



# Voice of the Engineer

Deep Dive Series: Web Authentication, Guest and Device Registration

# Voice of the Engineer

## Solutions approach to partner training

- Partner Enablement through series of WebEx Training Sessions
- Basics are introductory sessions open to AM, SE, FE
- Deep Dives are Field Engineer focus
  - Deployment information from the Experts for the Experts
- Recordings and Slides will be Archived on the Partner Community
- Voice of the Engineer – Deep Dives
  - <https://communities.cisco.com/docs/DOC-30977>
- Voice of the Engineer – Basics
  - <https://communities.cisco.com/docs/DOC-30718>

# Voice of the Engineer – Deep Dives

<https://communities.cisco.com/docs/DOC-30977>

- Identity Services Engine (ISE)
  - ✓ TrustSec & ISE Overview - 9/25/12
  - ✓ AAA, 802.1X, MAB - 10/9/12
  - ✓ ISE Profiling – 10/23/12
  - ✓ Web Auth, Guest & Device Registration – 11/6/12
  - ✓ Bring Your Own Device & EAP Chaining – 11/20/12
  - ✓ Posture & Security Group Access – 12/4/12
  - ✓ Best Practices – 12/18/12
  - ✓ **ISE TAC Tips: Processes, Planning, Live Troubleshooting – 1/8/13**
  - ✓ **ISE TAC Tips: Live Troubleshooting – 1/22/13**
- AnyConnect
  - ✓ AnyConnect VPN – 1/15/13
  - ✓ AnyConnect NAM – 1/29/13
  - ✓ AnyConnect Mobile – 2/12/13
  - ✓ Advanced AnyConnect Configuration – 2/26/13
  - ✓ AnyConnect TAC Tips – 3/12/13

# Agenda for Voice of the Engineer



TrustSec & ISE Overview



AAA, 802.1X, MAB



Profiling



→ Web Authentication, Guest & Device Registration



Bring your own Device & EAP-Chaining



Posture & SGA









Troubleshooting & Best Practices

# Web Authentication and Guest Services



# Agenda

-  Web Authentication
-  URL Redirection
-  Provisioning Guest Accounts
-  Guest Portals
-  Device Registration
-  Monitoring Guests

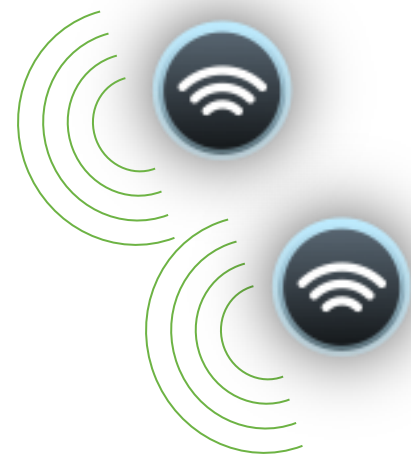
# Web Authentication



# Guest Access Needs



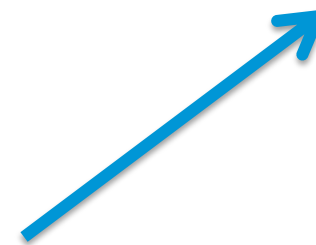
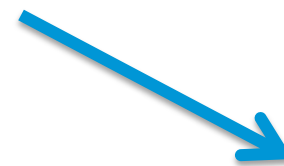
Guest authentication portal



Wireless Access Points



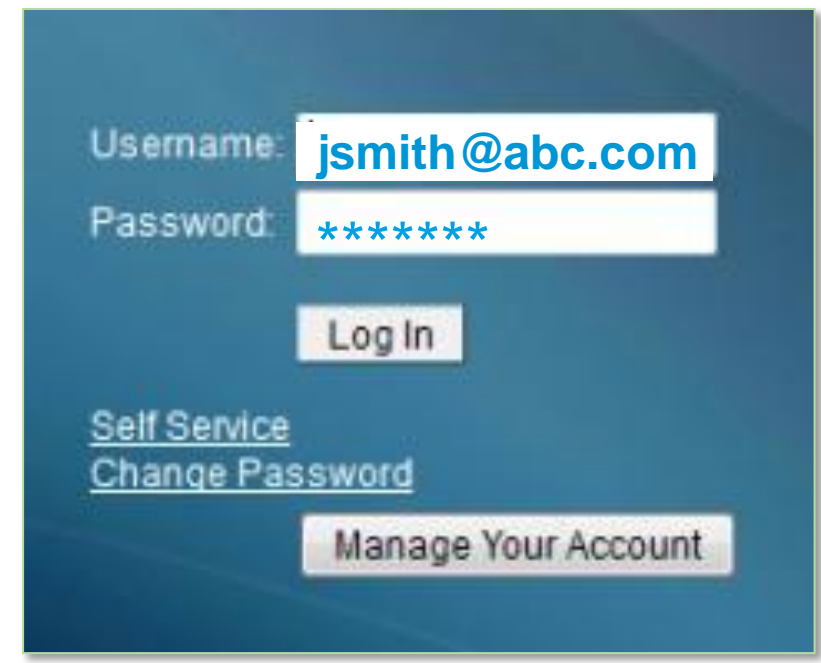
Internet





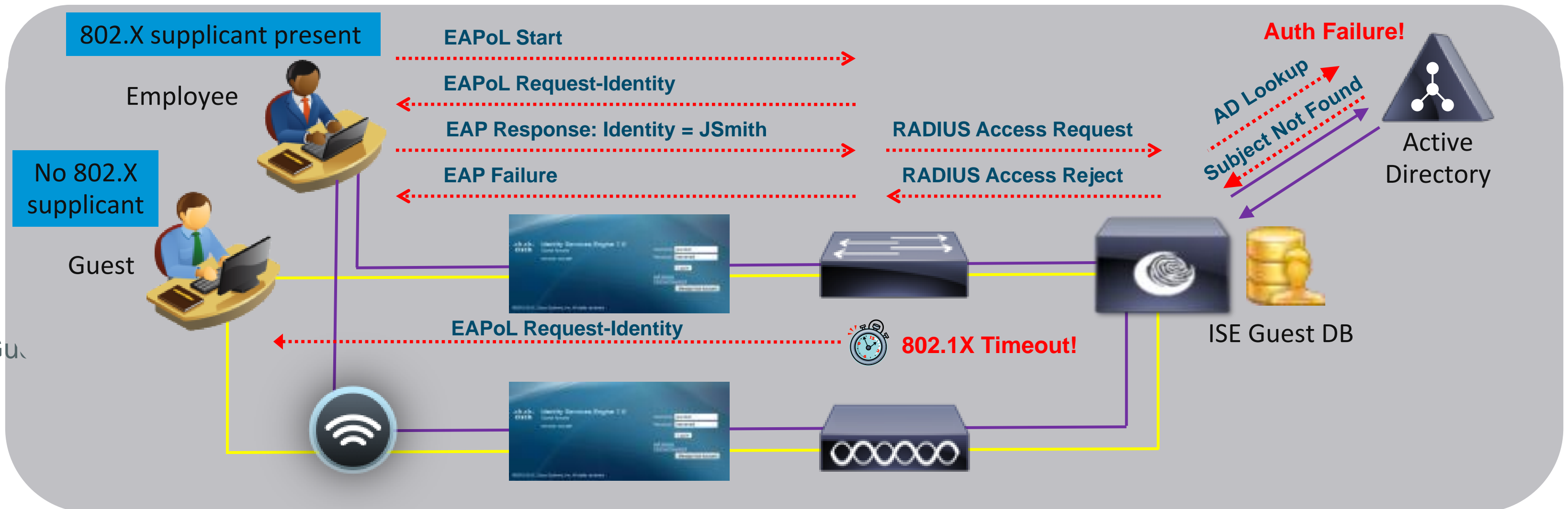
# Web Authentication Example

How Does it Work?



# Web Authentication for Guests/Employees

- Guests: Authenticate temporary/occasional users w/o 802.1X
- Employees: Provide permanent/frequent users fallback auth method if fail auth or 802.1X misconfigured



- ISE can use Identity Sequences to check the Local Guest Account repository → then Active Directory.
- ISE can assign different levels of access to Guest and Employee

# Web Auth Considerations

- Web Authentication is only for users (not devices)
  - Browser required
  - Manual entry of username/password
- Network equipment must intercept http/s requests and redirect to guest portal for authentication
- 2 ways to enforce on Cisco network access devices (WLC, switches)



## Local Web Auth (LWA)

Web auth done on the network device (web-auth feature on devices)

No CoA support

Authorization only with ACLs

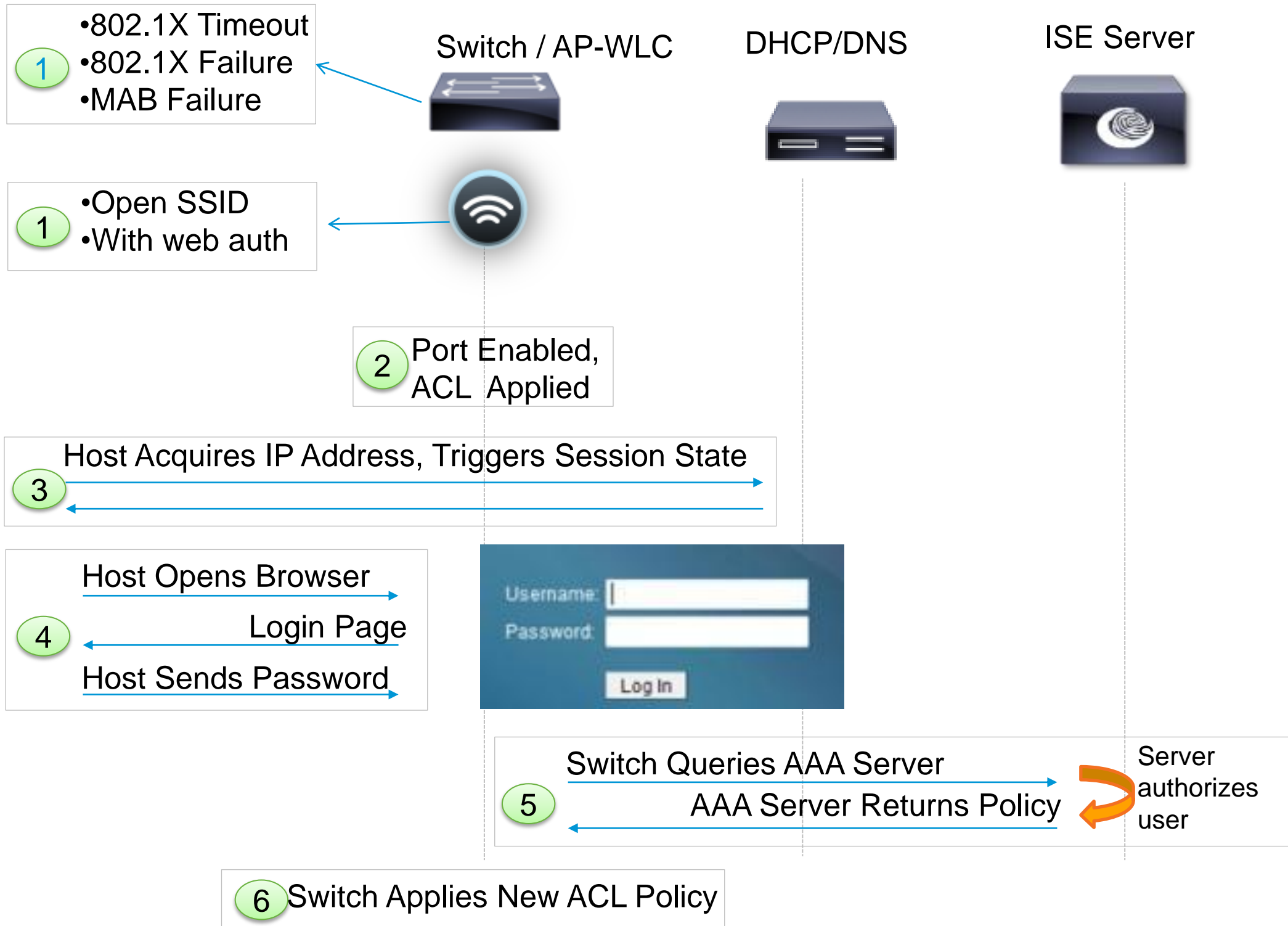
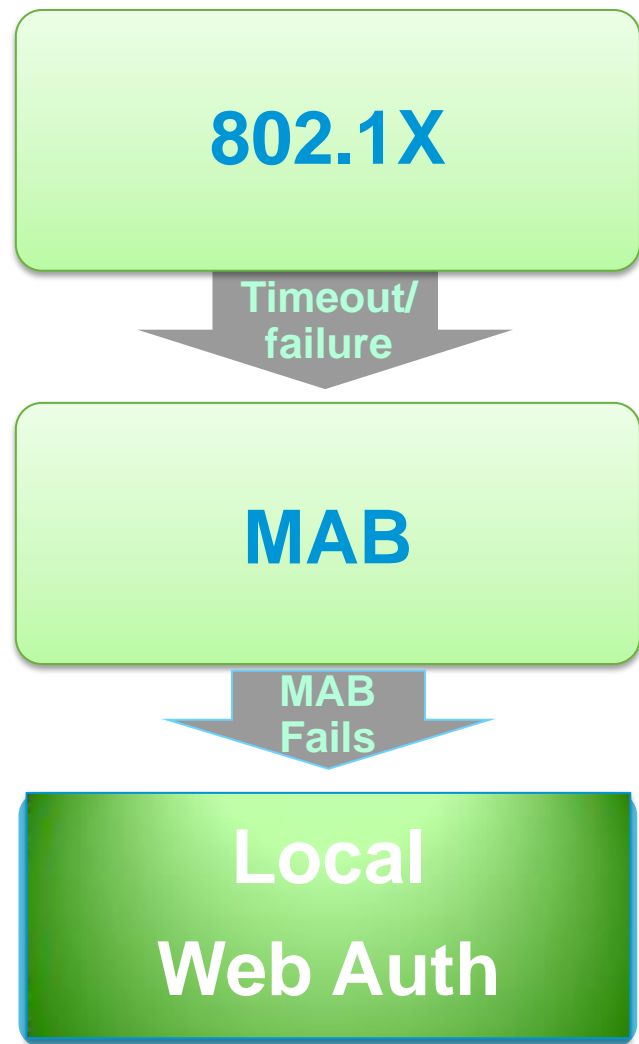
## Central Web Auth (CWA)

Web auth configuration pushed centrally

CoA support (for posture, profiling, ...)

Authorization can use VLAN or ACLs

# LWA – Session Flow



**Flex Auth:** After timeout or failure, port automatically tries “next-method” if another method configured.



# Wired LWA Config

```

ip admission name WEBAUTH proxy http
ip access-list extended PRE_AUTH_POLICY
 permit udp any any eq bootps
 permit udp any any eq domain
 fallback profile WEBAUTH_PROFILE
ip access-group PRE_AUTH_POLICY in
ip admission WEBAUTH
interface GigabitEthernet1/0/1
 authentication port-control auto
 authentication fallback WEBAUTH_PROFILE
 dot1x pae-authenticator
 mab
 authentication event fail action next-method
  
```

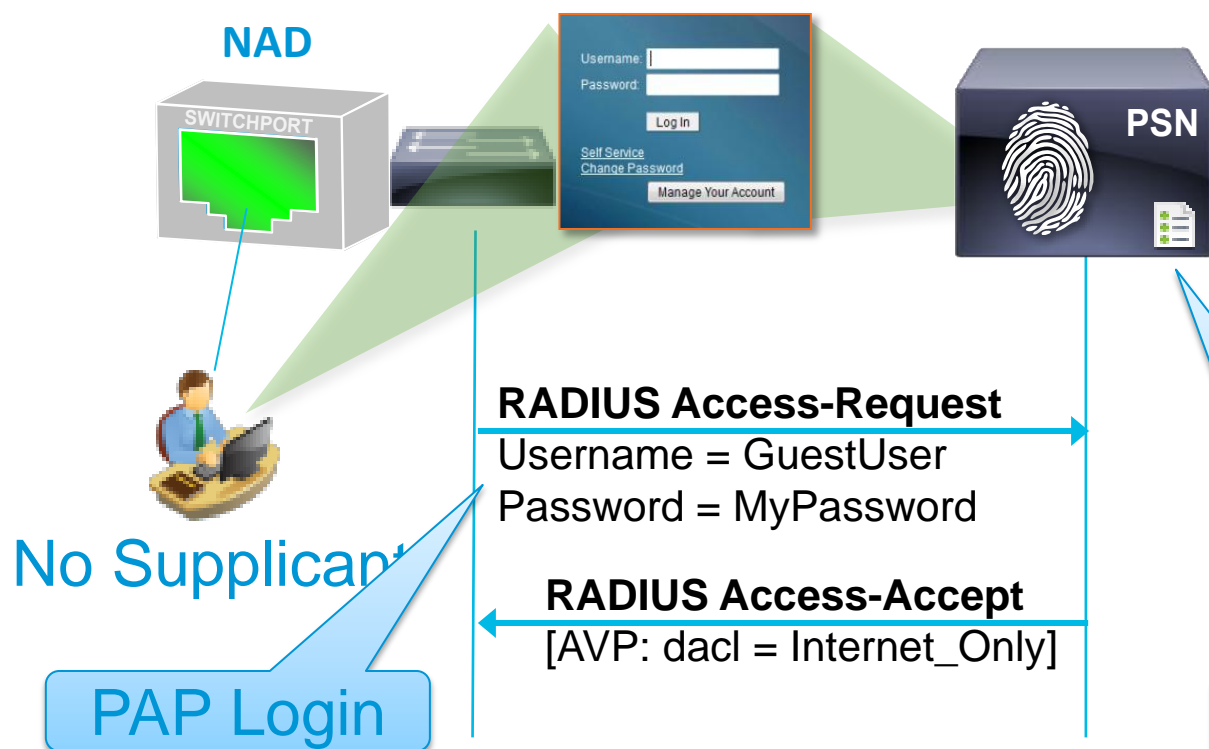
Matched AuthC Rule = LWA

## Authentication Policy

Status	Rule	Conditions	Identity Source
✓	MA	if Wired_MAB	then Internal Endpoints
✓	Do X	If Wired_802.1X	then AD1
✓	LWA	if RADIUS:Service-Type = Outbound RADIUS:NAS-Port-Type= Ethernet	then Internal Users
✓	Default	if <no match>	then AD1_Internal

## Authorization Policy

Status	Rule Name	Conditions	Permissions
✓	IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phone
✓	BYOD	if BYOD and Employee	then Employee
✓	Guest	if Guest	then Guest
✓	Contractor	if Contractor	then Contractor
✓	Employee	if Employee	then Employee
✓	Default	If no match then	WEBAUTH



Username matches

Matched AuthZ Rule = Guest

# Wireless LWA Config

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 3 Security None

Web Policy

Authentication

Passthrough

Conditional Web Redirect

Splash Page Web Redirect

On MAC Filter failure<sup>11</sup>

Preauthentication ACL ACL-WEBAUTH-REDIRECT

Over-ride Global Config  Enable

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

URL https://10.1.100.21:8443/guestportal/Login.action

Matched AuthC Rule = LWA

## Authentication Policy

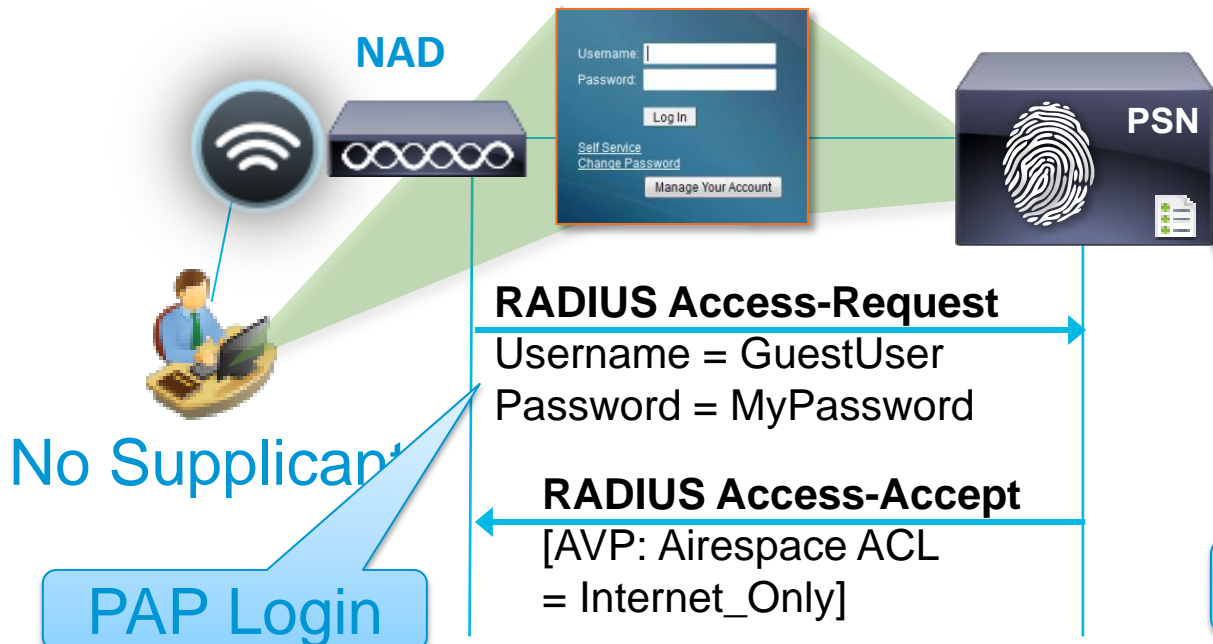
Status	Rule Name	Conditions	Identity Source
<input checked="" type="checkbox"/>	MAB	if Wired_MAB	then Internal Endpoints
<input checked="" type="checkbox"/>	Dot1X	If Wired_802.1X	then AD1
<input checked="" type="checkbox"/>	LWA	if RADIUS:Service-Type = Login RADIUS:NAS-Port-Type = Wireless – IEEE 802.11	then Internal Users
<input checked="" type="checkbox"/>	Default	if <no match>	then AD1_Internal

## Authorization Policy

Status	Rule Name	Conditions	Permissions
<input checked="" type="checkbox"/>	IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phone
<input checked="" type="checkbox"/>	BYOD	if BYOD and Employee	then Employee
<input checked="" type="checkbox"/>	Guest	if Guest	then Guest
<input checked="" type="checkbox"/>	Contractor	if Contractor	then Contractor
<input checked="" type="checkbox"/>	Employee	if Employee	then Employee
<input checked="" type="checkbox"/>	Default	If no match	then WEBAUTH

Username matches

Matched AuthZ Rule = Guest

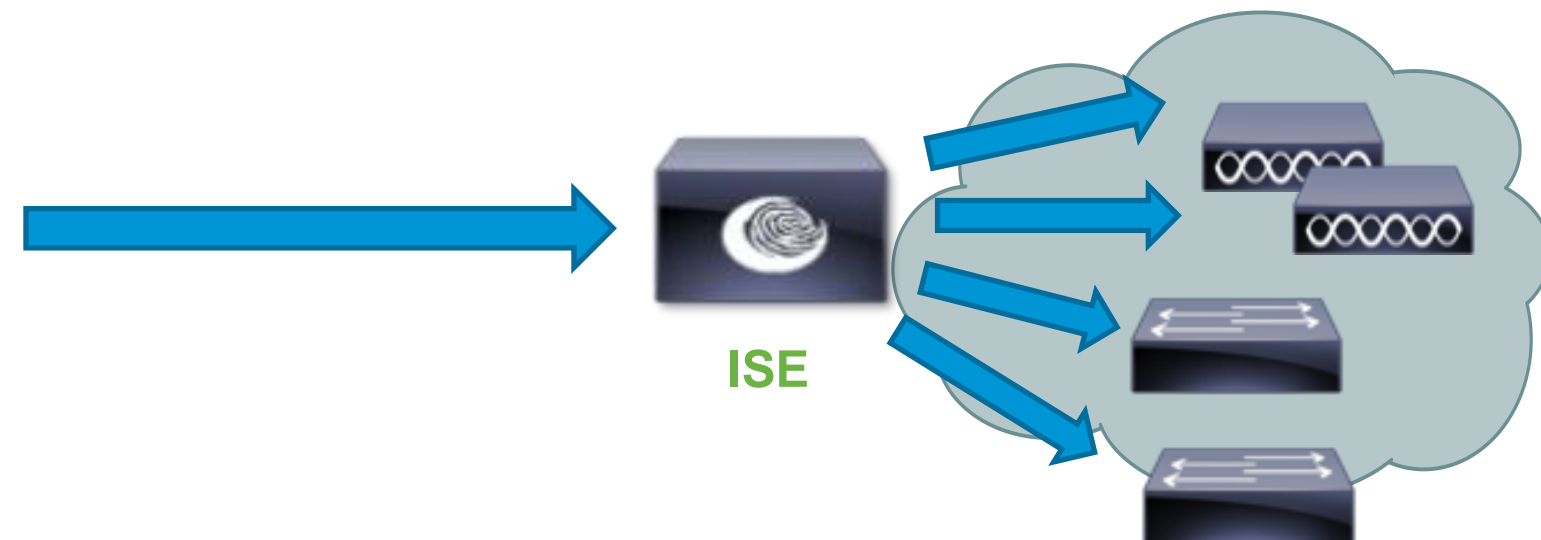


# Need for a Different Web Authentication Method

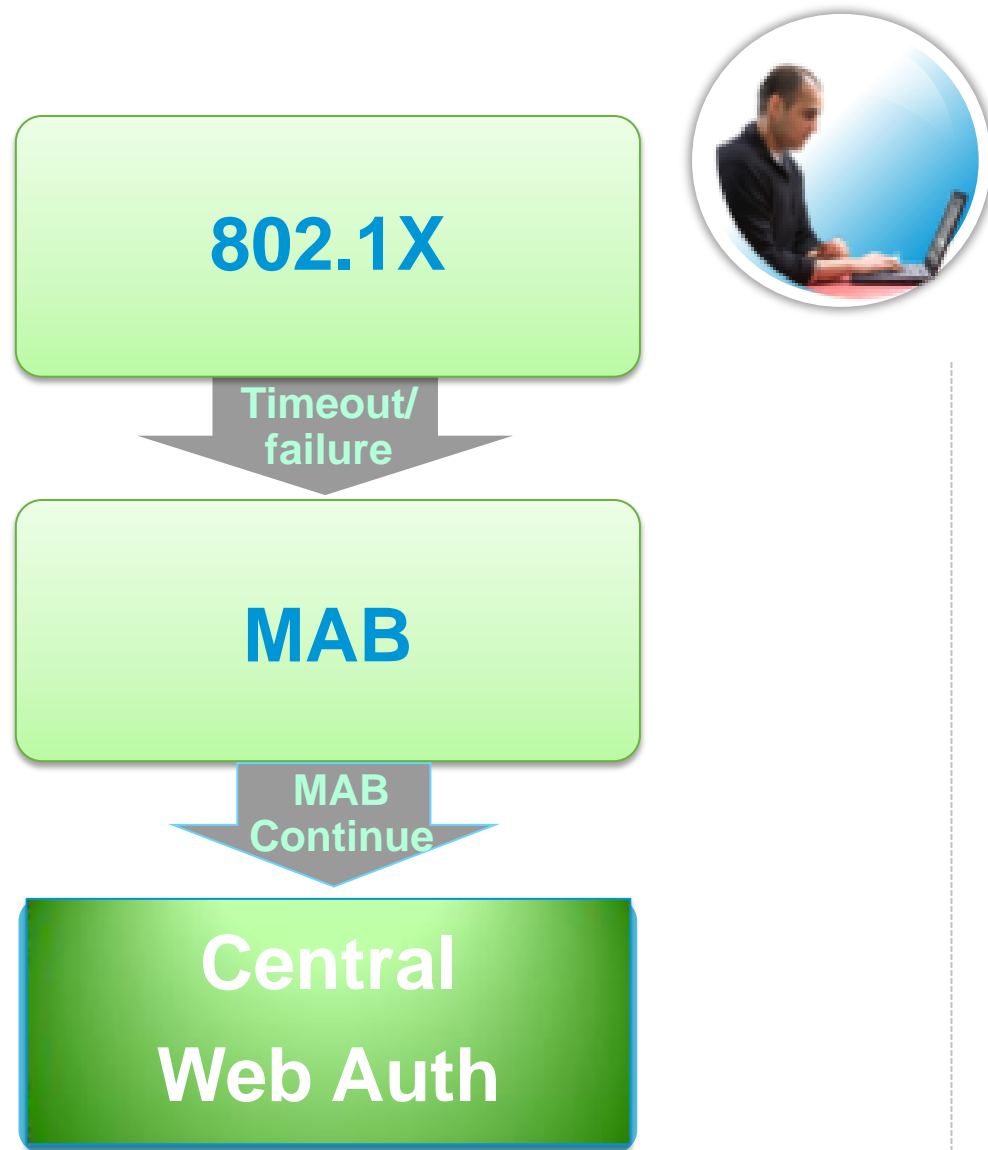
- LWA requires local configuration on each:
  - Switch
  - Wireless LAN controller
- Local portal limited and difficult to manage
- Limited redundancy options for external portals
- No dynamic VLAN support
- No change possible until re-authentication: posture, profiling



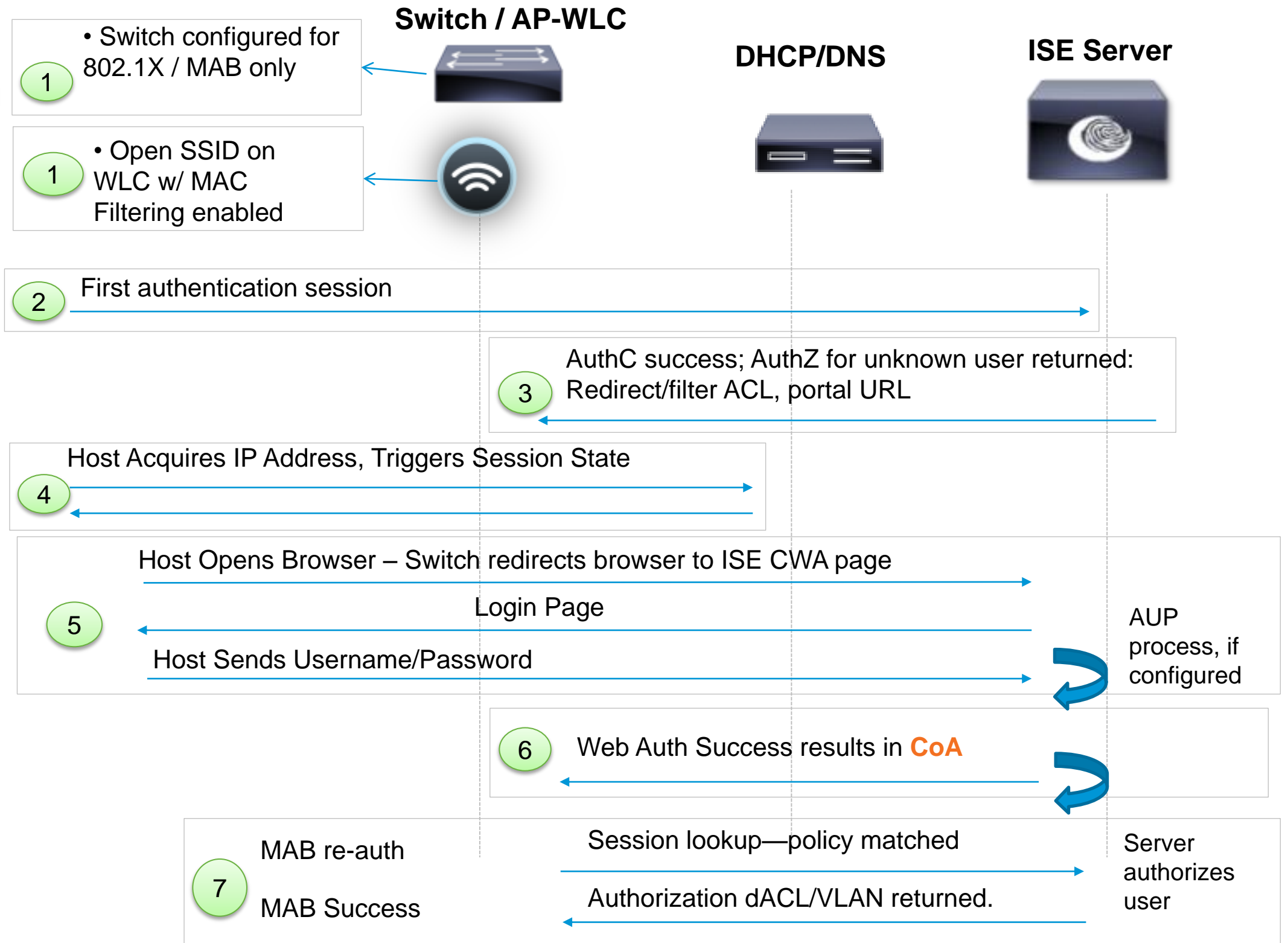
**Central Web Authentication (CWA) with ISE** was created by Cisco to improve deployment



# CWA – Session Flow



**Flex Auth:** If host not found (MAB lookup fails), then **Continue** to Authorization Policy processing





# Wired CWA Config

```

ip access-list extended PRE-AUTH-ACL
 permit udp any any eq bootps
 permit udp any any eq domain
 permit tcp any any eq http
 permit tcp any any eq https
ip access-list extended ACL-WEBAUTH-REDIRECT
 deny udp any any eq domain
 deny tcp any host PSN eq 8443
 permit ip any any
interface GigabitEthernet1/0/1
 authentication port-control auto
 dot1x pae-authenticator
 mab
 authentication order dot1x mab
 authentication event fail action next-method
    
```

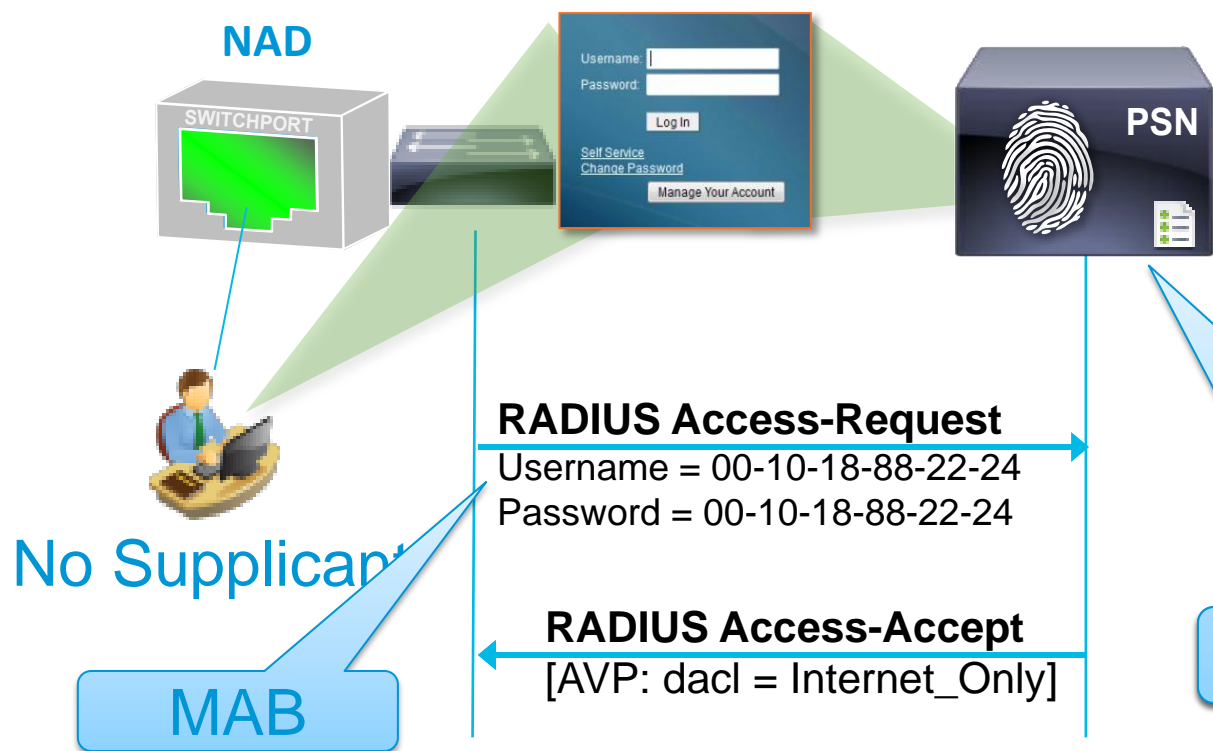
Matched AuthC Rule = MAB

## Authentication Policy

Status	Rule Name	Conditions	Identity Source
✓	MAB	if Wireless_MAB	Internal Endpoints
✓	Dot1X	if Wireless_802.1X	AD1
✓	Default	if <no match>	AD1_Internal

## Authorization Policy

Status	Rule Name	Conditions	Permissions
✓	IP Phones	if Cisco-IP-Phone	Cisco_IP_Phone
✓	BYOD	if BYOD and Employee	Employee
✓	Guest	if Guest	Guest
✓	Contractor	if Contractor	Contractor
✓	Employee	if Employee	Employee
✓	Default	If no match	WEBAUTH



CWA username matches

Matched AuthZ Rule = Guest

# Wireless CWA Config

**General Security QoS Advanced**

**Layer 2 Layer 3 AAA Servers**

Layer 2 Security   MAC Filtering

---

**General Security QoS Advanced**

Allow AAA Override  Enabled

**NAC**

NAC State

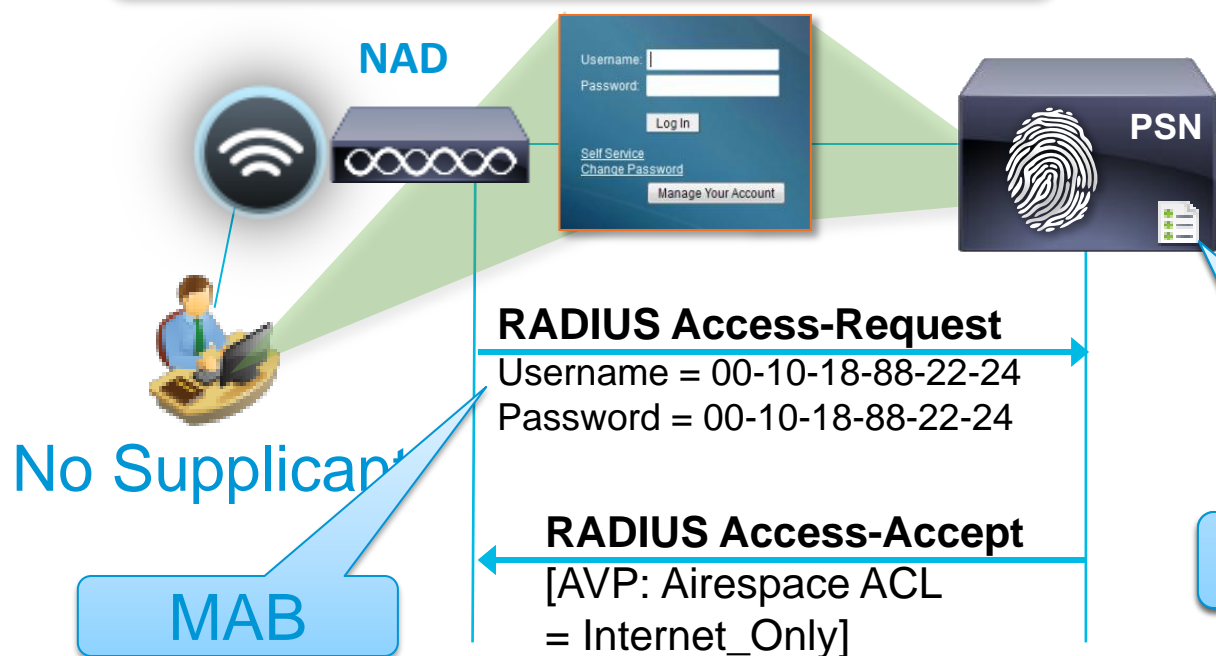
Matched AuthC Rule = MAB

## Authentication Policy

Status	Rule Name	Conditions	Identity Source
<input checked="" type="checkbox"/>	MAB	if Wireless_MAB	then Internal Endpoints
<input checked="" type="checkbox"/>	Dot1X	If Wireless_802.1X	then AD1
<input checked="" type="checkbox"/>	Default	if <no match>	then AD1_Internal

## Authorization Policy

Status	Rule Name	Conditions	Permissions
<input checked="" type="checkbox"/>	IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phone
<input checked="" type="checkbox"/>	BYOD	if BYOD and Employee	then Employee
<input checked="" type="checkbox"/>	Guest	if Guest	then Guest
<input checked="" type="checkbox"/>	Contractor	if Contractor	then Contractor
<input checked="" type="checkbox"/>	Employee	if Employee	then Employee
<input checked="" type="checkbox"/>	Default	If no match	then WEBAUTH



CWA username matches

Matched AuthZ Rule = Guest

# Wireless CWA + RADIUS Server Config

- Enable RADIUS Server for CoA

**RADIUS Authentication Servers > Edit**

Support for RFC 3576  Enabled ▼

- Enable AAA Override + NAC RADIUS

**General Security QoS Advanced**

**Layer 2 Layer 3 AAA Servers**

Layer 2 Security [6](#) None ▼

[9](#)MAC Filtering

- Enable WLAN for MAC Filtering

**General Security QoS Advanced**

Allow AAA Override  Enabled

**NAC**

NAC State Radius NAC ▼

- Configure ISE as RADIUS Server / Set Auth to RADIUS

**General Security QoS Advanced**

**Layer 2 Layer 3 AAA Servers**

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

**Radius Servers**

Radius Server Overwrite interface  Enabled

	Authentication Servers	Accounting Servers
Server 1	<input checked="" type="checkbox"/> Enabled IP:10.1.100.5, Port:1812 ▼	<input checked="" type="checkbox"/> Enabled IP:10.1.100.5, Port:1813 ▼
Server 2	None ▼	None ▼
Server 3	None ▼	None ▼

**Radius Server Accounting**

Interim Update  Interim Interval 600

**Authentication priority order for web-auth user**

Not Used

Order Used For Authentication

RADIUS LOCAL ▲ > Up

# ISE Authentication Configuration

The screenshot shows the ISE authentication configuration interface. Key elements include:

- Condition:** A green box highlights the condition: "Condition is to match RADIUS Attribute Service Type = 10 (Call-Check) AND [NAS-Type = 15 (Ethernet) OR NAS-Type= 19 (Wireless IEEE 802.11)]".
- Identity Source:** A green box highlights the "Identity Source" dropdown menu, which is set to "Internal Endpoints". A callout explains: "By default, use **Internal Endpoints DB** for ID Source if MAC Address is found in DB".
- Options:** A green box highlights the "Options" section, specifically the "If user not found" dropdown menu, which is set to "Continue". A callout explains: "If MAC address lookup fails, reject the request and send access-reject. If MAC address lookup returns no result, continue the process and move to authorization".
- Note:** A note at the bottom states: "Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP it is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests will be rejected."

- MAB Requests from Failed Auth user or Timed out user can still be processed to return specific authorization rule (VLAN, dACL, URL-Redirect, and SGT)
- By default, 'If user not found' value is set to 'Reject'

# ISE Authorization Configuration

## Authorization Profile Details

Name **WIFI\_Guest\_Portal**  
Description **Profile For Guest On Wireless**

### Attributes Details

Access Type **ACCESS\_ACCEPT**  
Centralized Web Authentication **ACL=REDIRECT\_ACL (https://ip:port/guestportal/gateway?sessionId=SessionIdValue&portal=ciscoliveportal&action=cwa)**

**CWA attributes for Wireless:  
URL + Redirect ACL**

## Authorization Rule

✓	S4 Contractor user Wireless	if <b>Contractor</b> AND (Radius:NAS-Port-Type EQUALS Wireless - IEEE 802.11 AND Network Access:UseCase EQUALS <b>Guest Flow</b> )	then <b>CONTRACTOR-PROFILE-WIRELESS</b>
✓	S4 Guest user Wireless	if <b>Guest</b> AND (Radius:NAS-Port-Type EQUALS Wireless - IEEE 802.11 AND Network Access:UseCase EQUALS <b>Guest Flow</b> )	then <b>GUEST-PROFILE-WIRELESS</b>
✓	S4 Contractor user Wired	if <b>Contractor</b> AND (Radius:NAS-Port-Type EQUALS Ethernet AND Network Access:UseCase EQUALS <b>Guest Flow</b> )	then <b>CONTRACTOR-PROFILE-WIRED</b>
✓	S4 Guest user Wired	if <b>Guest</b> AND (Radius:NAS-Port-Type EQUALS Ethernet AND Network Access:UseCase EQUALS <b>Guest Flow</b> )	then <b>GUEST-PROFILE-WIRED</b>
✓	S4 Guest Wireless Redirect	if Radius:NAS-Port-Type EQUALS Wireless - IEEE 802.11	then <b>WIFI_Guest_Portal</b>
✓	S4 Guest Wired Redirect	if Radius:NAS-Port-Type EQUALS Ethernet	then <b>LAN_Guest_Portal</b>
✓		then <b>DenyAccess</b>	

## Authorization Profile Details

Name **LAN\_Guest\_Portal**  
Description **Profile For Wired Devices**

### Attributes Details

Access Type **ACCESS\_ACCEPT**  
DACL Name **GUEST\_LAN\_PORTAL\_ACL**  
Centralized Web Authentication **ACL=REDIRECT\_ACL (url=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa)**

**CWA attributes for Wired:  
URL + Redirect ACL + filtering ACL**

# CWA Benefits & Support

- No extra local method like webauth
- dVLAN assignment support
- Centralization and dynamic push of configuration
  - Portal URL
  - Filtering ACL until guest authentication occurs
- Support for CoA
  - Posture
  - Profiling
  - Native Supplicant Provisioning



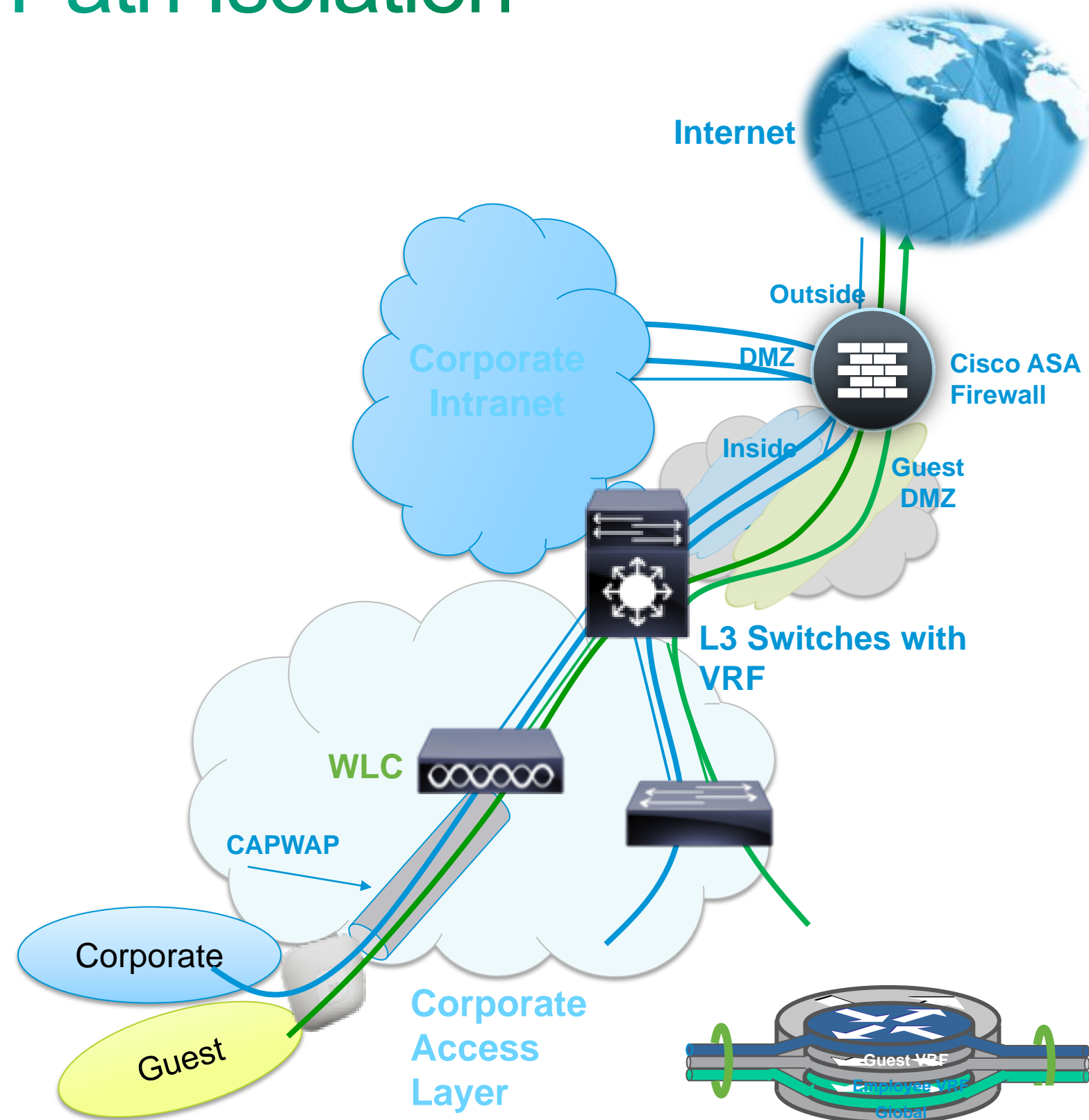
- **Catalyst 2960 (LAN Base) & 3560/3750:**  
12.2(55)SE3
- **Catalyst 4500 Series :**  
Sup 6E: 15.0(2)SG1  
Sup 7E: IOS-XE 3.3.0SG
- **Catalyst 6500 Series:**  
12.2(33)SXI7



- **Wireless LAN Controller (WLC/WiSM):**  
7.0.116.0 (CoA on 802.1X SSID only)  
7.2.103.0 (CoA on Open SSID)

# Guest Deployment and Path Isolation

- Isolation at access layer (port, SSID)
- Layer 2 path isolation:
  - CAPWAP & VLANs for wireless
  - L2 VLANs for wired
- Layer 3 path isolation:
  - VRF (Virtual Routing and Forwarding) to Firewall guest interface
  - Various tunnel methods
    - GRE
    - VPN
    - MPLS

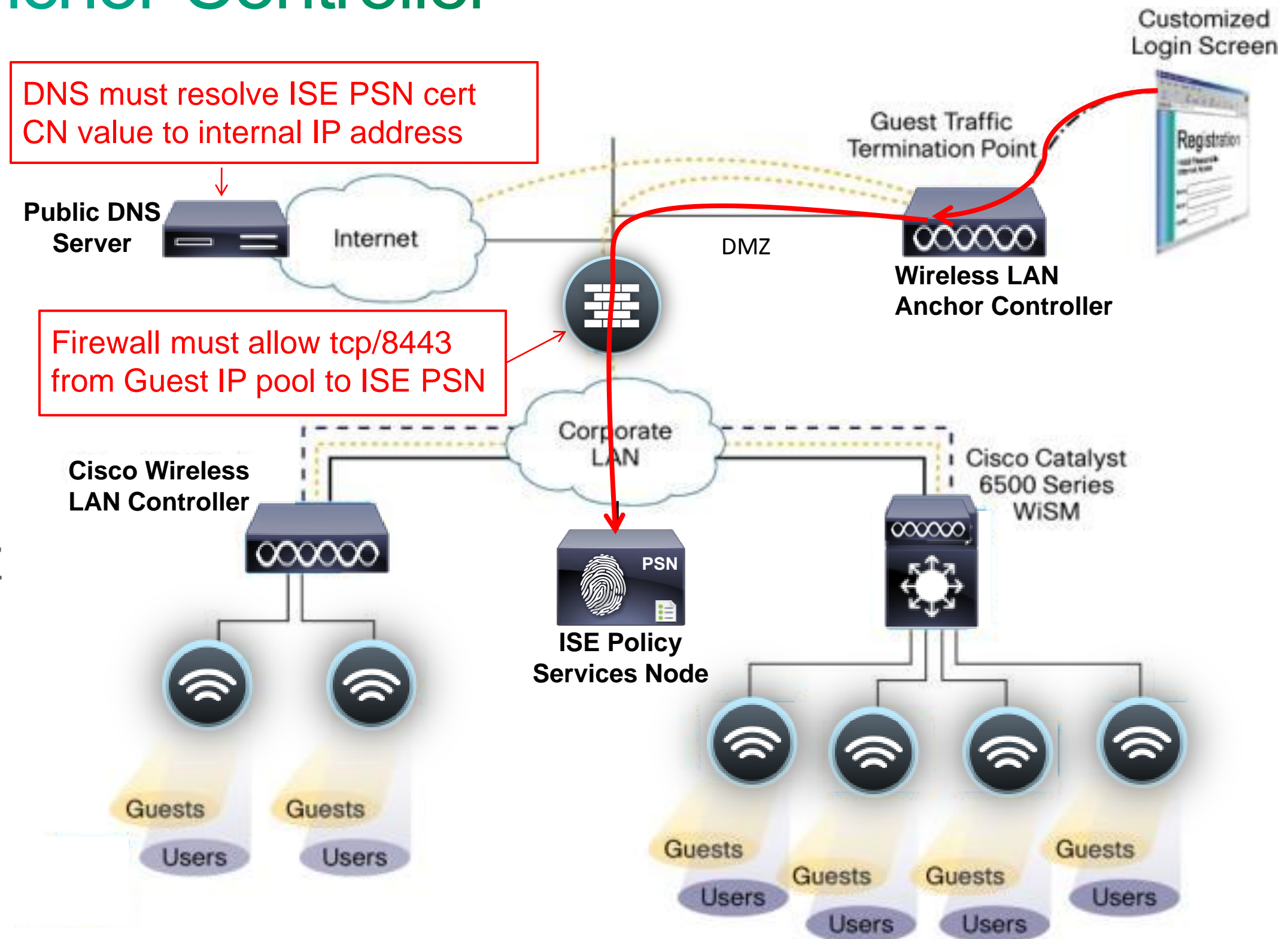




# Guest Access w/ Anchor Controller

- Anchor Controller provides path isolation via CAPWAP tunnel.
- Guest traffic terminates in DMZ.
- If use CWA (or LWA with ISE as web portal), then pinhole required in firewall from DMZ to ISE PSN:  

```
permit tcp <Guest_IPs>  
host <PSN> eq 8443
```
- If CWA used w/ public DNS, then server must resolve PSN certificate CN value to its IP:



`url-redirect=https://<PSN_CN>:8443/guestportal/gateway?sessionId=SessionIdValue&action=cwa`



# URL Redirection

# URL Redirection

ISE uses URL Redirection for:

- Central Web Auth
- Client Software Provisioning
- Posture Discovery / Assessment
- Device Registration WebAuth
- BYOD On-Boarding
  - Certificate Provisioning
  - Supplicant Configuration
- External Web Pages



# URL Redirection Components

- **Redirect URL:** For CWA, Client Provisioning, and Posture, URL value returned as a Cisco AV-pair RADIUS attribute.

Example: `cisco:cisco-av-pair=url-redirect=  
https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa`

- **Redirect ACL:** Access devices must be locally configured with ACL that specifies traffic to be permitted or to bypass redirection.

ACL value returned as a named ACL on NAD

Example: `cisco:cisco-av-pair=url-redirect-acl=ACL-POSTURE-REDIRECT`

IOS Redirect ACL Conventions:

Permit ACL entries define the traffic subject to redirection

Deny ACL entries define the traffic to bypass redirection

- **Port ACL (IOS Only):** ACL applied to the port that defines traffic allowed through port prior to redirection

Can be default port ACL or ACL returned as RADIUS authorization (dACL or named ACL).

# Common Redirect URLs

- **Central Web Auth (Default Portal)**

Cisco:cisco-av-pair=url-redirect= https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=**cwa**

- **CWA (Custom Portal):**

Cisco:cisco-av-pair=url-redirect= https://ip:port/guestportal/gateway?portal=**ClientPortalName**&sessionId=SessionIdValue&action=**cwa**

- **Device Registration WebAuth (Default Portal):**

Cisco:cisco-av-pair=url-redirect= https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=**drw**

- **Client Provisioning and Posture**

Cisco:cisco-av-pair=url-redirect= https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=**cpp**

Common Tasks

- Web Authentication
- Auto Smart Port
- Filter-ID

Centralized  ACL  Redirect  Value

Centralized  
Device Registration  
Posture Discovery  
Supplicant Provisioning

Centralized = CWA  
Device Registration = DRW  
Posture Discovery = CPP  
Supplicant Provisioning = NSP

**CWA: Simple URL/ACL selection using Common Tasks in Authorization Profile**

# Sample Redirect ACLs for CWA

- ISE URL Redirect ACL: Cisco:cisco-av-pair=url-redirect-acl=ACL-WEBAUTH-REDIRECT

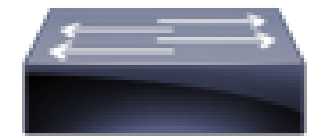
- 2k/3k/4k Example:

```
ip access-list extended ACL-WEBAUTH-REDIRECT
deny udp any eq bootpc any eq bootpc
deny udp any any eq domain
deny tcp any host <PSN1> eq 8443
permit ip any any
```

**Catalyst Switch:**  
deny = Bypass Redirection  
permit = Allow Redirection

Redirect ACL must be preconfigured and exist on the Catalyst switch or WLC.

HTTP and HTTPS Redirection



Catalyst Switch

- WLC Example:

Access List Name	ACL-WEBAUTH-REDIRECT									
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source	Destination	Port	Direction	Outbound	Inbound
<u>1</u>	Permit	0.0.0.0 / 0.0.0.0	10.1.100.10 / 255.255.255.255	UDP	Any					
<u>2</u>	Permit	10.1.100.10 / 255.255.255.255	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Outbound		
<u>3</u>	Permit	0.0.0.0 / 0.0.0.0	10.1.100.21 / 255.255.255.255	TCP	Any		8443	Any	Inbound	
<u>4</u>	Permit	10.1.100.21 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Outbound		
<u>5</u>	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	Any	

**Cisco WLC:**  
deny = Deny / Redirect if HTTP  
permit = Allow / Bypass Redirection

HTTP Only Redirection



Cisco WLC



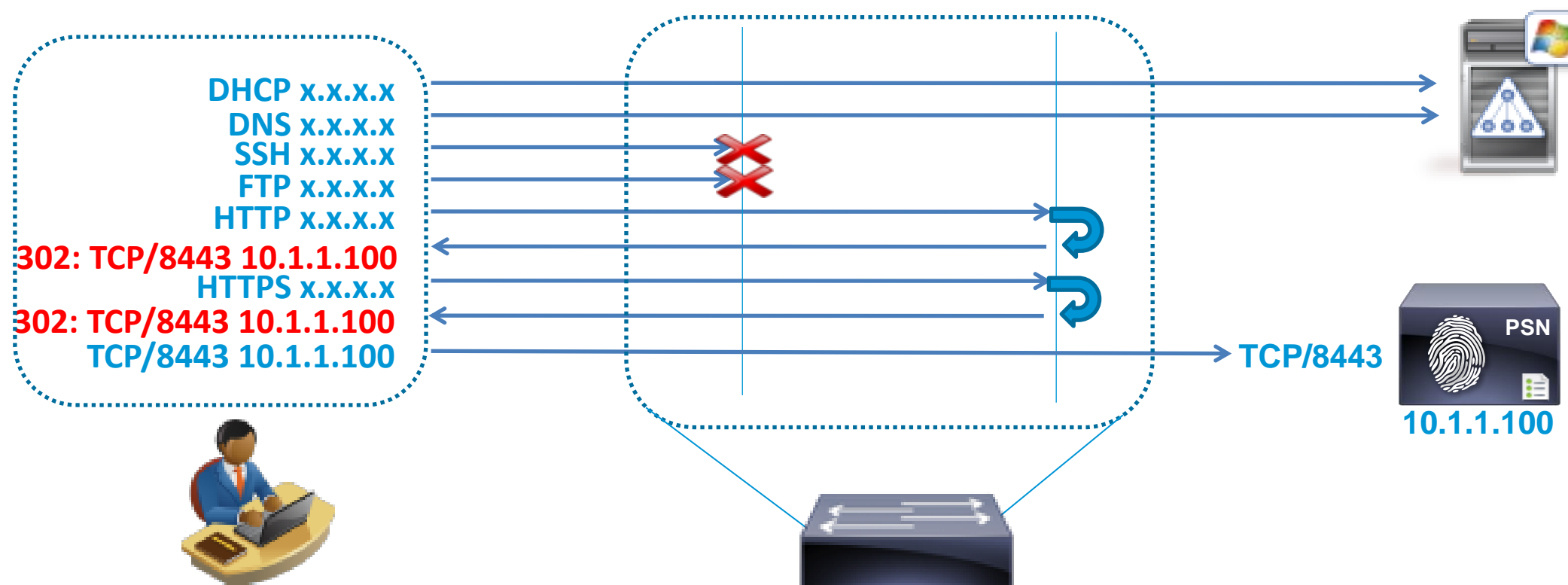
# Sample ACLs for CWA Redirection

```
ip access-list extended ACL-DEFAULT
 permit udp any eq bootpc any eq bootps
 permit udp any any eq domain
 permit tcp any any eq http
 permit tcp any any eq https
 permit tcp any host 10.1.1.100 eq 8080
 permit tcp any host 10.1.1.100 eq 8443
 (deny ip any any)
```

Port ACL  
or dACL

```
ip access-list extended ACL-WEBAUTH-REDIRECT
 deny udp any eq bootpc any eq bootps
 deny udp any any eq domain
 deny tcp any host 10.1.1.100 eq 8080
 deny tcp any host 10.1.1.100 eq 8443
 permit ip any any
```

Redirect  
ACL



# Wired URL Redirection Considerations

- Access switch configuration to enable redirection:

HTTP Redirection Support: `ip http server`

HTTPS Redirection Support: `ip http secure-server`

- For HTTPS, expect certificate warning as client browser will not trust switch cert for initial redirect

- Optionally decouple redirection from switch management:

Deactivate HTTP session modules: `ip http active-session-modules none`

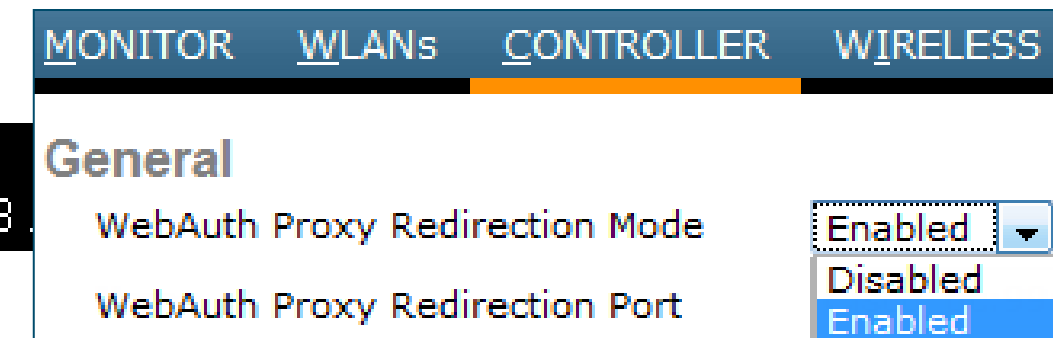
Deactivate HTTPS session modules: `ip http secure-active-session-modules none`

- Web Proxies: Consider Proxy/PAC config to allow access to ISE PSN

Wireless Option (Command available in WLC 7.0.116.0):

```
(Cisco Controller) >config network web-auth proxy-redirect enable
Web-auth Proxy redirection will be enabled for ports 80, 8080 and 3128.
```

Config Example: [http://www.cisco.com/en/US/products/ps10315/products\\_configuration\\_example09186a0080b8a909.shtml](http://www.cisco.com/en/US/products/ps10315/products_configuration_example09186a0080b8a909.shtml)



# Wired URL Redirection Considerations

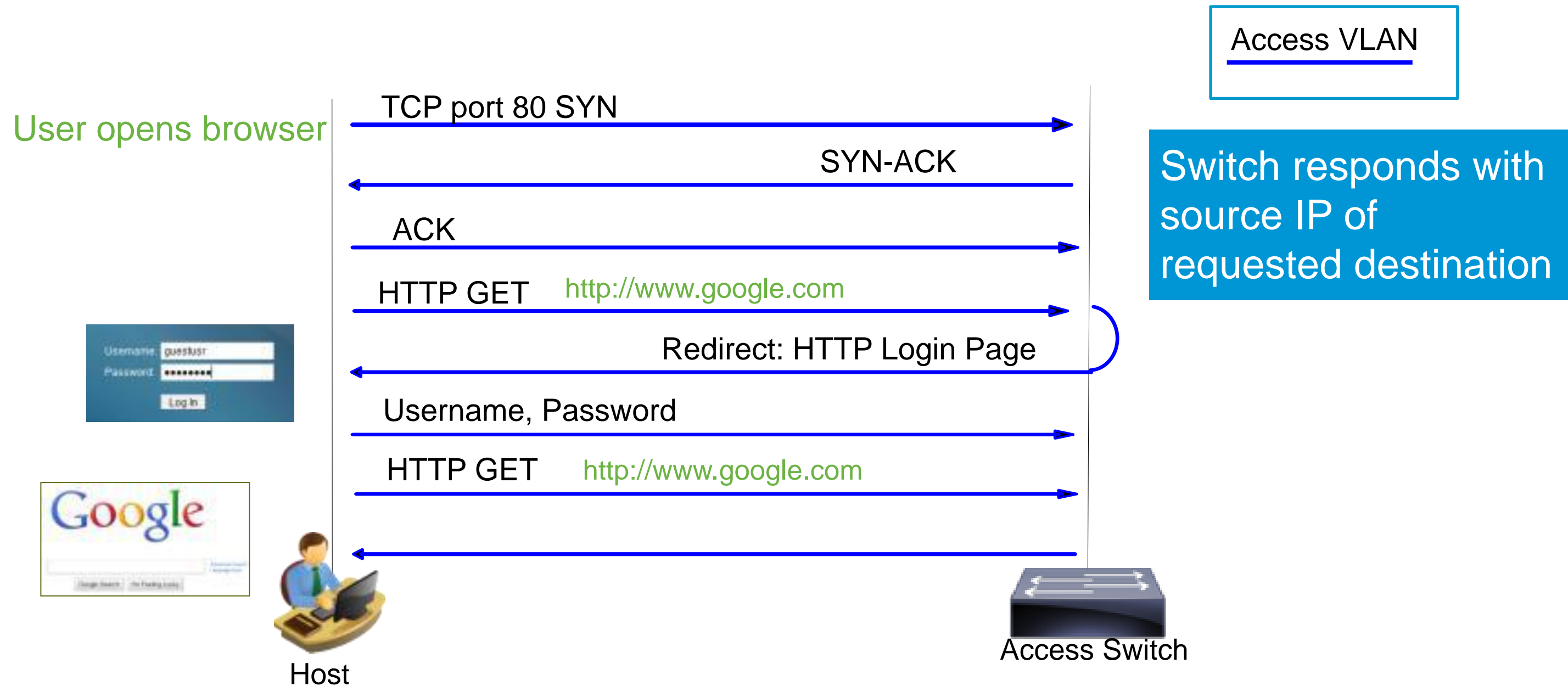
## L2 Access Switch without SVI for Access VLAN

- Require route from switch management IP to host IP (via upstream gateways)
- ACLs/Firewalls, VRFs, or other traffic isolation from management network will cause redirect traffic from switch to host to be dropped and redirect fails.
- dACLs time out due to ip device tracking not getting ARP response from host.
  - If SVI configured, tracking probe 'use-svi' option may help [12.2(55)SE]
  - If SVI for access VLAN not configured, then ARP sent with source IP 0.0.0.0
    - Some devices will not respond to ARP source 0.0.0.0.
    - Windows 7 users may report duplicate IP address error



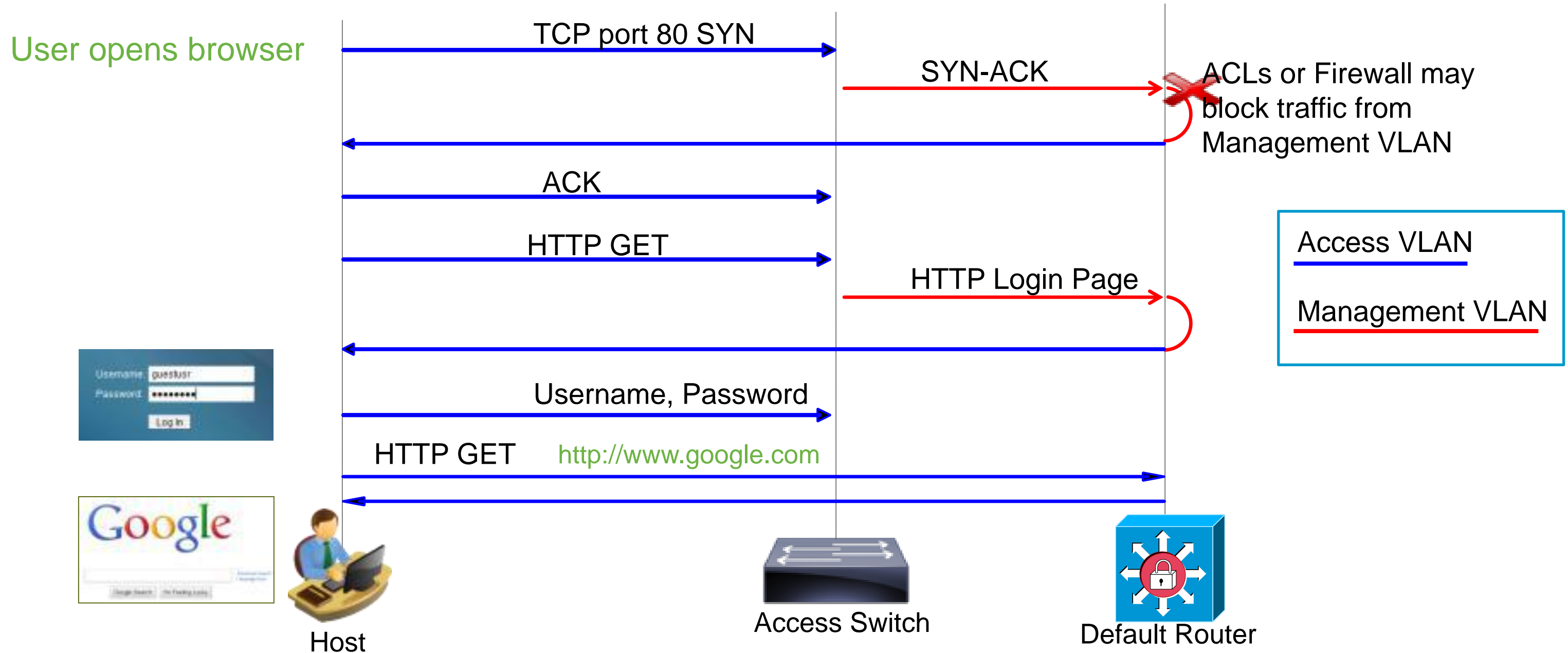
# URL Redirection – Access VLAN SVI

TCP Traffic Flow for Login Page When L3 SVI for Host VLAN on Access Switch



# URL Redirection - No Access VLAN SVI

TCP Traffic Flow for Login Page When No L3 SVI for Host VLAN on Access Switch



# Troubleshooting Redirection



- Verify IOS code release and feature set!
- **# show authentication session interface <int>**
  - Does the IP address display? Verify device tracking table entry.
  - Is the session ID matching?
  - Is the dACL downloaded, if applicable?
  - Is the Redirect ACL applied? If so, verify contents on local switch
- **# show ip access-list interface <int>**
  - Is the access list properly applied to the client IP address per above? If not...
    - Verify that endpoint has an IP address – If not, is “ip device tracking” and/or DHCP Snooping enabled?
    - Verify dACL contents in ISE—ISE may show dACL authorization applied but switch rejects if ANY syntax error
- Access switch without SVIs for local access VLANs (common L2 case)
  - Is there a route from Management VLAN to client VLAN?
  - Is firewall dropping redirects sourced from Management VLAN?
  - Are dACLs disappearing? If so, does host respond to ARP probes from 0.0.0.0?
    - `Switch(config-if)# ip device tracking probe use-svi`

# Troubleshooting Redirection



```
3k-access(config-if)# do sh auth sess int gi0/1
Interface: GigabitEthernet0/1
MAC Address: 0050.56b4.0169
IP Address: 10.1.10.101
User-Name: 00-50-56-b4-01-69
Status: Authz Success
Domain: DATA
Security Policy: Should Secure
Security Status: Unsecure
Oper host mode: multi-auth
Oper control dir: both
Authorized By: Authentication Server
Vlan Group: N/A
ACS ACL: xACSACLx-IP-POSTURE REMEDIATION-4d816c3a
URL Redirect ACL: ACL-POSTURE-REDIRECT
URL Redirect: https://ise-1.demo.local:8443/questportal/gateway?
sessionId=0A01640100000090728C037&action=cwa
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0A01640100000090728C037
```

```
Acct Session 3k-access(config-if)# do sh ip access-list int gi0/1
Han permit ip host 10.1.40.100 any
Runnable methods l permit udp host 10.1.10.101 any eq domain
Method St permit tcp host 10.1.10.101 any eq www
mab Au permit tcp host 10.1.10.101 any eq 443
dot1x No permit tcp host 10.1.10.101 host 10.1.100.21 eq 8443
permit tcp host 10.1.10.101 host 10.1.100.21 eq 8905
permit udp host 10.1.10.101 host 10.1.100.21 eq 8905
permit tcp host 10.1.10.101 host 10.1.100.21 eq 8909
permit udp host 10.1.10.101 host 10.1.100.21 eq 8909
permit tcp host 10.1.10.101 host 10.1.252.21 eq www
```

Separate Voice Authorization

# URL Redirection Considerations

## Apple Captive Network Assistant (CNA)



- **Problem Statement:** URL redirection on Apple devices may fail due to Apple CNA.

- Background on CNA:

Apple iOS feature to facilitate network access when captive portals present that requires login by automatically opening web browser in a controlled window. Feature attempts to detect the presence of captive portal by sending a web request upon WiFi connectivity to <http://www.apple.com/library/test/success.html>

If response received, then Internet access assumed and no further interaction

If no response received, Internet access is assumed to be blocked by captive portal and CNA auto-launches browser to requests portal login in a controlled window.

- **Solutions:**

1. Disable Auto-Login under WLAN settings (requires user knowledge and interaction)
2. Configure WLC to bypass CNA:

```
> config network web-auth captive-bypass enable
```

Command available in WLC 7.2:

<http://www.cisco.com/en/US/docs/wireless/controller/7.2/command/reference/cli72commands.html#wp15129591>

# Provisioning Guest Accounts



# Guest User Databases



**Identity Service Engine**



**Database**

## Internal DB

- Static entries
- Bulk import
- Enabled/  
disabled

## Guest DB

- Created by sponsors  
(bulk option)
- Guest “self  
service”
- Restricted  
access duration

## External DB

- LDAP / AD
- Managed  
externally
- Enabled/  
disabled



# Guest User Roles

## Different Policies Based on User Role

### Guest

- Internet access only
- Created by any user
- Limited connection time: 2 hours, ½ day, one day
- Wireless access only
- No access during non-business hours or weekends.

### Contractor

- Internet access
- Restricted access to specific internal resources
- Created by select users
- Longer connection time: one week, one month
- Access allowed only from specific networks
- Off-hours access allowed.

Name	Description
<input type="checkbox"/> Contractor	Accounts for contractor users
<input type="checkbox"/> Guest	Guest ID group



# Differentiating Guest Access via User Groups



Identity Service Engine



External Database

User Identity Groups	
Name	Description
<input type="checkbox"/> Contractor	Accounts for contractor users
<input type="checkbox"/> Guest	Guest ID group

- Multiple groups can be created in ISE
- Each group can contain:
  - Guest users (created by Sponsor and Self-service)
  - Internal users (created by Administrators)

- External groups mapped in ISE

Active Directory > AD2008R2	
Name	
<input type="checkbox"/> live.cisco.com/Builtin/Administrators	
<input type="checkbox"/> live.cisco.com/Builtin/Guests	
<input type="checkbox"/> live.cisco.com/Builtin/Users	
<input type="checkbox"/> live.cisco.com/Users/engineering	
<input type="checkbox"/> live.cisco.com/Users/marketing	
<input type="checkbox"/> live.cisco.com/Users/sales	

Mapping example for AD

Those groups can be used in different authorization rules to differentiate network access

# Guest Users DB – Account Creation Methods

- Two ways to populate ISE Internal guest DB:

Self-Service

Option on ISE 'Guest Portal'

Sponsoring

via ISE 'Sponsor Portal'



# Sponsor Groups and Privileges



## Sponsor 'AllAccounts'

- Can create user in groups 'contractor' and 'guest'
- Can use time profiles up to one week
- Can see all accounts in group

## Sponsor 'OwnAccounts'

- Can create user in group 'guest' only
- Can use time profiles up to one day
  - Cannot do bulk creation

# Sponsor Privileges



System Identity Management Network Resources Guest Management

Sponsor Group Policy Sponsor Groups Settings

Sponsor Group List > SponsorAllAccounts

### Sponsor Group

General Authorization Levels Guest Roles Time Profiles

\* Name **SponsorAllAccounts**

Description Sponsors with view on all accounts

### Sponsor Group

General Authorization Levels Guest Roles Time Profiles

Allow Login	Yes
Create Accounts	Yes
Create Bulk Accounts	Yes
Create Random Accounts	Yes
Import CSV	Yes
Send Email	Yes
Send SMS	Yes
View Guest Password	Yes
Allow Printing Guest Details	Yes
View/Edit Accounts	All Accounts
Suspend/Reinstate Accounts	All Accounts
* Account Start Time	1 Days (Valid Range 1 to 999999999)
* Maximum Duration of Account	5 Days (Valid Range 1 to 999999999)

### Sponsor Group

General Authorization Levels Guest Roles Time Profiles

Contractor

Guest

### Sponsor Group

General Authorization Levels Guest Roles Time Profiles

Available:

- DefaultOneHour
- DefaultFirstLogin
- DefaultStartEnd

Pick:

- 4\_hours
- One\_day
- One\_week

# Sponsor Authentication



- The sponsor account can be a
  - Local ISE user
  - LDAP user
  - Active Directory user
- DB checking order can be configured via 'Identity Source Sequence' in ISE

Identity Source Sequences List > Sponsor\_Portal\_Sequence

### Identity Source Sequence

▼ Identity Source Sequence

\* Name

Description

▼ Certificate Based Authentication

Select Certificate Authentication Profile

▼ Authentication Search List

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

Available	Selected
Internal Endpoints	Internal Users AD2008R2

In above example we interrogate the ISE DB first and then the AD



# Map Groups to Sponsor Privileges



- You can map any group: internal, AD, LDAP to a sponsor privilege group
- All users mapped to that group will log in with similar sponsor privileges as defined in the selected sponsor group

The screenshot shows the "Sponsor Group Policy" configuration page in Cisco ISE. It features a table with columns for "Status", "Policy Name", "Identity Groups", "Other Conditions", and "Sponsor Groups". Two policy rules are visible: "Manage All Accounts" and "Manage Group Accounts". Annotations include a green box at the top stating "Map internal or external groups to sponsor privilege groups" with arrows pointing to the "Identity Groups" and "Sponsor Groups" columns. A green box labeled "Internal groups" points to the "SponsorAllAccount" and "SponsorOwnAccounts" entries in the "Identity Groups" column. A green box labeled "AD groups" points to a dropdown menu in the "Other Conditions" column, which is currently set to "AD2008R2:External" and shows a list of domain paths including "live.cisco.com/Users/engineering" and "live.cisco.com/Builtin/Administrators".

Status	Policy Name	Identity Groups	Other Conditions	Sponsor Groups
<input checked="" type="checkbox"/>	Manage All Accounts	SponsorAllAccount	Condition(s)	SponsorAllAccounts
<input checked="" type="checkbox"/>	Manage Group Accounts	SponsorOwnAccounts	Condition(s)	SponsorOwnAccounts

Condition Name	Expression
	AD2008R2:External <b>Equals</b> live.cisco.com

- live.cisco.com/Users/engineering
- live.cisco.com/Builtin/Guests
- live.cisco.com/Users/marketing
- live.cisco.com/Users/sales
- live.cisco.com/Builtin/Users
- live.cisco.com/Builtin/Administrators



# Simple URL for Sponsor / My Devices Portal

**Problem Statement:** Default Sponsor / MDP URL difficult for users to remember or enter.

Examples:

<https://ise-psn-1.company.com:8443/sponsorportal>  
<https://ise-psn-3.company.com:8443/mydevices>

**Solution:** Simplified URL for Sponsor / MDP.

- Sponsor Portal and My Devices Portal can be accessed via a user-friendly URL.

Example: <http://sponsor.company.com>

Automatic redirect to `https://fqdn:port`

- FQDN for URL must be added to DNS and resolve to the Policy Service node(s) used for Guest Services.
- Recommend populating Subject Alternative Name (SAN) field of PSN local cert with this alternative FQDN to avoid SSL cert warnings due to name mismatch. name mismatch.

## Guest/Sponsor SSL Settings

### Admin Portal Settings

HTTP Port

HTTPS Port

### Guest Portal Settings

HTTPS Port  (Valid Range 1 to 65535)

### Sponsor Portal Settings

HTTPS Port  (Valid Range 1 to 65535)

### My Devices Portal Settings

HTTPS Port  (Valid Range 1 to 65535)

### Portal URLs

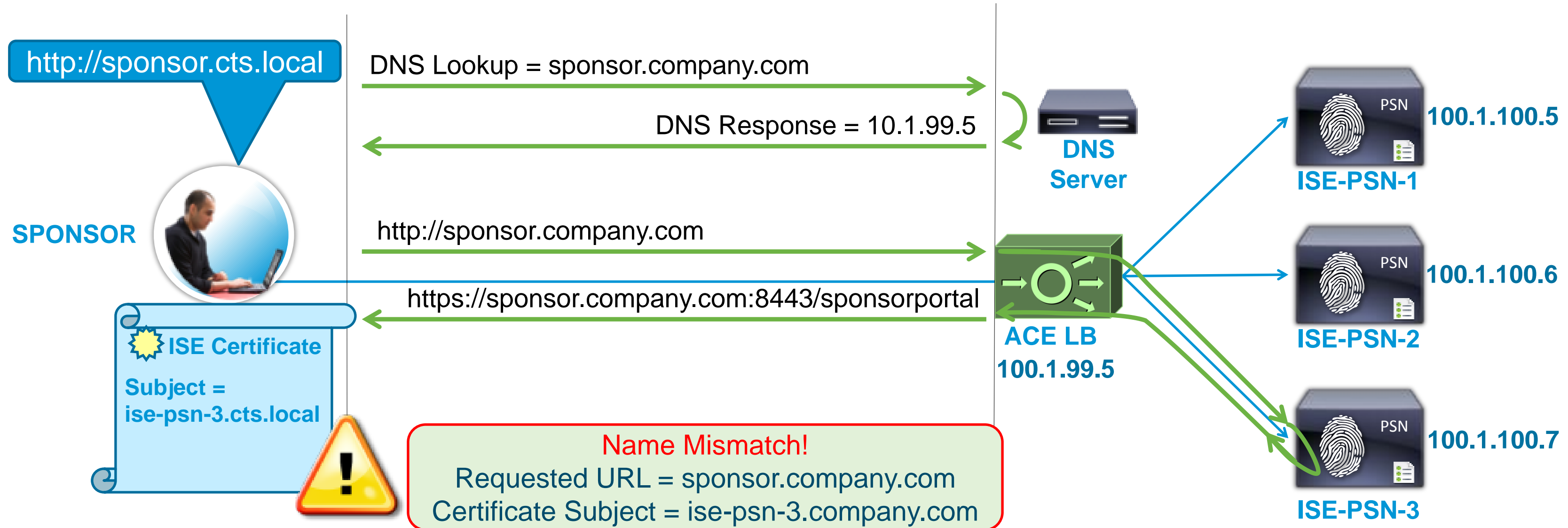
Default Sponsor Portal URL

Default My Devices Portal URL

**Note: This will restart ALL PAP/PSN nodes!**

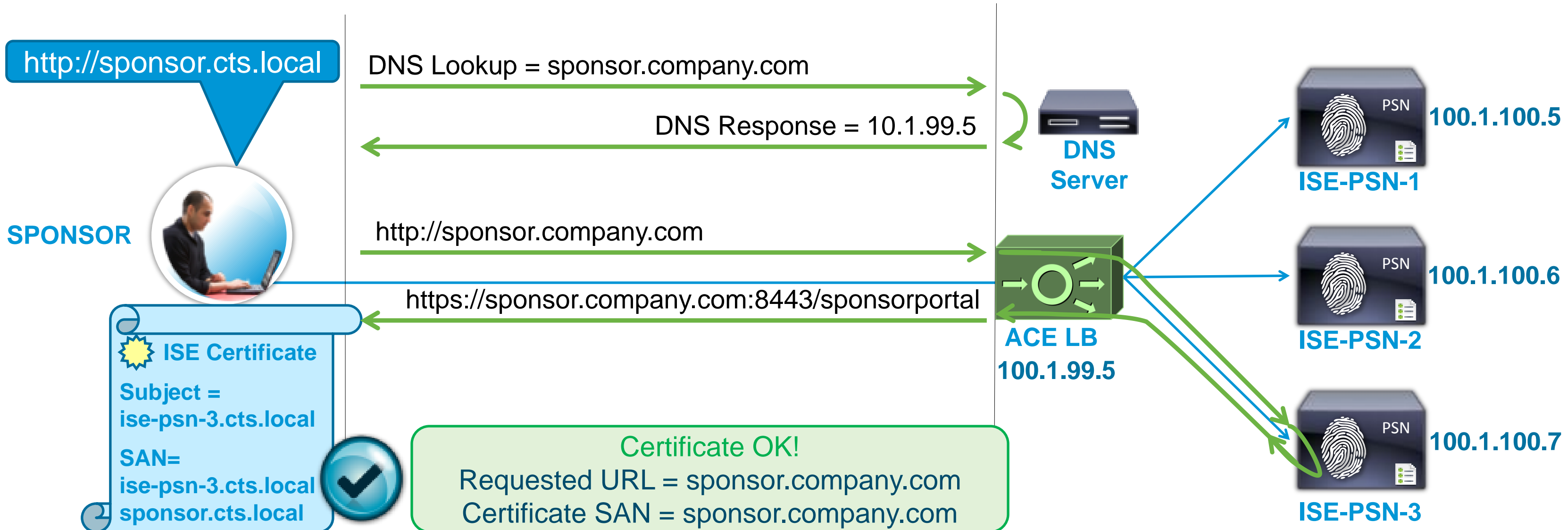
# ISE Certificate without SAN

## Certificate Warning - Name Mismatch



# ISE Certificate with SAN

## No Certificate Warning



# ISE – Sponsor Portal



- Customizable sponsor 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



# Sponsor Portal – Create Guest Account User



**CISCO Sponsor Portal**

Account Management > [View All Guest Accounts](#) > Create Guest Account

## Create Guest Account

First Name:

Last Name:

\* Email Address:

Phone Number:

Company:

\* Group Role:

\* Time Profile:

\* Timezone:

\* Language Template for Email/SMS Notifications:

\* = Required fields

### Customizable Fields

- Define if mandatory or optional
- Can add up to 5 other custom attributes

### Guest roles and Time Profiles

- Pre-defined by admin



# Guest Account Information



The screenshot shows the Cisco Sponsor Portal interface. The main content area displays a success message: 'Successfully Created Guest Account: muriel@guest.com'. Below this, a list of account details is shown. A green box highlights the 'Username' and 'Password' fields, with an arrow pointing to a callout box. The callout box contains two sections: 'Username configuration' and 'Password configuration', each with a list of bullet points. The 'Username configuration' section notes that the account was created from 'first & last name' or 'email'. The 'Password configuration' section notes that the password was generated automatically and has configurable complexity. The account details include: Username: muriel@guest.com, Password: cab, First Name: Muriel, Last Name: Bole, Email Address: muriel@guest.com, Phone Number: (blank), Company: Guest, Status: AWAITING INITIAL LOGIN, Suspended: false, Group Role: Contractor, Time Profile: One\_week, Timezone: Europe/London, Account Start Date: 2012-01-04 15:54:46 GMT, Account Expiration Date: 2012-01-09 15:54:46 GMT, and Language Template for Email/SMS Notifications: French. At the bottom, there are buttons for 'Email', 'SMS', 'Print', 'Create Another Account', and 'View All Accounts'.

**Successfully Created Guest Account: muriel@guest.com**

Username: muriel@guest.com  
Password: cab

First Name: Muriel  
Last Name: Bole  
Email Address: muriel@guest.com  
Phone Number:  
Company: Guest  
Status: AWAITING INITIAL LOGIN  
Suspended: false  
Group Role: Contractor  
Time Profile: One\_week

Timezone: Europe/London  
Account Start Date: 2012-01-04 15:54:46 GMT  
Account Expiration Date: 2012-01-09 15:54:46 GMT

Language Template for Email/SMS Notifications: French

Email SMS Print Create Another Account View All Accounts

**Username configuration**

- Created from 'first & last name' or 'email'

**Password configuration**

- Generated automatically
- Configurable password complexity



# Sponsor Portal: Informing Guests



- Multiple ways to notify Guest with their credentials and other access info

1. Print the details
2. Send via e-mail
3. Send via SMS

The screenshot shows the Cisco Sponsor Portal interface. The top header includes the Cisco logo and 'Sponsor Portal'. The left navigation menu has sections for 'Sponsor' (Home, Settings Customization) and 'Account Management' (View Guest Accounts, Create Multiple Accounts, Create Random Accounts, Import Accounts). The main content area shows a success message: 'Successfully Created Guest Account mbole@cisco.com' with a green checkmark icon. Below the message are the account details:

Username:	mbole@cisco.com
Password:	adc
First Name:	Muriel
Last Name:	Bole
Email Address:	mbole@cisco.com
Phone Number:	
Company:	cisco
Status:	AWAITING INITIAL LOGIN
Suspended:	false
Group Role:	Guest
Time Profile:	custom

Additional details include: Timezone: Europe/London, Account Start Date: 2011-10-13 16:00:00 BST, and Account Expiration Date: 2011-10-14 16:00:00 BST. At the bottom, there are buttons for 'Email', 'SMS', 'Print', 'Create Another Account', and 'View All Accounts'. A green arrow points from the list on the left to the 'Email', 'SMS', and 'Print' buttons.

# Guest Portals



# Guest Self-Service

The image displays three sequential screenshots of the Cisco Identity Services Engine 1.1 Guest Portal interface, illustrating the self-registration process.

**Screenshot 1 (Left):** Shows the main navigation menu. The "Self Service" option is highlighted with a green box. Other options include "Login", "Change Password", and "Device Registration".

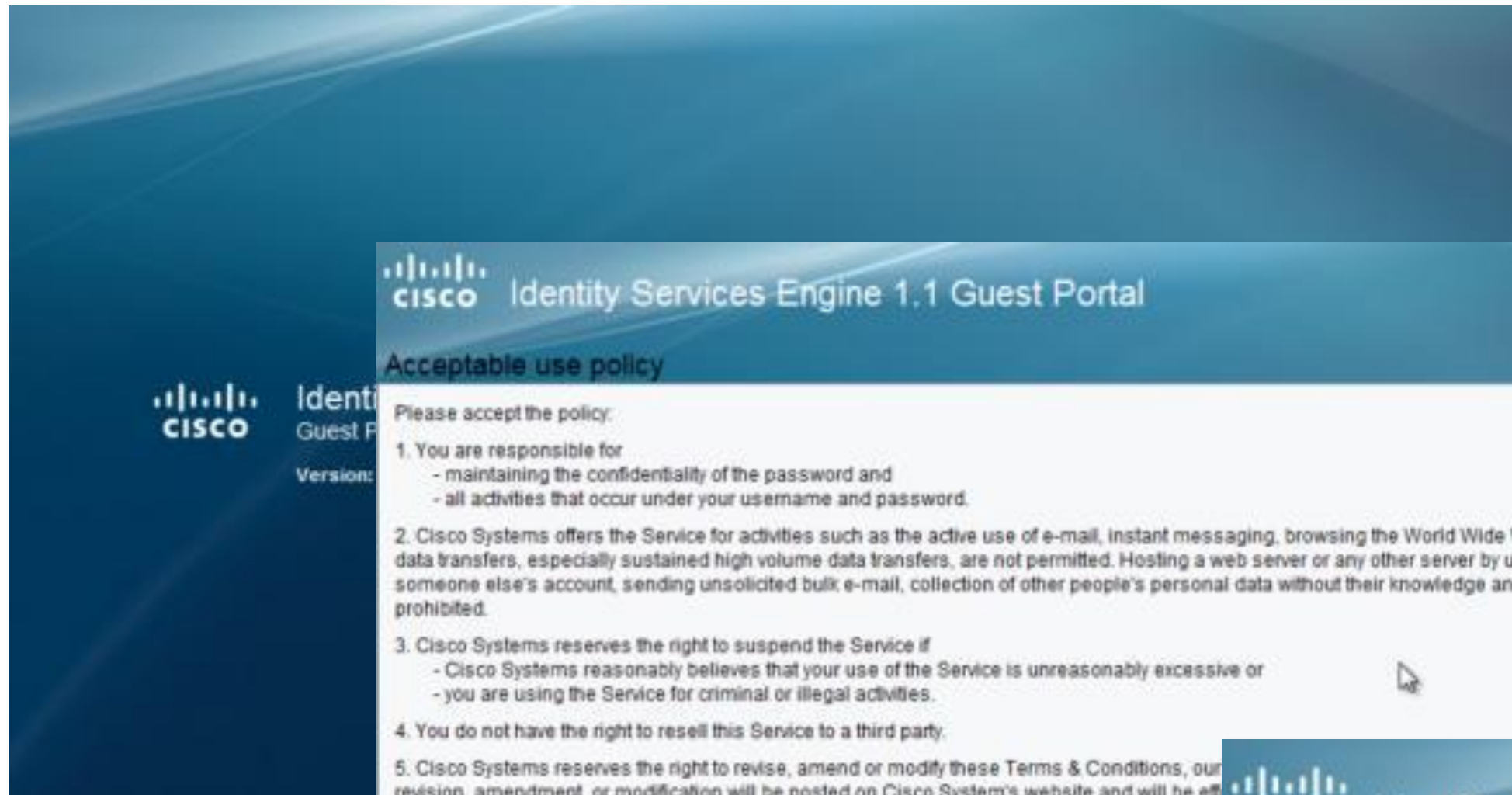
**Screenshot 2 (Middle):** Shows the "Self Registration" form. The form includes fields for First Name, Last Name, Email Address, Phone Number, Company, Reason for Visit, and Person(s) Visited. A Timezone dropdown menu is set to "US/Pacific". A legend indicates that fields with a gear icon are required. The "Submit" button is highlighted with a green box.

**Screenshot 3 (Right):** Shows the successful completion of registration. A green checkmark icon is displayed next to the message: "Successfully Created Guest Account: guser001". Below this, the "Self Registration" details are listed:

- Username: guser001
- Password: 3MN578bp
- First Name: Guest
- Last Name: User
- Email Address: guest@company.com
- Phone Number: (999) 555-1234
- Company: Company, Inc.
- Reason for Visit: Project Review Meeting
- Person(s) Visited: Mr. Company Sponsor
- Timezone: US/Pacific

The "OK" button at the bottom of the success message is highlighted with a green box. A green arrow points from this "OK" button back to the "Self Service" menu in the first screenshot.

# Guest User Experience



**Acceptable use policy**

Please accept the policy:

1. You are responsible for
  - maintaining the confidentiality of the password and
  - all activities that occur under your username and password.
2. 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 interference with other network users are all prohibited.
3. Cisco Systems reserves the right to suspend the Service if
  - Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or
  - you are using the Service for criminal or illegal activities.
4. You do not have the right to resell this Service to a third party.
5. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our revision, amendment, or modification will be posted on Cisco System's website and will be effective immediately.

Accept terms and conditions

**Identity Services Engine**

**Login Successful**

Please retry your original URL request.



# Portal Localization / Customization



- Several Languages are Supported Natively in ISE 1.1
- All guest user pages are translated:
  - Authentication page
  - Acceptable usage policy
  - Success/failure page
  - ...

Guest Portal Language Templates	
Language Template Name	Description
<input type="checkbox"/> ChineseSimplified	Guest Portal Language Template
<input type="checkbox"/> ChineseTraditional	Guest Portal Language Template
<input type="checkbox"/> English	English Guest Language Template
<input type="checkbox"/> French	Guest Portal Language Template
<input type="checkbox"/> German	Guest Portal Language Template
<input type="checkbox"/> Italian	Guest Portal Language Template
<input type="checkbox"/> Japanese	Guest Portal Language Template
<input type="checkbox"/> Korean	Guest Portal Language Template
<input type="checkbox"/> Portuguese	Guest Portal Language Template
<input type="checkbox"/> Russian	Guest Portal Language Template
<input type="checkbox"/> Spanish	Guest Portal Language Template

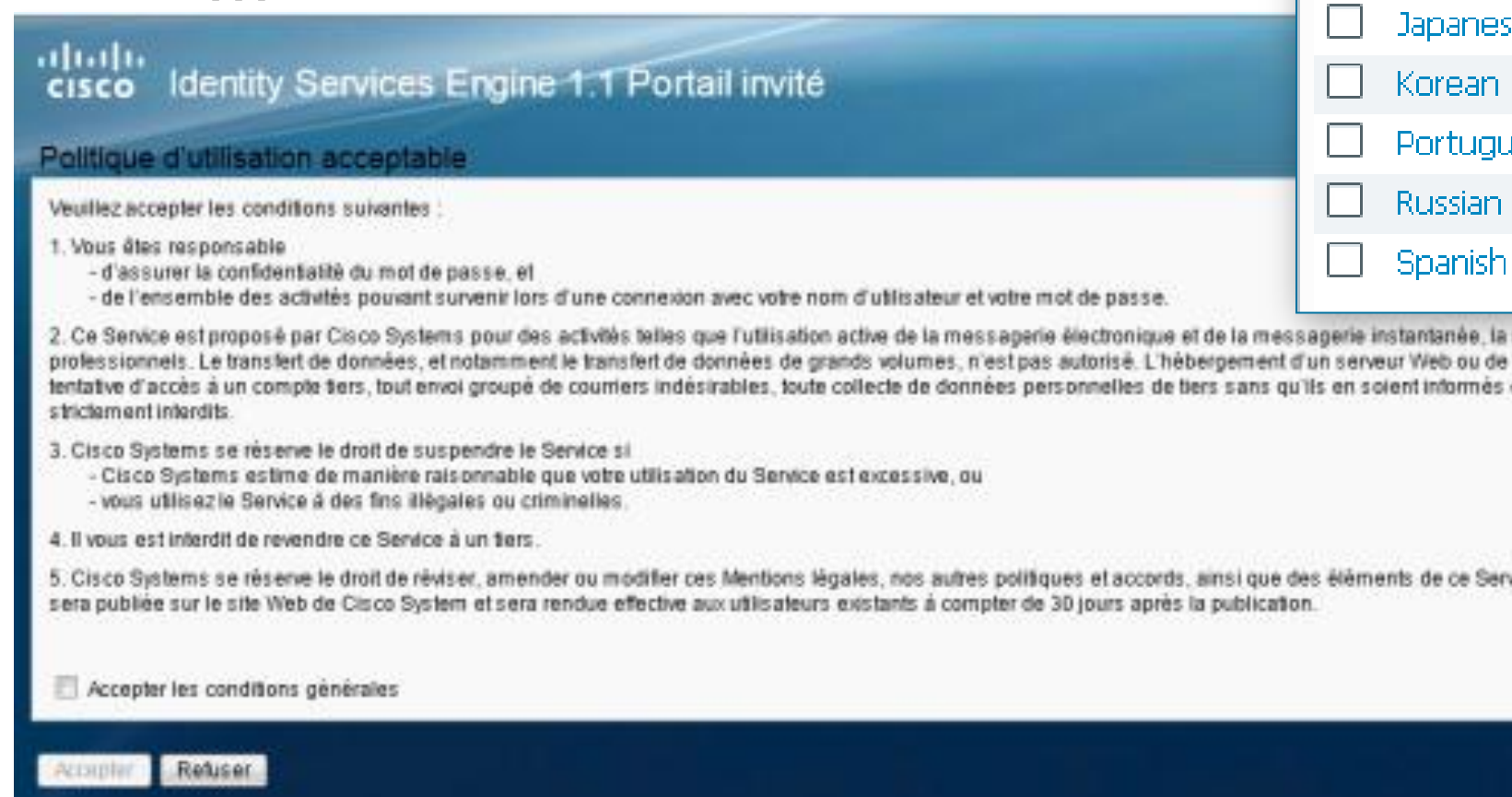
Guest Portal Language Templates > French Language Template

Configure Template Definition

---

**Configure Login Page**

* Username Field	Nom d'utilisateur :
* Password Field	Mot de passe :
* Login Button	Connexion
* Change Password Button	Modifier le mot de passe
* Self Service Button	Libre-service
* Device Registration Button	Enregistrement du périphérique



# Multiple Portals

Multiple portal might be needed based on:

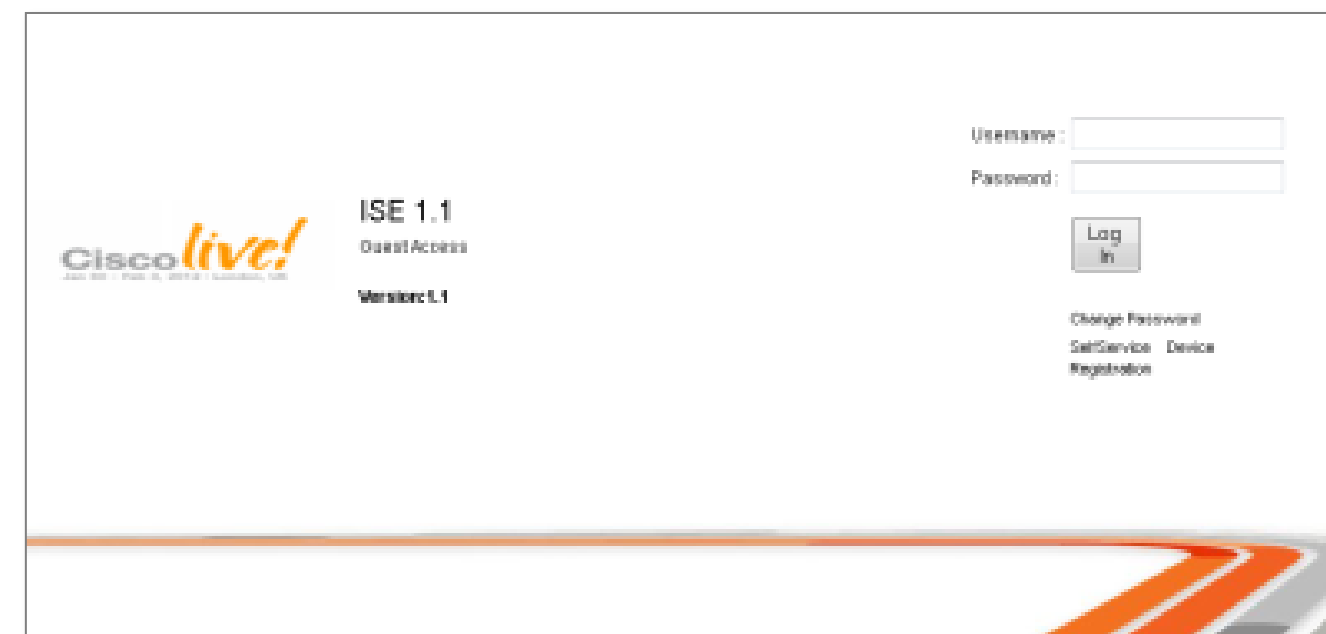
- Location / country
- When several organizational entities merge
- Type of device: WLC, switches
- For local language support



Default portal

Multi-Portal Configurations	
Multi-Portal Name	Portal Type
<input type="checkbox"/> DefaultGuestPortal	Default
<input type="checkbox"/> ciscoliveportal	CustomDefault

- Full portal customization or Default w/ selectable theme
- Simultaneous use of several portals for user and device registration



Sample customized portal theme



# Device Registration



# Device Registration Methods



## How Do I Register and Manage MAC Addresses in the Identity Stores?

Admin driven

- External Data Stores:  
Populate external directory (AD / LDAP) with devices to be allowed via MAB or Group lookup.

- Internal Data Stores:

**Manual entry or file import of accounts into Internal DB via Admin UI:** Simple method to add few entries or import large list of preconfigured accounts into ISE Internal Endpoint store. Allows specification of ID group for single entries, but requires admin to perform operation manually.

**Device Registration Web Auth (DRW):** Self-registration for current endpoint via special web portal. Does not require user credentials—only optional acceptance of AUP. MAC address of registering endpoint is entered into a predefined ID group. Once registered, access can be granted based on ID Group policy match.

**Web Auth Portal > Device Registration:** If enabled for web portal, option allows guest user accounts to self-register a predefined number of endpoints by MAC address. Registration results in static population of Internal Endpoint store **without** a default ID group assignment. User requires valid credentials (as defined under portal config) to register devices.

**My Devices Portal:** Employee portal for self-registration of personal devices by MAC Address with optional description up to a predefined number of endpoints. Static entry created in Internal Endpoint store with static ID group assignment to RegisteredDevices. Portal access is available via direct URL or Native Supplicant Provisioning (NSP) flow. Network Access User requires valid credentials as defined under My Devices portal configuration to register devices.

\* Currently no API support for create/update/delete operations for ISE endpoints

# Manual MAC Add/Import via Admin UI

Admin Registration—Static ID Groups of Known/Trusted Corporate MAC Addresses

- Administration > Identity Management > Identities > Endpoints

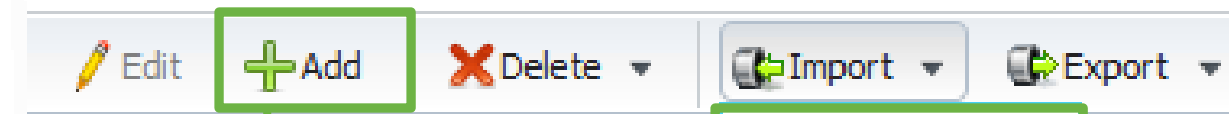
- Single device

  - Static Add

- Multiple devices

  - File Import

  - LDAP Import



**Endpoint**

\* MAC Address

Policy Assignment

Static Assignment

Identity Group Assignment

Static Group Assignment

Import from LDAP server:

\* Host

\* Port

Enable Secure Connection

Root CA Certificate Name

Anonymous Bind

Admin DN

Password

\* Base DN

\* MAC Address Object Class

\* MAC Address Attribute Name

Profile Attribute Name

\* Timeout  [seconds]

Must create matching ID group under profile

Select file to import:

\* File

**Note:** Please format your list of MAC address as follows:  **Example:** 00:1f:f3:4e:c1:8e, Cisco-Device

# Device Registration WebAuth (DRW)

## One-Time Registration from Special Web Portal

The screenshot shows the Cisco ISE configuration interface for a Multi-Portal Configuration. The breadcrumb path is "Multi-Portal Configuration List > New Multi-Portal Configuration". The "Settings" tab is active, and the "Operations" sub-tab is selected. The "Name" field is set to "DeviceRegistrationPortal". The "Description" field is empty. Under "Please select a portal type", the "Device Web Authorization Portal (Choose customization template and theme)" option is selected. The "EndPoint Identity Group" dropdown is set to "RegisteredDevices\_DRW".

**Annotations:**

- Optional AUP configuration:** Points to the "Operations" sub-tab.
- Default Portal Theme:** Points to the selected "Device Web Authorization Portal" radio button.
- Custom Portal option:** Points to the "Custom Device Web Authorization Portal (Upload files)" radio button.
- Static ID Group Assignment:** Points to the "RegisteredDevices\_DRW" dropdown selection.

# Device Registration WebAuth

## Sample Authorization Profile

- DRW configuration similar to CWA setup with URL Redirect and Redirect ACL

Authorization Profiles > New Authorization Profile

### Authorization Profile

\* Name

Description

\* Access Type

▼ Common Tasks

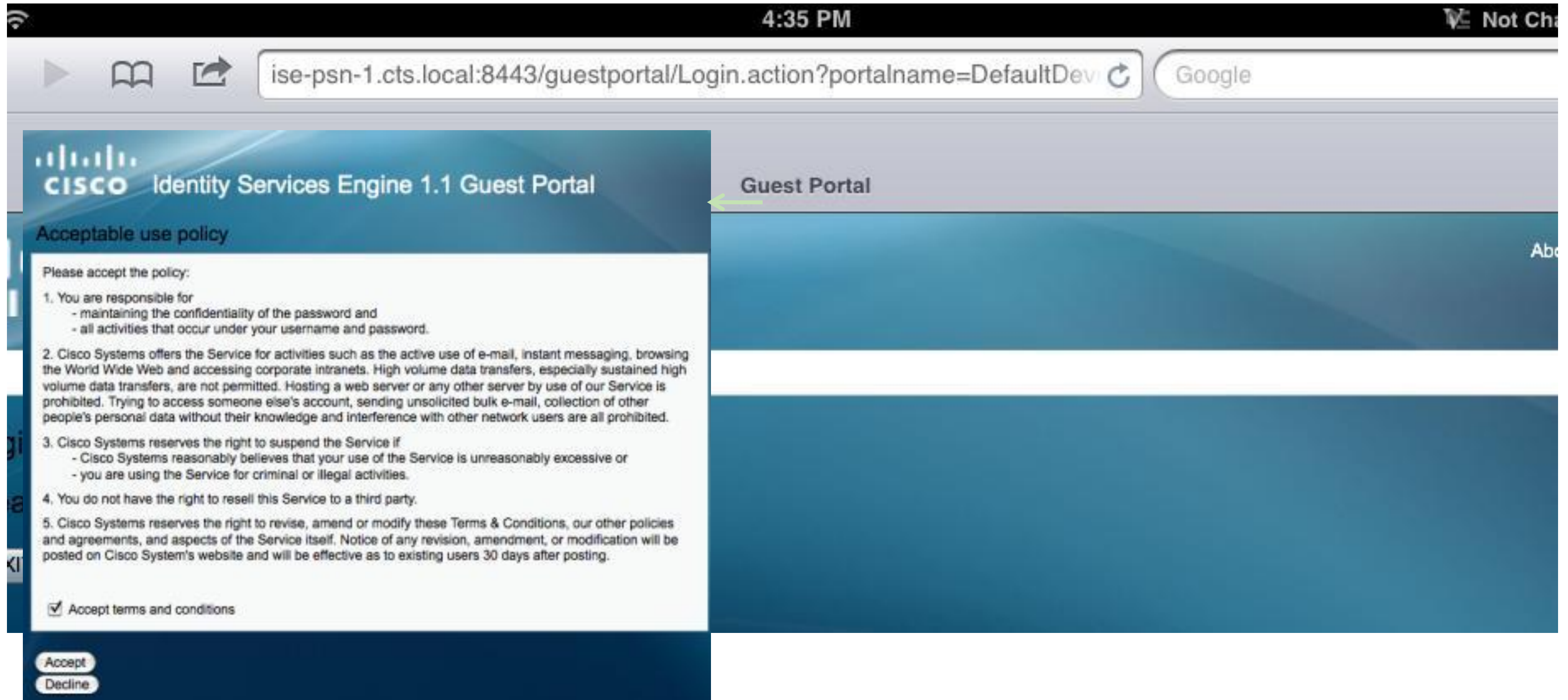
Web Authentication   Redirect

▼ Attributes Details

Access Type = ACCESS\_ACCEPT  
cisco-av-pair = url-redirect-acl=ACL-WEBAUTH-REDIRECT  
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&portal=DeviceRegistrationPortal&action=cwa&type=drw

# Device Registration WebAuth

## User Experience





# Guest Web Portal

## Device Registration for Guest Users

Administration > Web Portal Management > Settings > Guest > Multi-Portal Configuration

**Multi-Portal**

General **Operations** Customization Authentication

**Guest Portal Policy Configuration**  
Guest users should agree to an acceptable use policy

Not Used  
 First Login  
 Every Login

Enable Self-Provisioning Flow  
 Allow guest users to change password  
 Require guest users to change password at expiration and first login  
 Guest users should download the posture client  
 Guest users should be allowed to do self service  
 Guest users should be allowed to do device registration

Note: This is User ID Group used for self-service guest users, **not** self-service device registration

- Registered Devices are NOT assigned to an ID group by default.
- It is possible to use profiling with exception actions to statically assign ID group.\*

**Guest Portal Policy**

\* Self Registration Guest Role

\* Self Registration Time Profile

\* Maximum Login Failures  (Valid Range 1 to 9)

\* Device Registration Portal Limit  (Valid Range 1 to 20)

\* Guest Password Expiration (Days)  (Valid Range 1 to 999)

NOTE: Guest Password Expiration must be enabled in the Portal Configuration

Save Reset

\* ISE Device Registration and Policy Enforcement: <http://pmbuwiki.cisco.com/Products/ISE/Technical/Design-Config>

# Device Registration via Web Portal

## Guest User Experience

- Portal allows users to register their own devices
- Access can be granted to guests, employees, students
- Accessible by clicking **Device Registration** from ISE web auth portal.

The image illustrates the guest user experience for device registration on the Cisco Identity Services Engine (ISE) web portal. It consists of three sequential screenshots:

- Identity Services Engine 1.1 Guest Portal:** The user is prompted to enter a Username and Password. A **Device Registration** link is highlighted in the bottom navigation menu.
- Device Registration Portal:** The user is prompted to register their device. A **Register** button is highlighted.
- Device Registration Portal (Success):** The user receives a success message: "MAC Address is successfully registered." The MAC address 00:C4:23:59:C4:89 is displayed. Below the message is a table of registered devices.

Registered Devices	
<input type="checkbox"/>	MAC Address
<input type="checkbox"/>	00:C4:23:59:C4:89
<input type="checkbox"/>	AA:BB:CC:DD:EE:FF

# My Devices Portal

## Device Registration for Network Access Users\*

- Devices registered via MDP are statically assigned to RegisteredDevices endpoint ID group.

The screenshot shows the 'Settings' tab in the Cisco ISE configuration interface. The left sidebar contains a tree view with folders for 'General', 'Sponsor', 'My Devices', and 'Guest'. Under 'My Devices', 'Portal Configuration' is selected. The main content area is titled 'My Devices Portal Settings' and is highlighted with a green rounded rectangle. It contains the following sections:

- General**:  Enable My Devices Portal
- Acceptable Use Policy**:  Enable the Acceptable Use Policy link. Reminder: If the AUP link is enabled, please set the AUP text on all the appropriate My Devices Portal language templates.
- Device Management**: \* The maximum number of devices to register  (Valid Range 1 to 20)
- Help Desk**:
  - Email Address
  - Phone Number

# My Devices Portal

## Network Access User Experience

- <http://<PSN>:8443/mydevices> (or use simplified URL)

Flagging a device as 'Lost' will add it to the Blacklist; CoA with Session Terminate action also sent.

- Optionally configure port TCP/443 for portal access.
- Portal not available to Guest user accounts.

### Add a New Device

To add a device, please enter the Device ID (MAC Address) and a description (optional); then click submit to add the device.

\* Device ID

Description



**Marking this device as lost will remove it from the network and lock it out until reinstated via this portal. Are you sure you would like to proceed?**

### Your Devices

State	Device ID	Description	Action
	00:11:22:33:44:55	My Windows Laptop	Edit   <b>Lost?</b>
	11:22:33:44:55:66	My iPad	Edit   Lost?
	22:33:44:55:66:77	My Android Phone	Edit   Reinststate

# Device Registration Methods

## Comparison Summary Table

Device Registration Method	ID Group Assigned	Device Limit	Created By	De-Registration Method	Target Endpoints
Manual Update of Endpoint Database	Yes. Configurable per endpoint.	100k	Administrator (requires authentication to ISE Admin UI)	Administrator must manually change ID Group/Policy assignment or delete entry in endpoint database.	Administratively-defined endpoints—bulk import options supported
Device Registration WebAuth (DRW)	Yes. Configurable by DRW portal.	100k	Any endpoint with DRW portal access (no authentication required)		Self-Service – Access without requiring any auth credentials.
WebAuth Portal	No	Up to 20. (Global setting)	Guest or Network Access User authenticated via web portal		Self-Service – Guest / WebAuth users
My Devices Portal (MDP)	Yes. Static assignment to RegisteredDevices	Up to 20. (Global setting)	Network Access User authenticated using MDP or via Native Supplicant Provisioning flow (for example, user authenticated via CWA or 802.1X PEAP)	Network Access User can remove device from Registered Devices list via MDP, but Administrator must manually delete entry in endpoint database to permanently remove.	Self-Service – Network Access (non-Guest) users

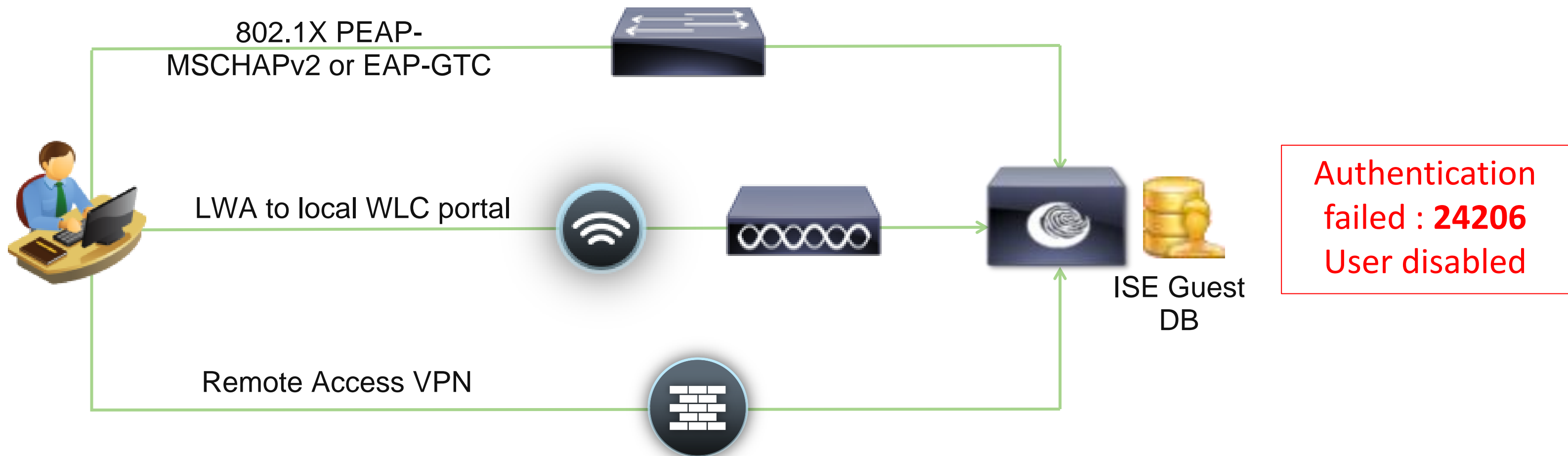
# Pre-Activated Guests





# Authenticating Sponsored Guests w/o Web Auth

- 802.1X users with EAP based on username/password
- LWA users that authenticate against non-ISE portal
- Remote Access VPN clients unable to login using ISE Sponsored Guest accounts.




# Sponsored Guest Authentication via 802.1X

## Problem Statement

- Auth methods **not** based on an initial web auth to ISE portal such as 802.1X, VPN, or LWA using local portal fail.

Authentication failed : **24206** User disabled

- Reason: Sponsored guest accounts require activation via ISE web portal
- Web auth to ISE portal supports compliance with any AUP and password change policy that may be configured.

 **Successfully Created Guest Account: auser001**

Username: auser001  
Password: p~0AuH869  
First Name: Another  
Last Name: User  
Email Address: auser@abc.com  
Phone Number: (888)555-2222  
Company: ABC



Status: **AWAITING INITIAL LOGIN**

Suspended: false  
Optional Data 1: tech support call  
Optional Data 2:  
Optional Data 3:  
Optional Data 4:  
Optional Data 5:

Group Role: **Guest**

Time Profile: DefaultOneHour

Timezone: US/Eastern

 Account Start Date: 2012-04-06 22:01:24 EDT  
 Account Expiration Date: 2012-04-06 23:01:24 EDT

Language Template for Email/SMS Notifications: English


[Email](#) [Print](#) [Create Another Account](#) [View All Accounts](#)

Standard Guest account in "AWAITING\_INITIAL\_LOGIN" state after creation

# Immediate Guest Account Activation

## Solution

- Pre-Activated Guest Accounts
- Assigning Guest users to the special **ActivatedGuest** Identity Group allows immediate activation of those accounts.
- Sponsor Group must be assigned privilege to create guests using this ID group.
- AUP and Change Password policies cannot be enforced with pre-activated guest accounts.

 **Successfully Created Guest Account: guser001**

Username: guser001  
Password: p~0AuH869  
First Name: Guest  
Last Name: User  
Email Address: guser@company.com  
Phone Number: (999)555-1111  
Company: Company, Inc.

Status: **ACTIVE**

Suspended: false  
Optional Data 1: Important Meeting  
Optional Data 2:  
Optional Data 3:  
Optional Data 4:  
Optional Data 5:

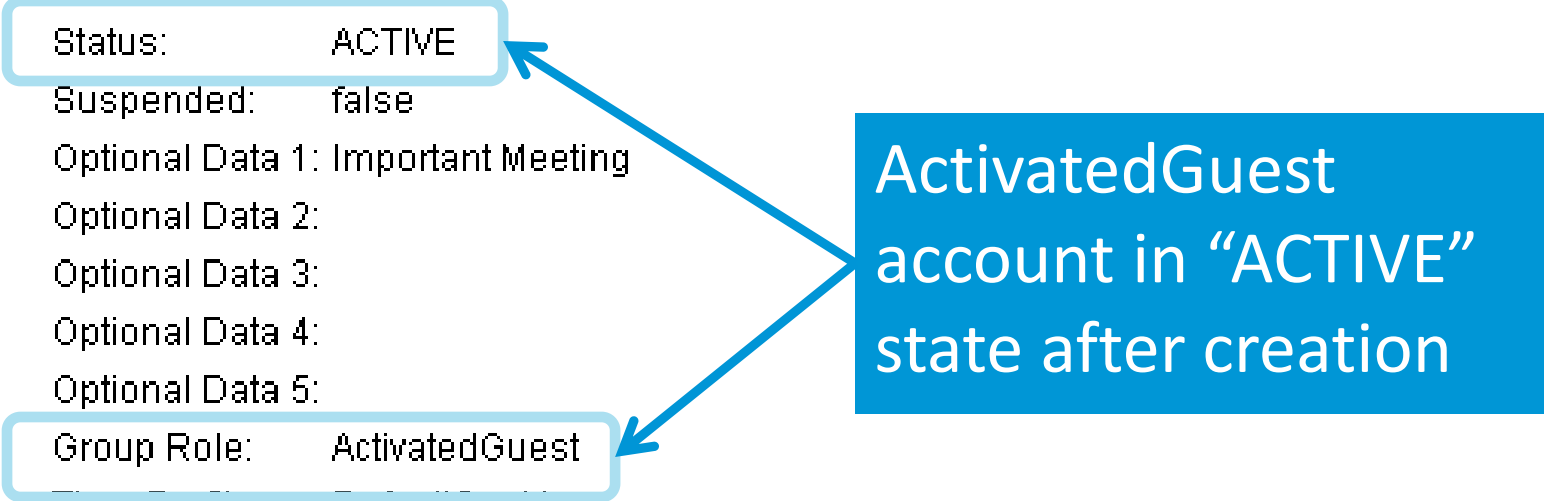
Group Role: **ActivatedGuest**  
Time Profile: DefaultOneHour

Timezone: US/Eastern  
🔧 Account Start Date: 2012-04-06 21:57:41 EDT  
🔧 Account Expiration Date: 2012-04-06 22:57:41 EDT

Language Template for Email/SMS Notifications: English

[Email](#) [Print](#) [Create Another Account](#) [View All Accounts](#)

**ActivatedGuest account in "ACTIVE" state after creation**



# Monitoring Guests



# Specific Guest Reports

The screenshot shows the Cisco ISE Reports interface. At the top, there are navigation tabs for 'Authentications', 'Endpoint Protection Service', and 'Alarms'. Below these are 'Favorites', 'Shared', 'Catalog', and 'System' buttons. A left sidebar lists various report categories, with 'User' selected. The main area displays a 'User' report list with a search filter and a table of reports. The 'Guest Accounting' report is highlighted with an orange box. Three callout boxes provide descriptions for different reports: 'User', 'Guest Accounting', and 'Guest Activity'. A green callout box notes that 'Guest Activity' shows guest URL activity when Firewall syslogs are sent to ISE.

**Description:**  
View the logged in/out information for the particular Guest user for a selected time period

**Description:**  
View the Guest information for a selected time period

**Shows guest URL activity when Firewall syslogs sent to ISE**

**Description:**  
View the sponsor information along with the graphical representation for a selected time period

# Configure ASA to Send HTTP Syslogs to ISE (1/2)

File View Tools Wizards Window Help Look For:  Go

Home Configuration Monitoring Save Refresh Back Forward Help

**Device Management**

- Management Access
- Licensing Activation Key
- System Image/Configuration
- High Availability
- Logging
  - Logging Setup
  - E-Mail Setup
  - Event Lists
  - Logging Filters
  - Rate Limit
  - Syslog Servers**
  - Syslog Setup
  - SMTP
  - NetFlow
- Smart Call-Home
- Users/AAA
- Certificate Management
- DHCP
- DNS
- Advanced

**Configuration > Device Management > Logging > Syslog Servers**

Specify up to 16 syslog servers. Make sure logging is enabled in Configuration > Device Management > Logging > Logging Setup.

Interface	IP Address	Protocol/Port	EMBLEM	Secure
inside	10.100.7.10	UDP/20514	No	No

Add Edit Delete

**Send syslogs to ISE MNT: UDP port 20514**

**Configuration > Device Management > Logging > Event Lists**

Use event lists to define a particular set of syslogs that you are interested in. The event list can be used to filter syslogs sent to a logging destination.

Name	Event Class / Severity	Message IDs
HTTP_URL_logs		304001

Add Edit Delete

**Filter messages ID # 304001: accessed URLs**



# Configure ASA to Send HTTP Syslogs to ISE (2/2)

**Configuration > Firewall > Service Policy Rules**

+ Add Edit Delete | ↑ ↓ | ✂ | Find Diagram

Traffic Classification								Rule Actions
Name	#	Enabled	Match	Source	Destination	Service	Time	
Interface: inside; Policy: inside-http-guest-policy								
guest-http-class 1	1	<input checked="" type="checkbox"/>	Match	guest-subnet	any	ip		Inspect HTTP
global; Policy: global_policy								
inspection_de...			Match	any	any	default-inspec...		Inspect DNS Map preset... Inspect ESMTTP

**Create Service Policy in ASA to inspect HTTP traffic for guest subnet**

**ISE shows accessed URLs in reports**

**User > Guest Activity**

Showing Page 1 of 1 | First Prev Next Last | Goto Page:  Go

**Guest > Guest Activity**

Date : November 22, 2011 05:03:15 PM - November 22, 2011 05:33:15 PM ( Last 30 Minutes | Last Hour | Last 12 Hours | Today | Yesterday | Last 7 Days | Last 30 D

Generated on November 22, 2011 5:33:15 PM GMT

[Reload](#)

Logged At	Guest	Guest IP	Message
Nov 22, 2011 5:31 PM	mumu@cisco.com	10.100.14.103	%ASA-5-304001: 10.100.14.103 Accessed URL 10.100.200.1:http://10.100.200.1/fpv.js
Nov 22, 2011 5:31 PM	mumu@cisco.com	10.100.14.103	%ASA-5-304001: 10.100.14.103 Accessed URL 10.100.200.1:http://10.100.200.1/discover.js
Nov 22, 2011 5:31 PM	mumu@cisco.com	10.100.14.103	%ASA-5-304001: 10.100.14.103 Accessed URL 10.100.200.1:http://10.100.200.1/framework.js
Nov 22, 2011 5:31 PM	mumu@cisco.com	10.100.14.103	%ASA-5-304001: 10.100.14.103 Accessed URL 10.100.200.1:http://10.100.200.1/ajax.js
Nov 22, 2011 5:31 PM	mumu@cisco.com	10.100.14.103	%ASA-5-304001: 10.100.14.103 Accessed URL 10.100.200.1:http://10.100.200.1/preflight.js
Nov 22, 2011 5:31 PM	mumu@cisco.com	10.100.14.103	%ASA-5-304001: 10.100.14.103 Accessed URL 10.100.200.1:http://10.100.200.1/
Nov 22, 2011 5:31 PM	mumu@cisco.com	10.100.14.103	%ASA-5-304001: 10.100.14.103 Accessed URL 10.100.200.1:http://10.100.200.1/
Nov 22, 2011 5:31 PM	mumu@cisco.com	10.100.14.103	%ASA-5-304001: 10.100.14.103 Accessed URL 10.100.200.1:http://10.100.200.1/

# Support Resources

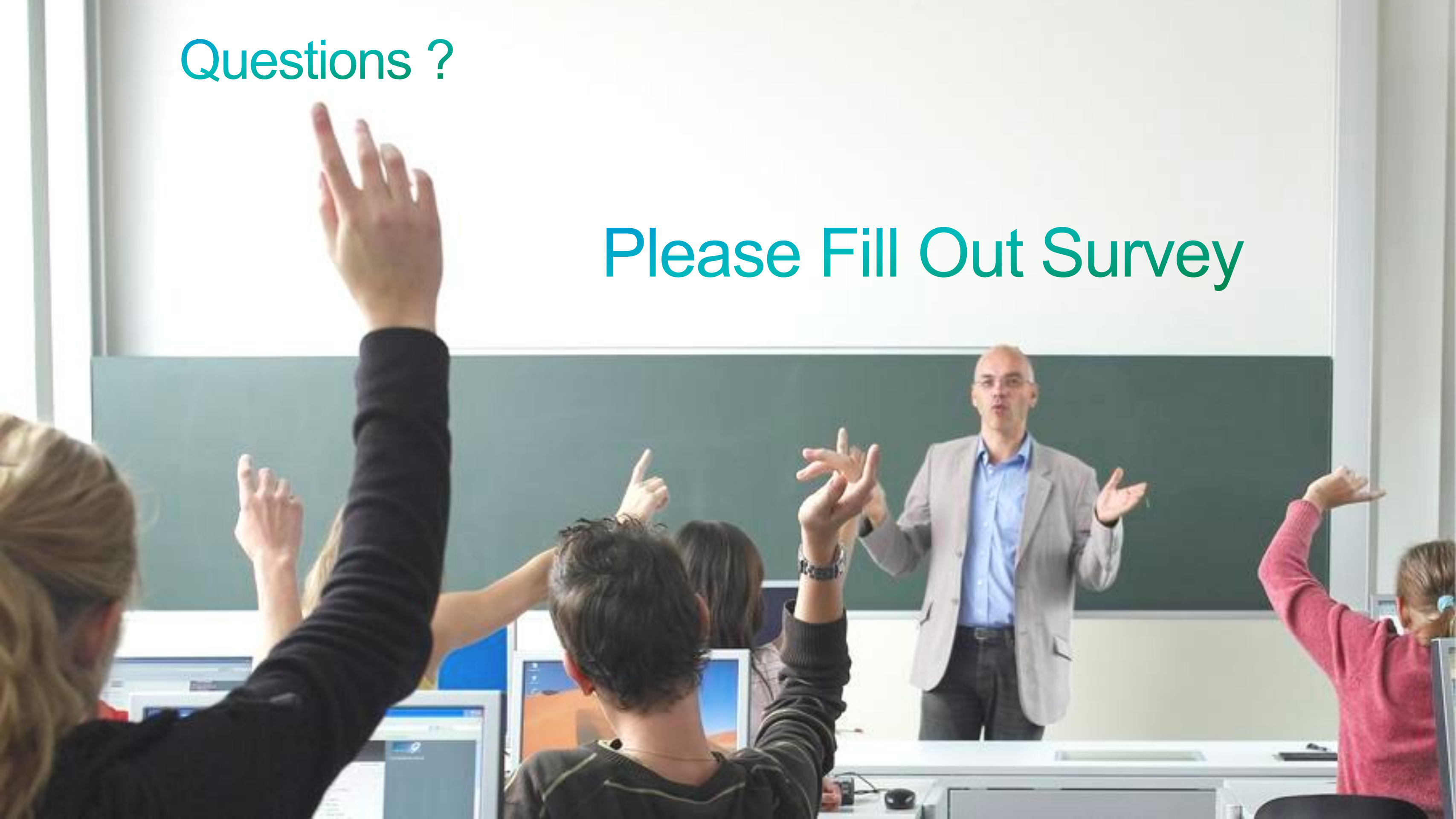
- ISE Product - <http://www.cisco.com/go/ise>
- TrustSec - <http://www.cisco.com/go/trustsec>
- ISE 1.1.1 Demos

<https://communities.cisco.com/community/partner/borderlessnetworks/security?view=video>

- dCloud BYOD Hosted Demos – <http://www.cisco.com/go/byoddemo>
- Free NFR Lab Software for Partners (1.1.1 Available)  
Cisco Marketplace - \$35 VMware image, perpetual license, 20 endpoints  
<http://cisco.mediuscorp.com/ise>
- PDI Helpdesk - Webpage: <http://www.cisco.com/go/pdihelpdesk>
- Program-related questions: [pdihd-bn@cisco.com](mailto:pdihd-bn@cisco.com)
- **Your Cisco PDM and CSE**

Questions ?

Please Fill Out Survey



# Cisco ISE ATP Resources

- ISE ATP Portal: <http://ciscosecurityatp.com/>
- Cisco Partner ISE Resources: <http://cisco.com/go/isepartner>
- ISE ATP HLD Webinar: <https://communities.cisco.com/docs/DOC-27689>
- ISE HLD Help Alias (US): [ise\\_hld\\_help@cisco.com](mailto:ise_hld_help@cisco.com)
- ATP requirements and guidelines for ISE:  
[http://www.cisco.com/web/partners/partner\\_with\\_cisco/channel\\_partner\\_program/resale/atp/ise.html](http://www.cisco.com/web/partners/partner_with_cisco/channel_partner_program/resale/atp/ise.html)
- Sales Acceleration Center (SAC) for HLD submissions: [sac-support@cisco.com](mailto:sac-support@cisco.com)
- SAMPG Partner Team:  
Sheila Rone [srone@cisco.com](mailto:srone@cisco.com)  
Phuong Nguyen [pvnguyen@cisco.com](mailto:pvnguyen@cisco.com)

# Additional Training

- ISE Security Basics - <https://communities.cisco.com/docs/DOC-30718>
- ISE Best Practices VoD - Security Express - Replays and Presentations  
<https://communities.cisco.com/docs/DOC-18350>
- 802.1X Training on PEC  
<http://tools.cisco.com/pecx/login?URL=searchOffering%3FcourseId=00028869>  
<http://tools.cisco.com/pecx/login?URL=searchOffering%3FcourseId=00028870>  
<http://tools.cisco.com/pecx/login?URL=searchOffering%3FcourseId=00028851>
- Team MIDAS Wireless ISE and BYOD classes  
Tech Sessions: <http://cisco.cvent.com/d/ccqs4s>  
Hands-On Lab Sessions: <http://cisco.cvent.com/d/kcqs43>  
Lab Guide: <https://communities.cisco.com/docs/DOC-30944>