Cisco live!

What You Make Possible

TOMORROW
starts here.

cisco

Cisco live!

Deploying Wireless Guest Access

BRKEWN-2013

TOMORROW starts here.

cisco

Abstract

This session focuses on design requirements and deployment considerations for a wireless guest access solution. It discusses the main components of an end-to-end guest access solution including how to provide network access to visitors and route guest traffic across the network that is safe and secure. Attendees will be introduced to a detailed discussion on various guest access services directly on the wireless LAN controllers (WLC), management of Guest services using Cisco Prime Infrastructure, and integration with the Identity Services Engine (ISE) for various external web authentication services such as sponsored and self-service options. We will also discuss FlexConnect, Guest Anchor, and enhanced guest security with WLC and ISE. This session is especially useful for those attendees responsible for the Design, Deployment, Operations and Management of Enterprise Campus Wireless Networks. It is assumed that those attending this session have a working knowledge of LAN switching and routing, fundamentals in 802.1x and Network Admission Control. Knowledge of 802.11 WLAN fundamentals and WLAN security is required.

Agenda

- Overview : Guest Access as a Supplementary User Authentication
- Guest Access Control & Path Isolation
- Secure Guest in FlexConnect
- Guest Authentication Portal
- Guest Provisioning
- Monitoring & Reporting

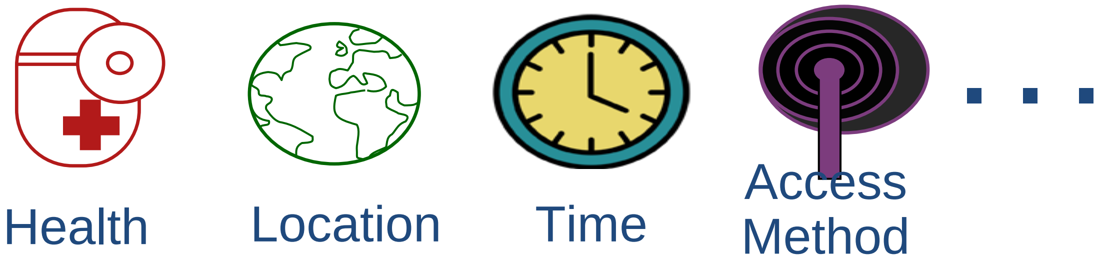
Session Objectives

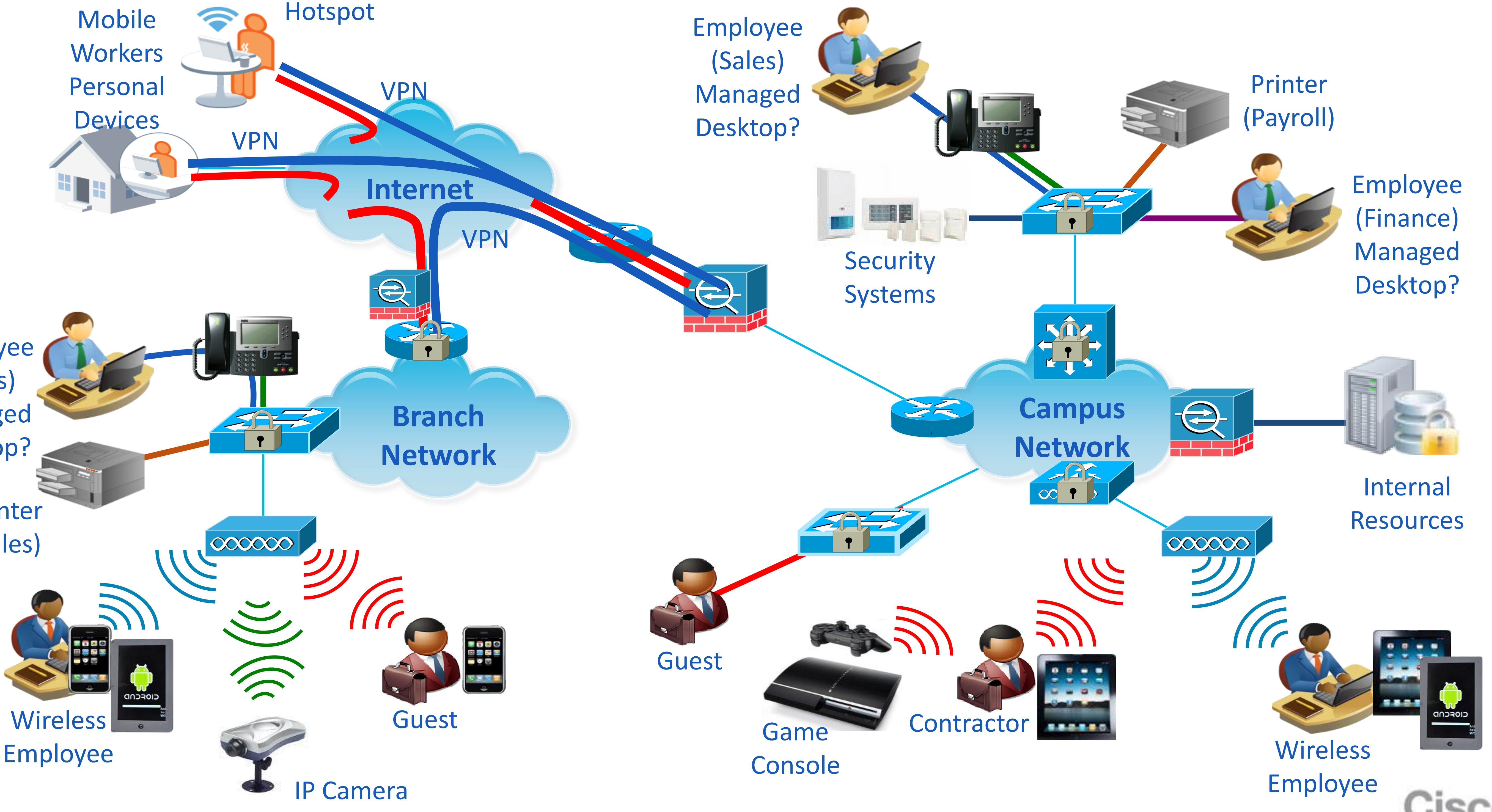
- Understand what makes up a wireless guest access service
- Learn about the importance of isolating guest traffic
- See how secure guest access is integrated in Cisco Wireless
- Understand guest services in a FlexConnect environment
- Discover how Cisco ISE enhances guest services

Guest Access Overview

Evolution of Network Access

Age of the Borderless Network





Context-Based Access

Who = User Identity

- Known/Managed Users (Long-term)

Examples: Employees/Staff, Faculty/Students, Extended Access Partners/Contractors

Primary Auth Methods: 802.1X or Agent-based

Considerations:

Identity Stores

EAP types and supplicant

- Unknown/Unmanaged Users (Temporary or Infrequent Access)

Examples: Guests, Visitors, Short-term Partners/Contractors

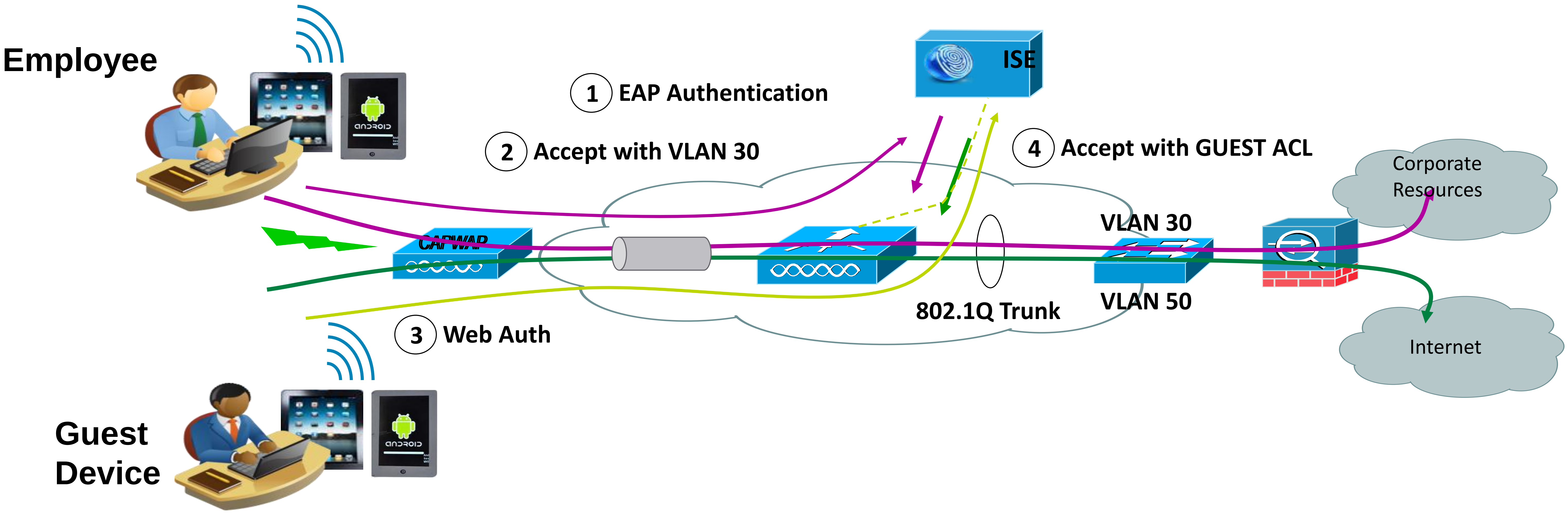
Primary Auth Method: Web authentication

Considerations:

Web Redirection and Authentication Portals

Guest Provisioning and Identity Stores

Corporate vs Guests



- Users with Corporate Devices with their AD user id can be assigned to Employee VLAN
- Guests authenticate via Web Auth and are assigned to a GUEST-ACL on the Guest VLAN

Requirements for Secure Guest Access

Technical

- No access until authorised
- Guest traffic should be segregated from the internal network
- Web-based authentication
- Full auditing of location, MAC, IP address, username
- Overlay onto existing enterprise network
- Bandwidth and QoS management

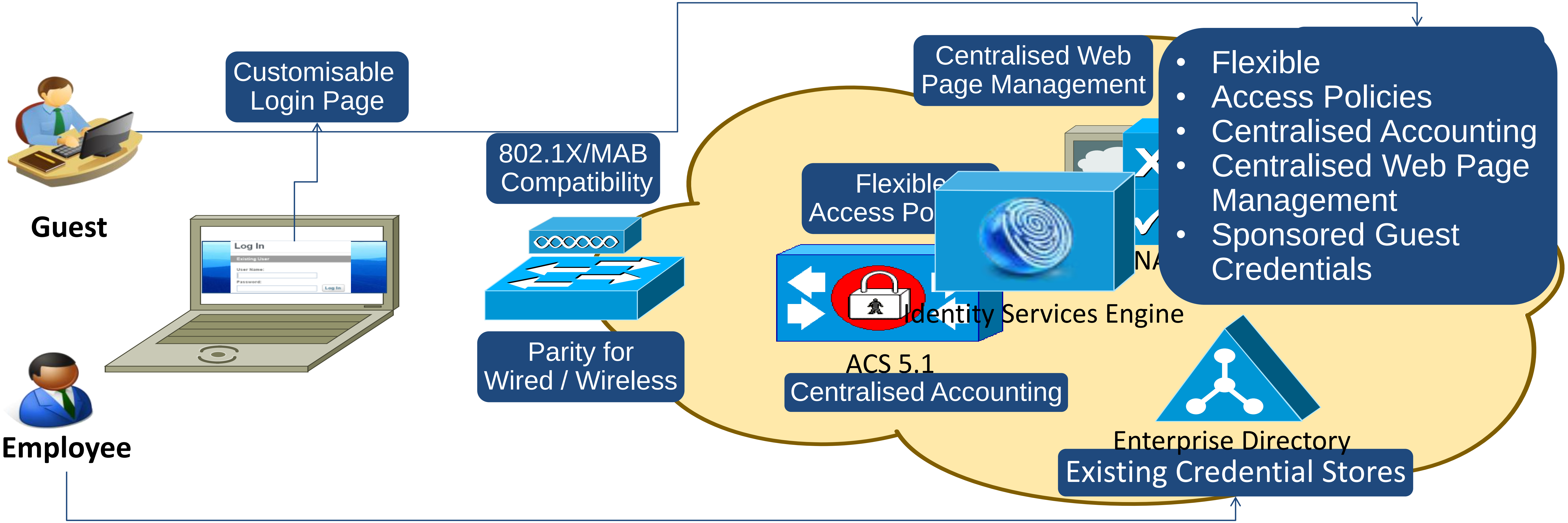
Usability

- No laptop reconfiguration, no client software required
- Plug & Play
- Splash screens and web content can differ by location
- Easy administration by non-IT staff
- “Guest network” must be free or cost-effective and non-disruptive

Monitoring

- Mandatory acceptance of disclaimer or Acceptable Use Policy (AUP) before access is granted
- Logging and Monitoring
- Must not require guest desktop software or configuration

Guest Access Components



- Flexible
- Access Policies
- Centralised Accounting
- Centralised Web Page Management
- Sponsored Guest Credentials

Integrated Access Authentication

Guest Access Control & Path Isolation

Access Control

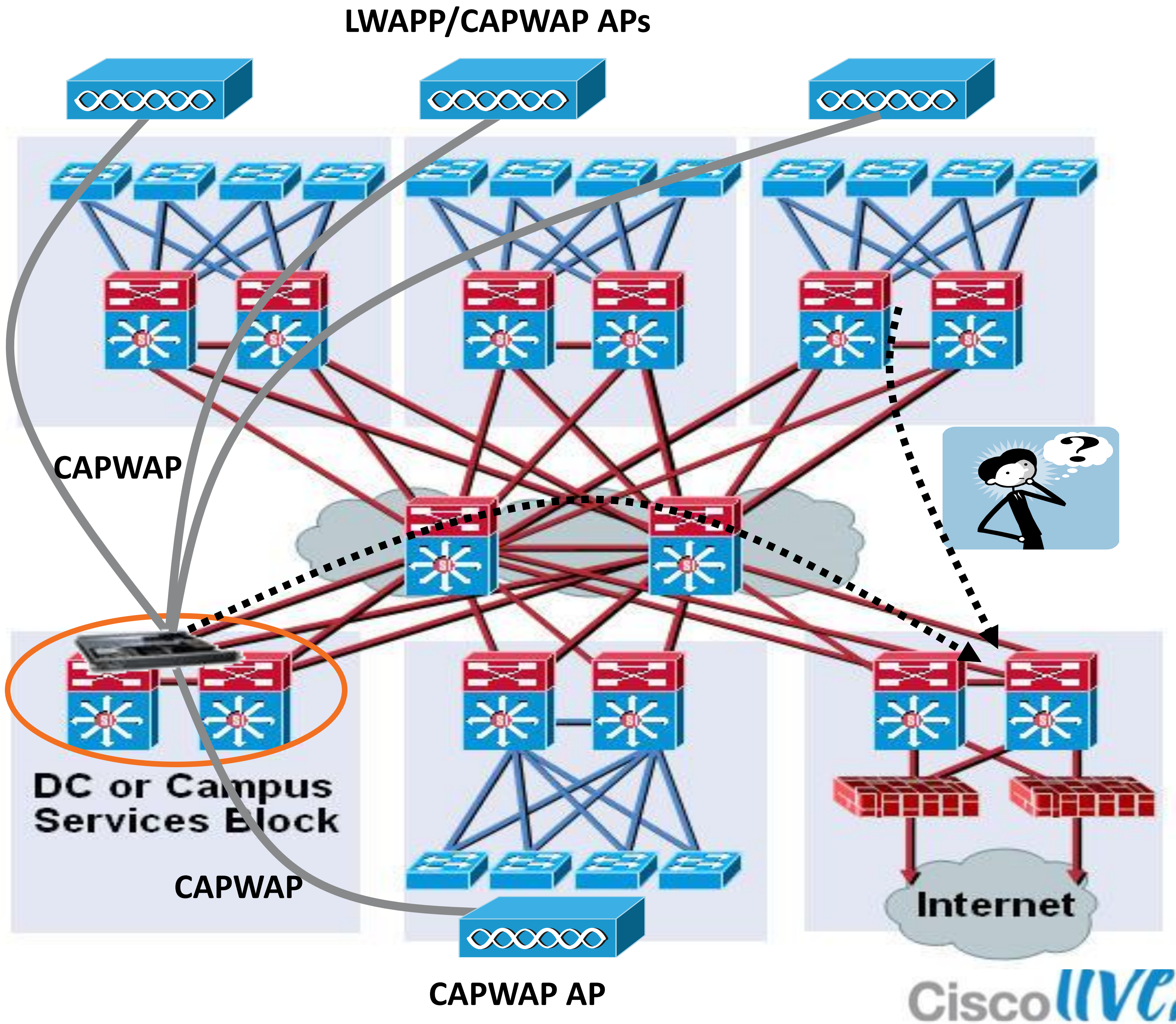
End-to-End Wireless Traffic Isolation

The fact

- Traffic isolation achieved via LWAPP/CAPWAP valid from the AP to the WLAN Controller

The challenge

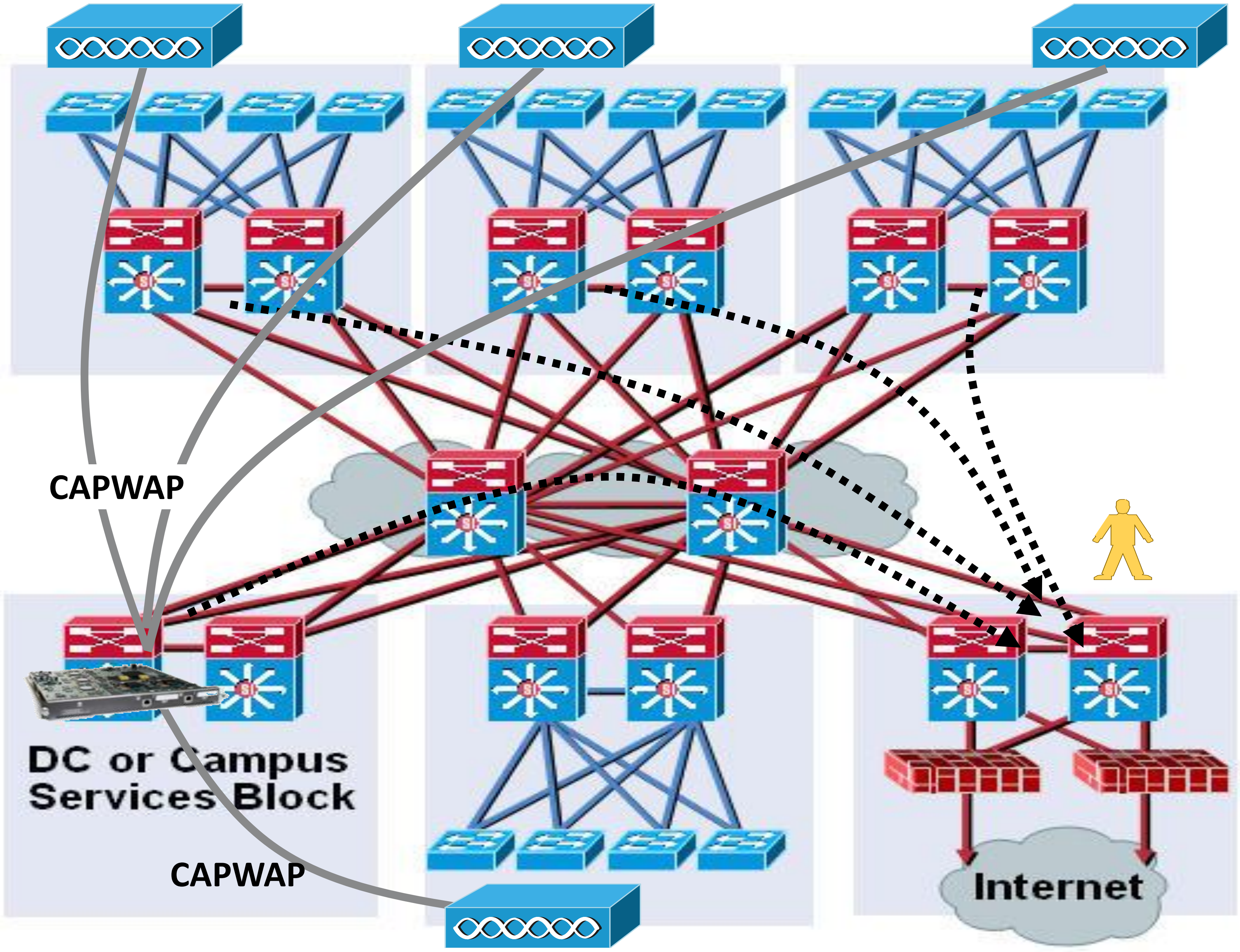
- How to provide end-to-end wireless guest traffic isolation, allowing internet access but preventing any other communications?



Path Isolation

Why Do We Need It for Guest Access?

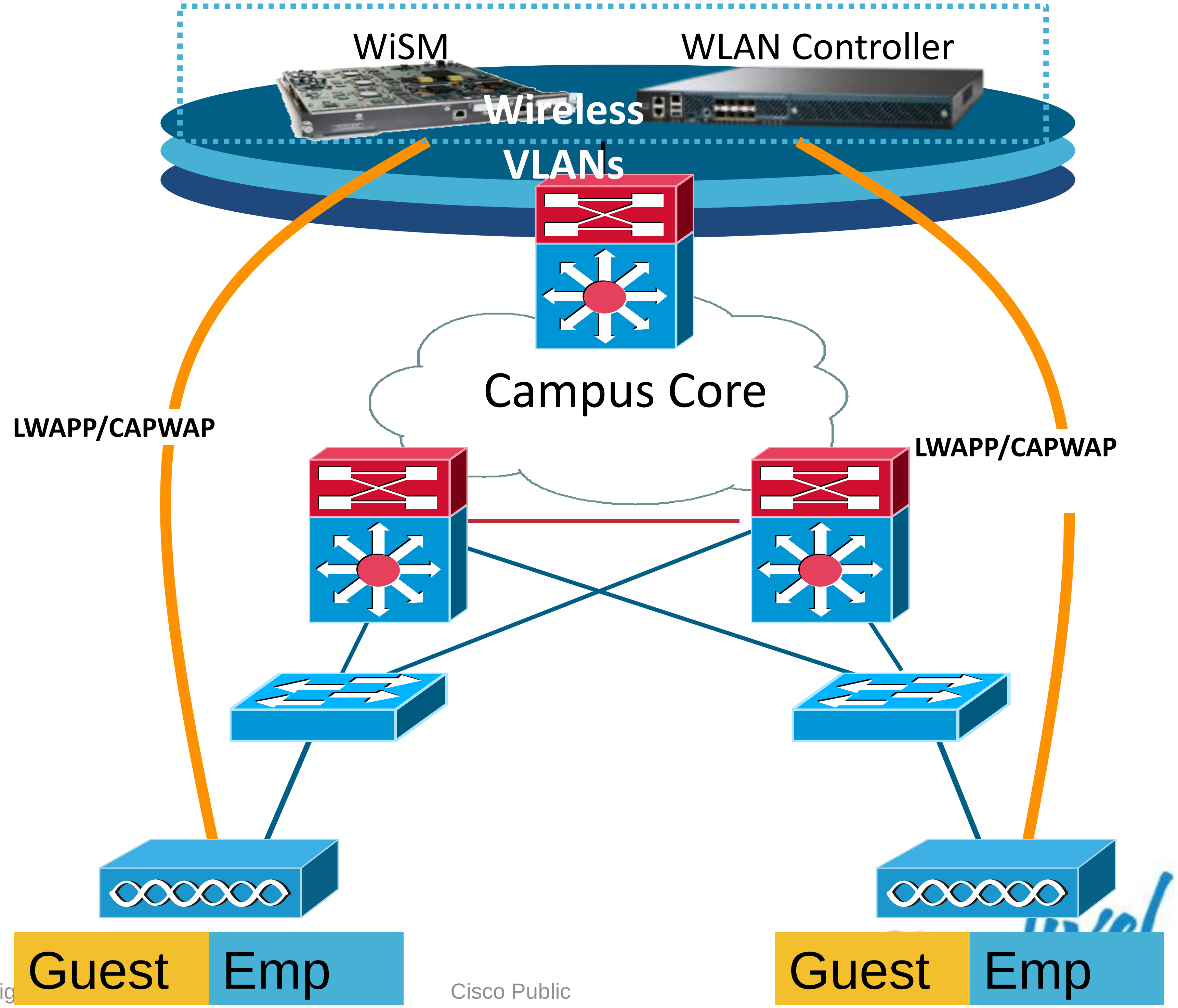
- Extend traffic logical isolation end-to-end over L3 network domain
- Separate and differentiate the guest traffic from the corporate internal traffic (security policies, QoS, bandwidth, etc.)
- Securely transport the guest traffic across the internal network infrastructure to DMZ



Guest Access Control

Cisco WLAN Controller Deployments

- LWAPP/CAPWAP tunnel is a Layer 2 tunnel (encapsulates original Ethernet frame)
- Same LWAPP/CAPWAP tunnel used for data traffic of different SSIDs
- Control and data traffic tunneled to the controller via LWAPP/CAPWAP:
  data uses UDP 12222/5247
  control uses UDP 12223/5246
- Data traffic bridged by WLAN controller on a unique VLAN corresponding to each SSID
- Traffic isolation provided by VLANs is valid up to the switch where the controller is connected



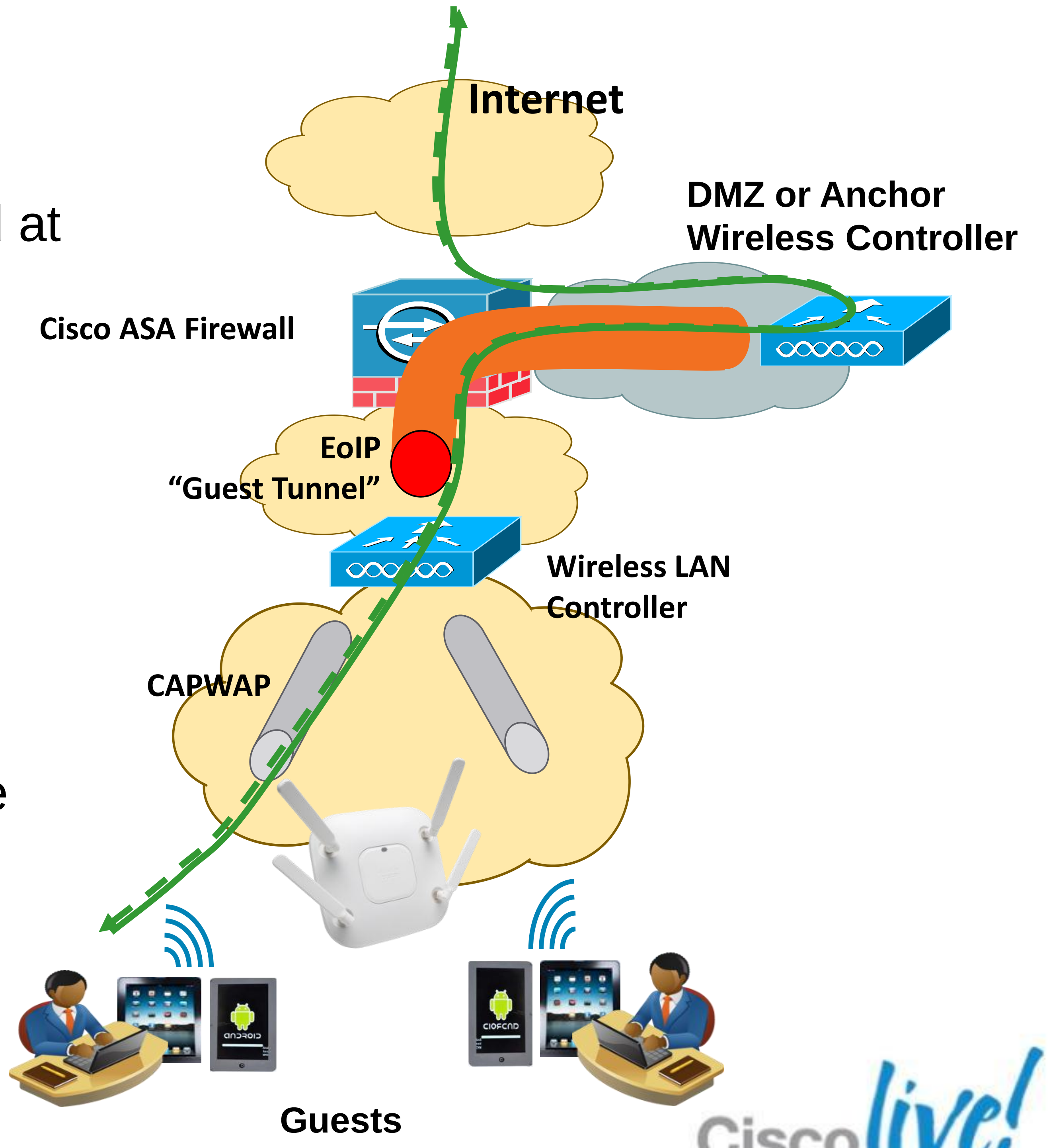
LWAPP—Lightweight Access Point Protocol

CAPWAP - Control And Provisioning of Wireless Access Points

Solution #1: Path Isolation using EoIP

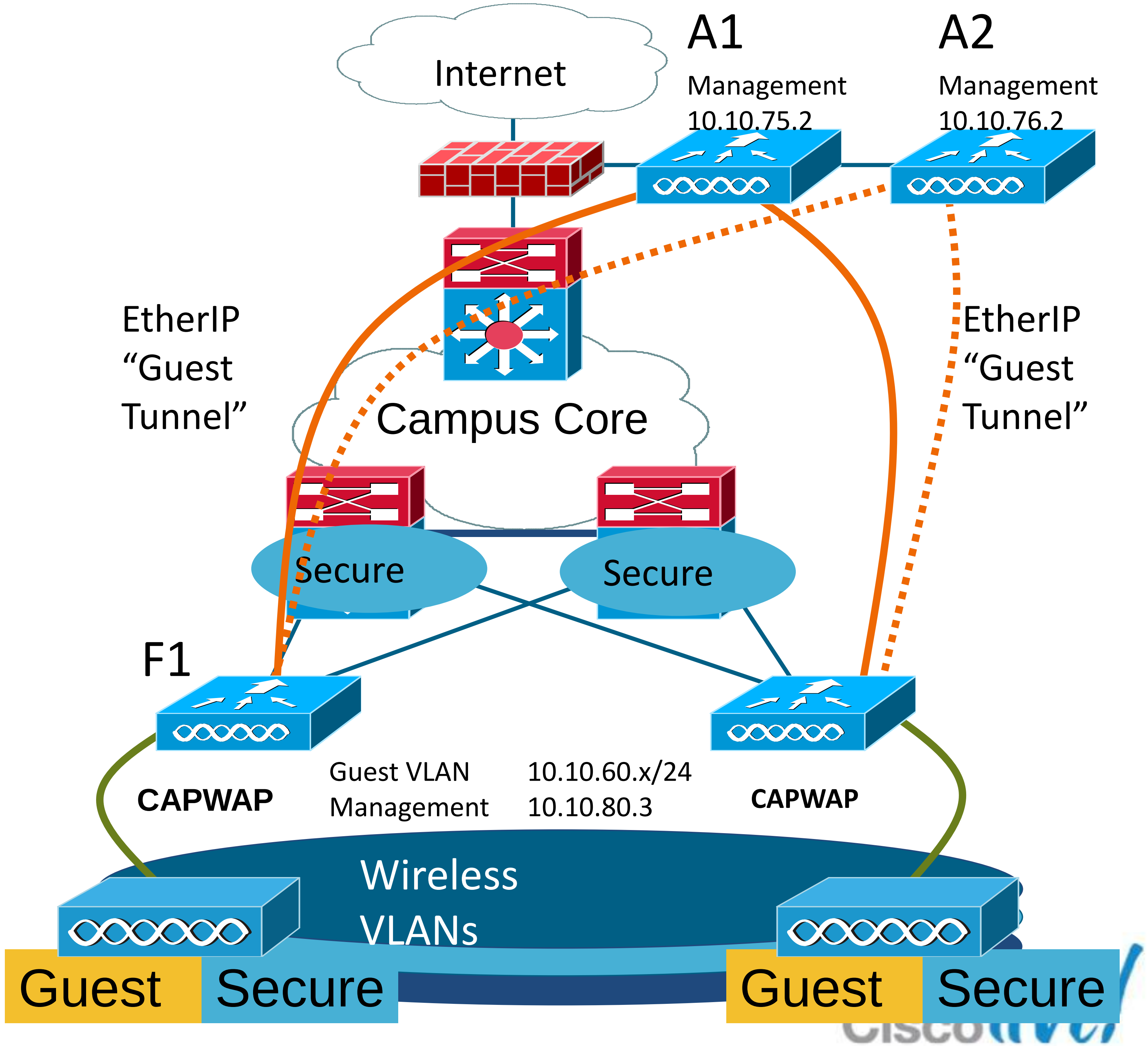
WLAN Controller Deployments with EoIP Tunnel

- Use of up to 71 EoIP tunnels to logically segment and transport the guest traffic between remote and anchor controllers
- Other traffic (employee for example) still locally bridged at the remote controller on the corresponding VLAN
- No need to define the guest VLANs on the switches connected to the remote controllers
- Original guest's Ethernet frame maintained across LWAPP/CAPWAP and EoIP tunnels
- Redundant EoIP tunnels to the Anchor WLC
- 2100/2500 series and WLCM models can not terminate EoIP connections (no anchor role) or support IPSec Encrypted Tunnels on the remote WLC



Guest Network Redundancy

- Using EoIP Pings (data path) functionality Anchor WLC reachability will be determined
- Foreign WLC will send pings at configurable intervals to see if Anchor WLC is alive
- Once an Anchor WLC failure is detected a DEAUTH is send to the client
- Remote WLC will keep on monitoring the Anchor WLC
- Under normal conditions round-robin fashion is used to balance clients between Anchor WLCs



Primary Link

Redundant Link

Implementing Guest Path Isolation Using WLC

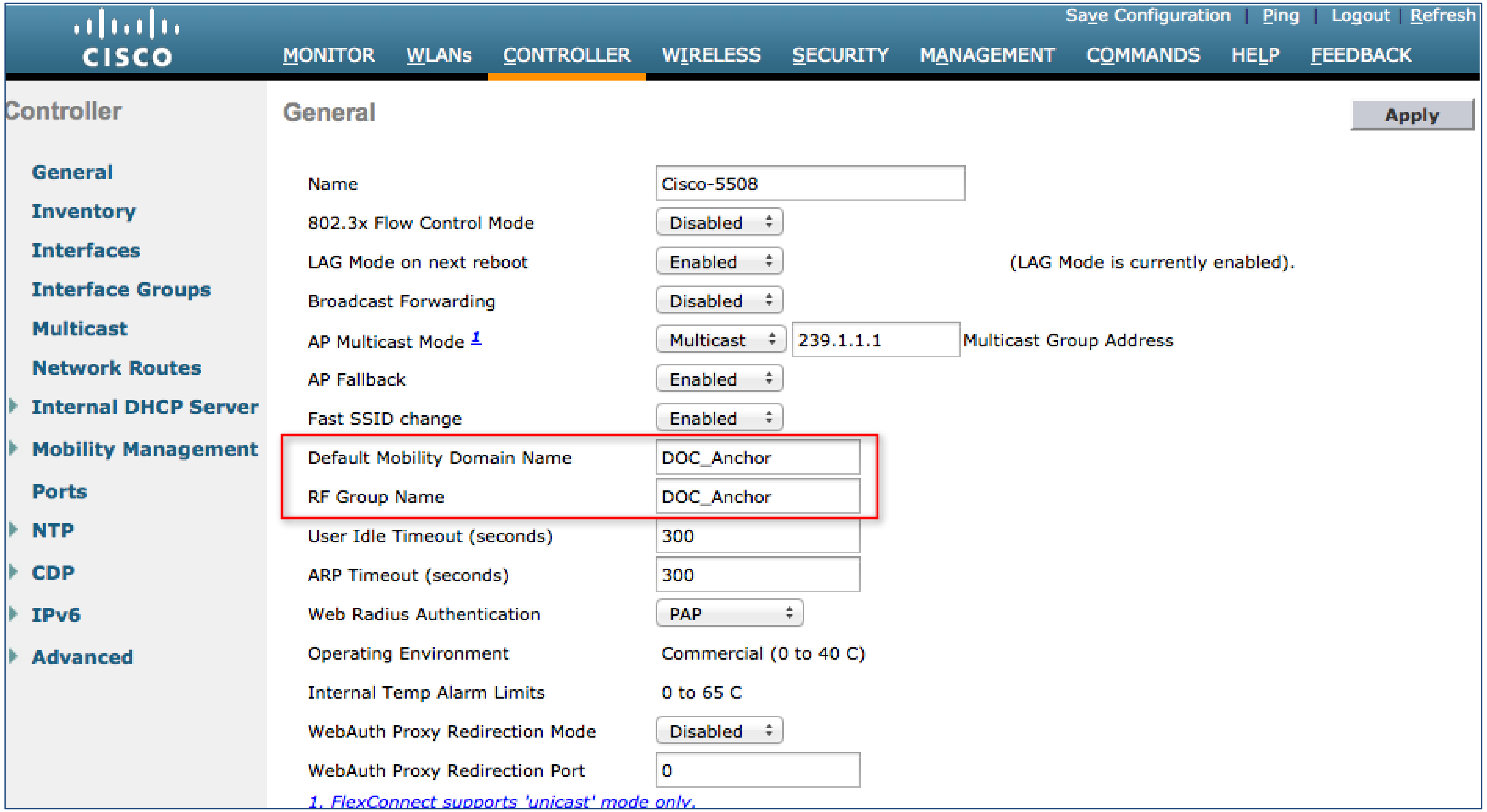
Building the EoIP Tunnel

1. Specify a mobility group for each WLC
2. Open ports for:
   - Inter-Controller Tunneled Client Data
   - Inter-Controller Control Traffic
   - EoIP tunnel protocol
   - Other ports as required
3. Create Guest VLAN on Anchor controller(s)
4. Create identical WLANs on the Remote and Anchor controllers
5. Configure the mobility groups and add the MAC-address and IP address of the remote WLC
6. Create the Mobility Anchor for the Guest WLAN
7. Modify the timers in the WLCs
8. Check the status of the Mobility Anchors for the WLAN

Guest Path Isolation

WLAN Controller Deployments with EoIP Tunnel
Remote Controller Configuration

- Anchor and Remote WLCs are configured in different Mobility Groups



General

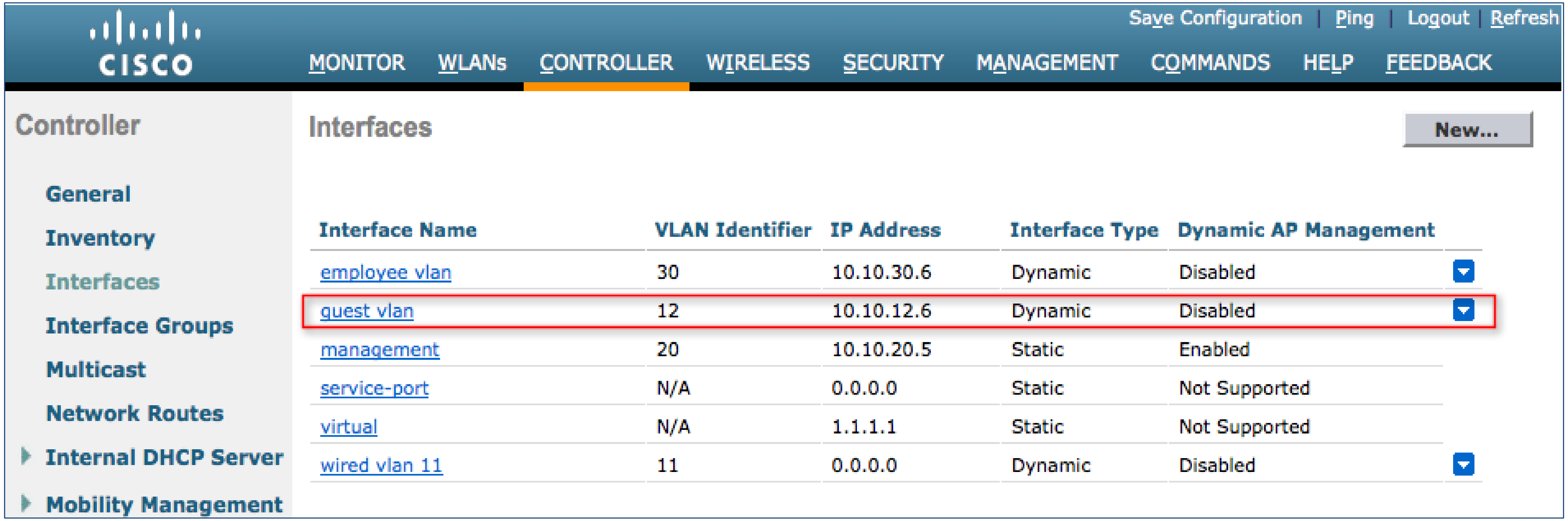
Name	Cisco-5508	
802.3x Flow Control Mode	Disabled	
LAG Mode on next reboot	Enabled	(LAG Mode is currently enabled).
Broadcast Forwarding	Disabled	
AP Multicast Mode [1]	Multicast 239.1.1.1	Multicast Group Address
AP Fallback	Enabled	
Fast SSID change	Enabled	
Default Mobility Domain Name	DOC_Anchor	
RF Group Name	DOC_Anchor	
User Idle Timeout (seconds)	300	
ARP Timeout (seconds)	300	
Web Radius Authentication	PAP	
Operating Environment	Commercial (0 to 40 C)	
Internal Temp Alarm Limits	0 to 65 C	
WebAuth Proxy Redirection Mode	Disabled	
WebAuth Proxy Redirection Port	0	

[1] FlexConnect supports 'unicast' mode only.

Guest Path Isolation

WLAN Controller Deployments with EoIP Tunnel
Anchor and Remote Controller Configuration

- Configure Guest WLANs on the Remote and Anchor controllers
- Configure Guest VLAN on the Anchor WLC



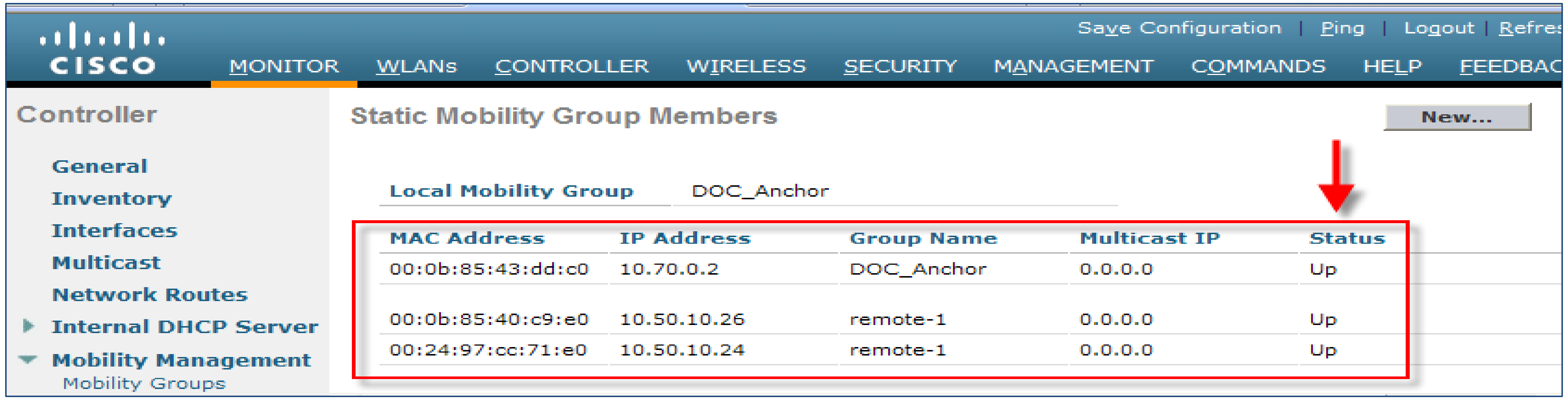
Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
employee vlan	30	10.10.30.6	Dynamic	Disabled
guest vlan	12	10.10.12.6	Dynamic	Disabled
management	20	10.10.20.5	Static	Enabled
service-port	N/A	0.0.0.0	Static	Not Supported
virtual	N/A	1.1.1.1	Static	Not Supported
wired vlan 11	11	0.0.0.0	Dynamic	Disabled

Guest Path Isolation

WLAN Controller Deployments with EoIP Tunnel
Anchor and Remote Controller Configuration

- Configure the mobility groups and add the MAC-address and IP address of the remote WLCs

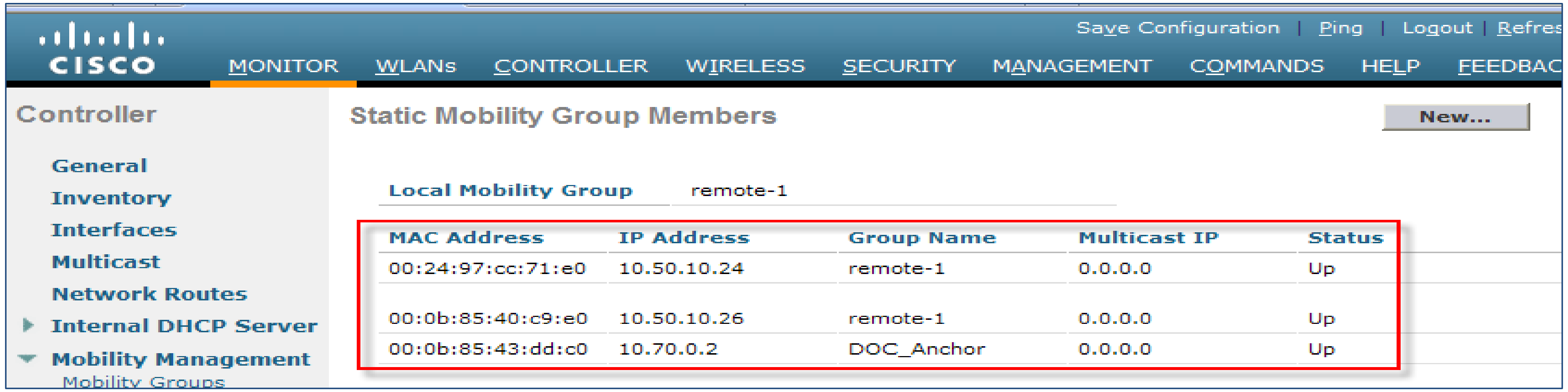


Static Mobility Group Members

Local Mobility Group DOC_Anchor

MAC Address	IP Address	Group Name	Multicast IP	Status
00:0b:85:43:dd:c0	10.70.0.2	DOC_Anchor	0.0.0.0	Up
00:0b:85:40:c9:e0	10.50.10.26	remote-1	0.0.0.0	Up
00:24:97:cc:71:e0	10.50.10.24	remote-1	0.0.0.0	Up

Anchor



Static Mobility Group Members

Local Mobility Group remote-1

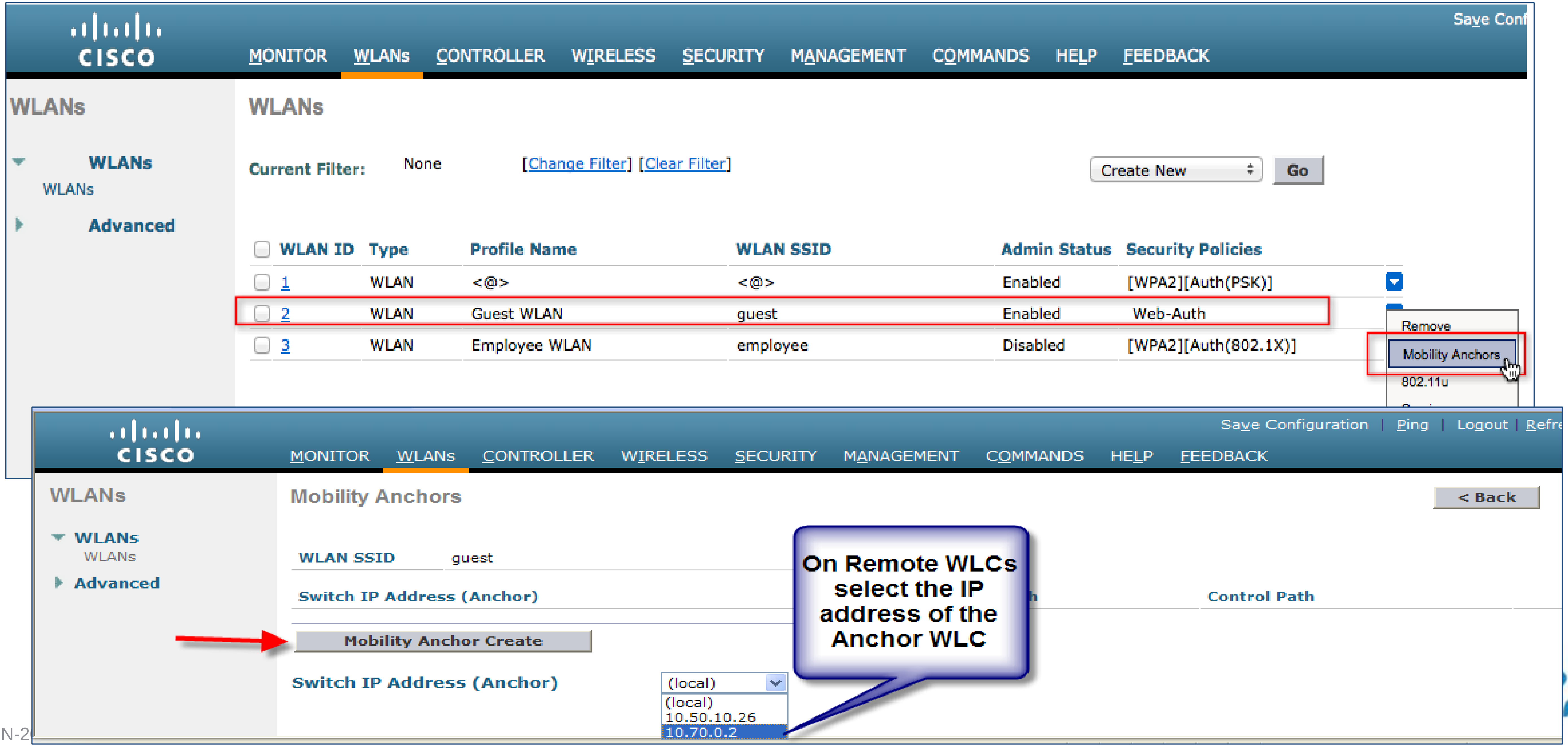
MAC Address	IP Address	Group Name	Multicast IP	Status
00:24:97:cc:71:e0	10.50.10.24	remote-1	0.0.0.0	Up
00:0b:85:40:c9:e0	10.50.10.26	remote-1	0.0.0.0	Up
00:0b:85:43:dd:c0	10.70.0.2	DOC_Anchor	0.0.0.0	Up

Remote

Guest Path Isolation

WLAN Controller Deployments with EoIP Tunnel
Remote Controller Configuration

- Create the mobility anchor for the guest WLAN on Remote WLCs



Current Filter: None [Change Filter] [Clear Filter]

Create New | Go

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	<@>	<@>	Enabled	[WPA2][Auth(PSK)]
2	WLAN	Guest WLAN	guest	Enabled	Web-Auth
3	WLAN	Employee WLAN	employee	Disabled	[WPA2][Auth(802.1X)]

Mobility Anchors

WLAN SSID guest

Switch IP Address (Anchor) | Control Path

Mobility Anchor Create

Switch IP Address (Anchor) (local)

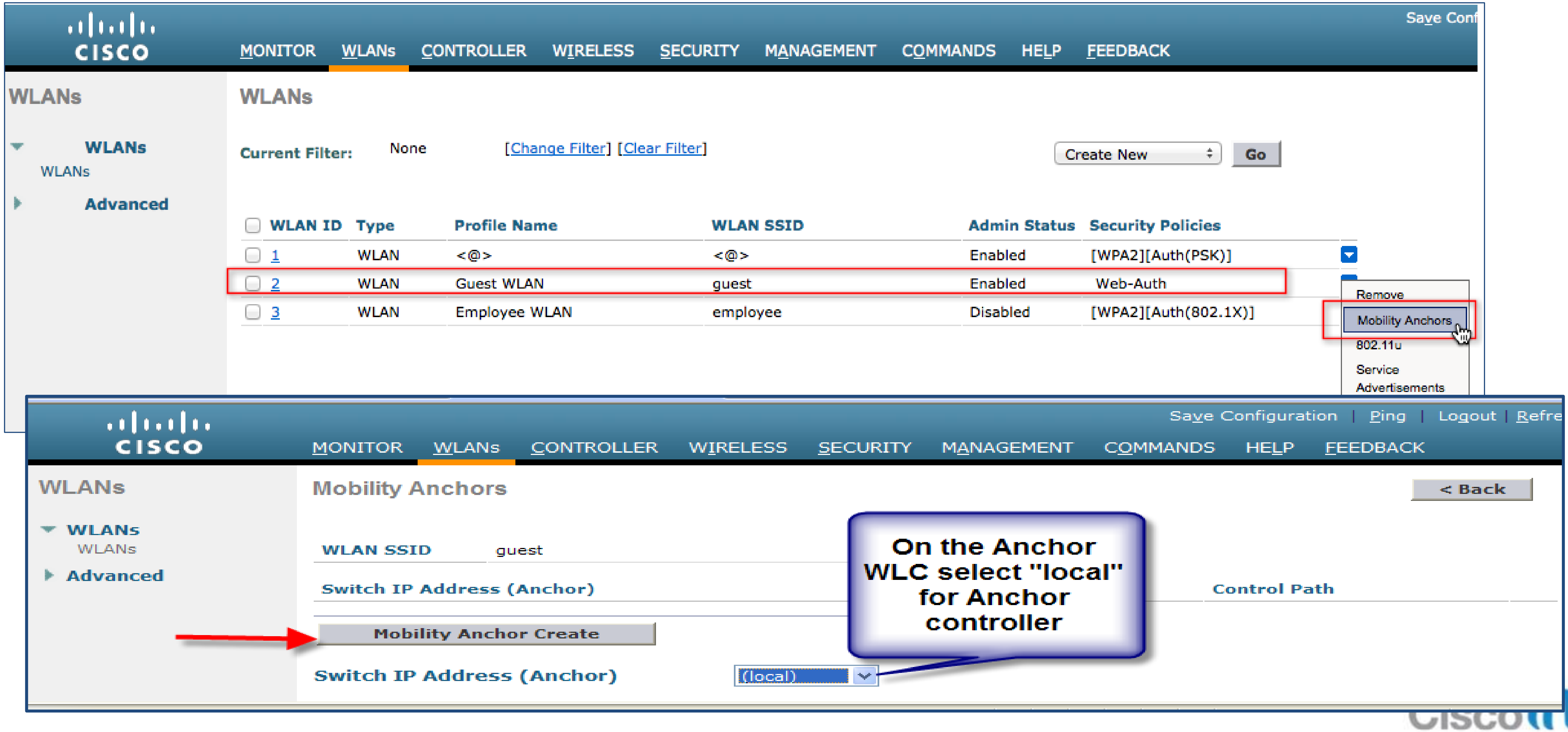
(local)
10.50.10.26
10.70.0.2

On Remote WLCs select the IP address of the Anchor WLC

Guest Path Isolation

WLAN Controller Deployments with EoIP Tunnel
Anchor Controller Configuration

- Create the Mobility Anchor for the guest WLAN on Anchor WLC



WLANs

Current Filter: None [Change Filter] [Clear Filter]

☐ WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
☐ 1	WLAN	<@>	<@>	Enabled	[WPA2][Auth(PSK)]
☐ 2	WLAN	Guest WLAN	guest	Enabled	Web-Auth
☐ 3	WLAN	Employee WLAN	employee	Disabled	[WPA2][Auth(802.1X)]

Mobility Anchors

WLAN SSID guest

Switch IP Address (Anchor) Control Path

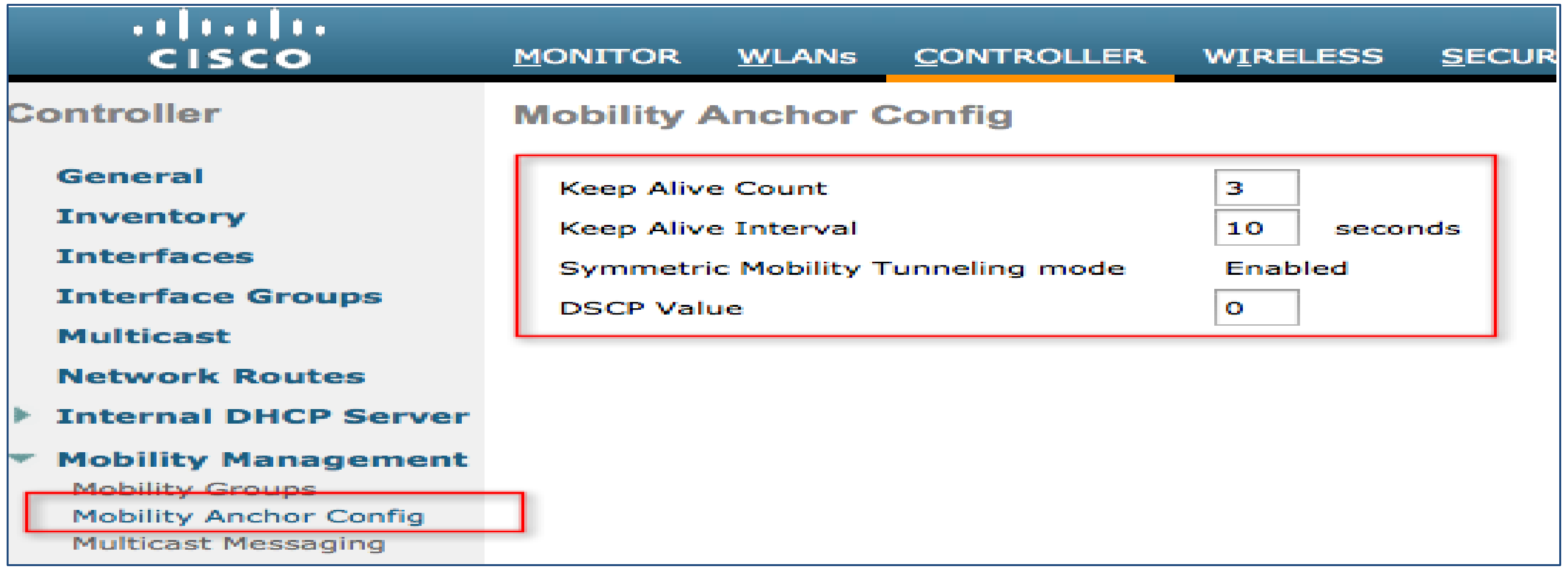
Switch IP Address (Anchor) (local)

On the Anchor WLC select "local" for Anchor controller

Path Isolation

WLAN Controller Deployments with EoIP Tunnel Anchor Controller

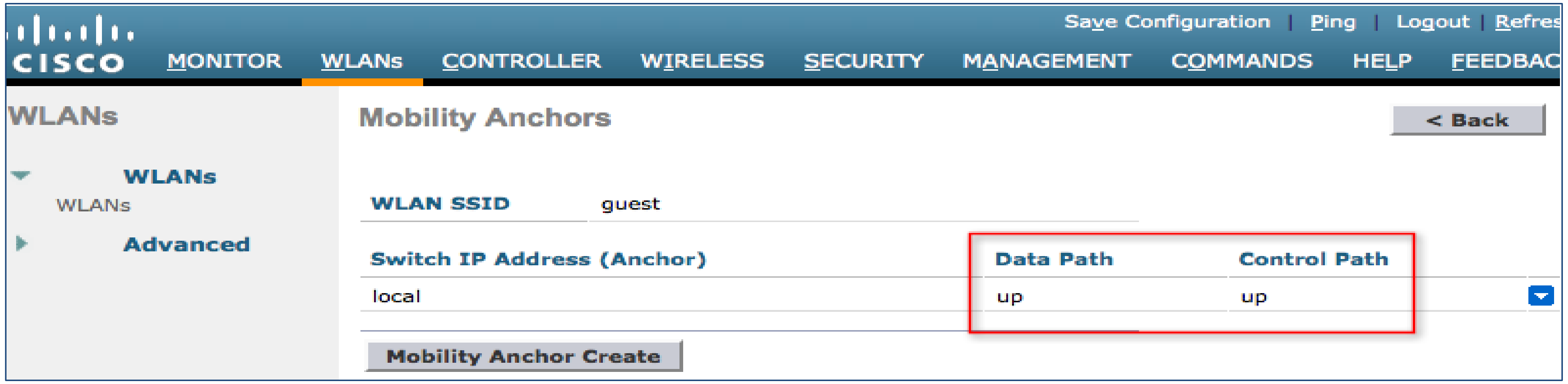
- Modify the timers and DSCP on the Anchor WLCs



Mobility Anchor Config

Keep Alive Count	3	
Keep Alive Interval	10	seconds
Symmetric Mobility Tunneling mode	Enabled	
DSCP Value	0	

- Check the status of the mobility anchors for the WLAN



Mobility Anchors

WLAN SSID guest

Switch IP Address (Anchor)	Data Path	Control Path
local	up	up

Guest Path Isolation

Firewall Ports and Protocols

- Open ports in both directions for:

EoIP packets	IP protocol 97		Must be Open!
Mobility	UDP Port 16666		
Inter-Controller CAPWAP (rel 5.0, 6.0, 7.0+)	Data/Control Traffic	UDP 5247/5246	Do NOT Open!
Inter-Controller LWAPP (before rel 5.0)	Data/Control Traffic	UDP 12222/12223	

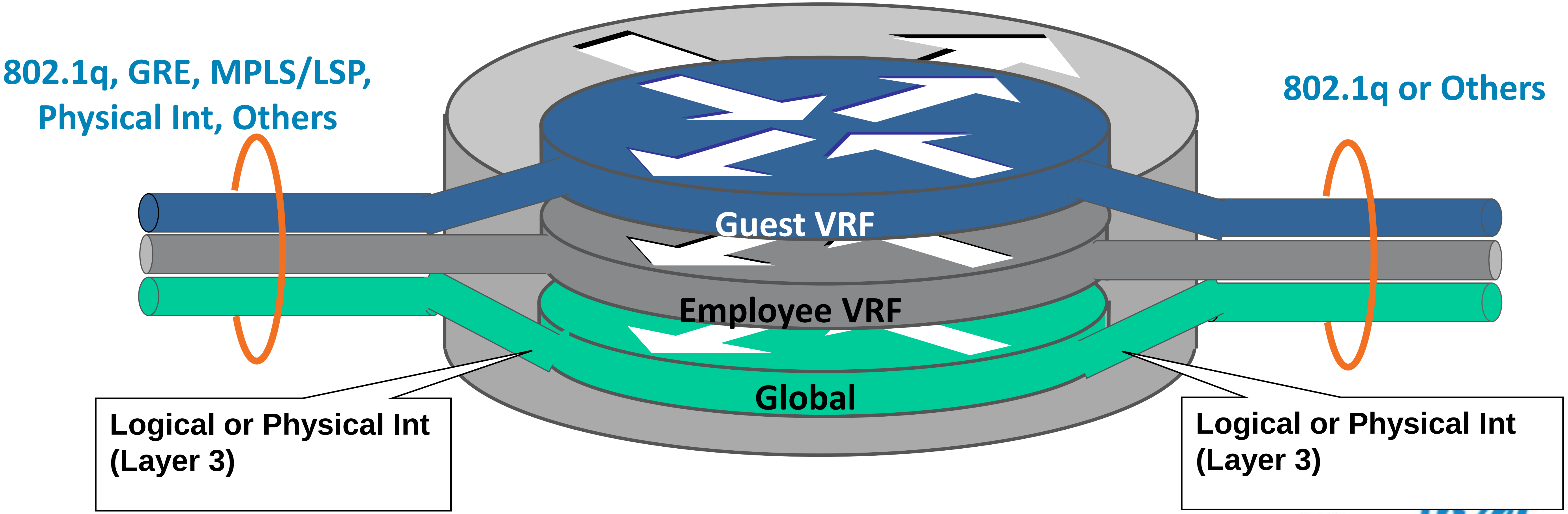
- Optional management/operational protocols:

– SSH/Telnet	TCP Port 22/23
– TFTP	UDP Port 69
– NTP	UDP Port 123
– SNMP	UDP Ports 161 (gets and sets) and 162 (traps)
– HTTPS/HTTP	TCP Port 443/80
– Syslog	TCP Port 514
– RADIUS Auth/Account	UDP Port 1812 and 1813

Solution #2: Guest Path Isolation using VRF

Campus Virtualisation

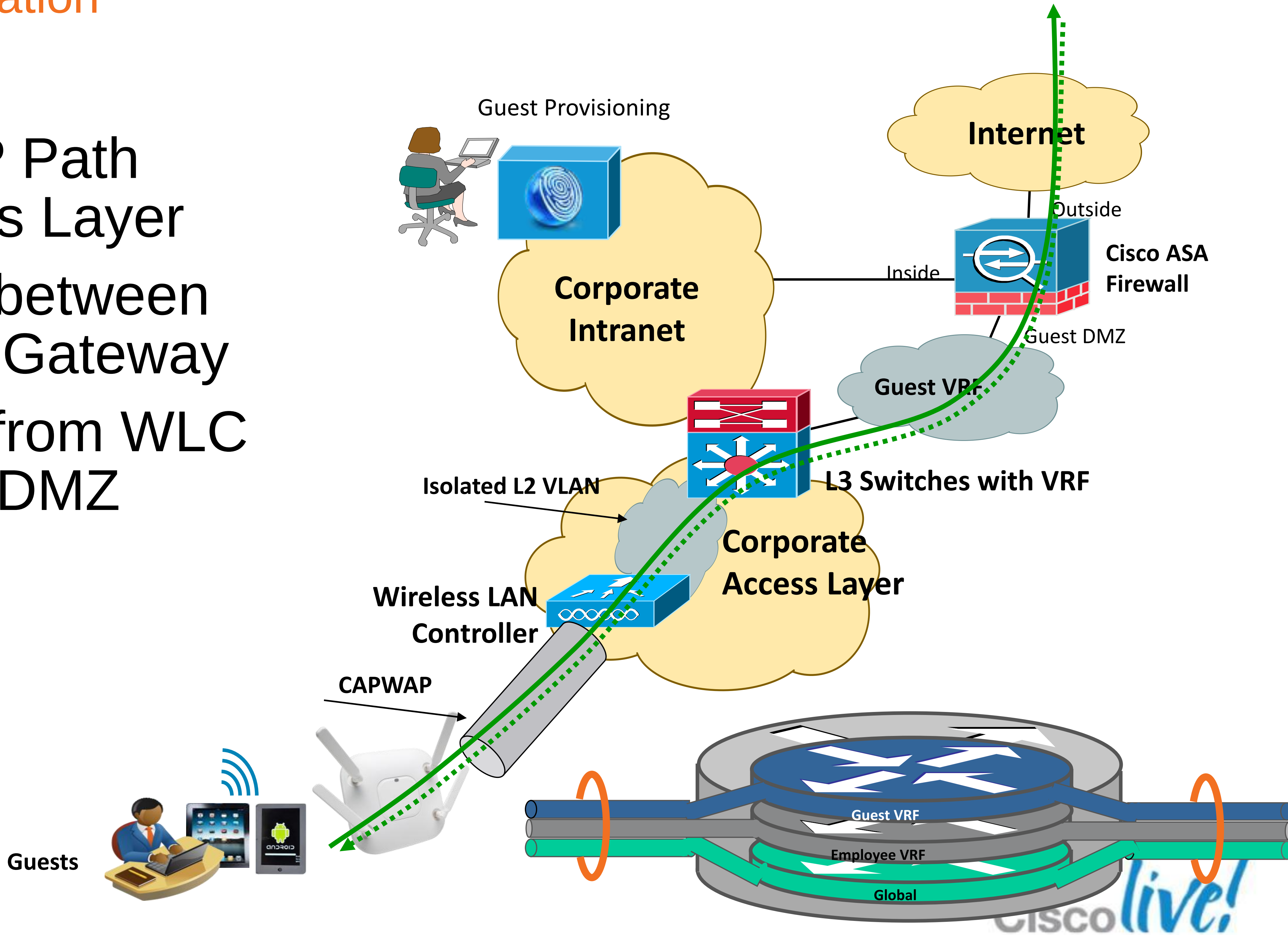
- Virtual Routing / Forwarding (VRF) or VRF- lite is the L3 virtualisation used in Enterprise Campus networks
- Guest isolation is done by dedicated VRF instances


802.1q, GRE, MPLS/LSP, Physical Int, Others
802.1q or Others
Guest VRF
Employee VRF
Global
Logical or Physical Int (Layer 3)
Logical or Physical Int (Layer 3)

Guest Path Isolation using VRF

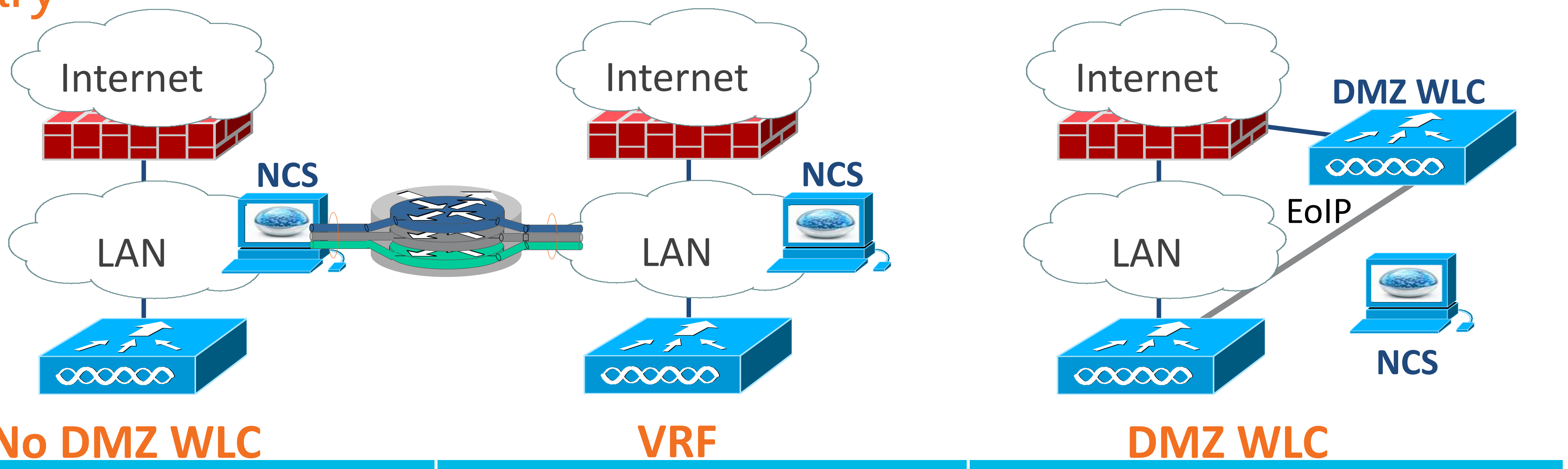
WLC and VRF Virtualisation

- LWAPP/CAPWAP Path Isolation at Access Layer
- L2 Path Isolation between WLC and Default Gateway
- L3 VRF Isolation from WLC to Firewall Guest DMZ interface



Wireless Guest Access

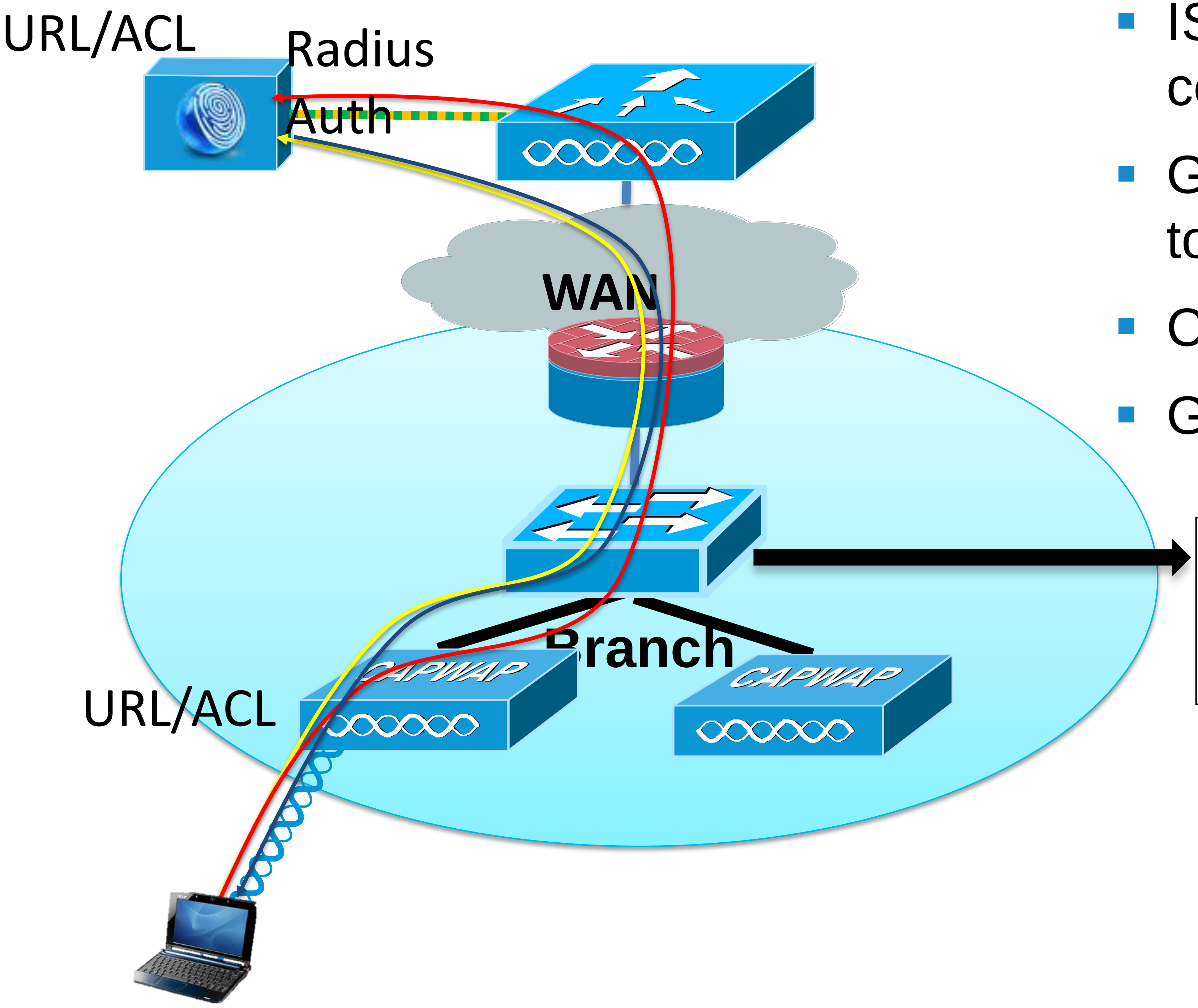
Deployment Options Summary



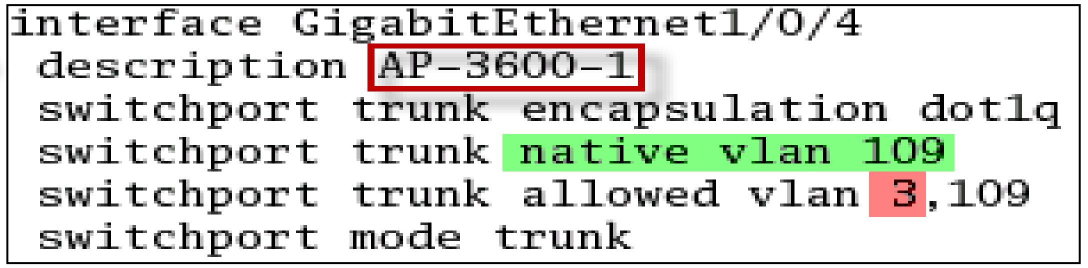
	Cisco Unified Wireless No DMZ Controller	Cisco Unified Wireless VRF	Cisco Unified Wireless DMZ Controller
Provisioning Portal	Yes	Yes	Yes
User Login Portal	Yes	Yes	Yes
Traffic Segmentation	VLANs thru Network	VRF thru Network	Yes—Tunnels or VLANs
User Policy Management	Yes	Yes	Yes
Reporting	Yes	Yes	Yes
Overall Functionality	Medium	High	High
Overall Design Complexity	Medium	High	Low

Securing Access with FlexConnect

FlexConnect and External WebAuth



- ISE for external webauth with FlexConnect central authentication with local switching.
- Guest client is provided with URL/ACL permit to ISE
- Clients does webauth with ISE
- Guest moves to local switching



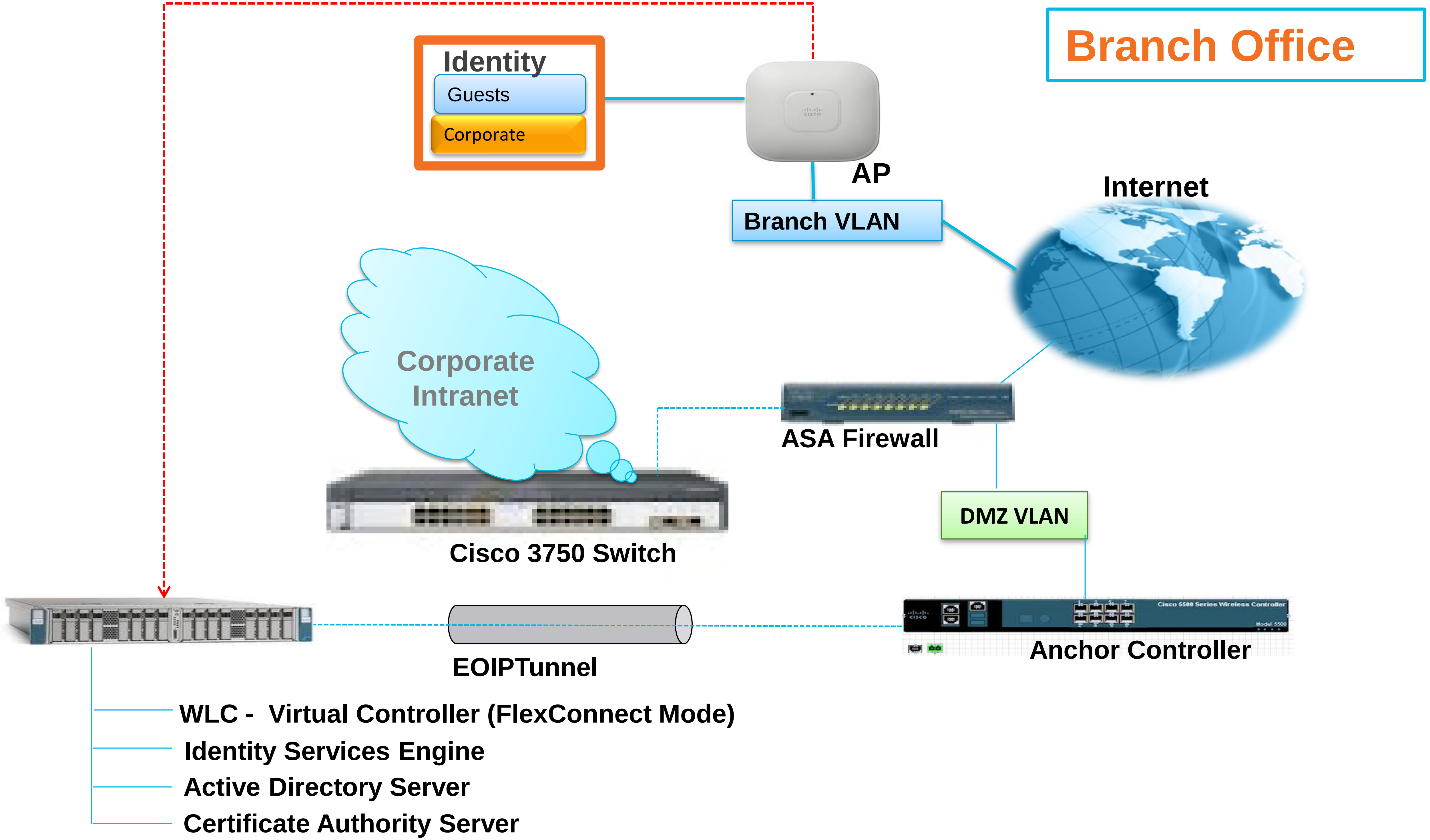
```
interface GigabitEthernet1/0/4
 description AP-3600-1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 109
 switchport trunk allowed vlan 3,109
 switchport mode trunk
```

→ Radius Auth

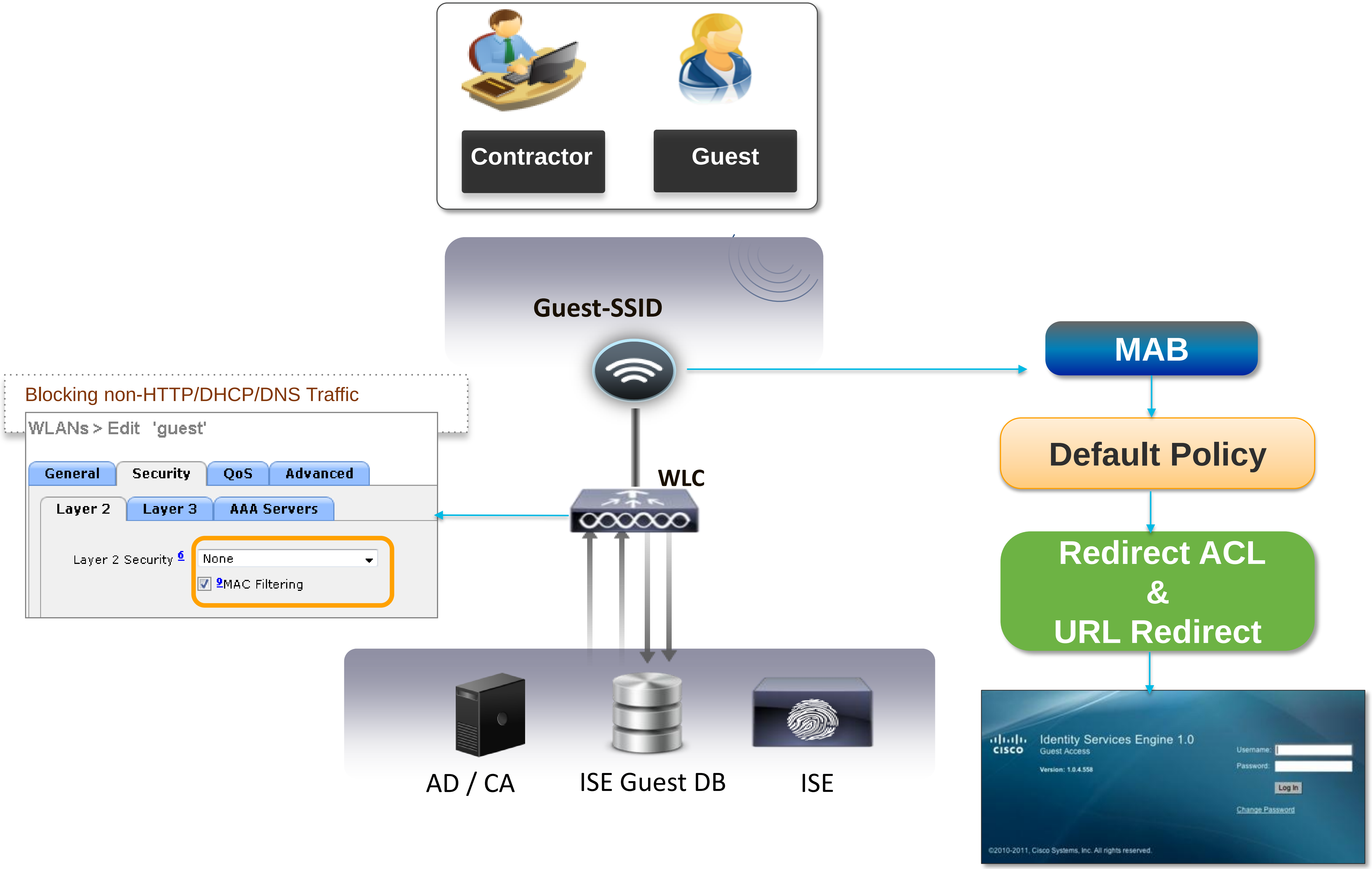
→ Webauth

→ VLAN Assignment

Guest with FlexConnect



CWA on Wireless Controllers



Blocking non-HTTP/DHCP/DNS Traffic

WLANs > Edit 'guest'

Layer 2 Security [6] None

☑ [9]MAC Filtering

Identity Services Engine 1.0

Guest Access

Version: 1.0.4.558

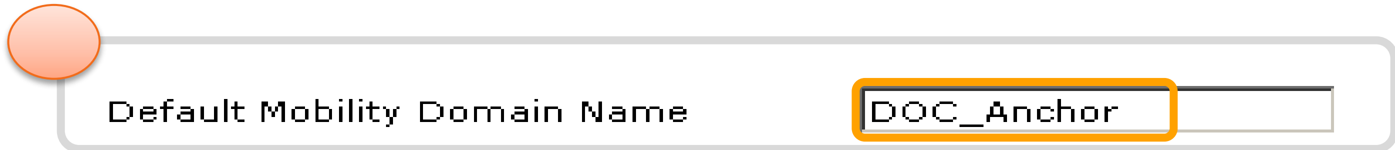
Username:

Password:

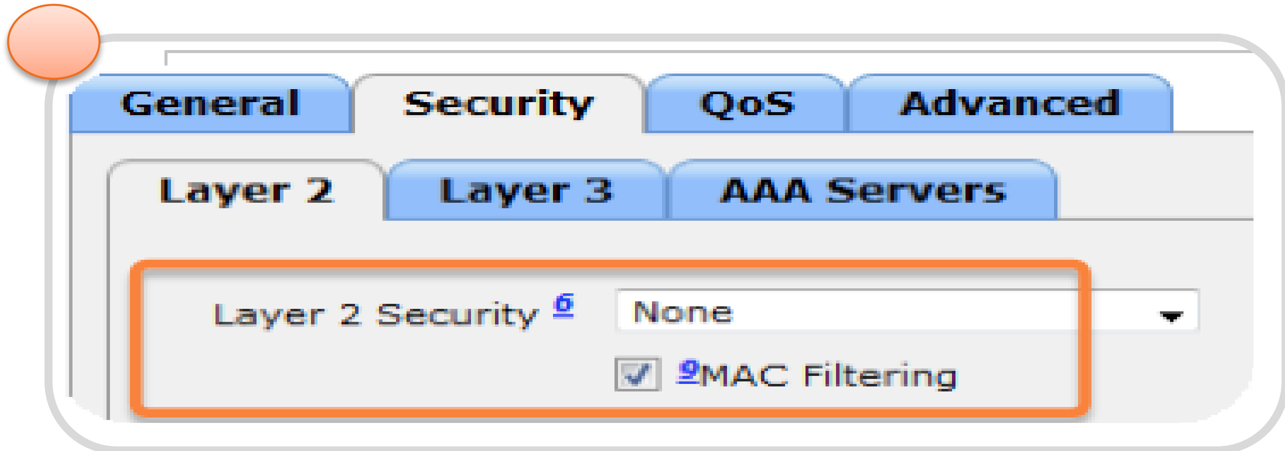
©2010-2011, Cisco Systems, Inc. All rights reserved.

Foreign Controller – Step-by-Step

Pre-Requisites

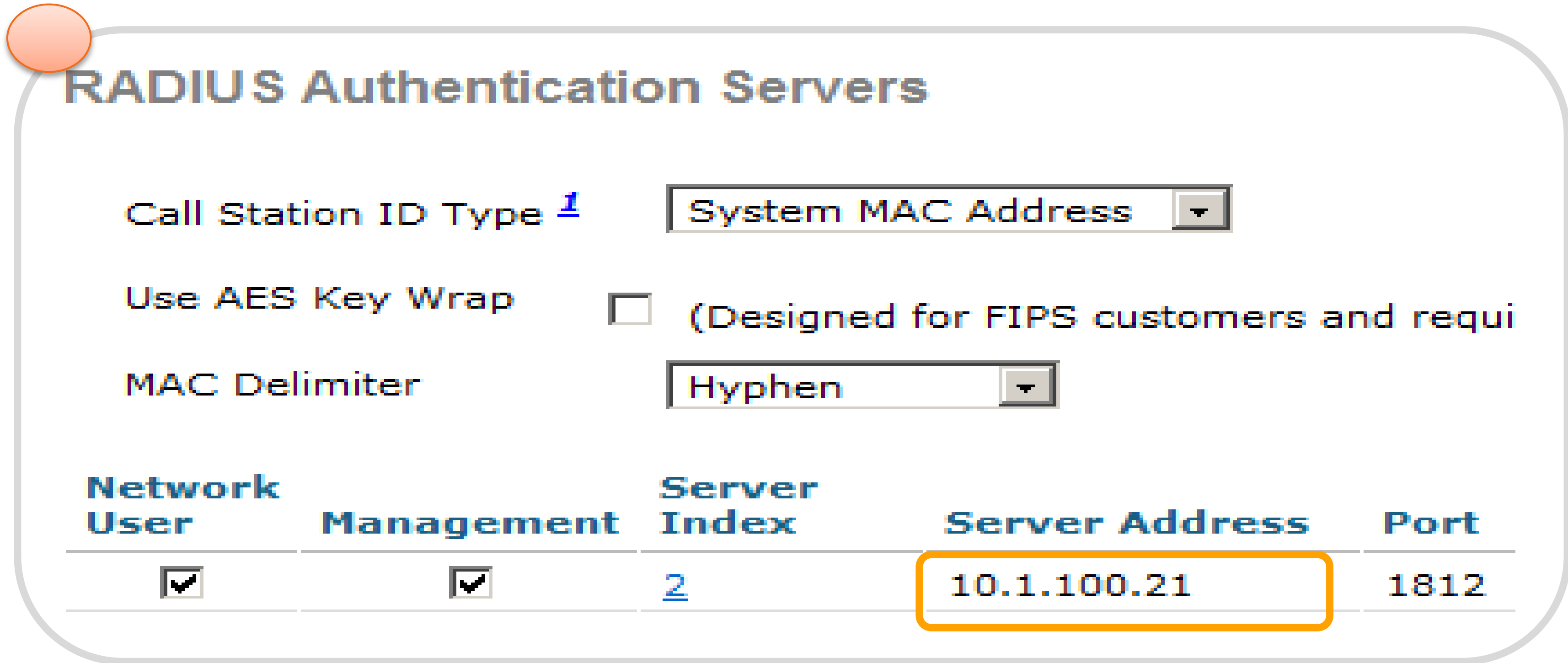


Default Mobility Domain Name: DOC_Anchor



Layer 2 Security [6]: None

☑ [9]MAC Filtering



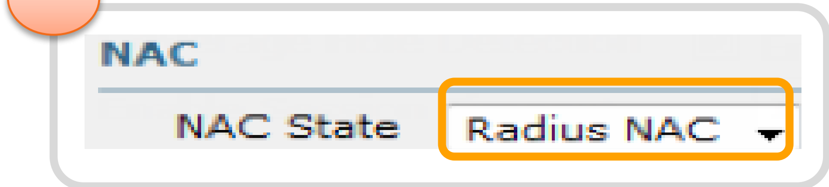
RADIUS Authentication Servers

Call Station ID Type [1]: System MAC Address

Use AES Key Wrap □ (Designed for FIPS customers and requi

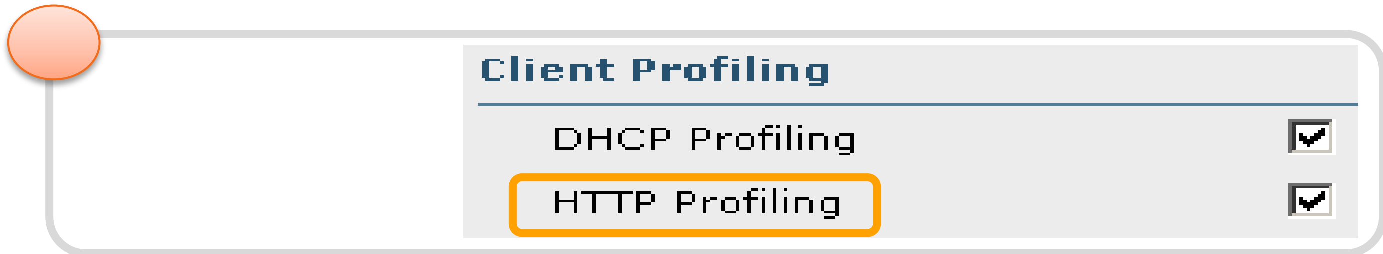
MAC Delimiter: Hyphen

Network User	Management	Server Index	Server Address	Port
☑	☑	2	10.1.100.21	1812



NAC

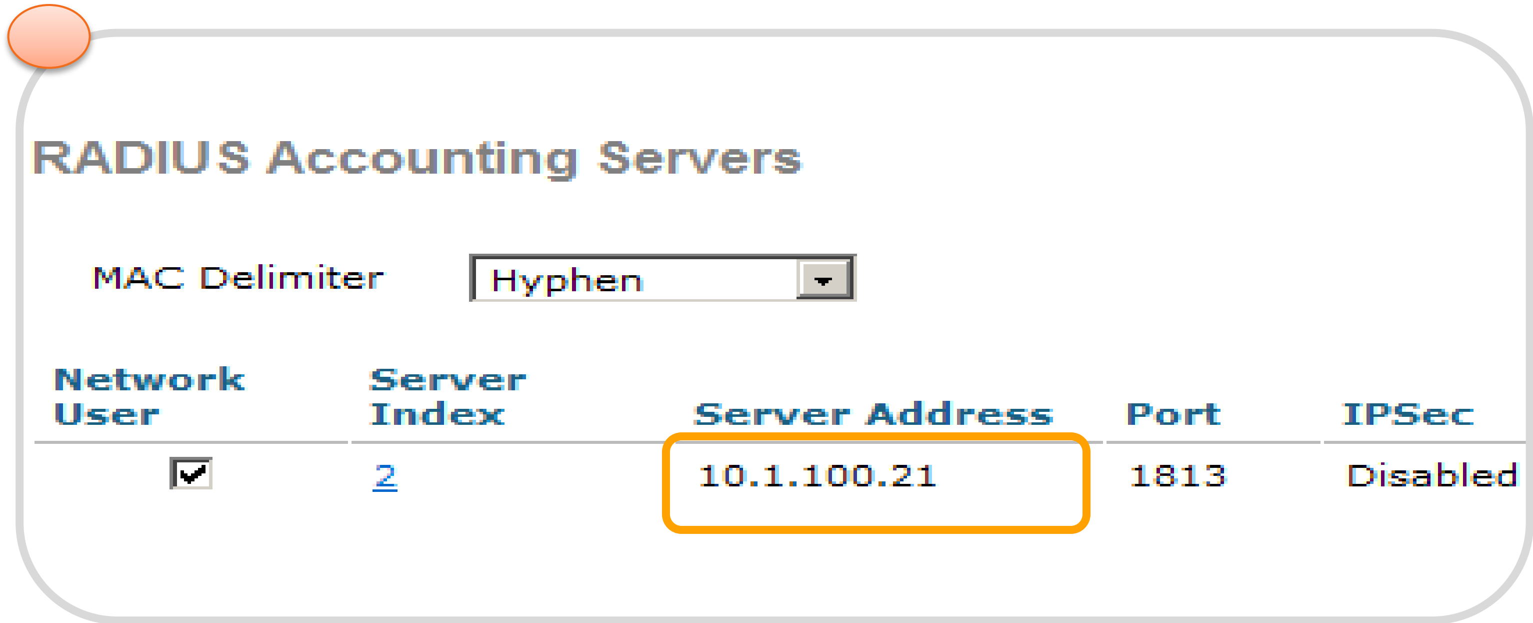
NAC State: Radius NAC



Client Profiling

DHCP Profiling ☑

HTTP Profiling ☑



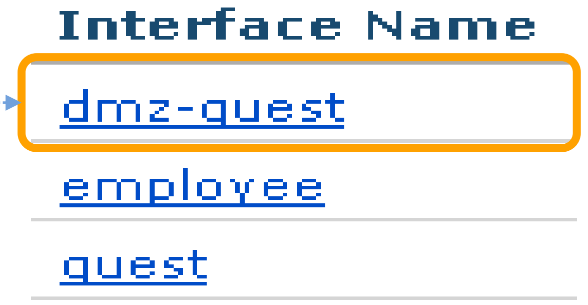
RADIUS Accounting Servers

MAC Delimiter: Hyphen

Network User	Server Index	Server Address	Port	IPSec
☑	2	10.1.100.21	1813	Disabled

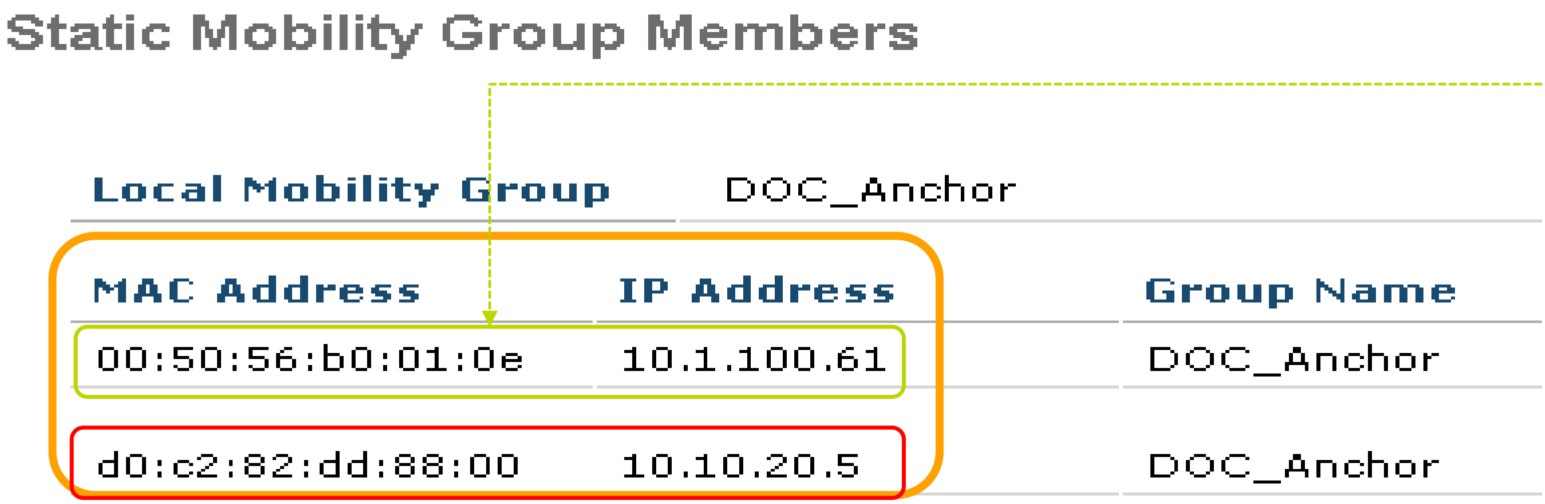
Foreign Controller – Step-by-Step

1 Configure Interfaces



Interface Name
dmz-guest
employee
guest

2 Configure Mobility Group Members



Static Mobility Group Members

Local Mobility Group DOC_Anchor

MAC Address	IP Address	Group Name
00:50:56:b0:01:0e	10.1.100.61	DOC_Anchor
d0:c2:82:dd:88:00	10.10.20.5	DOC_Anchor

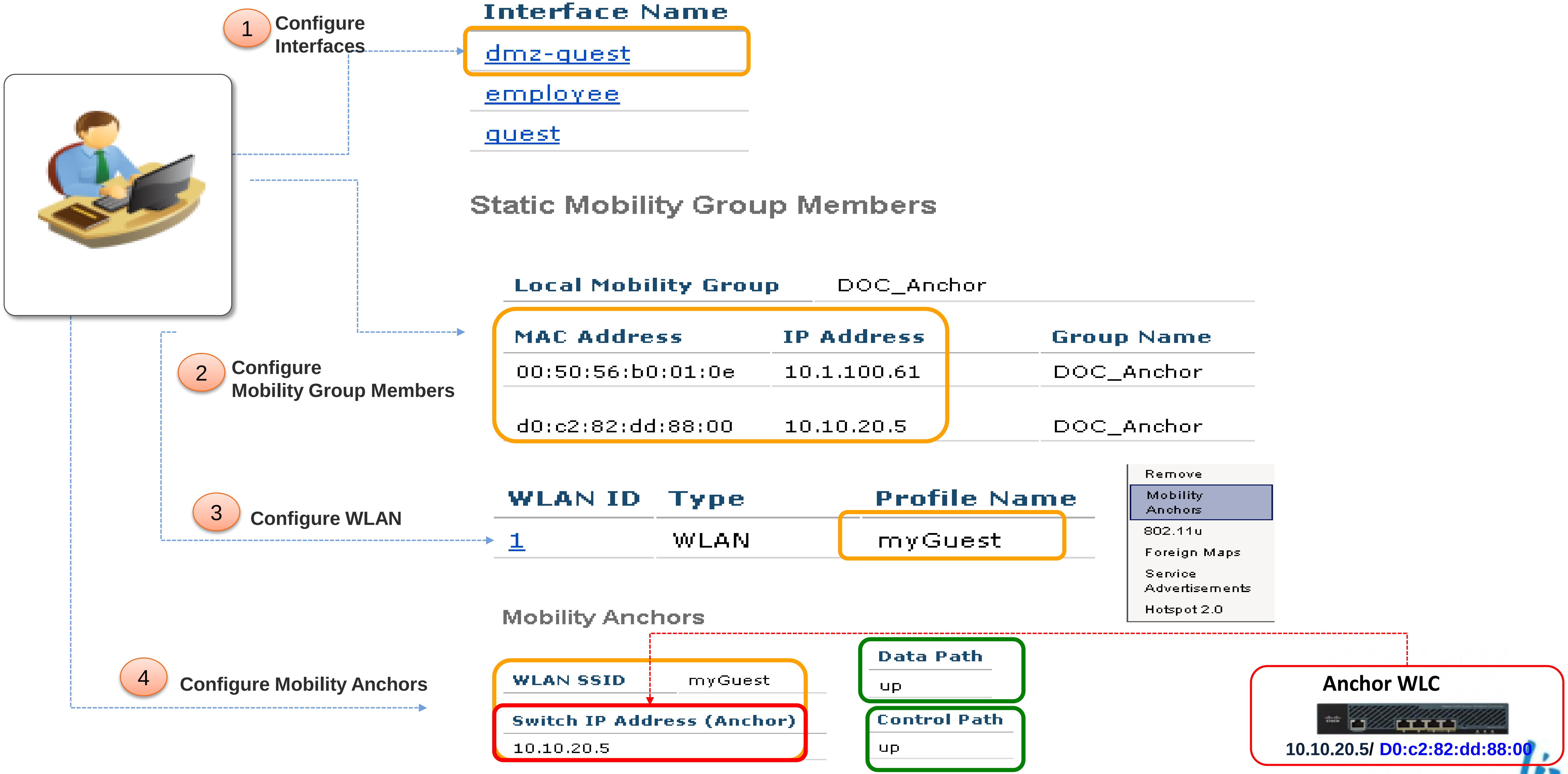
Foreign WLC

10.1.100.61/ 00:50:56:B0:01:0E

Anchor WLC

10.10.20.5/ D0:c2:82:dd:88:00

Foreign Controller – Step-by-Step



1 Configure Interfaces

Interface Name
dmz-guest
employee
guest

2 Configure Mobility Group Members

Static Mobility Group Members

Local Mobility Group DOC_Anchor

MAC Address	IP Address	Group Name
00:50:56:b0:01:0e	10.1.100.61	DOC_Anchor
d0:c2:82:dd:88:00	10.10.20.5	DOC_Anchor

3 Configure WLAN

WLAN ID	Type	Profile Name
1	WLAN	myGuest

4 Configure Mobility Anchors

Mobility Anchors

WLAN SSID	myGuest
Switch IP Address (Anchor)	
10.10.20.5	

Data Path
up

Control Path
up

Anchor WLC

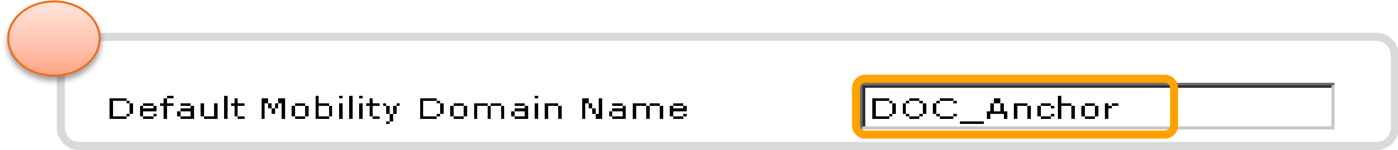
10.10.20.5/ D0:c2:82:dd:88:00

Pre-Requisites

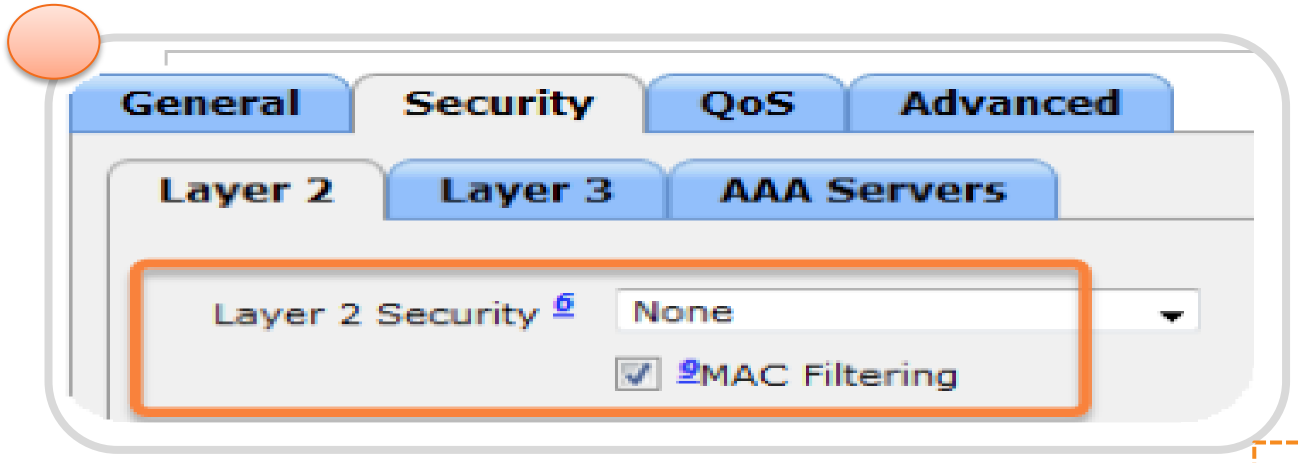
Anchor Controller

Step-by-Step

Allow Access to ISE for CWA (URL-Redirect)

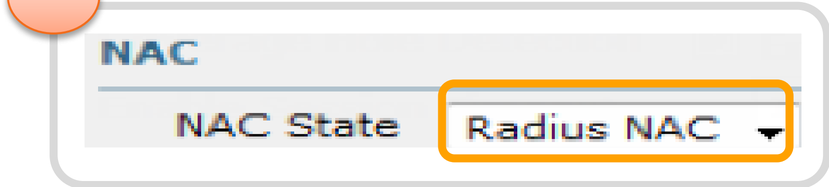


Default Mobility Domain Name: DOC_Anchor



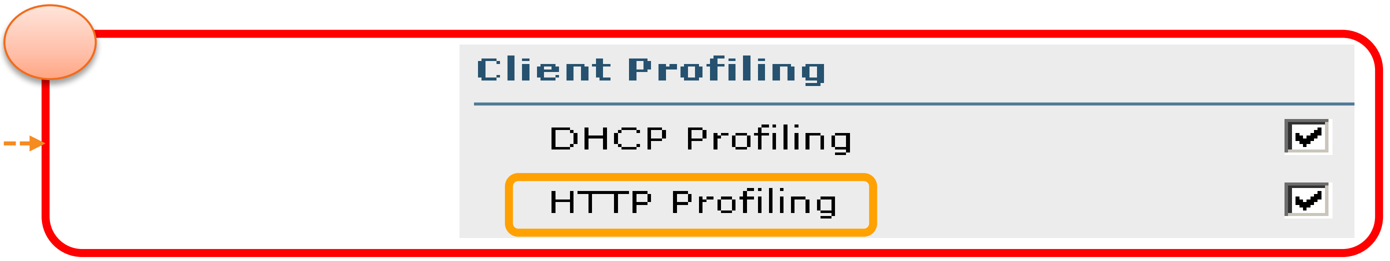
Layer 2 Security [6]: None

☑ [9]MAC Filtering



NAC

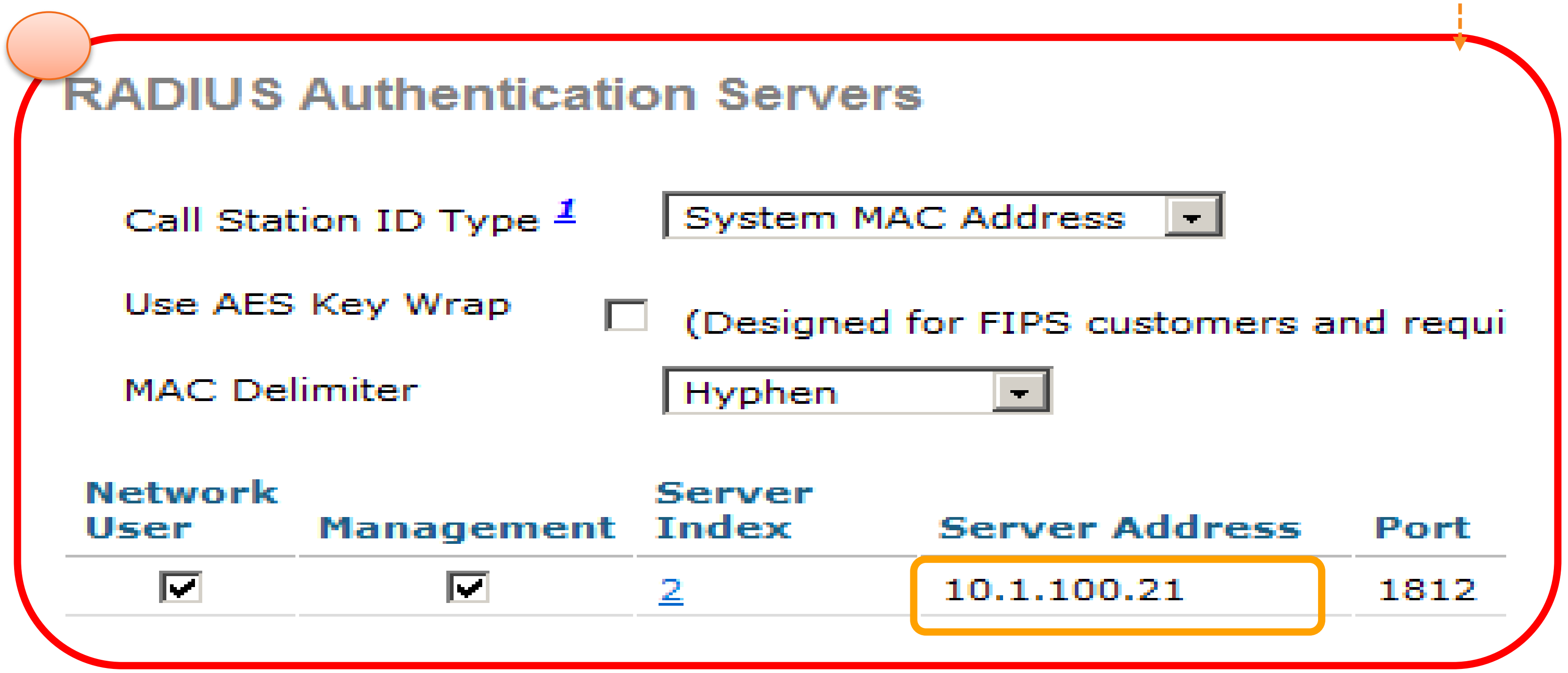
NAC State: Radius NAC



Client Profiling

DHCP Profiling	☑
HTTP Profiling	☑

NOT Required



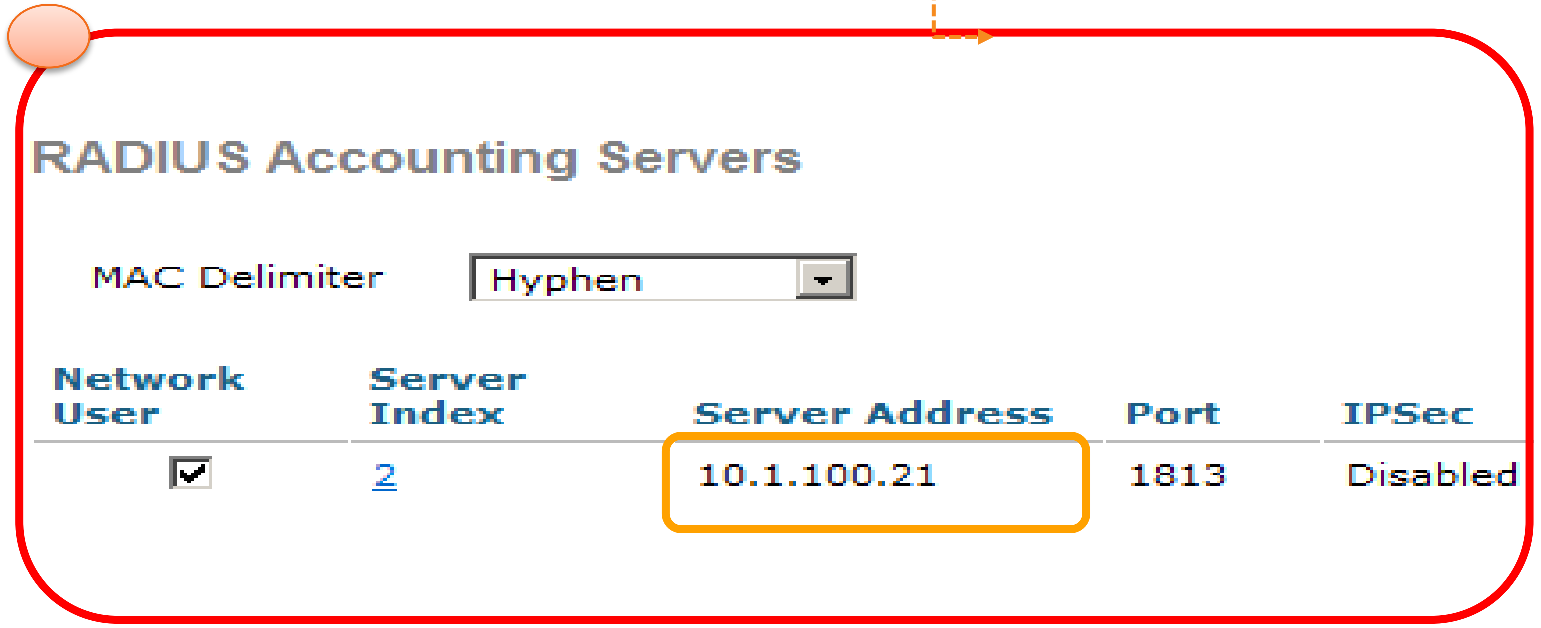
RADIUS Authentication Servers

Call Station ID Type [1]: System MAC Address

Use AES Key Wrap ☐ (Designed for FIPS customers and requi

MAC Delimiter: Hyphen

Network User	Management	Server Index	Server Address	Port
☑	☑	2	10.1.100.21	1812



RADIUS Accounting Servers

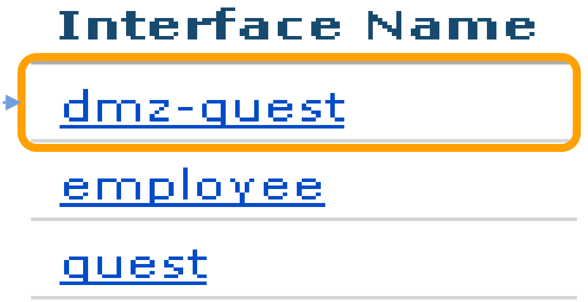
MAC Delimiter: Hyphen

Network User	Server Index	Server Address	Port	IPSec
☑	2	10.1.100.21	1813	Disabled

Anchor Controller

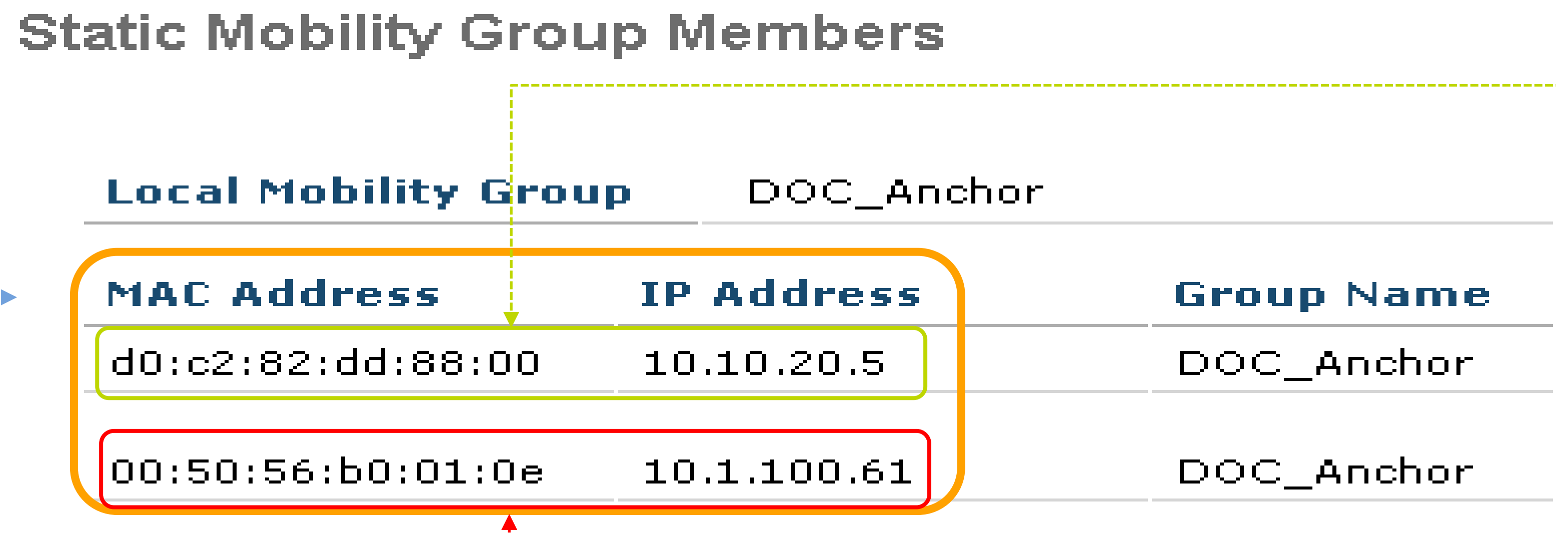
Step-by-Step

1 Configure Interfaces



Interface Name
dmz-guest
employee
guest

2 Configure Mobility Group Members



Static Mobility Group Members

Local Mobility Group DOC_Anchor

MAC Address	IP Address	Group Name
d0:c2:82:dd:88:00	10.10.20.5	DOC_Anchor
00:50:56:b0:01:0e	10.1.100.61	DOC_Anchor

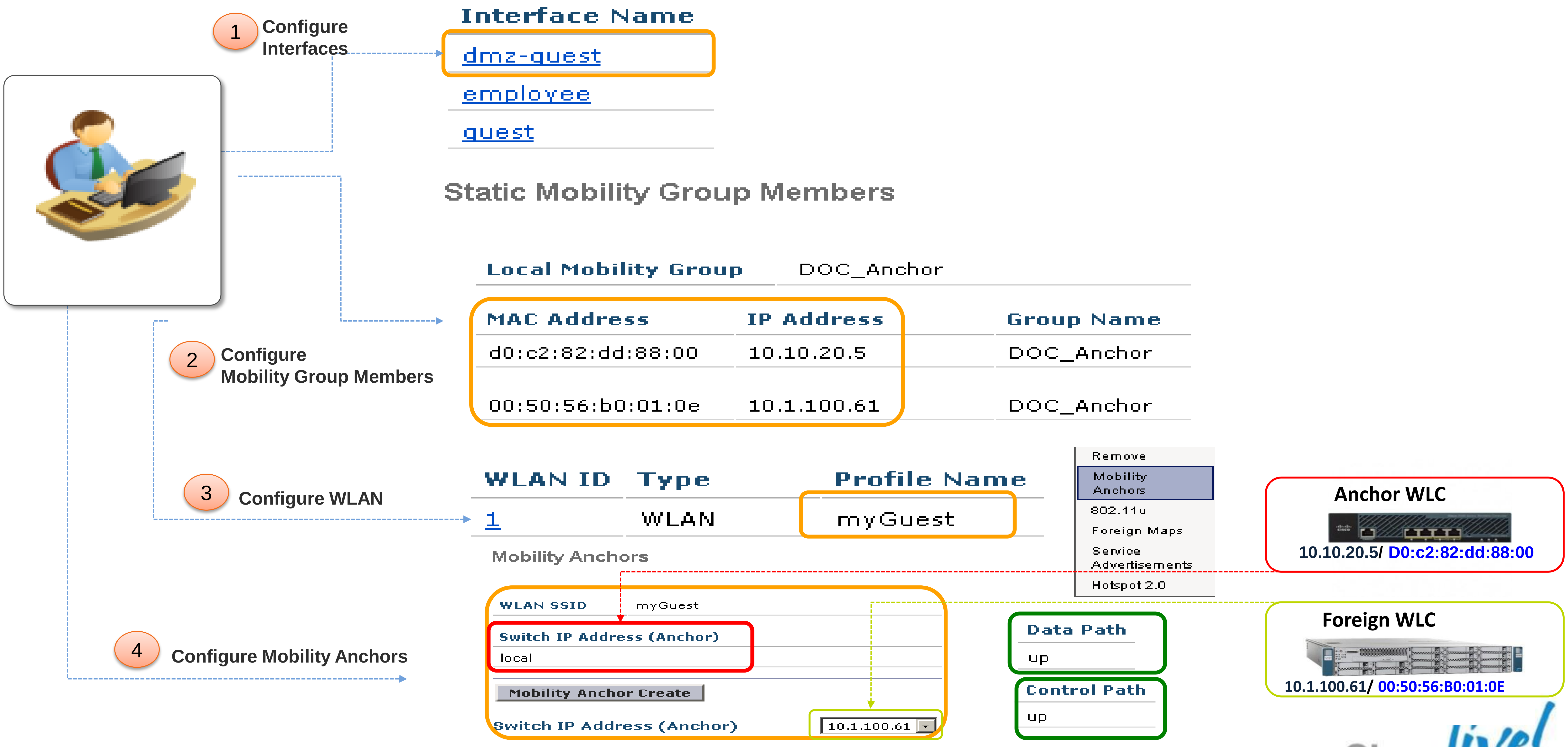
Foreign WLC

10.1.100.61/ 00:50:56:B0:01:0E

Anchor WLC

10.10.20.5/ D0:c2:82:dd:88:00

Anchor Controller - Step-by-Step



1 Configure Interfaces

Interface Name
dmz-guest
employee
guest

2 Configure Mobility Group Members

Static Mobility Group Members

Local Mobility Group DOC_Anchor

MAC Address	IP Address	Group Name
d0:c2:82:dd:88:00	10.10.20.5	DOC_Anchor
00:50:56:b0:01:0e	10.1.100.61	DOC_Anchor

3 Configure WLAN

WLAN ID	Type	Profile Name
1	WLAN	myGuest

4 Configure Mobility Anchors

Mobility Anchors

WLAN SSID myGuest

Switch IP Address (Anchor)	Data Path	Control Path
local	up	up

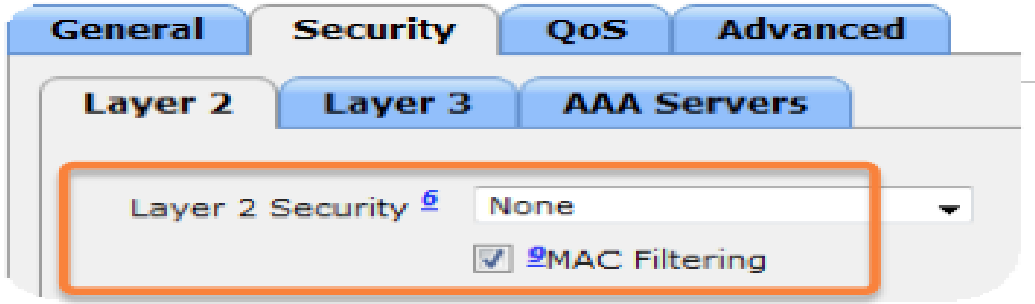
Mobility Anchor Create

Switch IP Address (Anchor) 10.1.100.61

Anchor WLC
10.10.20.5/ D0:c2:82:dd:88:00

Foreign WLC
10.1.100.61/ 00:50:56:B0:01:0E

Review Wireless CWA Config

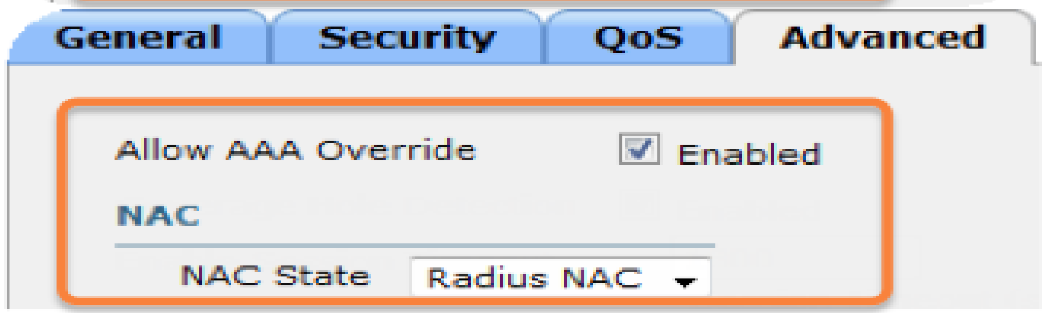


General | Security | QoS | Advanced

Layer 2 | Layer 3 | AAA Servers

Layer 2 Security [6] None

☑ [9]MAC Filtering

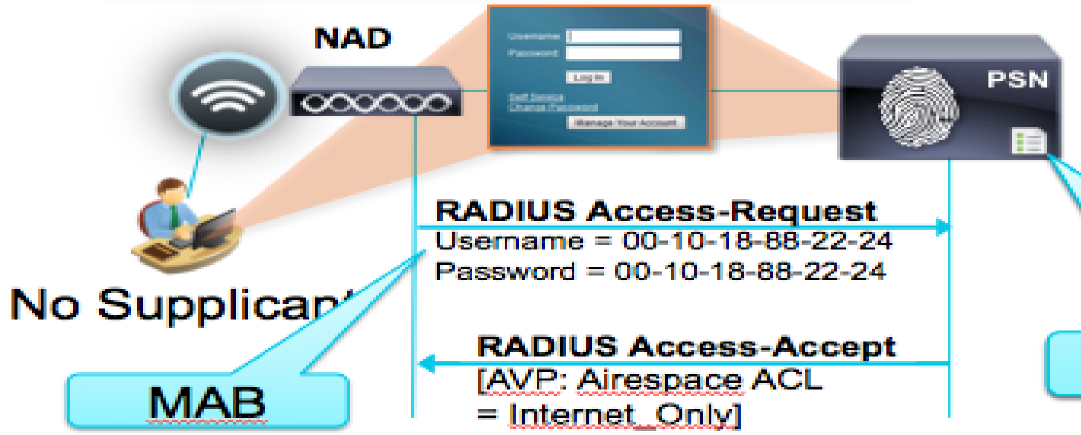


General | Security | QoS | Advanced

Allow AAA Override ☑ Enabled

NAC

NAC State Radius NAC



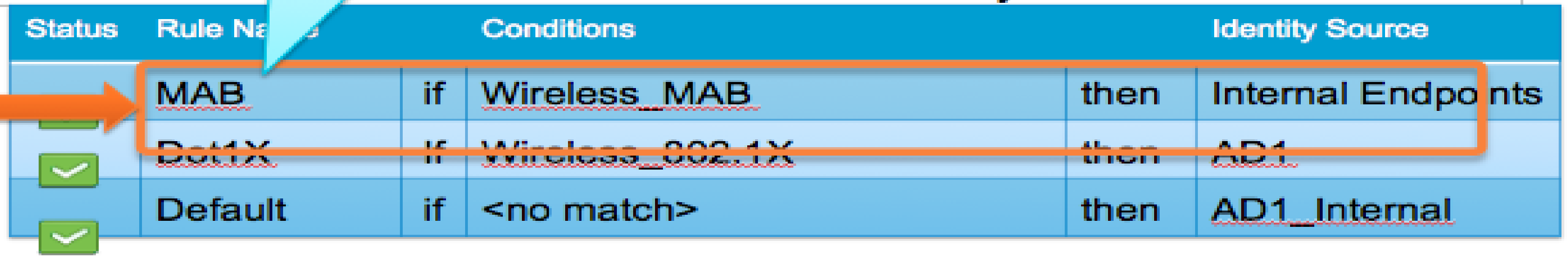
RADIUS Access-Request
Username = 00-10-18-88-22-24
Password = 00-10-18-88-22-24

RADIUS Access-Accept
[AVP: Airespace ACL
= Internet_Only]

MAB

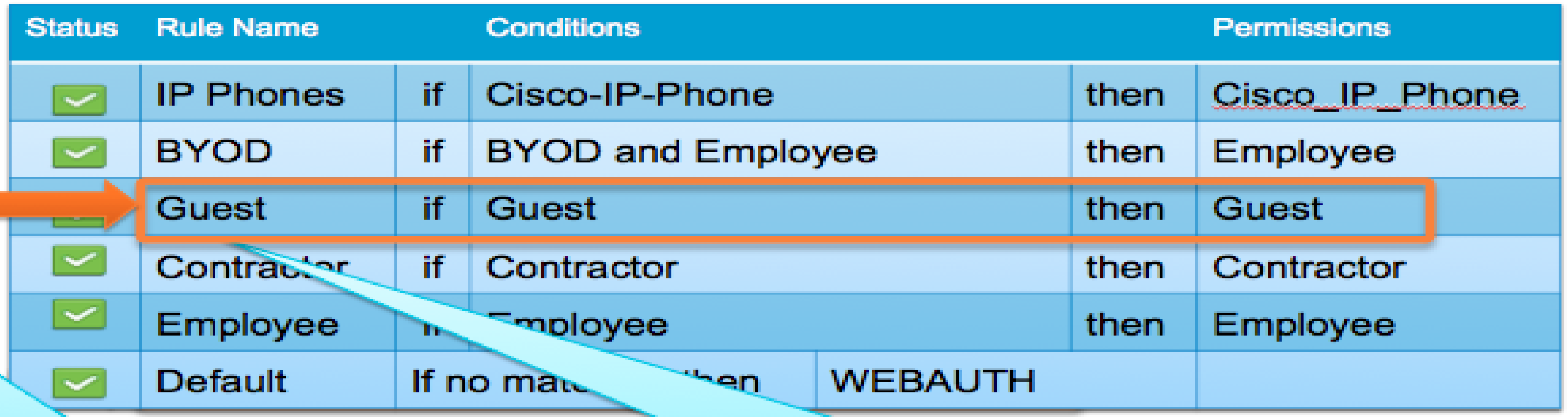
Matched AuthC Rule = MAB

Authentication Policy



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

Authorization Policy

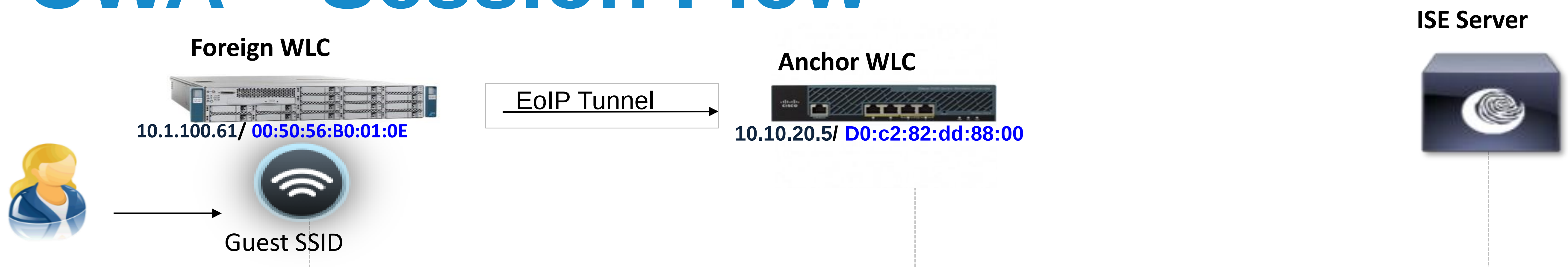


Status	Rule Name		Conditions		Permissions
✓	IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
✓	BYOD	if	BYOD and Employee	then	Employee
✓	Guest	if	Guest	then	Guest
✓	Contractor	if	Contractor	then	Contractor
✓	Employee	if	Employee	then	Employee
✓	Default	If no match then	WEBAUTH		

CWA username matches

Matched AuthZ Rule = Guest

CWA – Session Flow



Foreign WLC

10.1.100.61/ 00:50:56:B0:01:0E

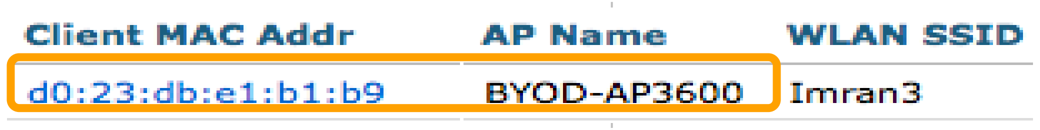
Guest SSID

EoIP Tunnel

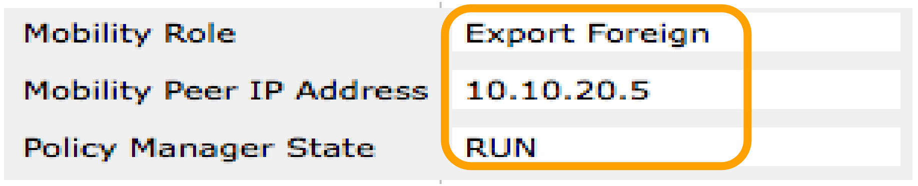
Anchor WLC

10.10.20.5/ D0:c2:82:dd:88:00

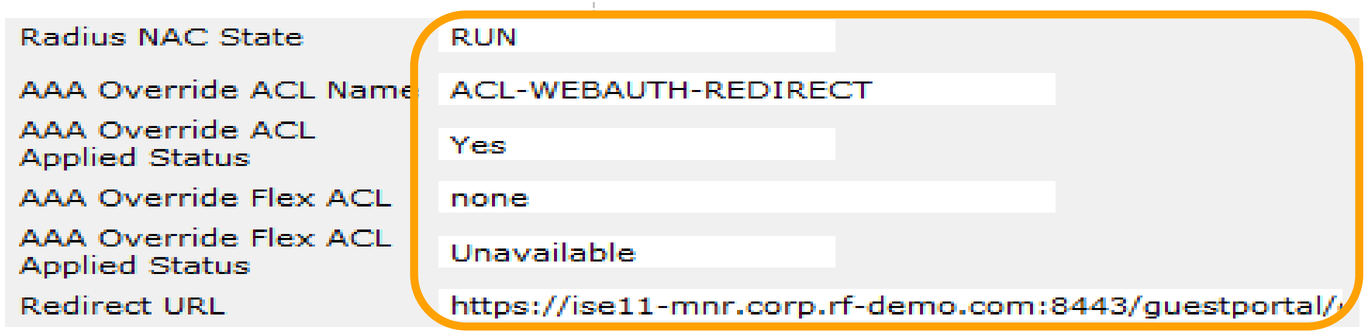
ISE Server



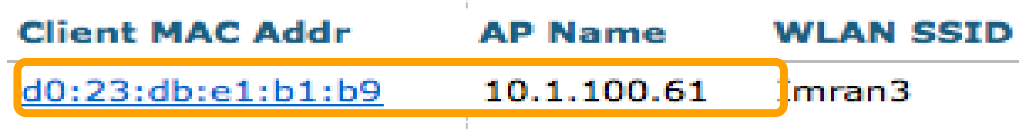
Client MAC Addr	AP Name	WLAN SSID
d0:23:db:e1:b1:b9	BYOD-AP3600	Imran3



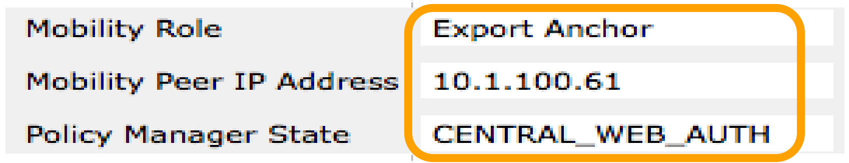
Mobility Role	Export Foreign
Mobility Peer IP Address	10.10.20.5
Policy Manager State	RUN



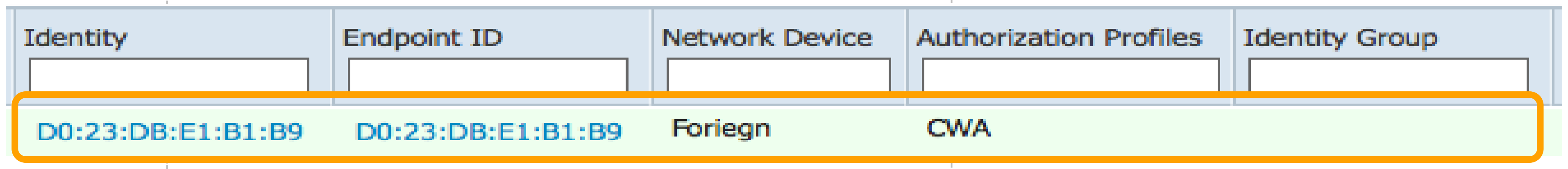
Radius NAC State	RUN
AAA Override ACL Name	ACL-WEBAUTH-REDIRECT
AAA Override ACL Applied Status	Yes
AAA Override Flex ACL	none
AAA Override Flex ACL Applied Status	Unavailable
Redirect URL	https://ise11-mnr.corp.rf-demo.com:8443/guestportal/



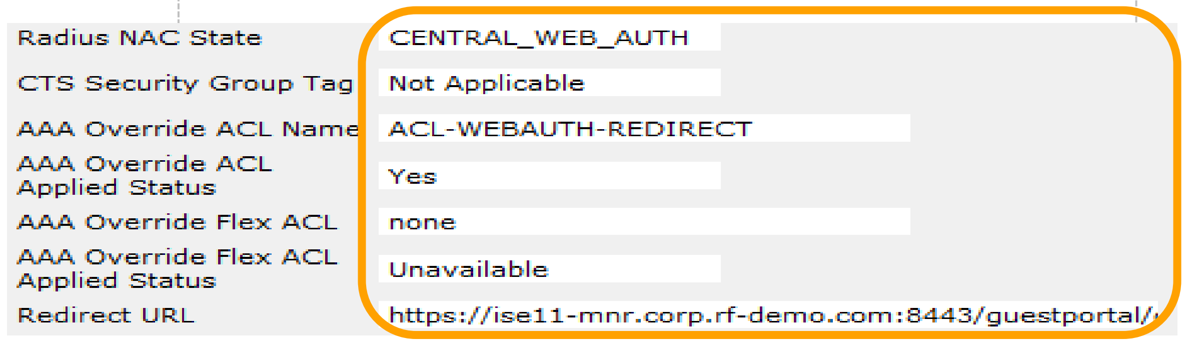
Client MAC Addr	AP Name	WLAN SSID
d0:23:db:e1:b1:b9	10.1.100.61	Imran3



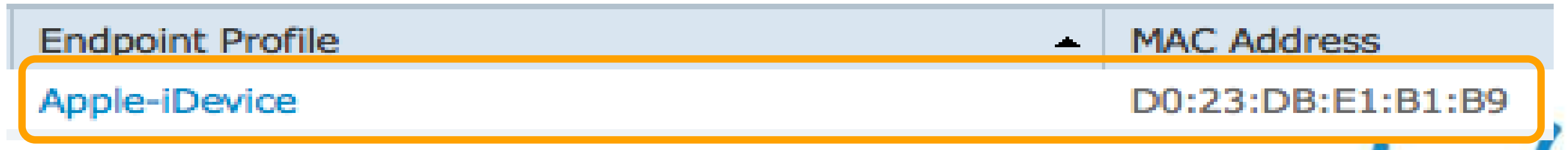
Mobility Role	Export Anchor
Mobility Peer IP Address	10.1.100.61
Policy Manager State	CENTRAL_WEB_AUTH



Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group
D0:23:DB:E1:B1:B9	D0:23:DB:E1:B1:B9	Foriegn	CWA	

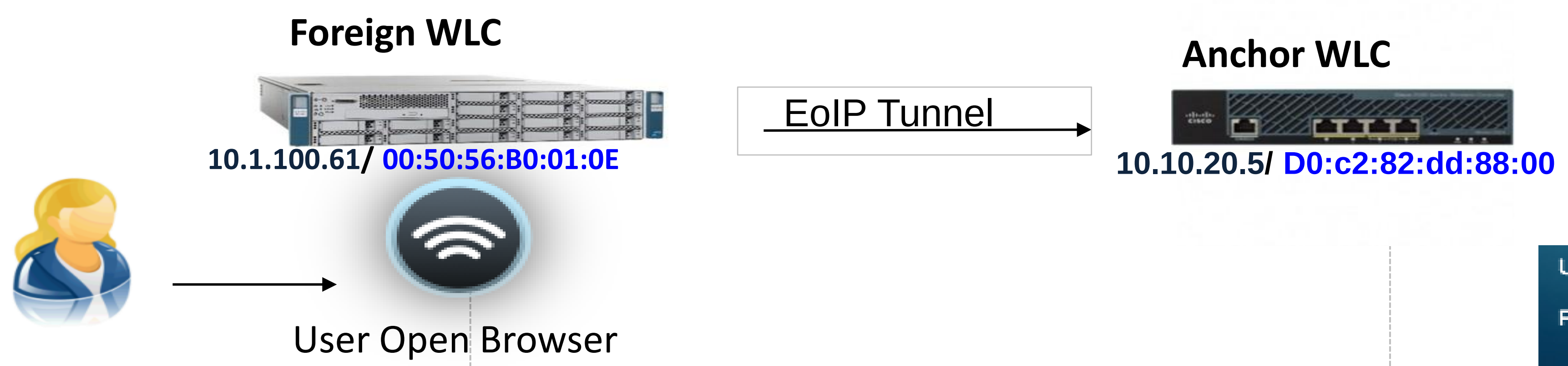


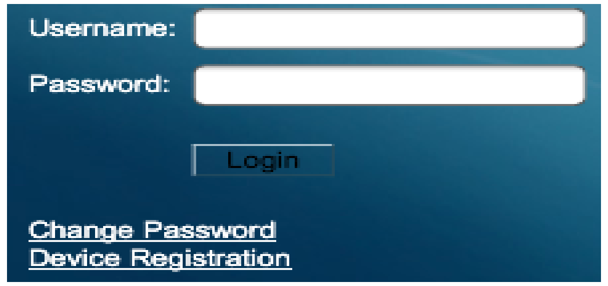
Radius NAC State	CENTRAL_WEB_AUTH
CTS Security Group Tag	Not Applicable
AAA Override ACL Name	ACL-WEBAUTH-REDIRECT
AAA Override ACL Applied Status	Yes
AAA Override Flex ACL	none
AAA Override Flex ACL Applied Status	Unavailable
Redirect URL	https://ise11-mnr.corp.rf-demo.com:8443/guestportal/

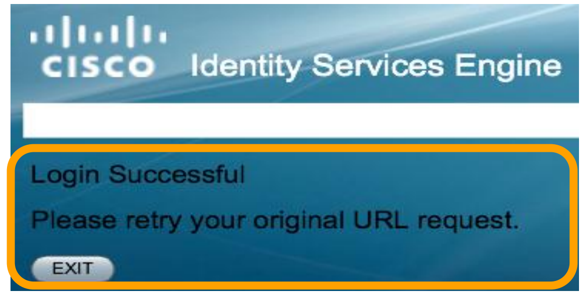


Endpoint Profile	MAC Address
Apple-iDevice	D0:23:DB:E1:B1:B9

CWA – Session Flow

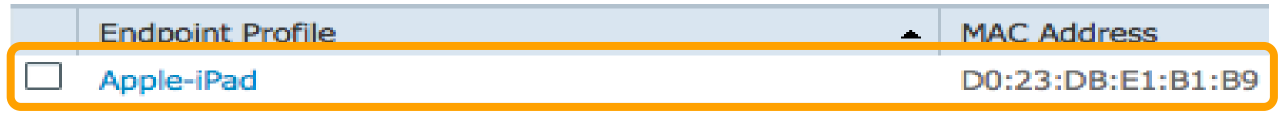




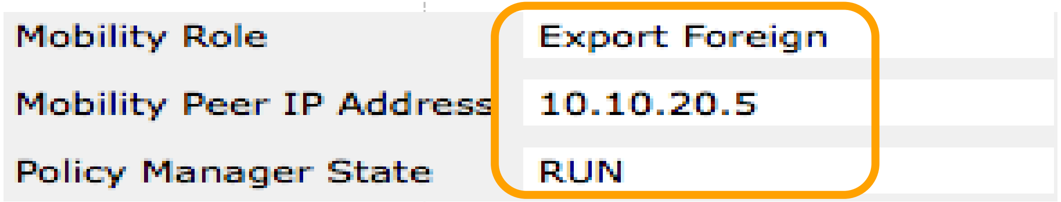


Login Successful

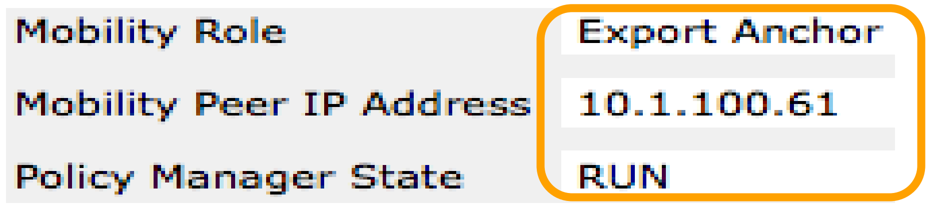
Please retry your original URL request.



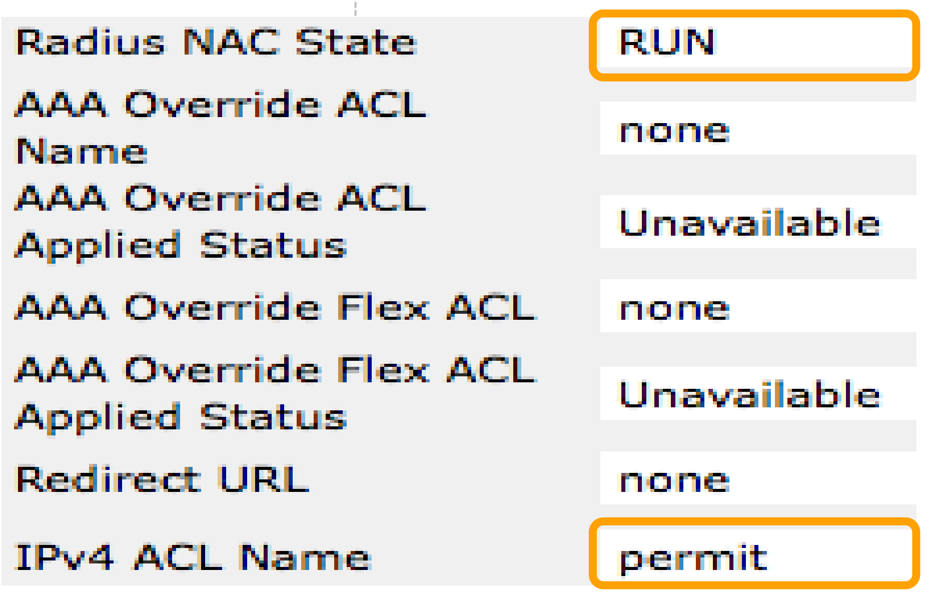
	Endpoint Profile	MAC Address
□	Apple-iPad	D0:23:DB:E1:B1:B9



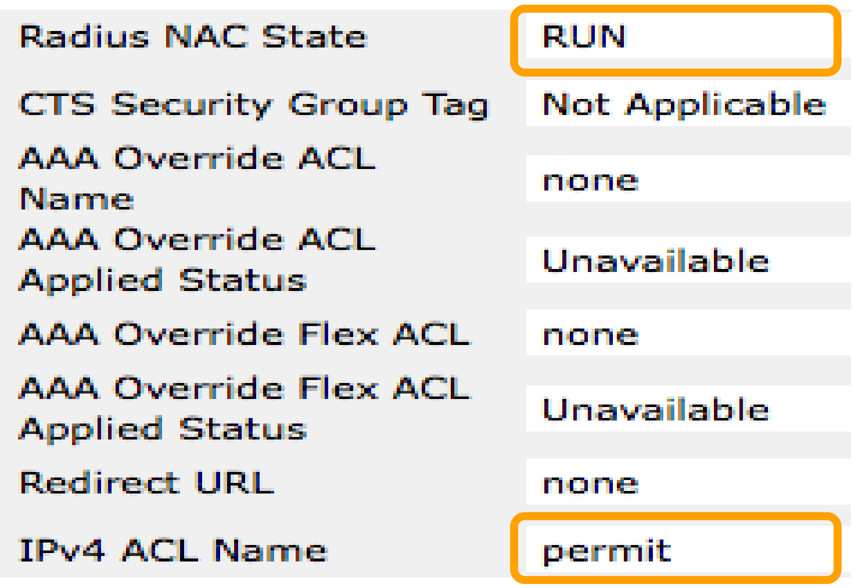
Mobility Role	Export Foreign
Mobility Peer IP Address	10.10.20.5
Policy Manager State	RUN



Mobility Role	Export Anchor
Mobility Peer IP Address	10.1.100.61
Policy Manager State	RUN

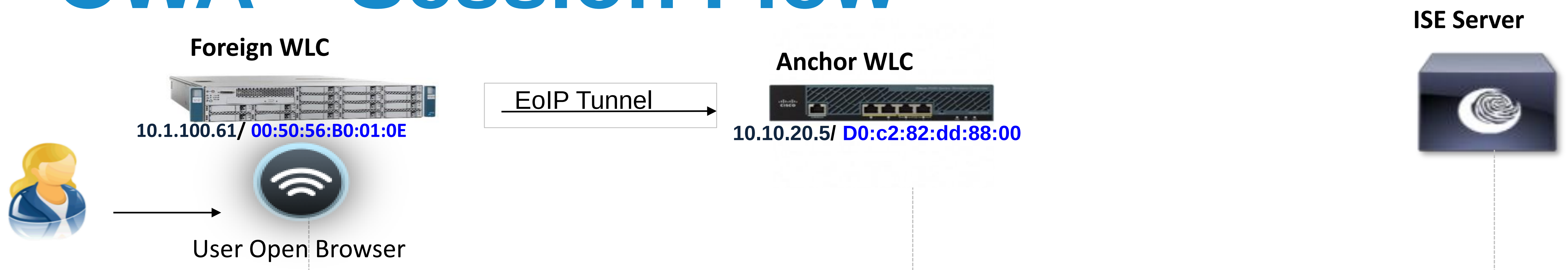


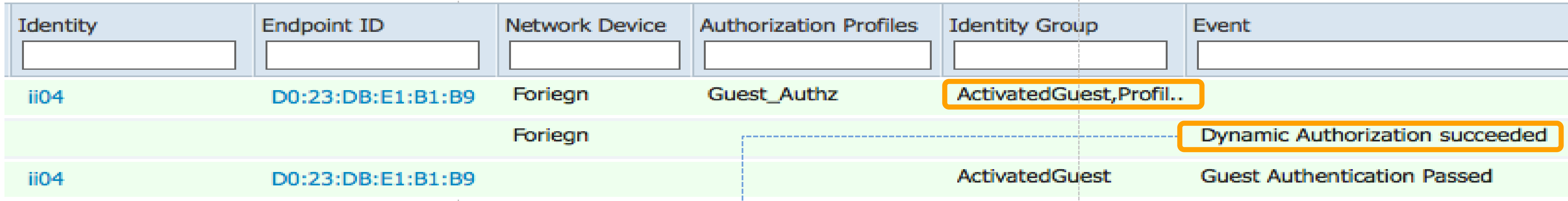
Radius NAC State	RUN
AAA Override ACL Name	none
AAA Override ACL Applied Status	Unavailable
AAA Override Flex ACL	none
AAA Override Flex ACL Applied Status	Unavailable
Redirect URL	none
IPv4 ACL Name	permit



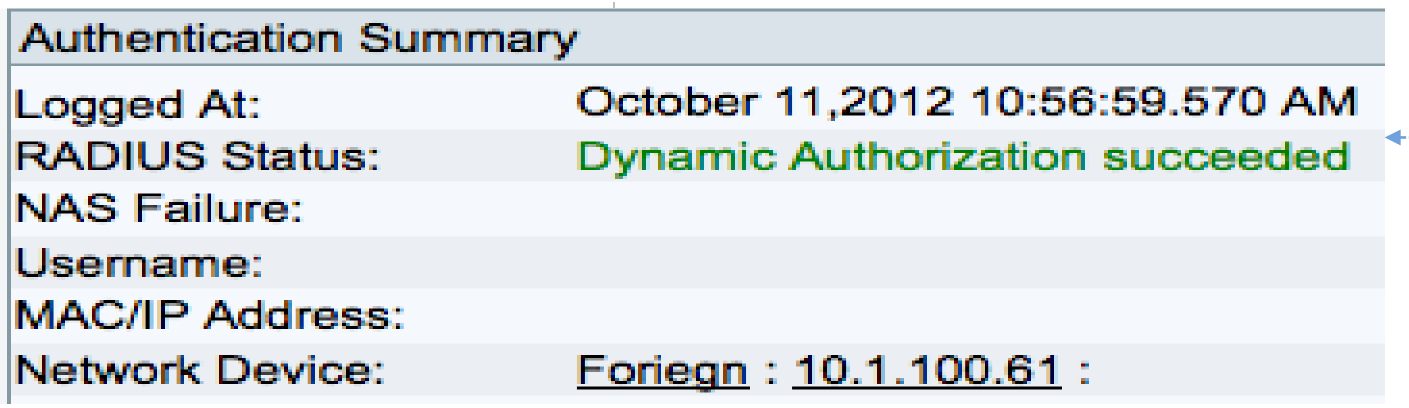
Radius NAC State	RUN
CTS Security Group Tag	Not Applicable
AAA Override ACL Name	none
AAA Override ACL Applied Status	Unavailable
AAA Override Flex ACL	none
AAA Override Flex ACL Applied Status	Unavailable
Redirect URL	none
IPv4 ACL Name	permit

CWA – Session Flow





Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Event
ii04	D0:23:DB:E1:B1:B9	Foriegn	Guest_Authz	ActivatedGuest,Profil..	
		Foriegn			Dynamic Authorization succeeded
ii04	D0:23:DB:E1:B1:B9			ActivatedGuest	Guest Authentication Passed



Authentication Summary

Logged At:	October 11,2012 10:56:59.570 AM
RADIUS Status:	Dynamic Authorization succeeded
NAS Failure:	
Username:	
MAC/IP Address:	
Network Device:	Foriegn : 10.1.100.61 :

Guest Services Portal

When to Use Web-Authentication ?

802.1X

Managed 802.1X-devices
Known users

Employee

MAB

(mac-address bypass)
Managed devices

Web Auth

Users without 802.1X devices
Users with Bad credentials

Employee
(bad credential)

Guest

- Web Auth is a **supplementary** authentication method

  Most useful when users can’t perform or pass 802.1X

- Primary Use Case: Guest Access

  Secondary Use Case: Employee who fails 802.1X

Guest Authentication Portal

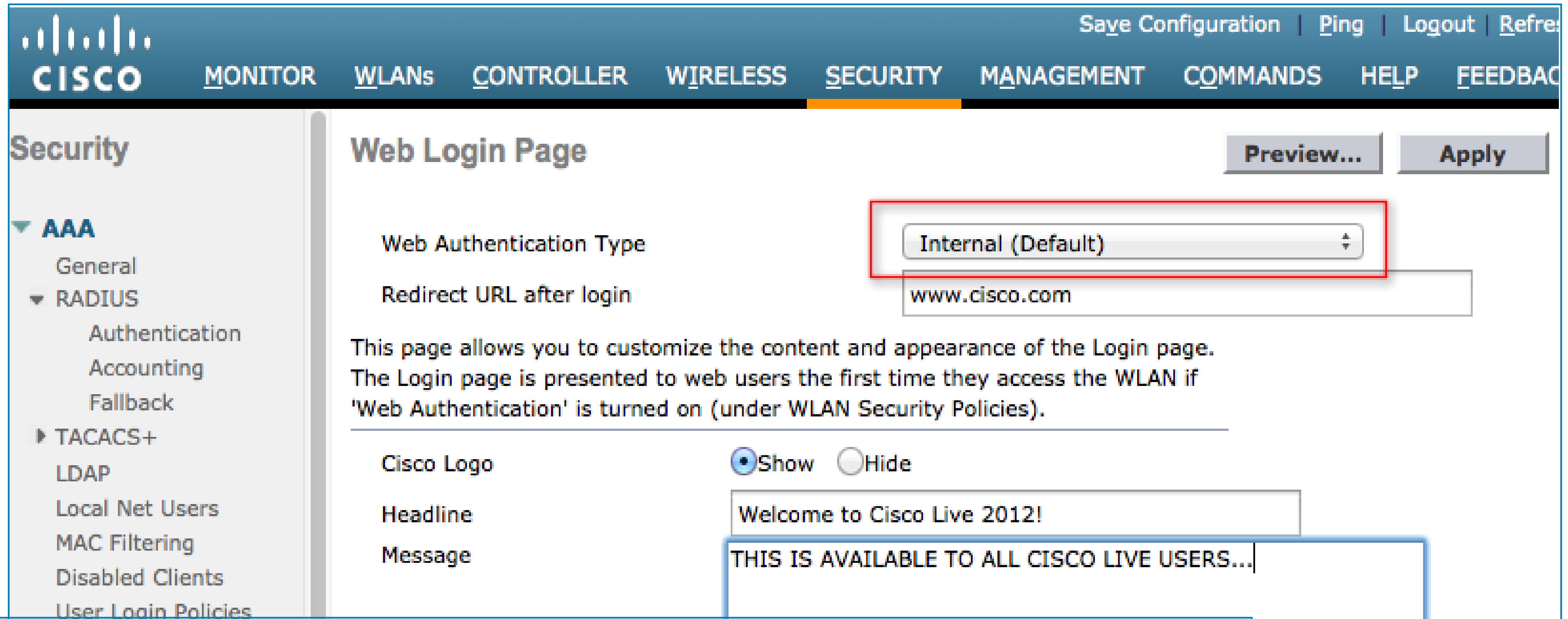
Internal (Default Web Authentication Pages)

- Wireless Guest Authentication Portal is available in 4 modes:
- Customised (Downloaded Customised Web Pages)
- External Using ISE Guest Server
- External (Re-directed to external server)

Wireless Guest Authentication Portal

Internal Web Portal

- Wireless guest user associates to the guest SSID
- Initiates a browser connection to any website
- Web login page will displayed



Web Login Page

Web Authentication Type: Internal (Default)

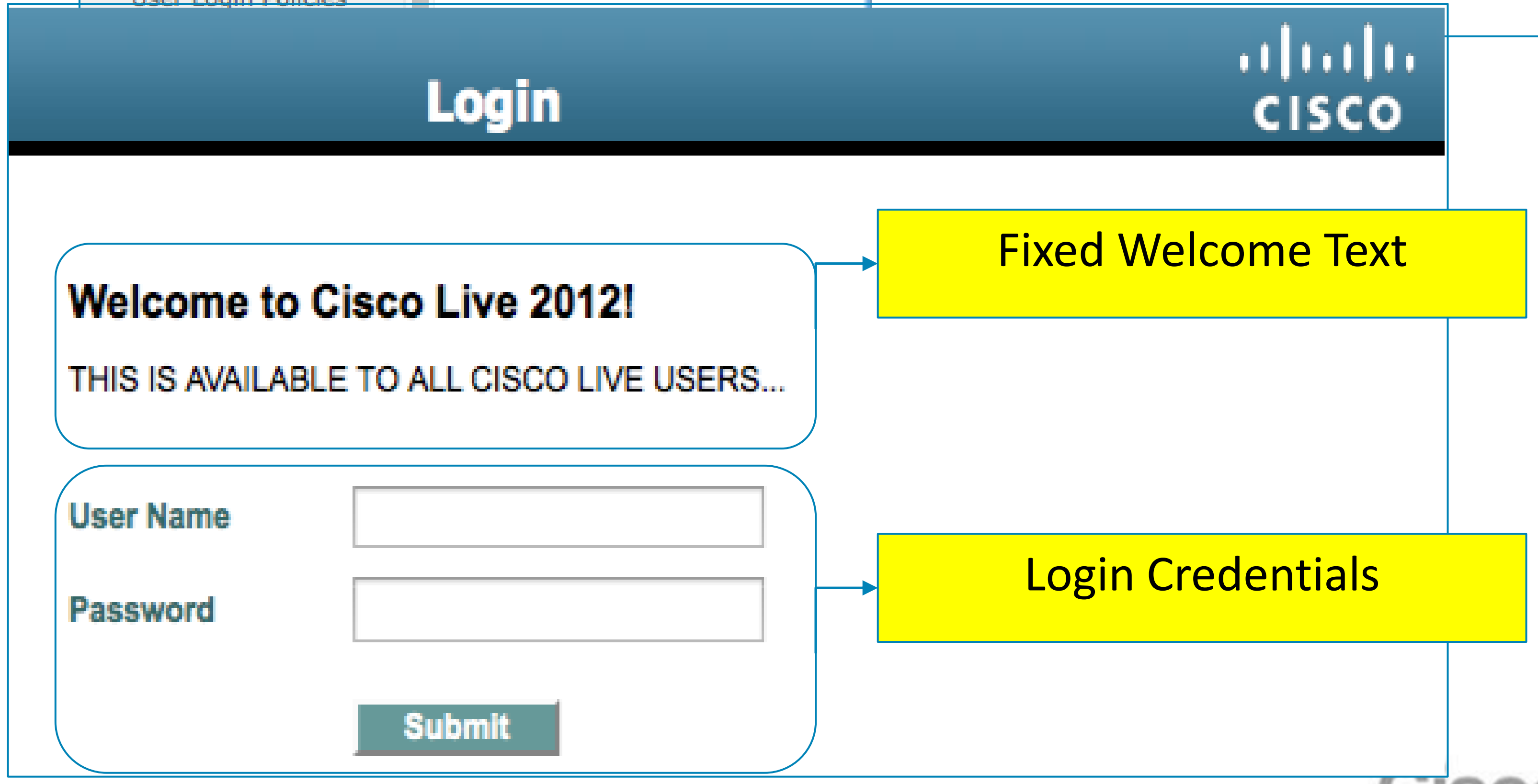
Redirect URL after login: www.cisco.com

This page allows you to customize the content and appearance of the Login page. The Login page is presented to web users the first time they access the WLAN if 'Web Authentication' is turned on (under WLAN Security Policies).

Cisco Logo: ● Show ○ Hide

Headline: Welcome to Cisco Live 2012!

Message: THIS IS AVAILABLE TO ALL CISCO LIVE USERS...



Welcome to Cisco Live 2012!

THIS IS AVAILABLE TO ALL CISCO LIVE USERS...

User Name:

Password:

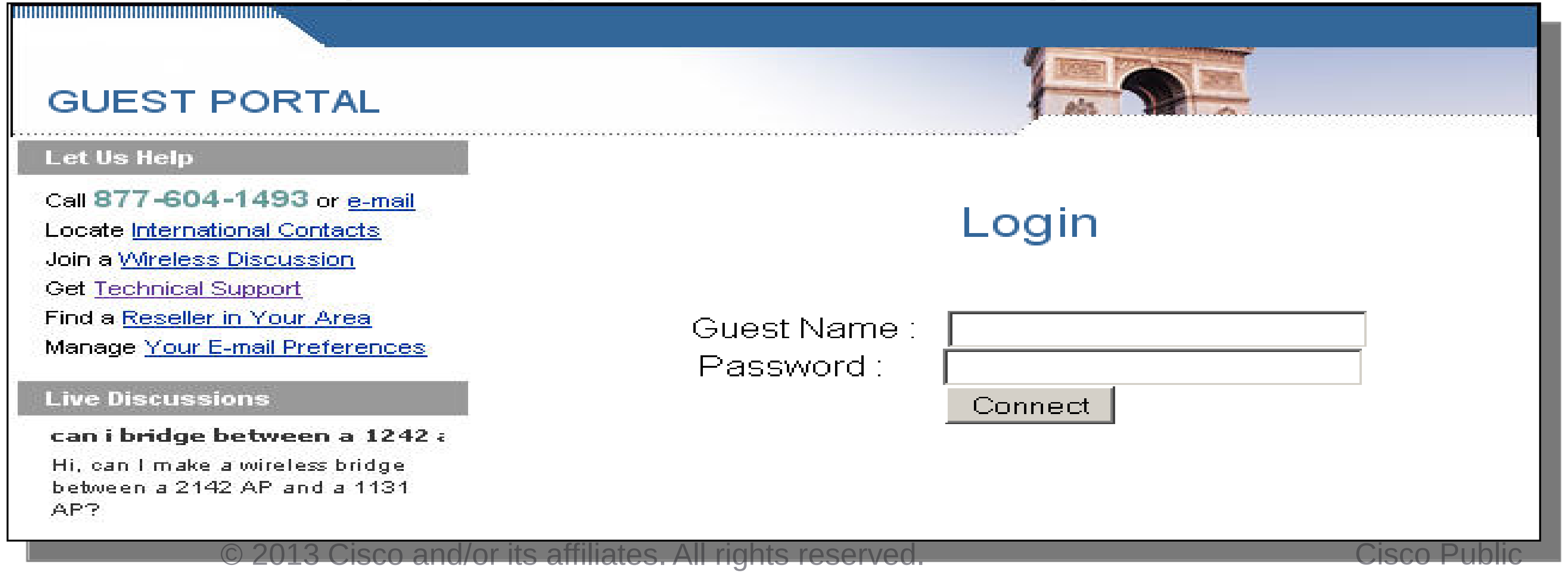
Fixed Welcome Text

Login Credentials

Wireless Guest Authentication Portal

Customisable Web Portal

- Create your own Guest Access Portal web pages
- Upload the customised web page to the WLC
- Configure the WLC to use “customisable web portal”
- Customised WebAuth bundle up to 5 Mb in size can contain
  - 22 login pages (16 WLANs , 5 Wired LANs and 1 Global)
  - 22 login failure pages (in WLC 5.0 and up)
  - 22 login successful pages (in WLC 5.0 and up)



GUEST PORTAL

Let Us Help

Call 877-604-1493 or e-mail
Locate International Contacts
Join a Wireless Discussion
Get Technical Support
Find a Reseller in Your Area
Manage Your E-mail Preferences

Live Discussions

can i bridge between a 1242 a

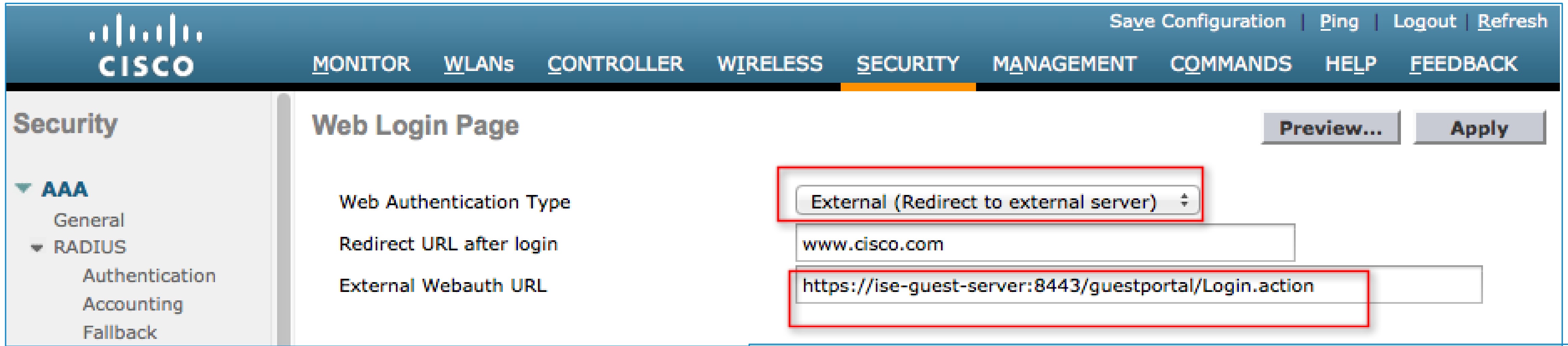
Hi, can I make a wireless bridge between a 2142 AP and a 1131 AP?

Login

Guest Name :
Password :

Wireless Guest Authentication Portal

External Web Portal

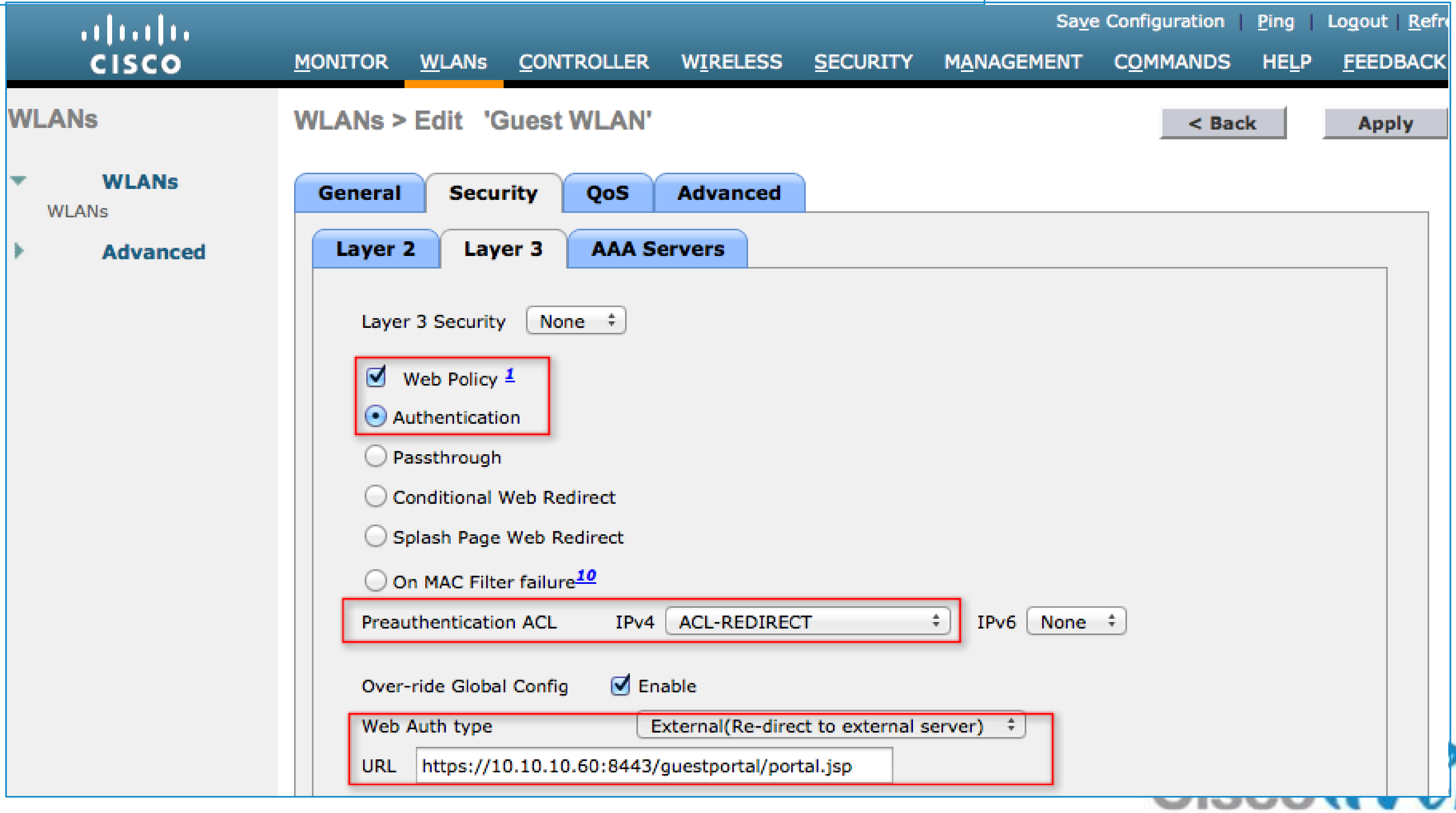


Web Login Page

Web Authentication Type: External (Redirect to external server)

Redirect URL after login: www.cisco.com

External Webauth URL: https://ise-guest-server:8443/guestportal/Login.action



WLANs > Edit 'Guest WLAN'

Layer 3 Security: None

☑ Web Policy [1]

● Authentication

○ Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

○ On MAC Filter failure[10]

Preauthentication ACL IPv4: ACL-REDIRECT IPv6: None

Over-ride Global Config ☑ Enable

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

URL: https://10.10.10.60:8443/guestportal/portal.jsp

- Set in WLC > Security > WebAuth > Login
- Or override at Guest WLAN
  - Option to use Pre-Auth ACL

Wireless Guest

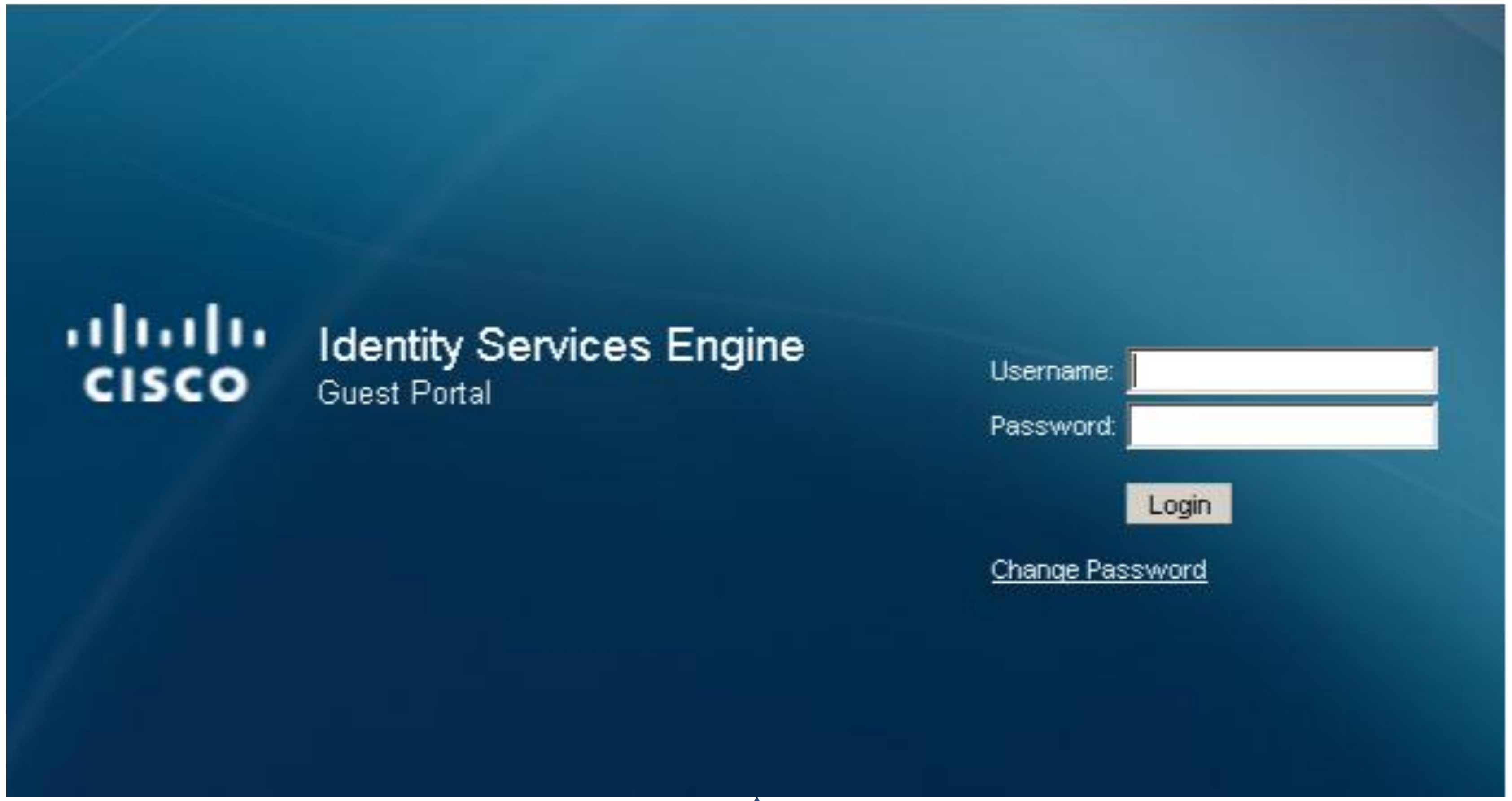
Centralised Login Page

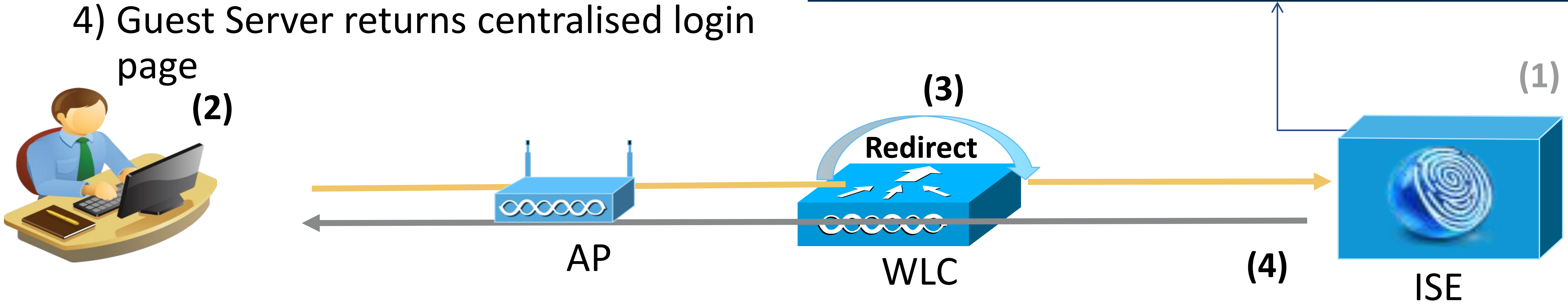
1) Administrator Creates WLAN Login Page on ISE

2) Wireless Guest Opens Web browser

3) Web traffic is intercepted by Wireless LAN Controller and redirected to Guest Server.

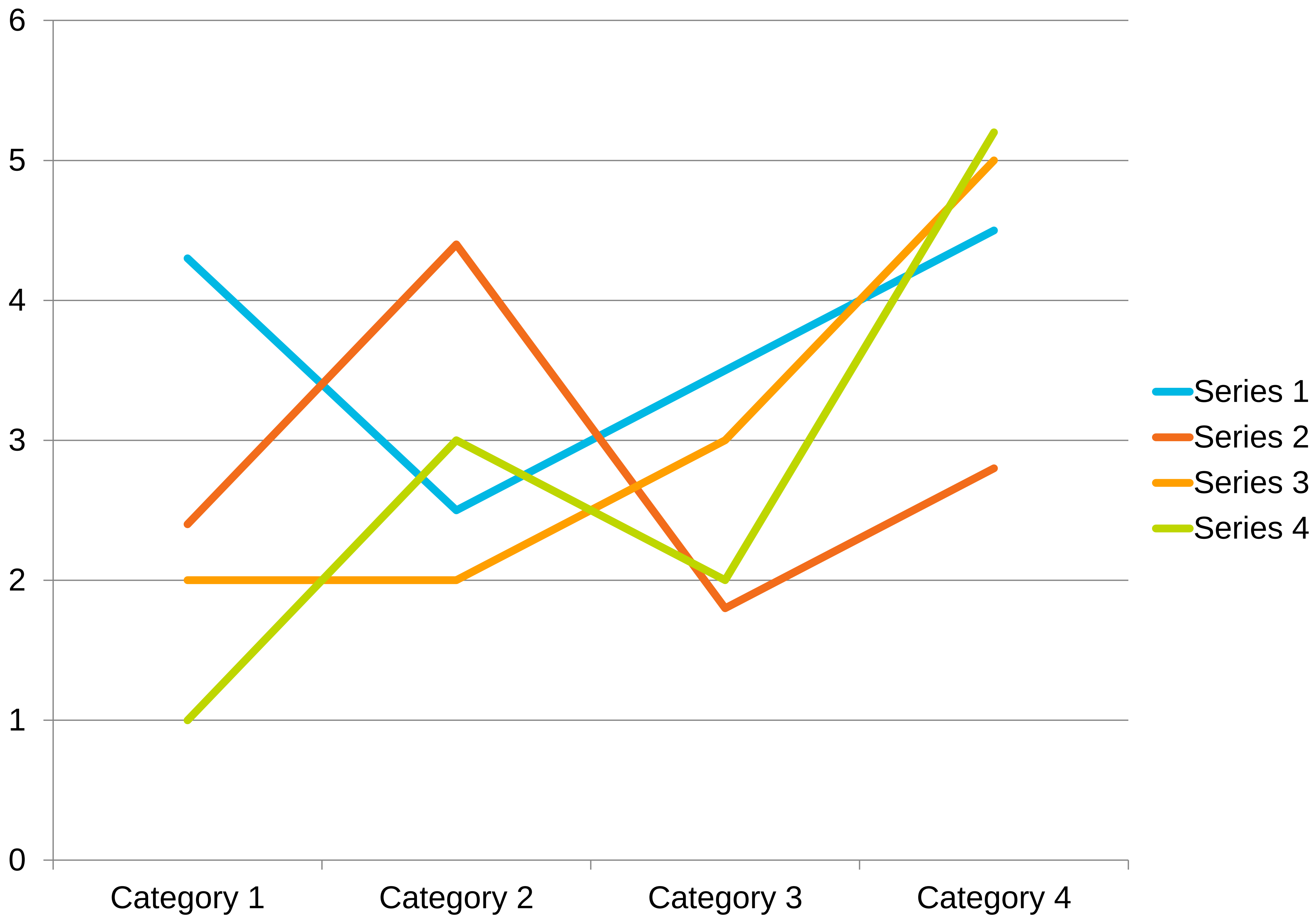
4) Guest Server returns centralised login page





Guest Services Provisioning

Line Chart Example



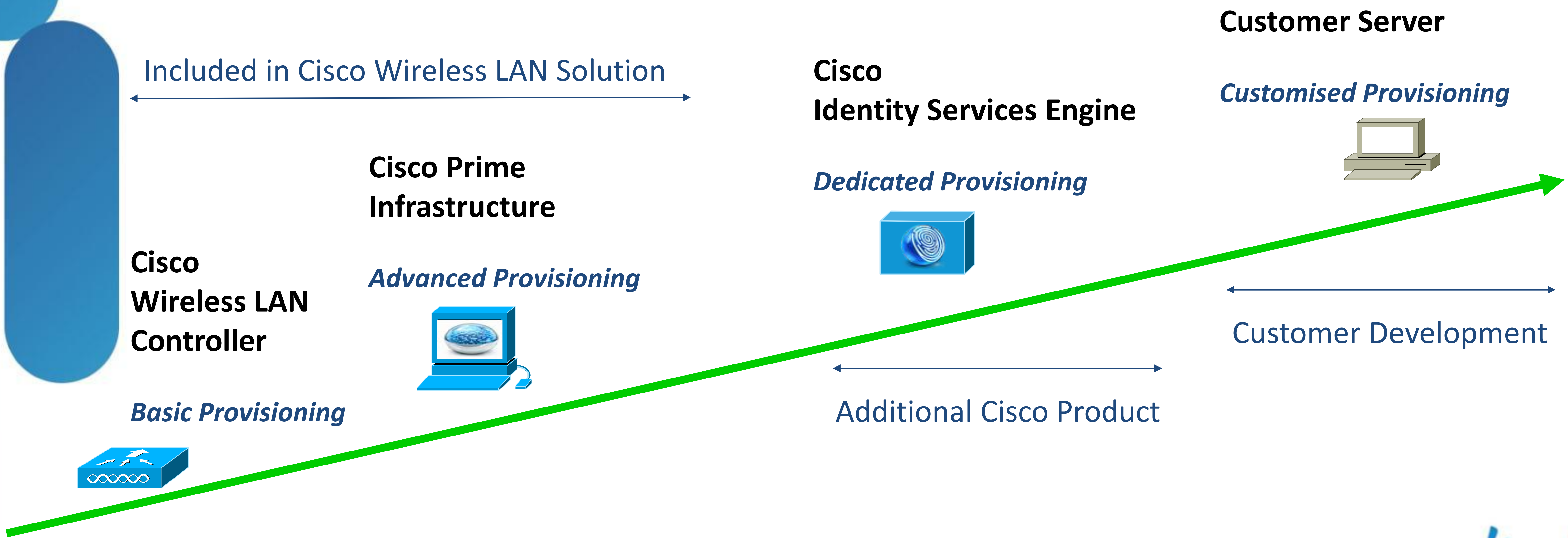
Source: Placeholder for Notes is 18 points

Requirements for Guest Provisioning

- Might be performed by non-IT user
- Must deliver basic features, but might also require advanced features:
  - Duration,
  - Start/End Time,
  - Bulk provisioning, …
- Provisioning Strategies :
  - Lobby Ambassador
  - Employees

Multiple Guest Provisioning Services

- Cisco Guest Access Solution support several provisioning tools, with different feature richness.



Included in Cisco Wireless LAN Solution

Cisco Wireless LAN Controller

Basic Provisioning

Cisco Prime Infrastructure

Advanced Provisioning

Cisco Identity Services Engine

Dedicated Provisioning

Additional Cisco Product

Customer Server

Customised Provisioning

Customer Development

Guest Provisioning Service : WLC

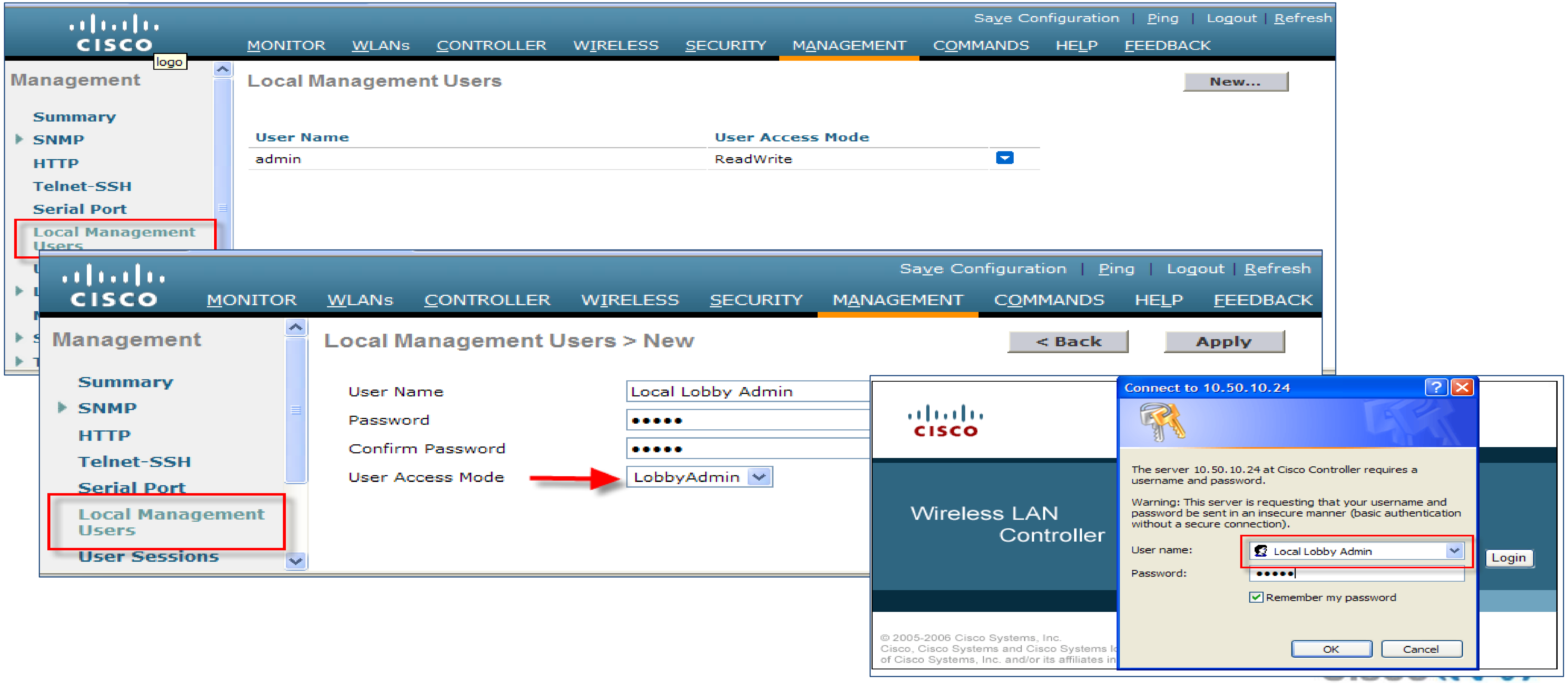
Cisco Wireless LAN Controller

- Lobby Ambassador accounts can be created directly on Wireless LAN Controllers
- Lobby Ambassadors have limited guest feature and must create the user directly on WLC:
  - Create Guest User – up to 2048 entries
  - Set time limitation – up to 35 weeks
  - Set Guest SSID
  - Set QoS Profile

Guest Provisioning Service

Create the Lobby Admin in WLC

- Lobby administrator can be created in WLC directly



Local Management Users

User Name	User Access Mode
admin	ReadWrite

Local Management Users > New

User Name	Local Lobby Admin
Password	•••••
Confirm Password	•••••
User Access Mode	LobbyAdmin

Connect to 10.50.10.24

The server 10.50.10.24 at Cisco Controller requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

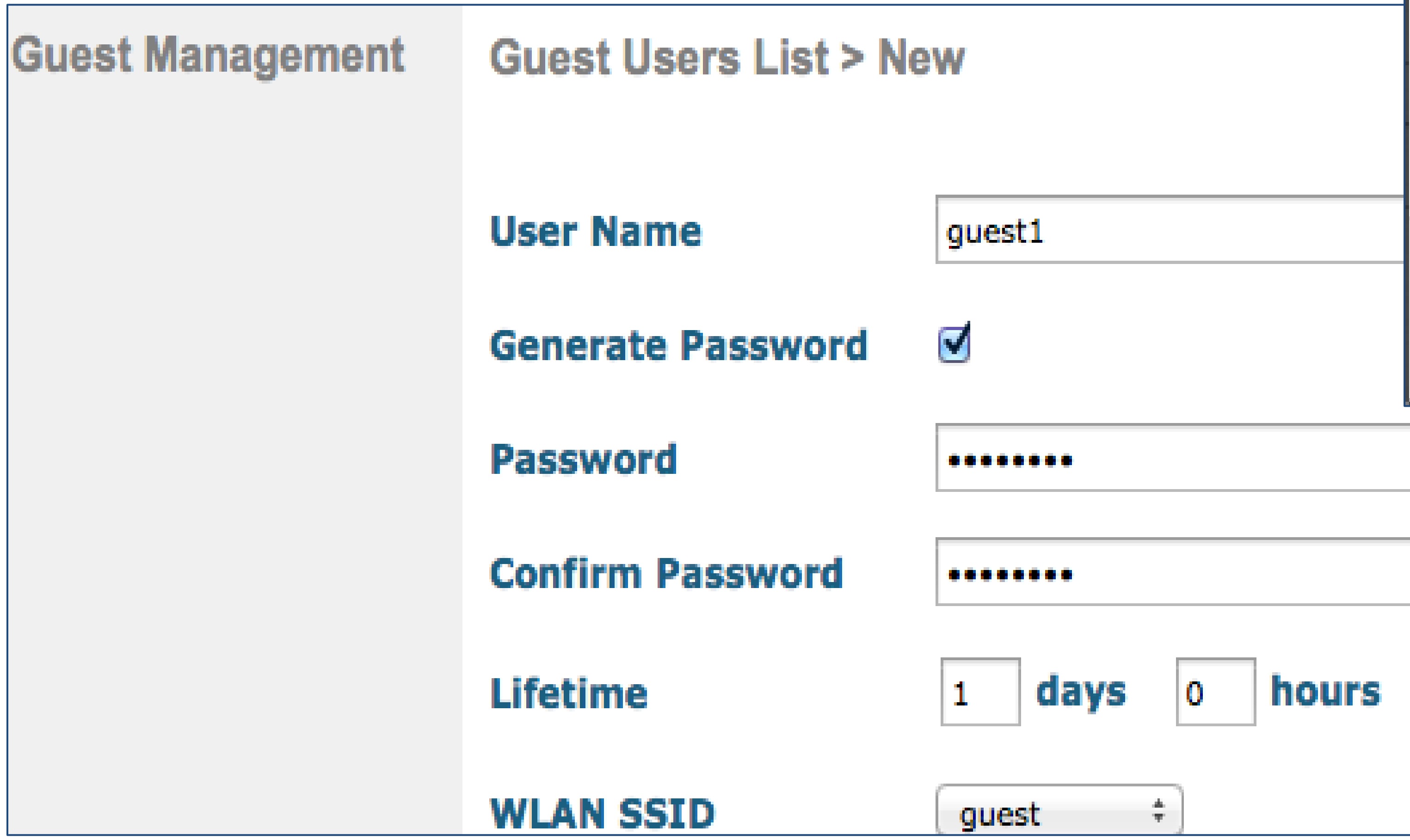
User name: Local Lobby Admin

Password: •••••

☑ Remember my password

© 2005-2006 Cisco Systems, Inc.
Cisco, Cisco Systems and Cisco Systems l
of Cisco Systems, Inc. and/or its affiliates in

Local WLC Guest Management

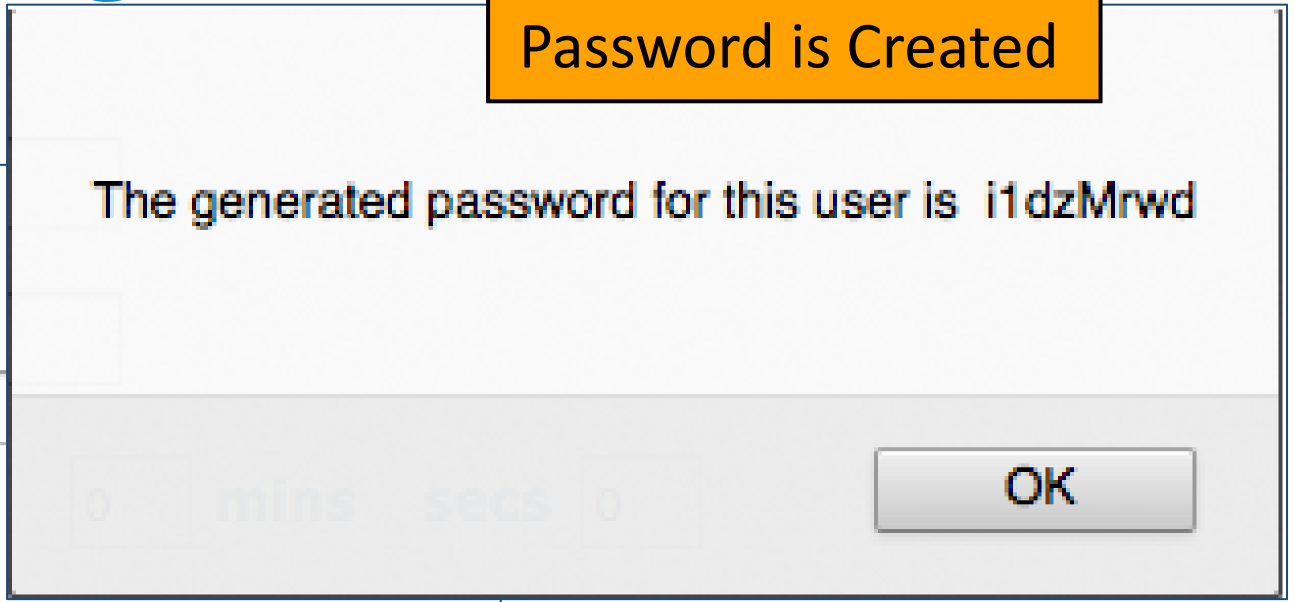


Guest Management

Guest Users List > New

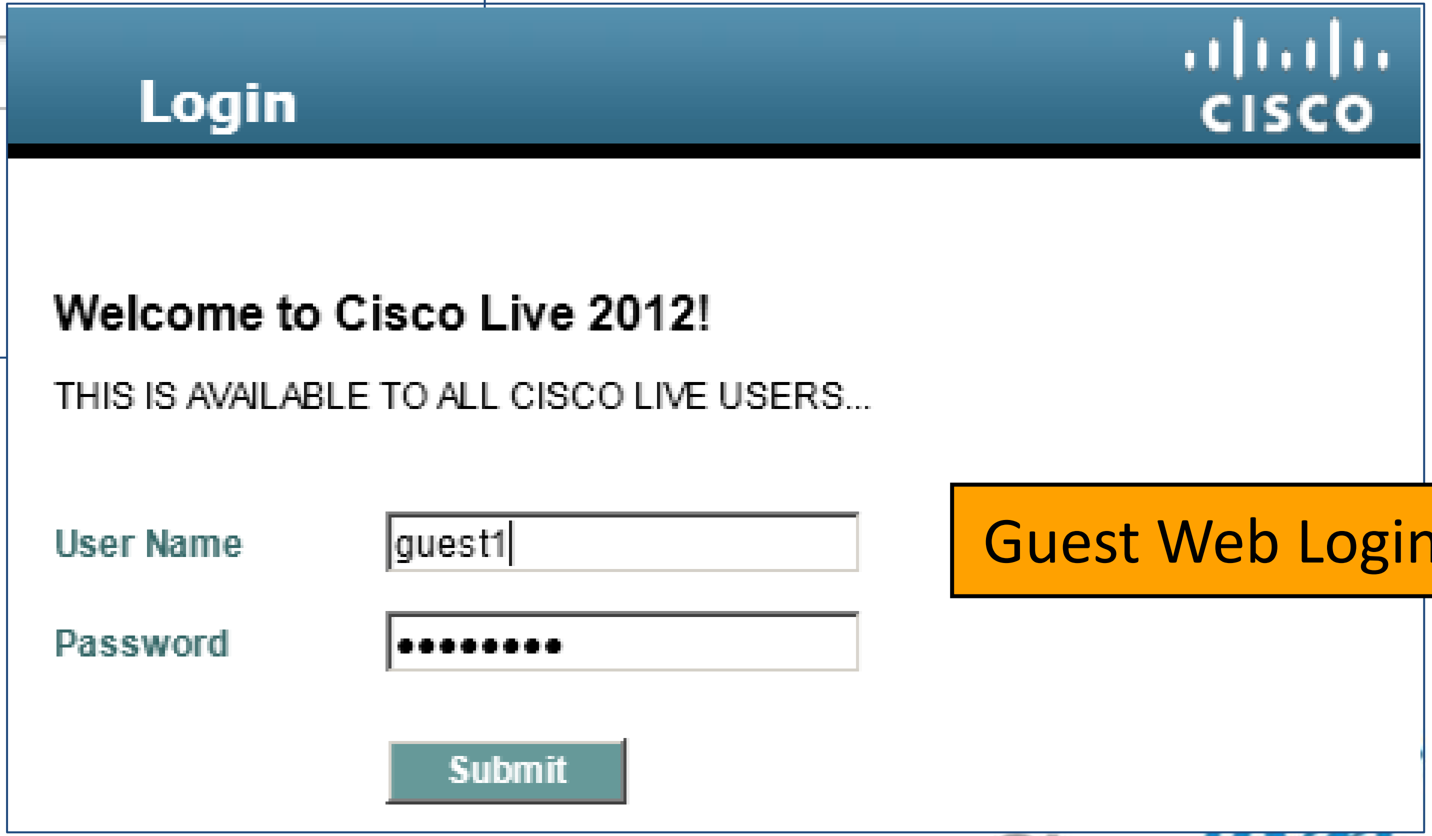
User Name	guest1
Generate Password	☑
Password	•••••••••
Confirm Password	•••••••••
Lifetime	1 days 0 hours
WLAN SSID	guest

Quickly Create Guest with Time and WLAN Profile



The generated password for this user is i1dzMrwd

Password is Created



Welcome to Cisco Live 2012!

THIS IS AVAILABLE TO ALL CISCO LIVE USERS...

User Name	guest1
Password	•••••••••

Guest Web Login

Guest Provisioning Service : NCS

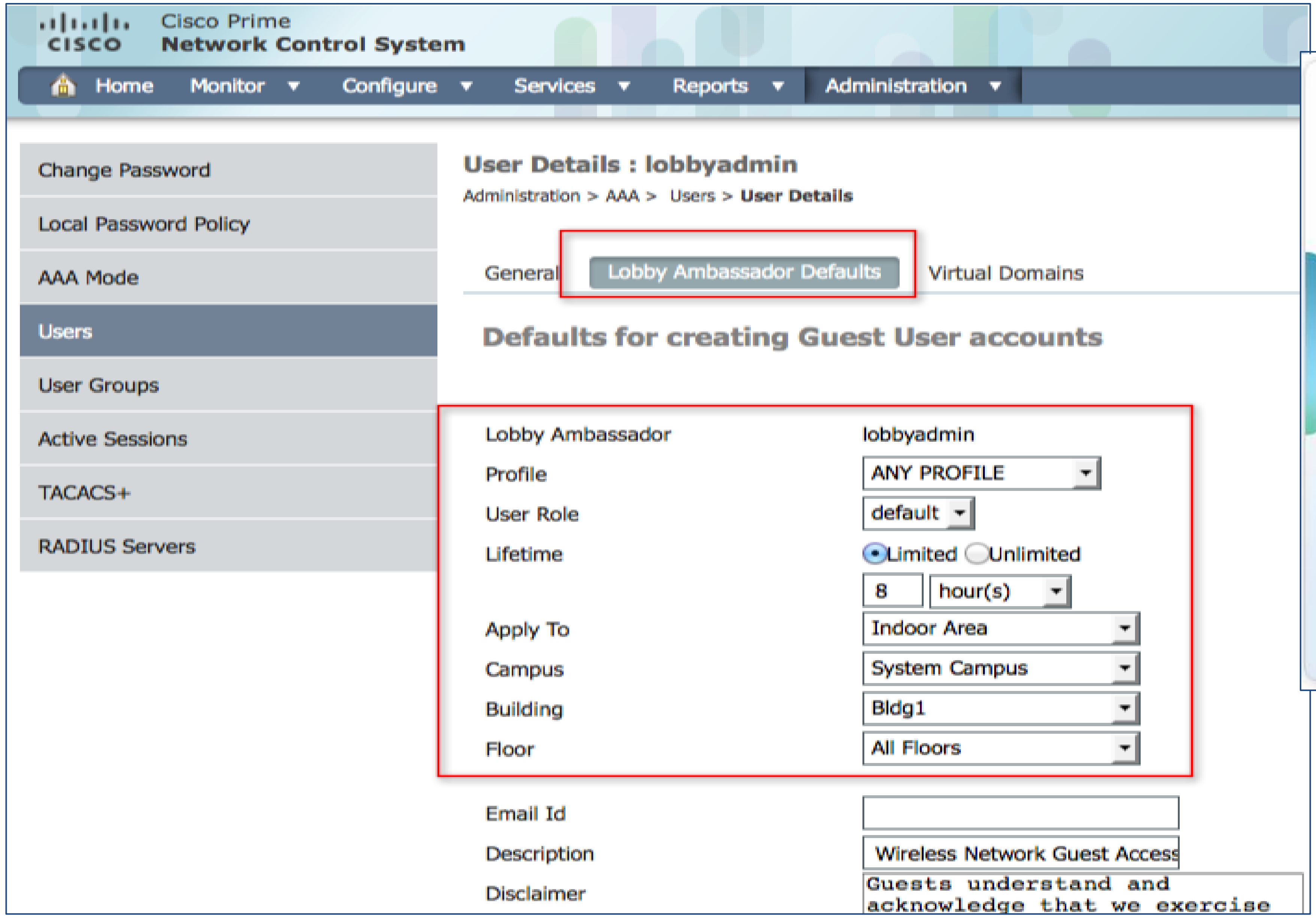
Cisco Prime Network Control System

- NCS offer specific Lobby Ambassador access for Guest management only
- Lobby Ambassador accounts can be created directly on NCS, or be defined on external RADIUS/TACACS+ servers
- Lobby Ambassadors on NCS are able to create guest accounts with advanced features like:
  - Start/End time and date, duration,
  - Bulk provisioning,
  - Set QoS Profiles,
  - Set access based on WLC, Access Points or Location

Guest Provisioning Service

Lobby Ambassador Feature in NCS

- Associate the lobby admin with Profile and Location specific information

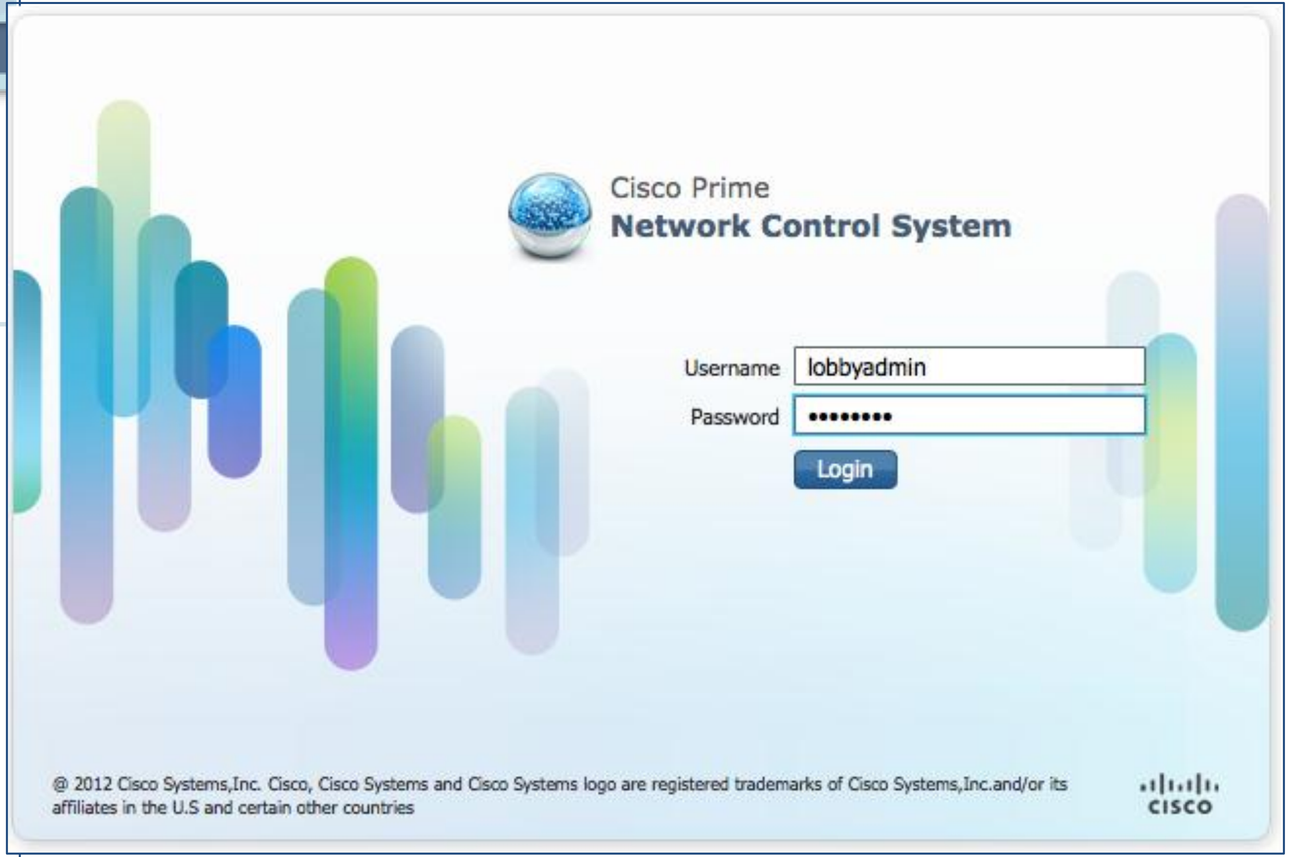


User Details : lobbyadmin

Administration > AAA > Users > **User Details**

Defaults for creating Guest User accounts

Lobby Ambassador	lobbyadmin
Profile	ANY PROFILE
User Role	default
Lifetime	● Limited ○ Unlimited
	8 hour(s)
Apply To	Indoor Area
Campus	System Campus
Building	Bldg1
Floor	All Floors
Email Id	
Description	Wireless Network Guest Access
Disclaimer	Guests understand and acknowledge that we exercise



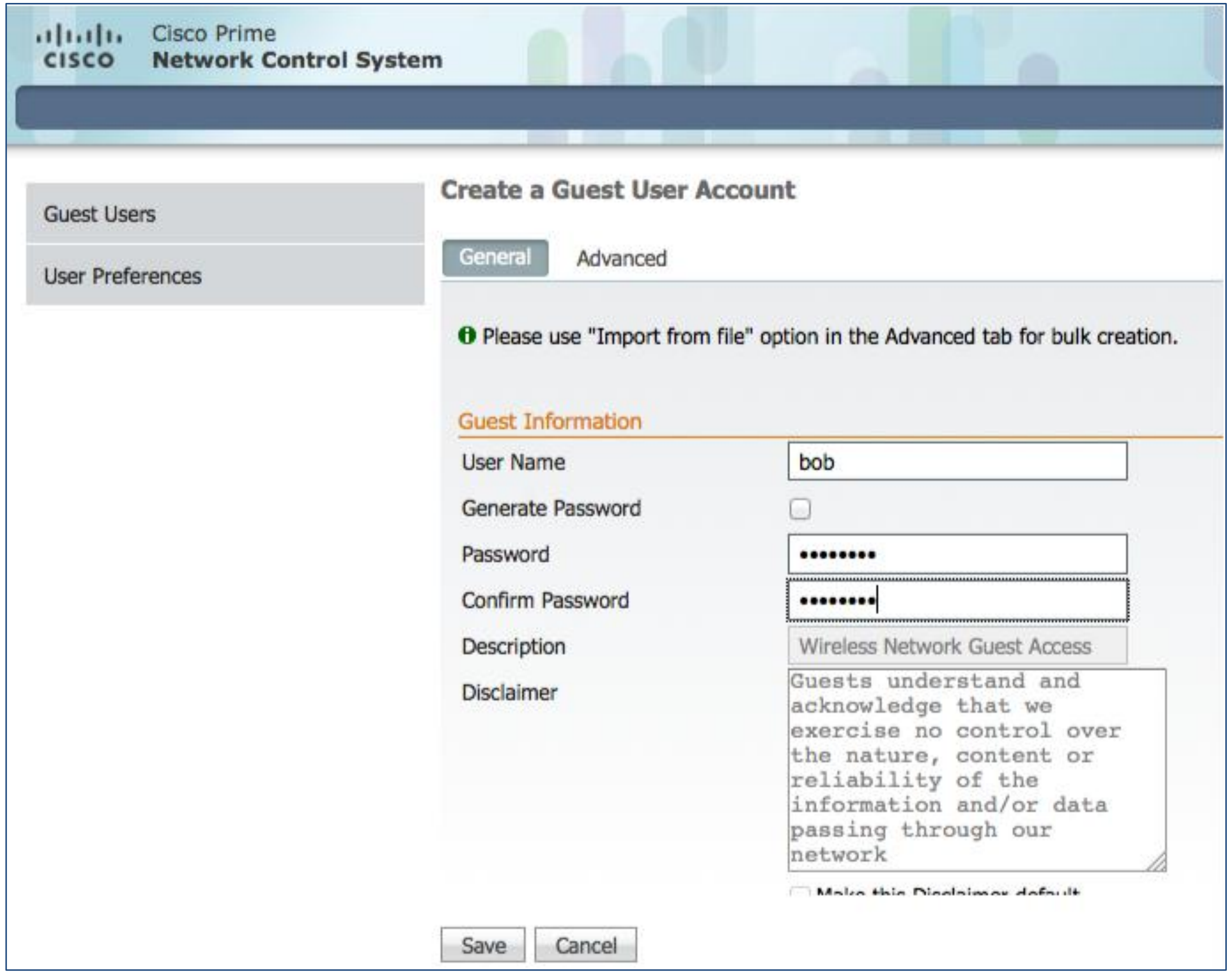
Username: lobbyadmin

Password: ••••••••

@ 2012 Cisco Systems,Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems,Inc.and/or its affiliates in the U.S and certain other countries

Guest Provisioning Service

Add a Guest User with NCS



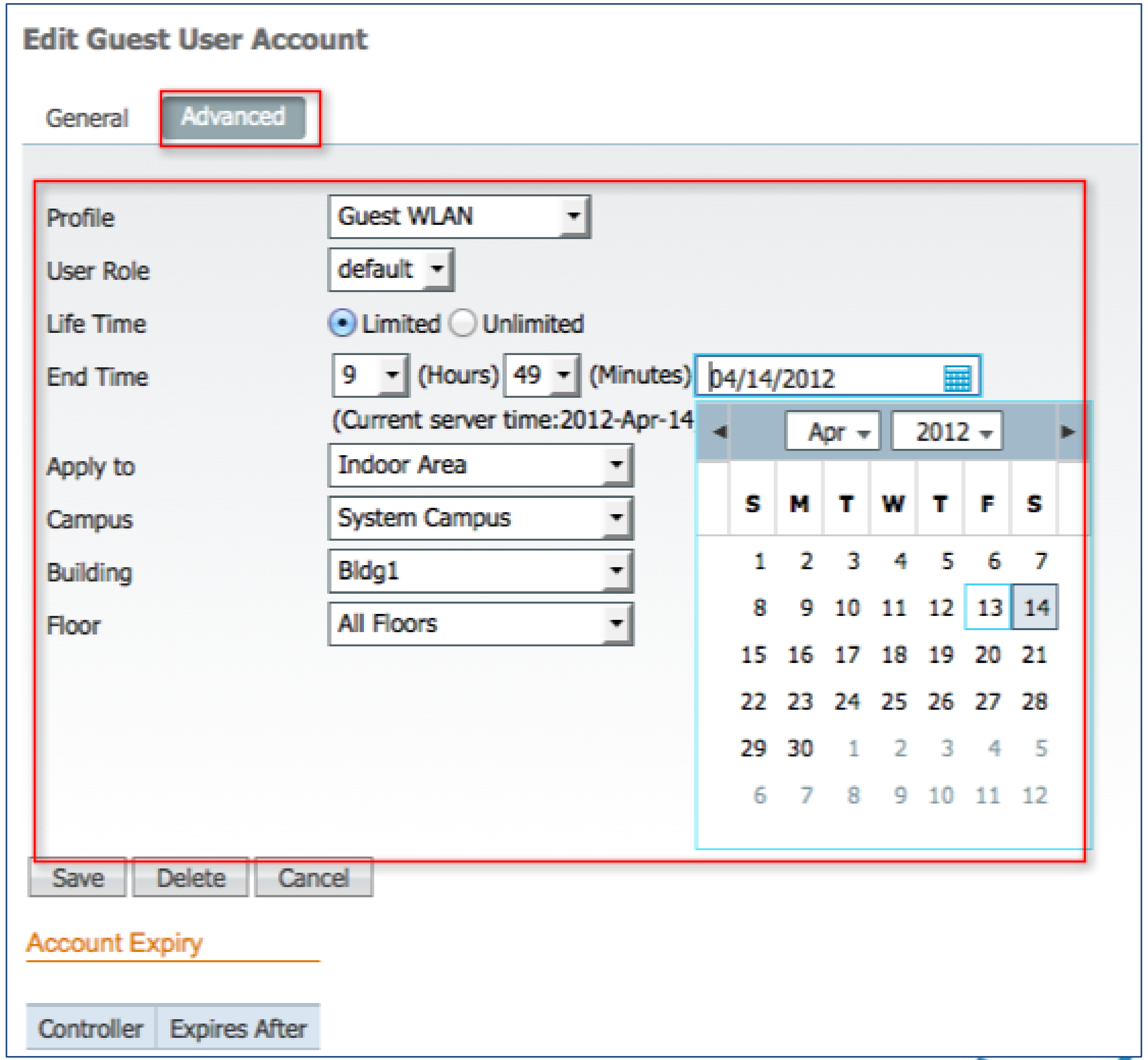
Create a Guest User Account

Please use "Import from file" option in the Advanced tab for bulk creation.

Guest Information

User Name	bob
Generate Password	□
Password	•••••••••
Confirm Password	•••••••••
Description	Wireless Network Guest Access
Disclaimer	Guests understand and acknowledge that we exercise no control over the nature, content or reliability of the information and/or data passing through our network

□ Make this Disclaimer default



Edit Guest User Account

Profile	Guest WLAN
User Role	default
Life Time	● Limited ○ Unlimited
End Time	9 (Hours) 49 (Minutes) 04/14/2012 (Current server time:2012-Apr-14
Apply to	Indoor Area
Campus	System Campus
Building	Bldg1
Floor	All Floors

Apr 2012

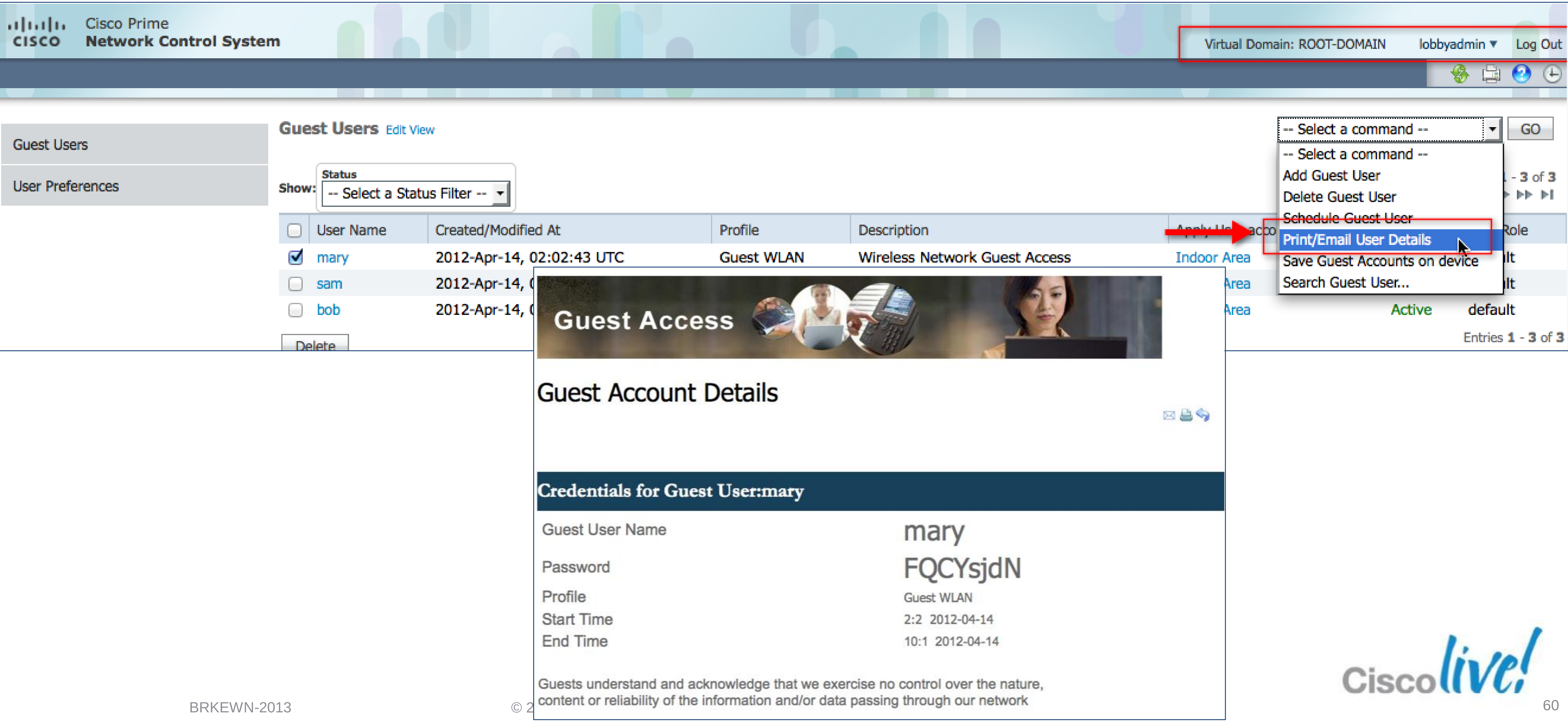
S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5
6	7	8	9	10	11	12

Account Expiry

Controller	Expires After

Guest Provisioning Service

Print/E-Mail Details of Guest User



☐	User Name	Created/Modified At	Profile	Description	Apply Us... acco		Role
☑	mary	2012-Apr-14, 02:02:43 UTC	Guest WLAN	Wireless Network Guest Access	Indoor Area		lt
☐	sam	2012-Apr-14, (			Area		lt
☐	bob	2012-Apr-14, (			Area	Active	default

Guest Account Details

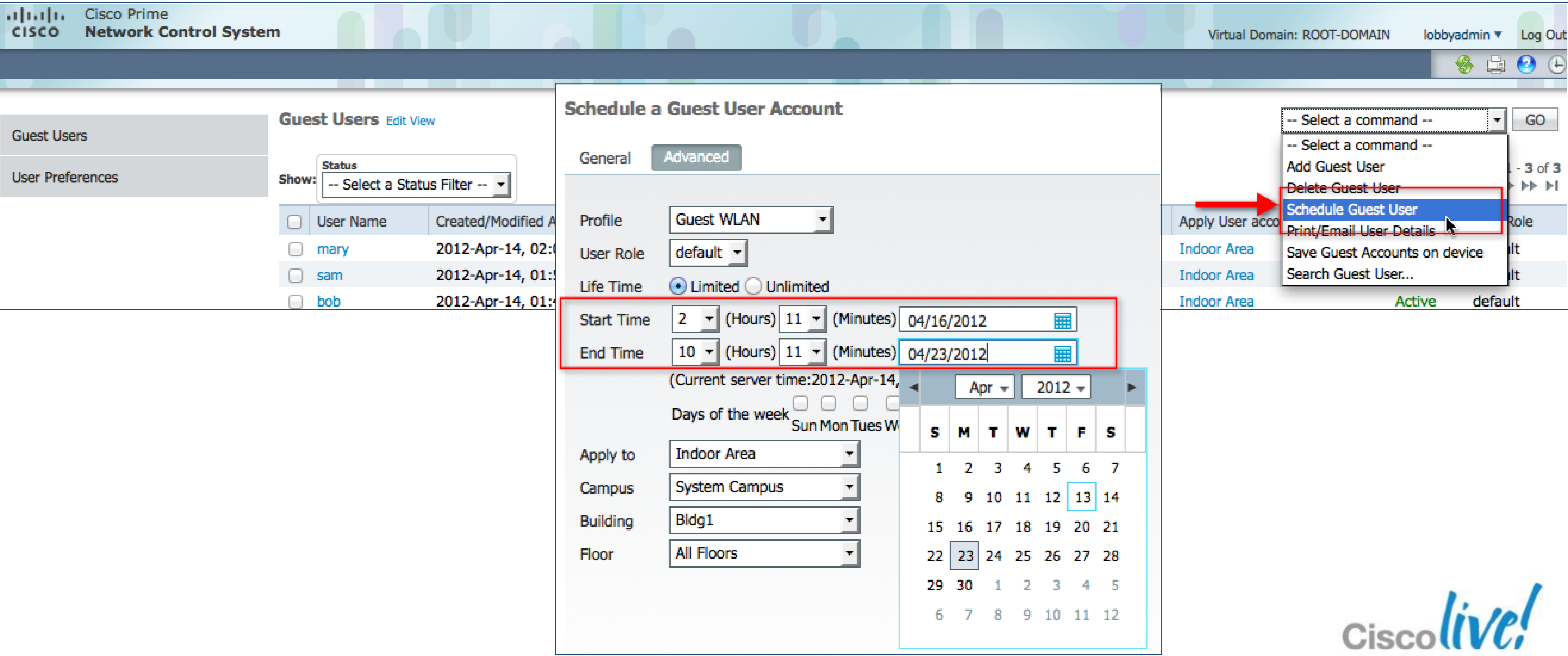
Credentials for Guest User:mary

Guest User Name	mary
Password	FQCYsjdN
Profile	Guest WLAN
Start Time	2:2 2012-04-14
End Time	10:1 2012-04-14

Guests understand and acknowledge that we exercise no control over the nature, content or reliability of the information and/or data passing through our network

Guest Provisioning Service

Schedule a Guest User



☐	User Name	Created/Modified A	Apply User acco		Role
☐	mary	2012-Apr-14, 02:(	Indoor Area		lt
☐	sam	2012-Apr-14, 01:5	Indoor Area		lt
☐	bob	2012-Apr-14, 01:4	Indoor Area	Active	default

Schedule a Guest User Account

Profile	Guest WLAN
User Role	default
Life Time	● Limited ○ Unlimited
Start Time	2 (Hours) 11 (Minutes) 04/16/2012
End Time	10 (Hours) 11 (Minutes) 04/23/2012
	(Current server time:2012-Apr-14,
Days of the week	☐ Sun ☐ Mon ☐ Tues ☐ W
Apply to	Indoor Area
Campus	System Campus
Building	Bldg1
Floor	All Floors

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5
6	7	8	9	10	11	12

Cisco Guest Services

Table Example

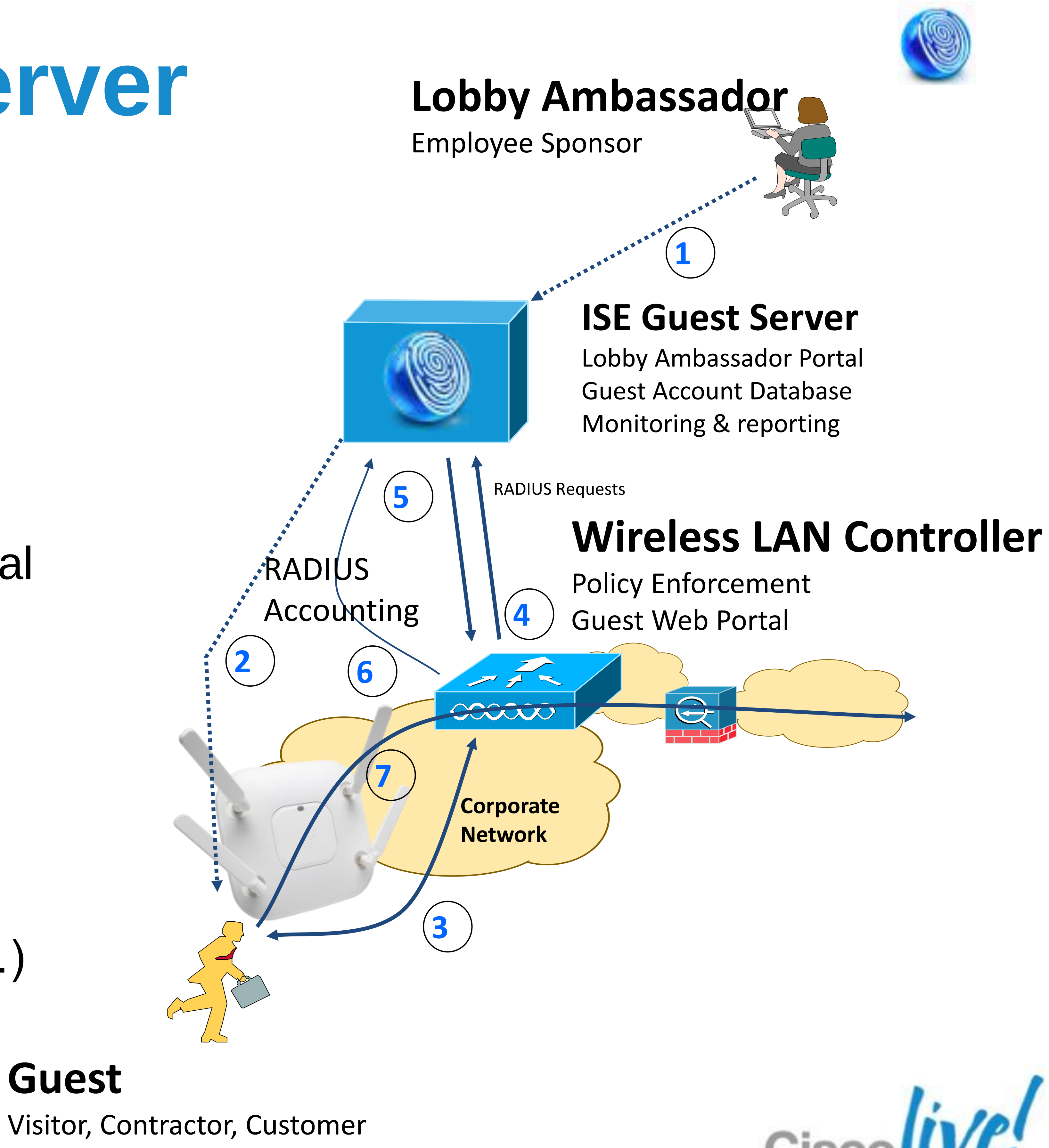
Header	Header	Header	Header	Header
Data	500	400	300	200
Data	100	200	300	400
Data	80	70	60	50
Data	5000	300	400	2000
Data	20	20	20	20
TOTAL	**5700**	**990**	**1080**	**2470**

Source: Placeholder for Notes is 18 points

Cisco ISE Guest Server

Guest User Creation

1. Sponsor creates Guest Account through dedicated ISE server
2. Credentials are delivered to Guest by print, email or SMS
3. Guest Authentication on Guest portal
4. RADIUS Request from WLC to Cisco ISE Server
5. RADIUS Response with policies (session timeout, …)
6. RADIUS Accounting with session information (time, login, IP, MAC, …)
7. Traffic can go through



Lobby Ambassador

Employee Sponsor

ISE Guest Server

Lobby Ambassador Portal
Guest Account Database
Monitoring & reporting

Wireless LAN Controller

Policy Enforcement
Guest Web Portal

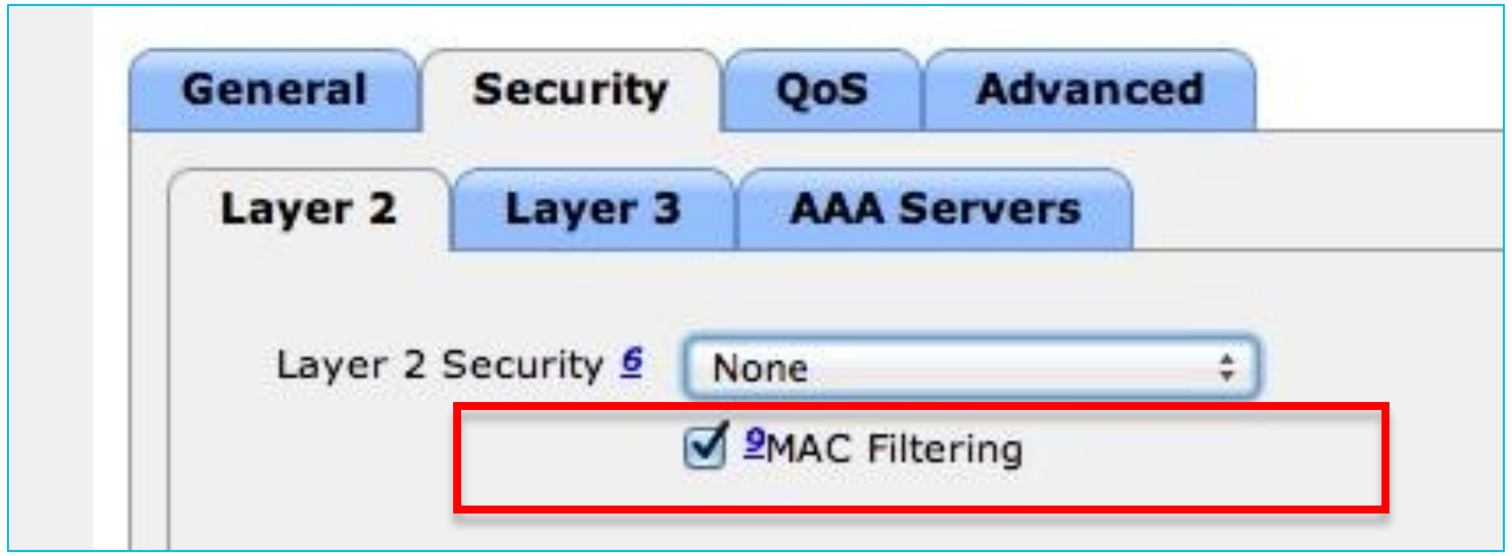
Guest

Visitor, Contractor, Customer

Web Auth and Guest Access

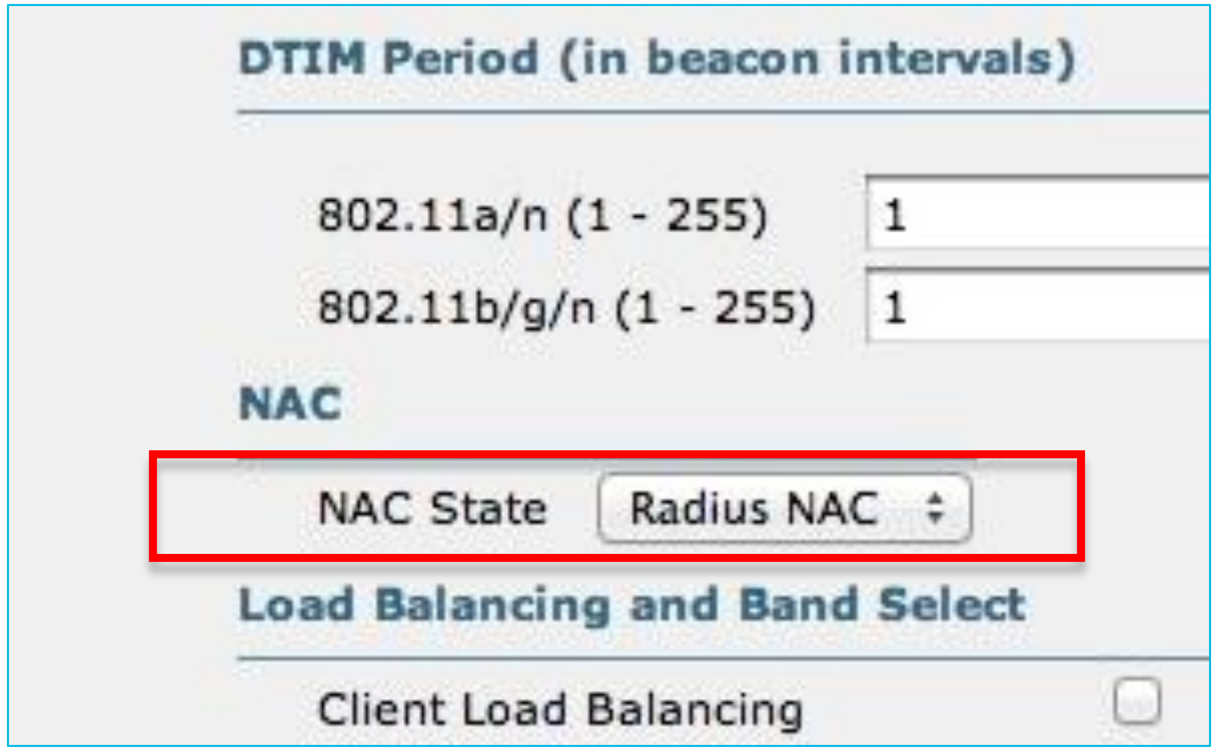
Wireless Considerations

- WLC 7.0 – Supports LWA; 7.2 adds CWA support
- ISE Guest Services requires account activation; Initial web auth must be against ISE guest portal (LWA or CWA). As a result…
  - Requires ISE be the web auth portal for LWA; No support for hosting guest portal on WLC
  - For anchor controller deployments, requires pinhole through DMZ firewall back to ISE PSN on tcp/8443 from guest IP address pool.



Layer 2 Security 6 None

☑ 9MAC Filtering



DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1

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

NAC

NAC State Radius NAC

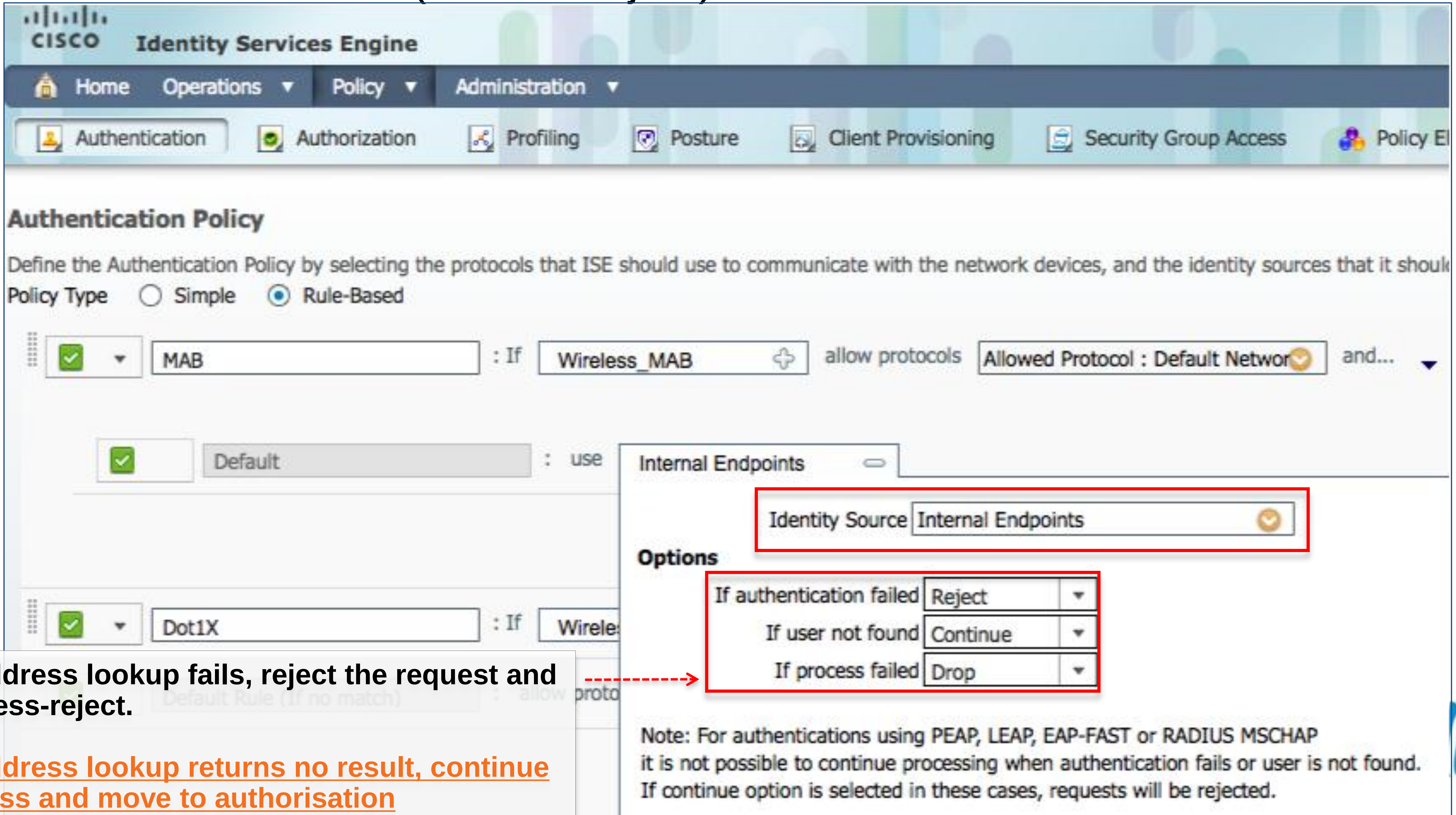
Load Balancing and Band Select

Client Load Balancing □

Web Auth and Guest Access

- LWA vs CWA piggybacks on MAB authentication policy rule. Configure:

  If User Not Found = Continue (default Reject)



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it shoul

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wireless_MAB allow protocols Allowed Protocol : Default Networ and...

☑ Default : use Internal Endpoints

Identity Source: Internal Endpoints

Options

If authentication failed: Reject

If user not found: Continue

If process failed: Drop

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.

☑ Dot1X : If Wirele

Default Rule (If no match) : allow proto

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 authorisation

URL Redirection

Central Web Auth, Client Provisioning, Posture

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

  Ex: cisco:cisco-av-pair=url-redirect= https://ip:8443/guestportal/gateway?sessionId=SessionIdValue&action=cwa

- **Redirect ACL:** Access devices must be locally configured with ACL that specifies traffic to be permitted (= redirected) or denied (= bypass redirection)

  ACL value returned as a named ACL on NAD

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

  ACL entries define traffic subject to redirection (permit) and traffic to bypass redirection (deny)

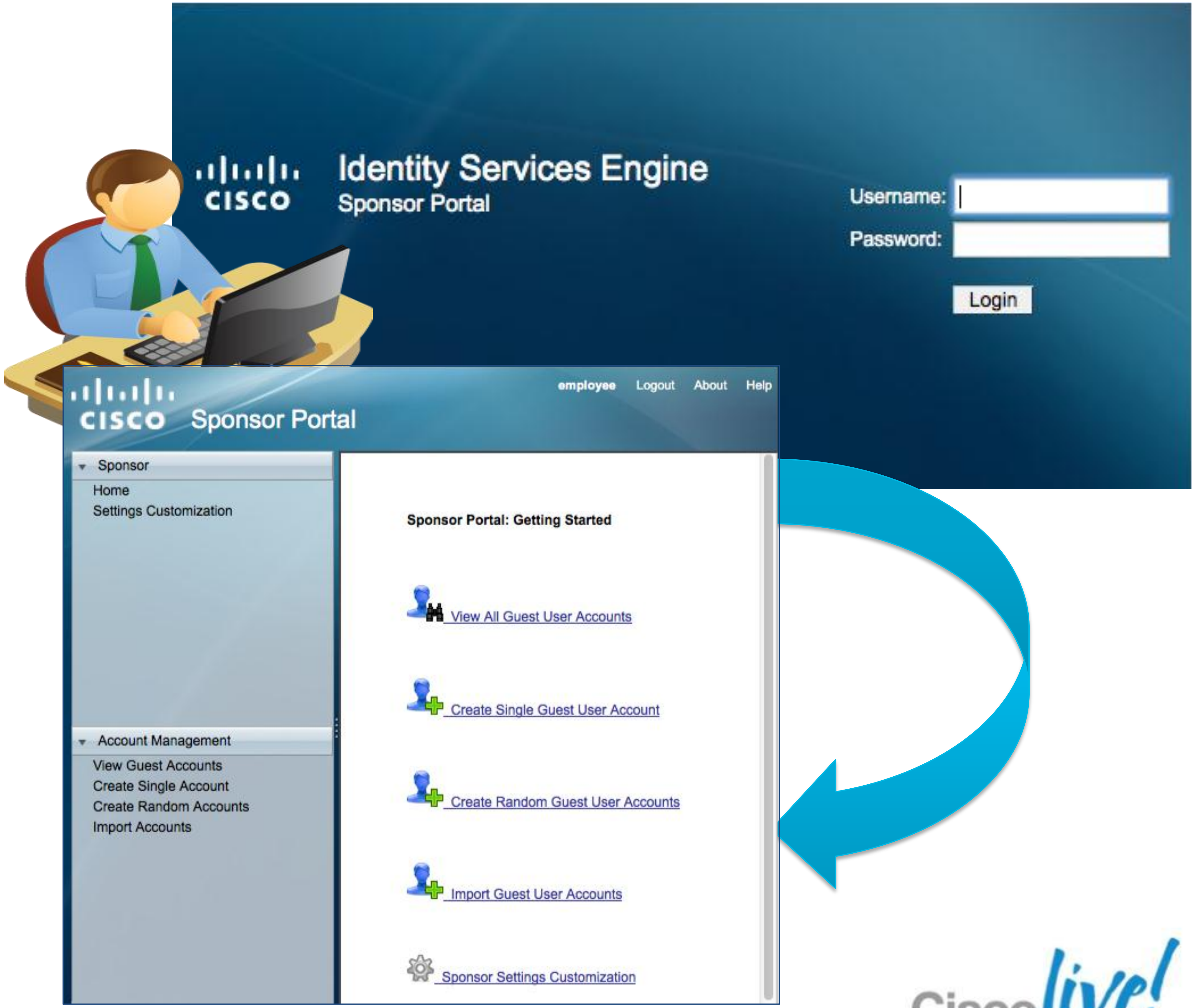
- **Port ACL:** ACL applied to the port (default ACL, dACL, named ACL) that defines traffic allowed through port prior to redirection

Common URLs for Redirection

- **URL Redirect for Central Web Auth**
  Cisco:cisco-av-pair=url-redirect=
  https://ip:8443/guestportal/gateway?sessionId=SessionIdValue&action=cwa
- **URL Redirect for Client Provisioning and Posture**
  Cisco:cisco-av-pair=url-redirect=
  https://ip:8443/guestportal/gateway?sessionId=SessionIdValue&action=cpp
- **URL Redirect ACL**
  Cisco:cisco-av-pair=url-redirect-acl=ACL-WEBAUTH-REDIRECT
- **LWA URL for Default ISE Guest Portal:**
  https://ip:8443/guestportal/portal.jsp
- **LWA URL for Custom ISE Guest Portal:**
  https://ip:8443/guestportal/portals/ClientPortalName/portal.jsp
- **CWA URL redirect for Custom ISE Guest Portal:**
  Cisco:cisco-av-pair=url-redirect=
  https://ip:8443/guestportal/gateway?portal=ClientPortalName&sessionId =SessionIdValue&action=cwa

ISE Sponsored Guests – Sponsor Portal

- Customisable Web Portal for Sponsors as well
- Authenticate Sponsors with corporate credentials
  - –Local Database
  - –Active Directory
  - –LDAP
  - –RADIUS
  - –Kerberos

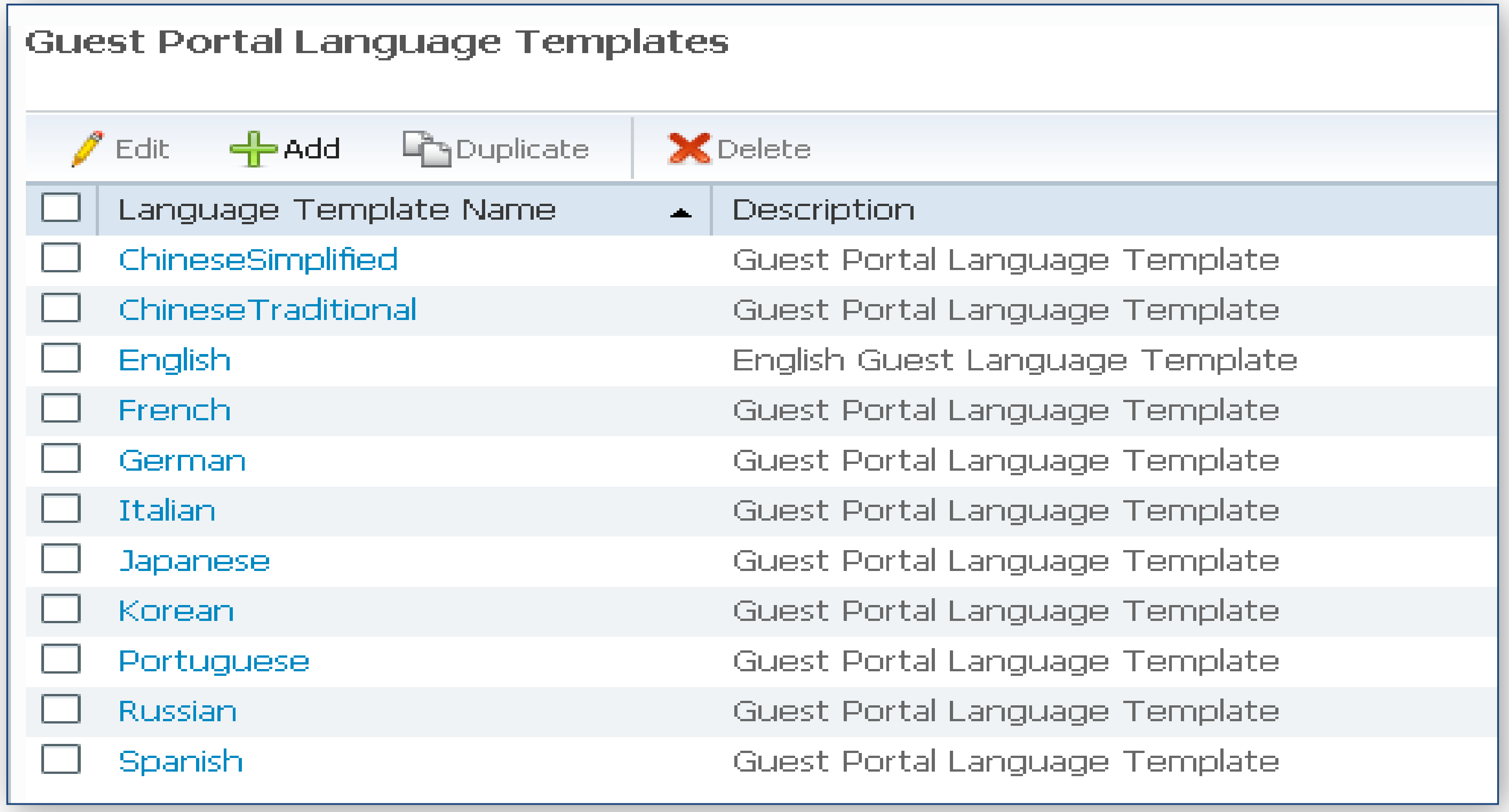


Guest Portal Localisation

Several Languages are Supported Natively in ISE 1.1

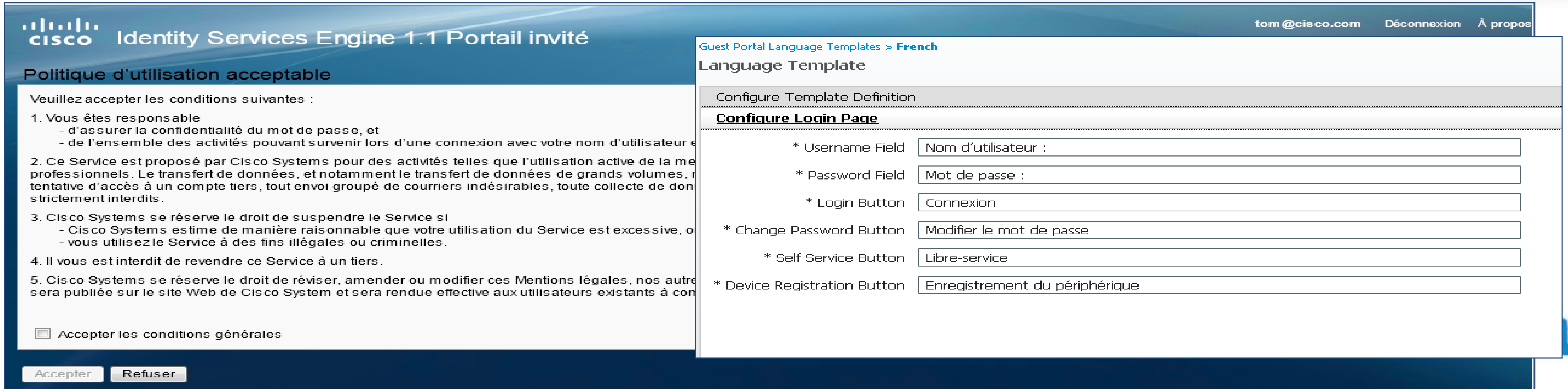
All guest user pages are translated:

- Authentication page
- Acceptable usage policy
- Success/failure page



Guest Portal Language Templates

□	Language Template Name	Description
□	ChineseSimplified	Guest Portal Language Template
□	ChineseTraditional	Guest Portal Language Template
□	English	English Guest Language Template
□	French	Guest Portal Language Template
□	German	Guest Portal Language Template
□	Italian	Guest Portal Language Template
□	Japanese	Guest Portal Language Template
□	Korean	Guest Portal Language Template
□	Portuguese	Guest Portal Language Template
□	Russian	Guest Portal Language Template
□	Spanish	Guest Portal Language Template



Politique d'utilisation acceptable

Veuillez accepter les conditions suivantes :

1. Vous êtes responsable
   - d'assurer la confidentialité du mot de passe, et
   - de l'ensemble des activités pouvant survenir lors d'une connexion avec votre nom d'utilisateur e

2. Ce Service est proposé par Cisco Systems pour des activités telles que l'utilisation active de la me professionnels. Le transfert de données, et notamment le transfert de données de grands volumes, tentative d'accès à un compte tiers, tout envoi groupé de courriers indésirables, toute collecte de don strictement interdits.

3. Cisco Systems se réserve le droit de suspendre le Service si
   - Cisco Systems estime de manière raisonnable que votre utilisation du Service est excessive, o
   - vous utilisez le Service à des fins illégales ou criminelles.

4. Il vous est interdit de revendre ce Service à un tiers.

5. Cisco Systems se réserve le droit de réviser, amender ou modifier ces Mentions légales, nos autre sera publiée sur le site Web de Cisco System et sera rendue effective aux utilisateurs existants à con

□ Accepter les conditions générales

Guest Portal Language Templates > **French**

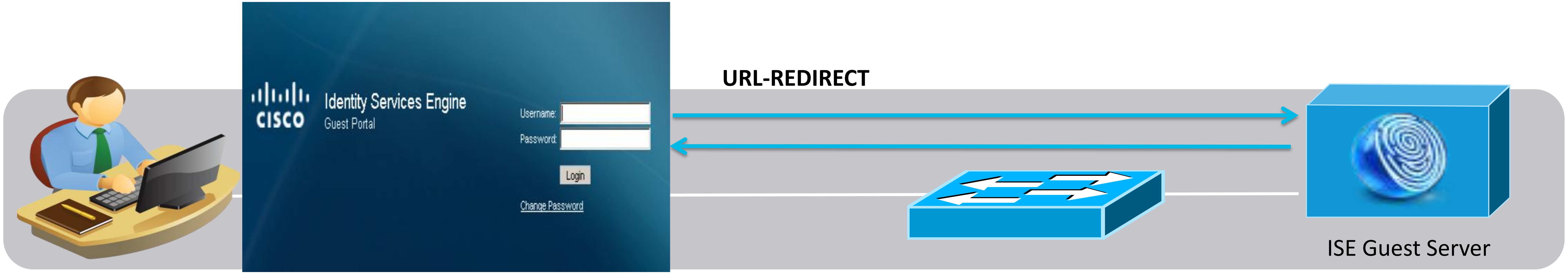
Language Template

Configure Template Definition

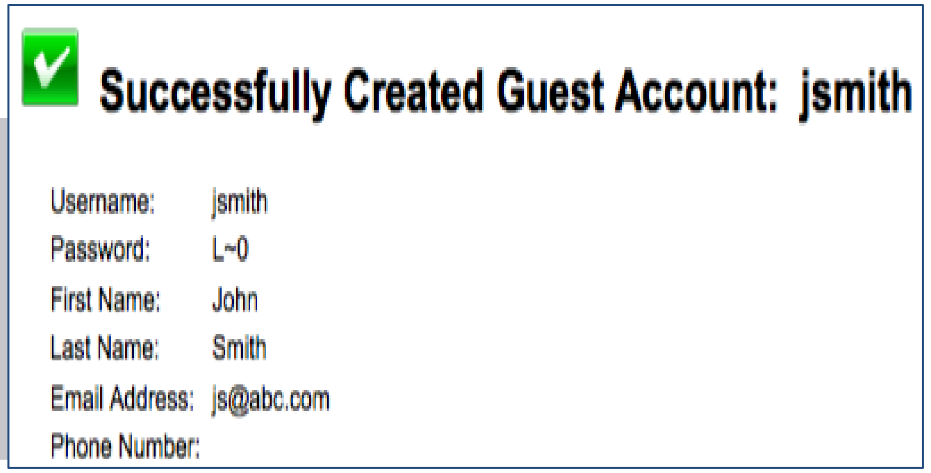
Configure Login Page

* 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

ISE Sponsored Guest



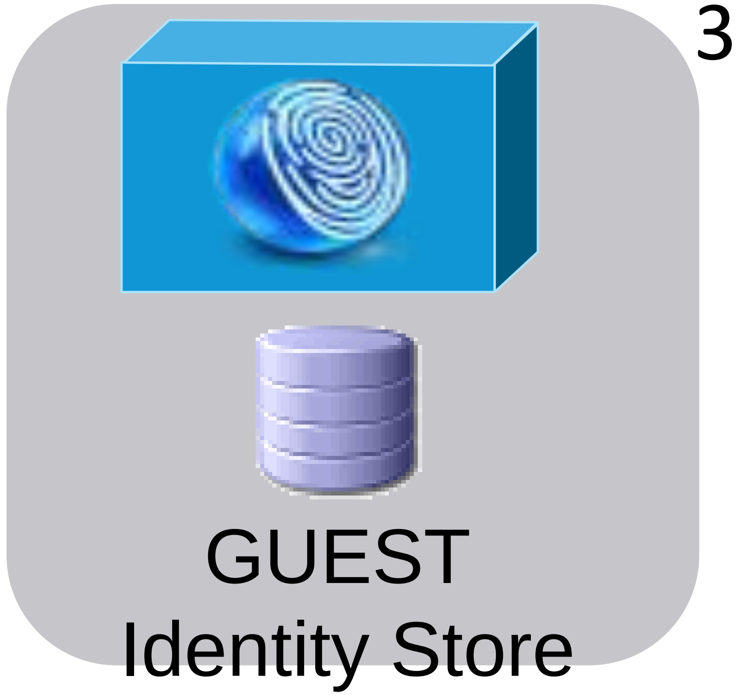
1. Guest is re-directed to the ISE Guest Portal when Browser is launched.



Successfully Created Guest Account: jsmith

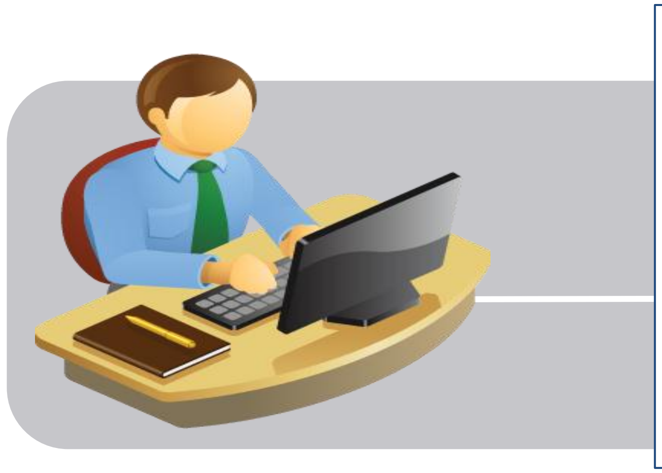
Username: jsmith
Password: L~0
First Name: John
Last Name: Smith
Email Address: js@abc.com
Phone Number:

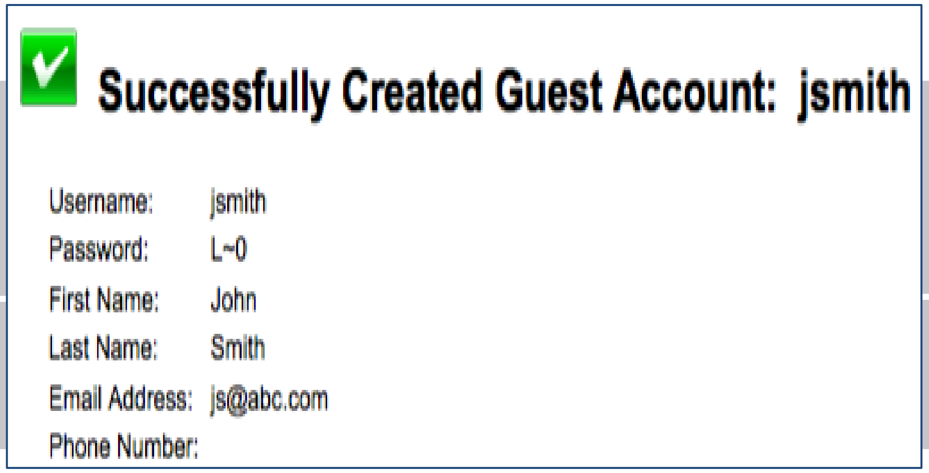
2. Guest enters the credentials created by the Sponsor



3. Account is verified on ISE decision point against the Guest User Identity Store

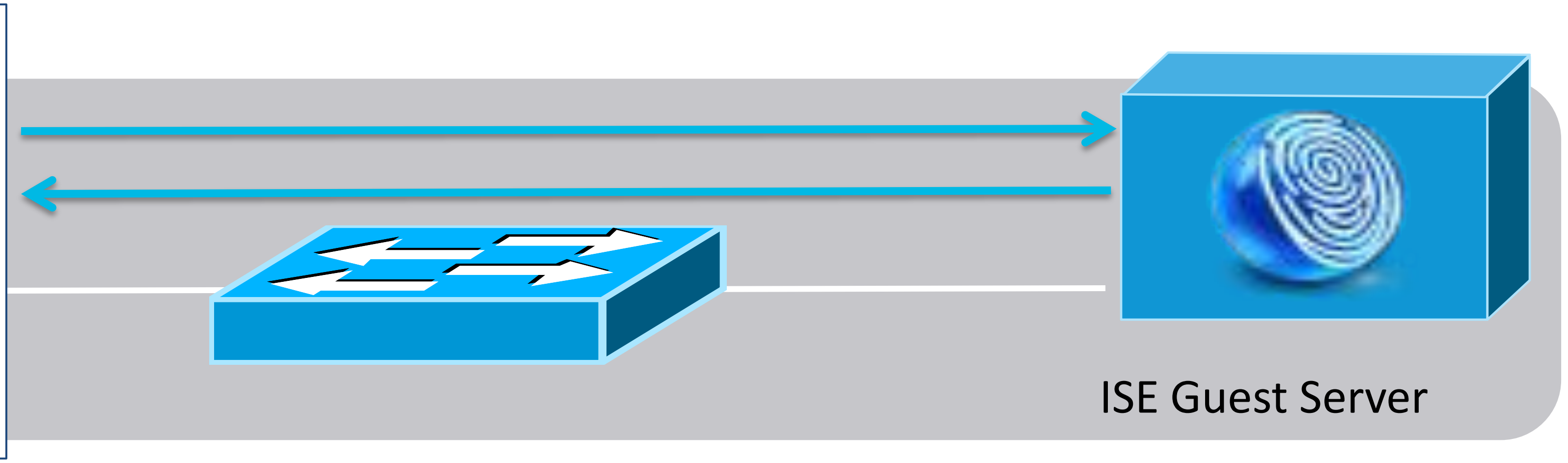
ISE Self-Registration



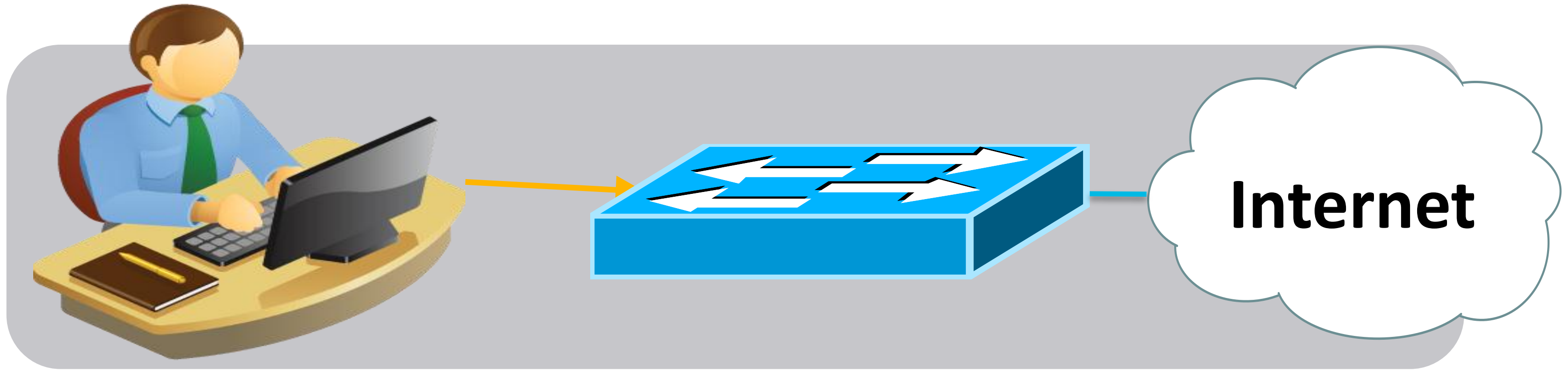


Successfully Created Guest Account: jsmith

Username: jsmith
Password: L~0
First Name: John
Last Name: Smith
Email Address: js@abc.com
Phone Number:



4. Guest is re-directed again to login again with auto generated username/ password.



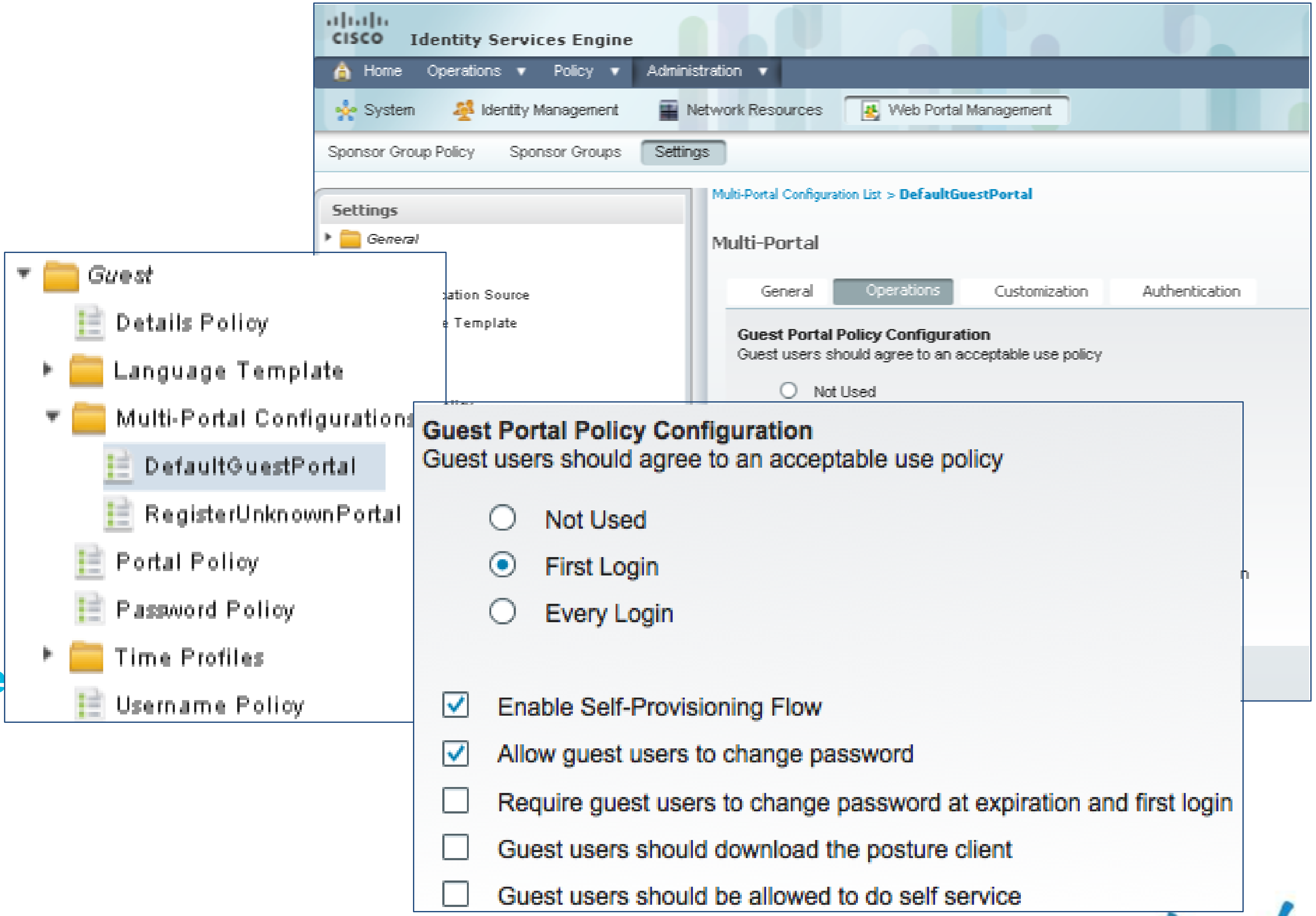
5. Guest is provisioned with Authorisation Policy for Web Access Only

GUEST
Identity Store

6. Account is monitored via the timed profile settings.

ISE Guest User Portal Settings

- Guest Portals define what Guests Users will be allowed to perform
  - Guests can **change password**
  - Guests **change password at first login**
  - Guests can be allowed to **download the posture client**
  - Guests can do **self service**
  - Guests can be allowed to do **device registration**



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

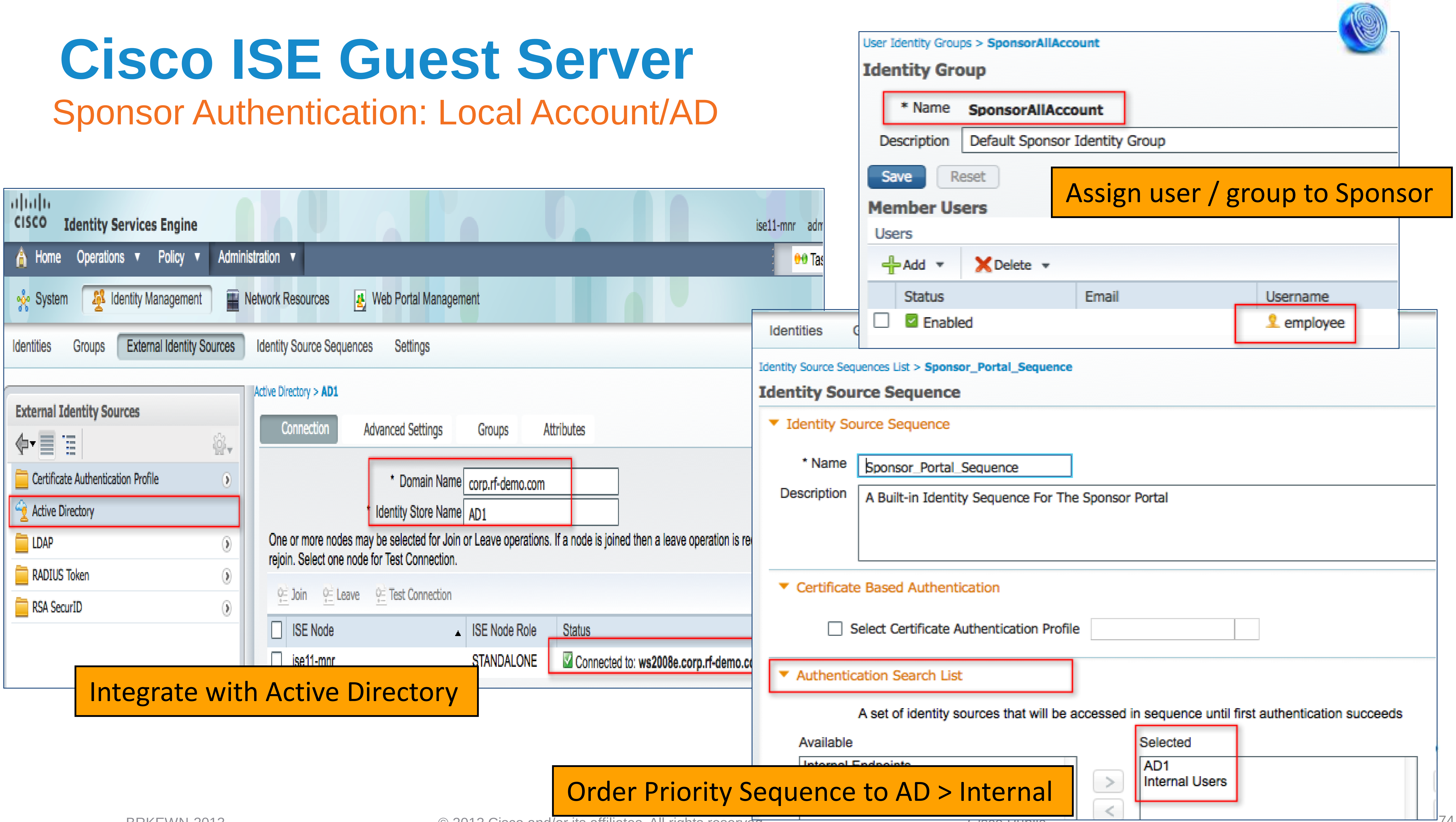
☐ Require guest users to change password at expiration and first login

☐ Guest users should download the posture client

☐ Guest users should be allowed to do self service

Cisco ISE Guest Server

Sponsor Authentication: Local Account/AD



Active Directory > AD1

* Domain Name corp.rf-demo.com

* Identity Store Name AD1

One or more nodes may be selected for Join or Leave operations. If a node is joined then a leave operation is re rejoin. Select one node for Test Connection.

□	ISE Node	ISE Node Role	Status
□	ise11-mnr	STANDALONE	☑ Connected to: ws2008e.corp.rf-demo.c

User Identity Groups > SponsorAllAccount

Identity Group

* Name SponsorAllAccount

Description Default Sponsor Identity Group

□	Status	Email	Username
□	☑ Enabled		employee

Identity Source Sequences List > Sponsor_Portal_Sequence

Identity Source Sequence

▾ Identity Source Sequence

* Name Sponsor_Portal_Sequence

Description A Built-in Identity Sequence For The Sponsor Portal

▾ 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: Internal Endpoints

Selected: AD1, Internal Users

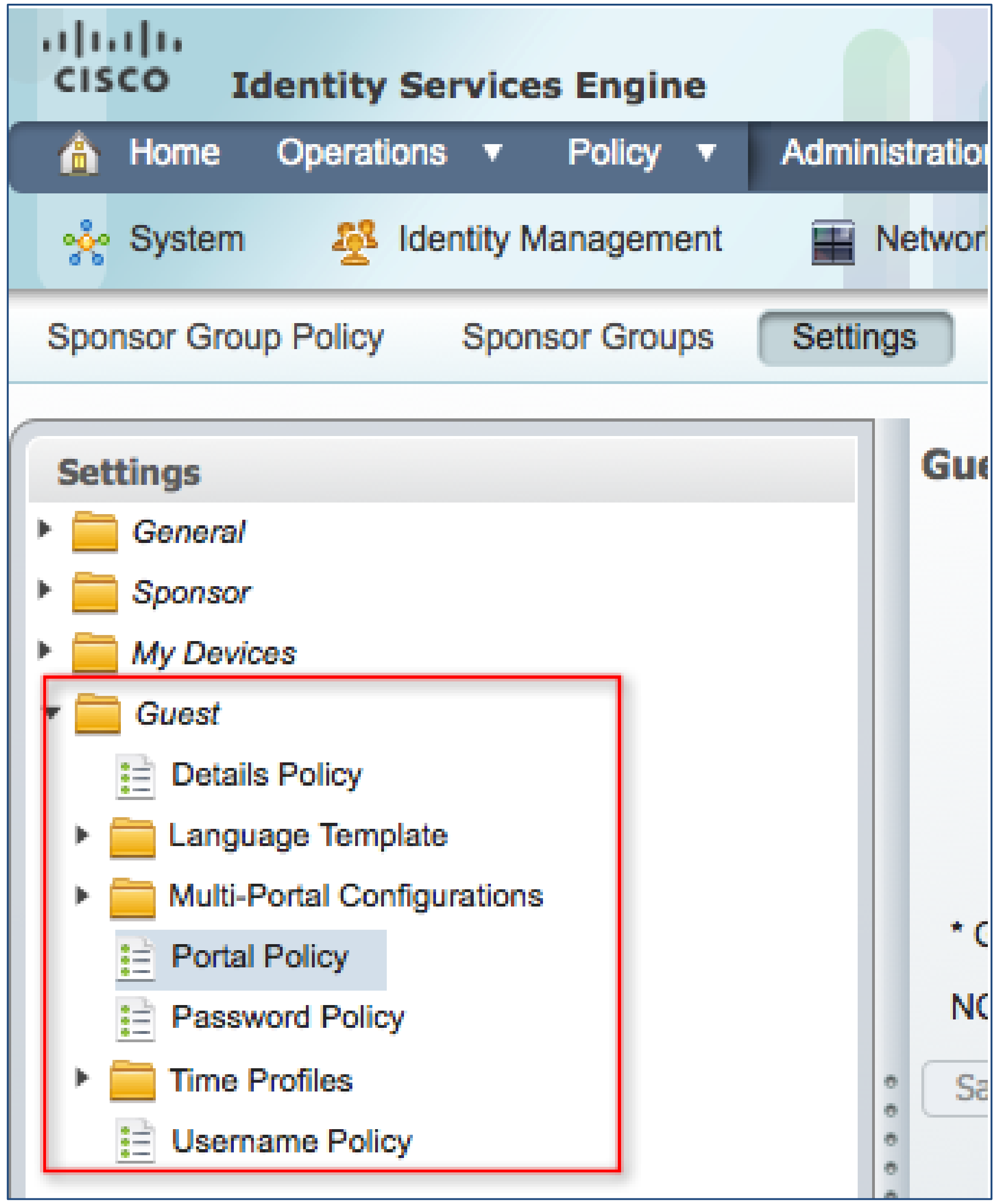
Assign user / group to Sponsor

Integrate with Active Directory

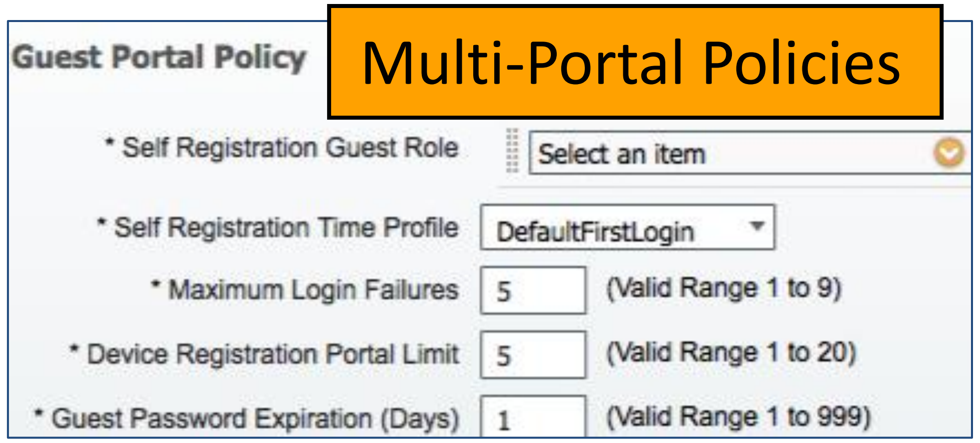
Order Priority Sequence to AD > Internal

Cisco ISE Guest Server

Guest Portal Customisation



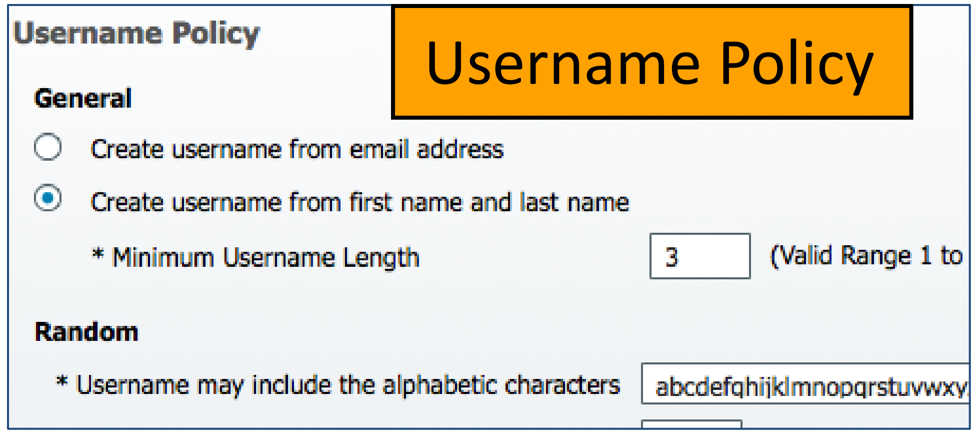
Settings
- General
- Sponsor
- My Devices
- Guest
  - Details Policy
  - Language Template
  - Multi-Portal Configurations
  - Portal Policy
  - Password Policy
  - Time Profiles
  - Username Policy



Multi-Portal Policies

Guest Portal Policy

* Self Registration Guest Role: Select an item
* Self Registration Time Profile: DefaultFirstLogin
* Maximum Login Failures: 5 (Valid Range 1 to 9)
* Device Registration Portal Limit: 5 (Valid Range 1 to 20)
* Guest Password Expiration (Days): 1 (Valid Range 1 to 999)



Username Policy

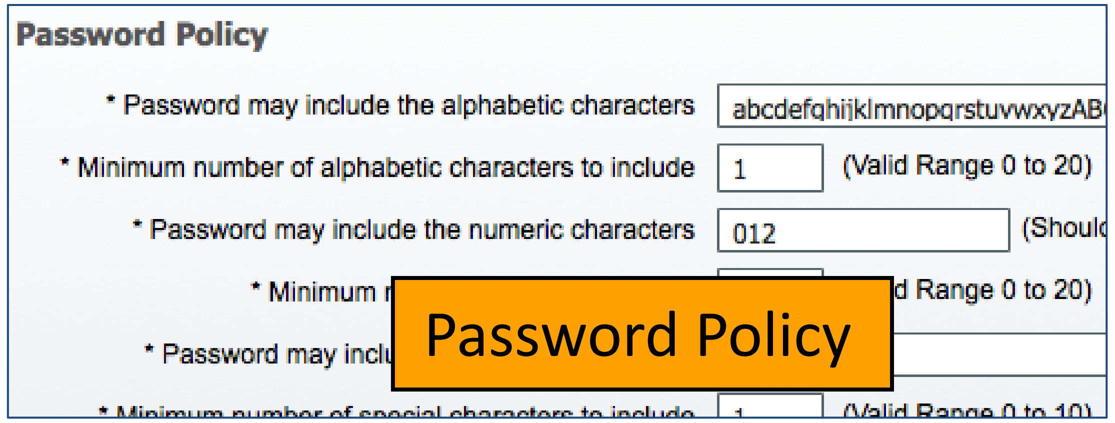
Username Policy

General

○ Create username from email address
● Create username from first name and last name
* Minimum Username Length: 3 (Valid Range 1 to

Random

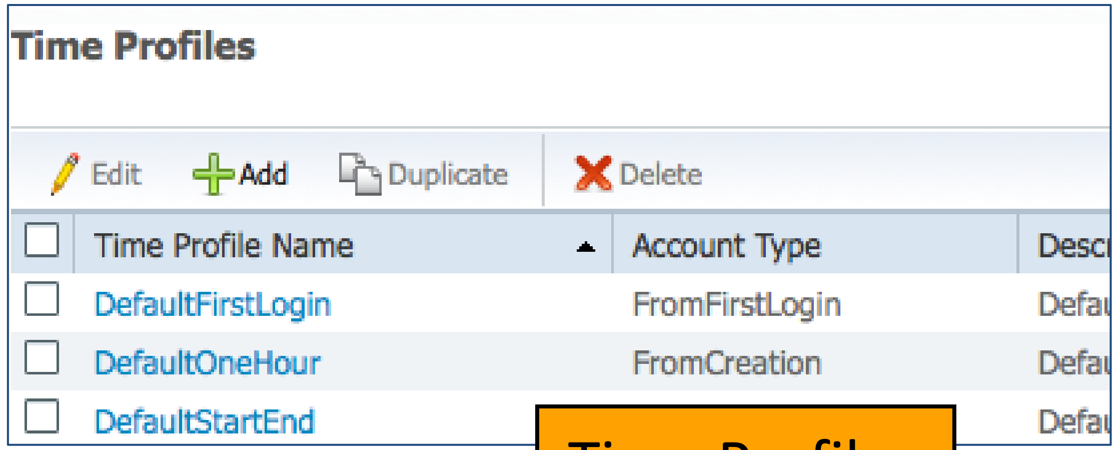
* Username may include the alphabetic characters: abcdefghijklmnopqrstuvwxy



Password Policy

* Password may include the alphabetic characters: abcdefghijklmnopqrstuvwxyzAB
* Minimum number of alphabetic characters to include: 1 (Valid Range 0 to 20)
* Password may include the numeric characters: 012 (Shoul
* Minimum r d Range 0 to 20)
* Password may incl
* Minimum number of special characters to include: 1 (Valid Range 0 to 10)

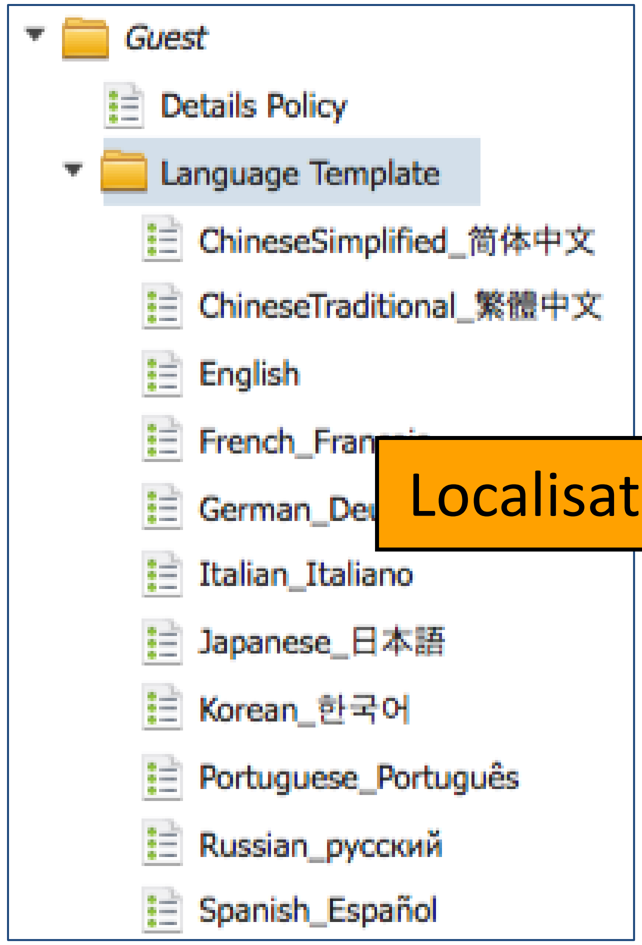
Password Policy



Time Profiles

☐	Time Profile Name ▲	Account Type	Desc
☐	DefaultFirstLogin	FromFirstLogin	Defa
☐	DefaultOneHour	FromCreation	Defa
☐	DefaultStartEnd		Defa

Time Profiles



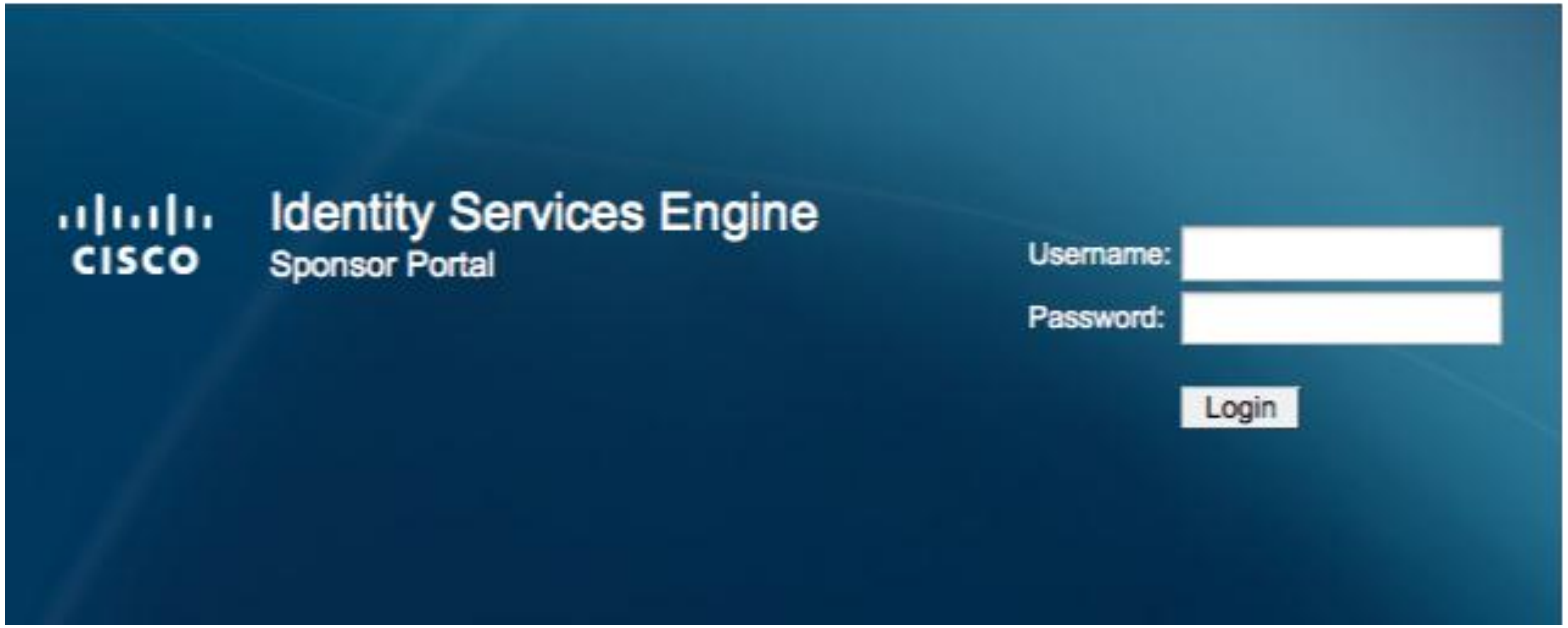
- Guest
  - Details Policy
  - Language Template
    - ChineseSimplified_简体中文
    - ChineseTraditional_繁體中文
    - English
    - French_Fran
    - German_De
    - Italian_Italiano
    - Japanese_日本語
    - Korean_한국어
    - Portuguese_Português
    - Russian_русский
    - Spanish_Español

Localisation

Cisco ISE Guest Server

Sponsor Portal

- https://<ise-server-ip>:8443/sponsorportal/



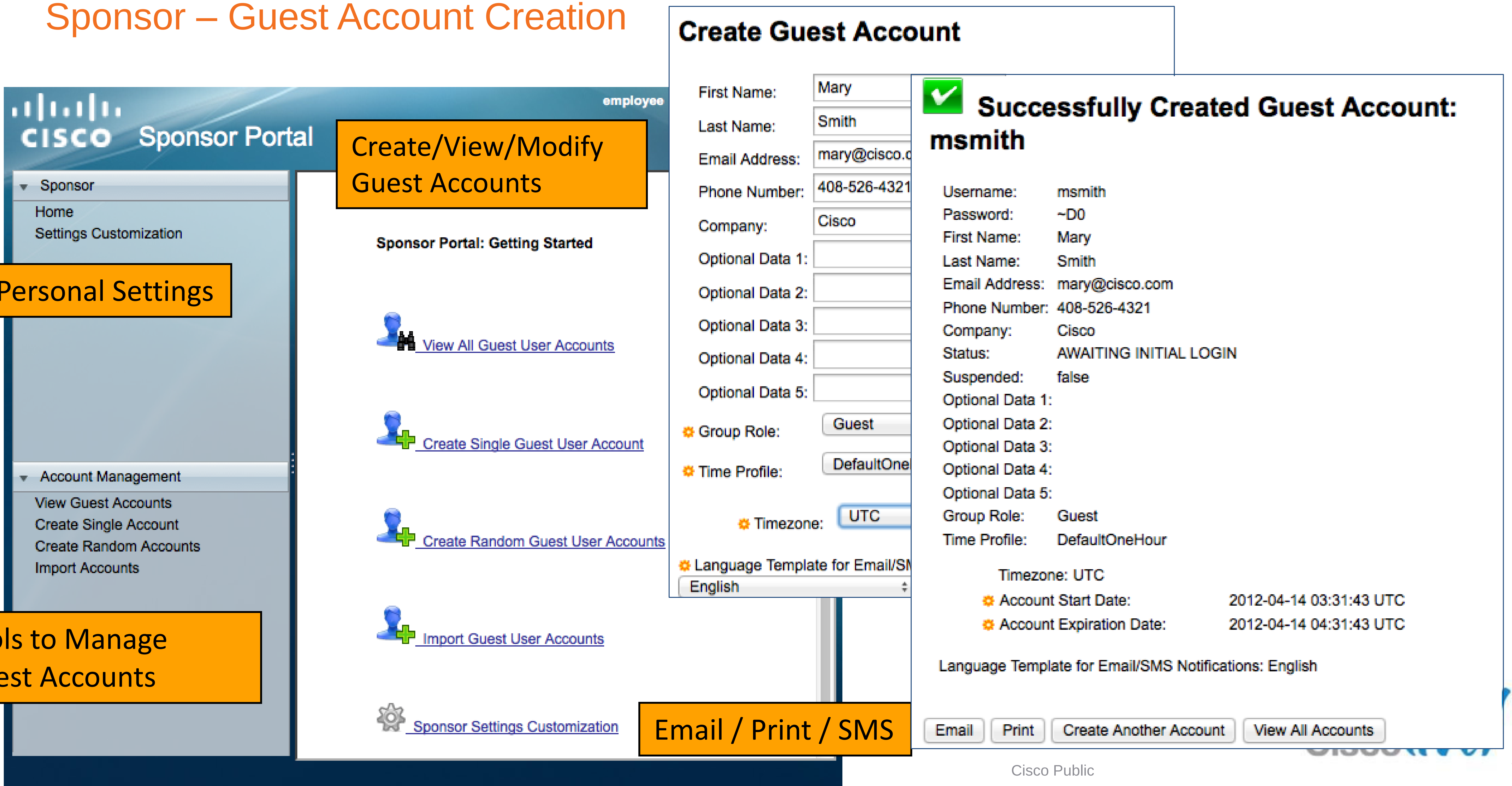
Identity Services Engine
Sponsor Portal

Username:

Password:

Cisco ISE Guest Server

Sponsor – Guest Account Creation



Create/View/Modify Guest Accounts

Personal Settings

Tools to Manage Guest Accounts

Email / Print / SMS

Create Guest Account

First Name:	Mary
Last Name:	Smith
Email Address:	mary@cisco.c
Phone Number:	408-526-4321
Company:	Cisco
Optional Data 1:	
Optional Data 2:	
Optional Data 3:	
Optional Data 4:	
Optional Data 5:	
Group Role:	Guest
Time Profile:	DefaultOne
Timezone:	UTC

Language Template for Email/SM

English

Successfully Created Guest Account: msmith

Username:	msmith
Password:	~D0
First Name:	Mary
Last Name:	Smith
Email Address:	mary@cisco.com
Phone Number:	408-526-4321
Company:	Cisco
Status:	AWAITING INITIAL LOGIN
Suspended:	false
Optional Data 1:	
Optional Data 2:	
Optional Data 3:	
Optional Data 4:	
Optional Data 5:	
Group Role:	Guest
Time Profile:	DefaultOneHour

Timezone: UTC

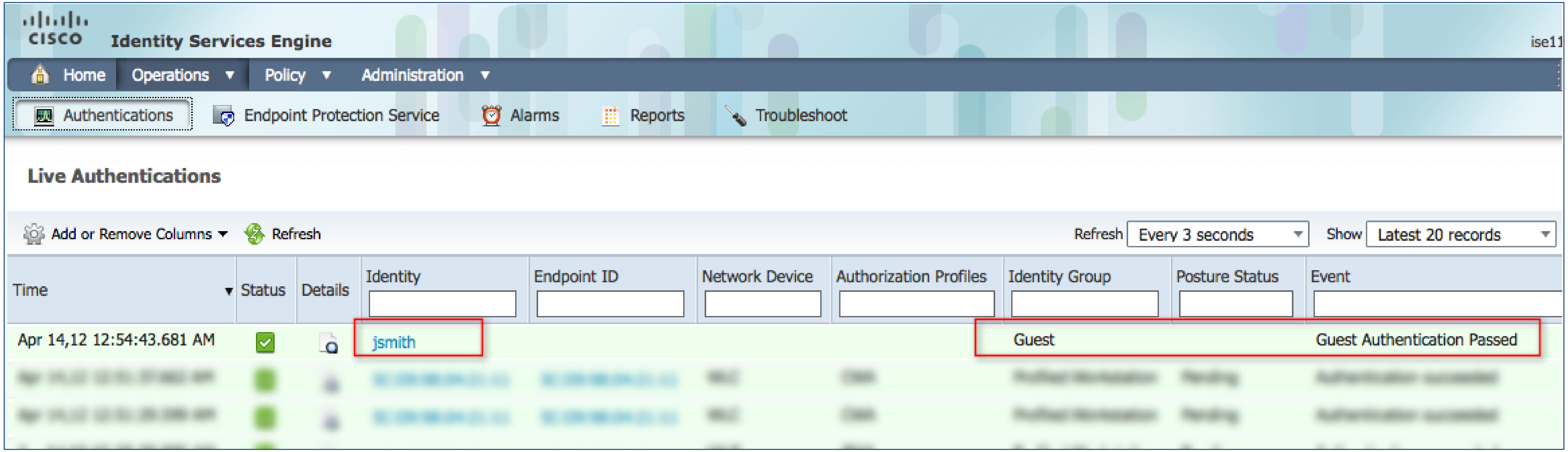
Account Start Date:	2012-04-14 03:31:43 UTC
Account Expiration Date:	2012-04-14 04:31:43 UTC

Language Template for Email/SMS Notifications: English

Guest Monitoring, Reporting and Troubleshooting

Live Guest Verification - ISE

- **Monitor > Operations > Authentications** window will show all Authentications including Guests
- Identity and Authorisation can be found for Guests



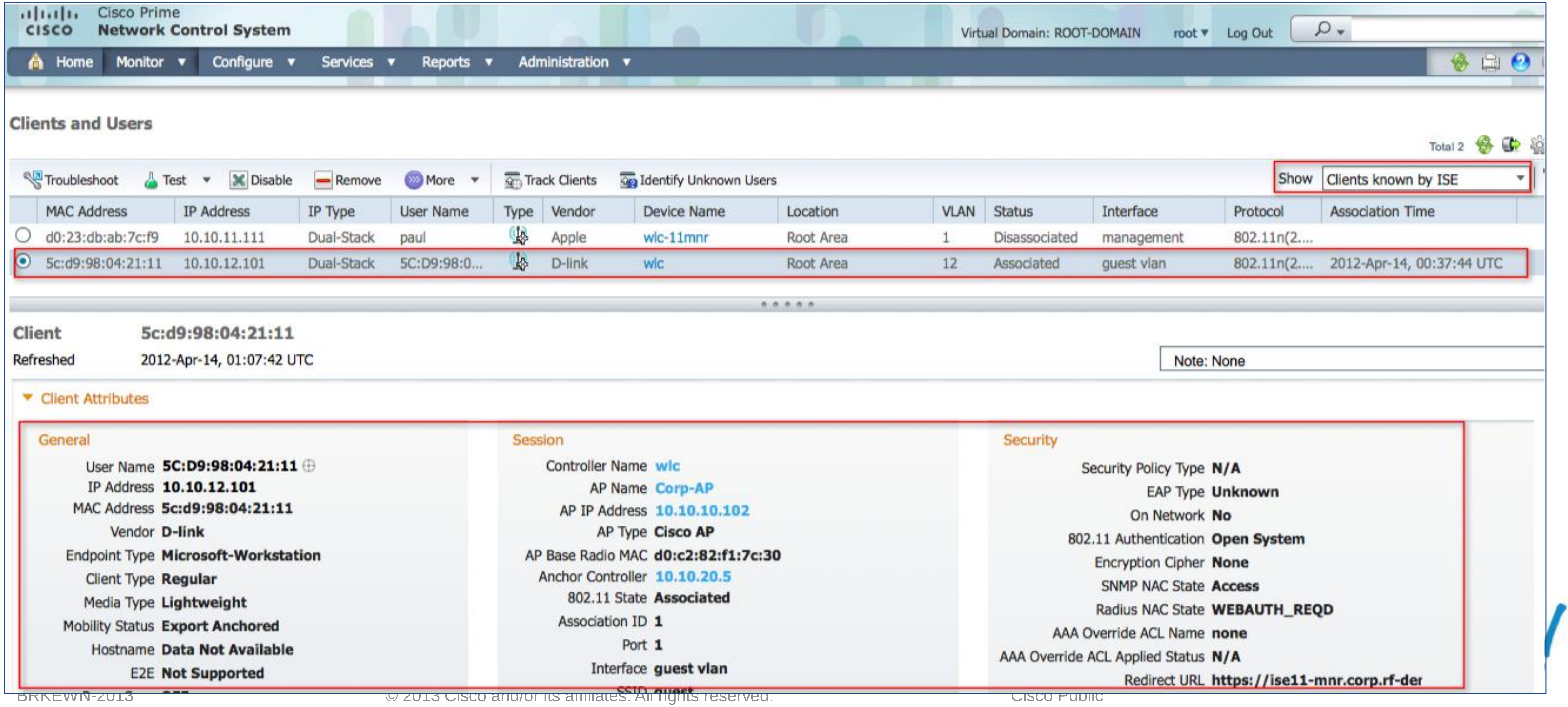
Live Authentications

Refresh: Every 3 seconds
Show: Latest 20 records

Time	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Apr 14,12 12:54:43.681 AM	✓		jsmith				Guest		Guest Authentication Passed
[illegible]			[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]			[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Guest Monitoring - NCS

- **Monitor > Clients and Users** window will show all Authentications including Guests
- Identity and Authorisation can be found for Guests



Clients and Users

Total 2

Show: Clients known by ISE

	MAC Address	IP Address	IP Type	User Name	Type	Vendor	Device Name	Location	VLAN	Status	Interface	Protocol	Association Time
○	d0:23:db:ab:7c:f9	10.10.11.111	Dual-Stack	paul		Apple	wlc-11mnr	Root Area	1	Disassociated	management	802.11n(2....	
●	5c:d9:98:04:21:11	10.10.12.101	Dual-Stack	5C:D9:98:0...		D-link	wlc	Root Area	12	Associated	guest vlan	802.11n(2....	2012-Apr-14, 00:37:44 UTC

Client 5c:d9:98:04:21:11

Refreshed 2012-Apr-14, 01:07:42 UTC

Note: None

Client Attributes

General

User Name	5C:D9:98:04:21:11
IP Address	10.10.12.101
MAC Address	5c:d9:98:04:21:11
Vendor	D-link
Endpoint Type	Microsoft-Workstation
Client Type	Regular
Media Type	Lightweight
Mobility Status	Export Anchored
Hostname	Data Not Available
E2E	Not Supported

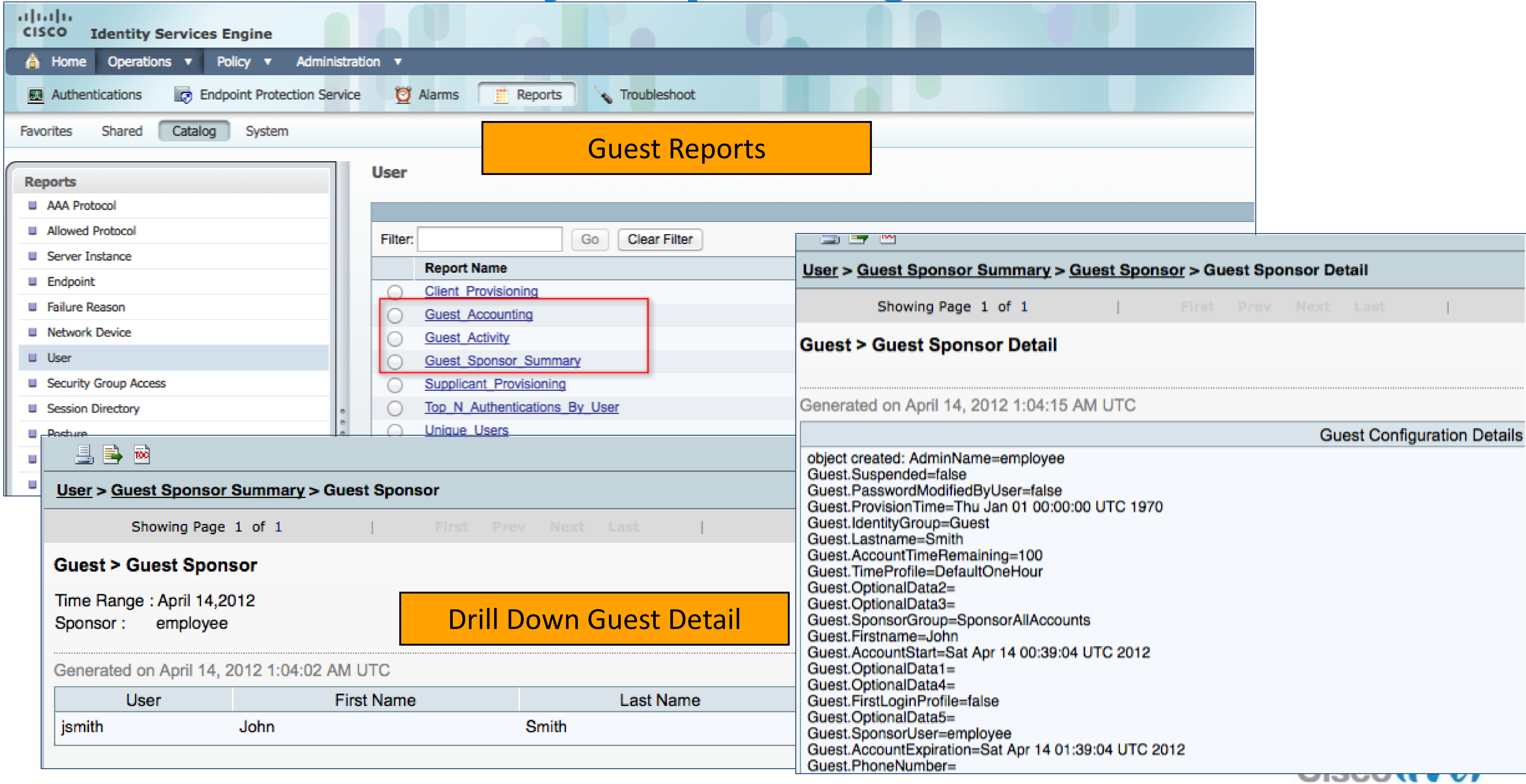
Session

Controller Name	wlc
AP Name	Corp-AP
AP IP Address	10.10.10.102
AP Type	Cisco AP
AP Base Radio MAC	d0:c2:82:f1:7c:30
Anchor Controller	10.10.20.5
802.11 State	Associated
Association ID	1
Port	1
Interface	guest vlan
SSID	guest

Security

Security Policy Type	N/A
EAP Type	Unknown
On Network	No
802.11 Authentication	Open System
Encryption Cipher	None
SNMP NAC State	Access
Radius NAC State	WEBAUTH_REQD
AAA Override ACL Name	none
AAA Override ACL Applied Status	N/A
Redirect URL	https://ise11-mnr.corp.rf-der

Guest Activity Reporting - ISE



Guest Reports

Reports

- AAA Protocol
- Allowed Protocol
- Server Instance
- Endpoint
- Failure Reason
- Network Device
- User
- Security Group Access
- Session Directory
- Posture

User

	Report Name
○	Client_Provisioning
○	Guest_Accounting
○	Guest_Activity
○	Guest_Sponsor_Summary
○	Supplicant_Provisioning
○	Top_N_Authentications_By_User
○	Unique_Users

User > Guest Sponsor Summary > Guest Sponsor

Showing Page 1 of 1

Guest > Guest Sponsor

Time Range : April 14,2012
Sponsor : employee

Drill Down Guest Detail

Generated on April 14, 2012 1:04:02 AM UTC

User	First Name	Last Name
jsmith	John	Smith

User > Guest Sponsor Summary > Guest Sponsor > Guest Sponsor Detail

Showing Page 1 of 1

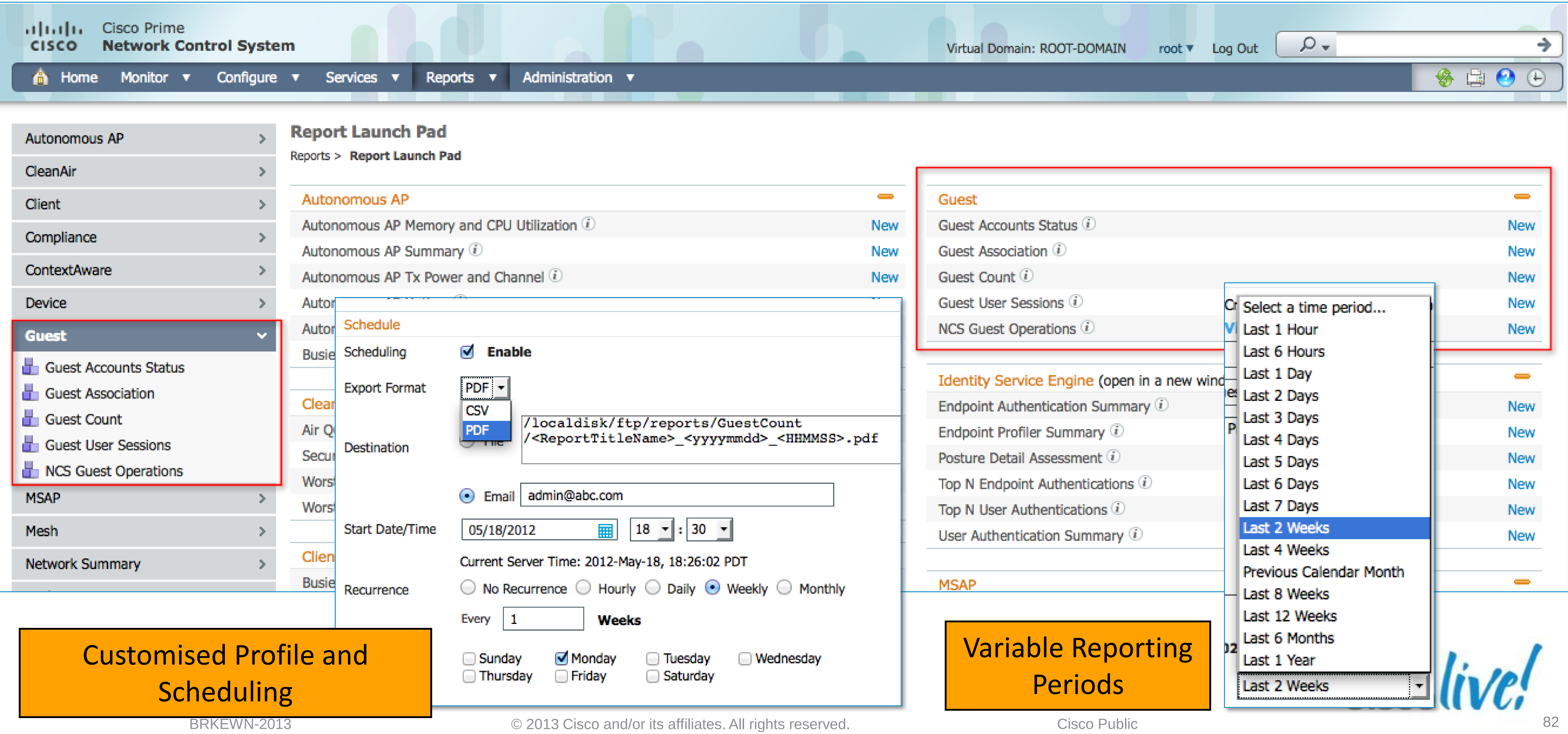
Guest > Guest Sponsor Detail

Generated on April 14, 2012 1:04:15 AM UTC

Guest Configuration Details

```
object created: AdminName=employee
Guest.Suspended=false
Guest.PasswordModifiedByUser=false
Guest.ProvisionTime=Thu Jan 01 00:00:00 UTC 1970
Guest.IdentityGroup=Guest
Guest.Lastname=Smith
Guest.AccountTimeRemaining=100
Guest.TimeProfile=DefaultOneHour
Guest.OptionalData2=
Guest.OptionalData3=
Guest.SponsorGroup=SponsorAllAccounts
Guest.Firstname=John
Guest.AccountStart=Sat Apr 14 00:39:04 UTC 2012
Guest.OptionalData1=
Guest.OptionalData4=
Guest.FirstLoginProfile=false
Guest.OptionalData5=
Guest.SponsorUser=employee
Guest.AccountExpiration=Sat Apr 14 01:39:04 UTC 2012
Guest.PhoneNumber=
```

Guest Activity Reporting - NCS



Report Launch Pad

Reports > **Report Launch Pad**

Autonomous AP	
Autonomous AP Memory and CPU Utilization ⓘ	New
Autonomous AP Summary ⓘ	New
Autonomous AP Tx Power and Channel ⓘ	New

Guest	
Guest Accounts Status ⓘ	New
Guest Association ⓘ	New
Guest Count ⓘ	New
Guest User Sessions ⓘ	New
NCS Guest Operations ⓘ	New

Identity Service Engine (open in a new wind	
Endpoint Authentication Summary ⓘ	New
Endpoint Profiler Summary ⓘ	New
Posture Detail Assessment ⓘ	New
Top N Endpoint Authentications ⓘ	New
Top N User Authentications ⓘ	New
User Authentication Summary ⓘ	New

MSAP

Schedule

Scheduling ☑ **Enable**

Export Format: PDF ▾ (CSV / PDF)

Destination: File /localdisk/ftp/reports/GuestCount /<ReportTitleName>_<yyyymmdd>_<HHMMSS>.pdf

● Email admin@abc.com

Start Date/Time: 05/18/2012 18 : 30

Current Server Time: 2012-May-18, 18:26:02 PDT

Recurrence: ○ No Recurrence ○ Hourly ○ Daily ● Weekly ○ Monthly

Every 1 **Weeks**

☐ Sunday ☑ Monday ☐ Tuesday ☐ Wednesday
☐ Thursday ☐ Friday ☐ Saturday

Customised Profile and Scheduling

Variable Reporting Periods

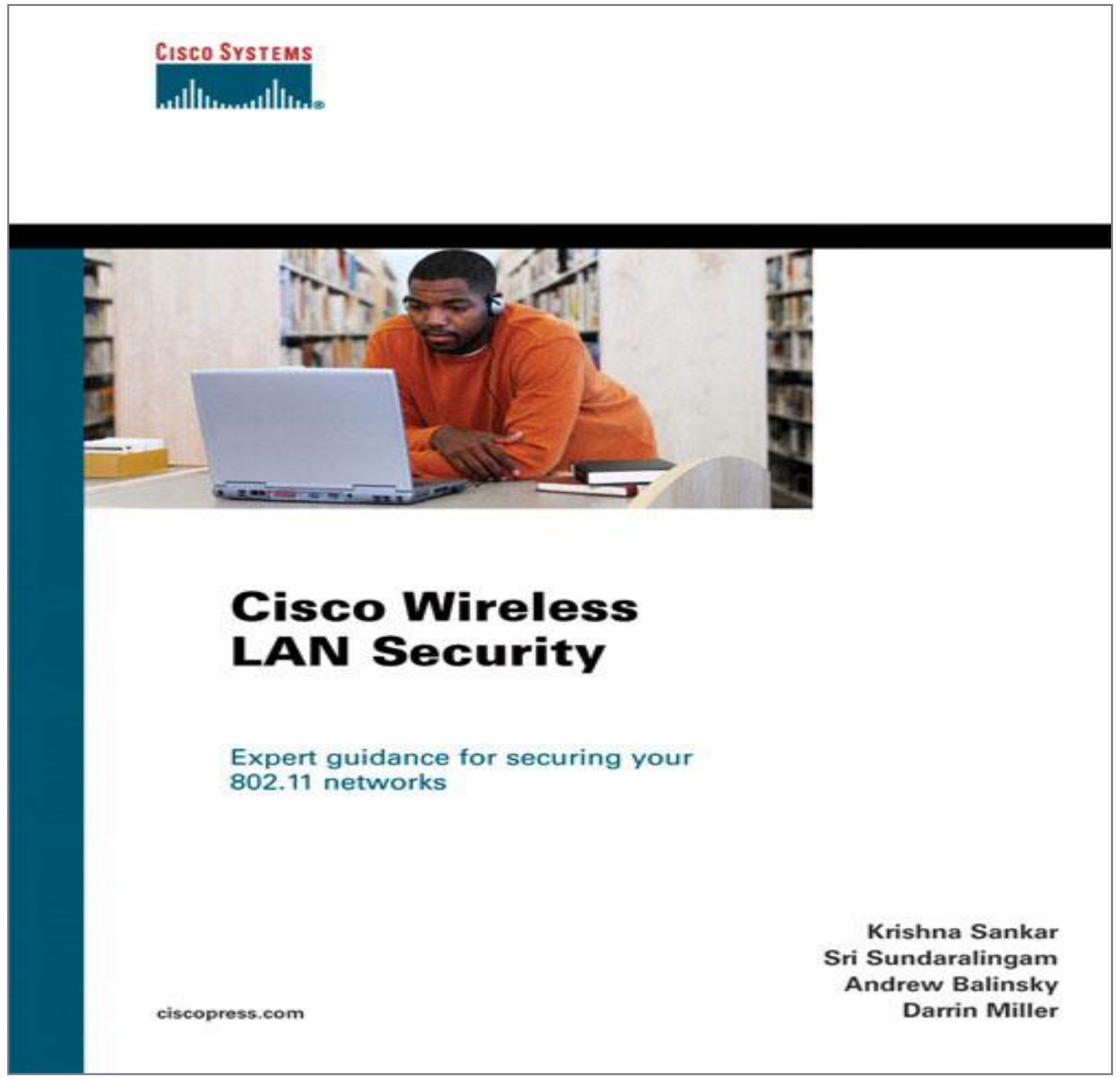
Summary

What We Have Covered…

- What Guest Access Services are made of.
- The need for a secured infrastructure to support isolated Guest traffic.
- Unified Wireless is a key component of this infrastructure.
- The Guest Service components are integrated in Cisco Wired and Wireless Solution.
- Securing FlexConnect is simple to understand and configure.
- Guest Access is one of the User Access Policy available to Control and Protect enterprise Borderless Network
- Cisco TrustSec enhances Guest Services overall.

BRKEWN-2013

Recommended Reading



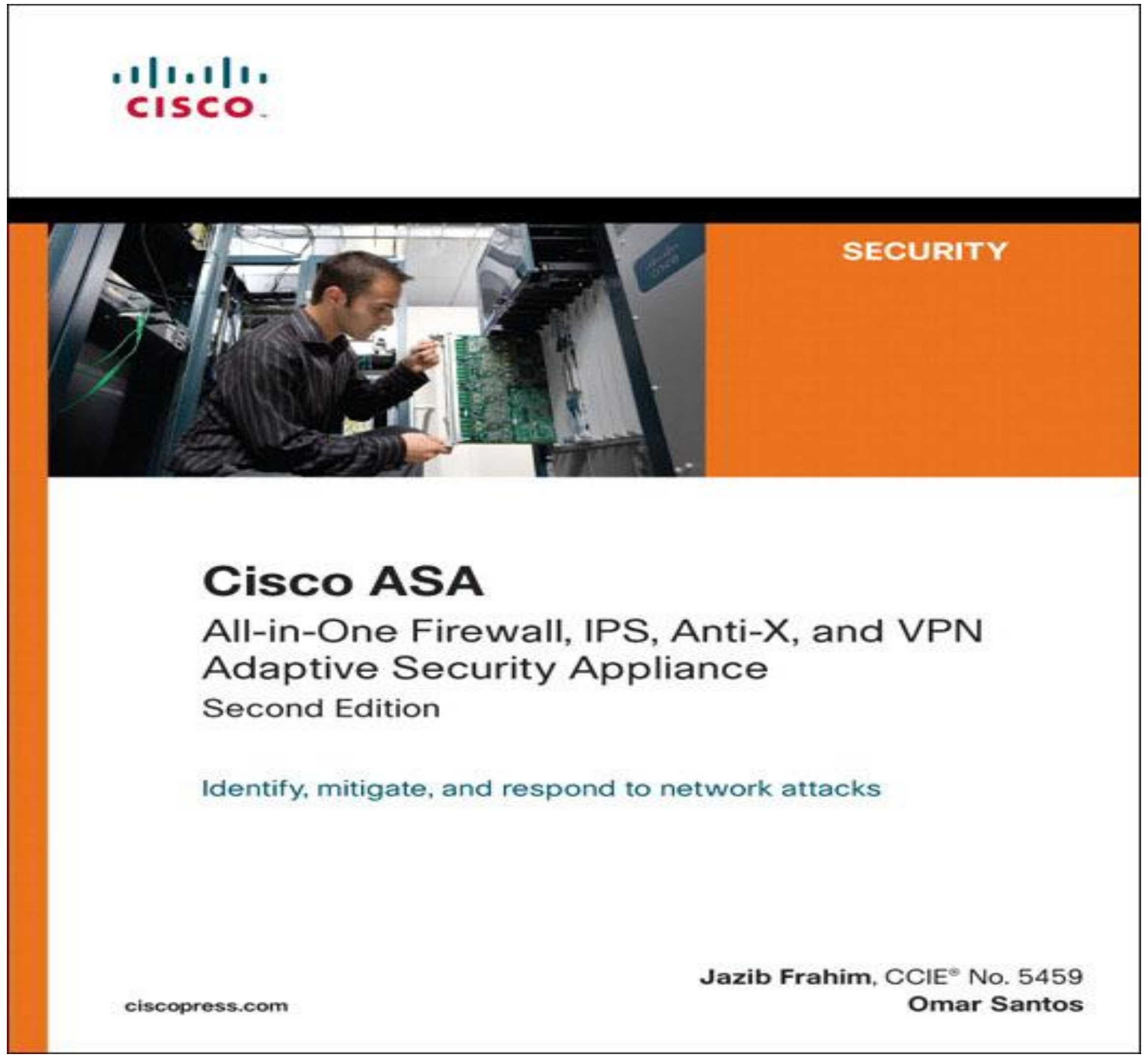
Cisco Systems

Cisco Wireless LAN Security

Expert guidance for securing your 802.11 networks

Krishna Sankar
Sri Sundaralingam
Andrew Balinsky
Darrin Miller

ciscopress.com



cisco

SECURITY

Cisco ASA

All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance

Second Edition

Identify, mitigate, and respond to network attacks

Jazib Frahim, CCIE® No. 5459
Omar Santos

ciscopress.com

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm

Cisco live! 365

Don’t forget to activate your Cisco Live 365 account for access to all session material, communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.
www.ciscoliveaustralia.com/portal/login.ww