

ISE and Location-Based Web Authentication Portals

An ISE Configuration Guide by Craig Hyps and Jason Kunst

This guide reviews multiple options for assigning network location and the basic configuration steps necessary to display a different Identity Services Engine (ISE) web authentication portal based on the location a user is accessing the network.

ISE 1.2 provides a default web authentication portal with a customizable portal theme. The portal theme allows an administrator to change logos, page and banner background images, and general color schemes. This theme applies to all web authentication portals using the default scheme. Language templates can be modified to customize the text displayed using the portal theme.

The default portal is often suitable for customers that require only a single portal for all web authenticated users regardless of location. However, many customers may require a unique web portal that offers customized web pages and language based on user location. Since the initial login page is displayed prior to validating the user's identity, ISE must leverage additional details presented during the authentication and authorization phases to determine location.

Location can be associated to many different RADIUS attributes communicated to ISE when a user connects to the network. One method to define location is to match the network access device (NAD) to which a user connects, for example, the Device-IP-Address or the NAS-IP-Address. It is even possible to match specific wired switchports using the NAS-Port-Id attribute. This may be necessary in few exceptions, but the most common method used to define network location is to group multiple network devices into Network Device Groups (NDGs) based on Location. See Figure 1 for sample Network Device Groups based on Location.

Figure 1 – Network Device Groups – Location

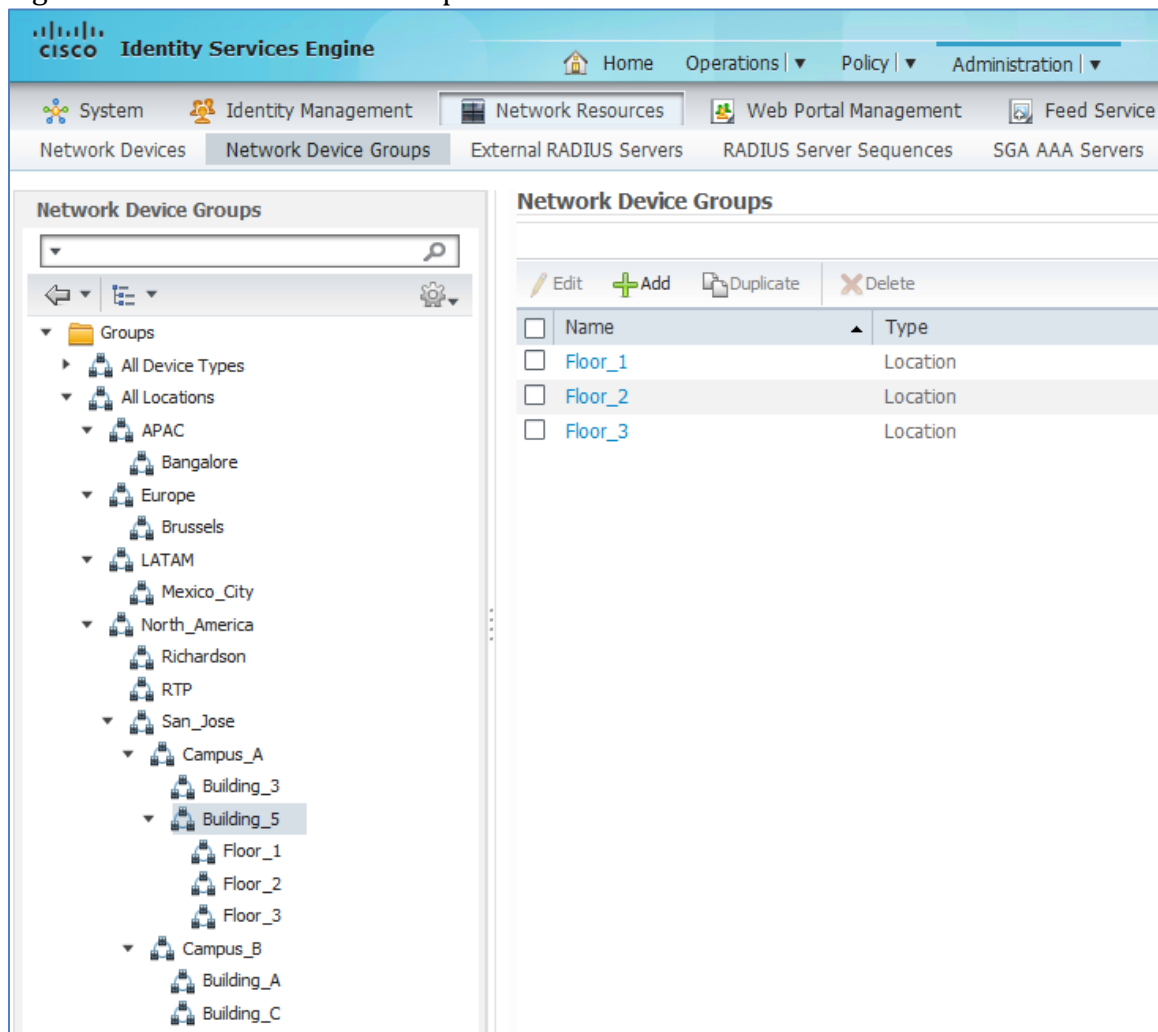


Figure 2 shows an example condition that matches NDG Location. Note the use of the EQUALS operator to match a specific child location. To match locations based on a parent container, use the CONTAINS operator.

Figure 2 – Example Authorization Policy Rule to Match NDG Location

Authorization Policy			
Standard			
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	CWA_SJC_Bldg5_Floor3	if DEVICE:Location EQUALS All Locations#North_America#San_Jose#Campus_A#Building_5#Floor_2 then	Central_Web_Auth

In mobile environments, many wireless access points may connect to a single, centrally-located controller. In this scenario, the network access device is the wireless controller and its location may provide little insight into a specific user's

point of connection. Therefore, it may be necessary to match location based on the specific access point and/or wireless LAN (WLAN) to which the user is connected. Figure 3 shows example policy rules to match on either a specific WLAN (SSID) or Access Point.

Figure 3 - Example Authorization Policy Rules to Match Specific WLAN or AP

▼ Authorization Policy				
Standard				
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
✓	CWA_NSP	if Radius:Called-Station-ID ENDS_WITH :BYOD-Open then	Central_Web_Auth_NSP	
✓	CWA_Specific_AP	if Radius:Called-Station-ID STARTS_WITH 68-86-a7-ca-fe-e0 then	Central_Web_Auth	

Figure 4 shows an example detailed Live Authentications log entry with key attributes available to match wireless location.

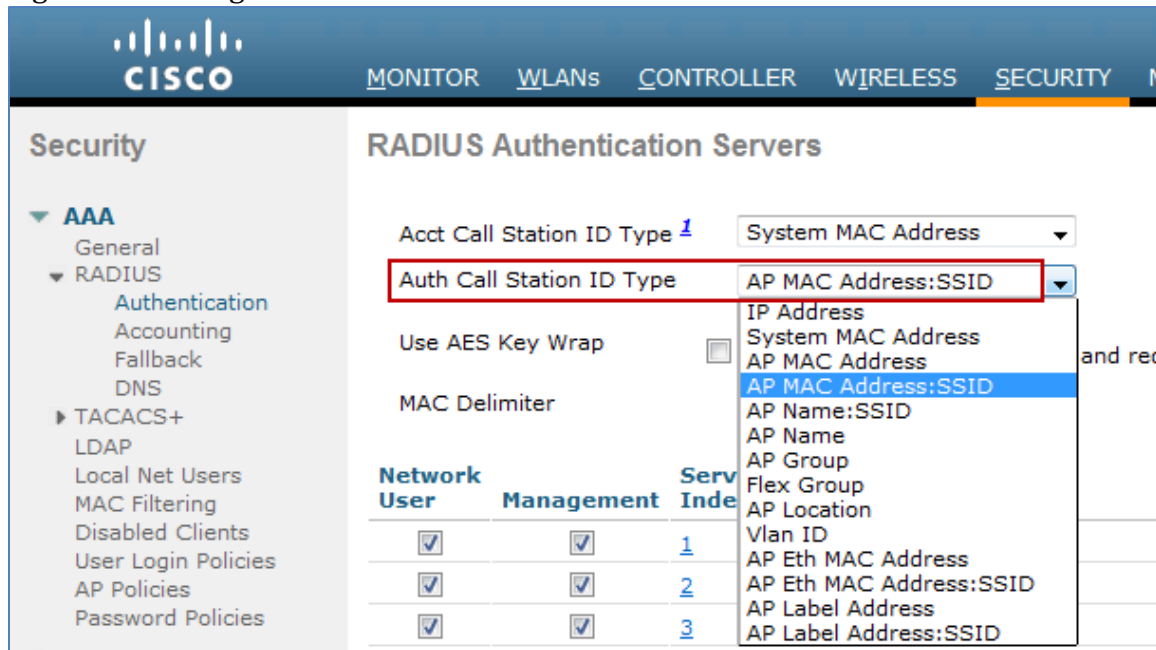
Figure 4 – Sample Live Authentications Log and Location Attributes

Other Attributes	
DestinationPort	1812
Protocol	Radius
NAS-Port	1
Airespace-Wlan-Id	3
AuthorizationPolicyMatchedRule	CWA_Specific_AP
CPMSessionID	0a012c5a000000305384953d
Location	Location#All Locations#North_America#San_Jose#Campus_A#Building_5#Floor_2
Device Type	Device Type#All Device Types#Wireless
RADIUS Username	7C:6D:62:E3:D5:05
Device IP Address	10.1.44.90
Called-Station-ID	68-86-a7-ca-fe-e0:guest-cwa

Note: An alternative to matching the SSID name is to use the Airespace-Wlan-Id. This attribute matches the specific ID assigned to the WLAN on the WLC. The downside to this approach is that the WLAN ID may change from one controller to another if not deliberately mapped to be the same across WLCs.

In order to match on the specific conditions shown in Figure 3, the WLC must be configured to populate the Called-Station-ID attribute in the RADIUS request with the required information. On the WLC, you can configure the format of this attribute under the Security → RADIUS → Authentication section of the web administration interface as shown in Figure 5.

Figure 5 – Setting the WLC Called-Station-ID Attribute



Note: The specific attribute values available will depend on the controller software version. Table 1 lists various values that may be set for the Called-Station-ID by WLC version.

Table 1 – Called-Station-ID by WLC Version

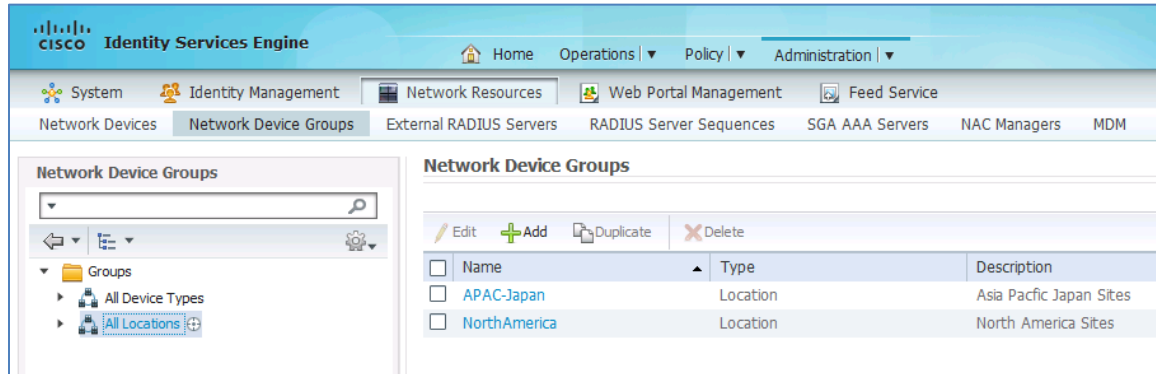
Called-Station-ID Setting	Description	Supported WLC Version
ipaddr	WLC IP Address	7.0
macaddr	WLC MAC Address	7.0
ap-macaddr (7.0)	AP MAC Address	7.0
ap-macaddr-only (7.2+)		
ap-macaddr-ssid	AP MAC Address:SSID	7.2
ap-location	AP Location	7.4
ap-name	AP Name	7.4
ap-name-ssid	AP Name:SSID	7.4
ap-group-name	AP Group Name	7.4
flex-group-name	Flex Group Name	7.4
vlan-id	VLAN ID	7.4
ap-ethmac-only	AP Ethernet MAC Address	7.6
ap-ethmac-ssid	AP Eth MAC Address:SSID	7.6
ap-label-address	AP Label Address	7.6
ap-label-address-ssid	AP Label Address:SSID	7.6

For wireless manageability and to help scale ISE authorization policy rules, it is recommended to group multiple APs and WLANs into groups and configure policies

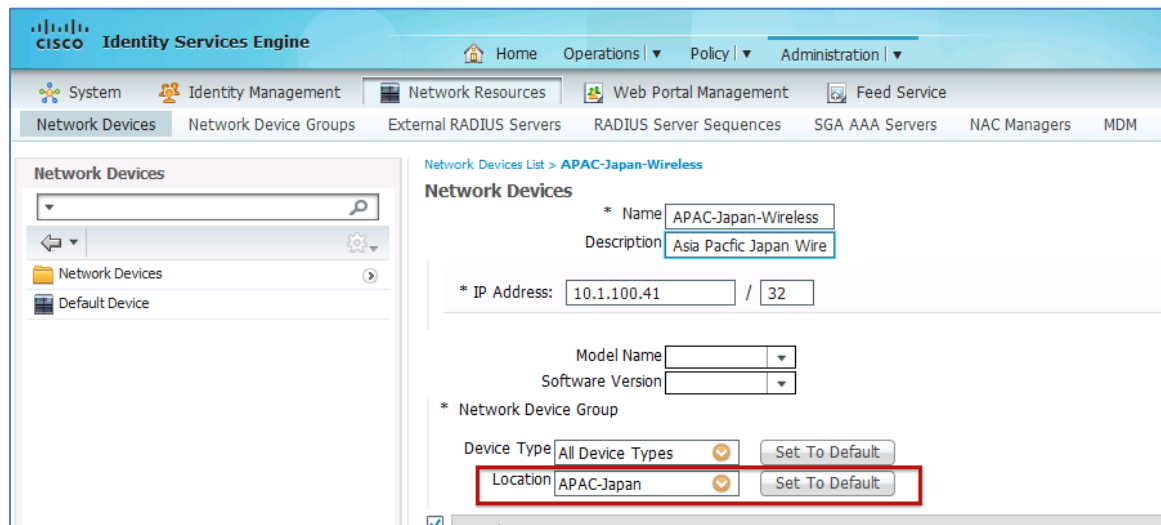
based on these groupings. Example groupings include AP Groups, Flex Groups, and AP Location.

Example Configuration #1: Location-Based Web Portals using NDGs

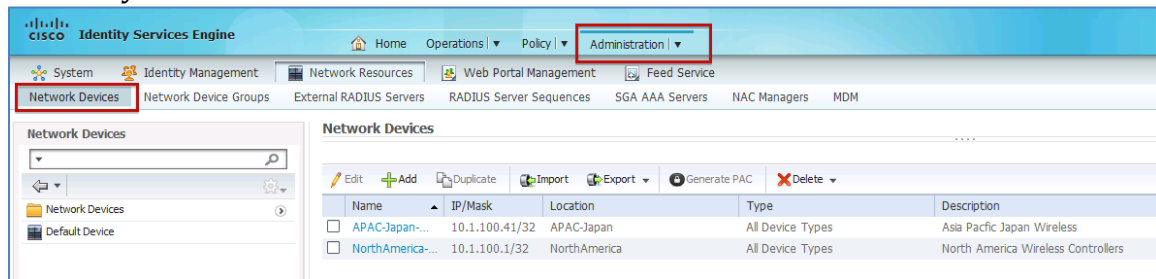
Step 1. Navigate to Administration → Network Resources → Network Device Groups and set up locations – APAC-Japan and NorthAmerica



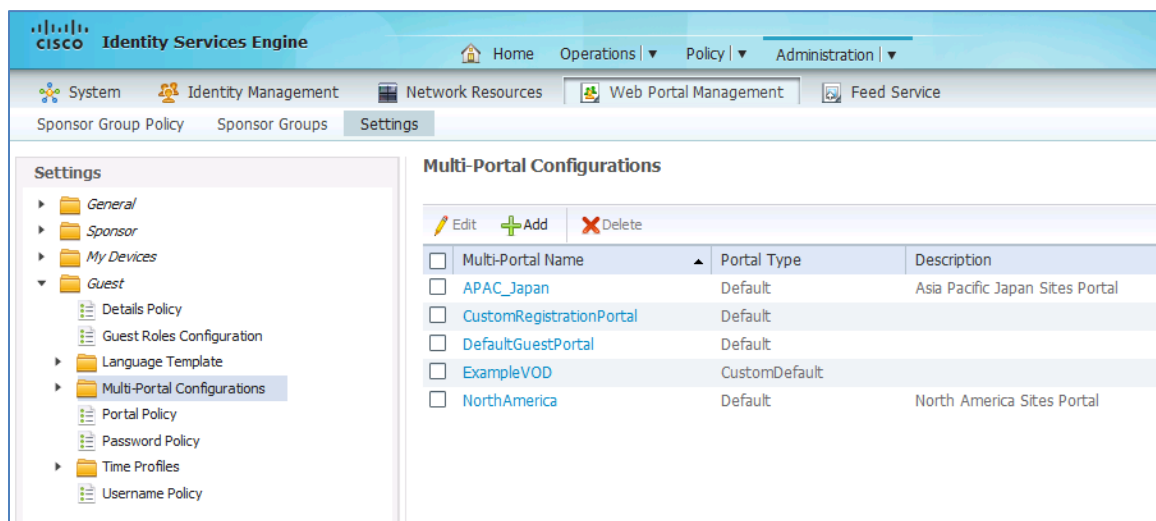
Step 2. Next navigate to Administration → Network Resources → Network Devices and then assign Network Devices to the corresponding locations.



Summary Screen:

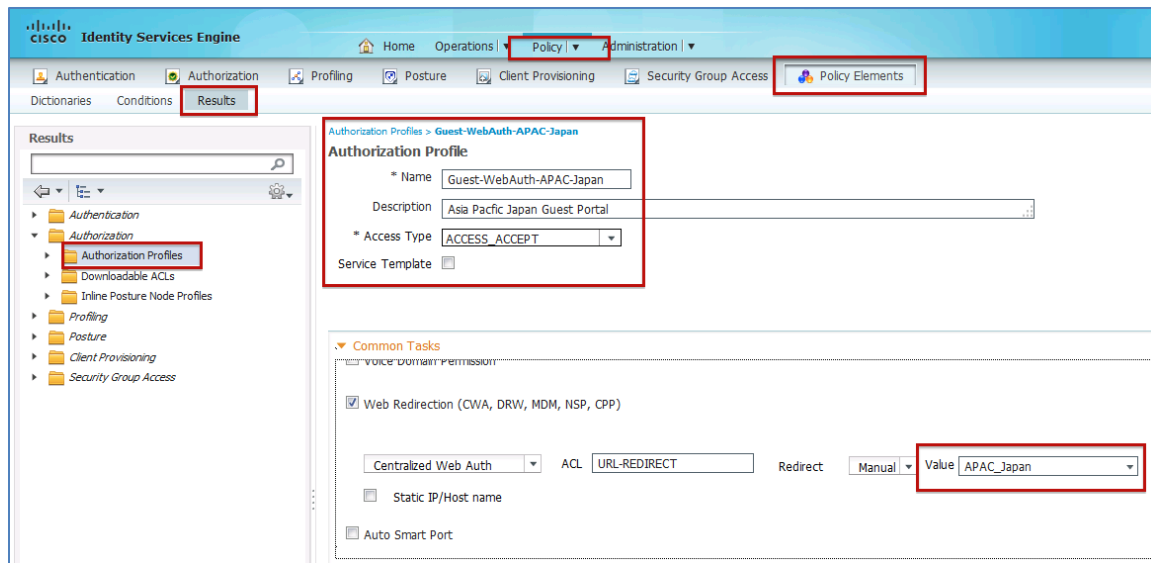


Step 3. Navigate to Administration → Web Portal Management → Guest → Multi-Portal Configurations and create or modify an existing portal for each of the locations.



Note: Since the end goal is to present a unique web portal by location, it is necessary to create custom web portals for each location. In ISE 1.2 and below, custom portals require that individual html and graphic files be uploaded and mapped in ISE. The default portal based on the global portal theme can be used as the fallback portal if no match to a specific location portal. This portal can be assigned to the default CWA rule in the Authorization Policy.

Step 4. Navigate to Policy → Policy Elements → Results → Authorization → Authorization Profiles. For each location, create Authorization Profiles that redirect guest users to Central Web Authentication (CWA). For each profile, select the custom web portal defined for that location.



We now have Authorization Profiles to support CWA at two sites, but also need policies to grant the appropriate guest access after successful web authentication.

- Step 5. Setup an Authorization Profile to permit guest access appropriate to each location once users are authenticated against the localized web portal.

Authorization Profile

* Name:

Description:

* Access Type:

Service Template: ☐

Common Tasks

☐ MALSEC POLICY

☐ NEAT

☐ Web Authentication (Local Web Auth)

☒ Airespace ACL Name:

☐ ASA VPN

Advanced Attributes Settings

Select an item: = +

Attributes Details

Access Type = ACCESS_ACCEPT
Airespace-ACL-Name = PERMIT-ACCESS

Here is a summary that shows the final Authorization Profiles:

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. The 'Policy' menu is expanded, showing 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', 'Security Group Access', and 'Policy Elements'. The 'Results' tab is selected under 'Authorization'. The left sidebar shows a tree view with 'Authorization' > 'Authorization Profiles' selected. The main area displays a table of 'Standard Authorization Profiles'.

Name	Description
BYOD_CWA	
BYOD_NSP	
Blackhole_Wireless_Access	Default profile used to blacklist wireless devices. Ensure
CWA_Wired_Contractor_Access	Contractor Wired AuthZ
CWA_Wired_Guest_Access	Guest Wired AuthZ
CWA_Wireless_Contractor_Access	Contractor Wireless AuthZ
CWA_Wireless_Guest_Access	Guest Wireless AuthZ
Chain_CorpUser_CorpDevice	
Chain_CorpUser_PersDevice	
Cisco_IP_Phones	Default profile used for Cisco Phones.
Contractor_Access	
DenyAccess	Default Profile with access type as Access-Reject
Employee_Access	
Guest-APAC-Japan	Asia Pacific Japan Guest Access
Guest-NorthAmerica	North America Site Guest Access
Guest-WebAuth-APAC-Japan	Asia Pacific Japan Guest Portal
Guest-WebAuth-NorthAmerica	North America Site Guest Portal
ITAdmin_Access	
Non_Cisco_IP_Phones	Default Profile used for Non Cisco Phones.
PermitAccess	Default Profile with access type as Access-Accept
Posture_Remediation	Permit access to posture and remediation services
WebAuth	Central WebAuth AuthZ

Step 6. After Authorization Profiles are configured, map each to device locations under separate Authorization Policy rules. Each site has a rule that redirects users to a location-based web portal and another rule that grants access once authenticated.

To add these new policy rules, navigate to Policy → (Policy Set) → Authorization Policy. Either modify existing Authorization Policy rules or create new rules similar to the following:

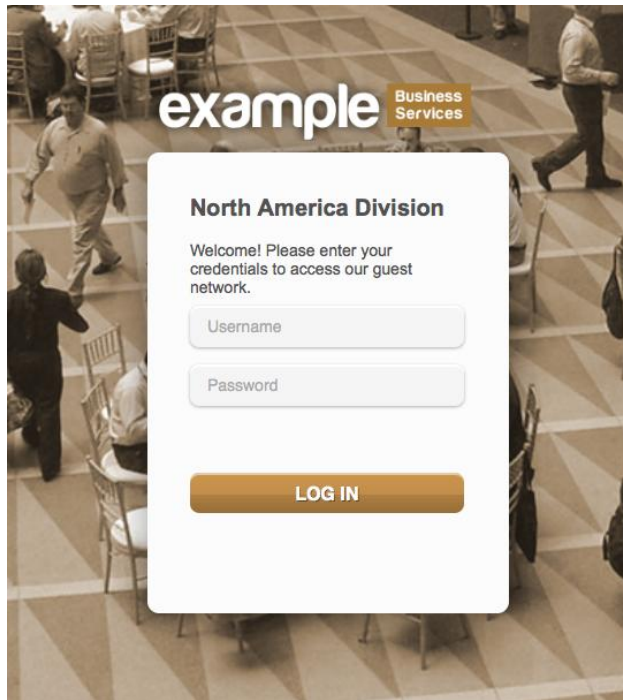
<input checked="" type="checkbox"/>	Guest-Wireless-Access-NorthAmeri	if Guest AND DEVICE:Location EQUALS All Locations#NorthAmerica	then Guest-NorthAmerica
<input checked="" type="checkbox"/>	Guest-Wireless-Access-APAC-Japan	if Guest AND DEVICE:Location EQUALS All Locations#APAC-Japan	then Guest-APAC-Japan
<input checked="" type="checkbox"/>	WebAuth-Wireless-APAC-Japan	if (Wireless_MAB AND DEVICE:Location EQUALS All Locations#APAC-Japan)	then Guest-WebAuth-APAC-Japan
<input checked="" type="checkbox"/>	WebAuth-Wireless-NorthAmerica	if (Wireless_MAB AND DEVICE:Location EQUALS All Locations#NorthAmerica)	then Guest-WebAuth-NorthAmerica
<input checked="" type="checkbox"/>	Default	if no matches, then	DenyAccess

- Step 7. When a guest attempts to access the network from a location in Japan they are presented with a web portal welcoming them to the Asia Pacific Japan Division.



- Step 8. The Operations → Authentications → Show Live Authentications log displays the Network Device with corresponding Authorization Profile for the Japan Wireless Site.

- Step 9. When a different guest in North America attempts to access the network they are presented with the North America Portal.

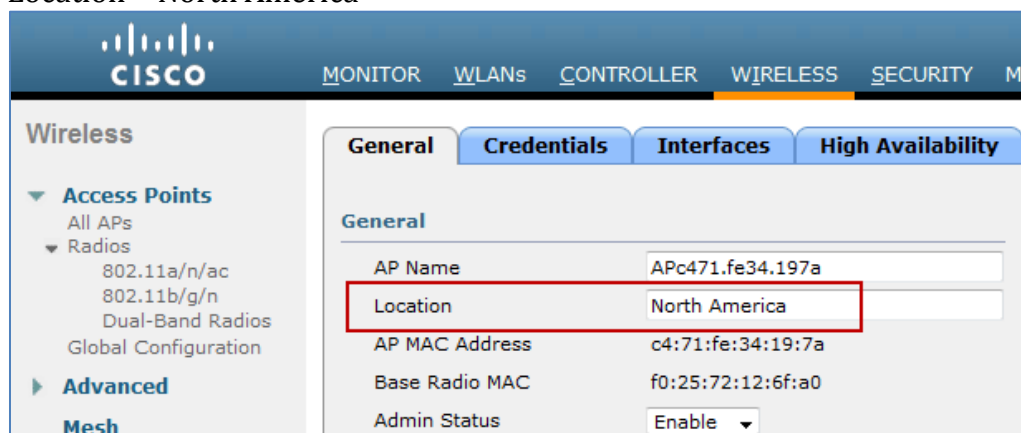


Example Configuration #2: Location-Based Web Portals using AP Location

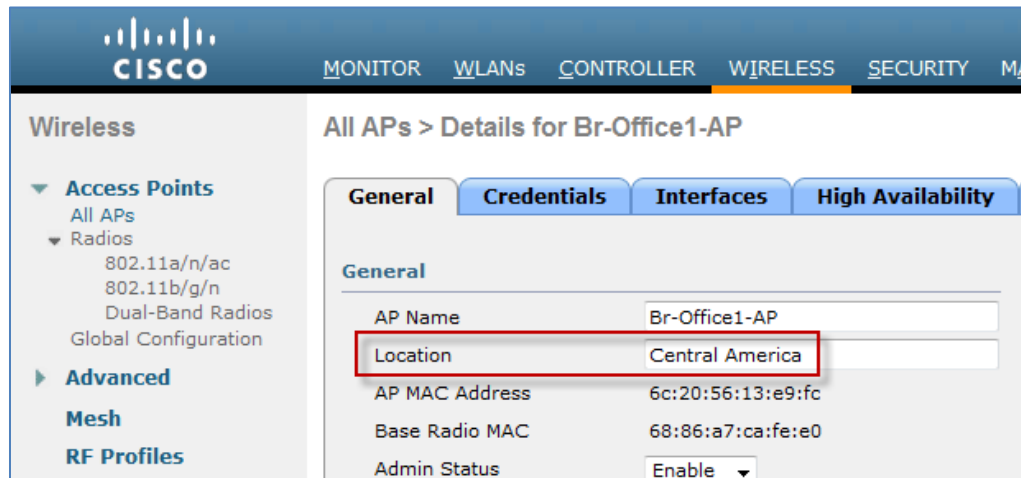
- Step 1. Set the Location attribute for the wireless access points.

On the Wireless LAN Controller, define the Location attribute for each wireless access point under Wireless → General → Access Points

Location = North America



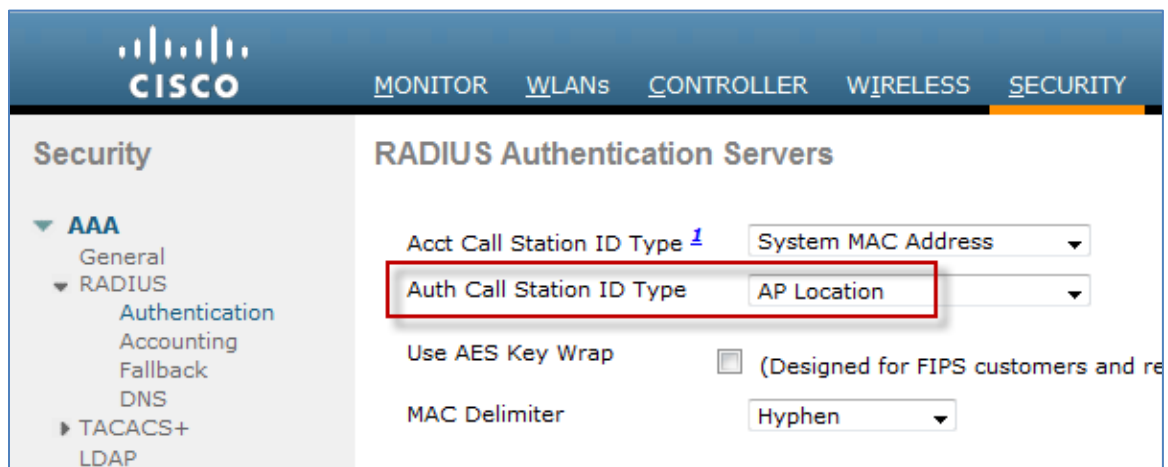
Location = Central America



The screenshot shows the Cisco ISE configuration interface for a specific Access Point (AP). The left sidebar is under the 'Wireless' section, with 'Access Points' expanded. The main content area is titled 'All APs > Details for Br-Office1-AP'. There are four tabs: 'General', 'Credentials', 'Interfaces', and 'High Availability'. The 'General' tab is active, showing a table of configuration details. A red box highlights the 'Location' field, which is set to 'Central America'.

General	
AP Name	Br-Office1-AP
Location	Central America
AP MAC Address	6c:20:56:13:e9:fc
Base Radio MAC	68:86:a7:ca:fe:e0
Admin Status	Enable

Step 2. Set the Called-Station-ID attribute for the WLC to AP Location under Security → AAA → RADIUS → Authentication.



The screenshot shows the Cisco ISE configuration interface for RADIUS Authentication Servers. The left sidebar is under the 'Security' section, with 'AAA' expanded and 'RADIUS' selected. The main content area is titled 'RADIUS Authentication Servers'. There are two dropdown menus: 'Acct Call Station ID Type' set to 'System MAC Address' and 'Auth Call Station ID Type' set to 'AP Location'. A red box highlights the 'Auth Call Station ID Type' dropdown. Below these are checkboxes for 'Use AES Key Wrap' and 'MAC Delimiter' set to 'Hyphen'.

RADIUS Authentication Servers	
Acct Call Station ID Type	System MAC Address
Auth Call Station ID Type	AP Location
Use AES Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and re)
MAC Delimiter	Hyphen

Note: This is a global configuration setting, so be sure the value is compatible with other operations that may be impacted by a change in the Called-Station-ID attribute.

Step 3. Create Authorization Profiles that return unique custom portals based on location.

From the ISE administrative interface, navigate to Policy → Policy Elements → Results → Authorization → Authorization Profiles. Create custom web authentication portals for each location and use case, for example, employee versus guest.

Example Authorization Profile for Guest Portal in Central America

Authorization Profiles > CWA_Guest_CentralAmerica

Authorization Profile

* Name:

Description:

* Access Type:

Service Template: ☐

Common Tasks

☒ Web Redirection (CWA, DRW, MDM, NSP, CPP)

ACL: Redirect: Value:

☐ Static IP/Host name

Summary of New Web Portals by Location and Use Case

CISCO Identity Services Engine

Home | Operations | Policy | Administration

System | Identity Management | Network Resources | Web Portal Management | Feed Se

Sponsor Group Policy | Sponsor Groups | Settings

Settings

- General
- Sponsor
- My Devices
- Guest
 - Details Policy
 - Guest Roles Configuration
 - Language Template
 - Multi-Portal Configurations
 - CustomDeviceWebAuthPortal
 - CustomPortal
 - DefaultDeviceWebAuthPortal
 - Employee_CentralAmerica
 - Employee_NorthAmerica
 - Guest_CentralAmerica
 - Guest_NorthAmerica

Multi-Portal Configurations

Edit Add Delete

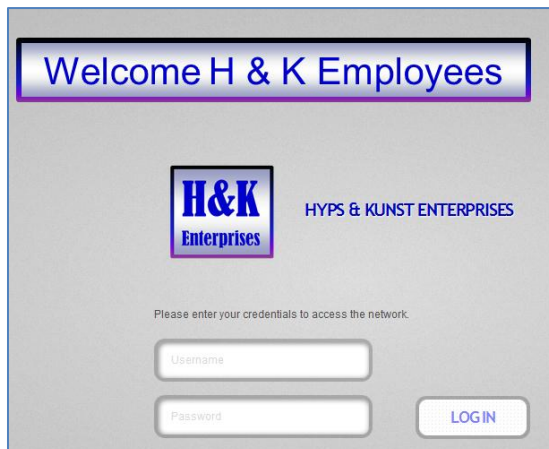
Multi-Portal Name	Portal Type
<input type="checkbox"/> CustomDeviceWebAuthPortal	CustomDeviceWebAuth
<input type="checkbox"/> CustomPortal	CustomDefault
<input type="checkbox"/> DefaultDeviceWebAuthPortal	DeviceWebAuth
<input type="checkbox"/> Employee_CentralAmerica	CustomDefault
<input type="checkbox"/> Employee_NorthAmerica	CustomDefault
<input type="checkbox"/> Guest_CentralAmerica	CustomDefault
<input type="checkbox"/> Guest_NorthAmerica	CustomDefault

- Step 4. Create Authorization Policy rules that match use case (WLAN = Employee or Guest) and on location (Called-Station-ID set to AP location attribute).

Navigate to Policy → (Policy Set) → Authorization Policy. Create or modify existing policy rules for web authentication to match use case and location.

▼ Authorization Policy				
► Exceptions (0)				
Standard				
Status	Rule Name	Conditions (identity groups and other conditions)		Permissions
✓	CWA_Guest_CentralAmerica	if (Airespace:Airespace-Wlan-Id EQUALS 3 AND Radius:Called-Station-ID EQUALS Central America)	then	CWA_Guest_CentralAmerica
✓	CWA_Guest_NorthAmerica	if (Airespace:Airespace-Wlan-Id EQUALS 3 AND Radius:Called-Station-ID EQUALS North America)	then	CWA_Guest_NorthAmerica
✓	CWA_Employee_CentralAmerica	if (Airespace:Airespace-Wlan-Id EQUALS 4 AND Radius:Called-Station-ID EQUALS Central America)	then	CWA_Employee_CentralAmerica
✓	CWA_Employee_NorthAmerica	if (Airespace:Airespace-Wlan-Id EQUALS 4 AND Radius:Called-Station-ID EQUALS North America)	then	CWA_Employee_NorthAmerica

Step 5. Example login to the Employee WLAN from the AP configured for Location = North America.



Welcome H & K Employees

H&K Enterprises HYPS & KUNST ENTERPRISES

Please enter your credentials to access the network.

Username

Password

LOGIN

Step 6. Example login to the Guest WLAN from the AP configured for Location = Central America.



Bienvenido Usuarios Invitados

H&K Enterprises HYPS & KUNST ENTERPRISES

Por favor, introduzca sus credenciales para acceder a la red.

Nombre de usuario

Contraseña

ACCEDER

Step 7. Sample Live Log Authentication details highlighting key location-based attributes.

Other Attributes	
ConfigVersionId	39
DestinationPort	1812
Protocol	Radius
NAS-Port	1
Framed-MTU	1300
Tunnel-Type	(tag=0) VLAN
Tunnel-Medium-Type	(tag=0) 802
Tunnel-Private-Group-ID	(tag=0) 41
Airespace-Wlan-Id	3
OriginalUserName	7c6d62e3d505
Acs SessionID	ise12-psn2/188977409/242475
UseCase	Host Lookup
SelectedAuthenticationIdentityStores	AD1
SelectedAuthenticationIdentityStores	Internal Endpoints
ADDomain	cts.local
AuthorizationPolicyMatchedRule	CWA_Guest_CentralAmerica
HostIdentityGroup	Endpoint Identity Groups:Profiled:Apple-iPad
Location	Location#All Locations#LATAM#Mexico_City
Device Type	Device Type#All Device Types#Wireless
RADIUS Username	7C:6D:62:E3:D5:05
Device IP Address	10.1.44.90
Called-Station-ID	Central America