The bridge to possible

Becoming a Wi-Fi Guest Star

Better Practices for Guest Networks on Cisco Catalyst Wireless

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

Special thanks to **Jérôme Henry, Principal Engineer, CCIE 24750**
Who contributed to and presented this resource

From rocking guest Wi-Fi...

...to guest Wi-Fi rock stars

Federico ➔ Fede

- ~16 years at Cisco Systems
  - 4 years as a Customer Support Engineer (CSE)
  - 3 years as a Specialized Systems Engineer
  - 5 years as a Consulting Systems Engineer (CSE)
  - ~4 year as a Technical Solutions Architect (TSA)
- Always focused on Wireless and NAC

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

Cisco Webex App

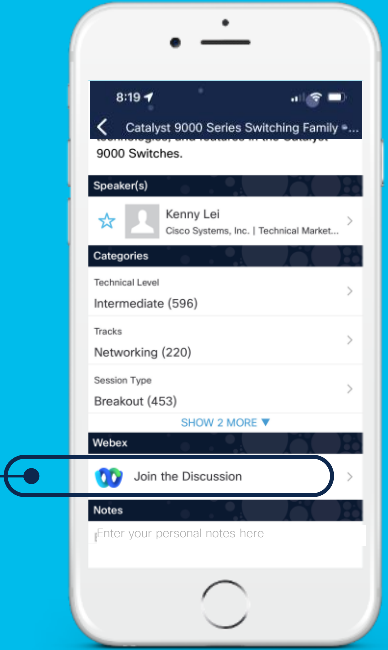
Questions?

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

How

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

Webex spaces will be moderated
until February 24, 2023.



8:19

Catalyst 9000 Series Switching Family ...

9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

A new breakout on wireless guest...

- Learn from past feedbacks, usefulness and popularity of a feature, requests for more content, etc.
- Some new topics, more details and updates
- References (BRKEWN-2014) [https://www.ciscolive.com/on-demand/on-demand-library.html?#/session/1636060078943001 7umm](https://www.ciscolive.com/on-demand/on-demand-library.html?#/session/16360600789430017umm)

* Screenshots may refer to different IOS-XE versions, but the options stay very similar

Agenda

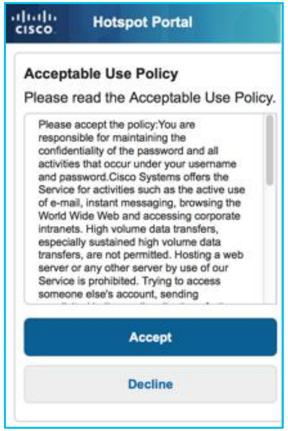
- What are guest networks?
- Guest portals techniques and configuration
- Portal-less options (Passpoint and OpenRoaming)
- Advanced settings for better end user experience

Guest Wi-Fi Options

“Open”

Wi-Fi
password is
123hackme

Guest Portal



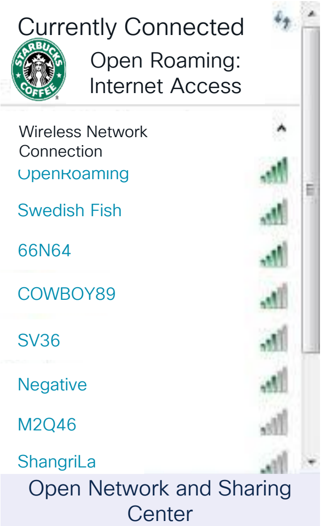
Hotspot Portal

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

OpenRoaming



Currently Connected

Open Roaming:
Internet Access

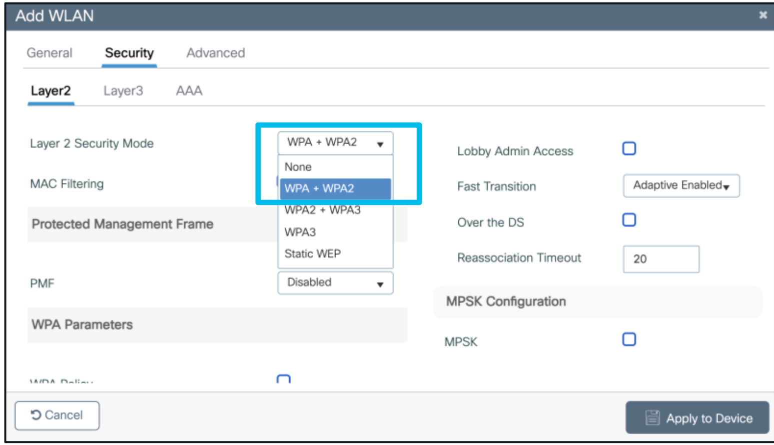
Wireless Network
Connection

OpenRoaming
Swedish Fish
66N64
COWBOY89
SV36
Negative
M2Q46
ShangriLa

The “Open” option

- No security, no authentication
  - Or “light” security (publicly available passphrase)
  - Or OWE*
- Easy to setup
- Useful for avoiding massive network resources usage (e.g., DHCP)
- Changing password may lead to poor user experience

WLAN creation on C9800



Add WLAN

Layer 2 Security Mode: WPA + WPA2

MAC Filtering

Protected Management Frame

PMF: Disabled

WPA Parameters

WPA Policy

Lobby Admin Access □

Fast Transition: Adaptive Enabled

Over the DS □

Reassociation Timeout: 20

MPSK Configuration

MPSK □

* Opportunistic Wireless Encryption…. assuming your clients are supporting it

For wireless, it’s either secure or open

- 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 on the same SSID.
- We can have a secure SSID (PSK or 802.1X) followed by web portal authentication. In such a scenario, PSK / 802.1X must succeed before the end user can be redirected to a web portal.

Guest Portals

Customer satisfaction

Analytics / $$$

Engagements

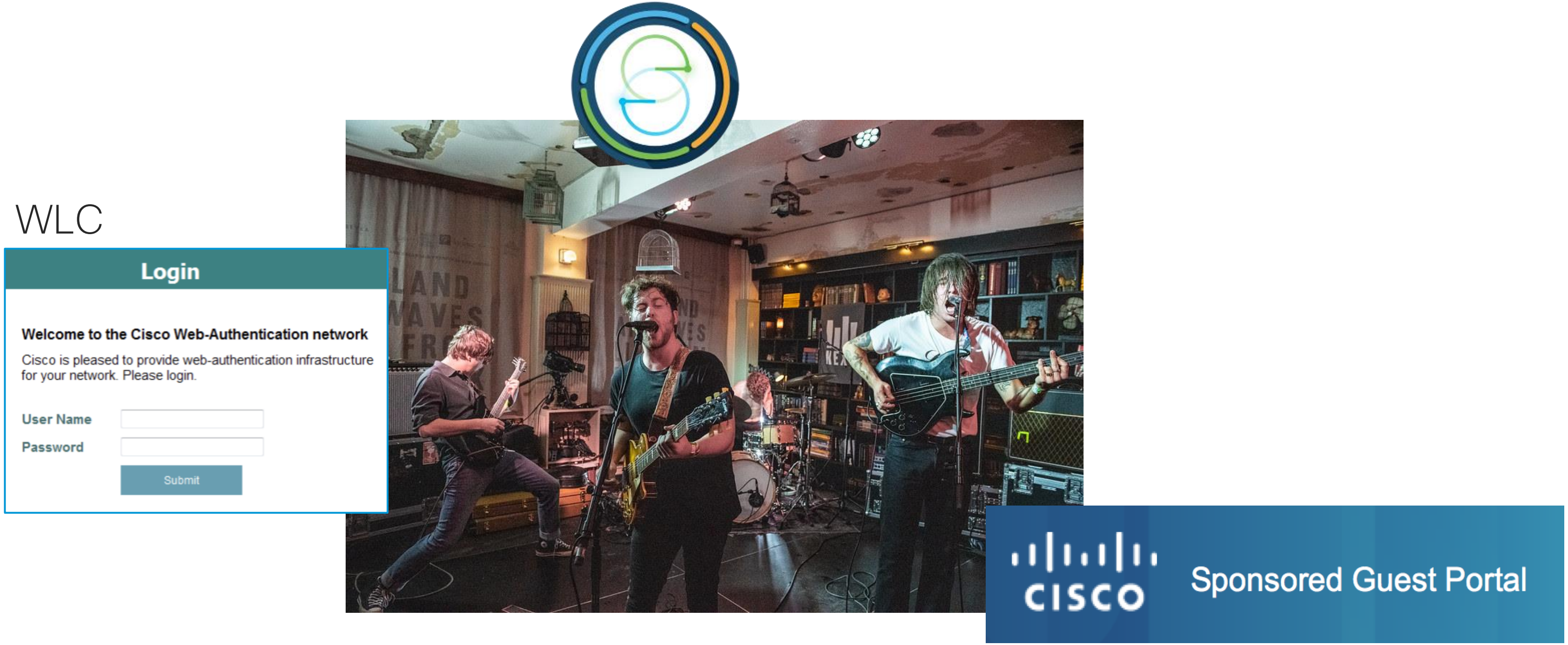
What guest portals do?

- Validate who is connecting
  - From "everyone" to "by invitation only"
  - Useful for business operations, or regulatory mandates (MAC address and/or contactable identity collection)
- Disclaimers (local regulations or liability limitation).
  - In some regulatory domains, no disclaimers may mean top tier security (firewalls, intrusion detection, etc.)

Guest portals techniques and configuration

Rocking the 3 portal options (what guests see)

Cisco Spaces



WLC

Login

Welcome to the Cisco Web-Authentication network

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

User Name

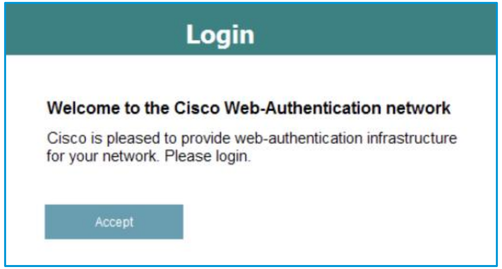
Password

Submit

Identity Services Engine (ISE)

In few words

WLC



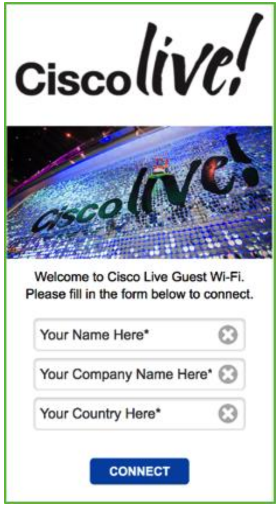
Login

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 local hotspot portals.
- LWA with consent.

Cisco Spaces



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

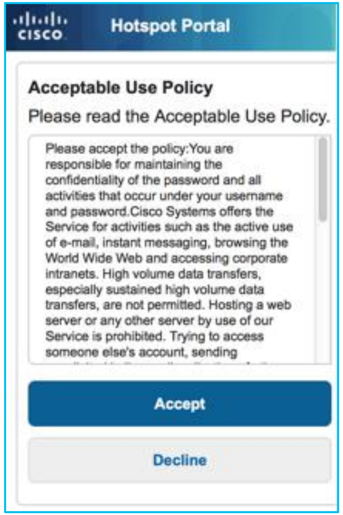
Your Name Here*

Your Company Name Here*

Your Country Here*

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

ISE



Hotspot Portal

Acceptable Use Policy

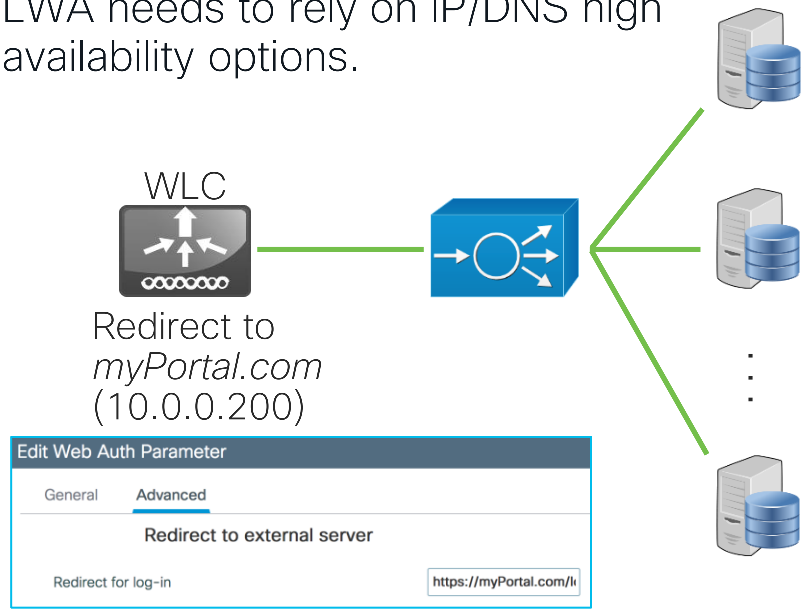
Please read the Acceptable Use Policy.

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

- Most versatile solution.
- Ideal for both hotspot and sponsored/self-reg portals.
- It requires an additional learning curve.
- LWA or CWA.

Where “authentication” happens

- Local Web Authentication (LWA) happens at L3.
- LWA needs to rely on IP/DNS high availability options.



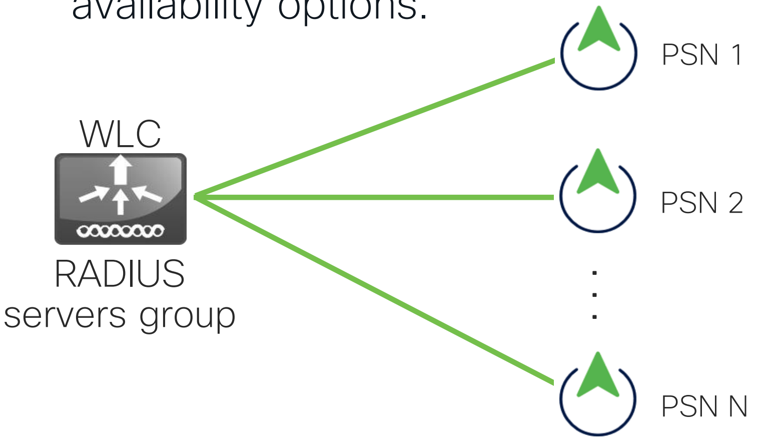
Edit Web Auth Parameter

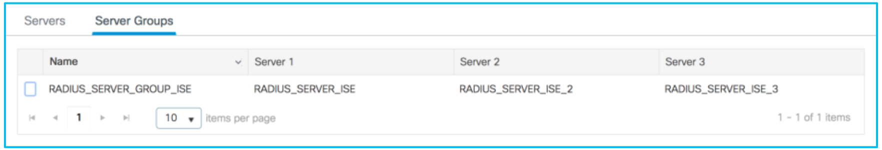
General | Advanced

Redirect to external server

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

- Central Web Authentication (CWA) happens at L2 and L3.
- CWA can rely on RADIUS / ISE high availability options.



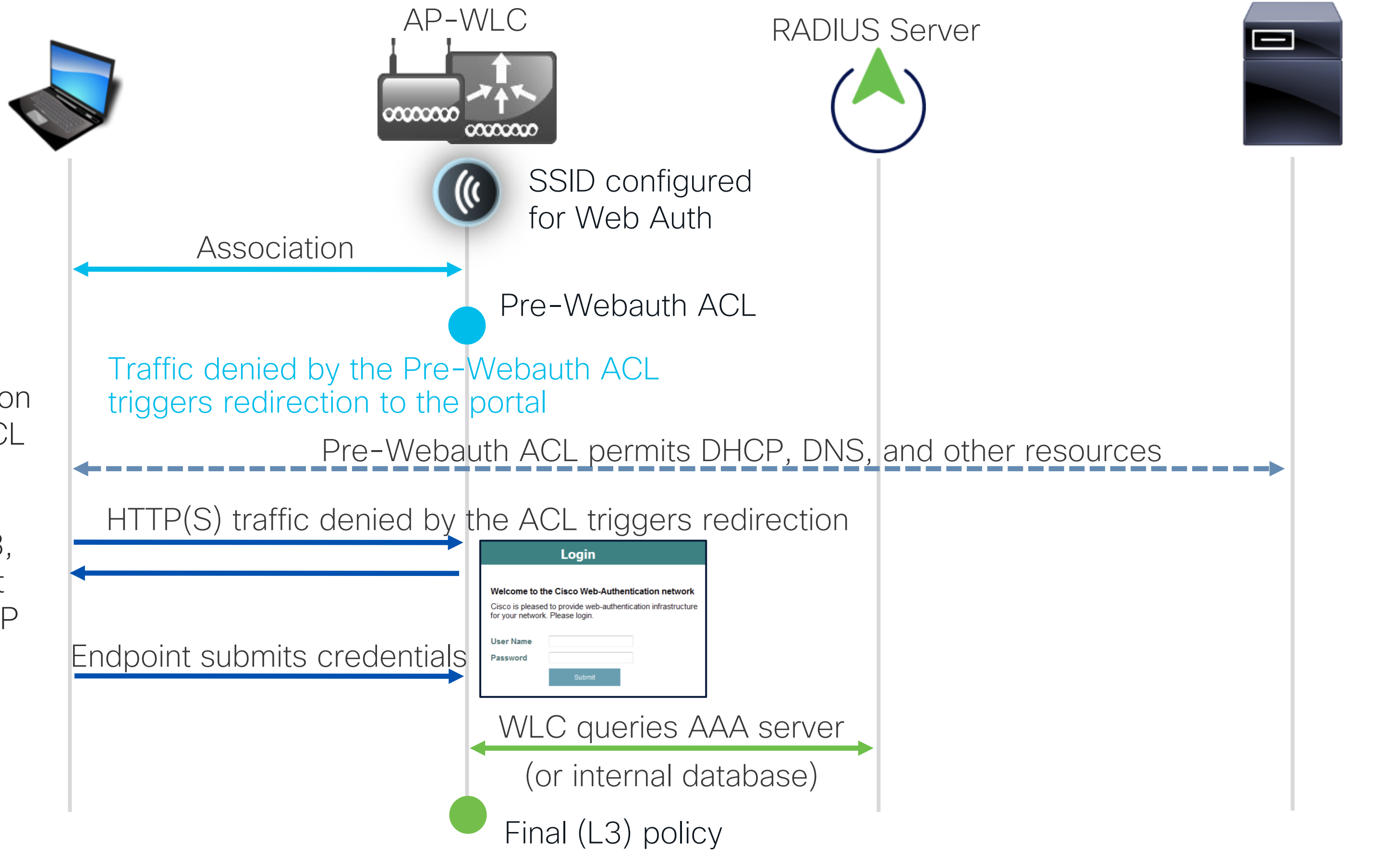


Servers | Server Groups

	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

Local Web Authentication (LWA)


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
Endpoint 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

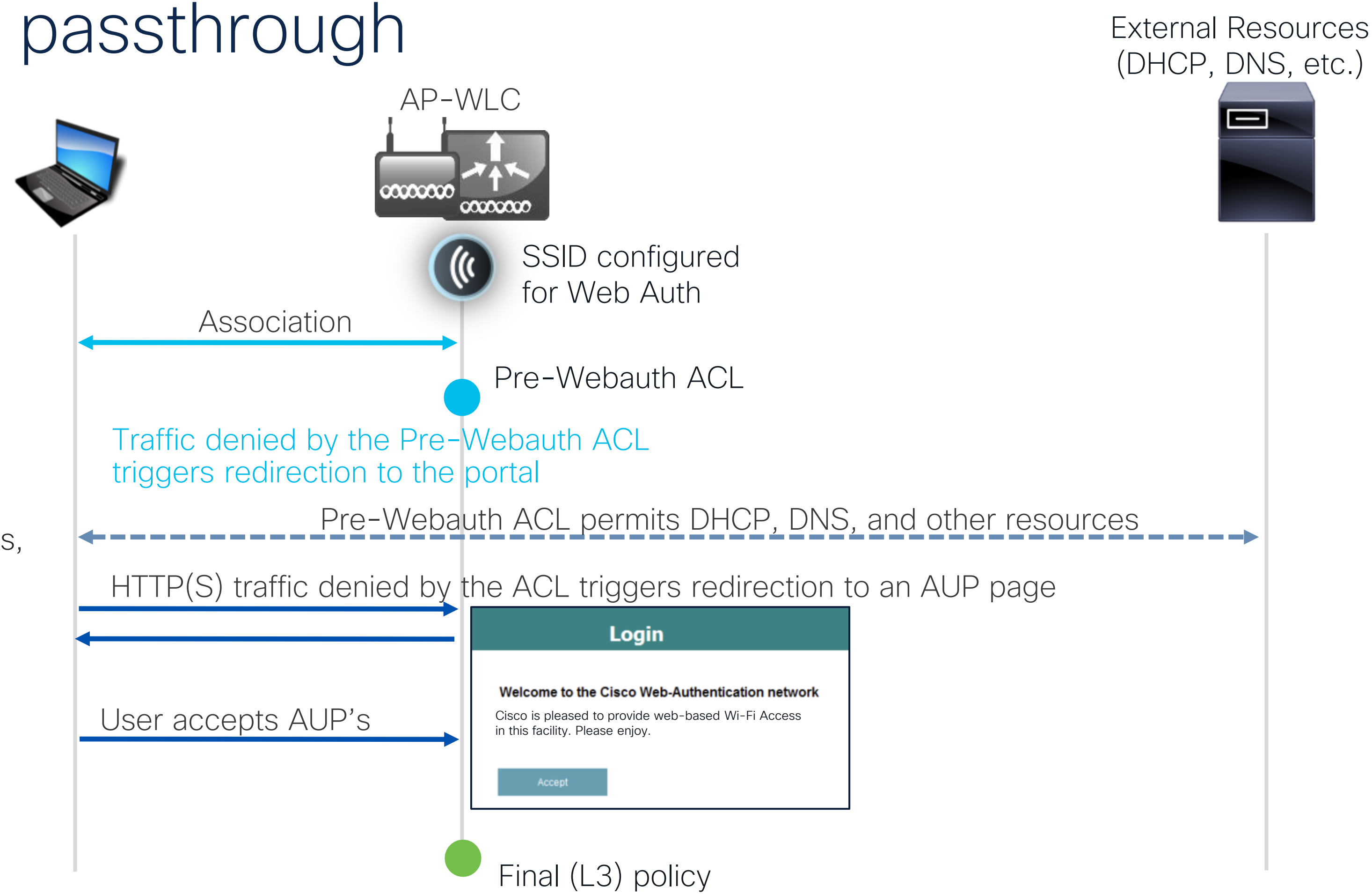
Submit

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

We say that LWA is purely L3, because it starts from a client trying to resolve a (server's) IP address.

LWA with passthrough

When you do not need to authenticate individual users, but connect anyone who asks, possibly with an Acceptable User Policy (AUP) page



External Resources (DHCP, DNS, etc.)

AP-WLC

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-based Wi-Fi Access in this facility. Please enjoy.

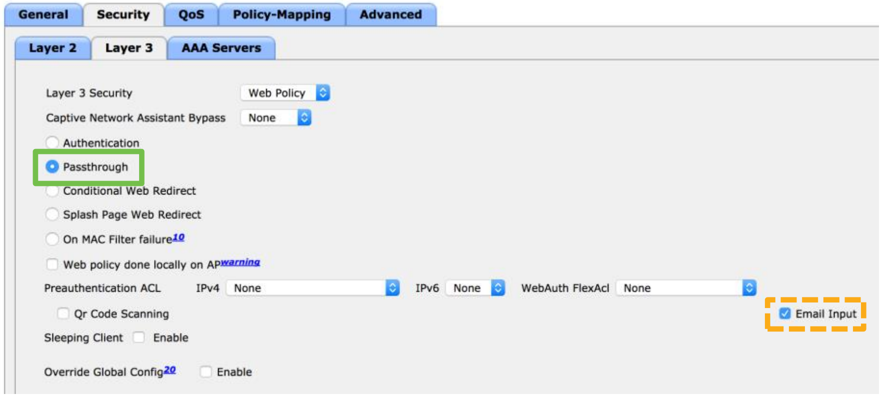
Accept

Final (L3) policy

Passthrough / Consent / Hotspot

- “Passthrough” on AireOS
- “Consent” on IOS-XE
- “Hotspot” on ISE

- The user may needs to complete some operation(s) on the web portal (e.g. click “accept”, enter an email address)
- There is no form of authentication performed by the WLC.



Layer 3 Security: Web Policy

Captive Network Assistant Bypass: None

○ Authentication

● Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

○ On MAC Filter failure[10]

□ Web policy done locally on AP[warning]

Preauthentication ACL IPv4 None IPv6 None WebAuth FlexAcl None

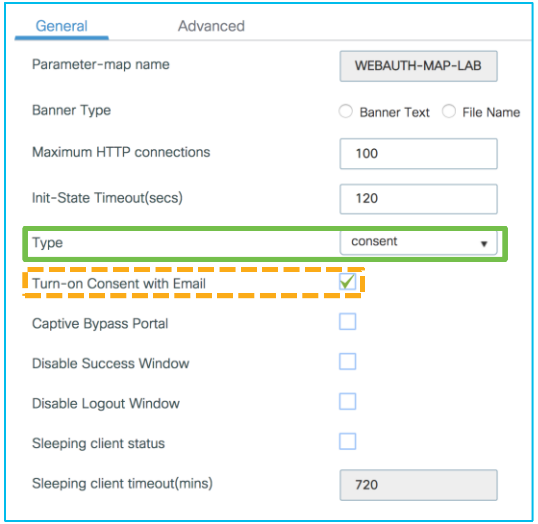
□ Qr Code Scanning ☑ Email Input

Sleeping Client □ Enable

Override Global Config[20] □ 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 □

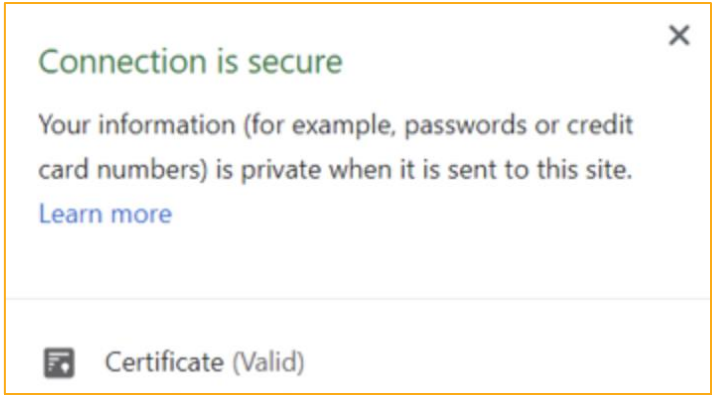
Sleeping client status □

Sleeping client timeout(mins): 720

IOS-XE

LWA and certificates

A certificate signed by a known root CA avoids scary messages

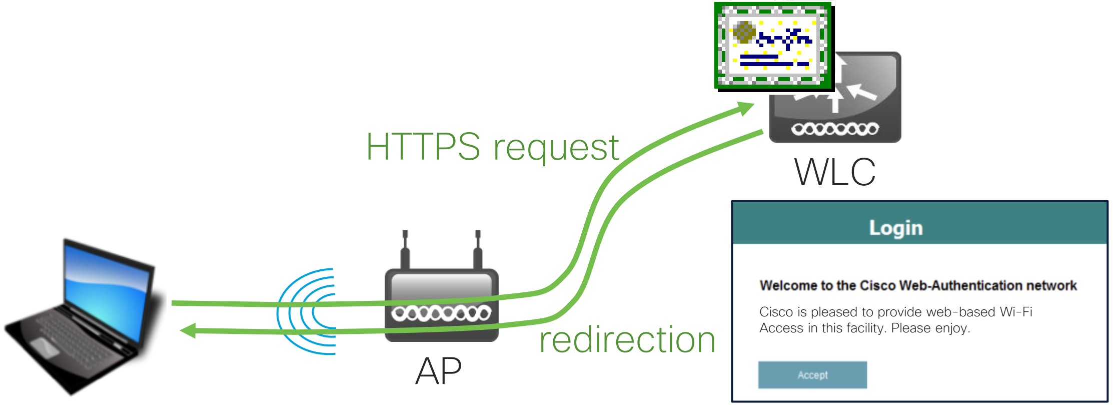


Connection is secure ✕

Your information (for example, passwords or credit card numbers) is private when it is sent to this site.

Learn more

Certificate (Valid)



Login

Welcome to the Cisco Web-Authentication network

Cisco is pleased to provide web-based Wi-Fi Access in this facility. Please enjoy.

Accept

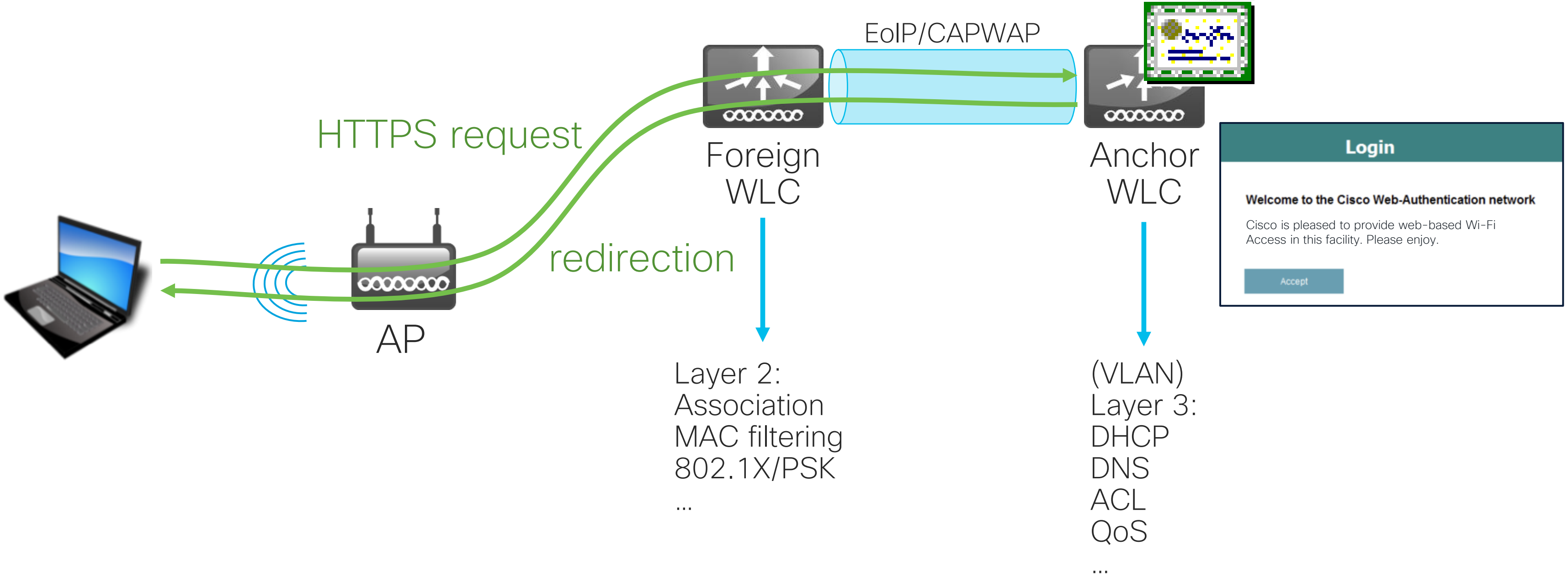
Certificates for the Controller Web Authentication:

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

A certificate signed by a known root CA avoids scary messages



Login

Welcome to the Cisco Web-Authentication network

Cisco is pleased to provide web-based Wi-Fi Access in this facility. Please enjoy.

Accept

Layer 2:
Association
MAC filtering
802.1X/PSK
…

(VLAN)
Layer 3:
DHCP
DNS
ACL
QoS
…

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

LWA configuration: 9800’s internal portal

For your reference

- AAA and method lists
- Pre-webauth ACL
- Web auth parameter map
- WLAN / Policy Profiles

LWA configuration: 9800's internal portal

AAA and method lists

For your reference

```
aaa new-model
!
aaa authentication login MLIST_AUTHC_LOGIN_LOCAL local
!
aaa authorization network default local
```

For local accounts

Alternatively, we could use an external RADIUS server too

```
radius server RADIUS_SRVR_ISE
 address ipv4 <RADIUS_IP> auth-port 1812 acct-port 1813
 key <SHARED_SECRET>
!
aaa group server radius RADIUS_SRVR_GRP_01
 server name RADIUS_SRVR_ISE
!
aaa authentication login MLIST_AUTHC_LOGIN_ISE group RADIUS_SRVR_GRP_01
aaa accounting identity MLIST_ACCT_ID_ISE start-stop group RADIUS_SRVR_GRP_01
```

LWA configuration: 9800’s internal portal

Pre-webauth ACL

For your reference

```
ip access-list extended ACL_LWA_REDIRECT
 permit udp any any eq bootps
 permit udp any eq bootps any
 permit udp any any eq domain
 permit udp any eq domain any
 permit tcp any host <SRVR_IP> eq 443
 permit tcp host <SRVR_IP> eq 443 any
 deny ip any any
```

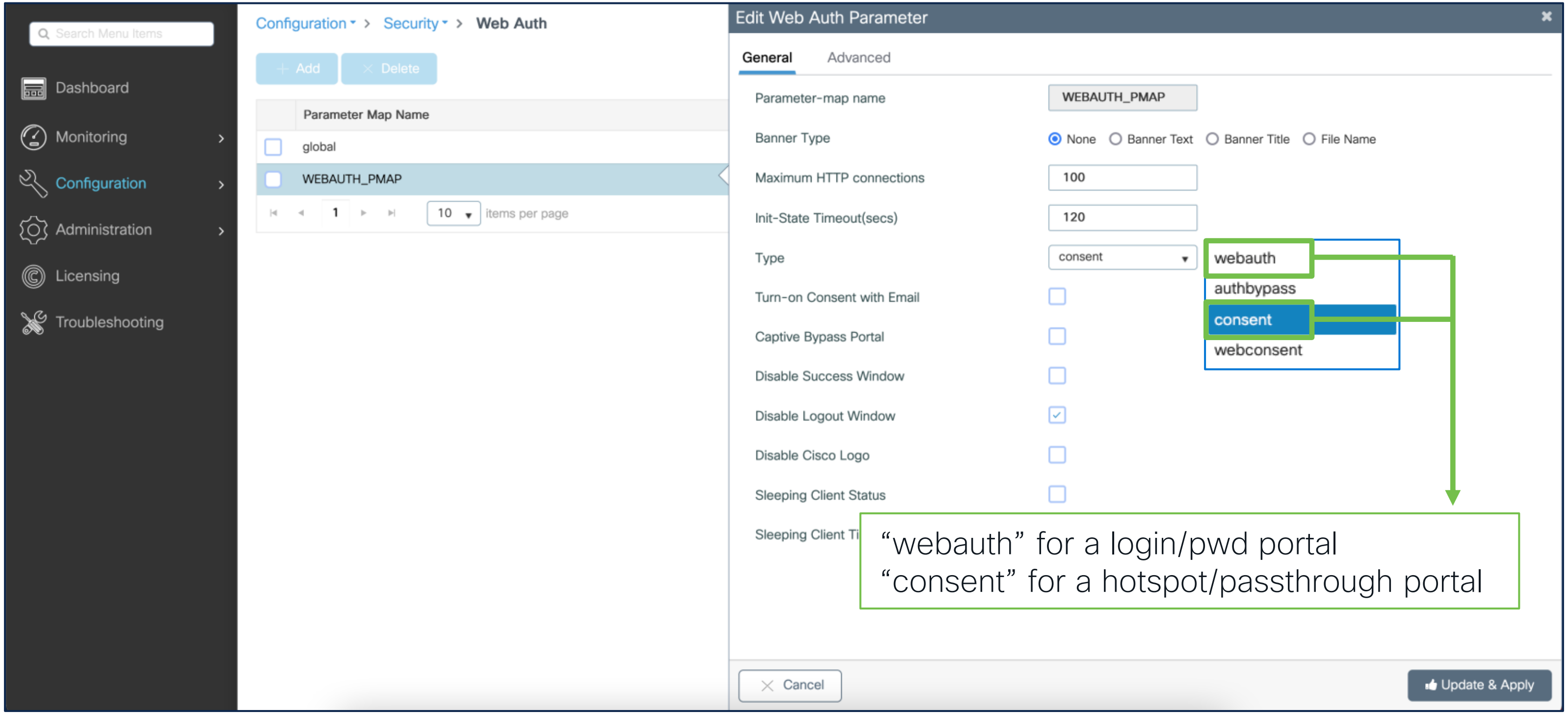
Anything permitted is permitted.
(for HTTP/S) Anything denied is redirected.

<SRVR_IP> in this example could be an internal HTTPS application we’d need to access even before authenticating to the guest portal. This could be readapted to other examples as needed.

LWA configuration: 9800’s internal portal

Web auth parameter map

For your reference



	Parameter Map Name
□	global
□	WEBAUTH_PMAP

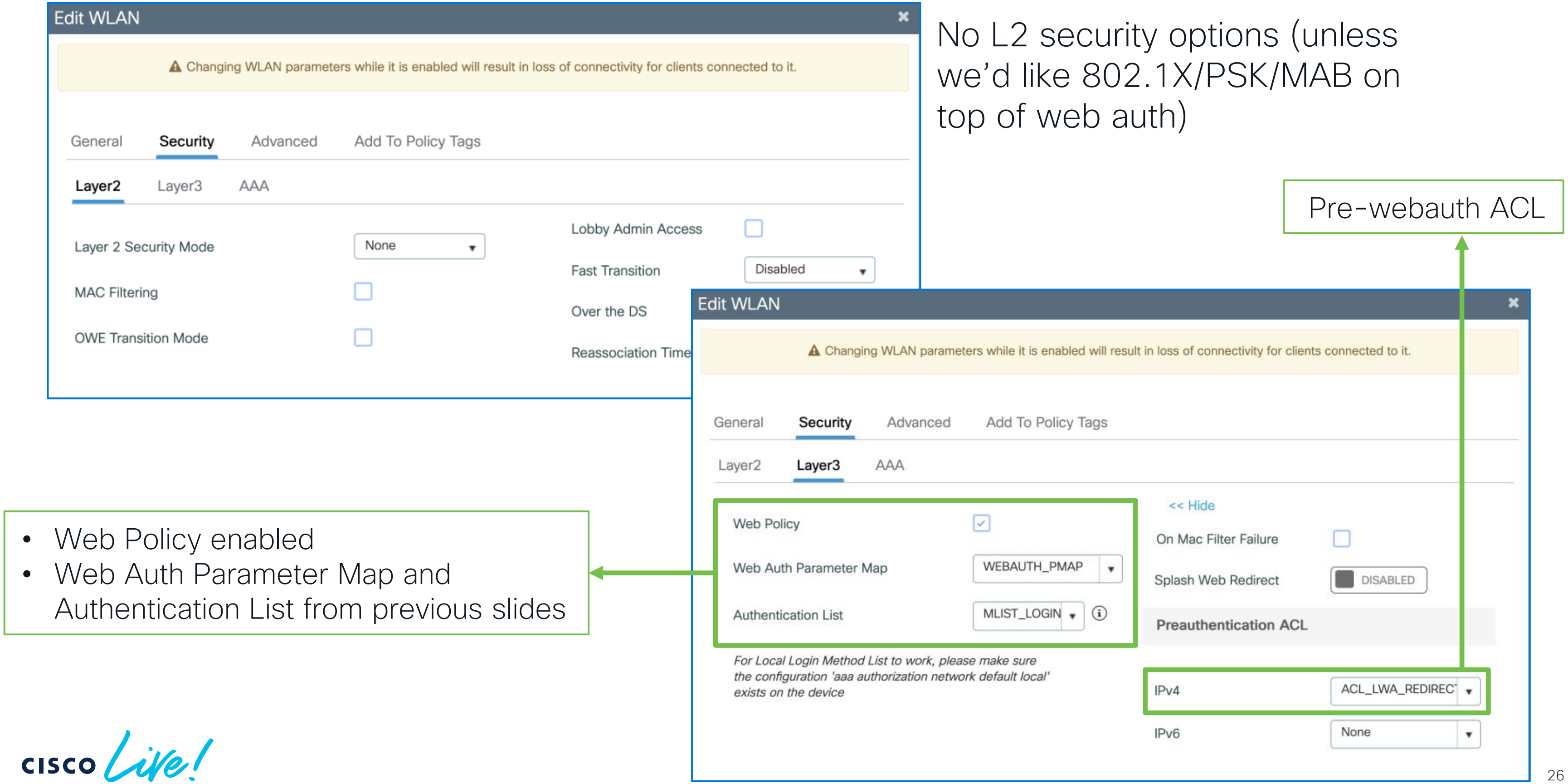
Parameter-map name	WEBAUTH_PMAP
Banner Type	● None ○ Banner Text ○ Banner Title ○ File Name
Maximum HTTP connections	100
Init-State Timeout(secs)	120
Type	consent
Turn-on Consent with Email	□
Captive Bypass Portal	□
Disable Success Window	□
Disable Logout Window	☑
Disable Cisco Logo	□
Sleeping Client Status	□
Sleeping Client Ti	

“webauth” for a login/pwd portal
“consent” for a hotspot/passthrough portal

LWA configuration: 9800’s internal portal

WLAN / Policy Profiles

For your reference



Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

Layer 2 Security Mode: None ▾

MAC Filtering: □

OWE Transition Mode: □

Lobby Admin Access: □

Fast Transition: Disabled ▾

Over the DS

Reassociation Time

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

Web Policy: ☑

Web Auth Parameter Map: WEBAUTH_PMAP ▾

Authentication List: MLIST_LOGIN ▾ ⓘ

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_REDIRECT ▾

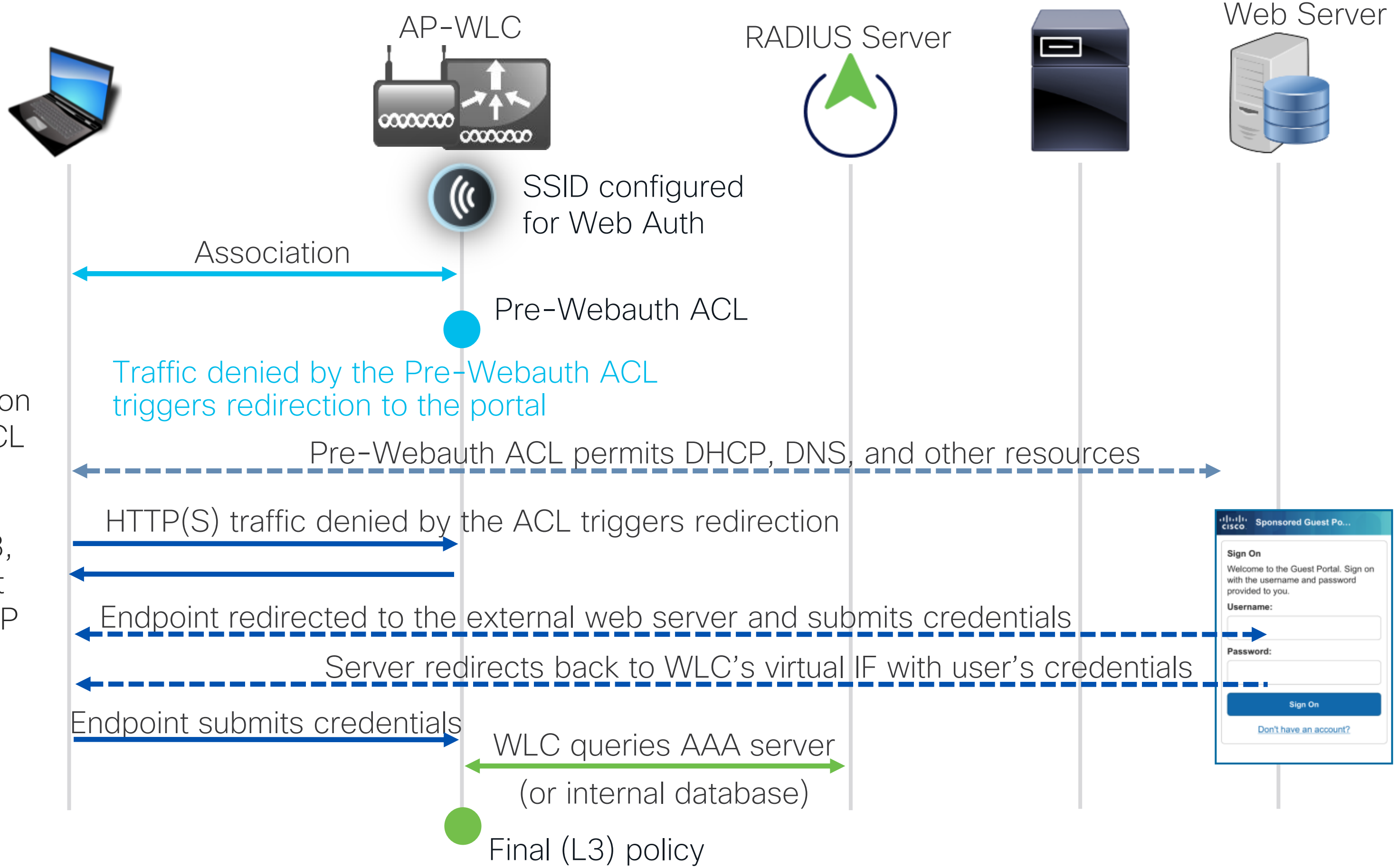
IPv6: None ▾

No L2 security options (unless we’d like 802.1X/PSK/MAB on top of web auth)

Pre-webauth ACL

- Web Policy enabled
- Web Auth Parameter Map and Authentication List from previous slides

LWA login with an ext. web server


External Resources
(DHCP, DNS, etc.)
External
Web Server
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
Endpoint redirected to the external web server and submits credentials
Server redirects back to WLC's virtual IF with user's credentials
Endpoint submits credentials
WLC queries AAA server
(or internal database)
Final (L3) policy

Sponsored Guest Po...

Sign On

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

Username:

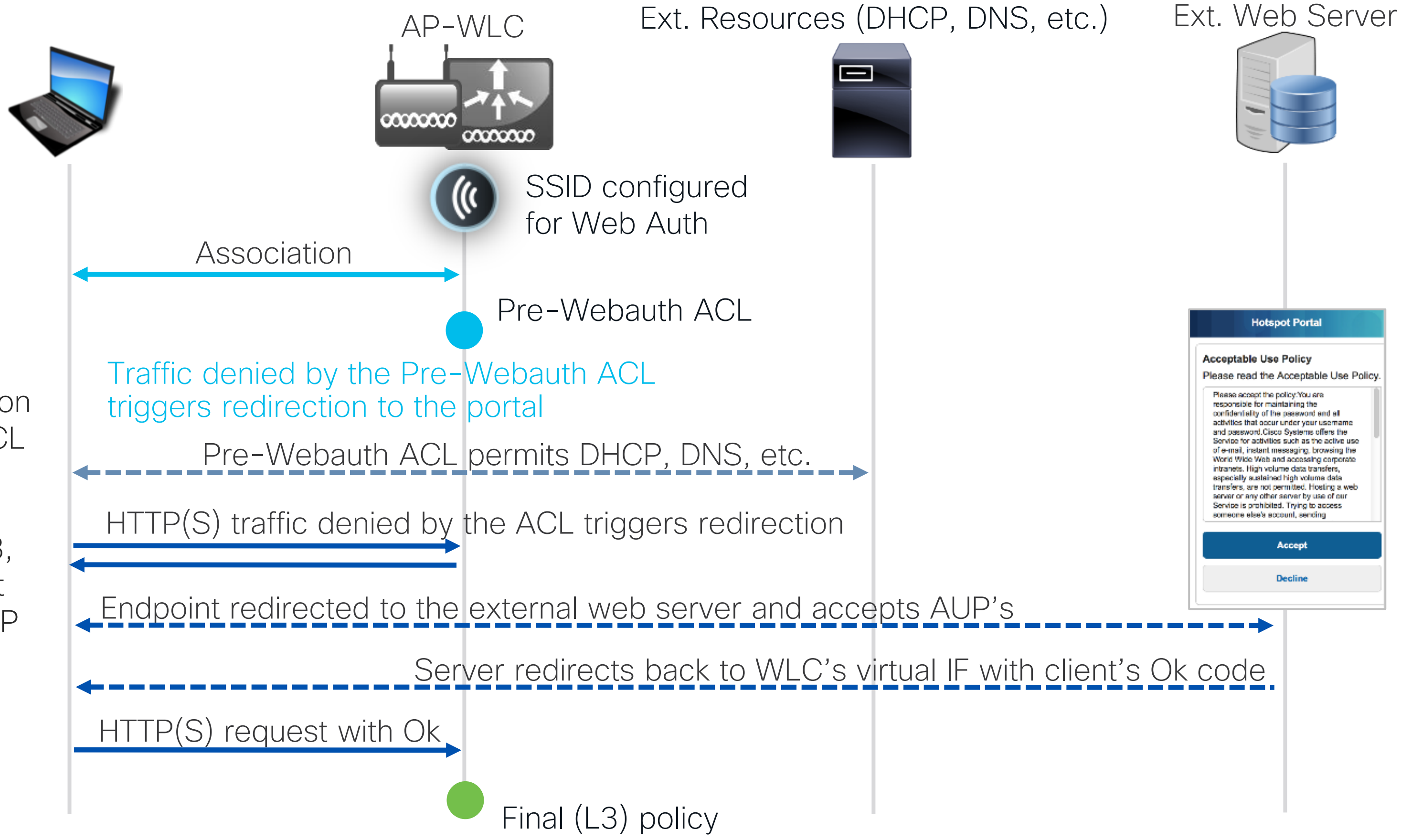
Password:

Sign On

Don't have an account?

LOCAL because the redirection URL and the pre-webauth ACL are **locally** configured on the WLC.
We say that LWA is purely L3, because it starts from a client trying to resolve a (server's) IP address.

LWA passthrough with an ext. web server


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
Endpoint redirected to the external web server and accepts AUP's
Server redirects back to WLC's virtual IF with client's Ok code
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

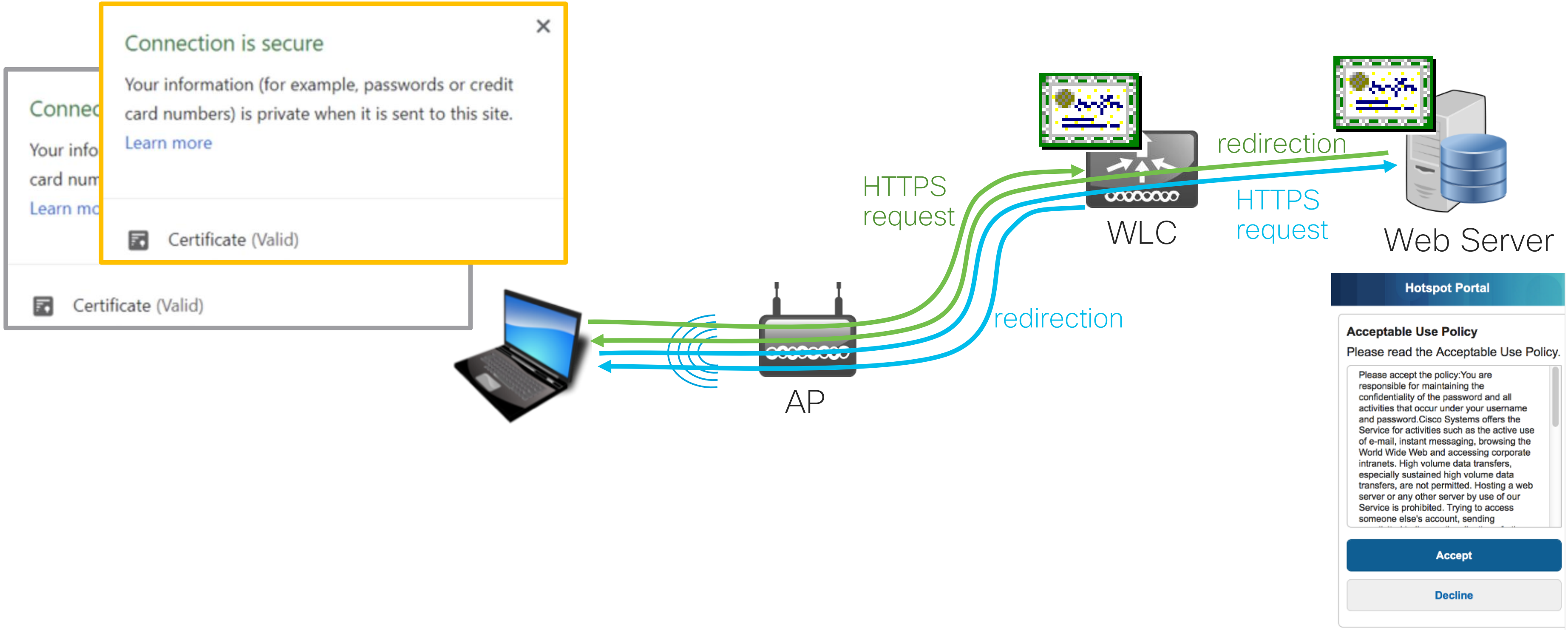
Accept

Decline

LOCAL because the redirection URL and the pre-webauth ACL are locally configured on the WLC.
We say that LWA is purely L3, because it starts from a client trying to resolve a (server's) IP address.

LWA and certificates

External web server



Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Certificate (Valid)

Connec
Your info
card num
Learn mo
Certificate (Valid)

Hotspot Portal

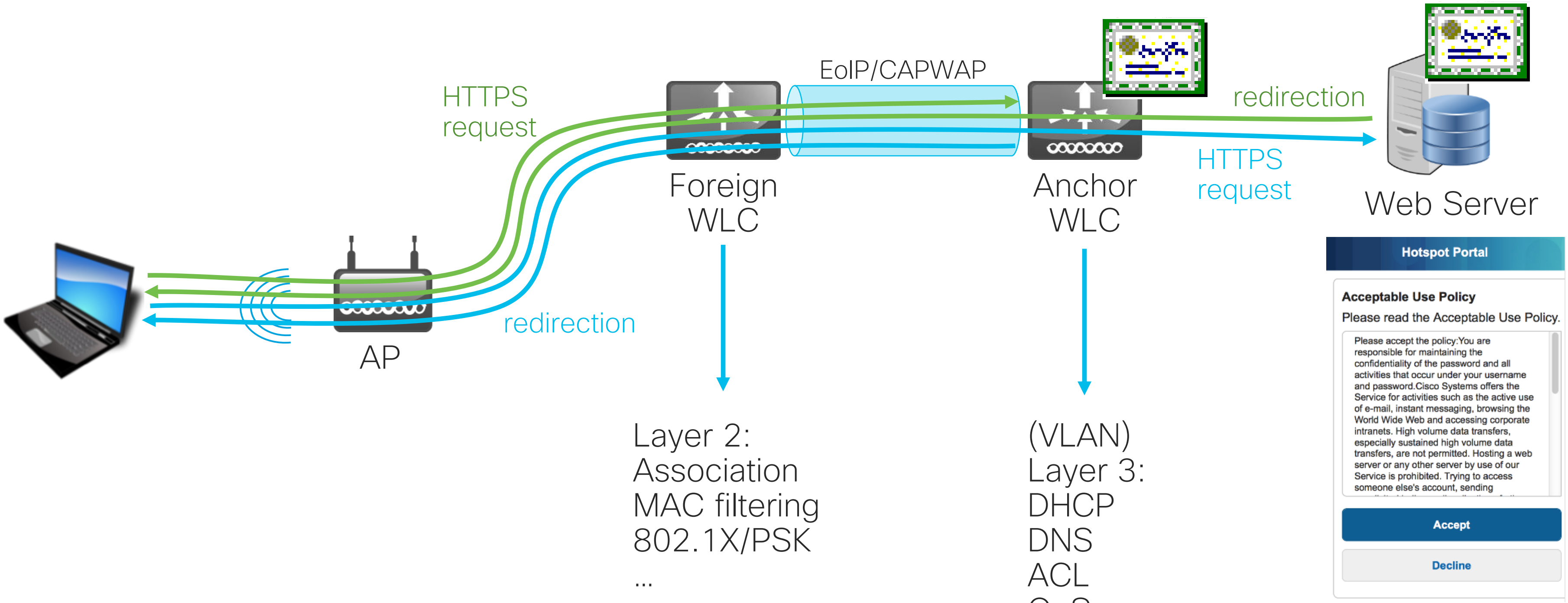
Acceptable Use Policy

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

LWA with an anchor controller

External web server



Layer 2:
Association
MAC filtering
802.1X/PSK
…

(VLAN)
Layer 3:
DHCP
DNS
ACL
QoS
…

Hotspot Portal

Acceptable Use Policy

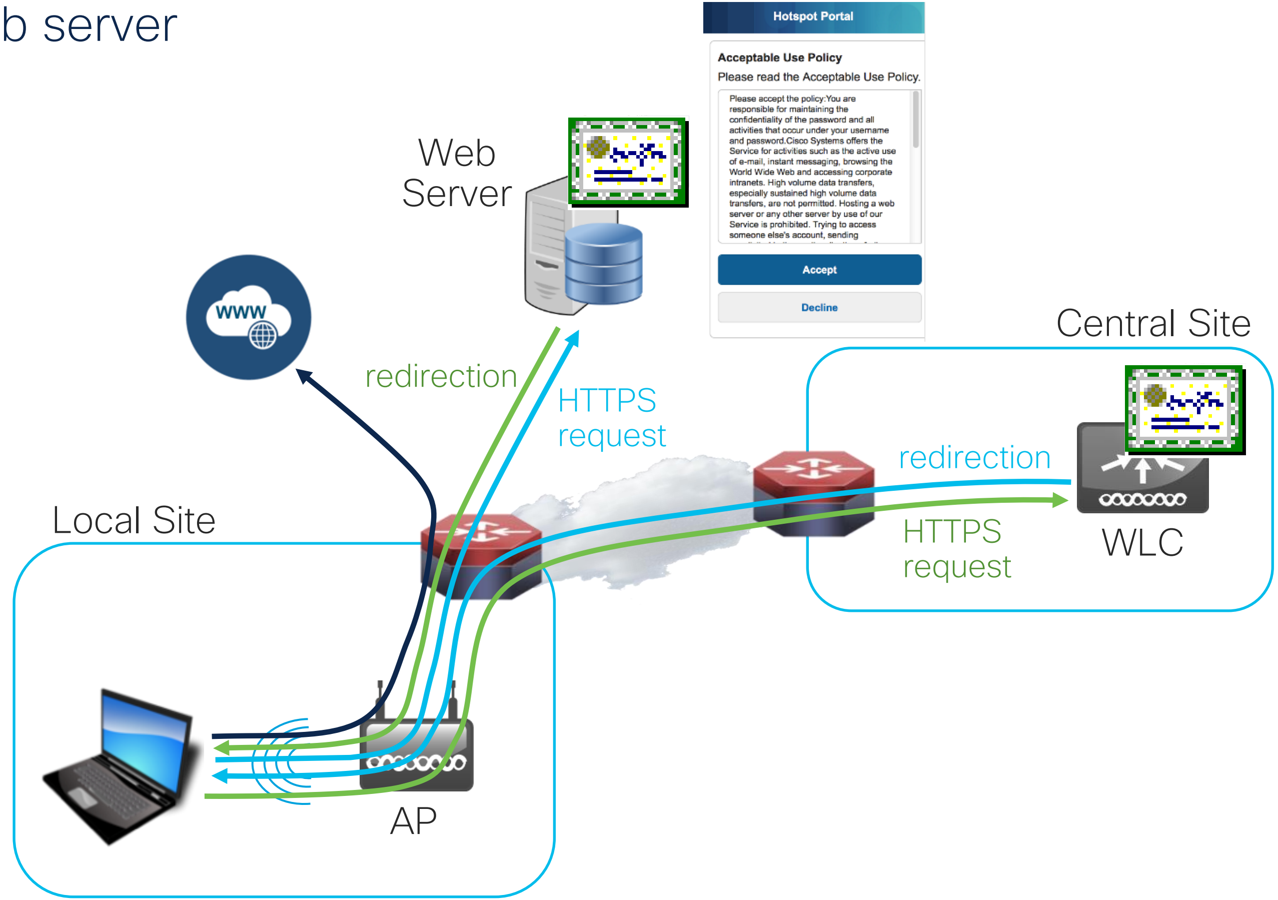
Please read the Acceptable Use Policy.

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

LWA with FlexConnect

External web server

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

LWA configuration: ext. web server

For your reference

- AAA and method lists
- Pre-webauth ACL
- Web auth parameter map
- WLAN / Policy Profiles

LWA configuration: ext. web server

AAA and method lists

```
aaa new-model
!
aaa authentication login MLIST_AUTHC_LOGIN_LOCAL local
!
aaa authorization network default local
```

For local accounts

Alternatively, we could use an external RADIUS server too

```
radius server RADIUS_SRVR_ISE
 address ipv4 <RADIUS_IP> auth-port 1812 acct-port 1813
 key <SHARED_SECRET>
!
aaa group server radius RADIUS_SRVR_GRP_01
 server name RADIUS_SRVR_ISE
!
aaa authentication login MLIST_AUTHC_LOGIN_ISE group RADIUS_SRVR_GRP_01
aaa accounting identity MLIST_ACCT_ID_ISE start-stop group RADIUS_SRVR_GRP_01
```

LWA configuration: ext. web server

AAA and method lists

For your reference

If our portal is a passthrough/consent/hotspot one, like with Cisco Spaces, we can just “relax”.
No local database or external RADIUS servers are needed, because there is no guest account to authenticate (authC/authZ method lists should still be configured).

LWA configuration: ext. web server

Pre-webauth ACL

For your reference

```
ip access-list extended ACL_LWA_REDIRECT
 permit udp any any eq bootps
 permit udp any eq bootps any
 permit udp any any eq domain
 permit udp any eq domain any
 permit tcp any host <WEB_SRVR_IP> eq <WEB_SRVR_PORT>
 permit tcp host <WEB_SRVR_IP> eq <WEB_SRVR_PORT> any
 deny ip any any
```

Example with DNA Spaces public IPs (ymmv):

```
ip access-list extended ACL_LWA_REDIRECT
 permit udp any any eq bootps
 permit udp any eq bootps any
 permit udp any any eq domain
 permit udp any eq domain any
 permit tcp any host 34.235.248.212 eq 443
 permit tcp host 34.235.248.212 eq 443 any
 permit tcp any host 52.55.235.39 eq 443
 permit tcp host 52.55.235.39 eq 443 any
 deny ip any any
```

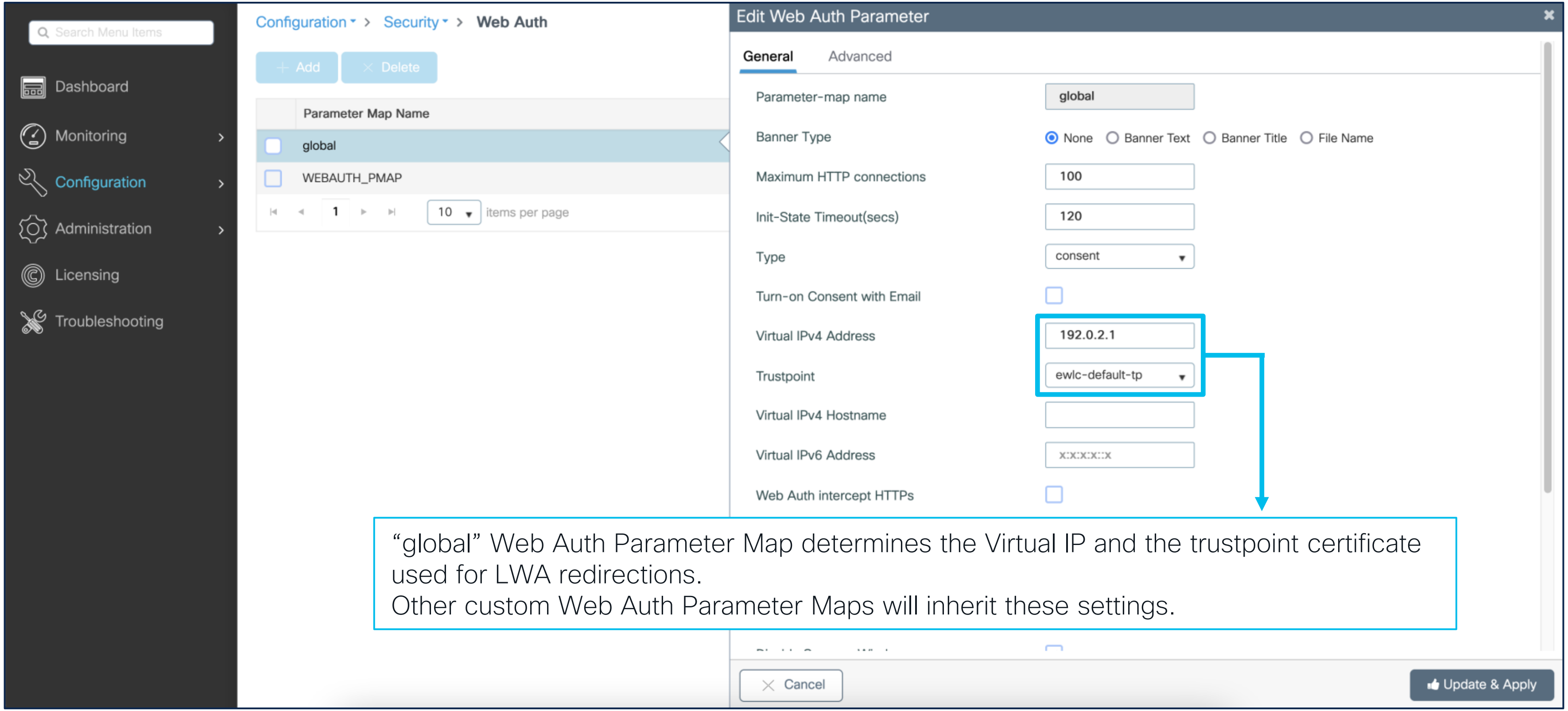
Anything permitted is permitted.
(for HTTP/S) Anything denied is redirected.

<WEB_SRVR_IP> and <WEB_SRVR_PORT> are the IP/port of the external web server, to allow access to its guest portal even before web authentication.

LWA configuration: ext. web server

Web auth parameter map

For your reference



Parameter Map Name
global
WEBAUTH_PMAP

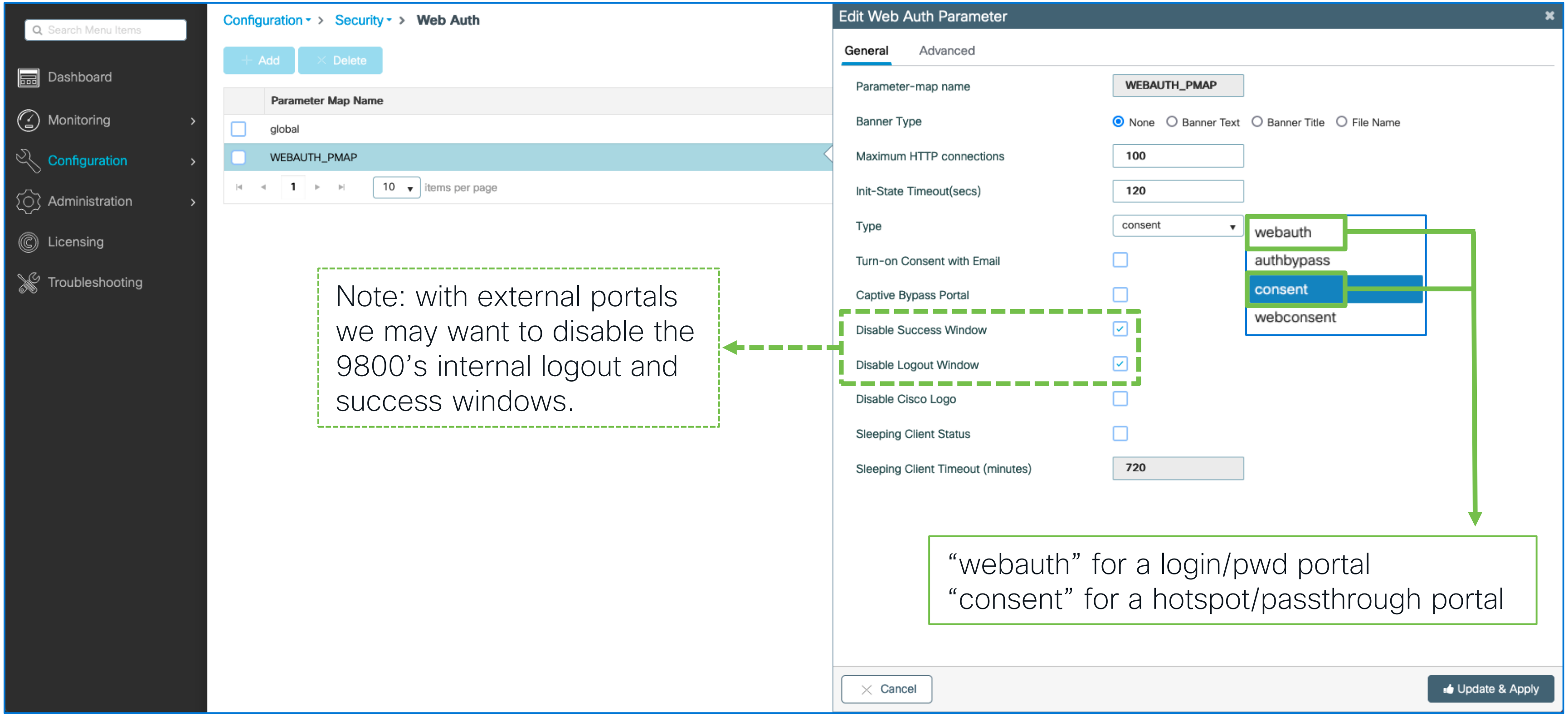
Parameter-map name	global
Banner Type	● None ○ Banner Text ○ Banner Title ○ File Name
Maximum HTTP connections	100
Init-State Timeout(secs)	120
Type	consent
Turn-on Consent with Email	□
Virtual IPv4 Address	192.0.2.1
Trustpoint	ewlc-default-tp
Virtual IPv4 Hostname	
Virtual IPv6 Address	X:X:X:X::X
Web Auth intercept HTTPs	□

"global" Web Auth Parameter Map determines the Virtual IP and the trustpoint certificate used for LWA redirections.
Other custom Web Auth Parameter Maps will inherit these settings.

LWA configuration: ext. web server

Web auth parameter map

For your reference



	Parameter Map Name
□	global
□	WEBAUTH_PMAP

Edit Web Auth Parameter

General | Advanced

Parameter-map name	WEBAUTH_PMAP
Banner Type	● None ○ Banner Text ○ Banner Title ○ File Name
Maximum HTTP connections	100
Init-State Timeout(secs)	120
Type	consent (webauth / authbypass / consent / webconsent)
Turn-on Consent with Email	□
Captive Bypass Portal	□
Disable Success Window	☑
Disable Logout Window	☑
Disable Cisco Logo	□
Sleeping Client Status	□
Sleeping Client Timeout (minutes)	720

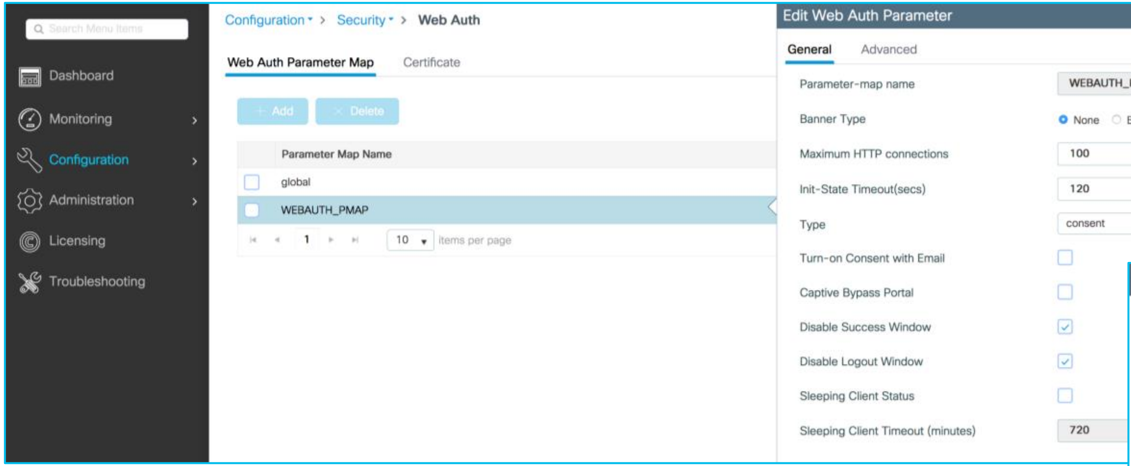
Note: with external portals we may want to disable the 9800’s internal logout and success windows.

“webauth” for a login/pwd portal
“consent” for a hotspot/passthrough portal

LWA configuration: ext. web server

Web auth parameter map for DNA Spaces

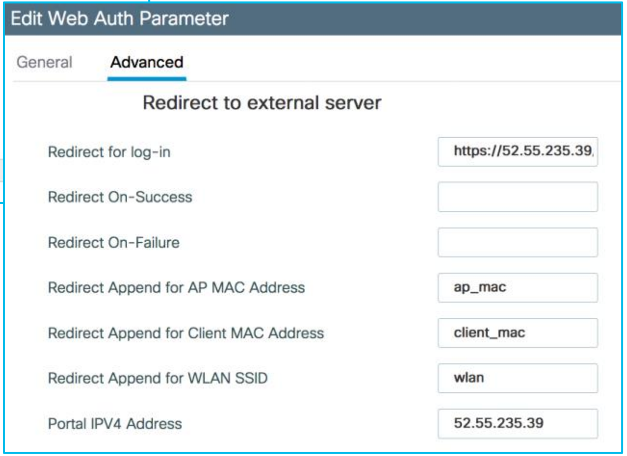
For your reference



Edit Web Auth Parameter

General | Advanced

Parameter-map name	WEBAUTH_PMAP
Banner Type	● None ○ 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 (minutes)	720



Edit Web Auth Parameter

General | Advanced

Redirect to external server

Redirect for log-in	https://52.55.235.39,
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	52.55.235.39

Change the Web Auth Parameter Map's "Type" to "consent"

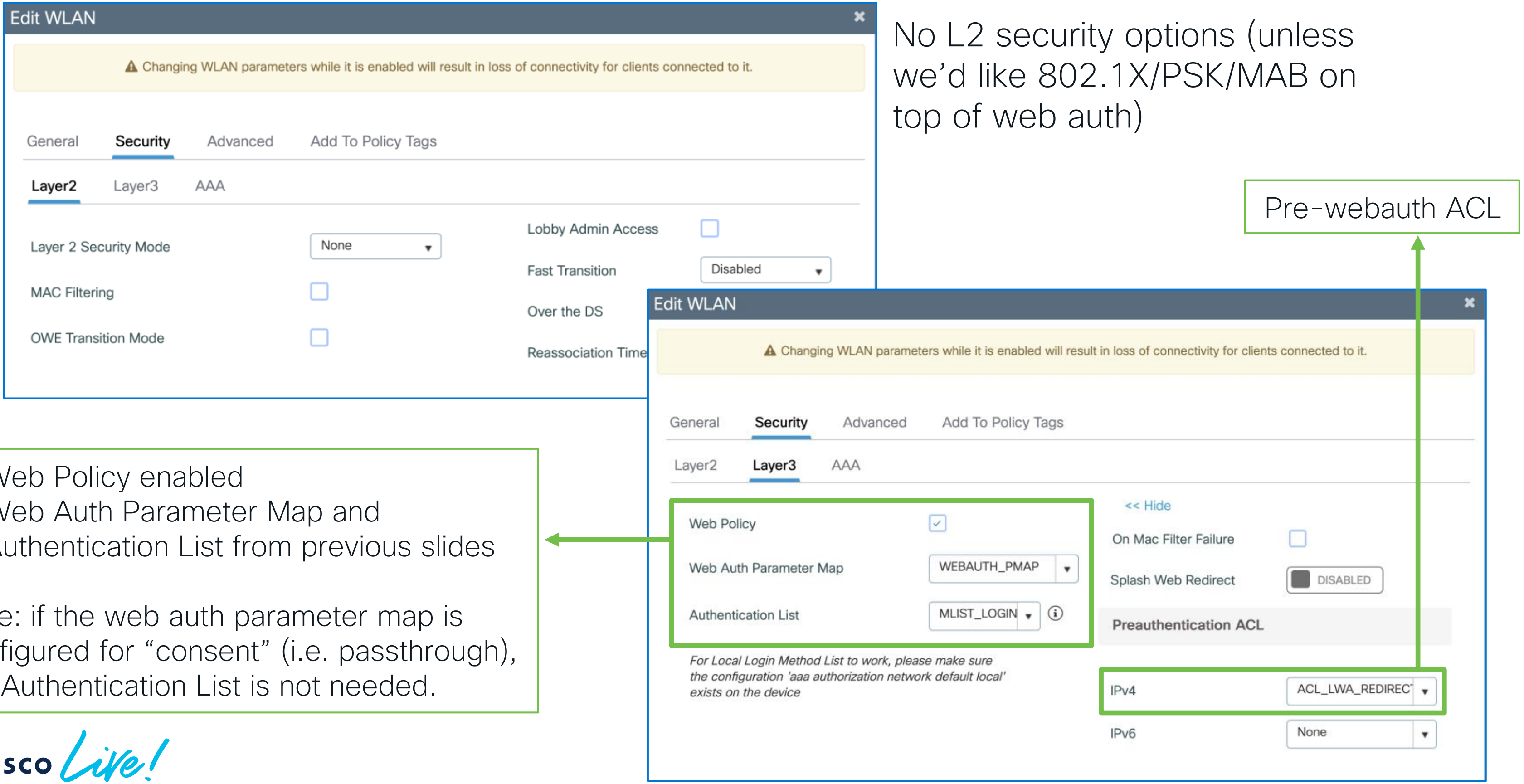
Modify the Advanced parameters with:

- Redirect for log-in = https://<DNA_SPACES_IP>/<PATH>
- 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 = <DNA_SPACES_IP>

LWA configuration: ext. web server

WLAN / Policy Profiles

For your reference



Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General | **Security** | Advanced | Add To Policy Tags

Layer2 | Layer3 | AAA

Layer 2 Security Mode: None ▾

MAC Filtering □

OWE Transition Mode □

Lobby Admin Access □

Fast Transition: Disabled ▾

Over the DS

Reassociation Time

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General | **Security** | Advanced | Add To Policy Tags

Layer2 | **Layer3** | AAA

Web Policy ☑

Web Auth Parameter Map: WEBAUTH_PMAP ▾

Authentication List: MLIST_LOGIN ▾ ⓘ

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

<< Hide

On Mac Filter Failure □

Splash Web Redirect: DISABLED

Preauthentication ACL

IPv4: ACL_LWA_REDIRECT ▾

IPv6: None ▾

No L2 security options (unless we'd like 802.1X/PSK/MAB on top of web auth)

Pre-webauth ACL

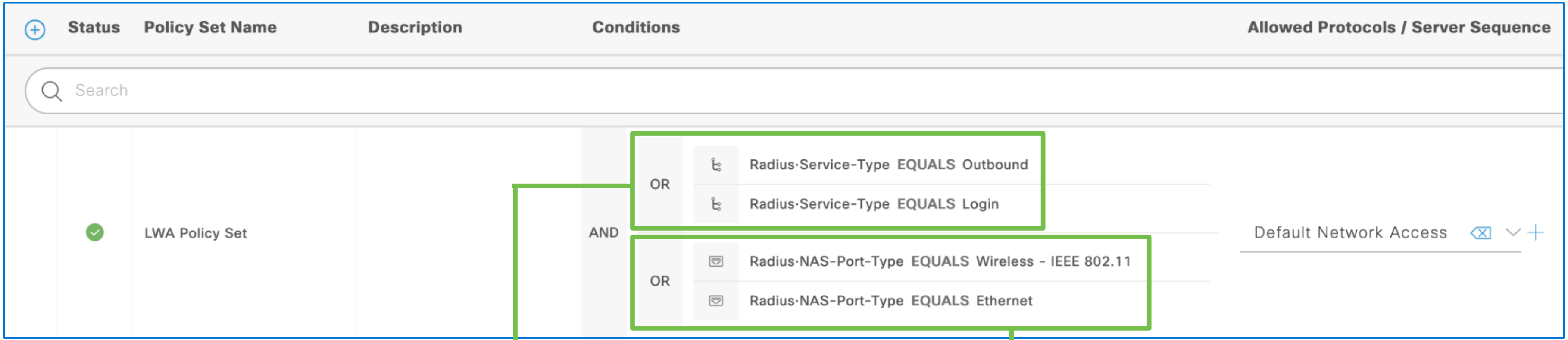
- Web Policy enabled
- Web Auth Parameter Map and Authentication List from previous slides

Note: if the web auth parameter map is configured for "consent" (i.e. passthrough), the Authentication List is not needed.

LWA configuration: ext. web server

ISE as the RADIUS authentication server: Policy Set

For your reference



Status	Policy Set Name	Description	Conditions		Allowed Protocols / Server Sequence
✓	LWA Policy Set		AND	OR Radius·Service-Type EQUALS Outbound Radius·Service-Type EQUALS Login	Default Network Access
				OR Radius·NAS-Port-Type EQUALS Wireless - IEEE 802.11 Radius·NAS-Port-Type EQUALS Ethernet	

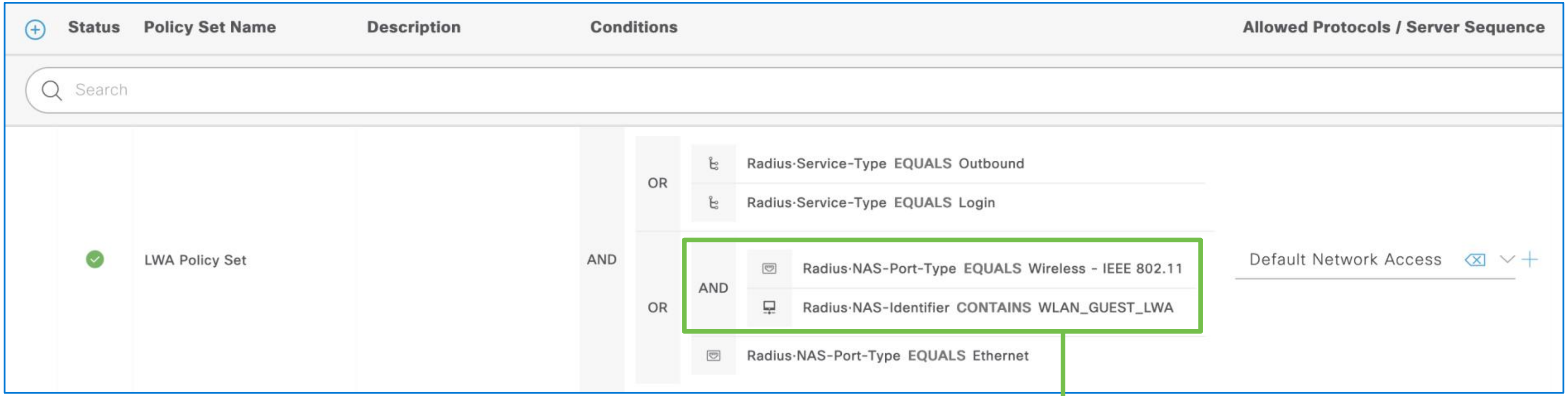
Some NADs (e.g., C9k switches and controllers) use Outbound, some others (e.g., other Catalyst switches and AireOS WLCs) use Login

Wireless NADs use Wireless – IEEE 802.11, wired NADs use Ethernet

LWA configuration: ext. web server

ISE as the RADIUS authentication server: Policy Set (alternative)

For your reference



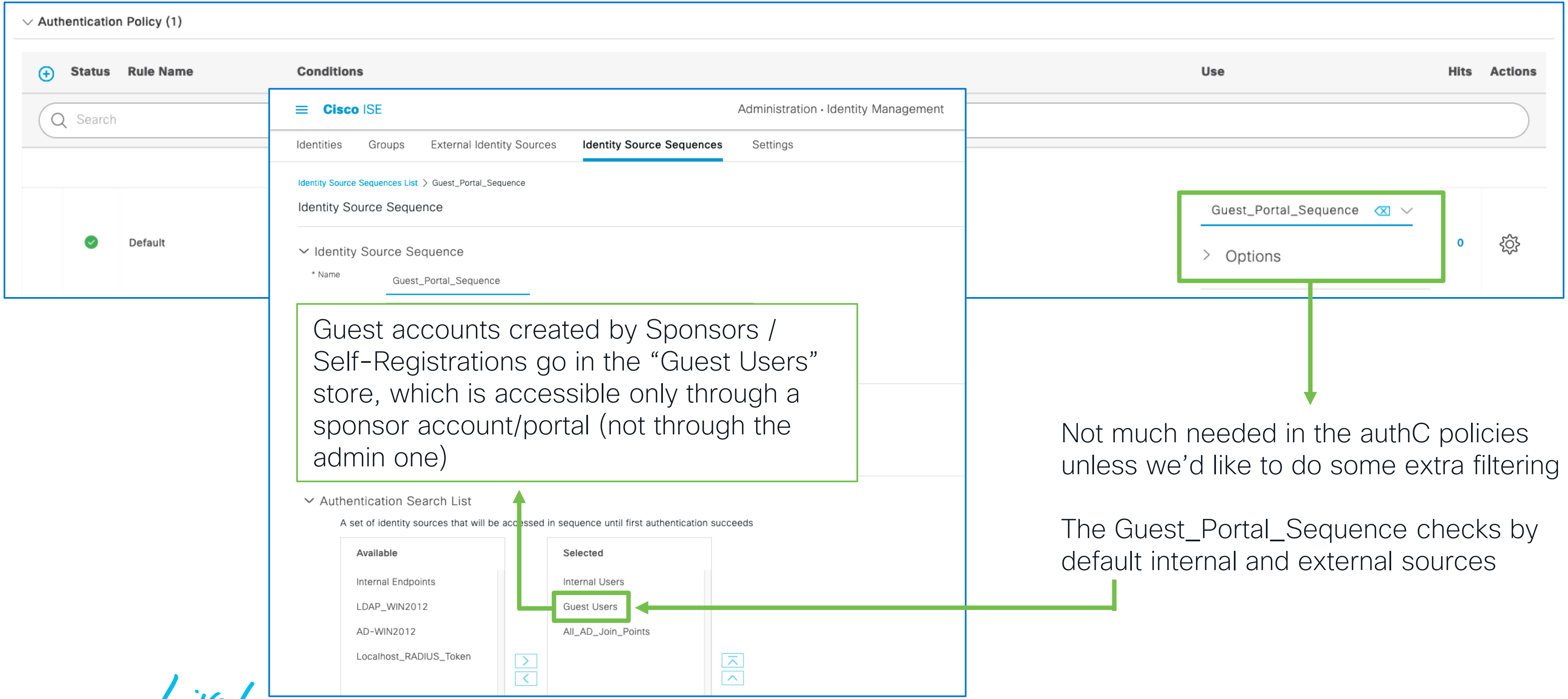
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
✓	LWA Policy Set		AND OR: Radius·Service-Type EQUALS Outbound; Radius·Service-Type EQUALS Login OR: (AND: Radius·NAS-Port-Type EQUALS Wireless - IEEE 802.11; Radius·NAS-Identifier CONTAINS WLAN_GUEST_LWA); Radius·NAS-Port-Type EQUALS Ethernet	Default Network Access

On top of “NAS-Port-Type = Wireless – IEEE 802.11”, we could additionally filter for a specific SSID with the RADIUS attribute [32] NAS-Identifier (more on this in later slides)

LWA configuration: ext. web server

For your reference

ISE as the RADIUS authentication server: authentication policies



Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		Guest_Portal_Sequence Options	0	

Cisco ISE — Administration · Identity Management

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

Identity Source Sequences List > Guest_Portal_Sequence

Identity Source Sequence

Identity Source Sequence

* Name: Guest_Portal_Sequence

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints	Internal Users
LDAP_WIN2012	Guest Users
AD-WIN2012	All_AD_Join_Points
Localhost_RADIUS_Token	

Guest accounts created by Sponsors / Self-Registrations go in the "Guest Users" store, which is accessible only through a sponsor account/portal (not through the admin one)

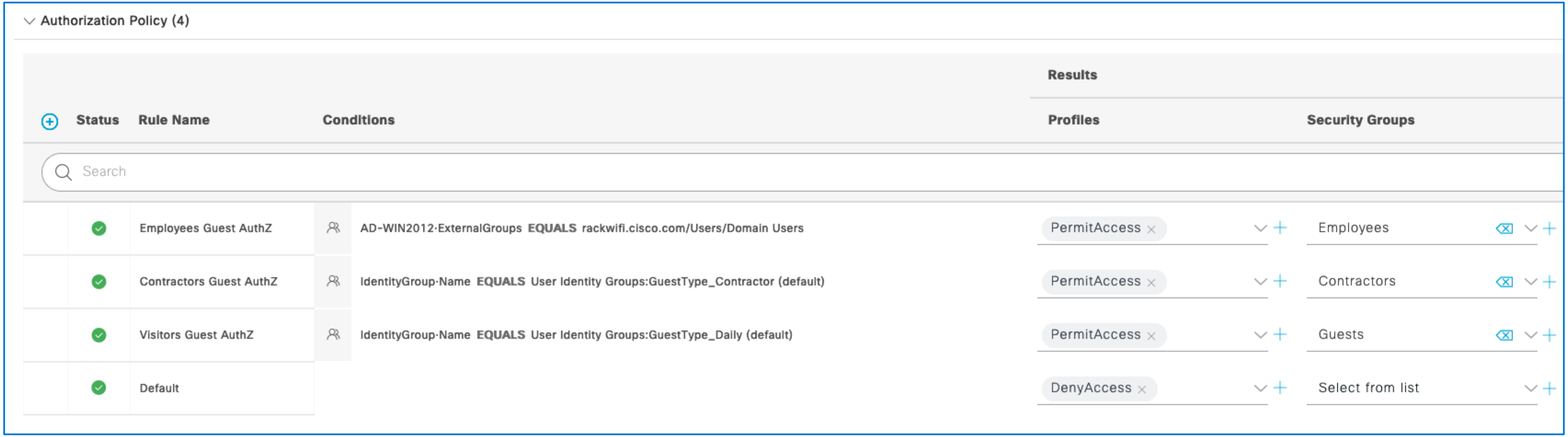
Not much needed in the authC policies unless we'd like to do some extra filtering

The Guest_Portal_Sequence checks by default internal and external sources

LWA configuration: ext. web server

ISE as the RADIUS authentication server: authorization policies

For your reference

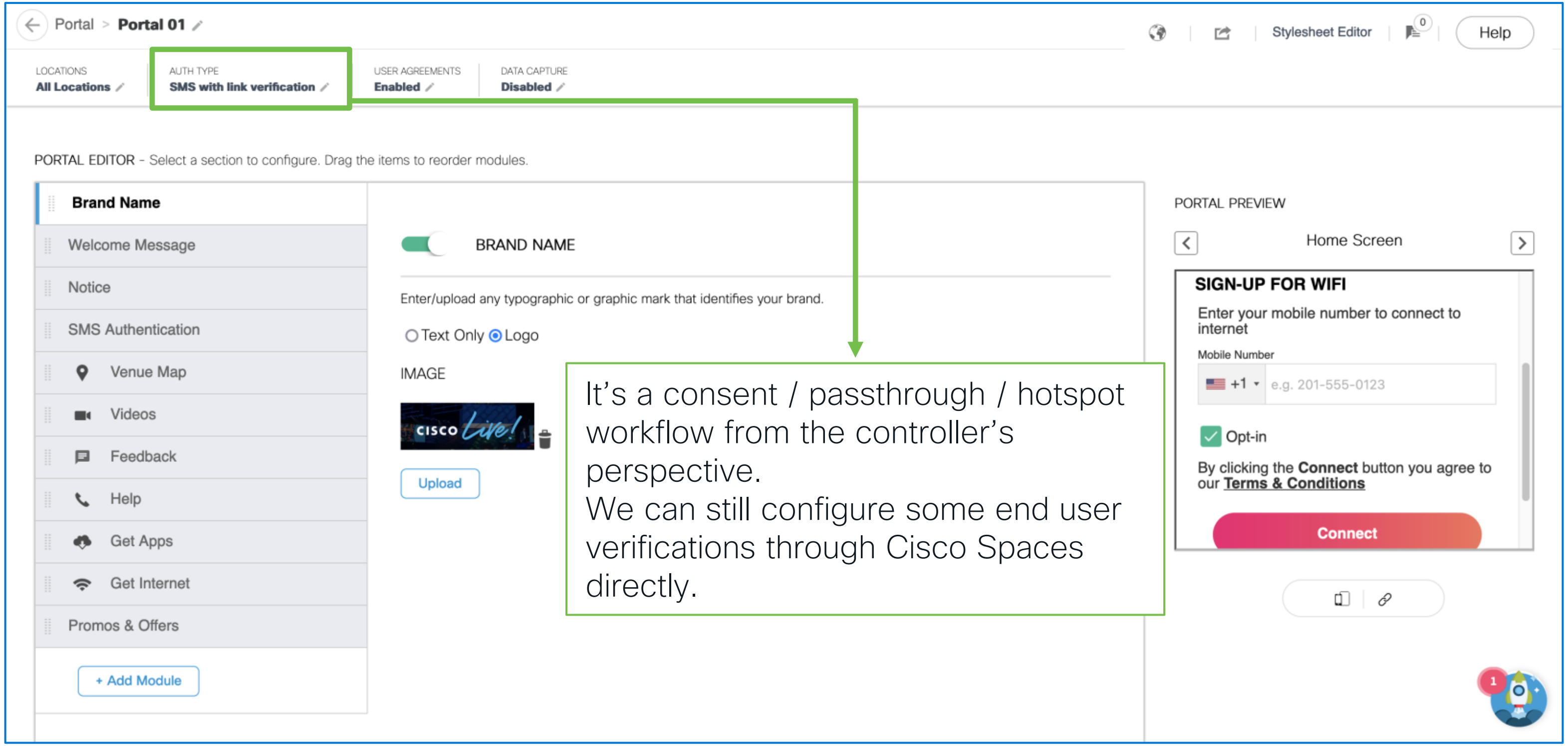


Authorization Policy (4)

				Results	
	Status	Rule Name	Conditions	Profiles	Security Groups
	✓	Employees Guest AuthZ	AD-WIN2012·ExternalGroups **EQUALS** rackwifi.cisco.com/Users/Domain Users	PermitAccess	Employees
	✓	Contractors Guest AuthZ	IdentityGroup·Name **EQUALS** User Identity Groups:GuestType_Contractor (default)	PermitAccess	Contractors
	✓	Visitors Guest AuthZ	IdentityGroup·Name **EQUALS** User Identity Groups:GuestType_Daily (default)	PermitAccess	Guests
	✓	Default		DenyAccess	Select from list

In the authZ policies we can configure pretty much whatever best suits the final needs (e.g., AD groups, guest groups, etc.)

Cisco Spaces passthrough portal example



Portal > **Portal 01**

LOCATIONS: **All Locations**

AUTH TYPE: **SMS with link verification**

USER AGREEMENTS: **Enabled**

DATA CAPTURE: **Disabled**

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

BRAND NAME

Enter/upload any typographic or graphic mark that identifies your brand.

○ Text Only ● Logo

IMAGE

PORTAL PREVIEW

Home Screen

SIGN-UP FOR WIFI

Enter your mobile number to connect to internet

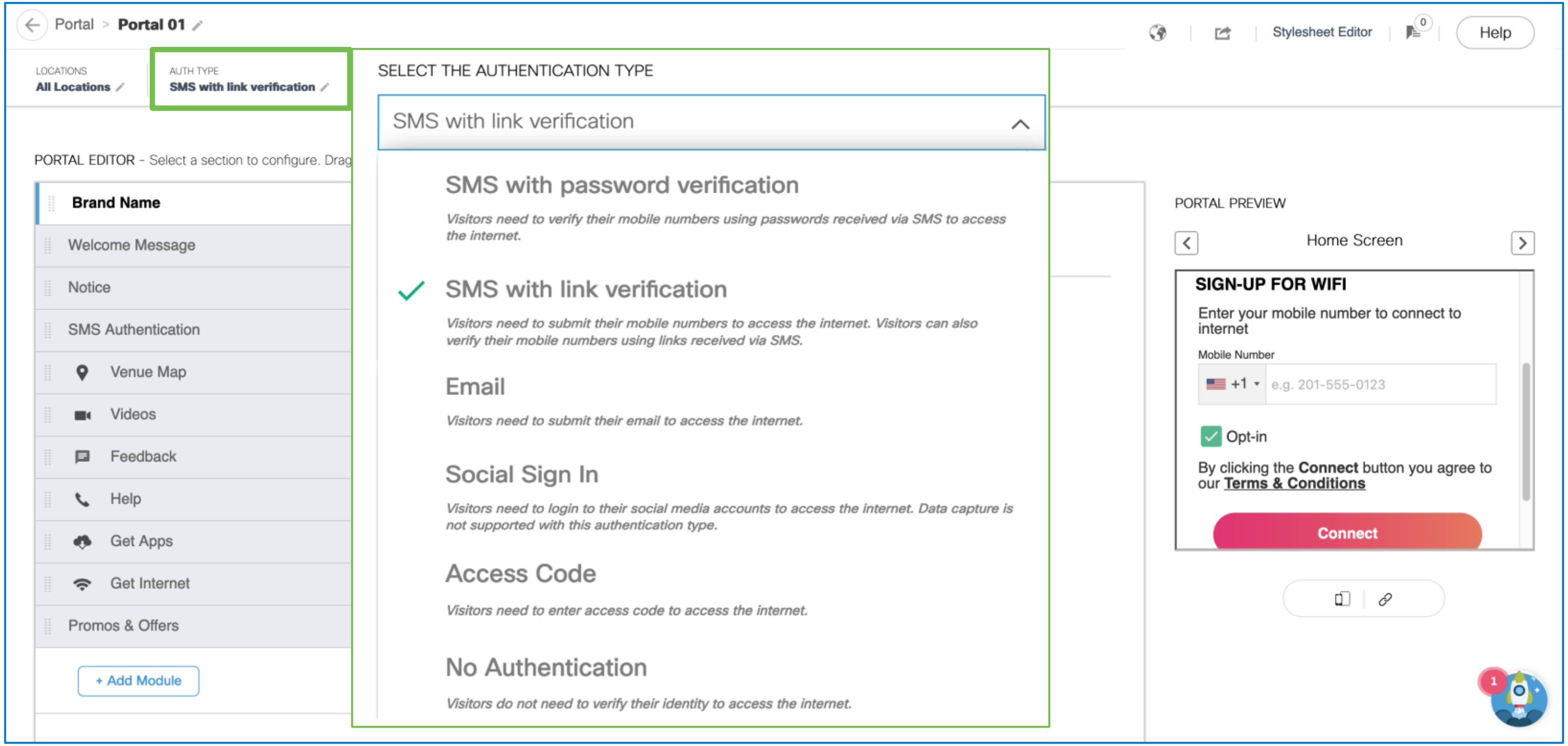
Mobile Number: +1 e.g. 201-555-0123

☑ Opt-in

By clicking the **Connect** button you agree to our **Terms & Conditions**

It's a consent / passthrough / hotspot workflow from the controller's perspective.
We can still configure some end user verifications through Cisco Spaces directly.

Cisco Spaces passthrough portal example



Portal > **Portal 01**

Stylesheet Editor | Help

LOCATIONS
All Locations

AUTH TYPE
SMS with link verification

SELECT THE AUTHENTICATION TYPE

SMS with link verification

SMS with password verification

Visitors need to verify their mobile numbers using passwords received via SMS to access the internet.

✓ 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.

Access Code

Visitors need to enter access code to access the internet.

No Authentication

Visitors do not need to verify their identity to access the internet.

PORTAL EDITOR - Select a section to configure. Drag

- **Brand Name**
- Welcome Message
- Notice
- SMS Authentication
- Venue Map
- Videos
- Feedback
- Help
- Get Apps
- Get Internet
- Promos & Offers

+ Add Module

PORTAL PREVIEW

Home Screen

SIGN-UP FOR WIFI

Enter your mobile number to connect to internet

Mobile Number

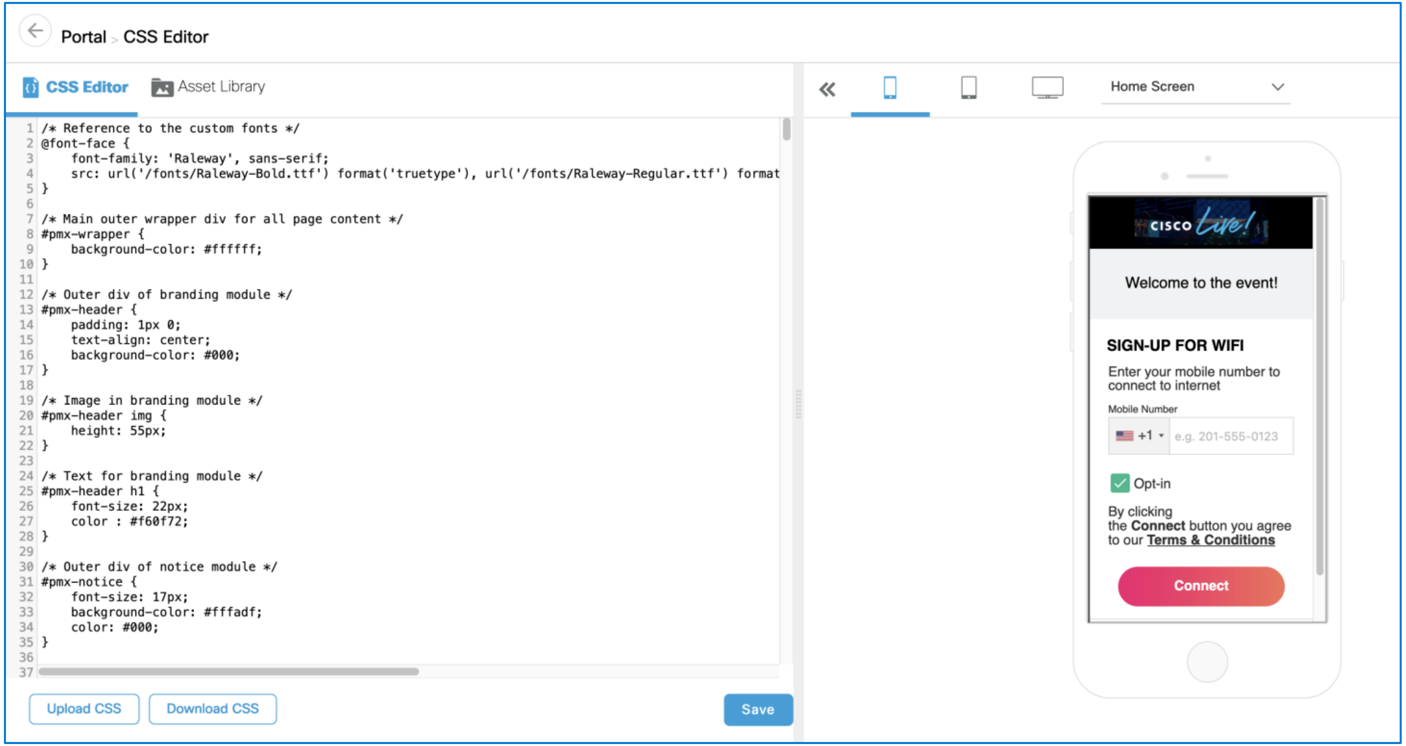
+1 e.g. 201-555-0123

☑ Opt-in

By clicking the **Connect** button you agree to our **Terms & Conditions**

Connect

Cisco Spaces passthrough portal example



```
/* Reference to the custom fonts */
@font-face {
    font-family: 'Raleway', sans-serif;
    src: url('/fonts/Raleway-Bold.ttf') format('truetype'), url('/fonts/Raleway-Regular.ttf') format
}

/* Main outer wrapper div for all page content */
#pmx-wrapper {
    background-color: #ffffff;
}

/* Outer div of branding module */
#pmx-header {
    padding: 1px 0;
    text-align: center;
    background-color: #000;
}

/* Image in branding module */
#pmx-header img {
    height: 55px;
}

/* Text for branding module */
#pmx-header h1 {
    font-size: 22px;
    color : #f60f72;
}

/* Outer div of notice module */
#pmx-notice {
    font-size: 17px;
    background-color: #fffadf;
    color: #000;
}

```

Welcome to the event!

SIGN-UP FOR WIFI

Enter your mobile number to connect to internet

Mobile Number

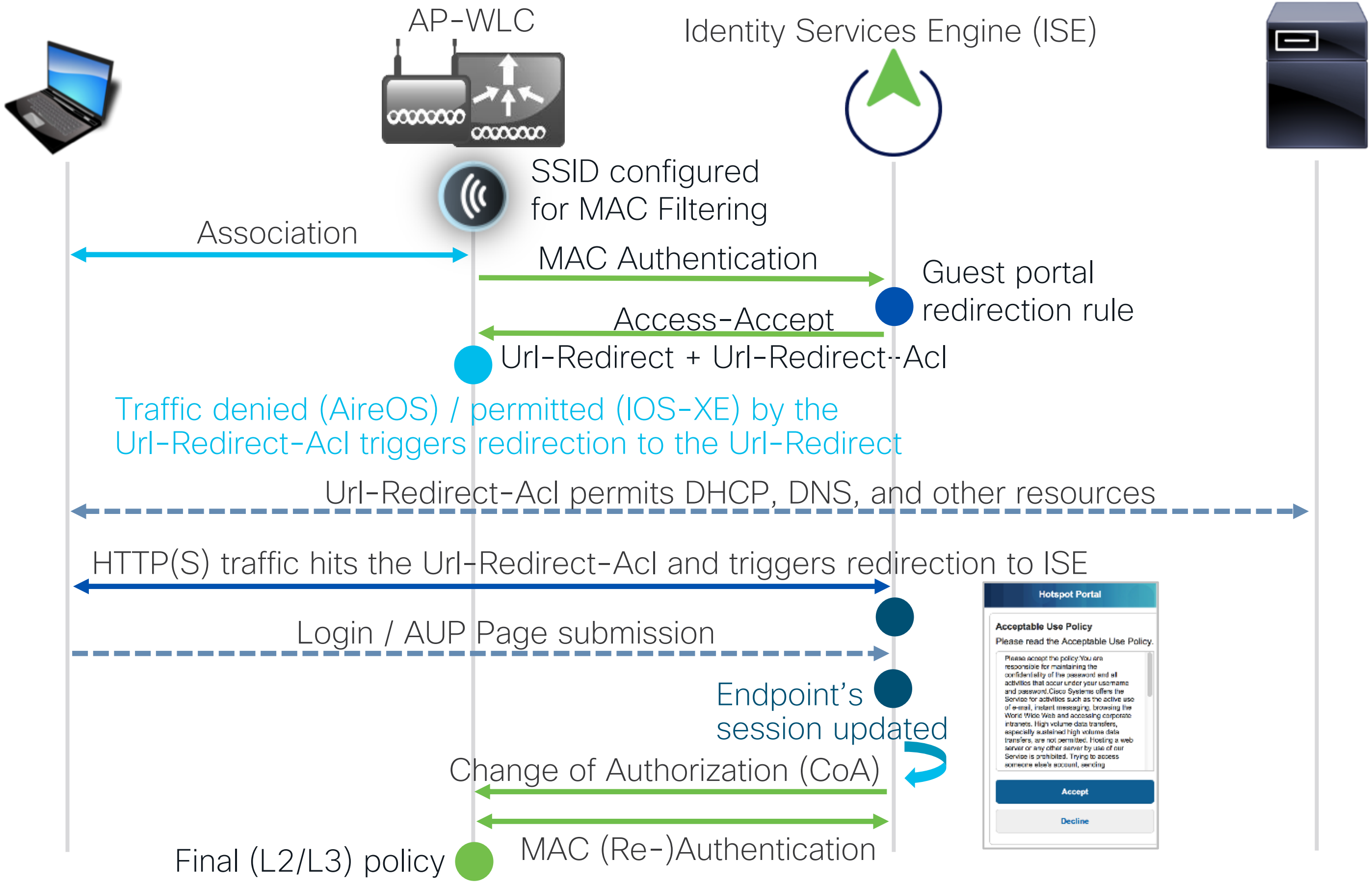
+1 ▾ e.g. 201-555-0123

☑ Opt-in

By clicking the **Connect** button you agree to our **Terms & Conditions**

Central Web Authentication (CWA)

CENTRAL because the redirection URL, the pre-webauth ACL are centrally configured on ISE and dynamically communicated to the WLC (NAD*) via RADIUS.
CWA is partially L2 (MAC Authentication) and partially L3 (redirect on IP resolution).



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

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

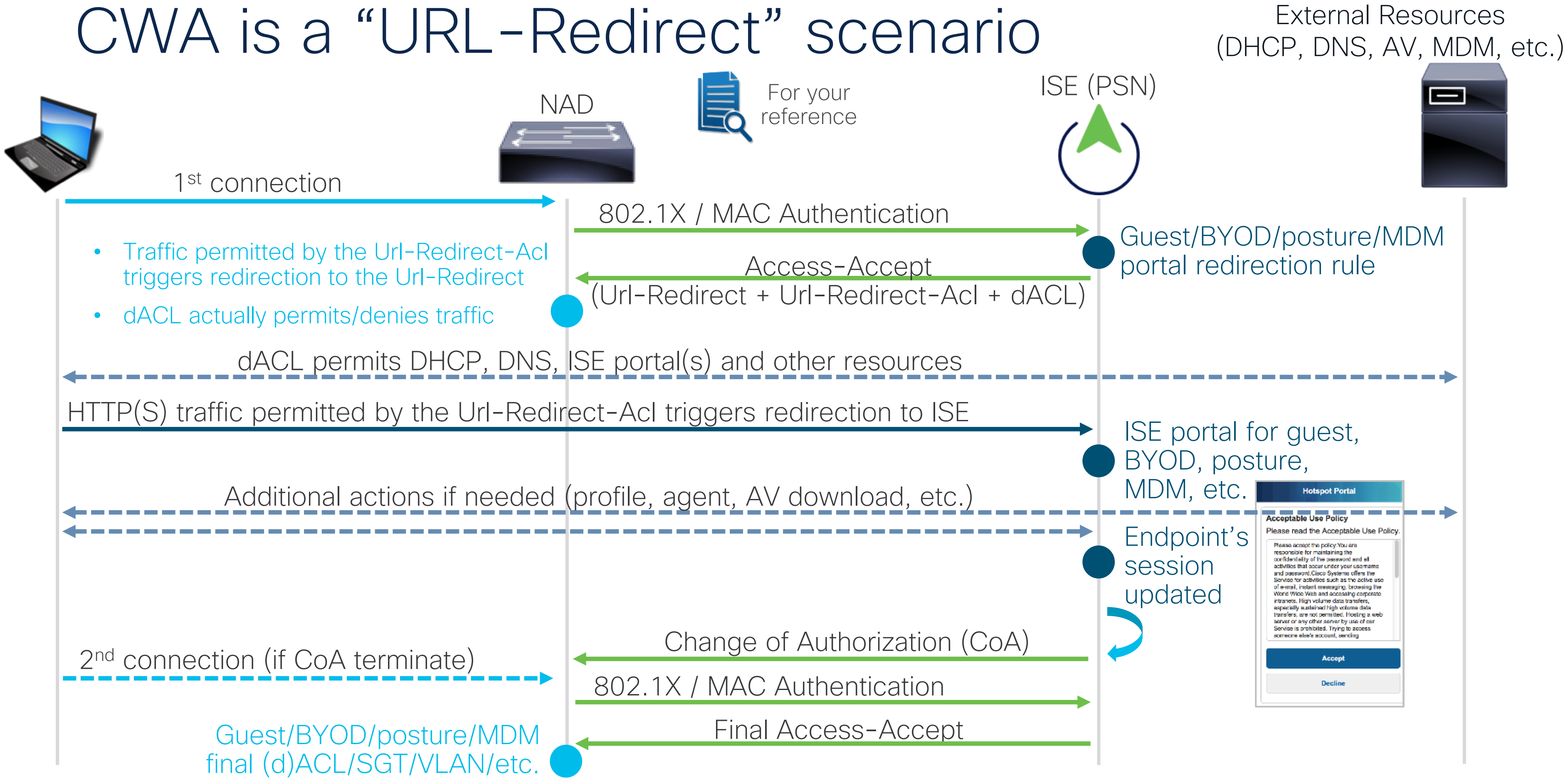
Accept

Decline

*Network Access Device

CWA is a "URL-Redirect" scenario

For your reference


External Resources
(DHCP, DNS, AV, MDM, etc.)
NAD
ISE (PSN)
1st connection
802.1X / MAC Authentication
Guest/BYOD/posture/MDM
portal redirection rule
Access-Accept
(Url-Redirect + Url-Redirect-Acl + dACL)
dACL permits DHCP, DNS, ISE portal(s) and other resources
HTTP(S) traffic permitted by the Url-Redirect-Acl triggers redirection to ISE
ISE portal for guest,
BYOD, posture,
MDM, etc.
Additional actions if needed (profile, agent, AV download, etc.)
Endpoint's
session
updated
Change of Authorization (CoA)
2nd connection (if CoA terminate)
802.1X / MAC Authentication
Final Access-Accept
Guest/BYOD/posture/MDM
final (d)ACL/SGT/VLAN/etc.

- Traffic permitted by the Url-Redirect-Acl triggers redirection to the Url-Redirect
- dACL actually permits/denies traffic

Hotspot Portal

Acceptable Use Policy

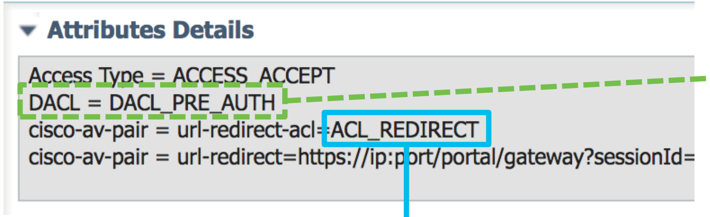
Please read the Acceptable Use Policy.

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

URL-Redirect-Acl

For Cisco IOS(-XE) based WLCs/NADs (e.g., Catalyst switches and wireless controllers), traffic permitted by the Url-Redirect-Acl triggers redirection to the Url-Redirect and traffic denied by the Url-Redirect-Acl is just permitted (if not denied by other dACL/Filter-ID, if any).
An optional dACL/Filter-ID can control more granularly which traffic is permitted/denied.

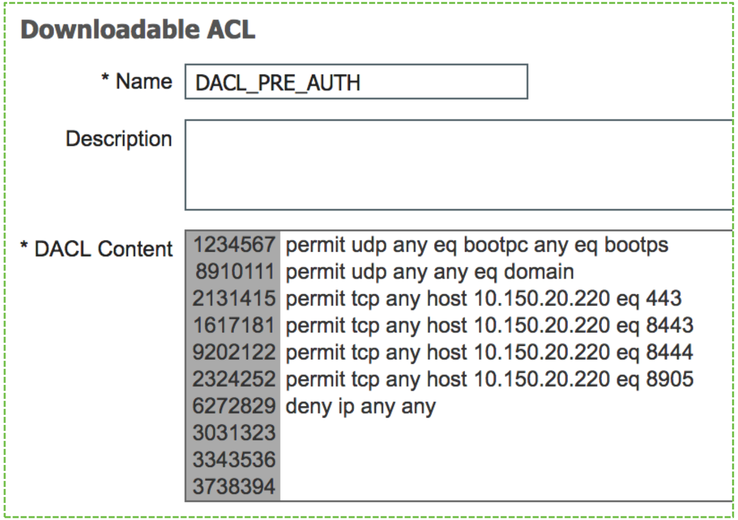
Note: Catalyst 9800 supports dACL starting from IOS-XE 17.10.1 (otherwise it's ignored)



Attributes Details

```
Access Type = ACCESS_ACCEPT
DACL = DACL_PRE_AUTH
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
 permit ip any any
```



Downloadable ACL

* Name	DACL_PRE_AUTH
Description	

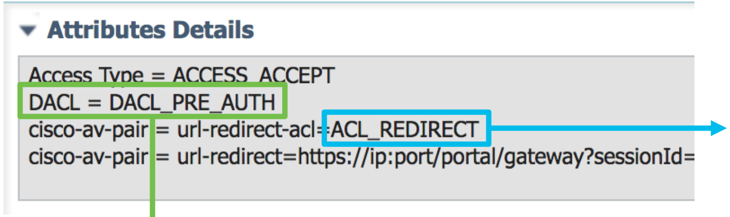
* DACL Content

```
permit udp any eq bootpc any eq bootps
permit udp any any eq domain
permit tcp any host 10.150.20.220 eq 443
permit tcp any host 10.150.20.220 eq 8443
permit tcp any host 10.150.20.220 eq 8444
permit tcp any host 10.150.20.220 eq 8905
deny ip any any
```

URL-Redirect-Acl

For your reference

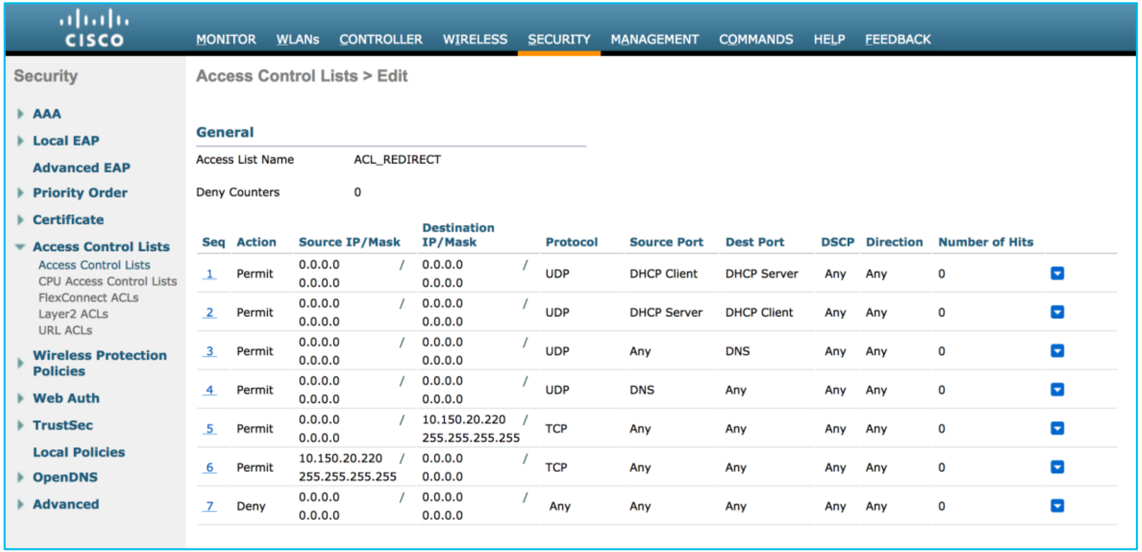
For Cisco AireOS based NADs (e.g., 3504, 5520, 8540 WLCs), traffic denied by the Url-Redirect-Acl triggers redirection to the Url-Redirect.
Other traffic permitted by the Url-Redirect-Acl is simply permitted.



Attributes Details

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

Ignored



Access Control Lists > Edit

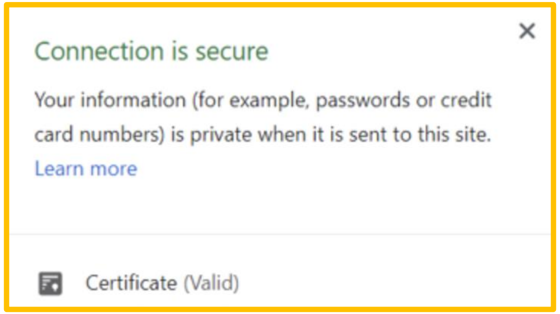
General

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

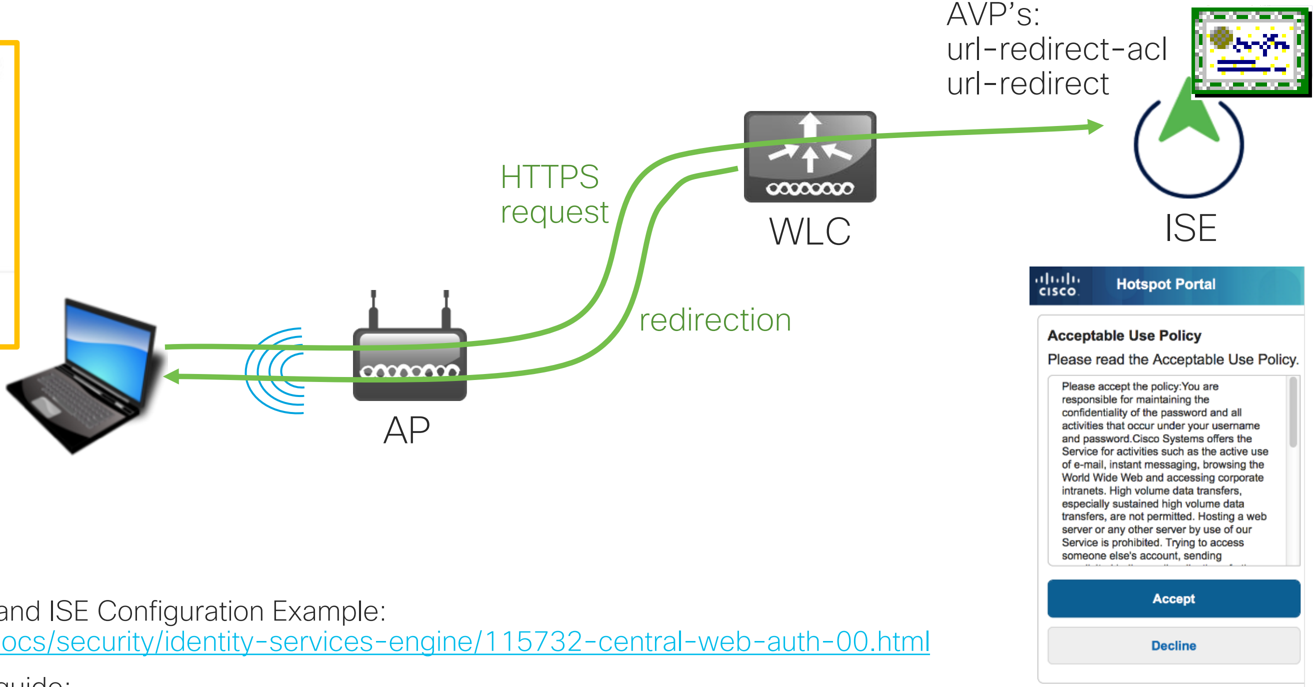
CWA and certificates



Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Certificate (Valid)



Acceptable Use Policy

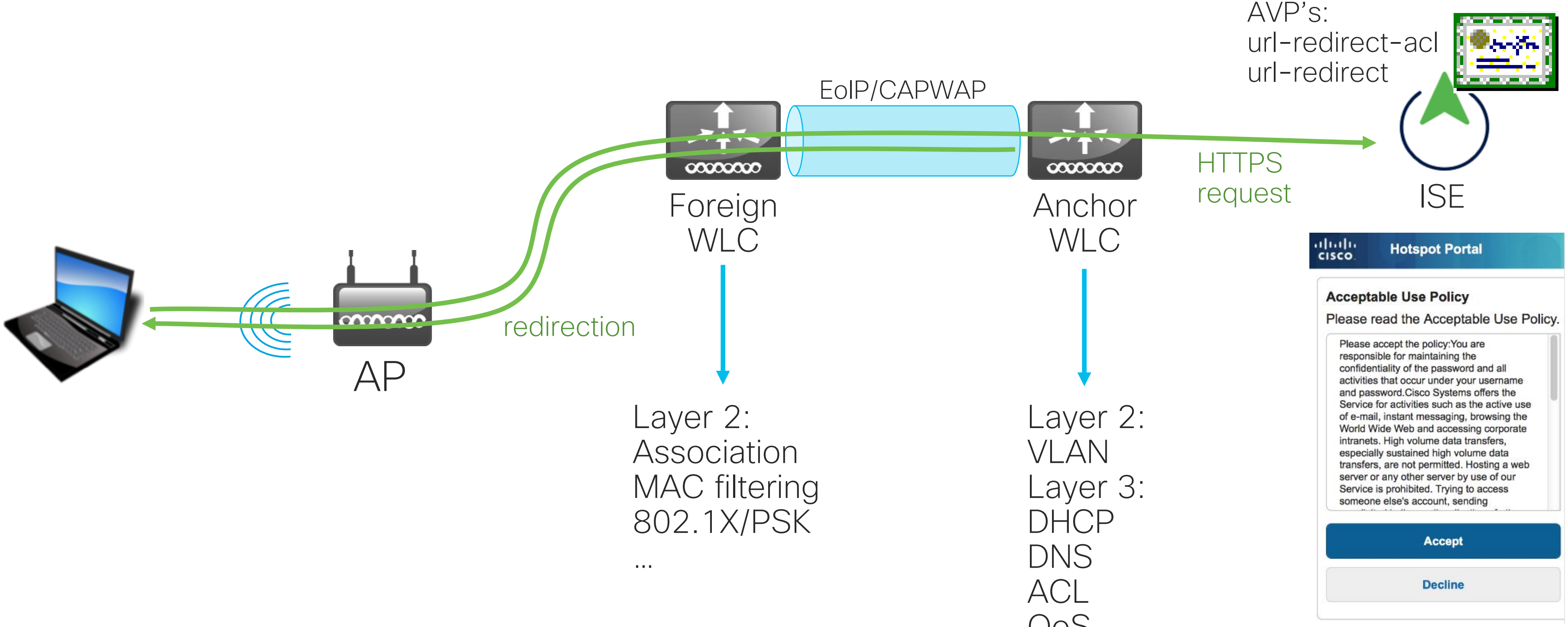
Please read the Acceptable Use Policy.

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



Acceptable Use Policy

Please read the Acceptable Use Policy.

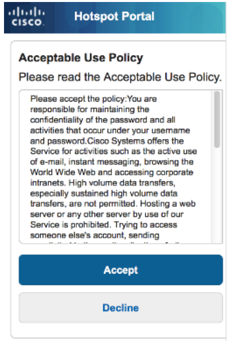
Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing 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
…

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

CWA with FlexConnect

For your reference

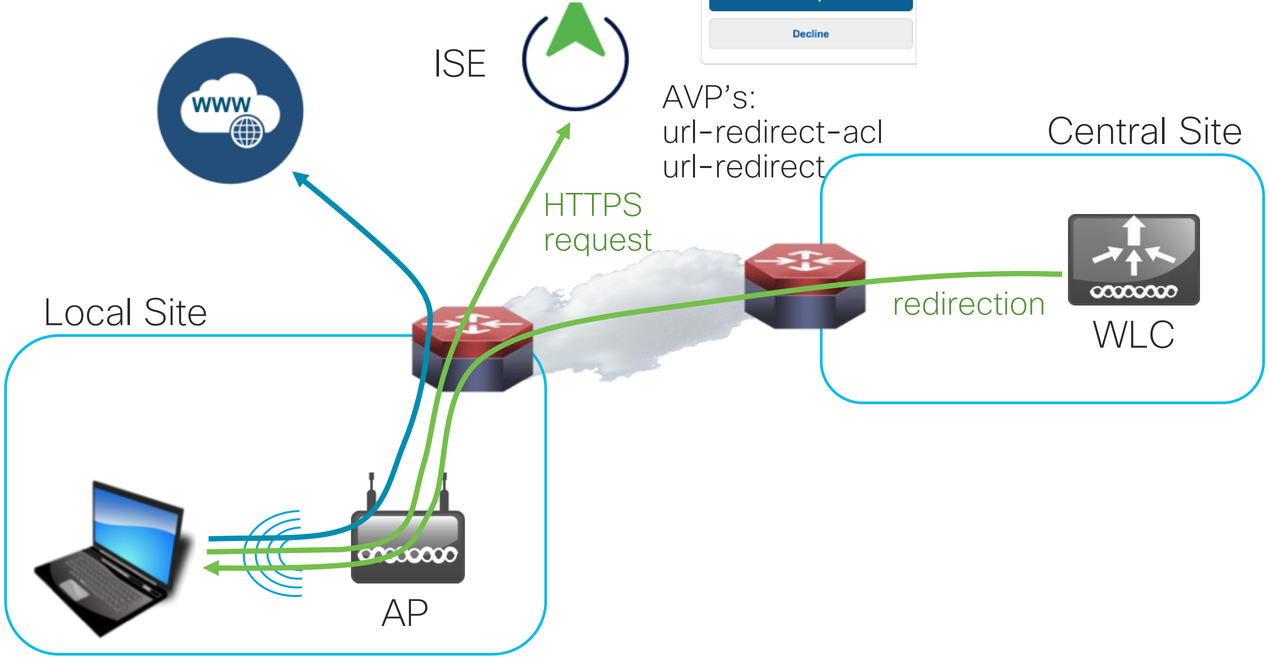


Hotspot Portal

Acceptable Use Policy

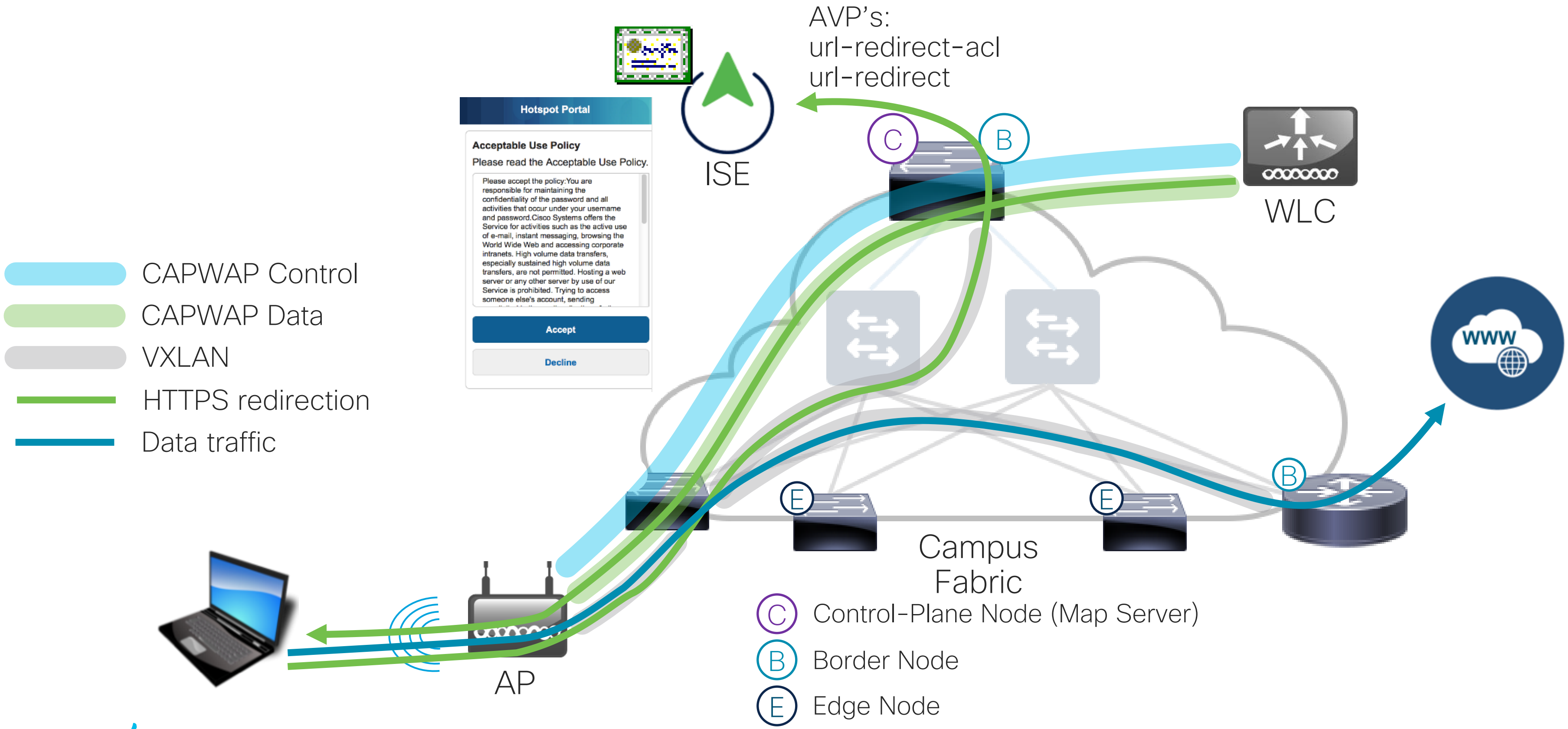
Please read the Acceptable Use Policy.

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



CWA with Software-Defined Access (SDA)

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

CWA configuration

- AAA and method lists
- Url-Redirect-Acl
- WLAN / Policy Profiles
- Policy set and authentication/authorization rules on ISE

CWA configuration

AAA and method lists

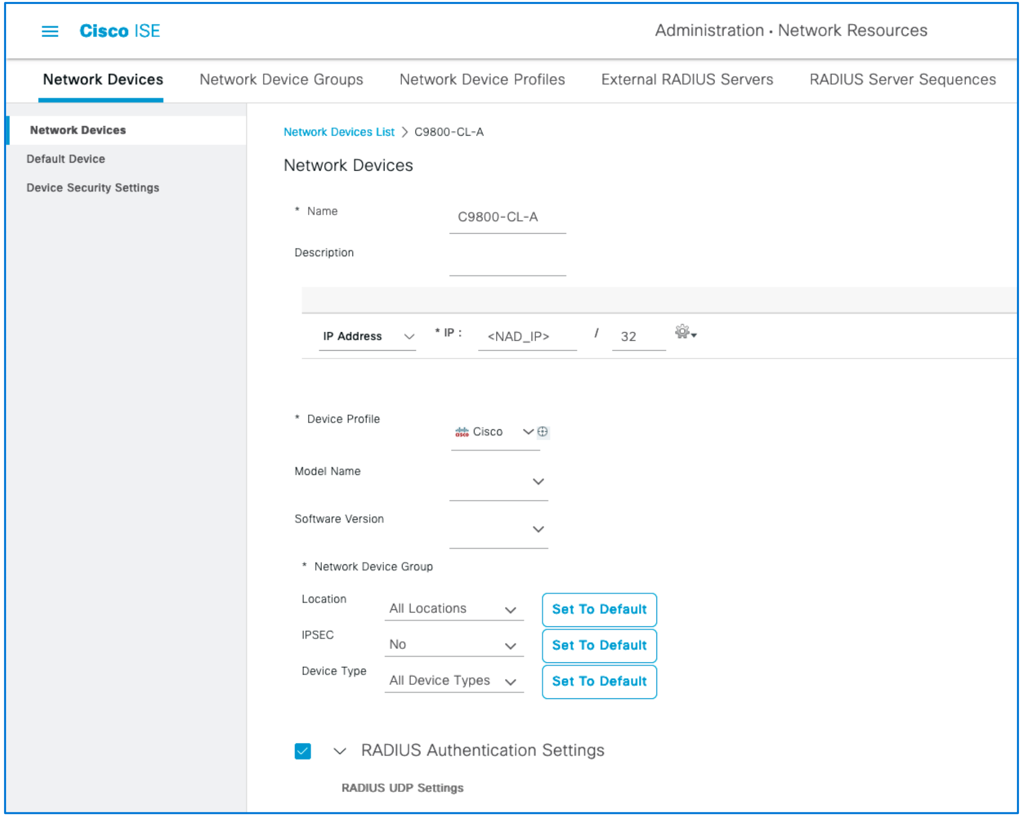
```
radius server RADIUS_SRVR_ISE
 address ipv4 <ISE_IP> auth-port 1812 acct-port 1813
 key <SHARED_SECRET>
!
aaa new-model
!
aaa group server radius RADIUS_SRVR_GRP_01
 server name RADIUS_SRVR_ISE
!
aaa authorization network MLIST_AUTHZ_NTWRK_ISE group RADIUS_SRVR_GRP_01
aaa accounting identity MLIST_ACCT_ID_ISE start-stop group RADIUS_SRVR_GRP_01
!
aaa server radius dynamic-author
 client <ISE_IP> server-key <SHARED_SECRET>
```

Particularly needed for CoA support for CWA

CWA configuration

ISE configuration: network device entry for the wireless controller

For your reference



Network Devices

* Name	C9800-CL-A
Description	
IP Address	* IP : <NAD_IP> / 32
* Device Profile	Cisco
Model Name	
Software Version	

* Network Device Group

Location	All Locations	Set To Default
IPSEC	No	Set To Default
Device Type	All Device Types	Set To Default

☑ RADIUS Authentication Settings

RADIUS UDP Settings

CWA configuration

Url-Redirect-Acl

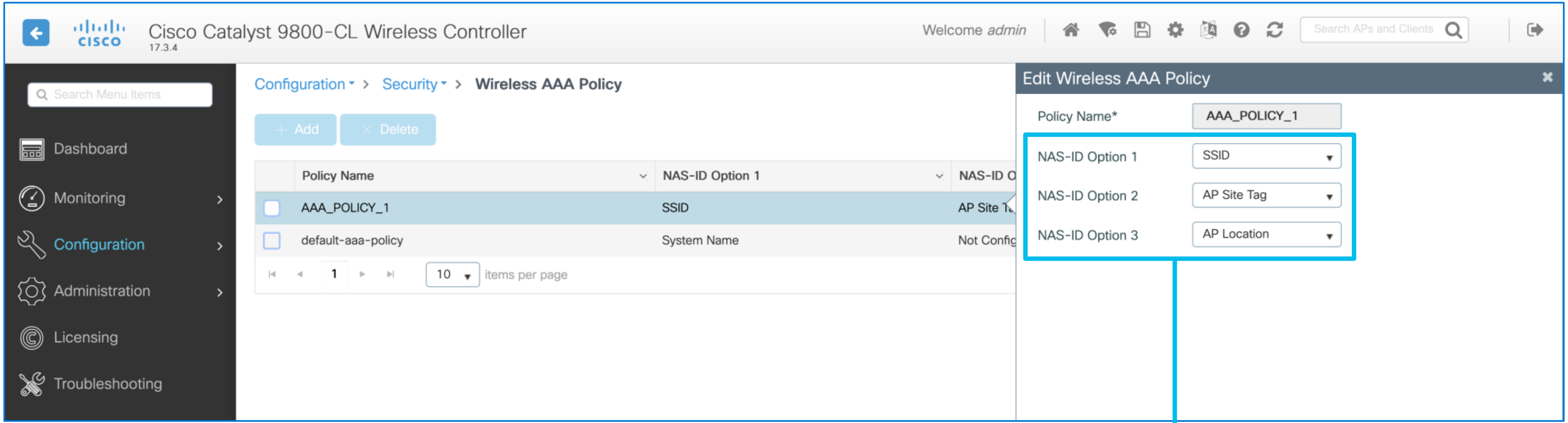
```
ip access-list extended ACL_CWA_REDIRECT
 deny udp any any eq bootps
 deny udp any eq bootps any
 deny udp any any eq domain
 deny udp any eq domain any
 deny tcp any host <ISE_IP> eq 8443
 deny tcp host <ISE_IP> eq 8443 any
 permit ip any any
```

Anything denied is permitted.
(for HTTP/S) Anything permitted is redirected.

<ISE_IP> here is the IP on which ISE PSN serves the guest portal (by default on TCP:8443).
If we're using multiple ports/interfaces on ISE, it may be different from ISE's admin IP or even from its IP used for RADIUS traffic, for example.

CWA configuration – C9800

Optional: NAS-Identifier to redirect to different portals based on site tag, AP location, WLAN name, etc.



	Policy Name	NAS-ID Option 1	NAS-ID O
☐	AAA_POLICY_1	SSID	AP Site Ta
☐	default-aaa-policy	System Name	Not Config

Edit Wireless AAA Policy

Policy Name* AAA_POLICY_1

NAS-ID Option 1 SSID

NAS-ID Option 2 AP Site Tag

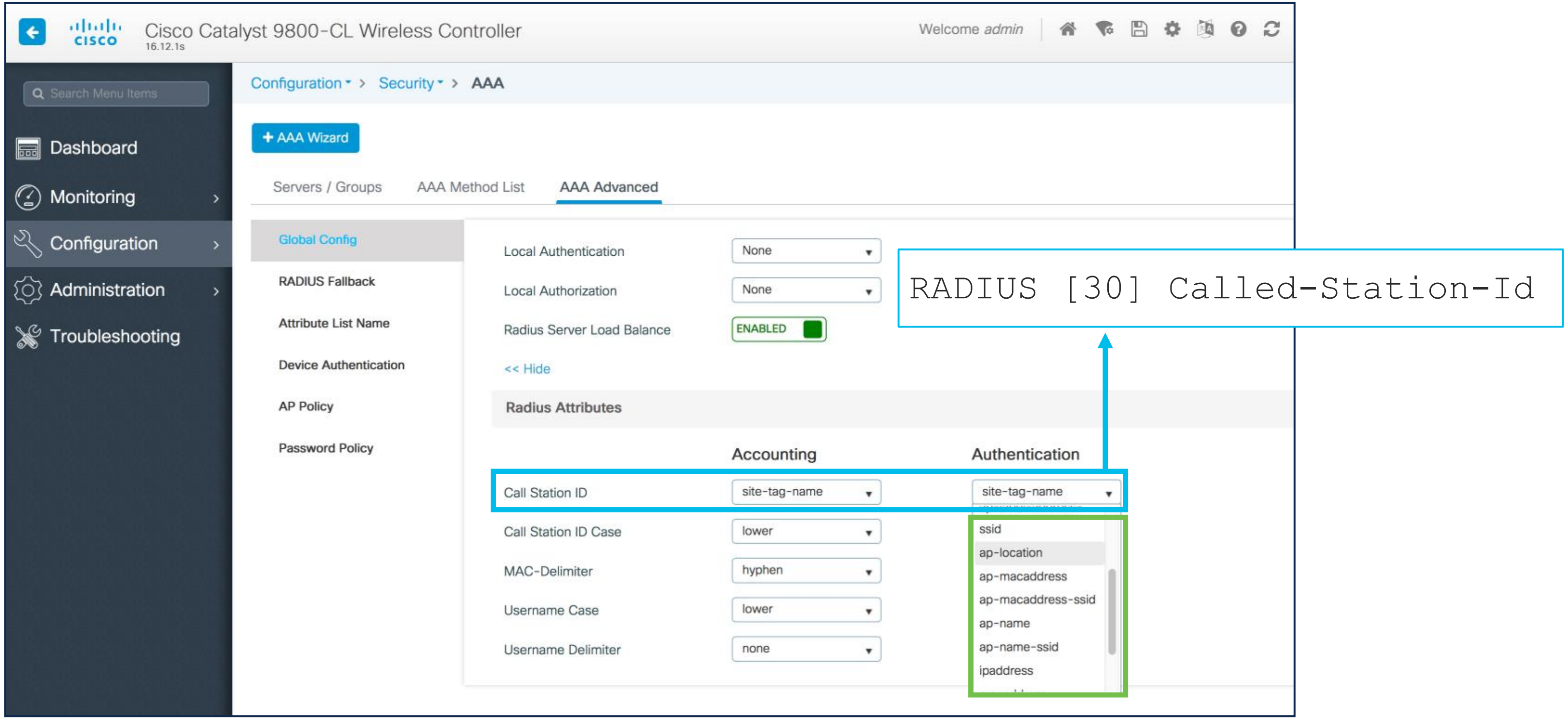
NAS-ID Option 3 AP Location

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

CWA configuration

Optional: Called-Station-Id to redirect to different portals based on AP location, AP name, etc.

For your reference



Local Authentication: None

Local Authorization: None

Radius Server Load Balance: ENABLED

Radius Attributes

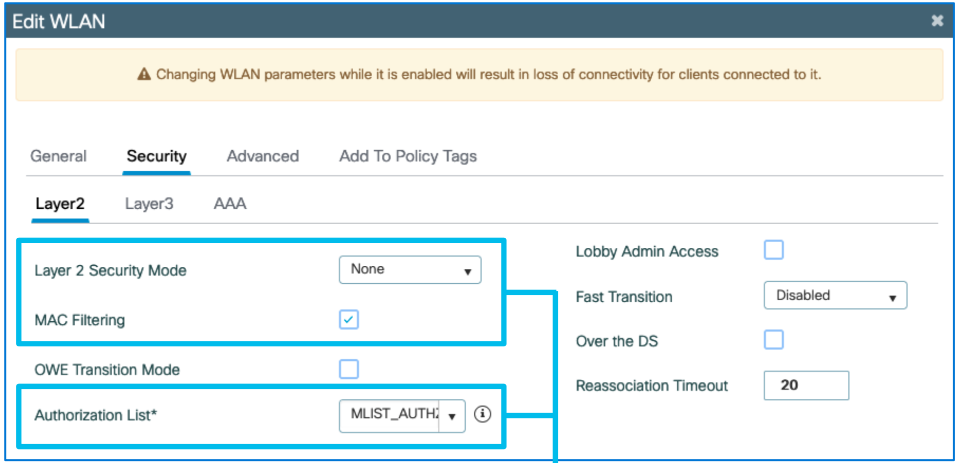
	Accounting	Authentication
Call Station ID	site-tag-name	site-tag-name
Call Station ID Case	lower	
MAC-Delimiter	hyphen	
Username Case	lower	
Username Delimiter	none	

RADIUS [30] Called-Station-Id

CWA configuration – C9800

WLAN / Policy Profiles

WLAN Profile



Edit WLAN ✖

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

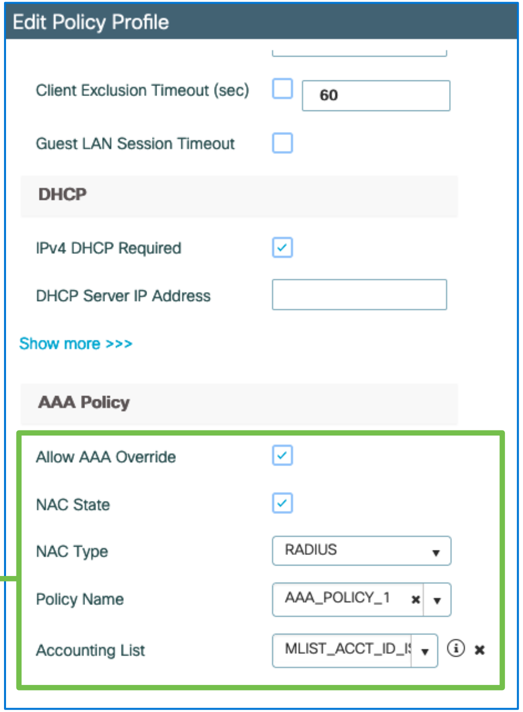
General | **Security** | Advanced | Add To Policy Tags

Layer2 | Layer3 | AAA

Layer 2 Security Mode	None ▾
MAC Filtering	☑
OWE Transition Mode	□
Authorization List*	MLIST_AUTHZ ▾ ⓘ
Lobby Admin Access	□
Fast Transition	Disabled ▾
Over the DS	□
Reassociation Timeout	20

- Open SSID, unless we'd like to add 802.1X/PSK on top
- MAC Filtering with the "MLIST_AUTHZ_NTWRK_ISE" authorization list

Policy Profile



Edit Policy Profile

Client Exclusion Timeout (sec)	□ 60
Guest LAN Session Timeout	□

DHCP

IPv4 DHCP Required	☑
DHCP Server IP Address	

Show more >>>

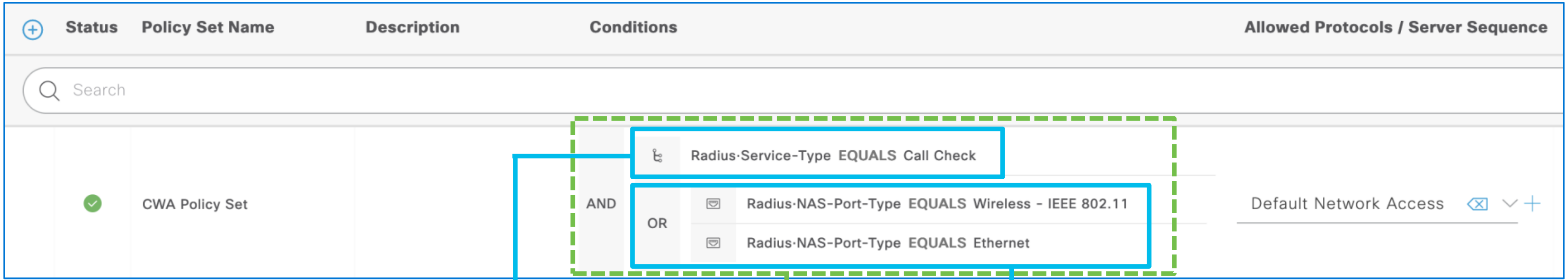
AAA Policy

Allow AAA Override	☑
NAC State	☑
NAC Type	RADIUS ▾
Policy Name	AAA_POLICY_1 ✖ ▾
Accounting List	MLIST_ACCT_ID_IS ▾ ⓘ ✖

- "Allow AAA Override" for the 9800 to accept RADIUS attributes
- "NAC State" enabled and "RADIUS" NAC Type for CoA support from ISE
- (optional) "AAA_POLICY_1" for a custom NAS-Identifier
- "MLIST_ACCT_ID_ISE" accounting list for CoA and accounting with ISE

CWA configuration – ISE

ISE configuration: Policy Set

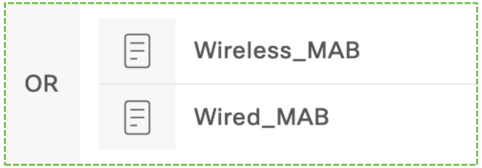


Search

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
✓	CWA Policy Set		AND Radius·Service-Type EQUALS Call Check OR Radius·NAS-Port-Type EQUALS Wireless - IEEE 802.11 Radius·NAS-Port-Type EQUALS Ethernet	Default Network Access

Cisco NADs use “Call Check”, for other 3rd party NADs we’d need to check what other values are used

Wireless NADs use “Wireless – IEEE 802.11”, wired NADs use “Ethernet”

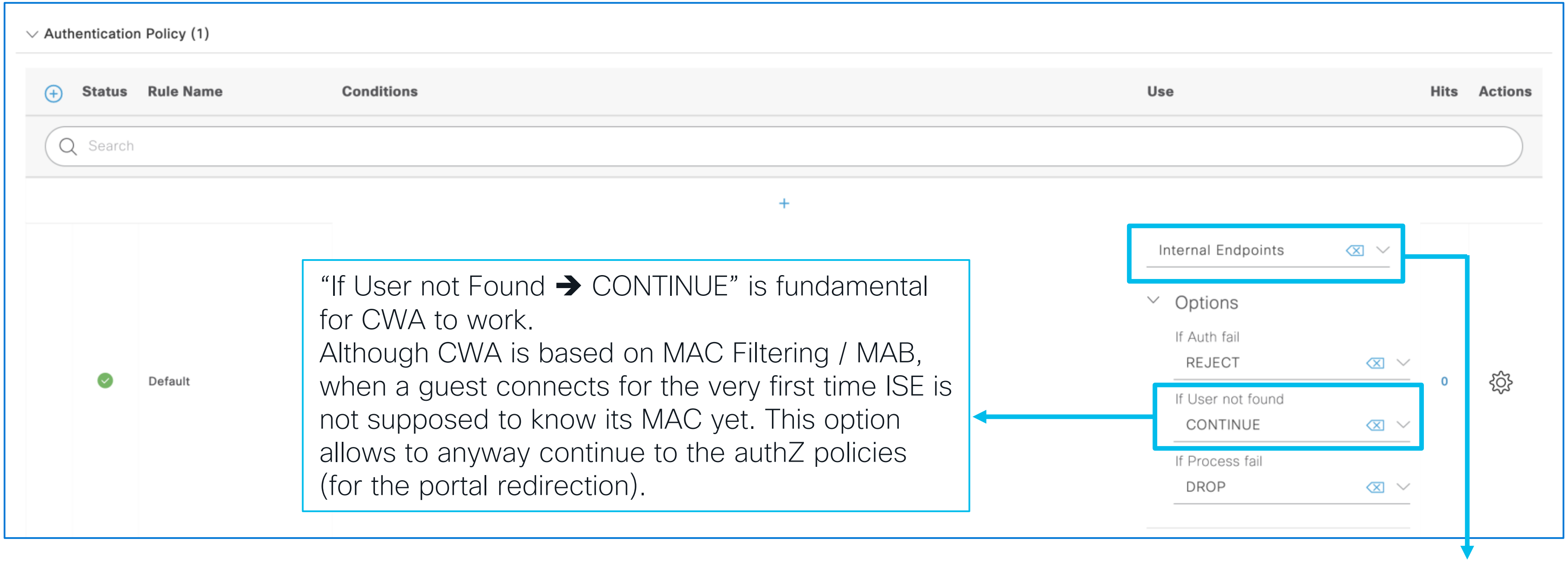


OR
- Wireless_MAB
- Wired_MAB

Usually we could just rely on the pre-defined smart conditions, which automatically adapt according to the NAD Profile

CWA configuration - ISE

ISE configuration: authentication policies



Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		Internal Endpoints Options If Auth fail: REJECT If User not found: CONTINUE If Process fail: DROP	0	⚙

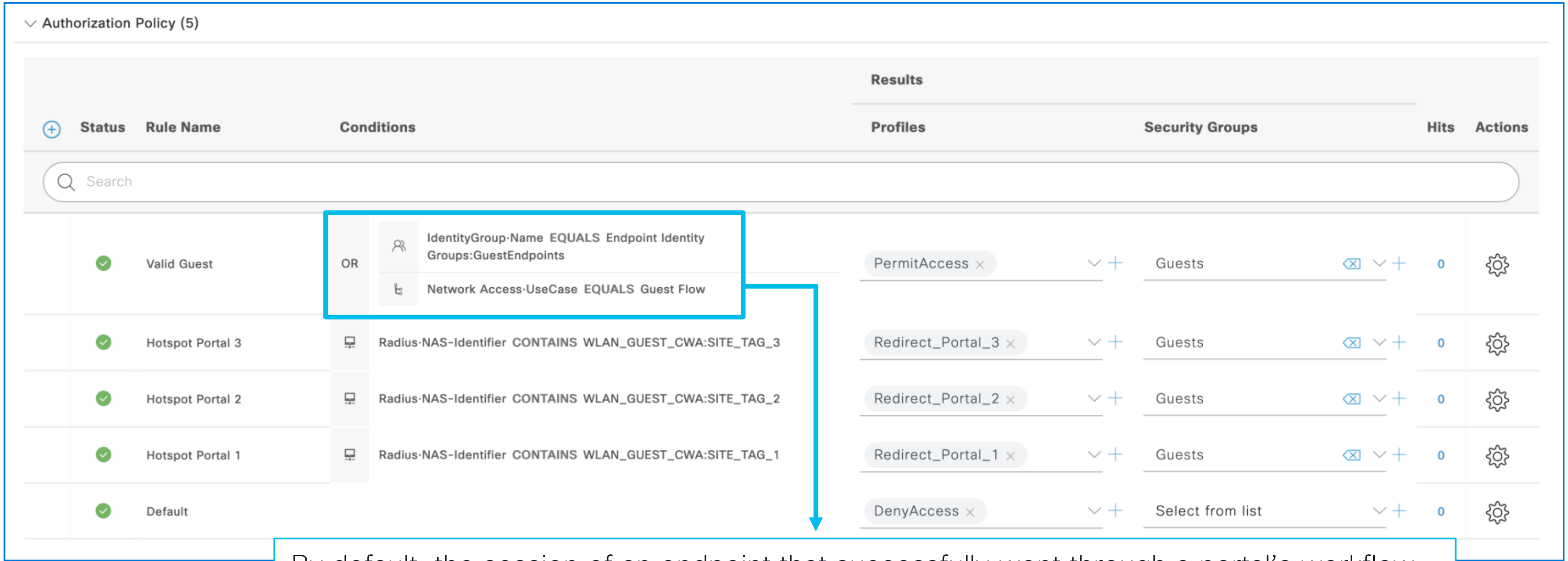
“If User not Found ➔ CONTINUE” is fundamental for CWA to work.
Although CWA is based on MAC Filtering / MAB, when a guest connects for the very first time ISE is not supposed to know its MAC yet. This option allows to anyway continue to the authZ policies (for the portal redirection).

Not much needed in the authC policies unless we’d like to do some extra filtering

CWA is based on MAC Filtering on the NAD, so the authC policy should point to the MACs database in ISE

CWA configuration – ISE

ISE configuration: authorization policies



Authorization Policy (5)

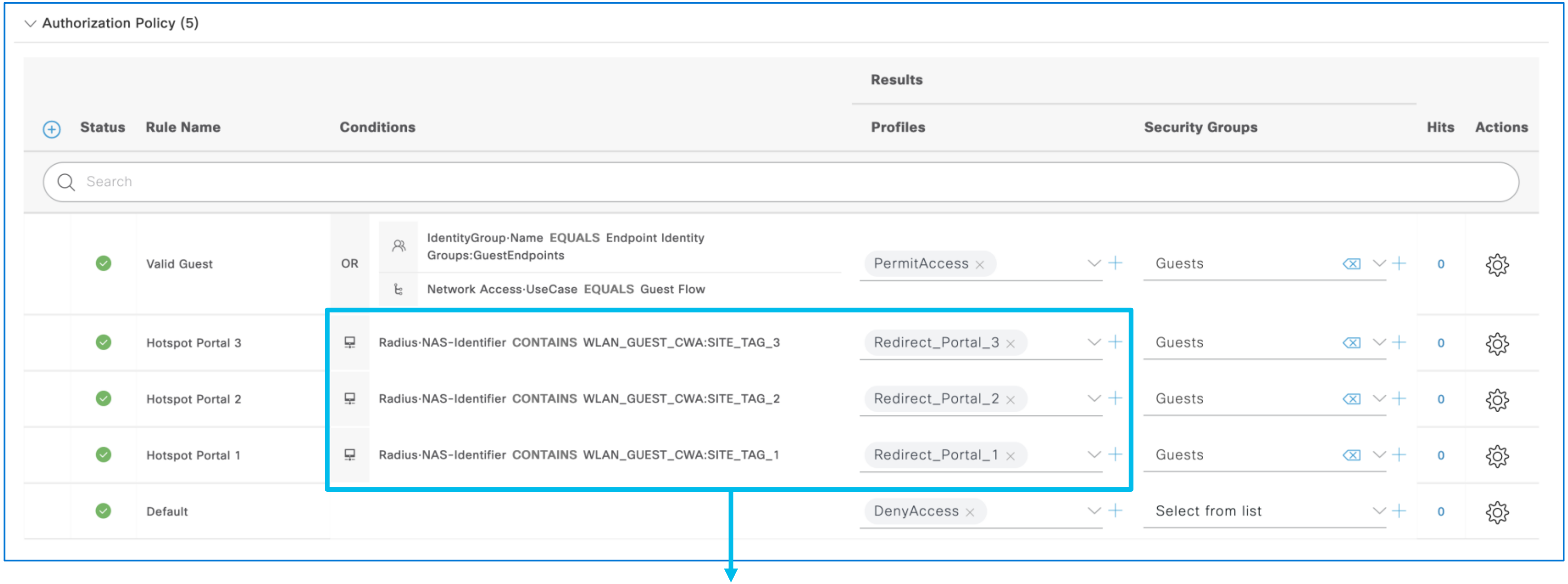
			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	Valid Guest	OR IdentityGroup·Name EQUALS Endpoint Identity Groups:GuestEndpoints Network Access·UseCase EQUALS Guest Flow	PermitAccess	Guests	0	⚙
✓	Hotspot Portal 3	Radius·NAS-Identifier CONTAINS WLAN_GUEST_CWA:SITE_TAG_3	Redirect_Portal_3	Guests	0	⚙
✓	Hotspot Portal 2	Radius·NAS-Identifier CONTAINS WLAN_GUEST_CWA:SITE_TAG_2	Redirect_Portal_2	Guests	0	⚙
✓	Hotspot Portal 1	Radius·NAS-Identifier CONTAINS WLAN_GUEST_CWA:SITE_TAG_1	Redirect_Portal_1	Guests	0	⚙
✓	Default		DenyAccess	Select from list	0	⚙

By default, the session of an endpoint that successfully went through a portal’s workflow is marked with the attribute “Use Case = Guest Flow” in the ISE’s internal database.

Alternatively, guest portal’s options allow to register the MAC of an endpoint that successfully went through the portal’s workflow into a specific Identity Group.

CWA configuration - ISE

ISE configuration: authorization policies



Authorization Policy (5)

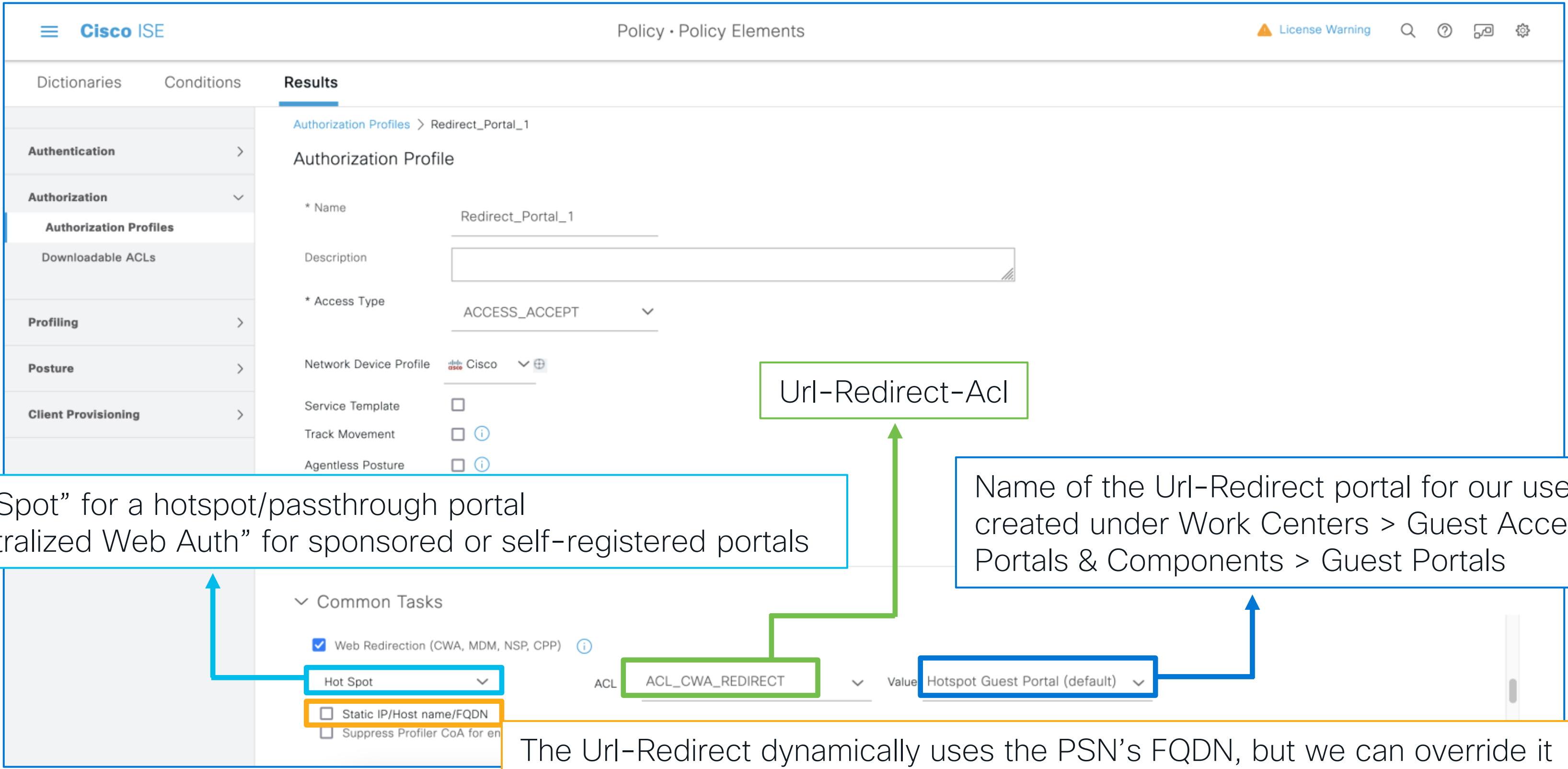
Search

			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	Valid Guest	OR IdentityGroup·Name EQUALS Endpoint Identity Groups:GuestEndpoints Network Access·UseCase EQUALS Guest Flow	PermitAccess	Guests	0	⚙
✓	Hotspot Portal 3	Radius·NAS-Identifier CONTAINS WLAN_GUEST_CWA:SITE_TAG_3	Redirect_Portal_3	Guests	0	⚙
✓	Hotspot Portal 2	Radius·NAS-Identifier CONTAINS WLAN_GUEST_CWA:SITE_TAG_2	Redirect_Portal_2	Guests	0	⚙
✓	Hotspot Portal 1	Radius·NAS-Identifier CONTAINS WLAN_GUEST_CWA:SITE_TAG_1	Redirect_Portal_1	Guests	0	⚙
✓	Default		DenyAccess	Select from list	0	⚙

By optionally customizing the RADIUS attribute [32] NAS-Identifier on the 9800, we can reuse this attribute in the authZ policies to redirect to different portals based on the Site Tag / Location / etc. of the AP, where the endpoint is connecting from.

CWA configuration - ISE

ISE configuration: authorization profile



Authorization Profile

* Name: Redirect_Portal_1

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template ☐

Track Movement ☐

Agentless Posture ☐

☑ Web Redirection (CWA, MDM, NSP, CPP)

Hot Spot | ACL: ACL_CWA_REDIRECT | Value: Hotspot Guest Portal (default)

☐ Static IP/Host name/FQDN

☐ Suppress Profiler CoA for en

Url-Redirect-Acl

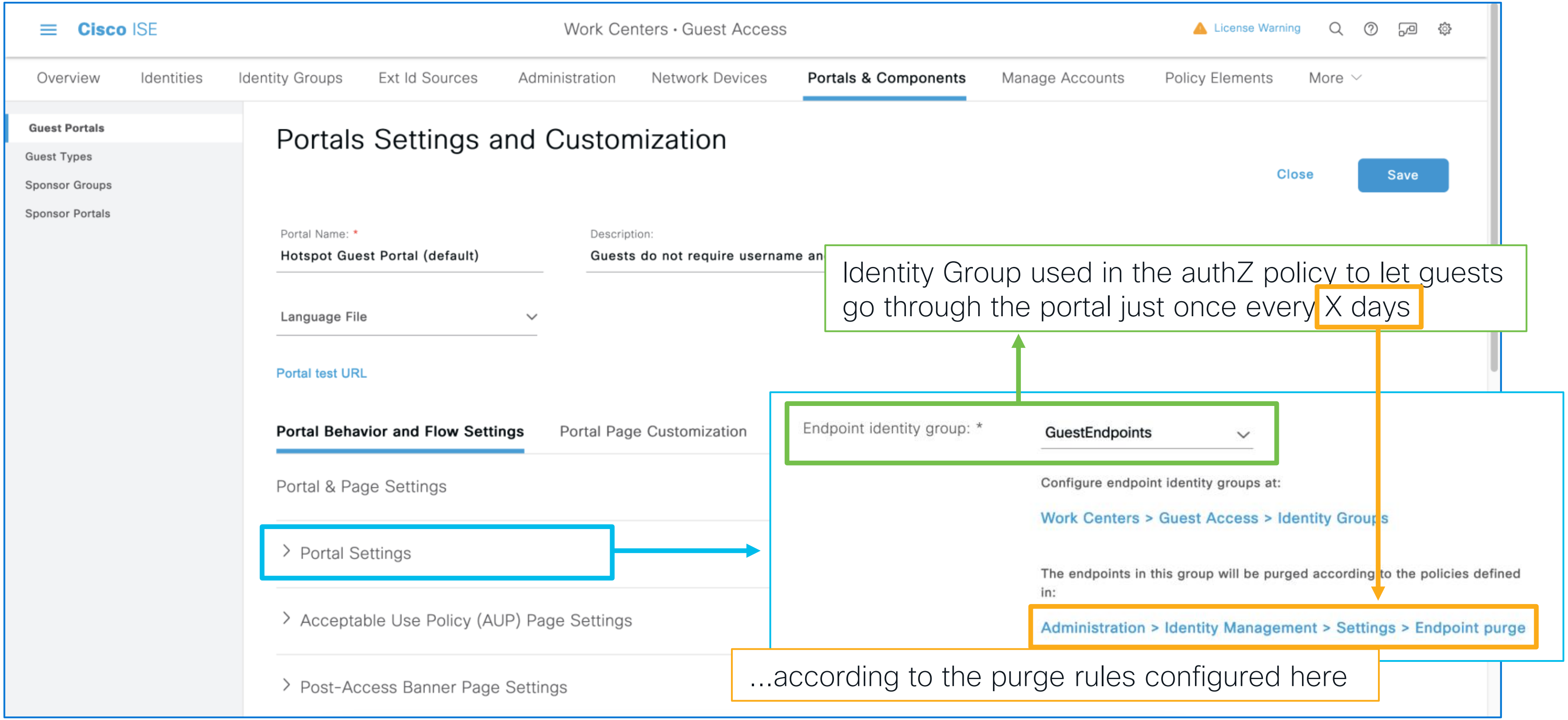
“Hot Spot” for a hotspot/passthrough portal
“Centralized Web Auth” for sponsored or self-registered portals

Name of the Url-Redirect portal for our use case, created under Work Centers > Guest Access > Portals & Components > Guest Portals

The Url-Redirect dynamically uses the PSN’s FQDN, but we can override it

CWA configuration - ISE

ISE configuration: hotspot portal settings



Portals Settings and Customization

Portal Name: * Hotspot Guest Portal (default)

Description: Guests do not require username an

Portal & Page Settings

Endpoint identity group: * GuestEndpoints

Configure endpoint identity groups at:

Work Centers > Guest Access > Identity Groups

The endpoints in this group will be purged according to the policies defined in:

Administration > Identity Management > Settings > Endpoint purge

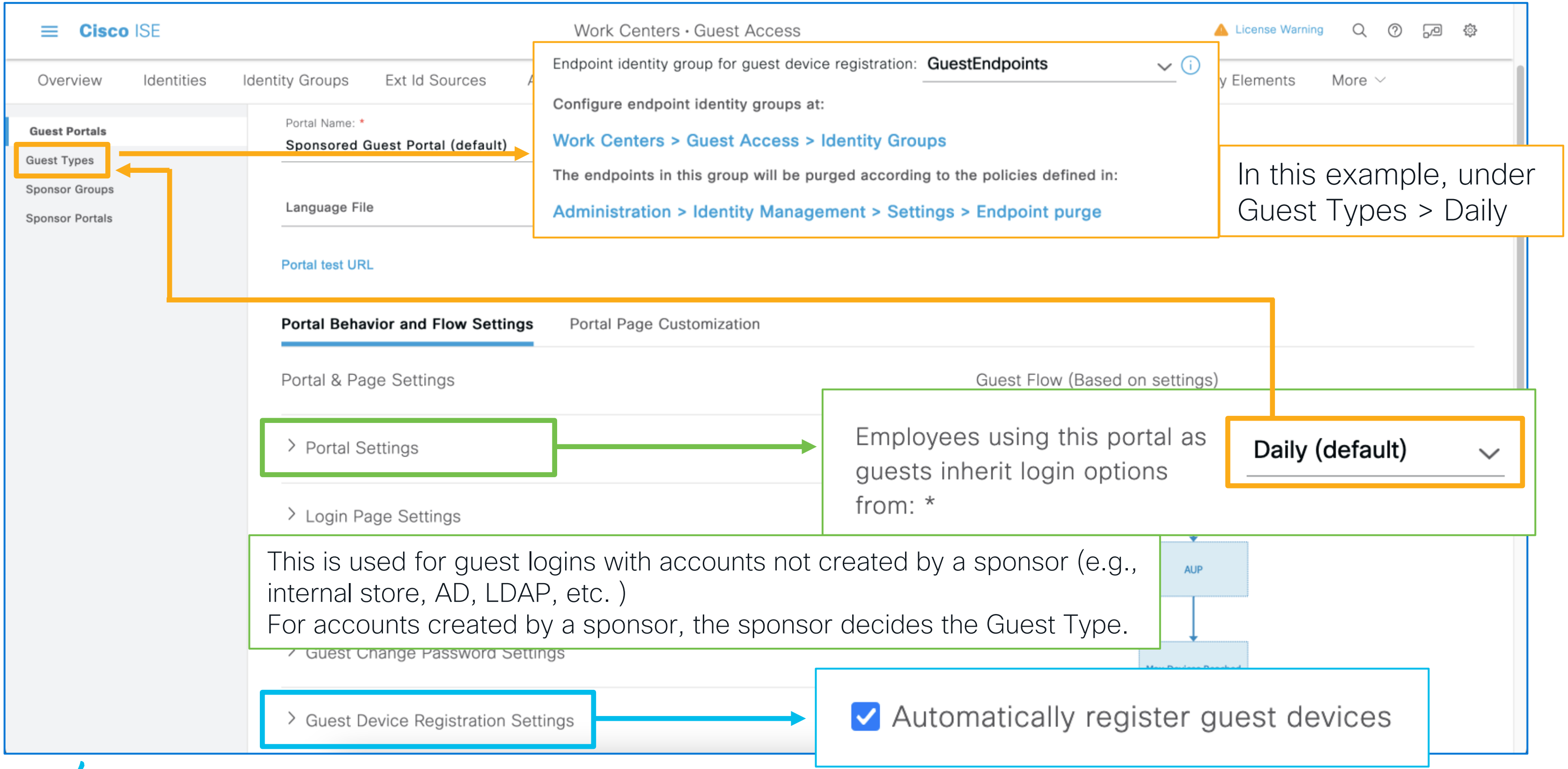
Identity Group used in the authZ policy to let guests go through the portal just once every X days

...according to the purge rules configured here

CWA configuration

ISE configuration: sponsored portal settings

For your reference



Portal Name: * Sponsored Guest Portal (default)

Language File

Endpoint identity group for guest device registration: GuestEndpoints

Configure endpoint identity groups at:

Work Centers > Guest Access > Identity Groups

The endpoints in this group will be purged according to the policies defined in:

Administration > Identity Management > Settings > Endpoint purge

In this example, under Guest Types > Daily

Employees using this portal as guests inherit login options from: * Daily (default)

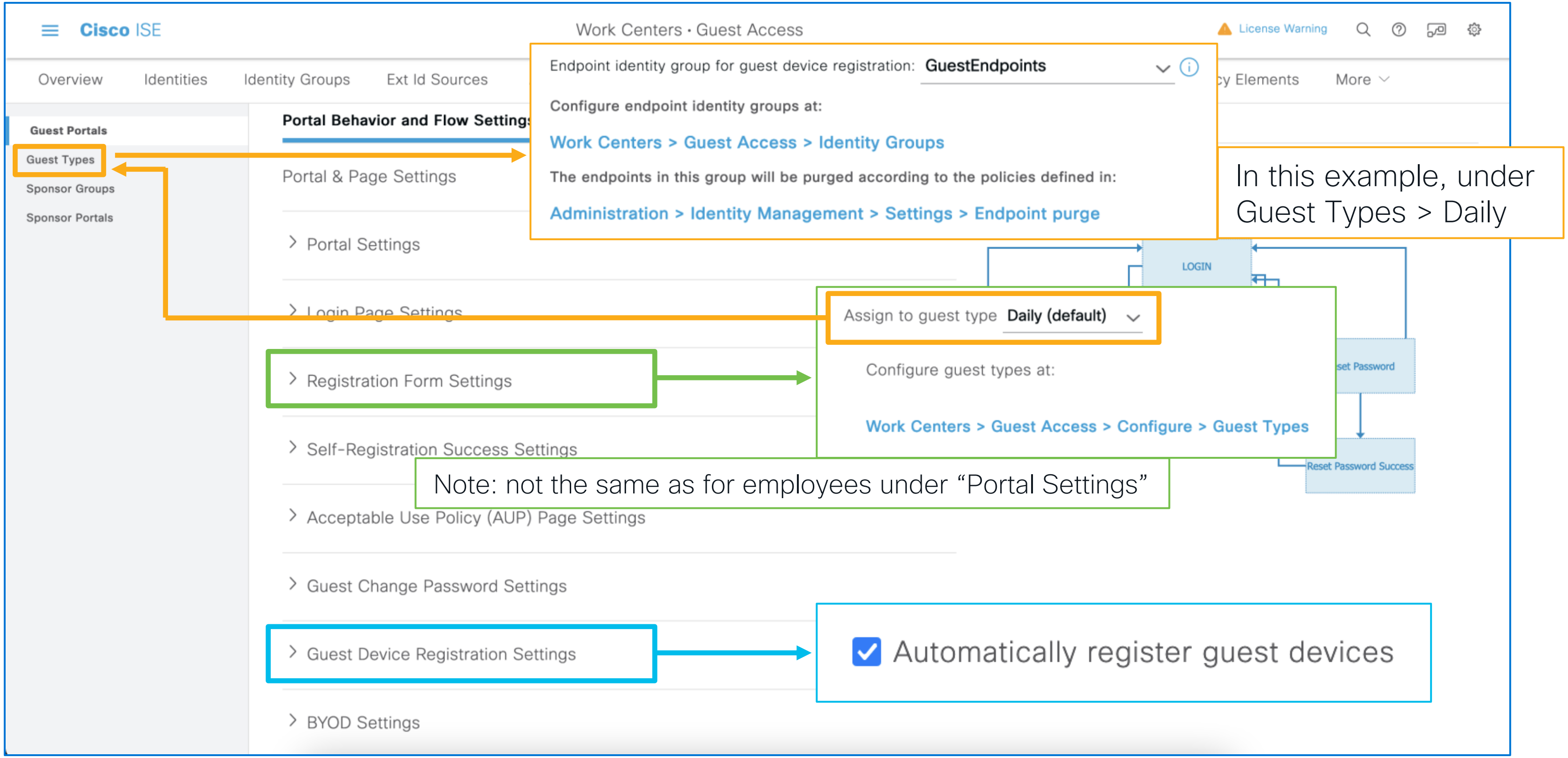
This is used for guest logins with accounts not created by a sponsor (e.g., internal store, AD, LDAP, etc.)
For accounts created by a sponsor, the sponsor decides the Guest Type.

☑ Automatically register guest devices

CWA configuration

ISE configuration: self-registered portal settings

For your reference



Endpoint identity group for guest device registration: GuestEndpoints

Configure endpoint identity groups at:

Work Centers > Guest Access > Identity Groups

The endpoints in this group will be purged according to the policies defined in:

Administration > Identity Management > Settings > Endpoint purge

In this example, under Guest Types > Daily

- Portal Settings
- Login Page Settings
- Registration Form Settings
- Self-Registration Success Settings
- Acceptable Use Policy (AUP) Page Settings
- Guest Change Password Settings
- Guest Device Registration Settings
- BYOD Settings

Assign to guest type Daily (default)

Configure guest types at:

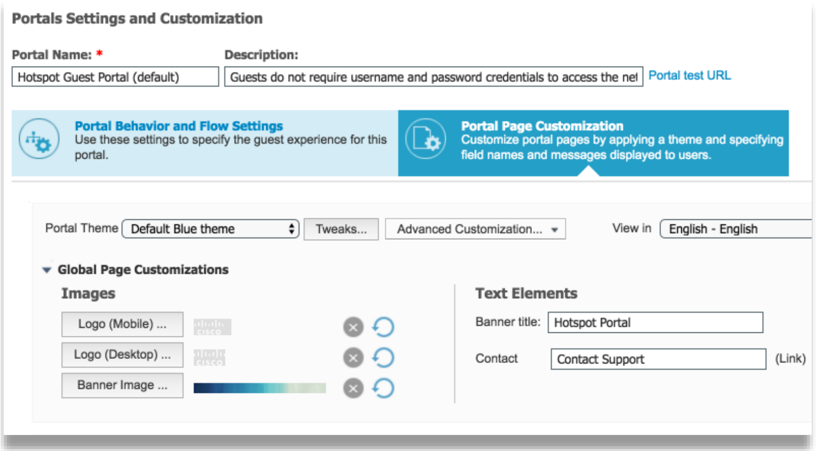
Work Centers > Guest Access > Configure > Guest Types

Note: not the same as for employees under “Portal Settings”

☑ Automatically register guest devices

ISE portal customization options

Granular options to customize guest and sponsor portals



Portals Settings and Customization

Portal Name: * Hotspot Guest Portal (default)

Description: Guests do not require username and password credentials to access the net

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.

Portal Theme: Default Blue theme | Tweaks... | Advanced Customization... | View in: English - English

Global Page Customizations

Images

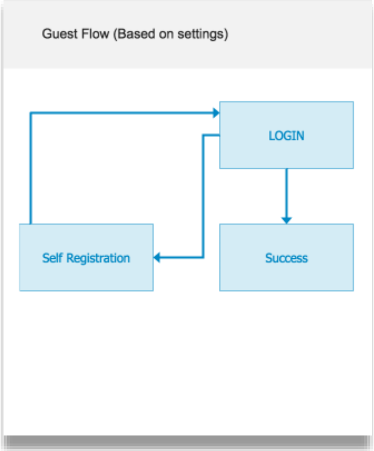
- Logo (Mobile) ...
- Logo (Desktop) ...
- Banner Image ...

Text Elements

Banner title: Hotspot Portal

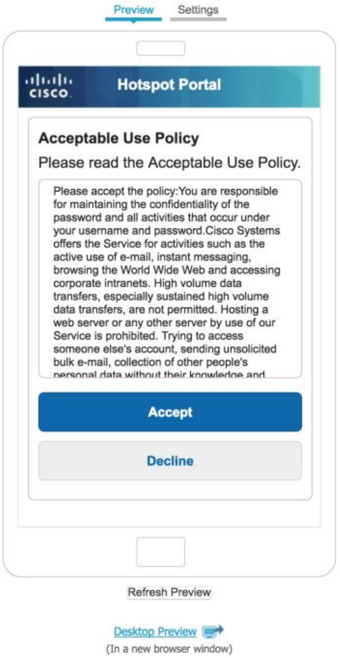
Contact: Contact Support (Link)

Visualize as you configure



Guest Flow (Based on settings)

Consistent branding across device-types

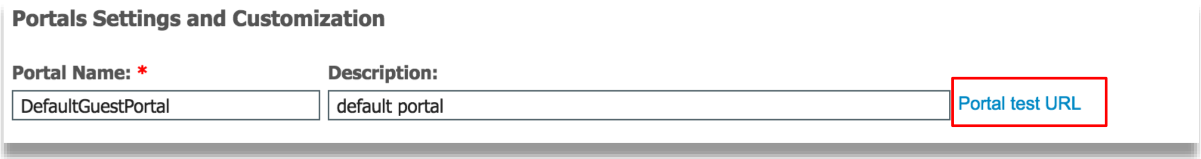


Acceptable Use Policy

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 unsolicited bulk e-mail, collection of other people's personal data without their knowledge and

Test portal URL then and there



Portals Settings and Customization

Portal Name: * DefaultGuestPortal

Description: default portal

Portal test URL

ISE guest portals: some other facts

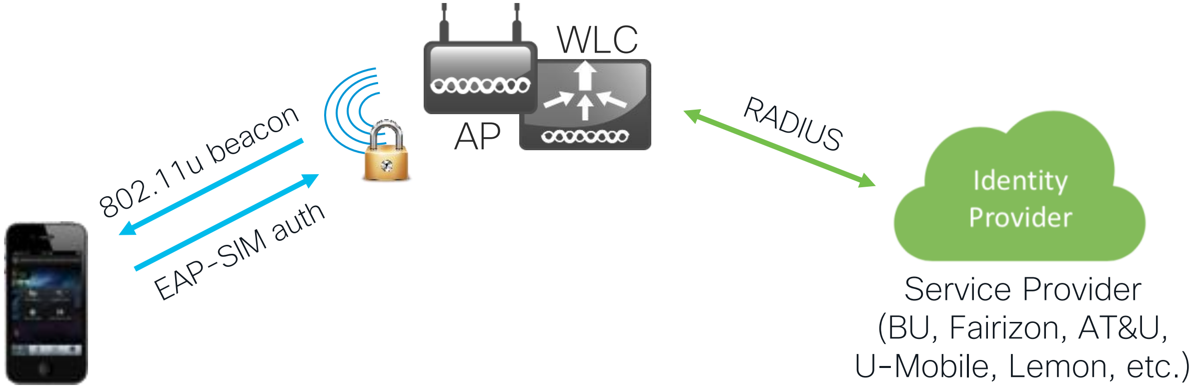
For your reference

- Up to max ~150 concurrent logins/web page requests per second per PSN (Policy Services Node): https://www.cisco.com/c/en/us/td/docs/security/ise/performance_and_scalability/b_ise_perf_and_scale.html#Cisco_Reference.dita_59adea36-0b36-4981-91e3-2ff0478d6ff4
- 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 dedicated portal builder: https://isepb.cisco.com
- It supports APIs for guest accounts creation and additional integration with external tools.

OpenRoaming

Passpoint

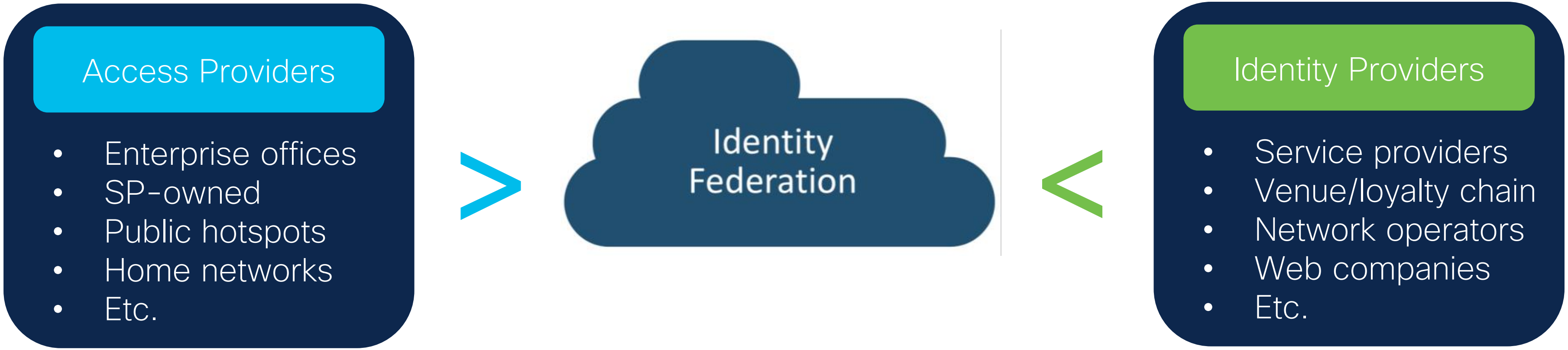
- The need: seamless and secure end user’s connectivity to Wi-Fi
- The former answer: 802.11u / Hotspot 2.0 / Passpoint



Service Provider
(BU, Fairizon, AT&U,
U-Mobile, Lemon, 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



Access Providers

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

>

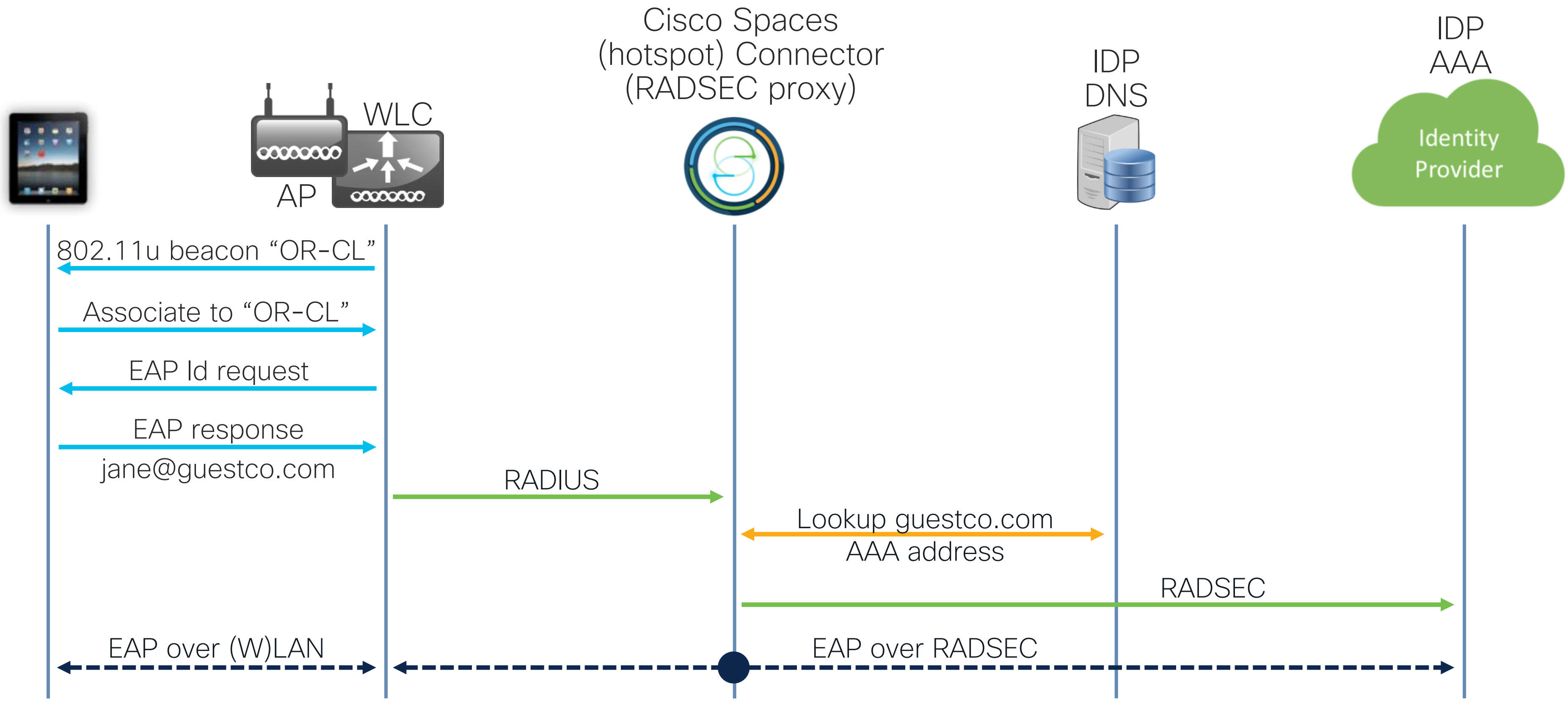
Identity Federation

<

Identity Providers

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

OpenRoaming



Cisco Spaces (hotspot) Connector (RADSEC proxy)

WLC

AP

IDP DNS

IDP AAA

802.11u beacon “OR-CL”

Associate to “OR-CL”

EAP Id request

EAP response jane@guestco.com

RADIUS

Lookup guestco.com AAA address

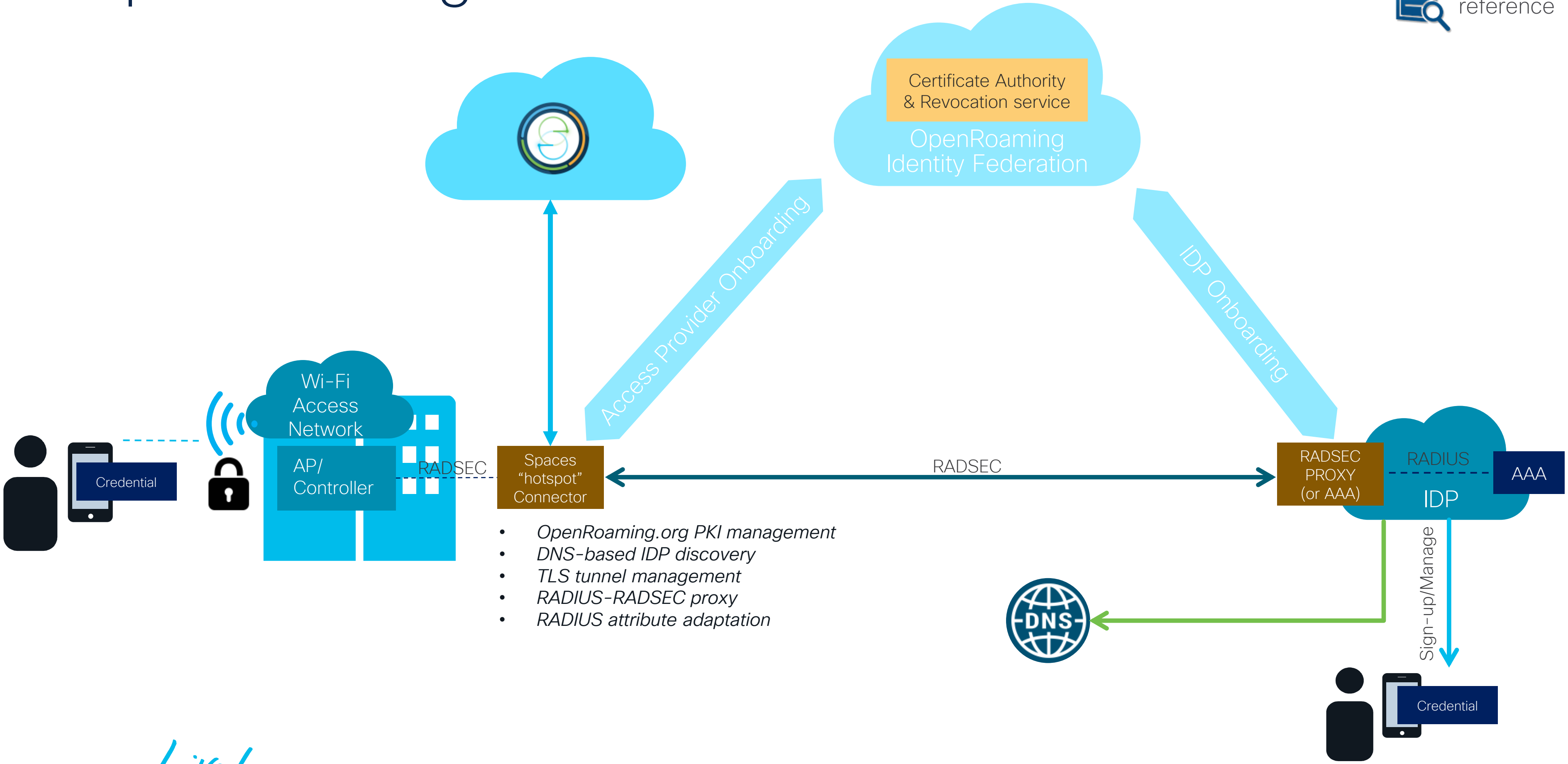
RADSEC

EAP over (W)LAN

EAP over RADSEC

OpenRoaming Architecture

For your reference



- *OpenRoaming.org PKI management*
- *DNS-based IDP discovery*
- *TLS tunnel management*
- *RADIUS-RADSEC proxy*
- *RADIUS attribute adaptation*

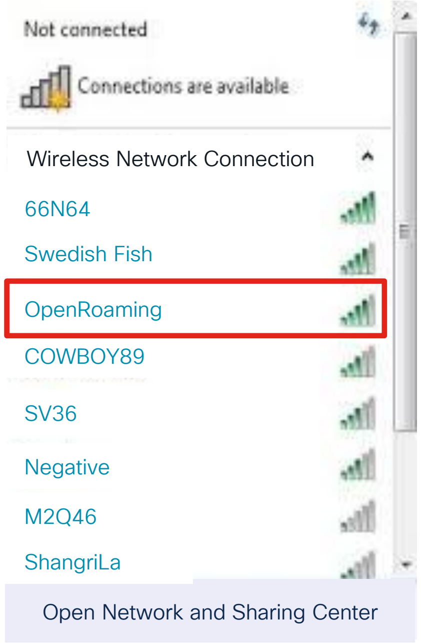
Prospected OpenRoaming user experience

1

User walks into a Starbucks, which is supported by OpenRoaming w/ Google as IDP.

Device Identifies SSID

2



Not connected

Connections are available

Wireless Network Connection

66N64

Swedish Fish

OpenRoaming

COWBOY89

SV36

Negative

M2Q46

ShangriLa

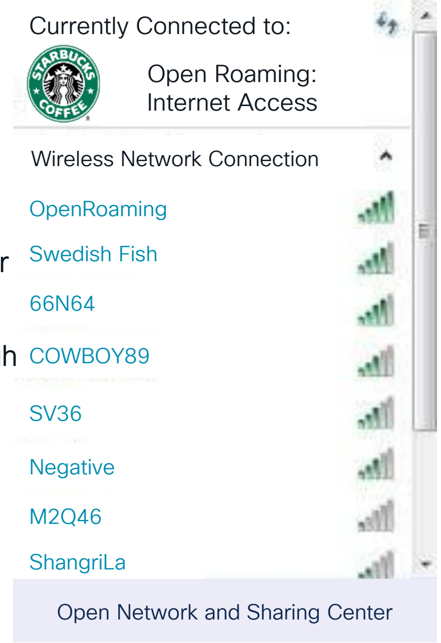
Open Network and Sharing Center

Zero-Touch by User

Authenticated through

Google

3



Currently Connected to:

Open Roaming:
Internet Access

Wireless Network Connection

OpenRoaming

Swedish Fish

66N64

COWBOY89

SV36

Negative

M2Q46

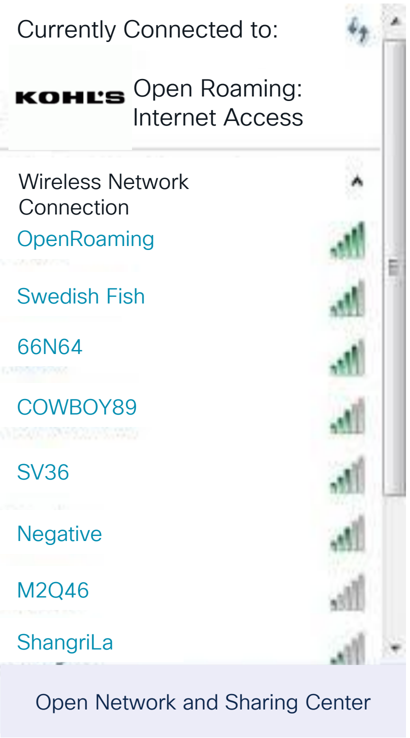
ShangriLa

Open Network and Sharing Center

Prospected OpenRoaming user experience

For your reference

4



Currently Connected to:

KOHL'S Open Roaming: Internet Access

Wireless Network Connection

- OpenRoaming
- Swedish Fish
- 66N64
- COWBOY89
- SV36
- Negative
- M2Q46
- ShangriLa

Open Network and Sharing Center

5

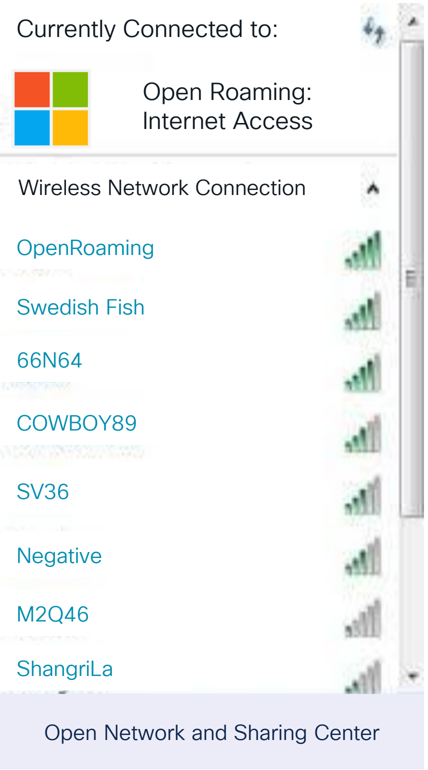
User walks onto the Microsoft campus, which only will authenticate using LinkedIn in OpenRoaming.

Zero-Touch by User

Authenticated through LinkedIn

since LinkedIn was added previously to their profile

6



Currently Connected to:

Open Roaming: Internet Access

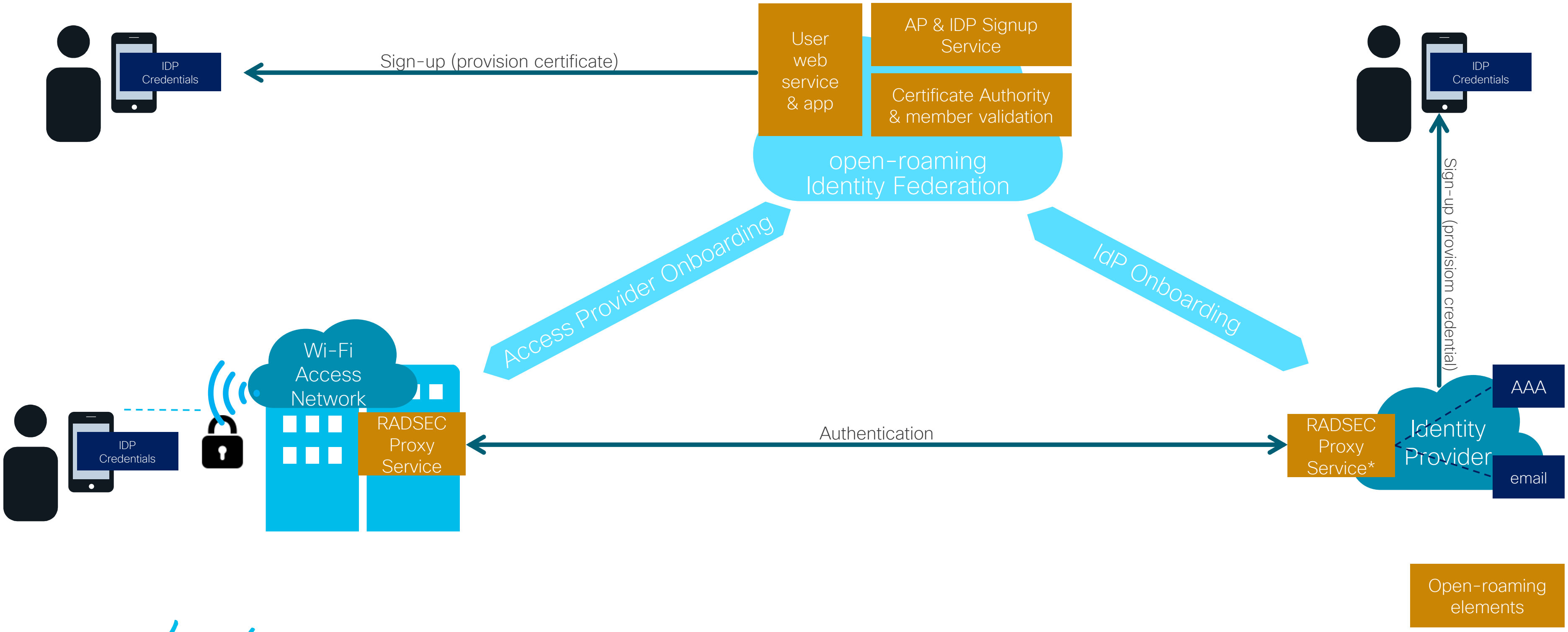
Wireless Network Connection

- OpenRoaming
- Swedish Fish
- 66N64
- COWBOY89
- SV36
- Negative
- M2Q46
- ShangriLa

Open Network and Sharing Center

Device Provisioning

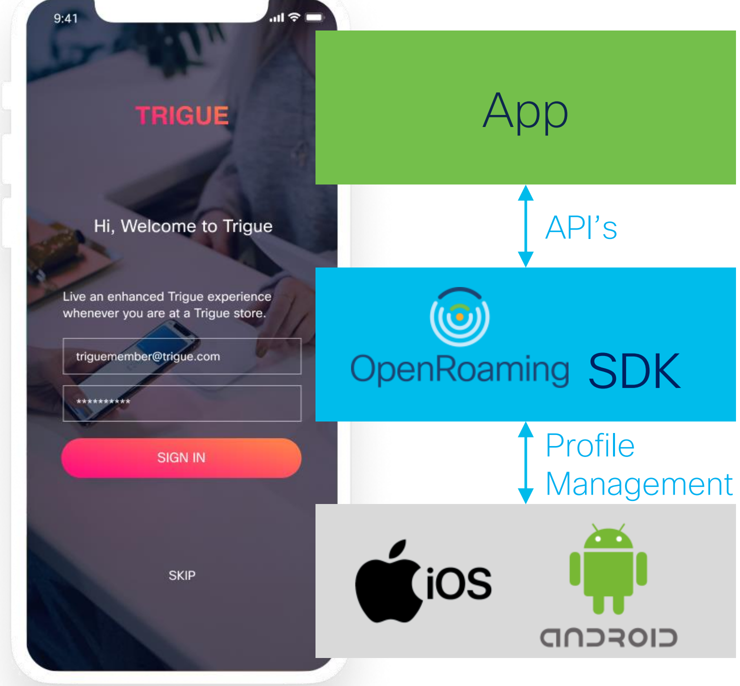
For your reference



OpenRoaming Mobile App, or Your Own

- OpenRoaming app: iOS and Android
- Sign in through the available cloud IDPs: Apple ID and Google Account

Build your own


9:41

TRIGUE

Hi, Welcome to Trigue

Live an enhanced Trigue experience whenever you are at a Trigue store.

triguemember@trigue.com

****

SIGN IN

SKIP

https://developer.cisco.com/dna-spaces-sdk/

Advanced settings for better end user experience

Wi-Fi Certified Enhanced Open

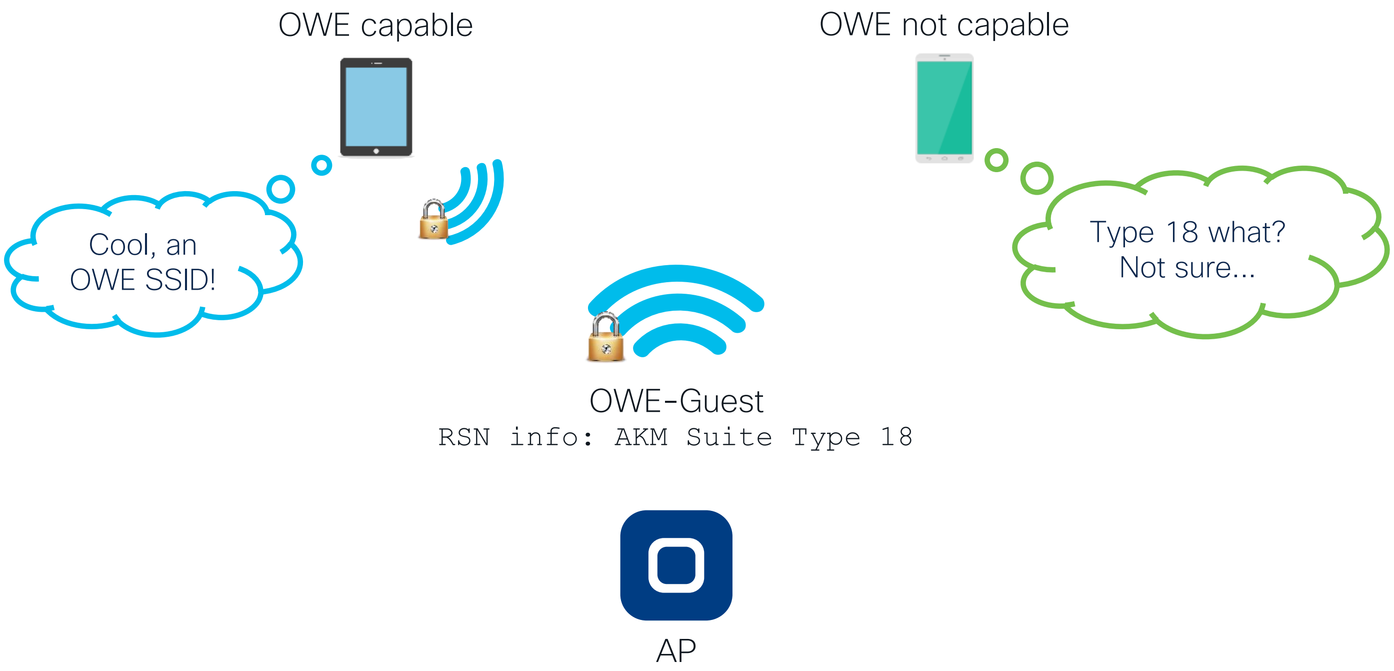
The next generation of hotspot security

- Another WFA certification (not part of WPA3), mostly for hotspots.
- Based on Opportunistic Wireless Encryption (OWE): APs and clients automatically negotiate encryption.
- It prevents passive attacks (i.e., traffic visibility).

⚠ Endpoints not supporting Enhanced Open might not correctly see/connect to an SSID with Enhanced Open configured.
But...

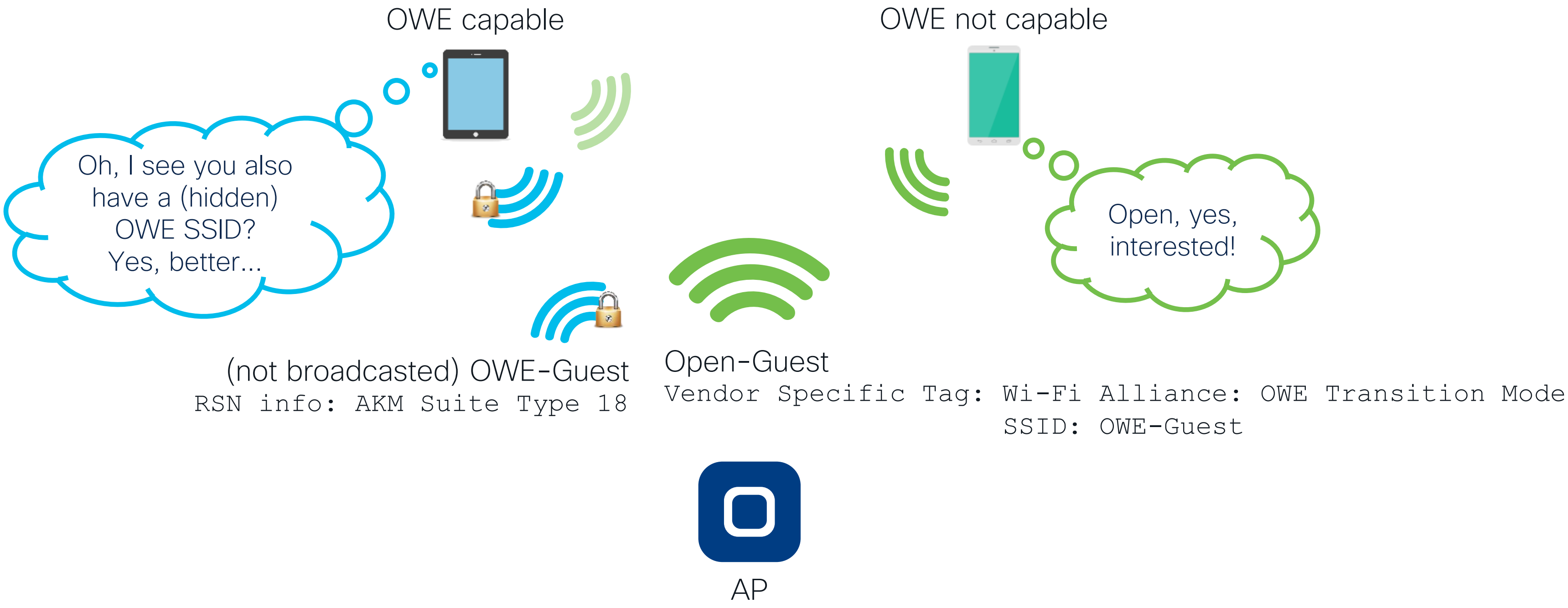
Wi-Fi Certified Enhanced Open

OWE Transition Mode to the “rescue”



Wi-Fi Certified Enhanced Open

OWE Transition Mode to the “rescue”



OWE capable

OWE not capable

Oh, I see you also have a (hidden) OWE SSID? Yes, better...

Open, yes, interested!

(not broadcasted) OWE-Guest

```
RSN info: AKM Suite Type 18
```

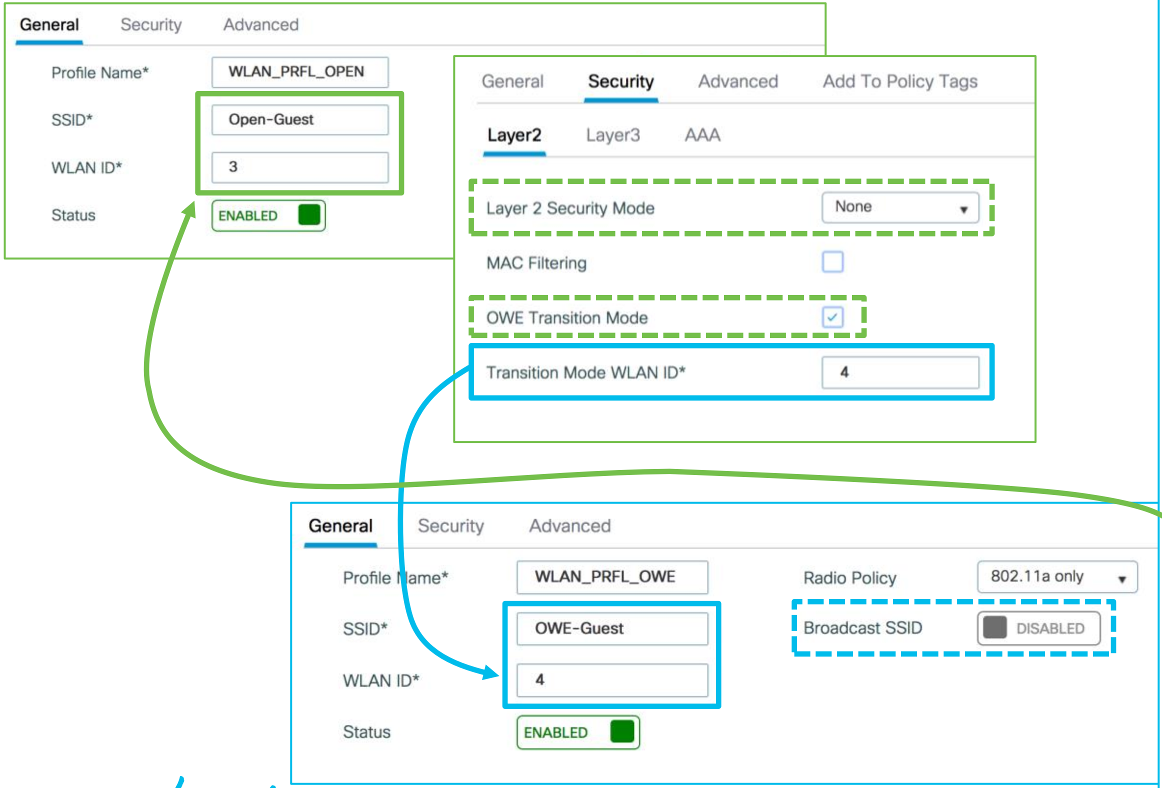
Open-Guest

```
Vendor Specific Tag: Wi-Fi Alliance: OWE Transition Mode
                     SSID: OWE-Guest
```

AP

Wi-Fi Certified Enhanced Open

OWE Transition Mode to the “rescue”



General | Security | Advanced

Profile Name*: WLAN_PRFL_OPEN

SSID*: Open-Guest

WLAN ID*: 3

Status: ENABLED

General | Security | Advanced | Add To Policy Tags

Layer2 | Layer3 | AAA

Layer 2 Security Mode: None

MAC Filtering: □

OWE Transition Mode: ☑

Transition Mode WLAN ID*: 4

General | Security | Advanced

Profile Name*: WLAN_PRFL_OWE

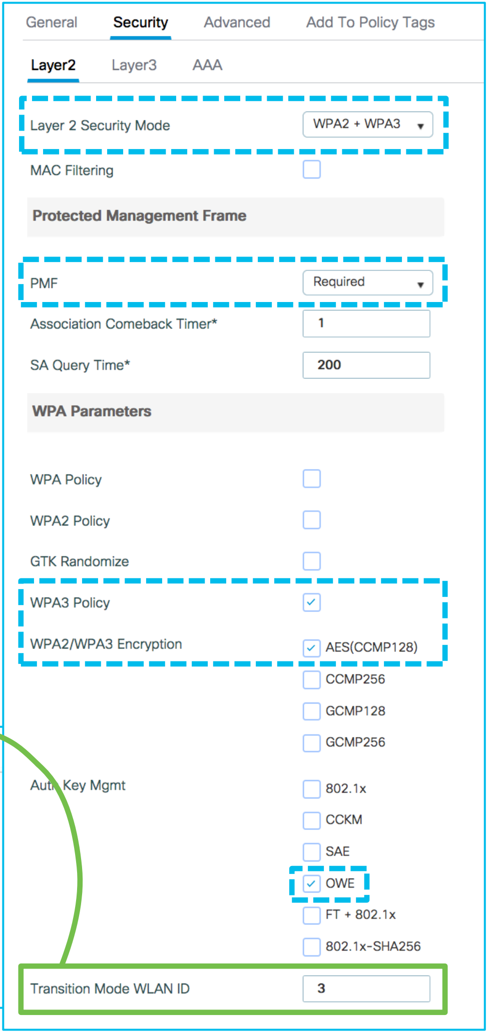
SSID*: OWE-Guest

WLAN ID*: 4

Status: ENABLED

Radio Policy: 802.11a only

Broadcast SSID: DISABLED



General | Security | Advanced | Add To Policy Tags

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: □

GTK Randomize: □

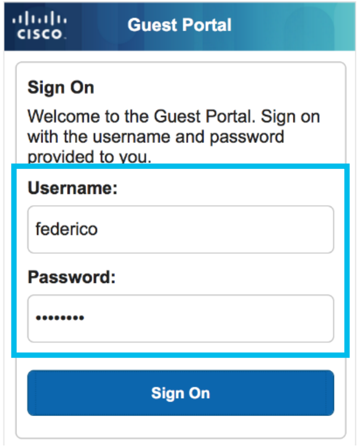
WPA3 Policy: ☑

WPA2/WPA3 Encryption: ☑ AES(CCMP128) □ CCMP256 □ GCMP128 □ GCMP256

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

Transition Mode WLAN ID: 3

Guest Experts don’t change VLAN (CWA)



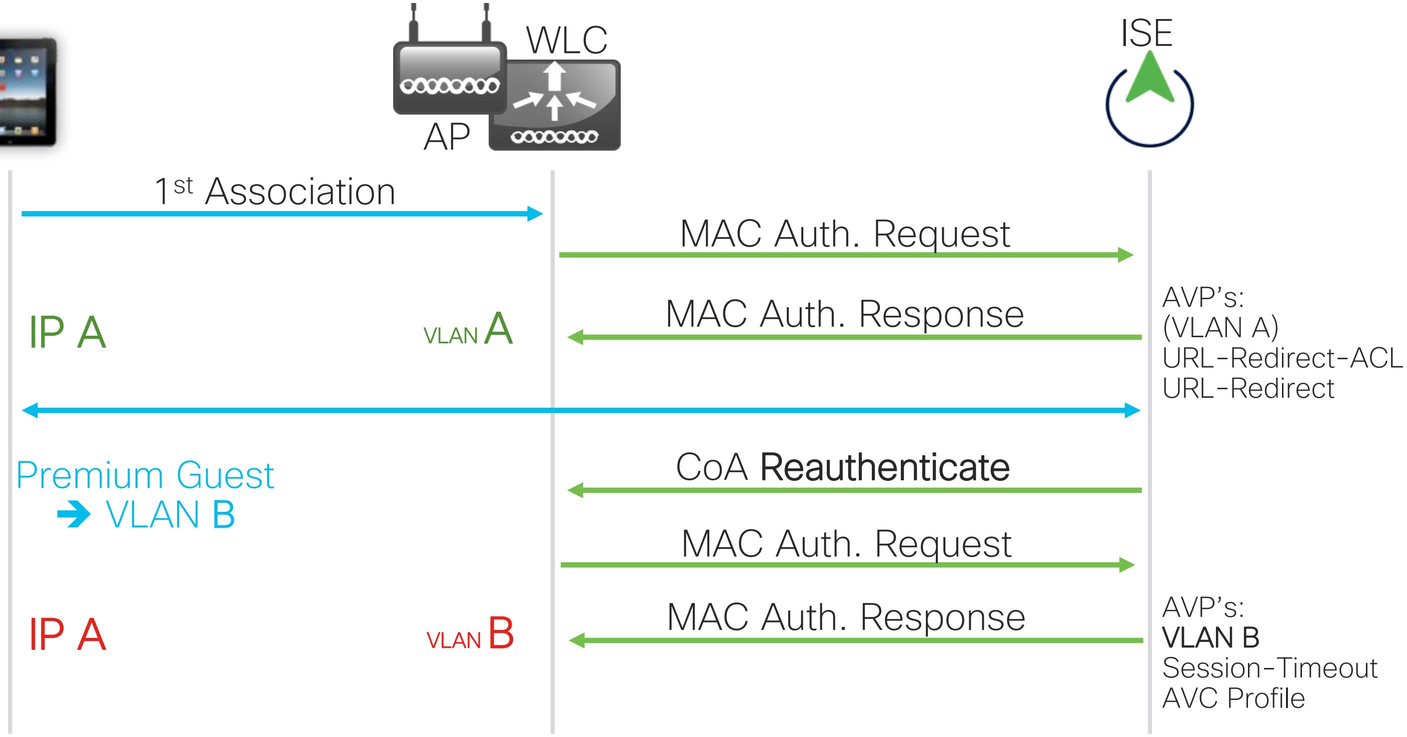
Guest Portal

Sign On

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

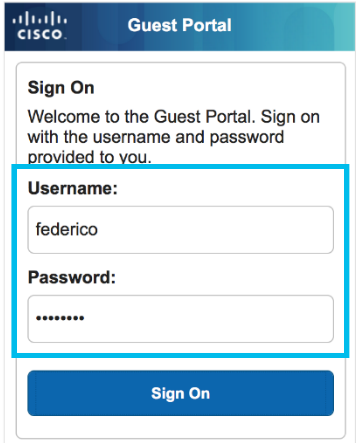
Username: federico

Password: ••••••••



Guest Experts don't change VLAN (CWA)

For your reference



Guest Portal

Sign On

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

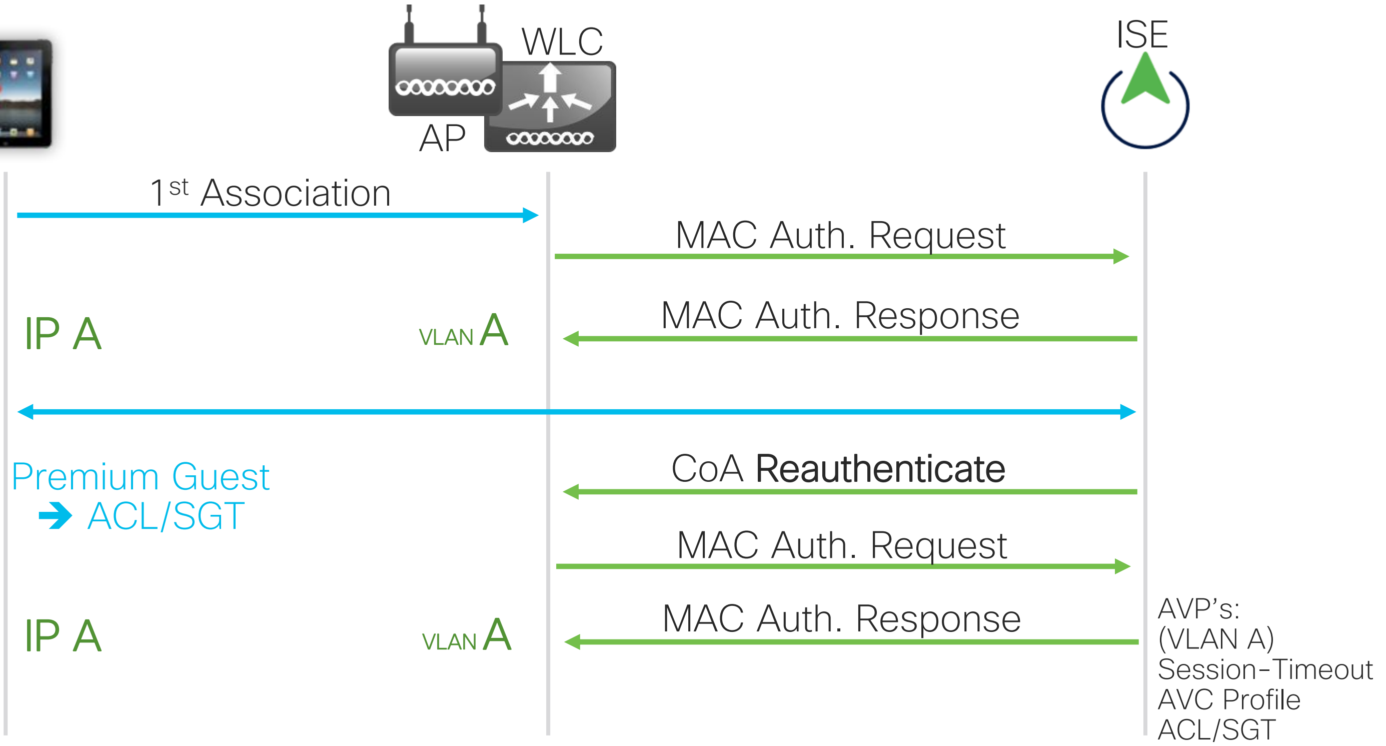
Username:

federico

Password:

••••••••

Sign On



WLC

AP

ISE

1st Association

MAC Auth. Request

IP A

VLAN A

MAC Auth. Response

Premium Guest

➔ ACL/SGT

CoA **Reauthenticate**

MAC Auth. Request

IP A

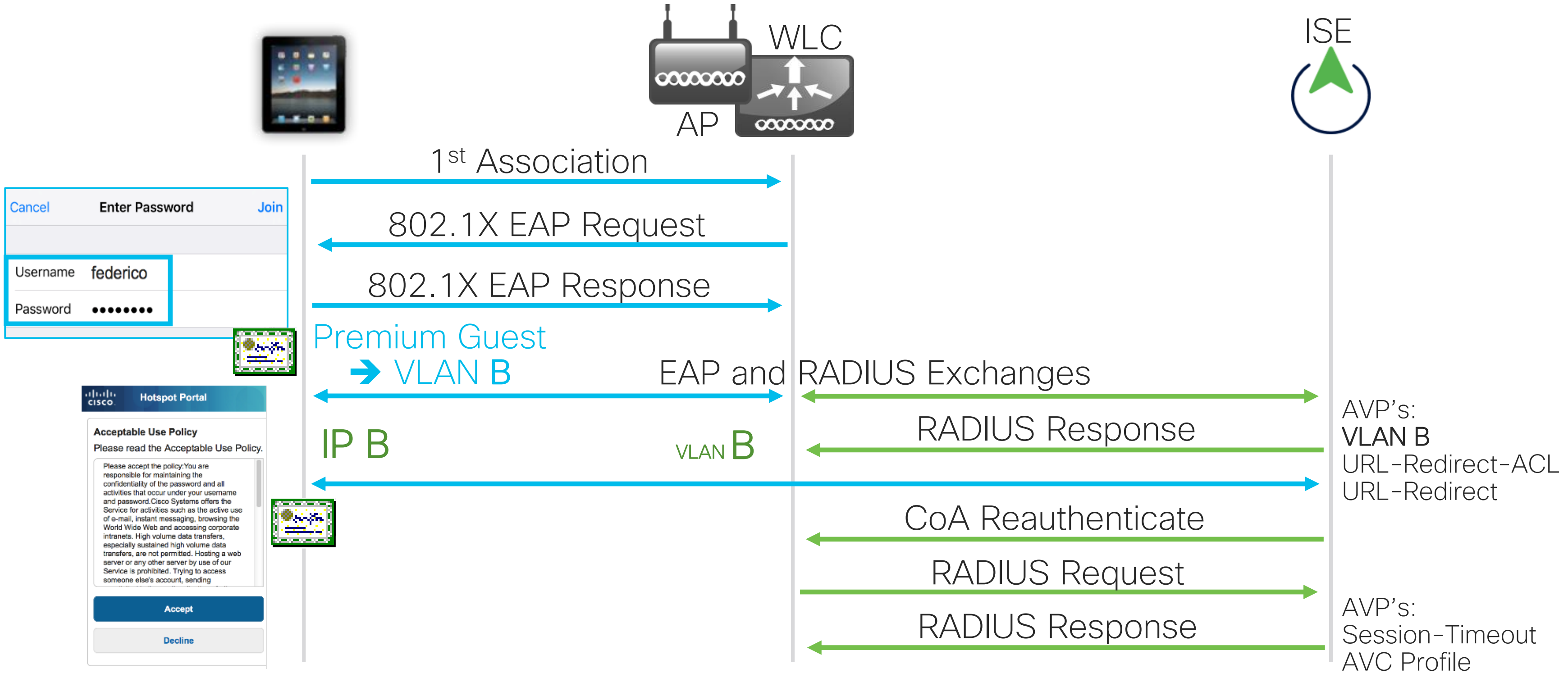
VLAN A

MAC Auth. Response

AVP's:
(VLAN A)
Session-Timeout
AVC Profile
ACL/SGT

Guest Experts sometime change VLAN (CWA)

For your reference



Username federico

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

AVP's:
VLAN B
URL-Redirect-ACL
URL-Redirect

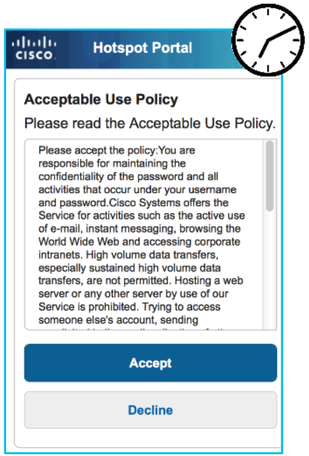
AVP's:
Session-Timeout
AVC Profile

Timeouts and caching the endpoint’s session

CWA example

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

Webauth Init



Hotspot Portal

Acceptable Use Policy

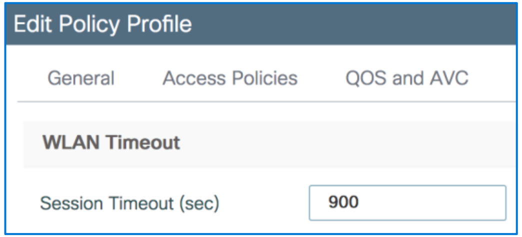
Please read the Acceptable Use Policy.

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
WLC
AP

ISE



WLAN Timeout

Session Timeout (sec): 900

Session Timeout

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

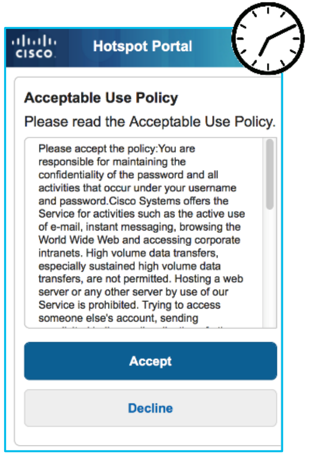
```
Access Type = ACCESS_ACCEPT
Filter-ID = ACL_PUBLIC_INTERNET
Session-Timeout = 36000
```

Timeouts and caching the endpoint's session

CWA example

Endpoints that went through a portal can be "cached" in ISE by registering their MACs in an Identity Group to be used in the authZ policy, so to go through the portal just once every X days/weeks/months.

Webauth Init

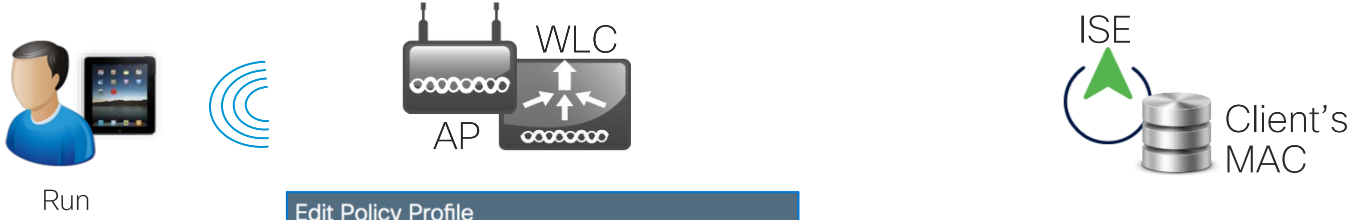


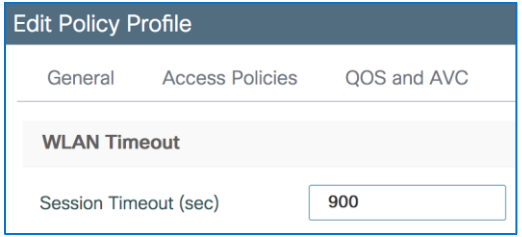
Hotspot Portal

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





Edit Policy Profile

WLAN Timeout

Session Timeout (sec): 900

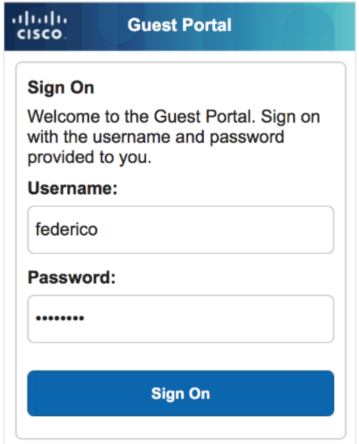
Access Type = ACCESS_ACCEPT

Filter-ID = ACL_PUBLIC_INTERNET

Session-Timeout = 36000

Session Timeout

What if the MAC address keeps changing?



Guest Portal

Sign On

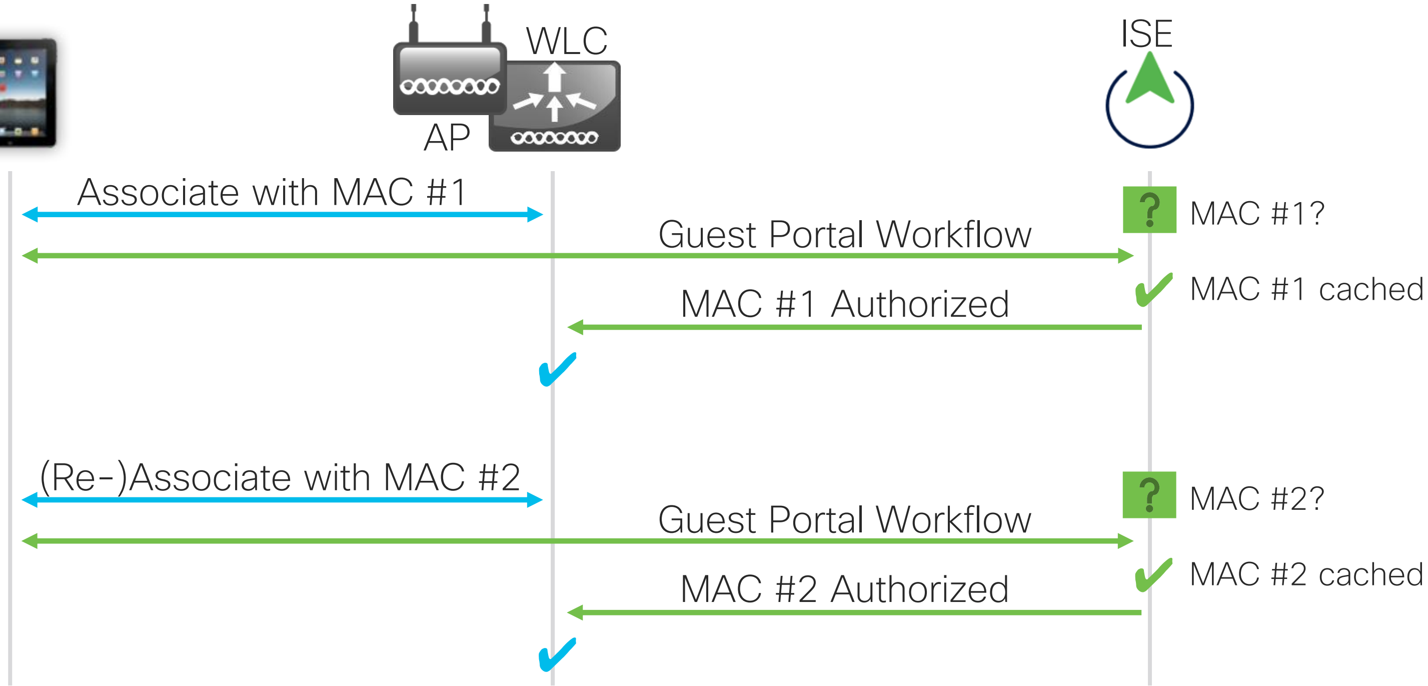
Welcome to the Guest Portal. Sign on with the username and password provided to you.

Username:

federico

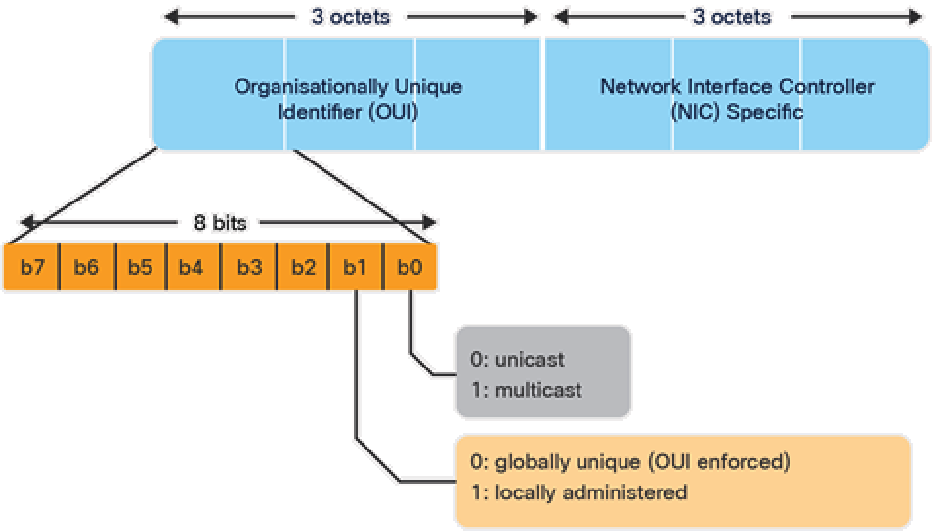
Password:

••••••••



No matter the web auth technique (LWA or CWA) or the guest portal solution that we choose (WLC's internal portal, Cisco Spaces, ISE, 3rd party non-Cisco solution, etc.)

Locally administered (a.k.a., randomized) MAC


3 octets
3 octets
Organisationally Unique Identifier (OUI)
Network Interface Controller (NIC) Specific
8 bits
b7
b6
b5
b4
b3
b2
b1
b0
0: unicast
1: multicast
0: globally unique (OUI enforced)
1: locally administered

- 32-28-6D-51-13-AF
- 56-EF-68-F6-0D-30
- 0A-13-A8-8E-B5-EF
- AE-83-37-55-A7-22

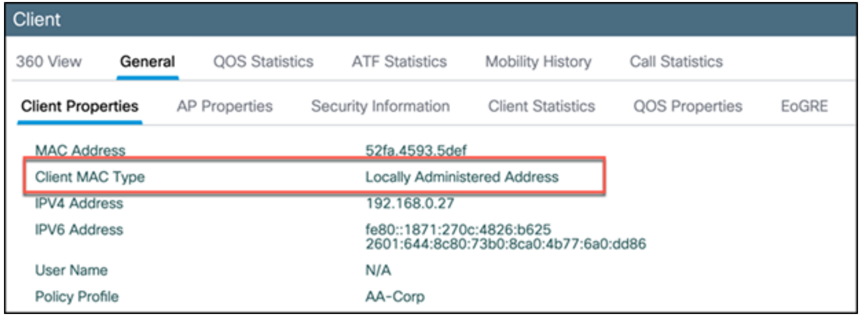
So far…

- Windows
  - Randomization disabled by default
  - Once a random MAC is generated for an SSID, the endpoint keeps using it until deletion of the SSID
  - Can be configured to use a different randomized MAC every day
- Android
  - Randomization enabled by default
  - Android 10 and 11, the same randomized MAC is used for the same SSID, even if deleted/re-added
  - Android 12, under some frequent conditions a new randomized MAC is generated for every new association
- Apple
  - Randomization enabled by default
  - Once a random MAC is generated for an SSID, the endpoint keeps using it until deletion of the SSID

What options do we have?

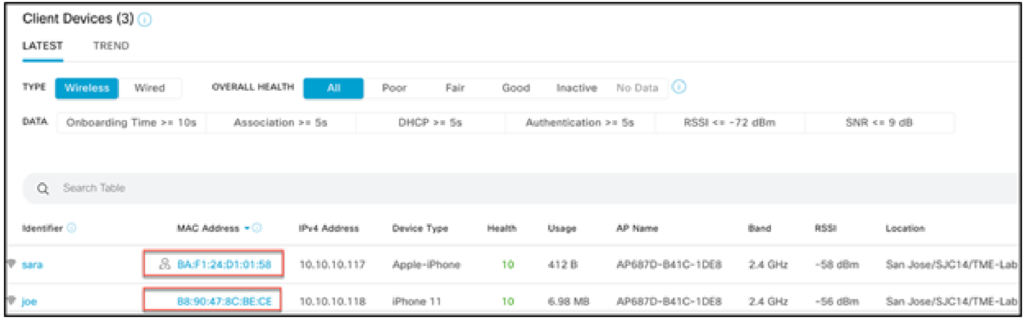
1. Let it be and monitor

On the 9800, starting from IOS-XE 17.5.1, under the endpoint's details



MAC Address	52fa.4593.5def
Client MAC Type	Locally Administered Address
IPV4 Address	192.168.0.27
IPV6 Address	fe80::1871:270c:4826:b625 2601:644:8c80:73b0:8ca0:4b77:6a0:dd86
User Name	N/A
Policy Profile	AA-Corp

On DNAC, starting from 2.2.3, in the clients list and AI Endpoint Analytics too



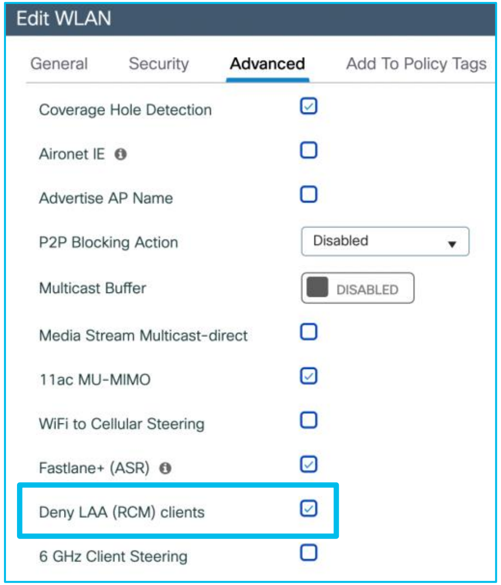
Identifier	MAC Address	IPv4 Address	Device Type	Health	Usage	AP Name	Band	RSSI	Location
sara	BA:F1:24:D1:01:58	10.10.10.117	Apple-iPhone	10	412 B	AP687D-B41C-1DE8	2.4 GHz	-58 dBm	San Jose/SJC14/TME-Lab
joe	B8:90:47:8C:BE:CE	10.10.10.118	iPhone 11	10	6.98 MB	AP687D-B41C-1DE8	2.4 GHz	-56 dBm	San Jose/SJC14/TME-Lab

What options do we have?

1. Let it be and monitor

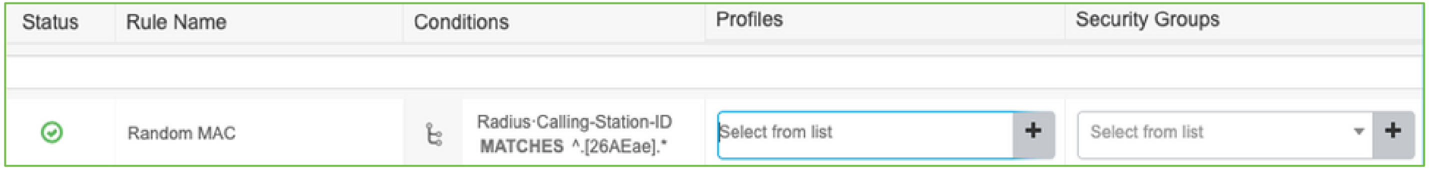
2. Block randomized MACs
   - On the 9800, starting from IOS-XE 17.5.1 (the randomized MAC cannot even associate)
   - On ISE, with an authC/authZ condition (the randomized MAC gets past association)
     `Calling-Station-ID MATCHES ^.[26AEae].*`

WLAN Profile > Advanced > Deny LAA (RCM) clients



Edit WLAN

- Coverage Hole Detection ☑
- Aironet IE ☐
- Advertise AP Name ☐
- P2P Blocking Action: Disabled
- Multicast Buffer: DISABLED
- Media Stream Multicast-direct ☐
- 11ac MU-MIMO ☑
- WiFi to Cellular Steering ☐
- Fastlane+ (ASR) ☑
- Deny LAA (RCM) clients ☑
- 6 GHz Client Steering ☐



Status	Rule Name	Conditions	Profiles	Security Groups
✓	Random MAC	Radius·Calling-Station-ID MATCHES ^.[26AEae].*	Select from list +	Select from list +

What options do we have?

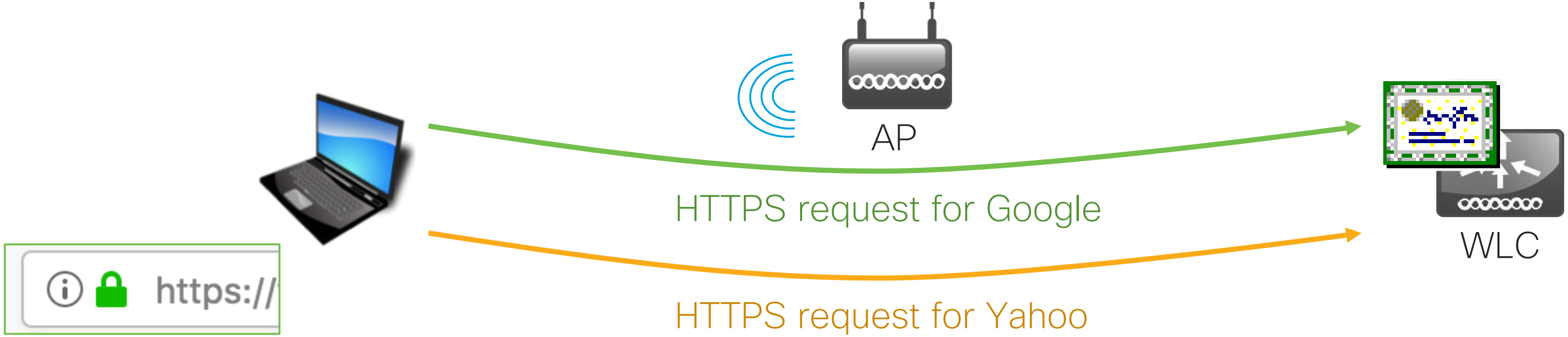
1. Let it be and monitor

2. Block randomized MACs

3. Force disabling randomized MACs through an MDM solution (more adapted to enterprise/BYOD use cases)

More details:
https://www.cisco.com/c/en/us/products/collateral/wireless/randomized-changing-mac-dg.html
and
https://community.cisco.com/t5/security-knowledge-base/random-mac-address-how-to-deal-with-it-using-ise/ta-p/4049321

Guest portal redirection with HTTPS pages



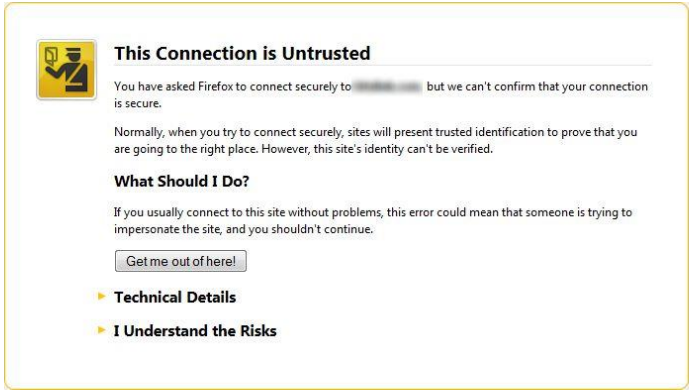
AP

HTTPS request for Google

HTTPS request for Yahoo

WLC

https://



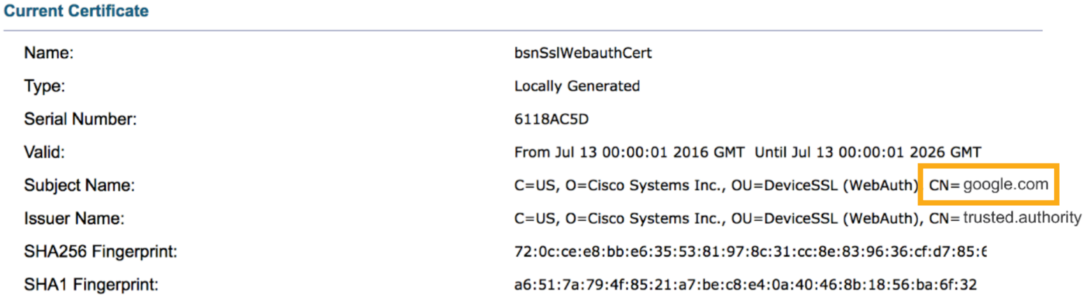
This Connection is Untrusted

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.

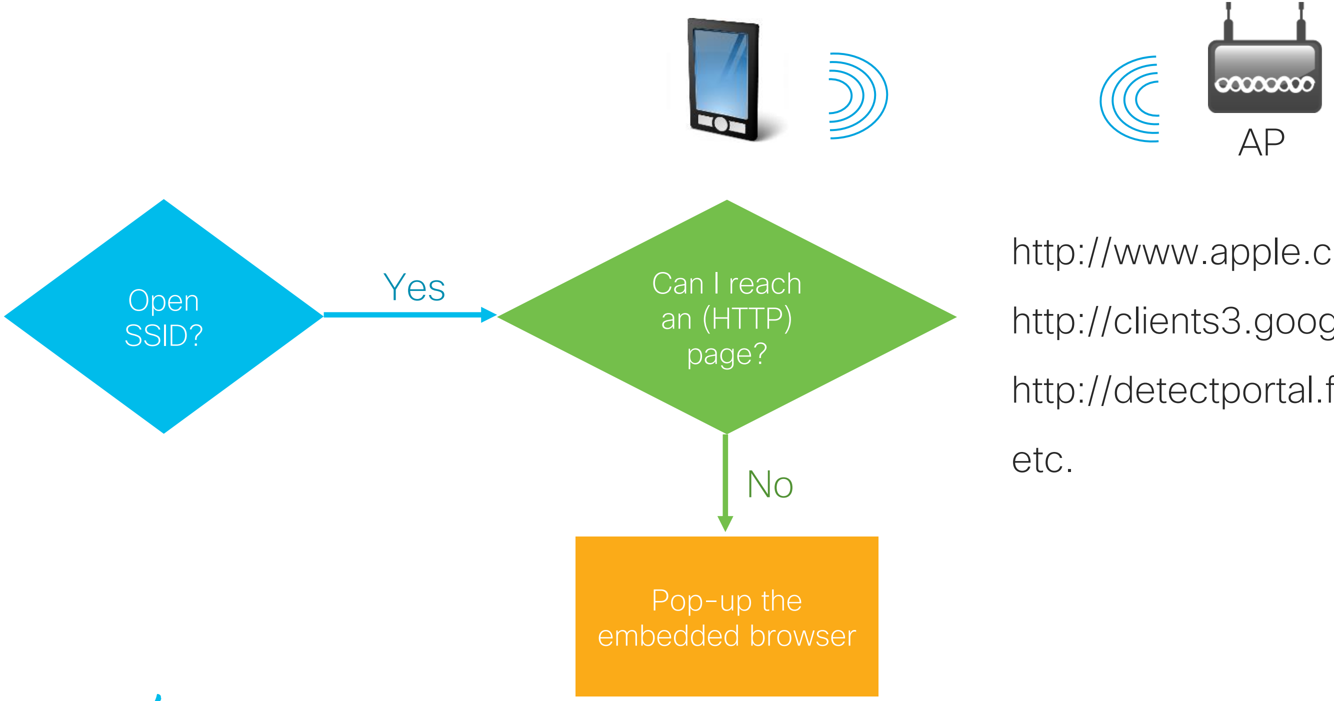


Current Certificate

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

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



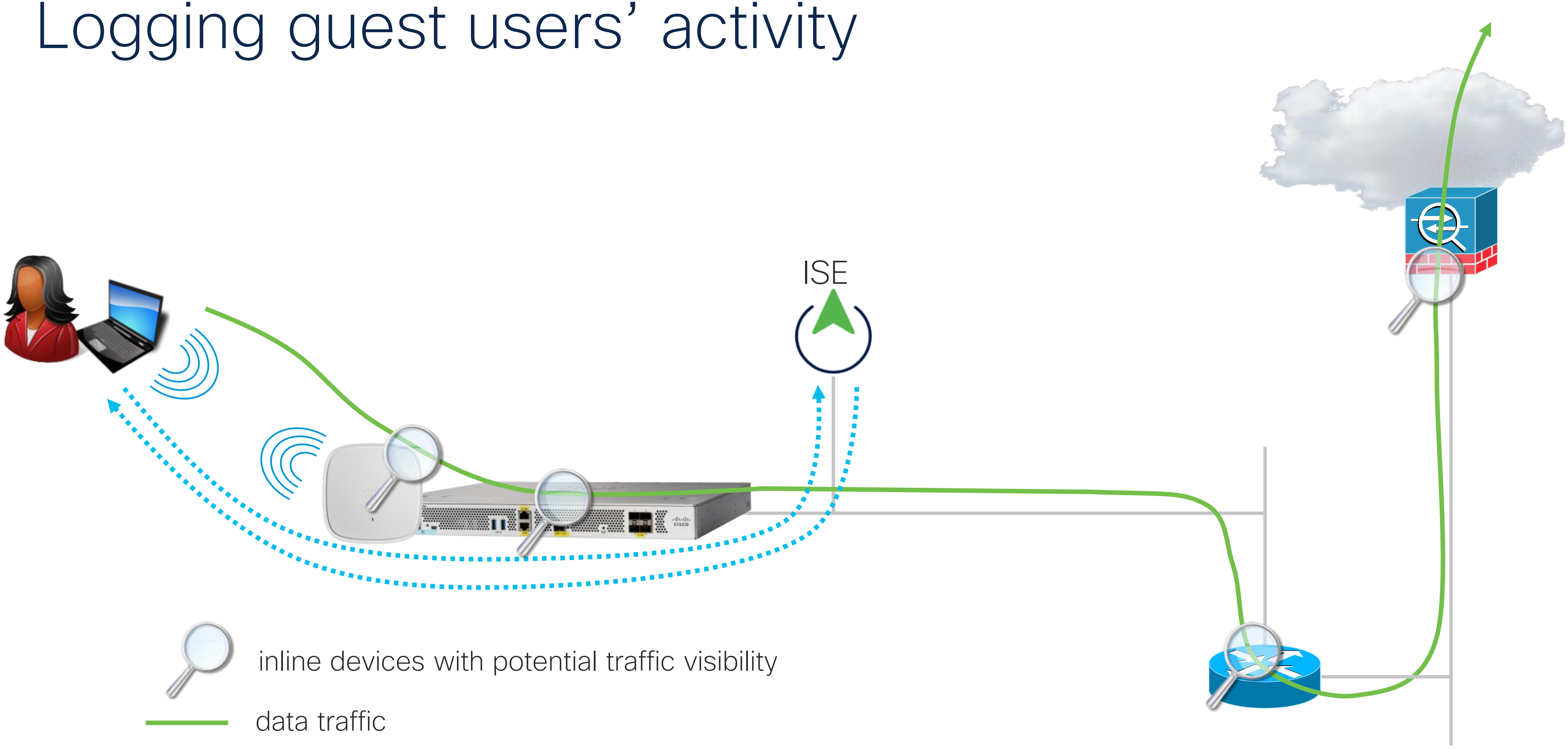
http://www.apple.com/library/test/success.html

http://clients3.google.com/generate_204

http://detectportal.firefox.com

etc.

Logging guest users' activity

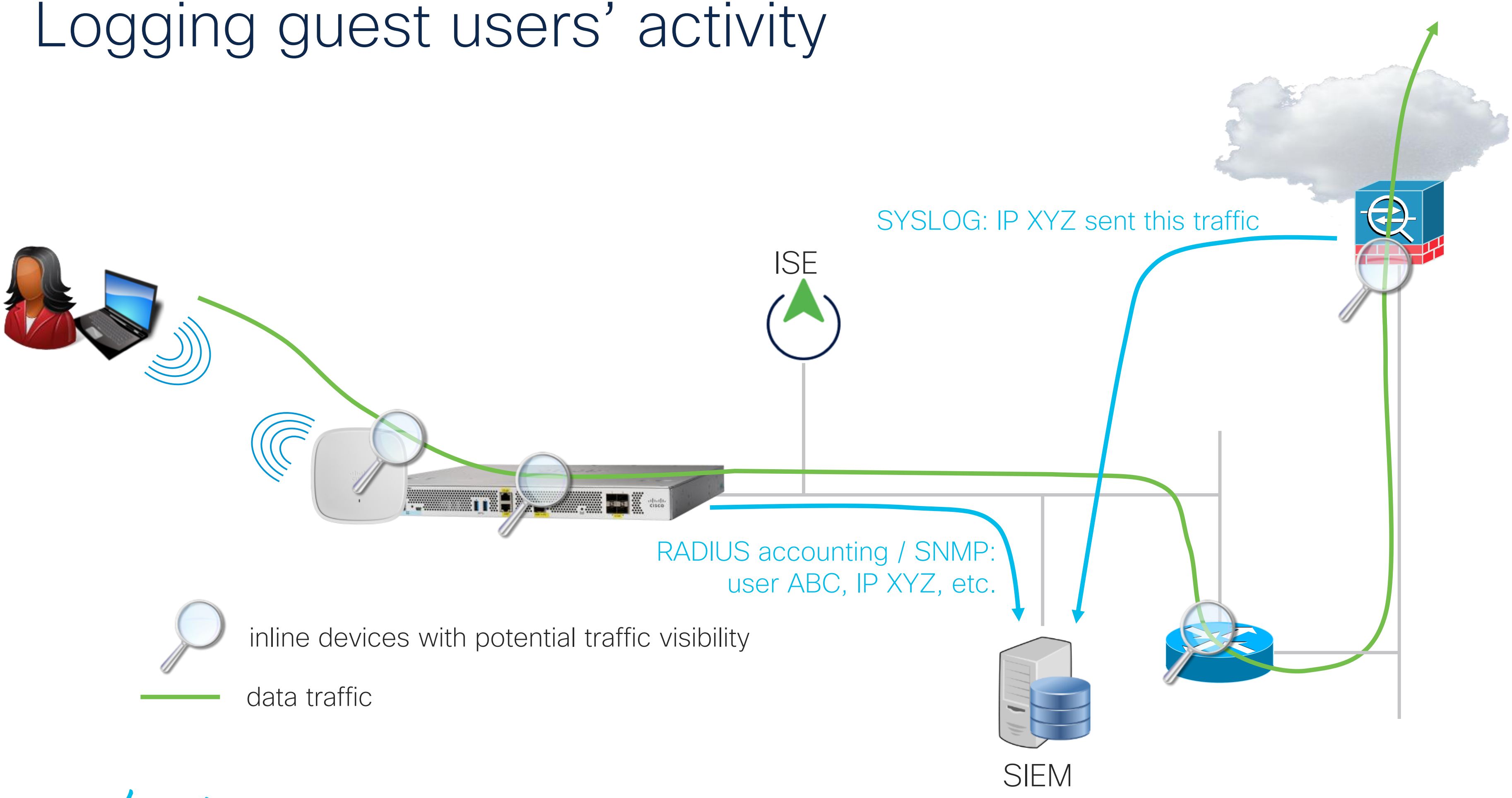


inline devices with potential traffic visibility

🟩 data traffic

▪▪▪▪▪ web portal traffic

Logging guest users' activity



SYSLOG: IP XYZ sent this traffic

ISE

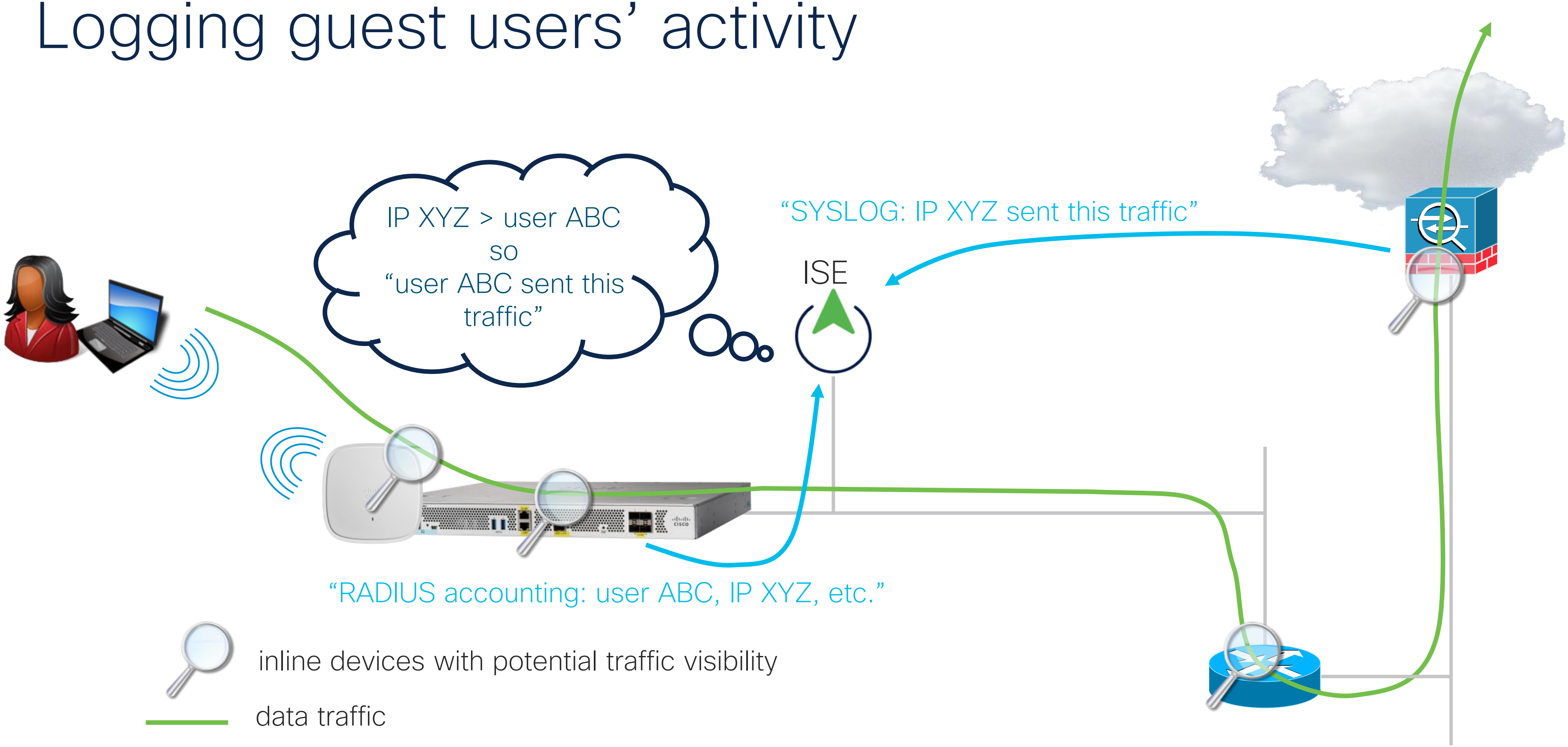
RADIUS accounting / SNMP:
user ABC, IP XYZ, etc.

SIEM

inline devices with potential traffic visibility

data traffic

Logging guest users’ activity



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

It's never too late to read the guide

For your reference

LTRWEN-2724 Be My Guest: Designing and Troubleshooting Wireless Guest Networks with Catalyst 9800 Wireless Controller
https://www.ciscolive.com/emea/learn/sessions/session-catalog.html?search=LTREWN-2724#/

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

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

The path of a guest (rock)star

Understanding the environment/use case

Mastering tools and options

Caring for end users/visitors

Complete your 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 (open from 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 Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

- Visit the Cisco Showcase for related demos.
- Book your one-on-one Meet the Engineer meeting.
- Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

The bridge to possible

Thank you

cisco Live!