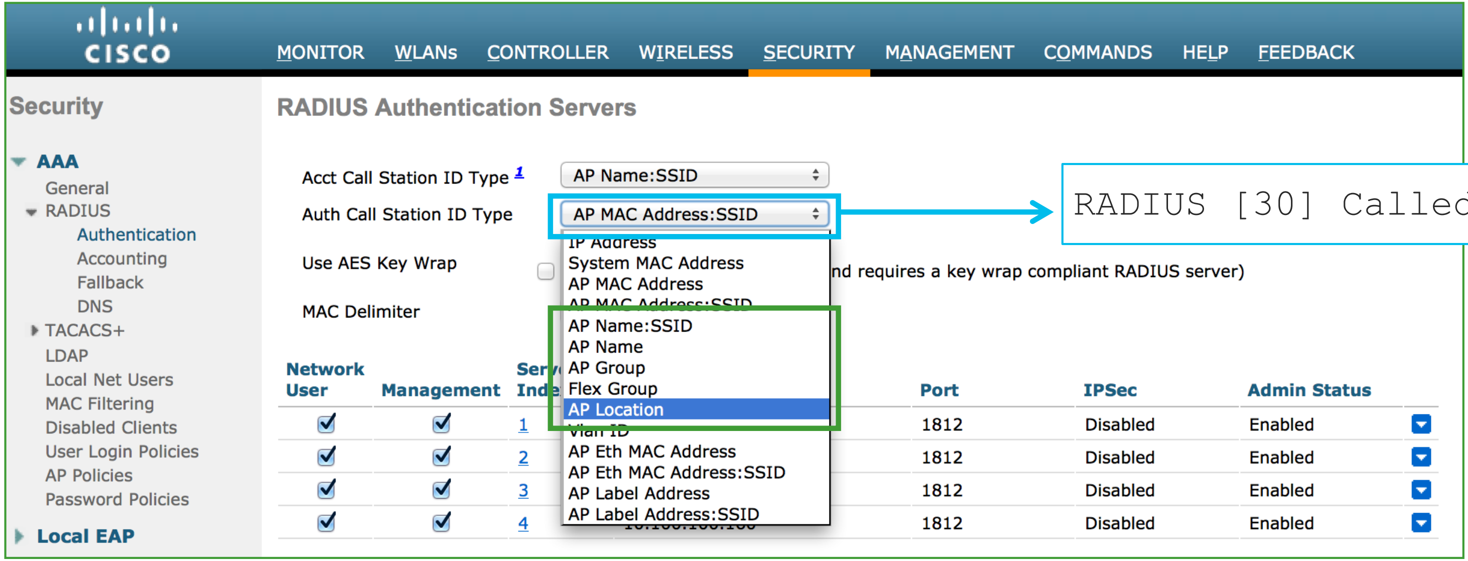
✓ Cisco Live Guest Redirect Radius·Called-Station-ID **STARTS_WITH** Cisco-Live × Cisco Live Guest Portal +

# Differentiating Guest Portals

## AireOS

For your reference

- How could we redirect guests to separate portals based on their location or their WLAN?



RADIUS Authentication Servers

Acct Call Station ID Type [1] AP Name:SSID

Auth Call Station ID Type AP MAC Address:SSID

Use AES Key Wrap ☐ …nd requires a key wrap compliant RADIUS server)

MAC Delimiter

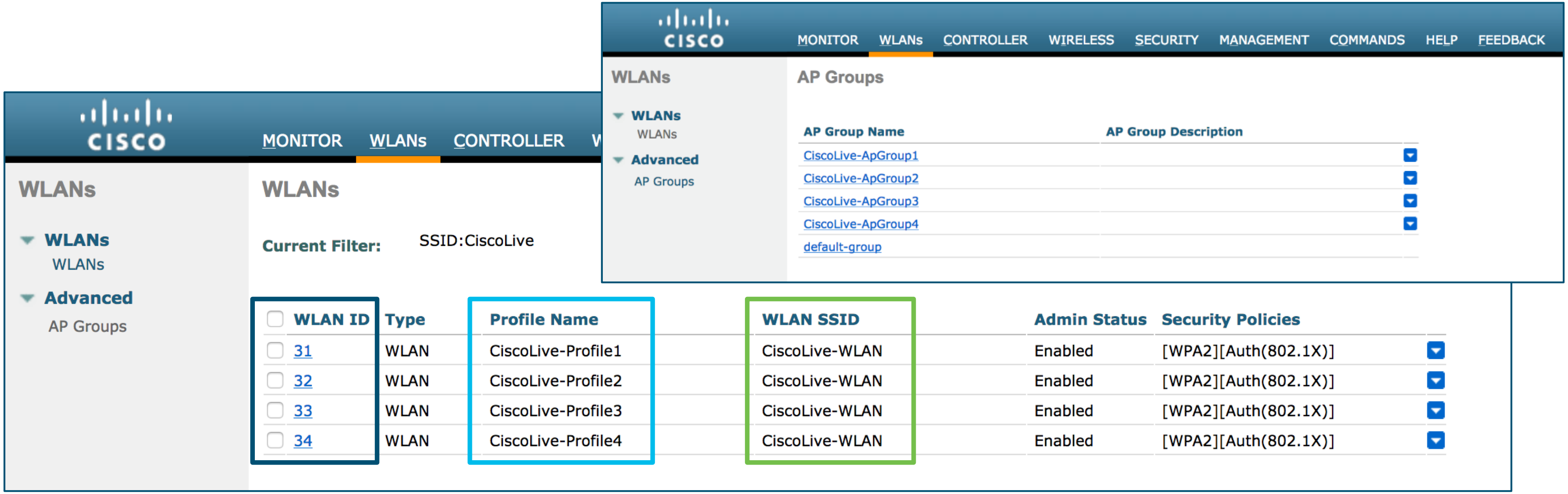
| Network User | Management | Serv Inde | Port | IPSec | Admin Status |
|---|---|---|---|---|---|
| ☑ | ☑ | 1 | 1812 | Disabled | Enabled |
| ☑ | ☑ | 2 | 1812 | Disabled | Enabled |
| ☑ | ☑ | 3 | 1812 | Disabled | Enabled |
| ☑ | ☑ | 4 | 1812 | Disabled | Enabled |

RADIUS [30] Called-Station-ID

# Location Based Authorization

## Alternative 1 – AireOS

For your reference



**AP Groups**

| AP Group Name | AP Group Description |
|---|---|
| CiscoLive-ApGroup1 | |
| CiscoLive-ApGroup2 | |
| CiscoLive-ApGroup3 | |
| CiscoLive-ApGroup4 | |
| default-group | |

**WLANs**

Current Filter: SSID:CiscoLive

| □ WLAN ID | Type | Profile Name | WLAN SSID | Admin Status | Security Policies |
|---|---|---|---|---|---|
| □ 31 | WLAN | CiscoLive-Profile1 | CiscoLive-WLAN | Enabled | [WPA2][Auth(802.1X)] |
| □ 32 | WLAN | CiscoLive-Profile2 | CiscoLive-WLAN | Enabled | [WPA2][Auth(802.1X)] |
| □ 33 | WLAN | CiscoLive-Profile3 | CiscoLive-WLAN | Enabled | [WPA2][Auth(802.1X)] |
| □ 34 | WLAN | CiscoLive-Profile4 | CiscoLive-WLAN | Enabled | [WPA2][Auth(802.1X)] |

Different ID

Different Profile Name

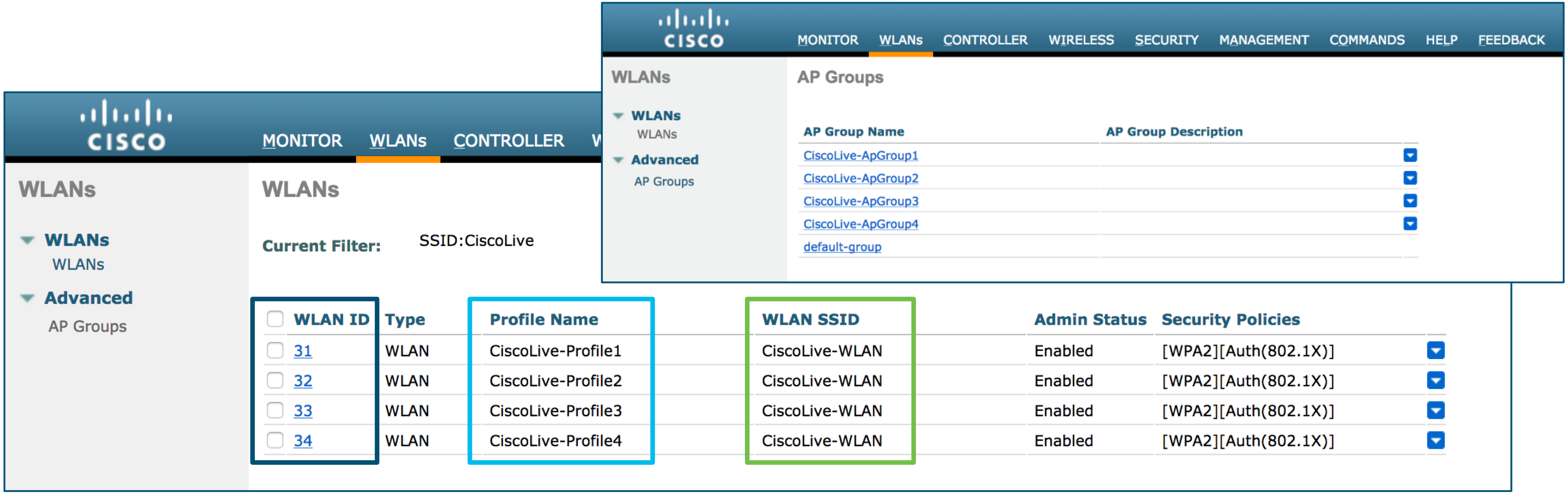
Same SSID

```
Airespace RADIUS VSA Airespace-Wlan-Id
```

# Location Based Authorization

## Alternative 1 – AireOS

For your reference



AP Groups

| AP Group Name | AP Group Description |
|---|---|
| CiscoLive-ApGroup1 | |
| CiscoLive-ApGroup2 | |
| CiscoLive-ApGroup3 | |
| CiscoLive-ApGroup4 | |
| default-group | |

WLANs

Current Filter: SSID:CiscoLive

| □ WLAN ID | Type | Profile Name | WLAN SSID | Admin Status | Security Policies |
|---|---|---|---|---|---|
| □ 31 | WLAN | CiscoLive-Profile1 | CiscoLive-WLAN | Enabled | [WPA2][Auth(802.1X)] |
| □ 32 | WLAN | CiscoLive-Profile2 | CiscoLive-WLAN | Enabled | [WPA2][Auth(802.1X)] |
| □ 33 | WLAN | CiscoLive-Profile3 | CiscoLive-WLAN | Enabled | [WPA2][Auth(802.1X)] |
| □ 34 | WLAN | CiscoLive-Profile4 | CiscoLive-WLAN | Enabled | [WPA2][Auth(802.1X)] |

Different ID

Different Profile Name

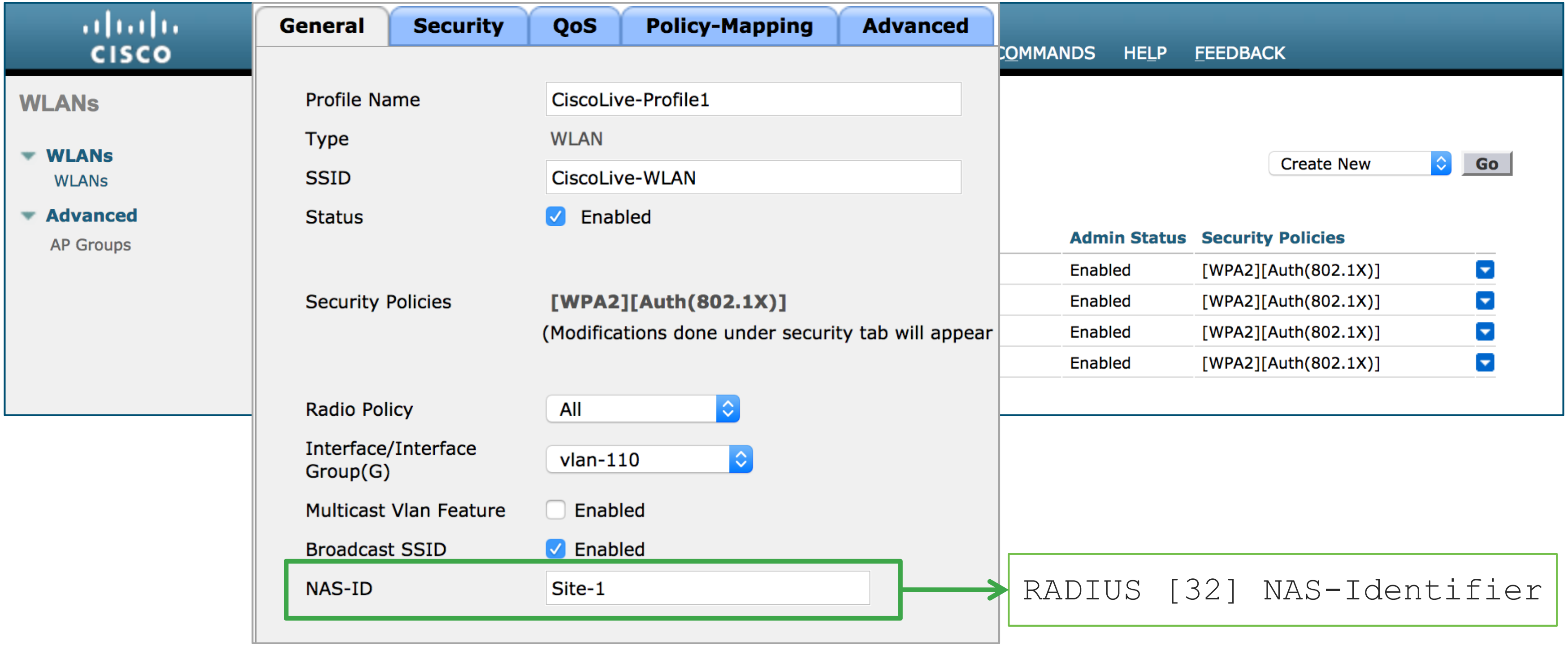
Same SSID

```
Airespace RADIUS VSA Airespace-Wlan-Id
```

# Location Based Authorization

## Alternative 2 – AireOS

For your reference



| | |
|---|---|
| Profile Name | CiscoLive-Profile1 |
| Type | WLAN |
| SSID | CiscoLive-WLAN |
| Status | ☑ Enabled |
| Security Policies | **[WPA2][Auth(802.1X)]**<br>(Modifications done under security tab will appear |
| Radio Policy | All |
| Interface/Interface Group(G) | vlan-110 |
| Multicast Vlan Feature | □ Enabled |
| Broadcast SSID | ☑ Enabled |
| NAS-ID | Site-1 |

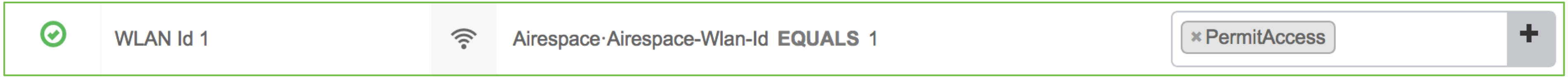
| Admin Status | Security Policies |
|---|---|
| Enabled | [WPA2][Auth(802.1X)] |
| Enabled | [WPA2][Auth(802.1X)] |
| Enabled | [WPA2][Auth(802.1X)] |
| Enabled | [WPA2][Auth(802.1X)] |

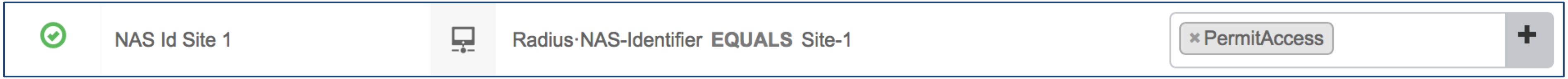
RADIUS [32] NAS-Identifier

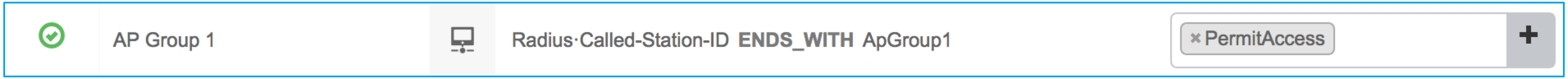
# Location based authorization options

## AireOS

For your reference

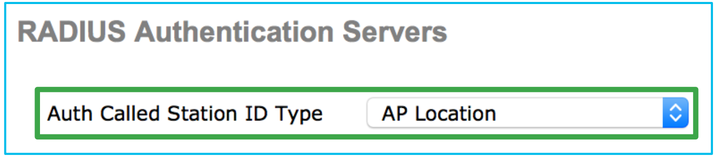

WLAN Id 1 | Airespace·Airespace-Wlan-Id **EQUALS** 1 | × PermitAccess


NAS Id Site 1 | Radius·NAS-Identifier **EQUALS** Site-1 | × PermitAccess


AP Group 1 | Radius·Called-Station-ID **ENDS_WITH** ApGroup1 | × PermitAccess

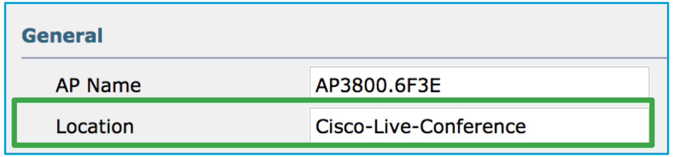
Common example for zone based guest redirect

On the WLC


**RADIUS Authentication Servers**

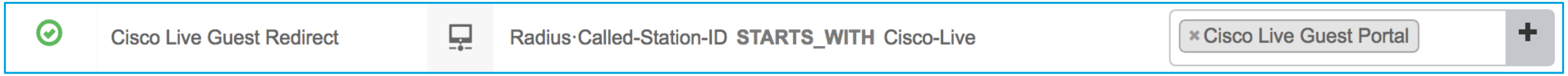
Auth Called Station ID Type: AP Location

On the WLC


**General**

AP Name: AP3800.6F3E

Location: Cisco-Live-Conference


Cisco Live Guest Redirect | Radius·Called-Station-ID **STARTS_WITH** Cisco-Live | × Cisco Live Guest Portal

On ISE

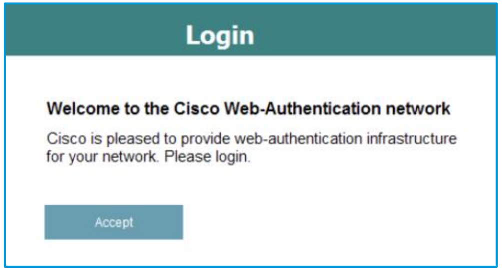
# ISE guest portals – some other facts

For your reference

- Up to ~100 concurrent logins/web page requests per second per PSN (Policy Services Node).
- Up to 1M guest accounts with the internal database.
- Support for Facebook Wi-Fi as of ISE 2.3.
- More customization options available with the portal builder: https://isepb.cisco.com
- It supports APIs for guest accounts creation and additional integration with external tools.

# In few words

WLC



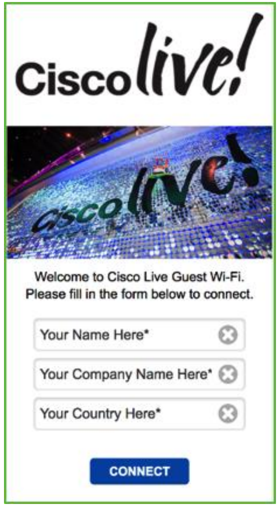
**Login**

**Welcome to the Cisco Web-Authentication network**

Cisco is pleased to provide web-authentication infrastructure for your network. Please login.

- Native and easy to use.
- Ideal for passthrough with AUP pages.
- LWA with consent.

Cisco DNA Spaces



Welcome to Cisco Live Guest Wi-Fi.
Please fill in the form below to connect.

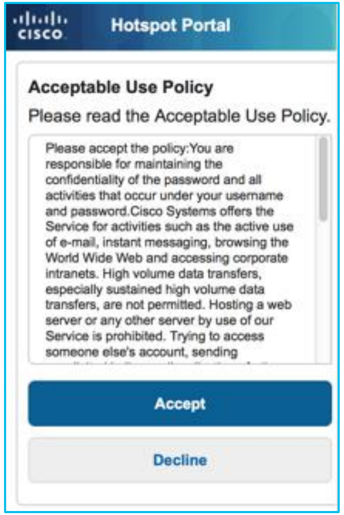
Your Name Here*

Your Company Name Here*

Your Country Here*

- Very easy/powerful to customize and assign portals based on sites.
- Ideal for passthrough with AUP pages, or for one-time SMS/email codes.
- LWA with consent.

ISE



**Acceptable Use Policy**

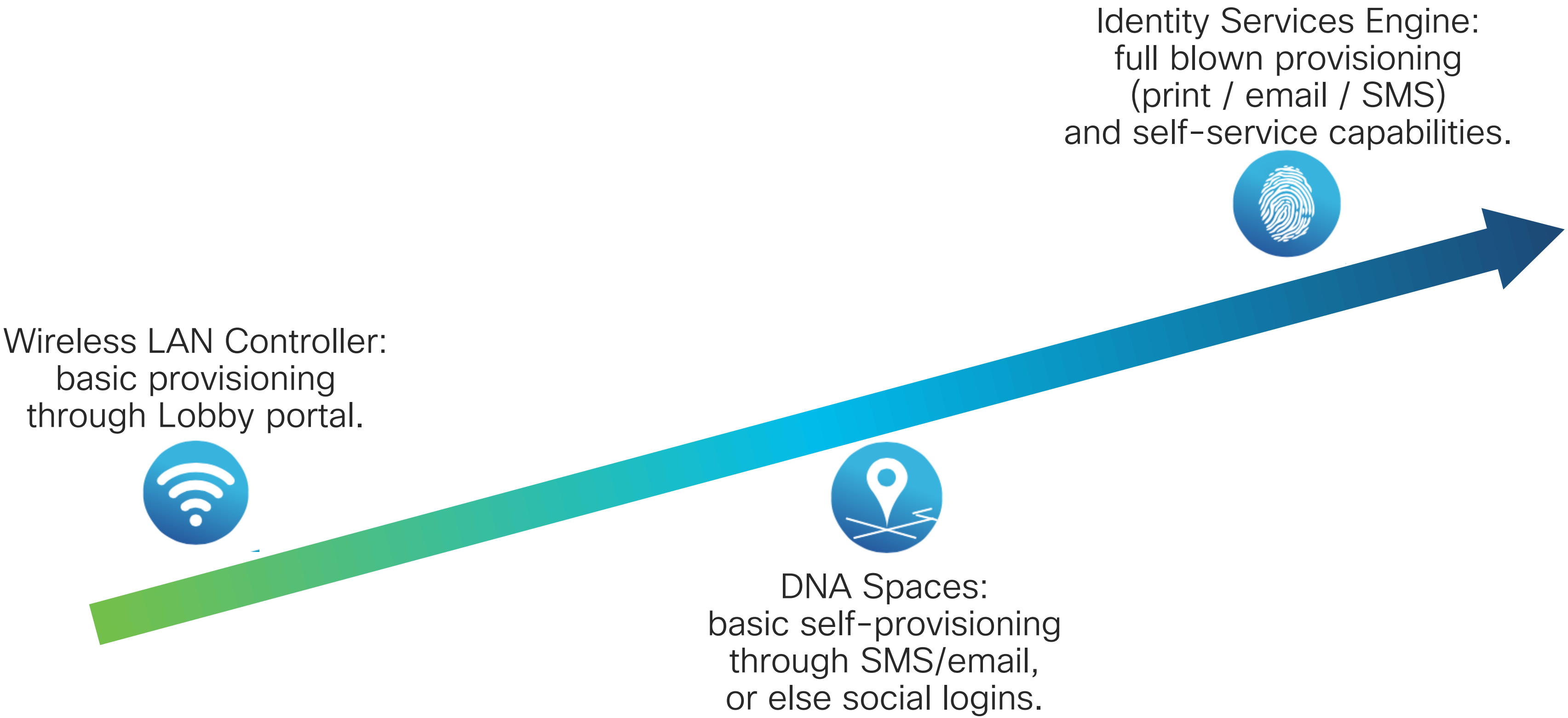
Please read the Acceptable Use Policy.

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending

- Most versatile solution.
- Ideal both for login and AUP portals.
- It requires an additional learning curve.
- LWA or CWA.

# Guest provisioning choices

For your reference



Wireless LAN Controller:
basic provisioning
through Lobby portal.

DNA Spaces:
basic self-provisioning
through SMS/email,
or else social logins.

Identity Services Engine:
full blown provisioning
(print / email / SMS)
and self-service capabilities.

# Example – Small Campus

For your reference

## Typical needs:

- Basic guest account creation options and customization.
- Support for sponsor/lobby administrator.
- Few locations.

## Positioning:

- Native WLC's guest portal with customizable web auth bundle: https://software.cisco.com/download/release.html?mdfid=282600534&flowid=7012&softwareid=282791507&release=1.0.2

# Example – Medium/Large Campus

For your reference

## Typical needs:

- Differentiated guest account creation options and customization.
- Support for multiple sponsor groups and privileges.
- Multiple locations with 802.1X most likely already in place.

## Positioning:

- ISE with the latest guest/sponsor features.
- Extended customization, with guest and sponsor management.
- Support for differentiating portals based on locations (e.g., AP location, AP group, FlexConnect group, etc.).

# Example – Public Hotspot

For your reference

Typical needs:

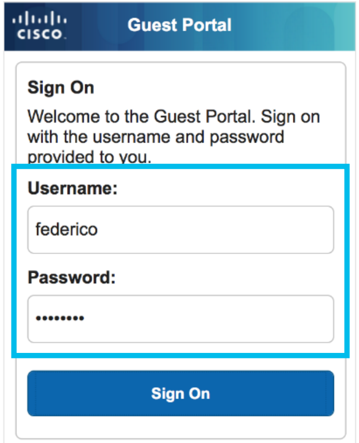
- Mass guest logins management for hotspot only, not for employees.
- Simple fill-in forms and analytics.
- Multiple locations with quick customization and advertisement options.

Positioning:

- DNA Spaces.
- Very quick customization options and no guest database management needed.

# Tips, tricks and use cases

# Guest Access Experts don’t change VLANs (CWA)



Guest Portal

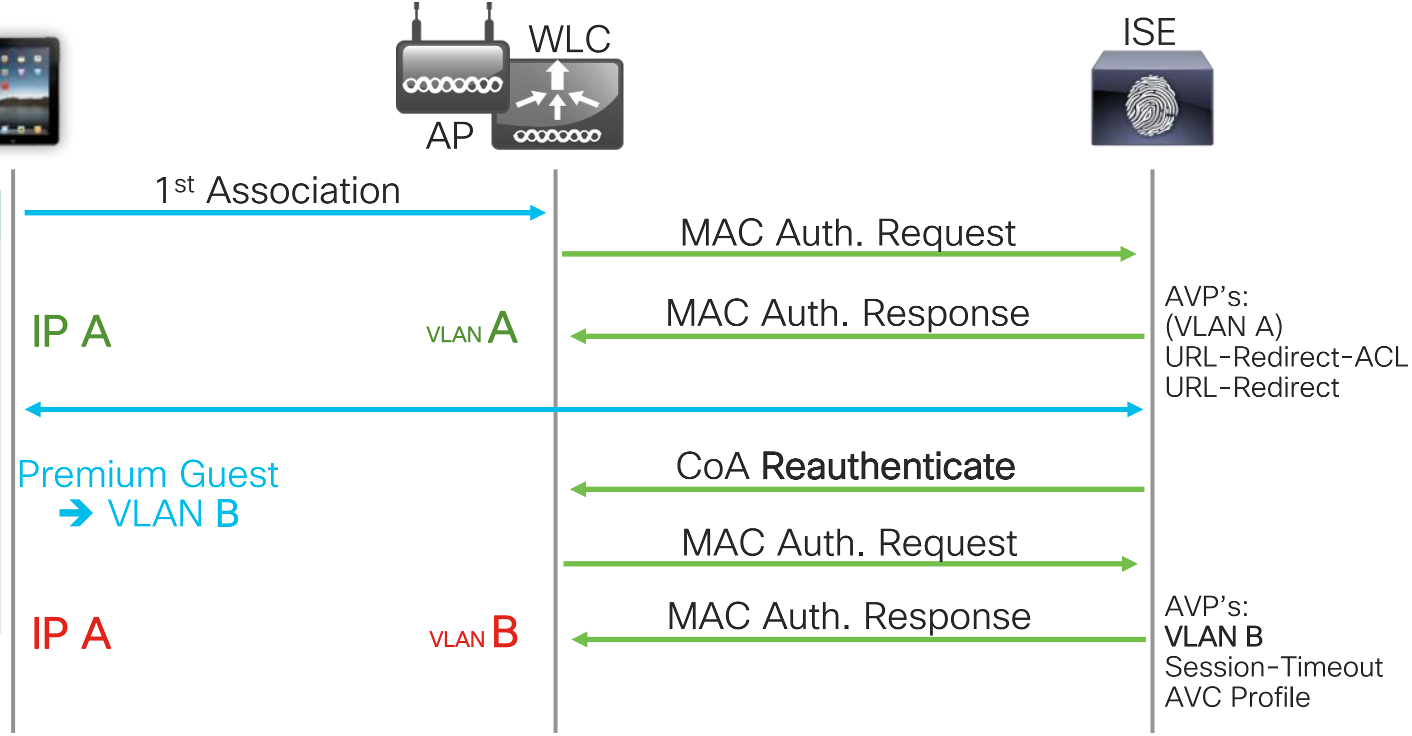
**Sign On**

Welcome to the Guest Portal. Sign on with the username and password provided to you.

**Username:** federico

**Password:** ••••••••

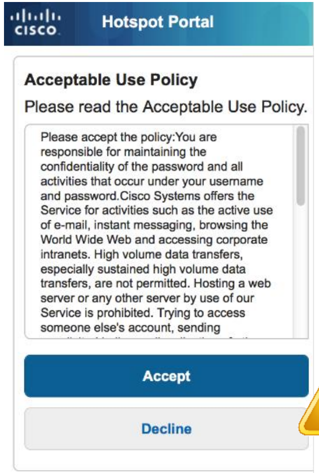
Sign On



# ISE Hotspot portal CoA

## Terminate (not recommended) vs. Reauthenticate (recommended)

For your reference



Hotspot Portal

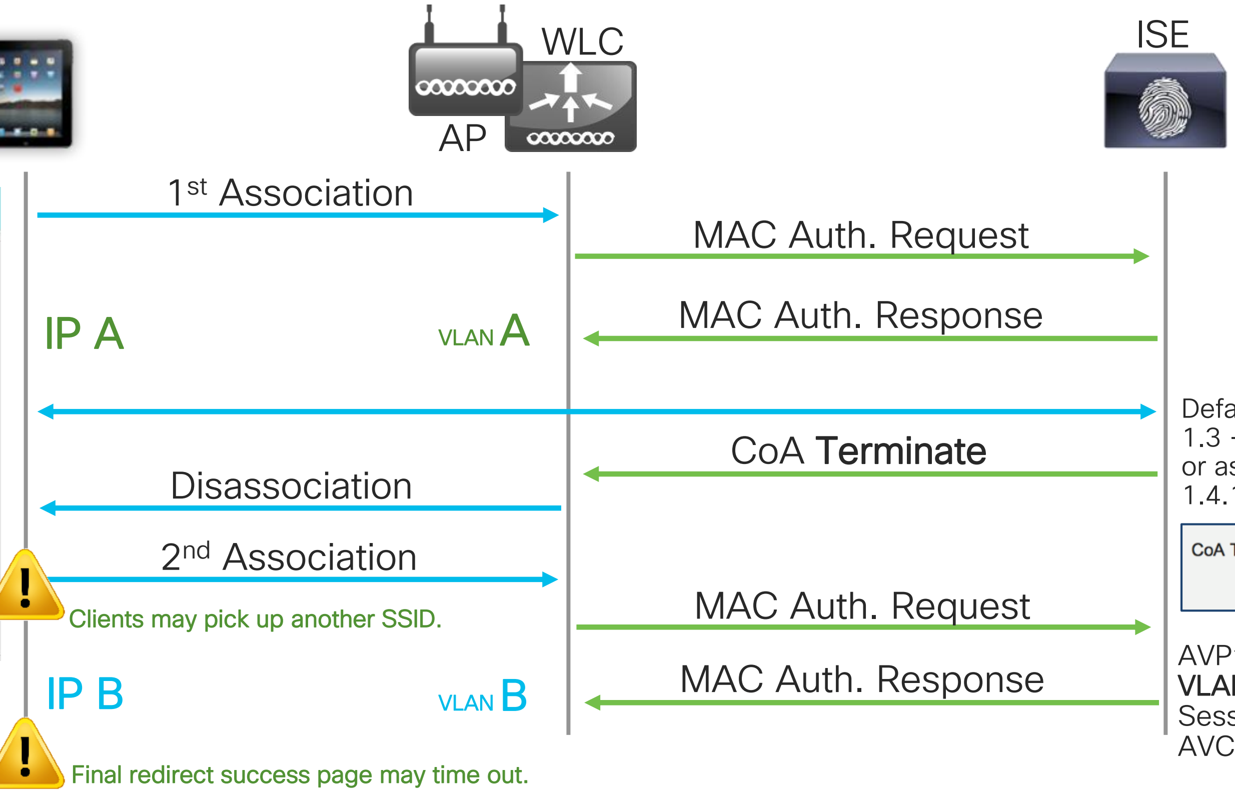
**Acceptable Use Policy**

Please read the Acceptable Use Policy.

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending

Accept

Decline



1st Association

MAC Auth. Request

IP A

VLAN A

MAC Auth. Response

CoA **Terminate**

Disassociation

2nd Association

Clients may pick up another SSID.

MAC Auth. Request

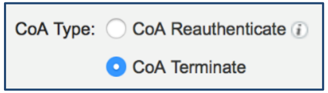
IP B

VLAN B

MAC Auth. Response

Final redirect success page may time out.

Default behavior for ISE 1.3 - 2.1
or as an option for ISE 1.4.1, 2.1p1, 2.2+



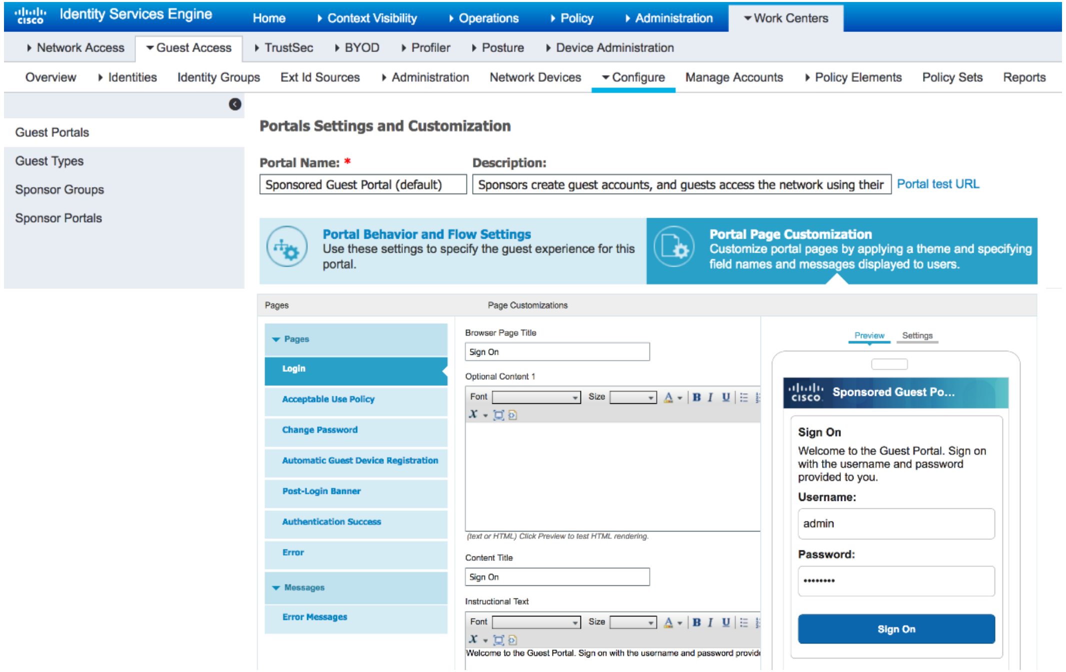
CoA Type: ○ CoA Reauthenticate ⓘ
● CoA Terminate

AVP's:
**VLAN B**
Session-Timeout
AVC Profile

# ISE Hotspot portal CoA: terminate vs. reauthenticate

## ISE 1.3 – 2.1: using Sponsored portals (CoA Reauthenticate) as Hotspot

For your reference



Portals Settings and Customization

Portal Name: * Sponsored Guest Portal (default)

Description: Sponsors create guest accounts, and guests access the network using their

Portal test URL

Portal Behavior and Flow Settings: Use these settings to specify the guest experience for this portal.

Portal Page Customization: Customize portal pages by applying a theme and specifying field names and messages displayed to users.

Browser Page Title: Sign On

Optional Content 1

(text or HTML) Click Preview to test HTML rendering.

Content Title: Sign On

Instructional Text: Welcome to the Guest Portal. Sign on with the username and password provid

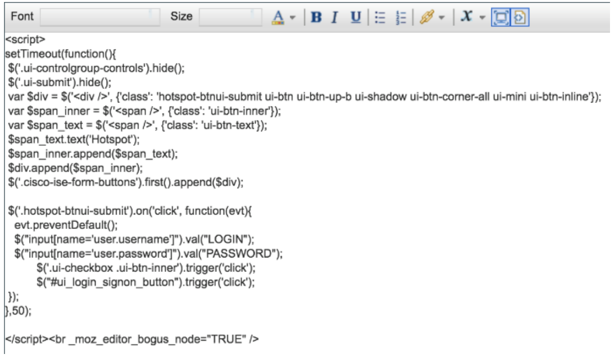
Sponsored Guest Po...

Sign On

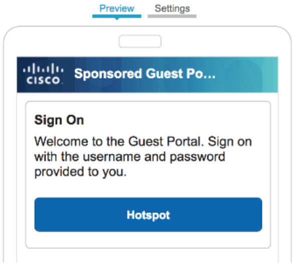
Welcome to the Guest Portal. Sign on with the username and password provided to you.

Username: admin

Password: ••••••••



```
<script>
setTimeout(function(){
 $('.ui-controlgroup-controls').hide();
 $('.ui-submit').hide();
 var $div = $('<div />', {'class': 'hotspot-btnui-submit ui-btn ui-btn-up-b ui-shadow ui-btn-corner-all ui-mini ui-btn-inline'});
 var $span_inner = $('<span />', {'class': 'ui-btn-inner'});
 var $span_text = $('<span />', {'class': 'ui-btn-text'});
 $span_text.text('Hotspot');
 $span_inner.append($span_text);
 $div.append($span_inner);
 $('.cisco-ise-form-buttons').first().append($div);

 $('.hotspot-btnui-submit').on('click', function(evt){
  evt.preventDefault();
  $("input[name='user.username']").val("LOGIN");
  $("input[name='user.password']").val("PASSWORD");
        $('.ui-checkbox .ui-btn-inner').trigger('click');
        $("#ui_login_signon_button").trigger('click');
 });
},50);

</script><br _moz_editor_bogus_node="TRUE" />
```



Sponsored Guest Po...

Sign On

Welcome to the Guest Portal. Sign on with the username and password provided to you.

# ISE Hotspot CoA: terminate vs. reauthenticate

## ISE 1.3 – 2.1: using Sponsored portals (CoA Reauthenticate) as Hotspot

For your reference

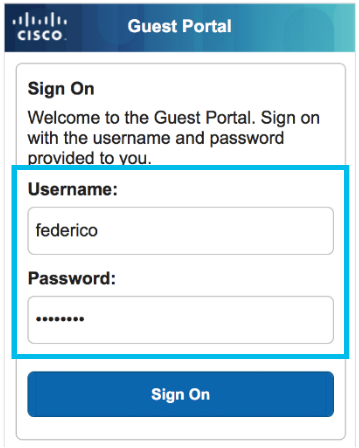
To be used in “Optional Content 2” of a Sponsored Portal

```
<script>
setTimeout(function(){
 $('.ui-controlgroup-controls').hide();
 $('.ui-submit').hide();
 var $div = $('<div />', {'class': 'hotspot-btnui-submit ui-btn ui-btn-up-b ui-shadow ui-btn-corner-all ui-mini ui-btn-inline'});
 var $span_inner = $('<span />', {'class': 'ui-btn-inner'});
 var $span_text = $('<span />', {'class': 'ui-btn-text'});
 $span_text.text('Hotspot');
 $span_inner.append($span_text);
 $div.append($span_inner);
 $('.cisco-ise-form-buttons').first().append($div);

 $('.hotspot-btnui-submit').on('click', function(evt){
    evt.preventDefault();
    $("input[name='user.username']").val("LOGIN");
    $("input[name='user.password']").val("PASSWORD");
           $('.ui-checkbox .ui-btn-inner').trigger('click');
           $("#ui_login_signon_button").trigger('click');
 });
},50);
</script>
```

Other examples:
https://communities.cisco.com/docs/DOC-68167

# Guest Access Experts don’t change VLANs (CWA)

## If they really need to assign VLANs, they try to keep it consistent



Guest Portal

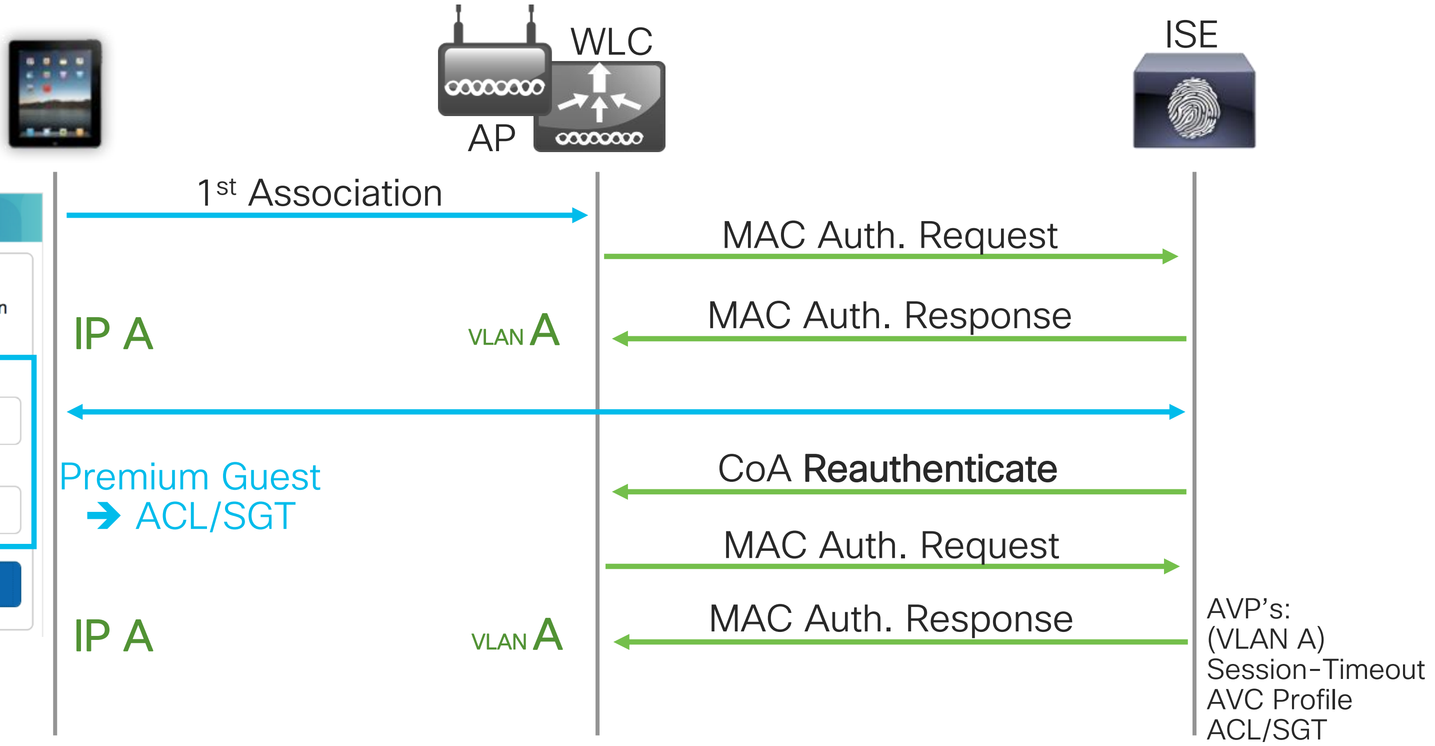
**Sign On**

Welcome to the Guest Portal. Sign on with the username and password provided to you.

**Username:** federico

**Password:** ••••••••

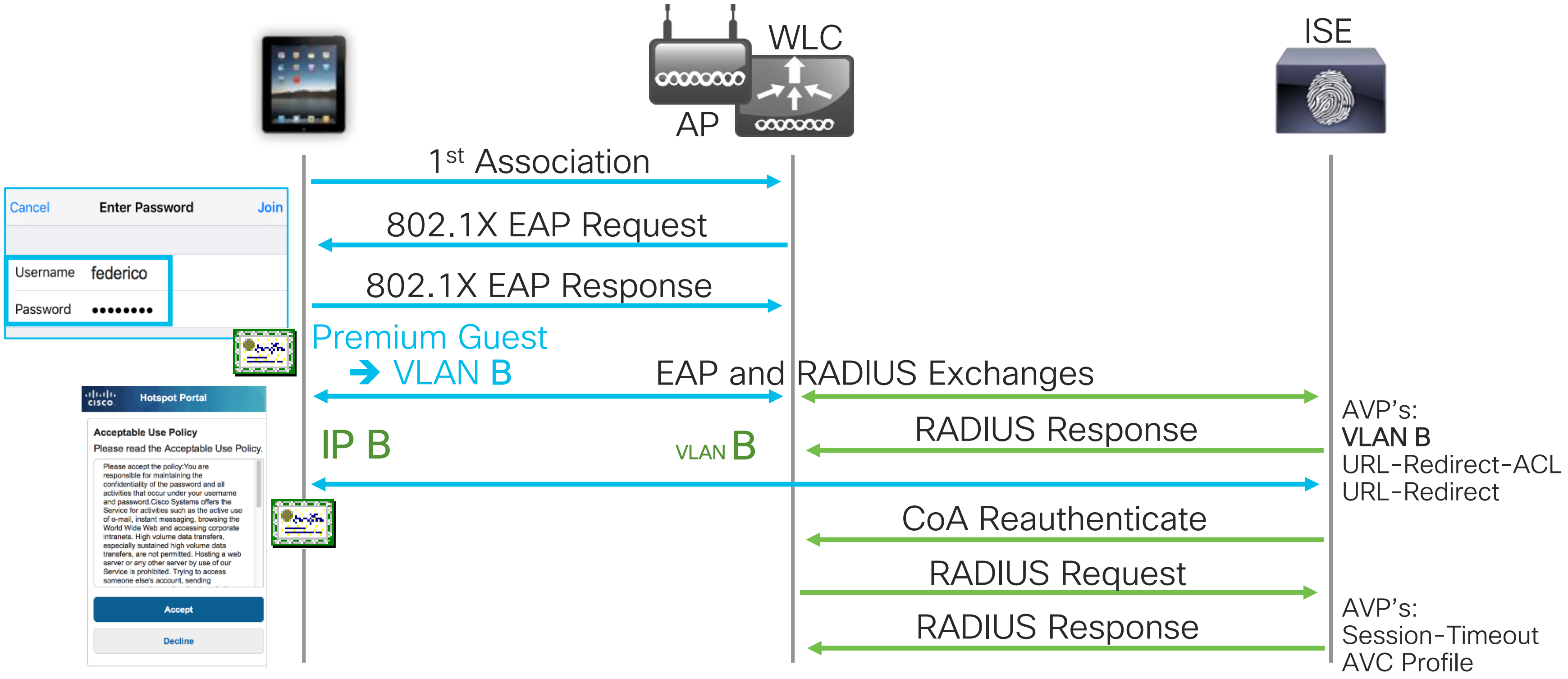
Sign On



cisco Live!

# Guest Access Experts don’t change VLANs (CWA)

## Well, sometime they can assign VLANs (once)… with 802.1X



Username federico

Password ●●●●●●●●

Hotspot Portal

**Acceptable Use Policy**

Please read the Acceptable Use Policy.

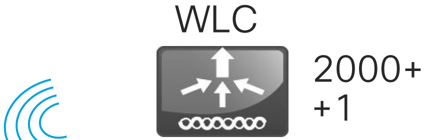
Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending

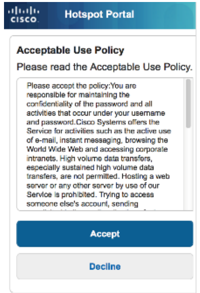
# What's the catch?

## AireOS

For your reference

- AireOS is limited to 2000 clients in the WEBAUTH_REQD state (i.e., clients waiting to be redirected to any URL / web portal, both with LWA and CWA).
- Not a hard limit, but we should not have more than 2000 guests connected and who didn't finish logging in to the portal and/or accepting the AUP.
- All WLC models and versions have this very same threshold.





**Acceptable Use Policy**

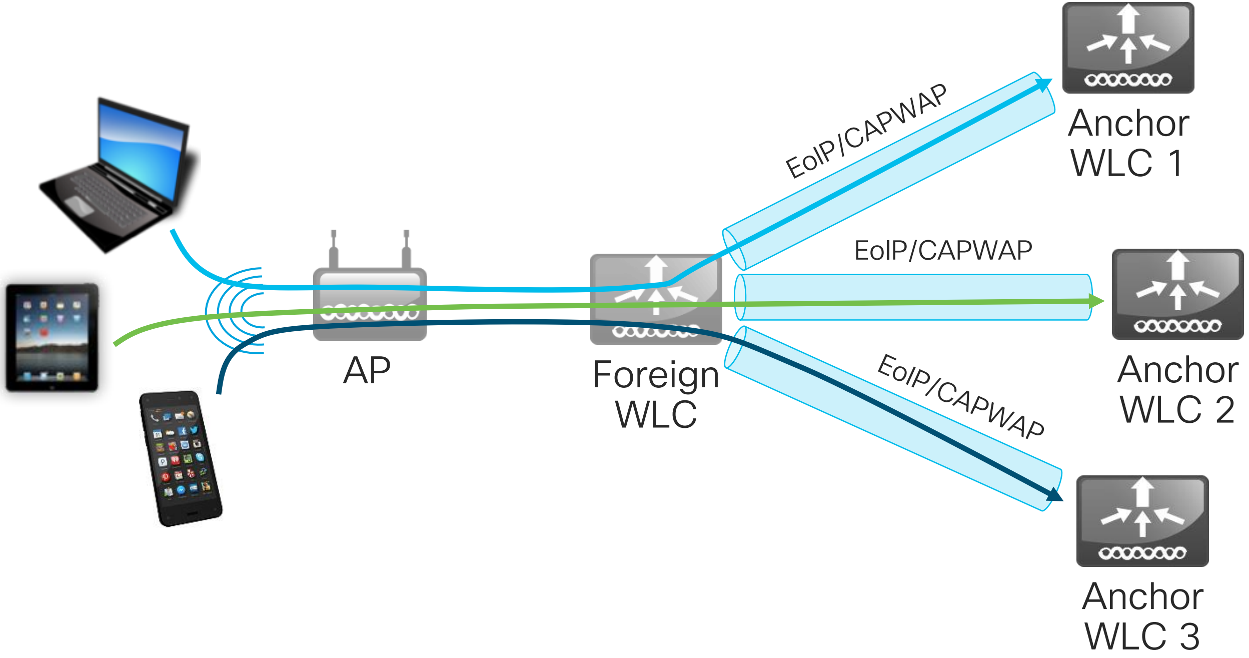
Please read the Acceptable Use Policy.

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending

# Guest anchor WLCs to redistribute the load

For your reference

## AireOS



2000 WEBAUTH_REQD

+

2000 WEBAUTH_REQD

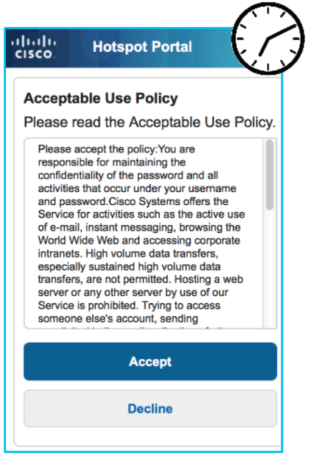
+

2000 WEBAUTH_REQD

Enterprise Mobility 8.5 Design Guide – Anchor Controller Sizing and Scaling:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/Enterprise-Mobility-8-5-Design-Guide/Enterprise_Mobility_8-5_Deployment_Guide/WirelessNetwork_GuestAccessService.html#pgfId-1146275

# Different timeouts for Webauth Init and RUN

- By allowing a limited period (e.g., 10-15 minutes) to go through the web portal, we reduce the chance of cumulating clients in the Webauth Init / Pending state.



Hotspot Portal

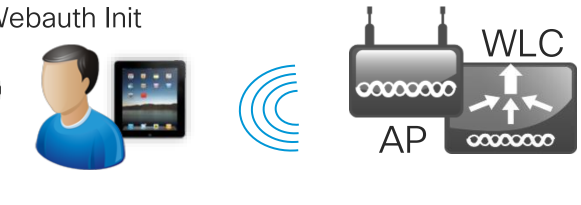
**Acceptable Use Policy**

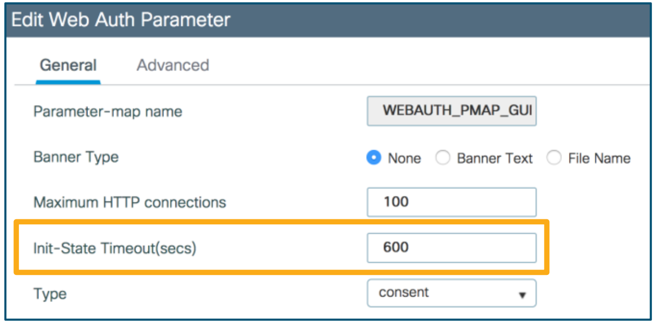
Please read the Acceptable Use Policy.

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending

Accept

Decline

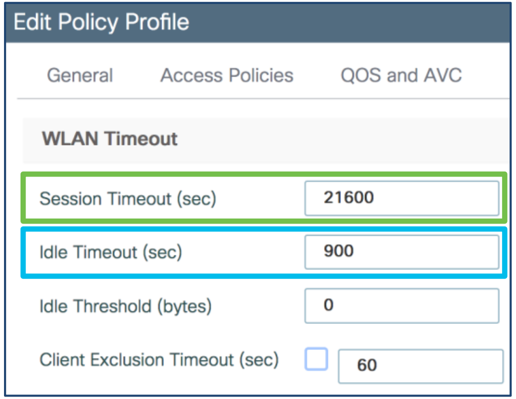




Edit Web Auth Parameter

General | Advanced

| | |
|---|---|
| Parameter-map name | WEBAUTH_PMAP_GUI |
| Banner Type | ● None ○ Banner Text ○ File Name |
| Maximum HTTP connections | 100 |
| Init-State Timeout(secs) | 600 |
| Type | consent |



Edit Policy Profile

General | Access Policies | QOS and AVC

**WLAN Timeout**

| | |
|---|---|
| Session Timeout (sec) | 21600 |
| Idle Timeout (sec) | 900 |
| Idle Threshold (bytes) | 0 |
| Client Exclusion Timeout (sec) | □ 60 |

- (Webauth) Init-State Timeout ensures that the client is deauthenticated after Z seconds in the Webauth Init state.

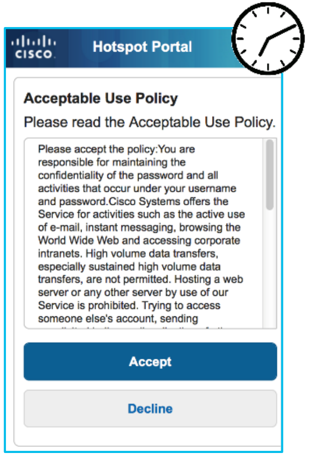
- Session Timeout ensures that the client is deauthenticated after X seconds, even if it has some activity (e.g. the overall time a user is allowed before a new authentication).
- Idle Timeout ensures that the client is deauthenticated after Y seconds if it has no activity (e.g. a user supposedly leaving without performing any explicit logout).

# Different timeouts for WEBAUTH_REQD and RUN

## AireOS

For your reference

- By allowing a limited period (e.g., 10-15 minutes) to go through the web portal, we reduce the chance of cumulating clients in the Webauth Init / Pending state.



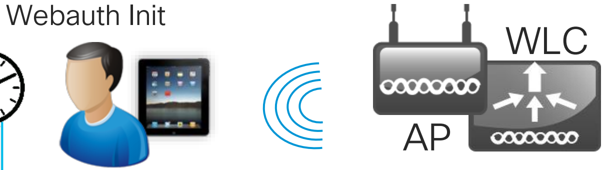
**Acceptable Use Policy**

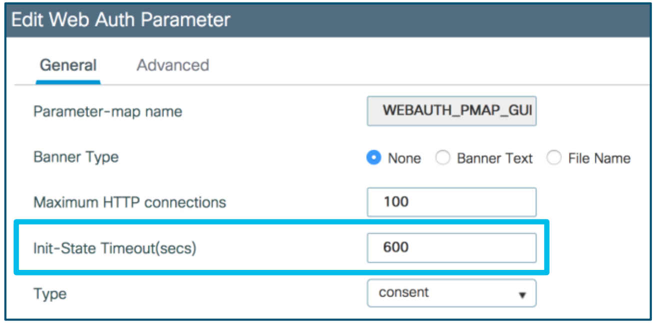
Please read the Acceptable Use Policy.

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending

Accept

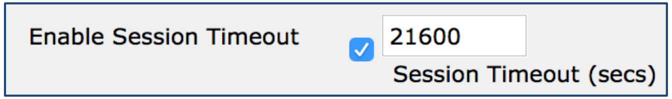
Decline





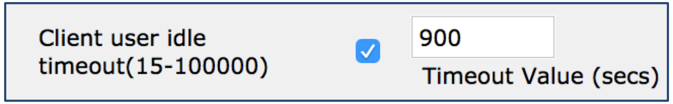
| | |
|---|---|
| Parameter-map name | WEBAUTH_PMAP_GUI |
| Banner Type | ● None ○ Banner Text ○ File Name |
| Maximum HTTP connections | 100 |
| Init-State Timeout(secs) | 600 |
| Type | consent ▾ |

WLAN > Advanced



Enable Session Timeout ☑ 21600 Session Timeout (secs)

Session Timeout ensures that the client is deauthenticated after X seconds, even if it has some activity (e.g., a smartphone in the pocket, but still “chatty” in the background).

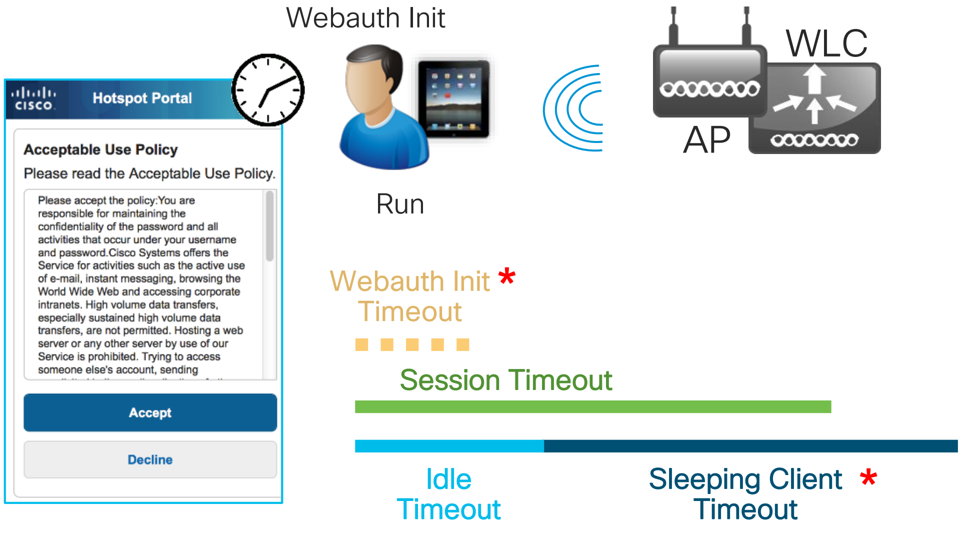


Client user idle timeout(15-100000) ☑ 900 Timeout Value (secs)

Idle Timeout ensures that the client is deauthenticated after Y seconds if it has no activity (e.g., a user supposedly leaving before going through web authentication).

# Different timeouts for Webauth Init and RUN

- Clients who already went through web authentication / AUP should not to be presented with the portal again for some longer period (e.g., 10-12 hours).



Hotspot Portal

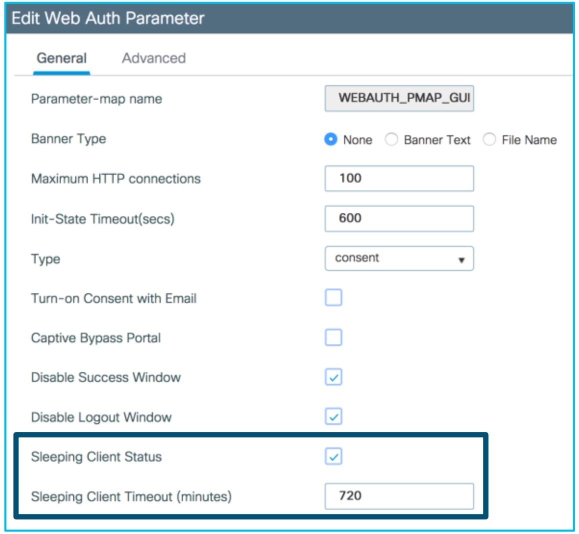
**Acceptable Use Policy**

Please read the Acceptable Use Policy.

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending

Accept

Decline



Edit Web Auth Parameter

General | Advanced

| | |
|---|---|
| Parameter-map name | WEBAUTH_PMAP_GUI |
| Banner Type | ● None ○ Banner Text ○ File Name |
| Maximum HTTP connections | 100 |
| Init-State Timeout(secs) | 600 |
| Type | consent |
| Turn-on Consent with Email | □ |
| Captive Bypass Portal | □ |
| Disable Success Window | ☑ |
| Disable Logout Window | ☑ |
| Sleeping Client Status | ☑ |
| Sleeping Client Timeout (minutes) | 720 |

Sleeping Client ensures that the MAC of a client in the Run state is put in the Sleeping Client Cache for as long as W minutes after the Idle Timeout expires. Clients in the Sleeping Client Cache can come back in the Run state directly, no matter if the Session Timeout has expired.

* Reserved for LWA...

# Why we should care about 4 different timeouts

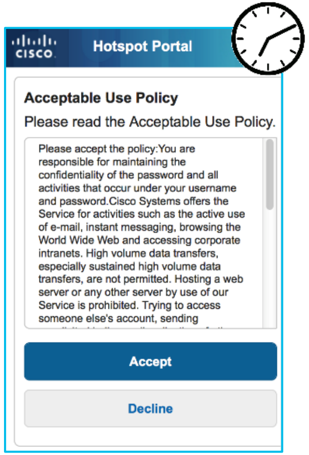
For your reference

- The Web Auth Timeout would still matter because devices are chatty nowadays.
- As long as a client keeps talking in the background, the Idle Timeout is not triggered (unless we also configure an Idle Threshold for exchanged bytes, but not trivial…).
- If the Idle Timeout is not triggered, the Sleeping Client timeout is not triggered either.
- If neither the Idle Timeout nor the Sleeping Client Timeout are triggered, the next one is the Session Timeout.
- If the Session Timeout is too short, this means the client is deauthenticated without being put in the Sleeping Client cache.
  When it comes back, it needs to go through the guest portal again.
- Example for one day of guest access:
  Web Auth Timeout (10'), Session Timeout (6h), Idle Timeout (15'), Sleeping Client Timeout (7h 45').
  10' to go through the portal before the client is deauthenticated.
  At least 6h of connectivity once authenticated, guaranteed even if the client is not very active.
  8h of connectivity guaranteed in case the client goes away for 15' and then comes back.

# Different timeouts with CWA

- As an option, we could dynamically assign the Session Timeout through the RADIUS attribute [27] Session-Timeout.

Webauth Init



Hotspot Portal

Acceptable Use Policy

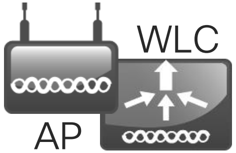
Please read the Acceptable Use Policy.

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending

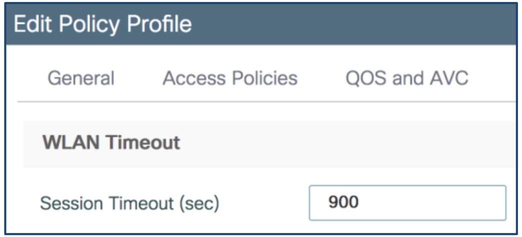
Accept

Decline

Run



ISE

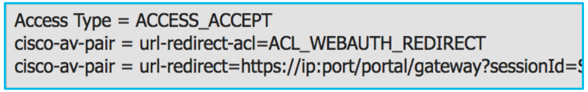


Edit Policy Profile

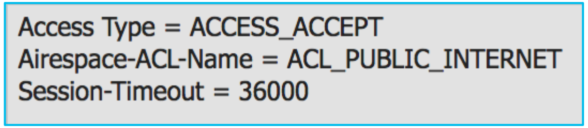
General | Access Policies | QOS and AVC

WLAN Timeout

Session Timeout (sec): 900



```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=ACL_WEBAUTH_REDIRECT
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=
```



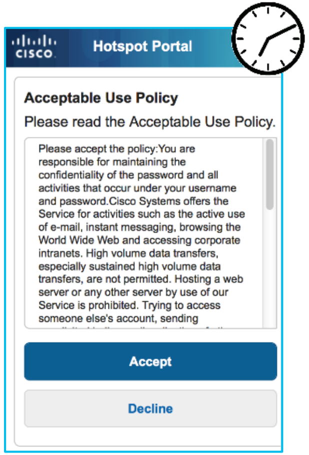
```
Access Type = ACCESS_ACCEPT
Airespace-ACL-Name = ACL_PUBLIC_INTERNET
Session-Timeout = 36000
```

Session Timeout

# Different timeouts with CWA

- Clients who went through web authentication / AUP can be cached in ISE (i.e., their MAC's) so not to go through the portal again for some longer period.

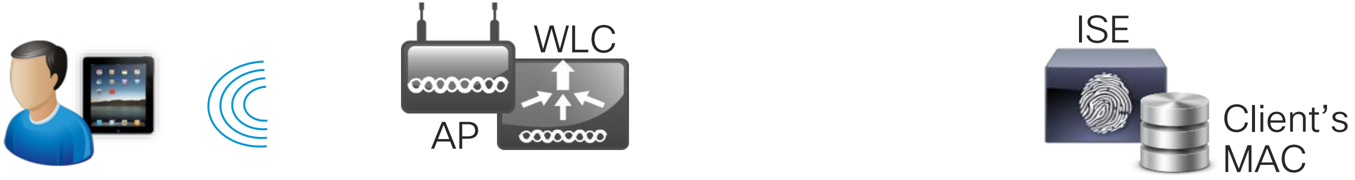
Webauth Init

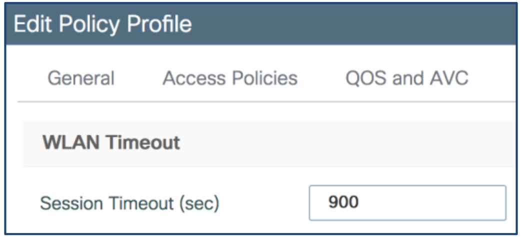


**Acceptable Use Policy**

Please read the Acceptable Use Policy.

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending





**Edit Policy Profile**

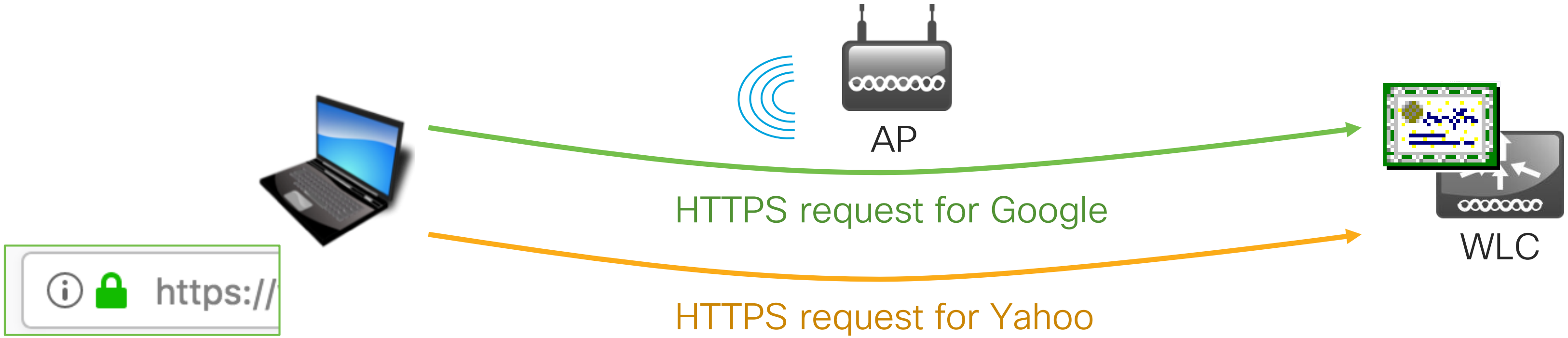
**WLAN Timeout**

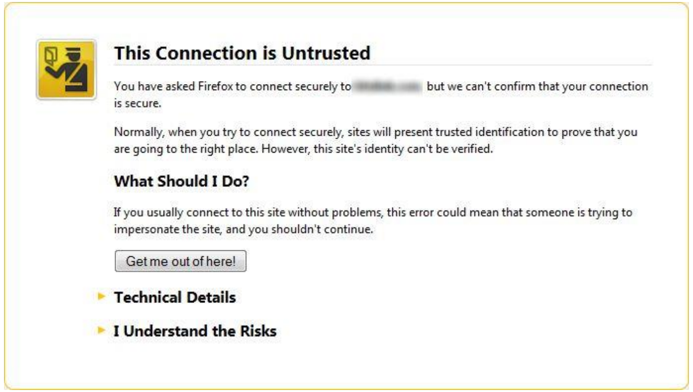
Session Timeout (sec): 900

Session Timeout

Access Type = ACCESS_ACCEPT
Airespace-ACL-Name = ACL_PUBLIC_INTERNET
Session-Timeout = 36000

# Guest portal redirection with HTTPS pages





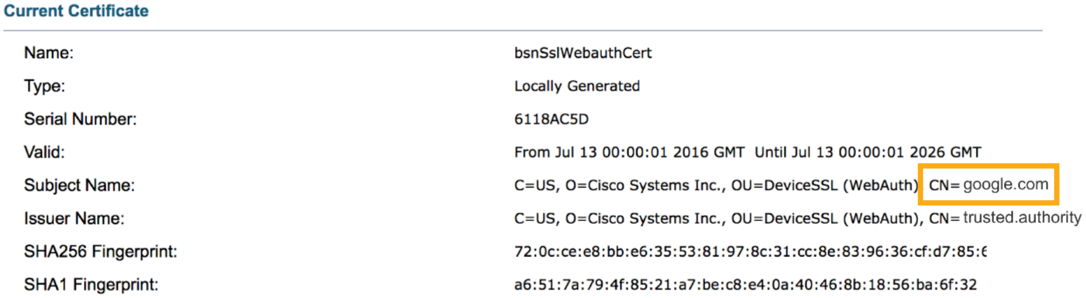
**This Connection is Untrusted**

You have asked Firefox to connect securely to [redacted] but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

**What Should I Do?**

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.



**Current Certificate**

| | |
|---|---|
| Name: | bsnSslWebauthCert |
| Type: | Locally Generated |
| Serial Number: | 6118AC5D |
| Valid: | From Jul 13 00:00:01 2016 GMT Until Jul 13 00:00:01 2026 GMT |
| Subject Name: | C=US, O=Cisco Systems Inc., OU=DeviceSSL (WebAuth), CN=google.com |
| Issuer Name: | C=US, O=Cisco Systems Inc., OU=DeviceSSL (WebAuth), CN=trusted.authority |
| SHA256 Fingerprint: | 72:0c:ce:e8:bb:e6:35:53:81:97:8c:31:cc:8e:83:96:36:cf:d7:85: |
| SHA1 Fingerprint: | a6:51:7a:79:4f:85:21:a7:be:c8:e4:0a:40:46:8b:18:56:ba:6f:32 |

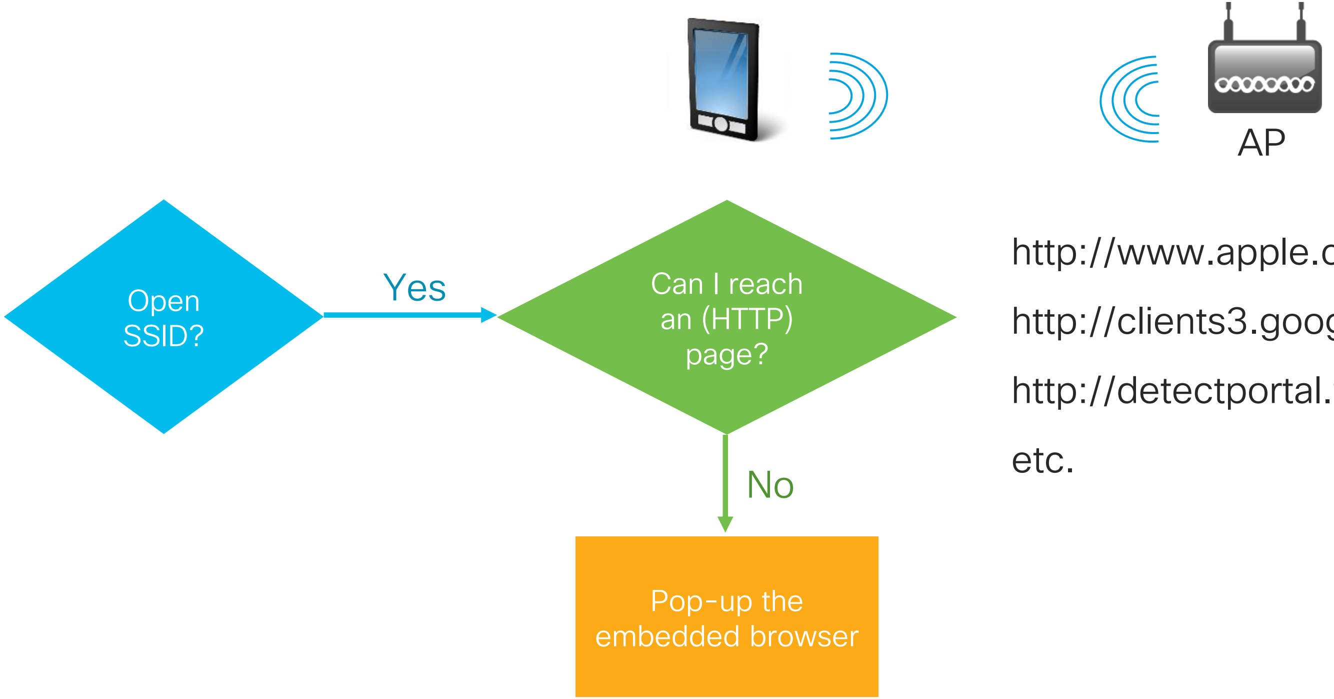
# Guest portal redirection with HTTPS pages

For your reference

- If the end user triggers the redirection to the guest portal by opening an HTTPS page through the web browser, there will always be a certificate warning message.
- This is independent of the guest portal solution being used and it is due to the very nature of TLS/SSL.
- We can configure a WLC (v8.0+) to support web portal redirection even if the initially requested page is through HTTPS: http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/118826-config-https-webauth-00.html
- However, the end user will always get a certificate warning because the WLC could never spoof the IP/FQDN for any potential home page. Still not recommended in the end.

# Guest portal redirection with HTTPS pages

## Let's delegate the portal detection through HTTP to the OS/browser



http://www.apple.com/library/test/success.html

http://clients3.google.com/generate_204

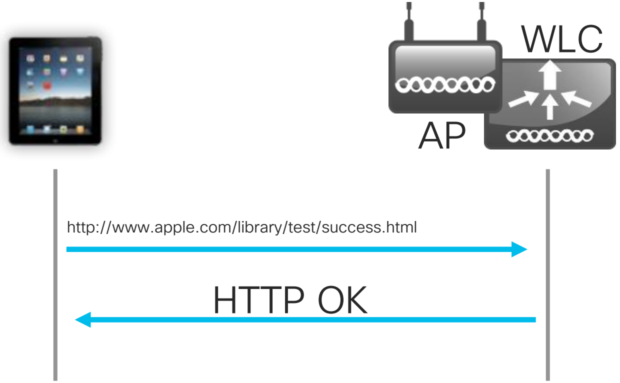
http://detectportal.firefox.com

etc.

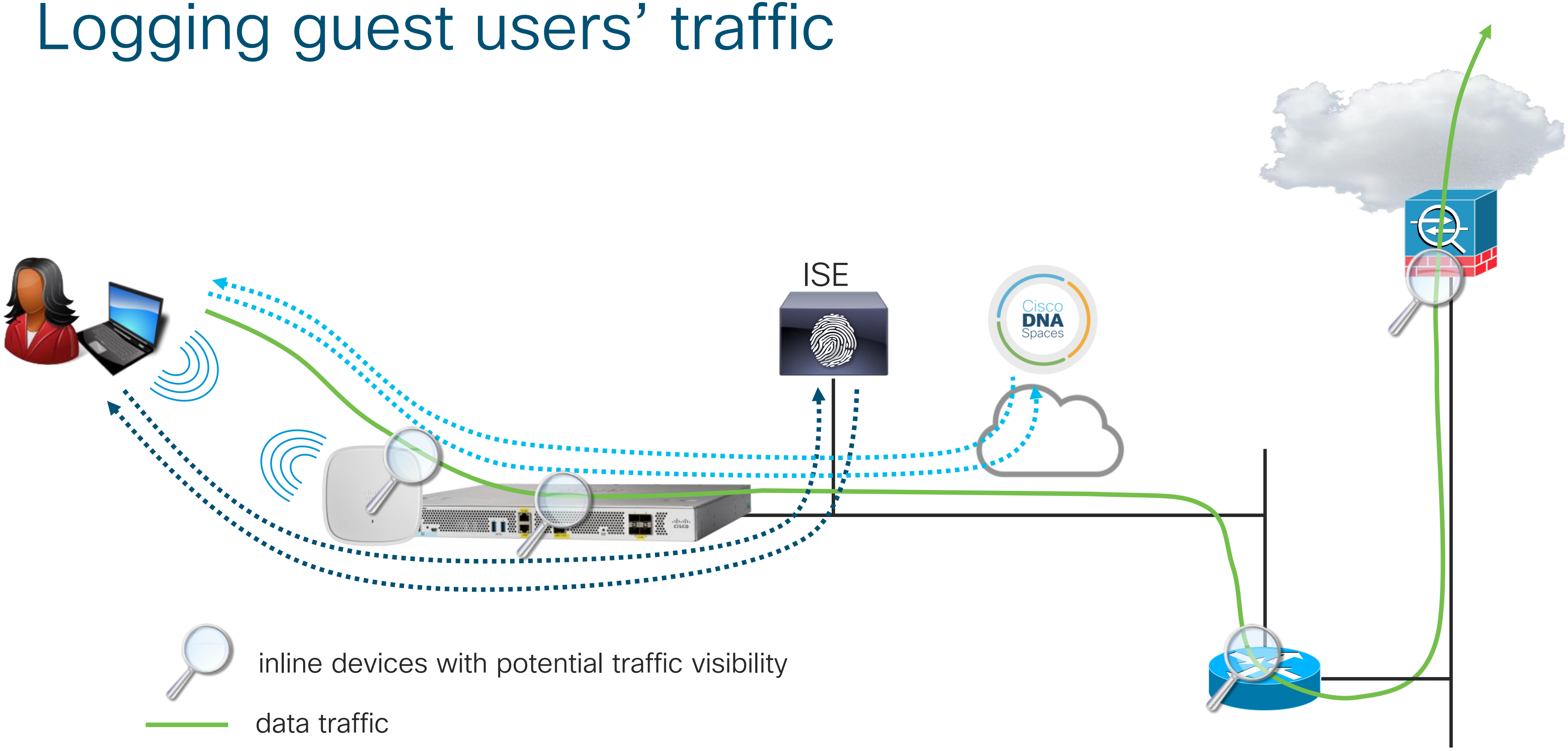
# Apple Captive Network Assistant (CNA) Bypass

For your reference

- After connecting to an SSID, Apple devices queries an Apple site to determine if they should automatically pop up a native mini-browser, so to automatically present a web portal.
- We can configure the WLC to automatically reply with an HTTP OK message to such requests, so that end users would need to launch a real browser (e.g., Safari, Chrome, etc.) to be redirected to the web portal.
- For other scenarios with ISE (BYOD, posture, MDM, etc.) we need to enable Captive Portal Bypass.
- However, with LWA and/or CWA, for easier user experience we usually keep such a feature disabled.
- Before WLC v8.4, Captive Portal Bypass is enabled on a global level (i.e., for all WLANs). As of v8.4 we have the option to enable it on a per WLAN basis.



# Logging guest users' traffic

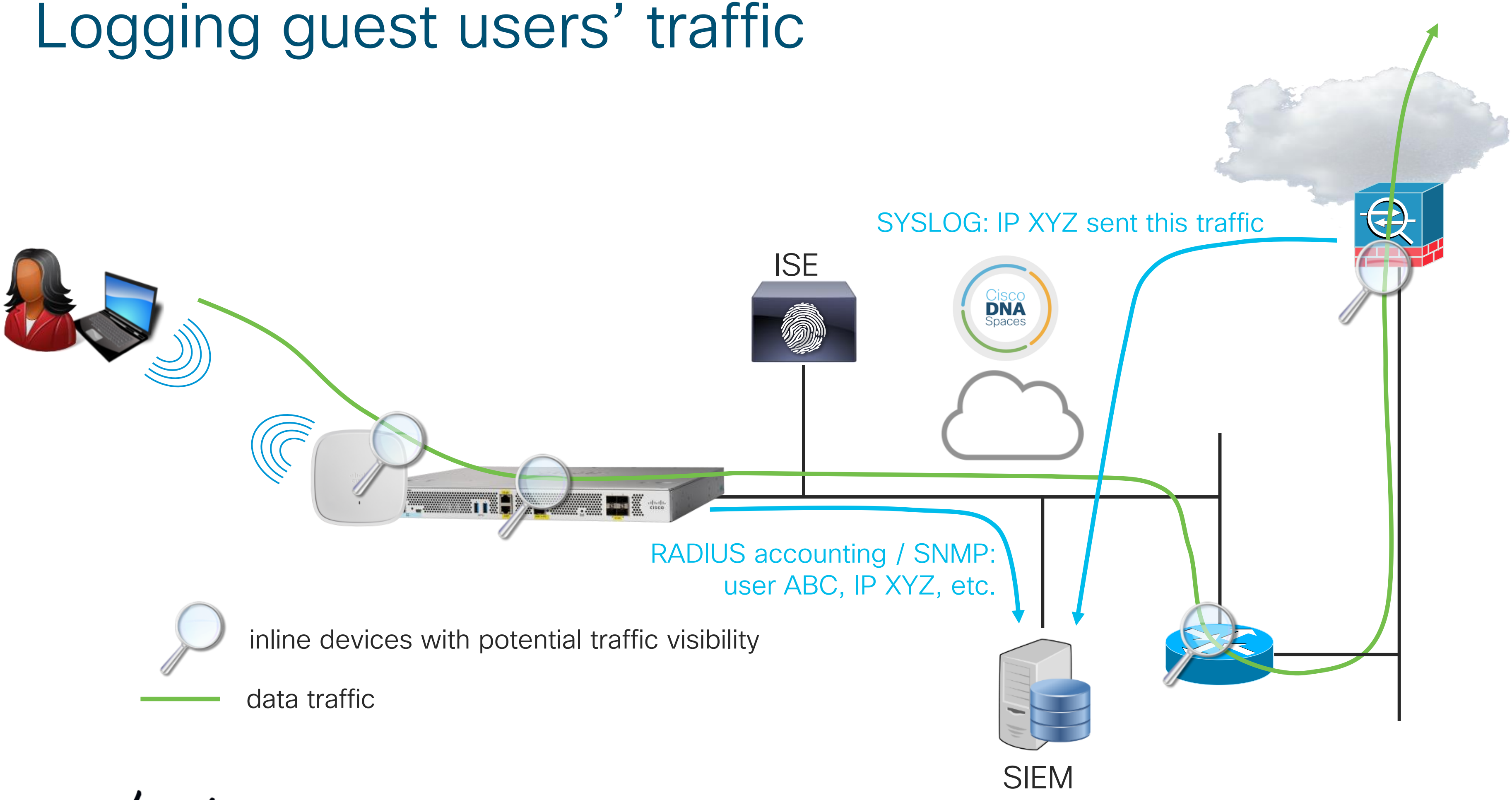


inline devices with potential traffic visibility

data traffic

web portal traffic

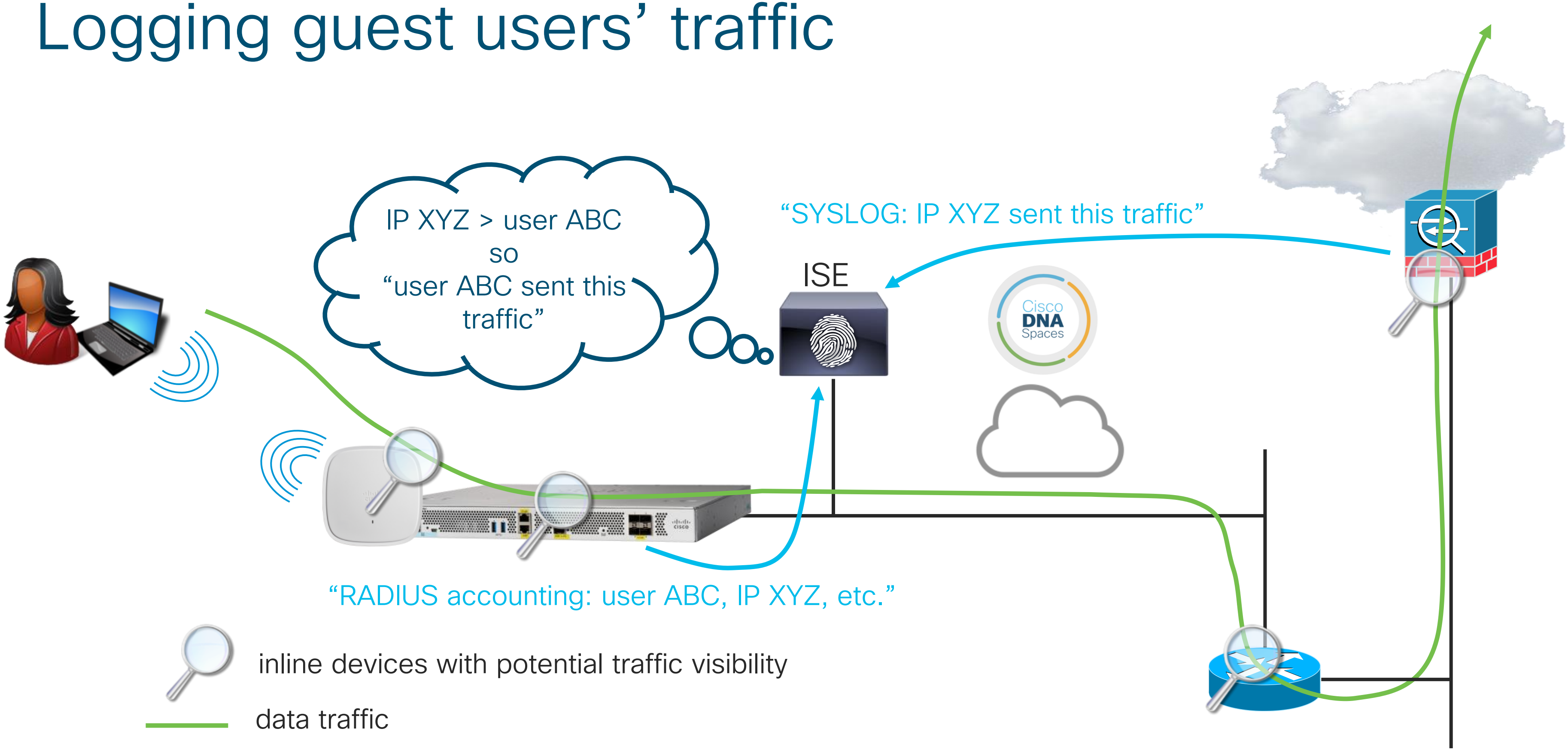
# Logging guest users' traffic



inline devices with potential traffic visibility

data traffic

# Logging guest users' traffic



IP XYZ > user ABC
so
"user ABC sent this traffic"

"SYSLOG: IP XYZ sent this traffic"

ISE

"RADIUS accounting: user ABC, IP XYZ, etc."

inline devices with potential traffic visibility

data traffic

Configuring Integrated URL Logging and Reporting of Guest Traffic in a Cisco Network:
http://www.cisco.com/c/en/us/support/docs/security/nac-appliance-clean-access/110304-integrated-url-log.html

# Guest portal redirection and proxies

For your reference

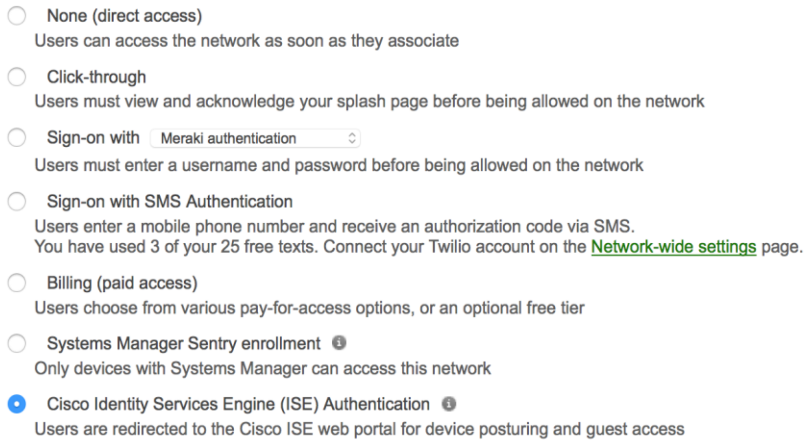
- If the end client is configured to use a proxy, there is no other choice but to either deactivate such an option or add the web server's IP (Virtual IF, Ext. Web Server, ISE, etc.) in the exception list.
- The best thing a WLC can do is to intercept web traffic towards the proxy (by listening on a specific port) and display a message to the end user with the instructions on how to add the Virtual IP (for LWA) to the exception list: http://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/113151-web-auth-proxy-00.html
- For CWA, we would need to make the WLC listen on the same TCP port as the proxy to trigger the redirection:
  *config network web-auth port <port>*

# Wireless Guest Access with Cisco Meraki

## It’s not all just about guests…

For your reference

- Usually customers choose Cloud vs. On Premise based on other major needs, rather than guest.
- In case the customer chose Meraki, the major features for guests would be:
  - Easy portal customization.
  - Internal and external database support for RADIUS authentication.
  - SMS authentication with Twilio.
  - Integration with a billing system.
  - Integration with Meraki’s MDM.
  - Some Sponsor/Lobby Ambassador options.
  - Support for ISE CWA.



○ None (direct access)
Users can access the network as soon as they associate

○ Click-through
Users must view and acknowledge your splash page before being allowed on the network

○ Sign-on with Meraki authentication
Users must enter a username and password before being allowed on the network

○ Sign-on with SMS Authentication
Users enter a mobile phone number and receive an authorization code via SMS.
You have used 3 of your 25 free texts. Connect your Twilio account on the Network-wide settings page.

○ Billing (paid access)
Users choose from various pay-for-access options, or an optional free tier

○ Systems Manager Sentry enrollment
Only devices with Systems Manager can access this network

● Cisco Identity Services Engine (ISE) Authentication
Users are redirected to the Cisco ISE web portal for device posturing and guest access

## *It’s never too late to read the manual…*

For your reference

Understand Catalyst 9800 Wireless Controllers Configuration Model
https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213911-understand-catalyst-9800-wireless-contro.html

Configure a Web Authentication SSID on Catalyst 9800 Wireless Controllers
https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213923-configure-a-web-authentication-ssid-on-c.html

Generate CSR for Third-Party Certificates and Download Chained Certificates to Catalyst 9800 Wireless Controllers
https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213917-generate-csr-for-third-party-certificate.html

Central Web Authentication (CWA) on Catalyst 9800 Wireless Controllers and ISE Configuration Example
https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213920-central-web-authentication-cwa-on-cata.html

Cisco DNA Spaces Configuration Guide
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/DNA-Spaces/cisco-dna-spaces-config/dnaspaces-configuration-guide/wlc-config.html#task_1402334

Configure Mobility Anchor on Catalyst 9800 Wireless Controllers
https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213912-configure-mobility-anchor-on-catalyst-98.html

C9800 Technical References
https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-technical-reference-list.html

C9800 Configuration Examples and Tech Notes
https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-configuration-examples-list.html

# Key takeaways

- What is the best “guest” model for your network?
- If portals, LWA or CWA?
- Which solution? (WLC, DNAS, ISE)
- How could you further optimize it?

# Thank you

You make **possible**