Configure ISE Wireless CWA and Hotspot Flows with AireOS and Next Generation WLCs

Contents

Introduction

This document describes how to configure three guest cases in Identity Services engine with Cisco AireOS and Next Generation Wireless LAN Controllers.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Wireless LAN Controllers (Unified and Converged Access)
- Identity Services Engine (ISE)

Components Used

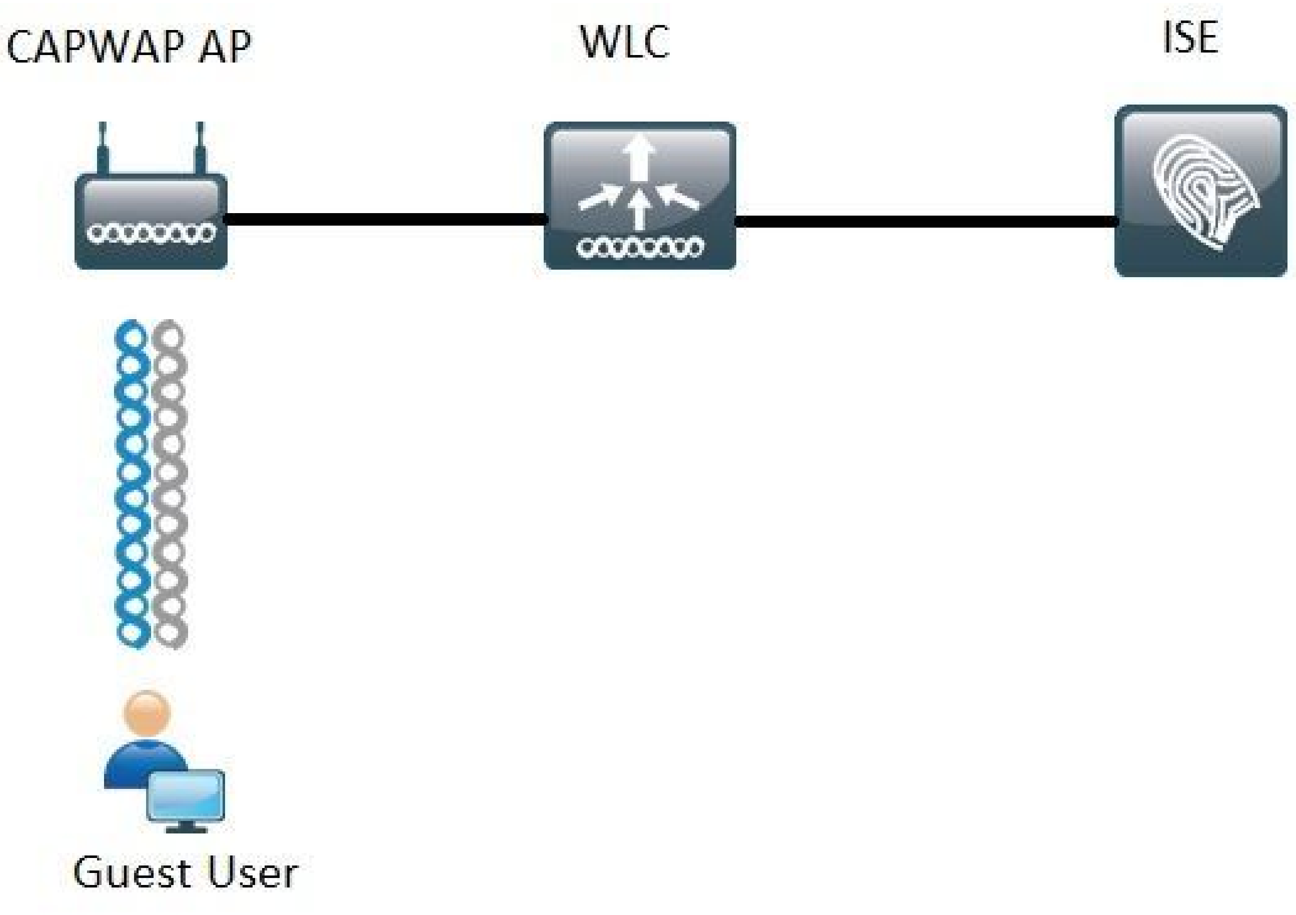
The information in this document is based on these software and hardware versions:

- Cisco Identity Services Engine version 2.1
- Cisco Wireless LAN controller 5508 with 8.0.121.0
- Next Generation Wireless Controller (NGWC) catalyst 3850(WS-C3850-24P) with 03.06.04.E

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram



Steps covered in this document describe the typical configuration on both Unified and Converged Access WLCs to support any Guest flow with ISE.

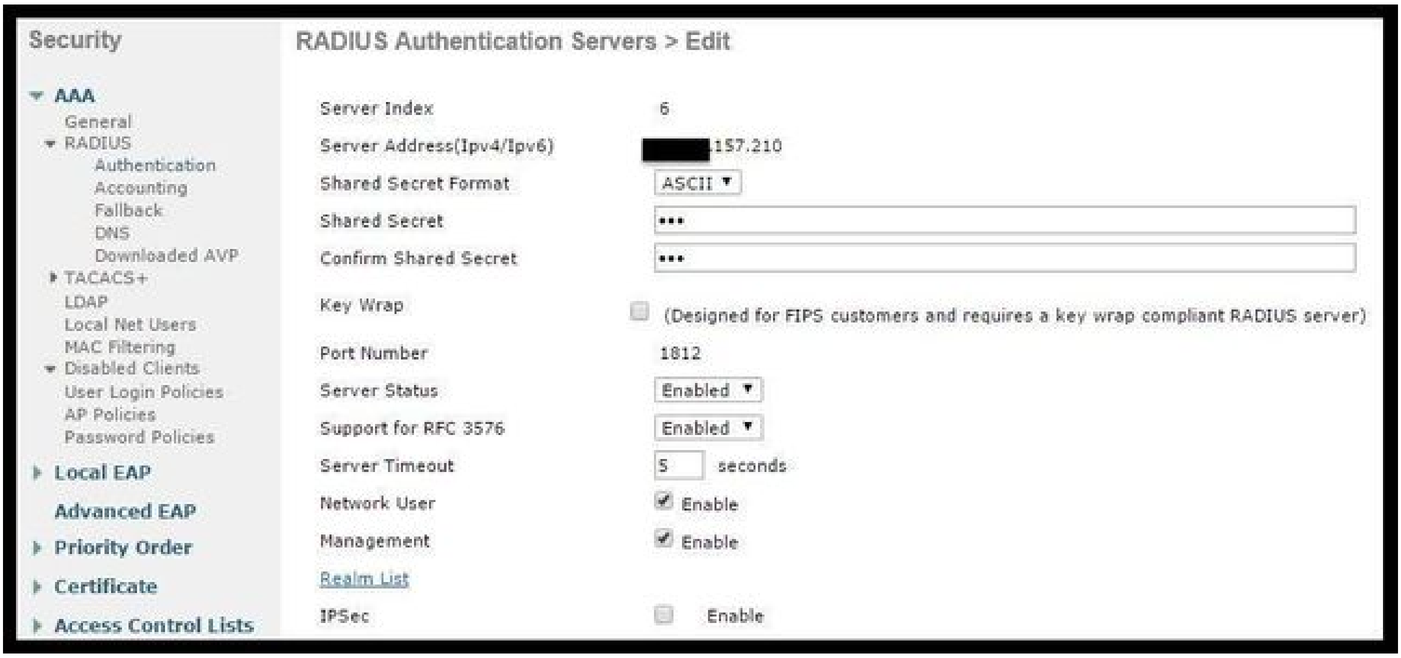
Configure Unified 5508 WLC

Regardless of the use case configured in ISE, from the WLC perspective it all starts with a wireless endpoint that connects to an Open SSID with MAC filtering enabled (Plus AAA override and RADIUS NAC) that points to ISE as the authentication and accounting server. This ensures that ISE can dynamically push the necessary attributes to the WLC for successful enforcement of a redirect to ISE's Guest Portal.

Global Configuration

1. Add ISE globally as an Authentication and Accounting server.

- Navigate to **Security > AAA > Authentication** and click **New**



RADIUS Authentication Servers > Edit

Server Index 6
Server Address(Ipv4/Ipv6) [redacted].157.210
Shared Secret Format ASCII ▼
Shared Secret •••
Confirm Shared Secret •••
Key Wrap □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number 1812
Server Status Enabled ▼
Support for RFC 3576 Enabled ▼
Server Timeout 5 seconds
Network User ☑ Enable
Management ☑ Enable
Realm List
IPSec □ Enable

- Enter ISE server IP and shared secret
- Ensure that the Server Status and **Support for RFC 3676** (Change of Authorization or CoA support) are both set to **Enabled**.
- Under server timeout by default AireOS WLCs has have 2 seconds. Hinge on on the network characteristics (latency, ISE and WLC in different locations) it can be beneficial to increase the server timeout to at least 5 seconds to avoid unnecessary failover events.
- Click **Apply**.
- If there are multiple Policy Services Nodes (PSN) to configure proceed to create additional server entries.

Note: This particular configuration example includes 2 ISE instances

- Navigate to **Security > AAA > RADIUS > Accounting** and click **New**
- Enter ISE server IP and Shared secret
- Ensure that Server Status is set to Enabled
- Increase the server timeout if necessary (default is 2 seconds).

2. Fallback configuration.

In unified environment once the server timeout is triggered the WLC moves to the next configured server. Next in line from WLAN. If no other is available then the WLC selects the next one in the global servers list. When multiple servers are configured on the SSID (Primary, Secondary) once the failover occurs the WLC by default continues to send authentication and (or) accounting traffic permanently to the Secondary instance even if the primary server is back online.

In order to mitigate this behavior enable fallback. Navigate to **Security > AAA > RADIUS > Fallback.** The default behavior is off. The only way to recover from a server-down event requires admin intervention (globally bounce the server's admin status).

To enable fallback you have two options:

- **Passive -** In passive mode, if a server does not respond to the WLC authentication request, the WLC moves the server to inactive queue and sets a timer (Interval in Sec option). When the timer expires, the WLC moves the server to active queue irrespective of the servers actual status. If the authentication request results in a timeout event (which means the server is still down) the server entry is moved again to the Inactive queue and the timer kicks in again. If the server successfully responds back, it remains in the Active queue. Configurable values here go from 180 to 3600 seconds.

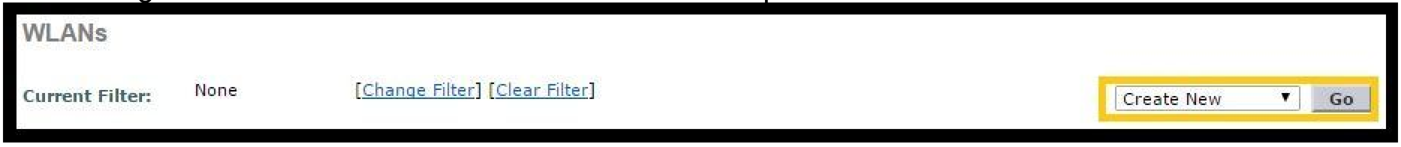
- **Active -** In active mode, when a server does not respond to the WLC authentication request, the WLC marks the server as dead, then moves the server to non-active server pool and starts sending probe messages periodically until that server responds. If the server responds, then the WLC moves the dead server to active pool and stops sending probe messages.

In this mode the WLC requires you to enter a username and a probe interval in seconds (180 to 3600).

Note: WLC probe does not require a successful authentication. Either way, a successful or failed authentications are considered a server response which is enough to promote the server to the Active queue.

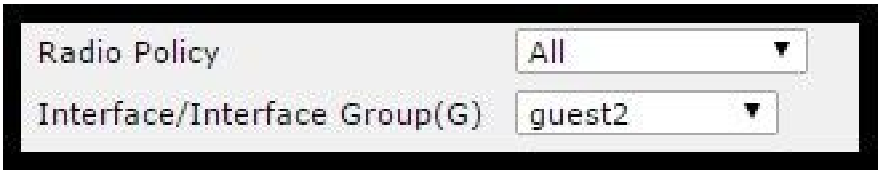
Configure the Guest's Service Set Identifier (SSID):

- Navigate to WLANs tab and under Create New option click **Go**:


WLANs

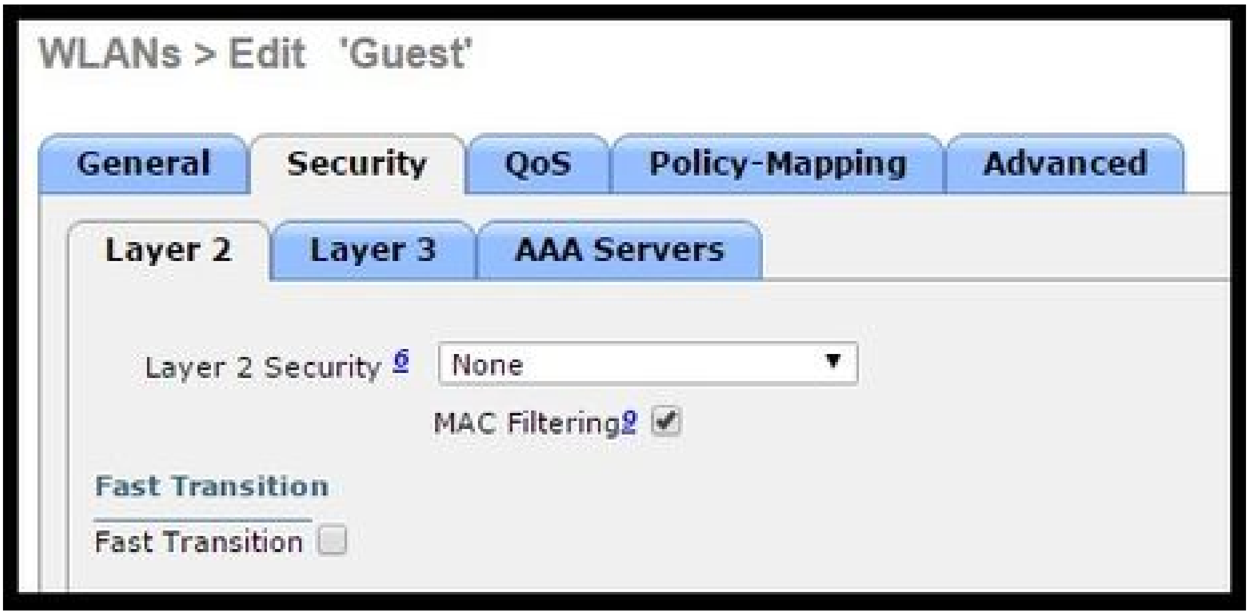
Current Filter: None [Change Filter] [Clear Filter]

- Enter Profile Name and SSID name. Click **Apply**.
- Under the General Tab select the Interface or Interface Group to be used (Guest VLAN).


Radio Policy: All

Interface/Interface Group(G): guest2

- Under **Security > Layer 2 > Layer 2 Security** select **None** and enable **Mac Filtering** checkbox.


WLANs > Edit 'Guest'

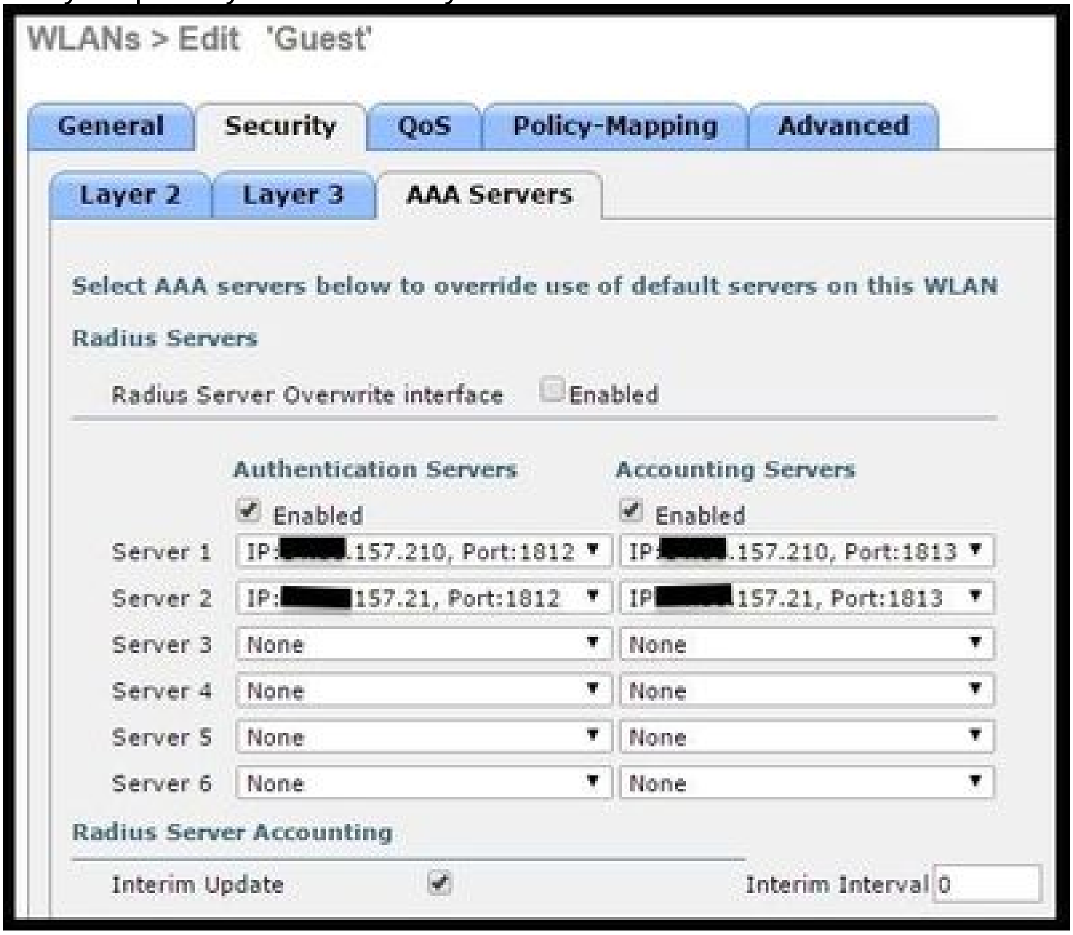
Layer 2 Security 6: None

MAC Filtering 9 ☑

Fast Transition

Fast Transition □

- Under **AAA Servers** tab set Authentication and Accounting servers to **enabled** and select your primary and secondary servers.



WLANs > Edit 'Guest'

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

Radius Servers

Radius Server Overwrite interface □ Enabled

	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	IP:[redacted].157.210, Port:1812 ▼	IP:[redacted].157.210, Port:1813 ▼
Server 2	IP:[redacted]157.21, Port:1812 ▼	IP[redacted]157.21, Port:1813 ▼
Server 3	None ▼	None ▼
Server 4	None ▼	None ▼
Server 5	None ▼	None ▼
Server 6	None ▼	None ▼

Radius Server Accounting

Interim Update ☑ Interim Interval 0

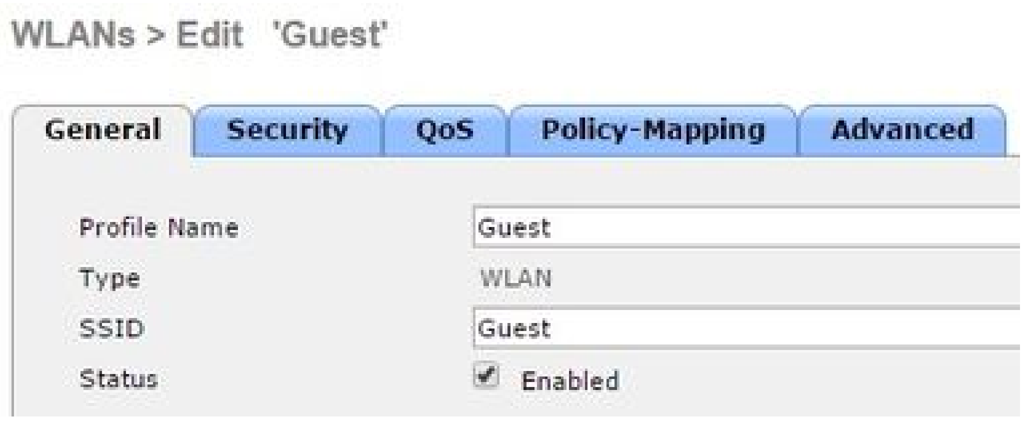
- **Interim Update**: This is an optional configuration that does not add any benefits to this flow. If you prefer to enable it, the WLC i must run 8.x or higher code:

Disabled: The feature is completely disabled.

Enabled with 0 Interval: The WLC sends accounting updates to ISE every time there is a change in the client's Mobile Station Control Block(MSCB) entry (ie. IPv4 or IPv6 address assignment or change, client roaming event.) No additional periodic updates are sent out.

Enabled with a configured Interim Interval: In this mode the WLC sends notifications to ISE upon client's MSCB entry changes and it also sends additional periodic accounting notifications at the configured interval (regardless of any changes).

- Under Advanced Tab Enable **Allow AAA Override** and Under **NAC state** select **RADIUS NAC**. This ensures that the WLC applies any attribute value pairs (AVPs) that come from ISE.
- Navigate to the SSID general tab and set the SSID status to **Enabled**



WLANs > Edit 'Guest'

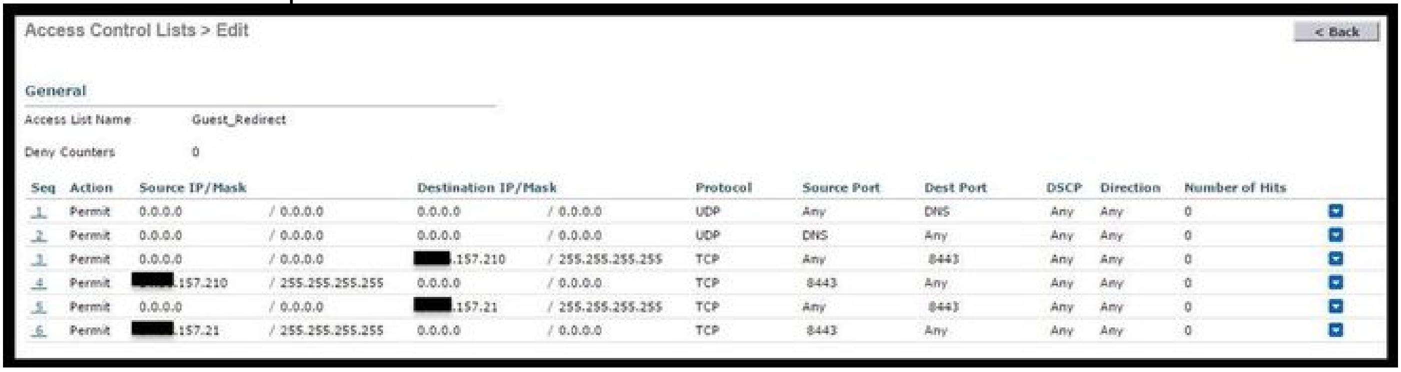
Profile Name	Guest
Type	WLAN
SSID	Guest
Status	☑ Enabled

- **Apply** the changes.

Configure the Redirect ACL

This ACL is referenced by ISE and it determines what traffic gets redirected and what traffic is allowed through.

- Go to **Security** Tab > **Access Control Lists** and click **New**
- This is an example of ACL



Access Control Lists > Edit

General

Access List Name	Guest_Redirect
Deny Counters	0

Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
1	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	UDP	Any	DNS	Any	Any	0	▾
2	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	UDP	DNS	Any	Any	Any	0	▾
3	Permit	0.0.0.0	/ 0.0.0.0	[redacted].157.210	/ 255.255.255.255	TCP	Any	8443	Any	Any	0	▾
4	Permit	[redacted].157.210	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	TCP	8443	Any	Any	Any	0	▾
5	Permit	0.0.0.0	/ 0.0.0.0	[redacted].157.21	/ 255.255.255.255	TCP	Any	8443	Any	Any	0	▾
6	Permit	[redacted].157.21	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	TCP	8443	Any	Any	Any	0	▾

This ACL must allow access to and from DNS services and ISE nodes over TCP port 8443. There is an implicit deny at the bottom that means the rest of the traffic gets redirected to ISE's Guest Portal URL.

HTTPS Redirect

This feature is supported in AireOS versions 8.0.x and up but it is turned off by default. To enable HTTPS support go to the WLC **Management** > **HTTP-HTTPS > HTTPS Redirection** and set it to **Enabled** or apply the this command in CLI:

```
(Cisco Controller) >config network web-auth https-redirect enable
```

Certificate Warnings after HTTPS redirect is enabled

After https-redirect is enabled, the user can experience certificate trust issues during the redirect. This is seen even if there is a valid chained certificate on the controller and even if this certificate is signed by a 3rd party trusted Certificate Authority. The reason is that the certificate installed on the WLC is issued to its Virtual interface hostname or IP address. When the client tries https://cisco.com, the browser expects the certificate to be issued to cisco.com. However, for the WLC to be able to intercept the GET issued by the client, it first needs to establish the HTTPS session for which the WLC presents its Virtual Interface Certificate during SSL handshake phase.

This causes the browser to display a warning as the certificate presented during the SSL handshake has not been issued to the original web site the client is trying to access (ie. cisco.com opposed to WLC's Virtual interface hostname). You can see different certificate error messages in different browsers but all relate to the same problem.

Aggressive Failover

This feature is enabled by default in AireOS WLCs. When aggressive failover is enabled, the WLC marks the AAA server as unresponsive and it moves to the next configured AAA server after a RADIUs timeout event affects one client.

When the feature is disabled the WLC fails over to the next server only if the RADIUS timeout event occurs with at least 3 client sessions. This feature can be disabled by this command (No reboot is required for this command):

```
(Cisco Controller) >config radius aggressive-failover disable
```

To verify the current status of the feature:

```
(Cisco Controller) >show radius summary

Vendor Id Backward Compatibility................. Disabled
Call Station Id Case............................. lower
Acct Call Station Id Type........................ Mac Address
Auth Call Station Id Type........................ AP's Radio MAC Address:SSID
Extended Source Ports Support.................... Enabled
Aggressive Failover.............................. Disabled
```

Captive Bypass

The endpoints that support a Captive Network Assistant (CNA) mechanism to discover a captive-portal and auto-launch a logon page usually do this through a pseudo-browser in a controlled window while other endpoints launch a fully capable browser to trigger this. For endpoints where the CNA launches a pseudo-browser, this can break the flow when redirected to an ISE captive portal. This typically affect Apple IOS devices and it has especially negative effects in flows that require device registration, VLAN DHCP-Rlease, compliance check.

Hinge on on the complexity of the flow in use it can be recommended to enable Captive Bypass. In such scenario, the WLC ignores the CNA portal discovery mechanism and the client needs to open a browser to initiate the redirect process.

Verify the status of the feature:

```
(Cisco Controller) >show network summary

Web Auth CMCC Support ...................... Disabled
Web Auth Redirect Ports .................... 80,3128
Web Auth Proxy Redirect  ................... Disable
Web Auth Captive-Bypass   .................. Disabled
Web Auth Secure Web  ....................... Enable
Web Auth Secure Redirection  .............. Enable
```

To enable this feature type this command:

```
(Cisco Controller) >config network web-auth captive-bypass enable
Web-auth support for Captive-Bypass will be enabled.

You must reset system for this setting to take effect.
```

The WLC alerts the user that for changes to take effect a reset-system (restart) is needed.

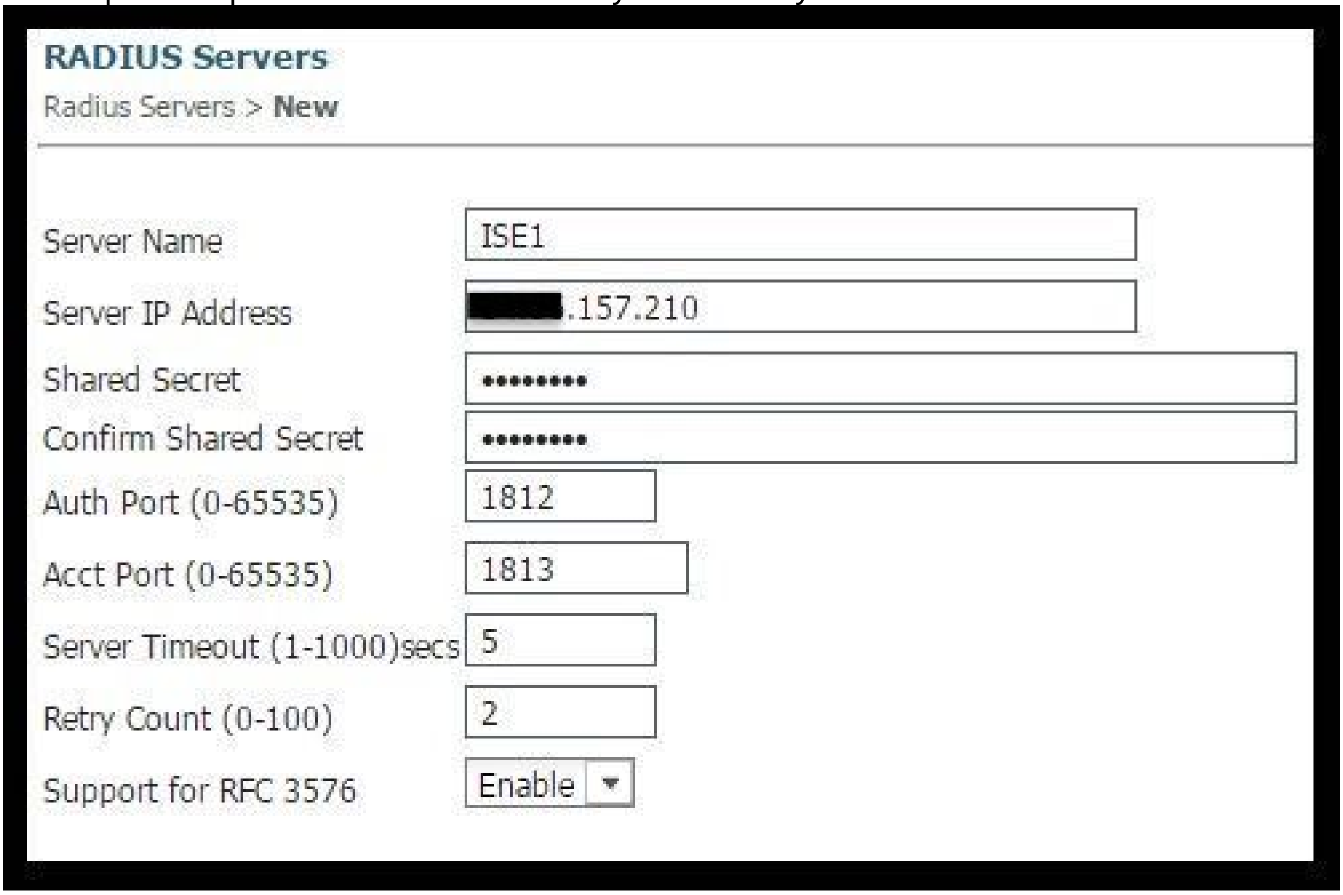
At this point a **show network summary** shows the feature as enabled, but for changes to take effect the WLC needs to be restarted.

Configure Converged 3850 NGWC

Global Configuration

1. **Add ISE globally as an Authentication and Accounting server**

- Navigate to **Configuration > Security > RADIUS > Servers** and click **New**
- Enter the ISE **Server IP address**, **shared secret**, **server timeout** and **Retry Count** that reflects your environmental conditions.
- Ensure that **Support for RFC 3570** (CoA support) is enabled.
- Repeat the process to add a Secondary Server entry.



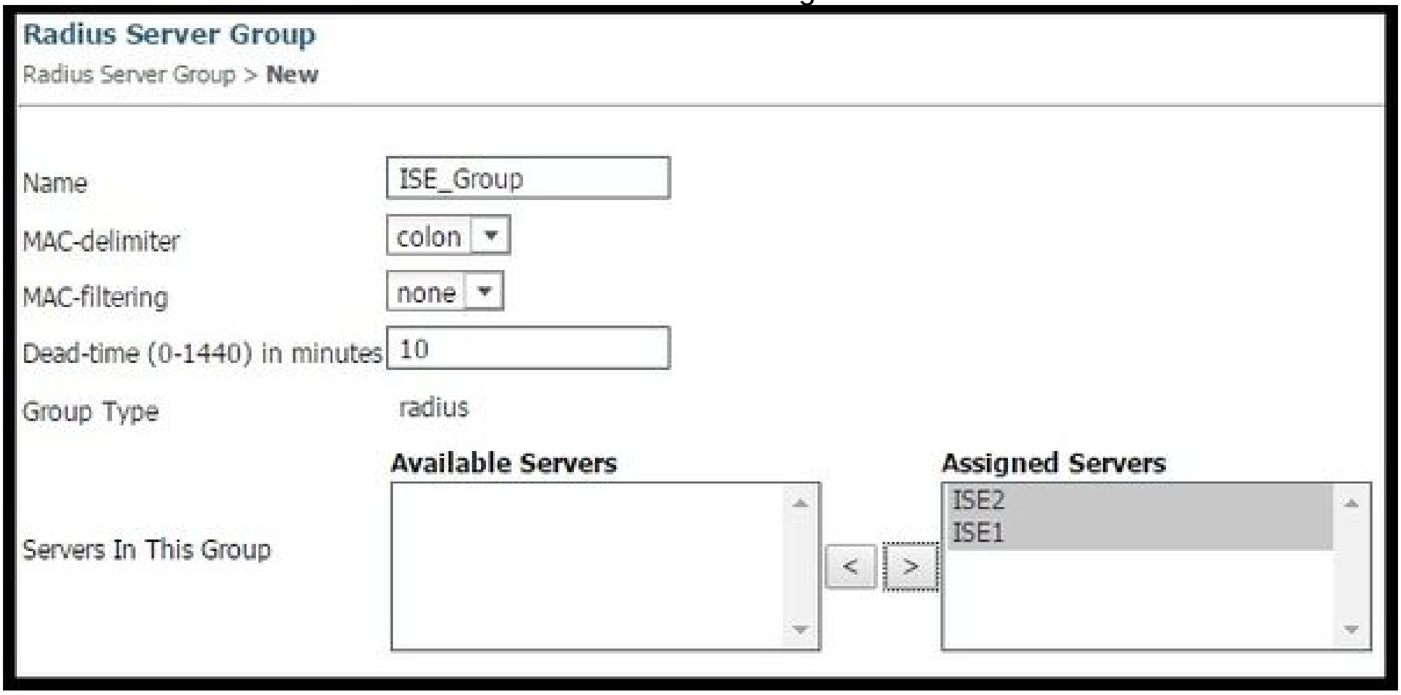
RADIUS Servers

Radius Servers > **New**

Server Name	ISE1
Server IP Address	[redacted].157.210
Shared Secret	•••••••••
Confirm Shared Secret	•••••••••
Auth Port (0-65535)	1812
Acct Port (0-65535)	1813
Server Timeout (1-1000)secs	5
Retry Count (0-100)	2
Support for RFC 3576	Enable

2. **Create ISE's server group**

- Navigate to **Configuration > Security > Server Groups** And click **New**
- Assign a name to the group and enter a **Dead-time** value in minutes. This is the time that the controller keeps the server in the Inactive queue before it is promoted again to the active server list.
- From the Available Servers list add them to the Assigned Servers column.



Radius Server Group

Radius Server Group > **New**

Name	ISE_Group
MAC-delimiter	colon
MAC-filtering	none
Dead-time (0-1440) in minutes	10
Group Type	radius

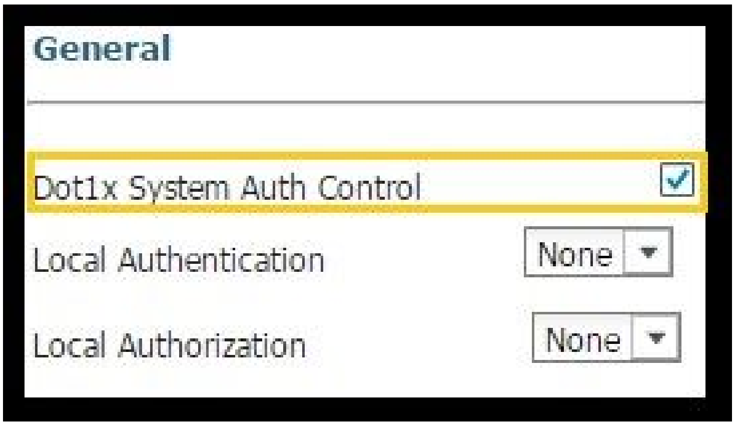
Servers In This Group

Available Servers

Assigned Servers
ISE2
ISE1

3. **Globally Enable Dot1x**

- Navigate to **Configuration > AAA > Method Lists > General** and enable **Dot1x system Auth Control**

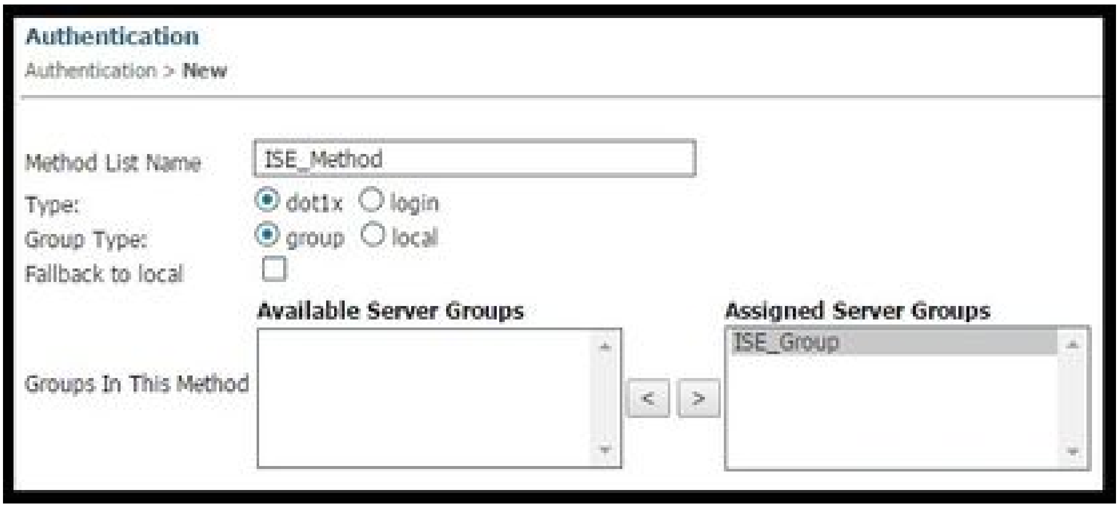


General

Dot1x System Auth Control	☑
Local Authentication	None
Local Authorization	None

4. **Configure Method Lists**

- Navigate to **Configuration** > **AAA** > **Method Lists** > **Authentication** and create a new Method List. In this case it is Type Dot1x and Group ISE_Group (group created in previous step). Then hit **Apply**



Authentication

Authentication > New

Method List Name: ISE_Method

Type: ● dot1x ○ login

Group Type: ● group ○ local

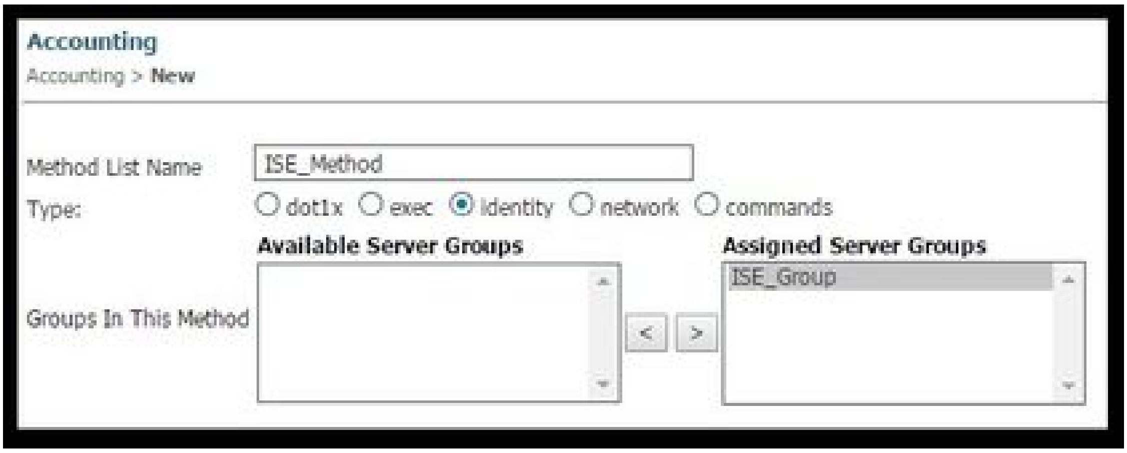
Fallback to local: □

Groups In This Method

Available Server Groups:

Assigned Server Groups: ISE_Group

- Do the same for accounting (**Configuration > AAA > Method Lists > accounting**) and Authorization (**Configuration > AAA > Method Lists > Authorization**). They must look like this



Accounting

Accounting > New

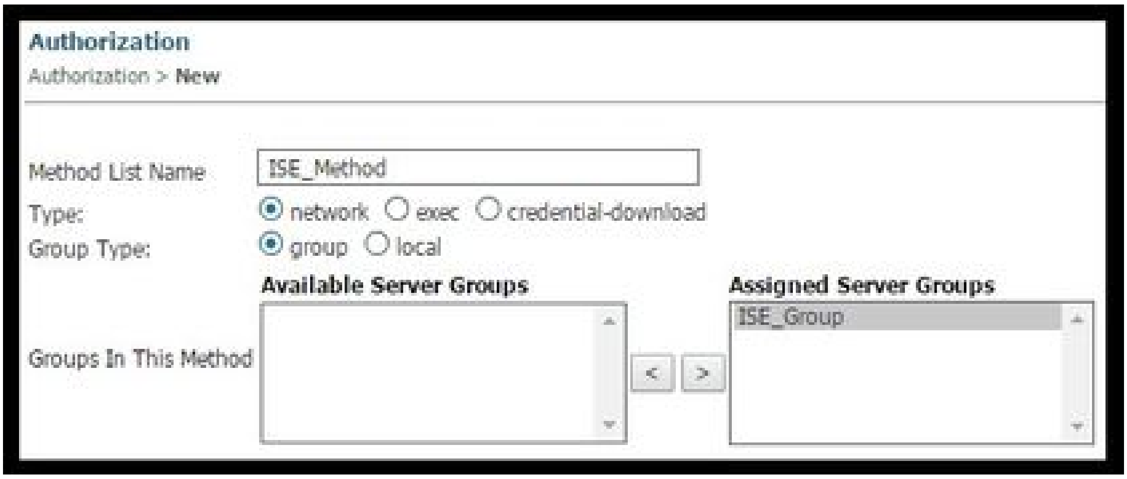
Method List Name: ISE_Method

Type: ○ dot1x ○ exec ● identity ○ network ○ commands

Groups In This Method

Available Server Groups:

Assigned Server Groups: ISE_Group



Authorization

Authorization > New

Method List Name: ISE_Method

Type: ● network ○ exec ○ credential-download

Group Type: ● group ○ local

Groups In This Method

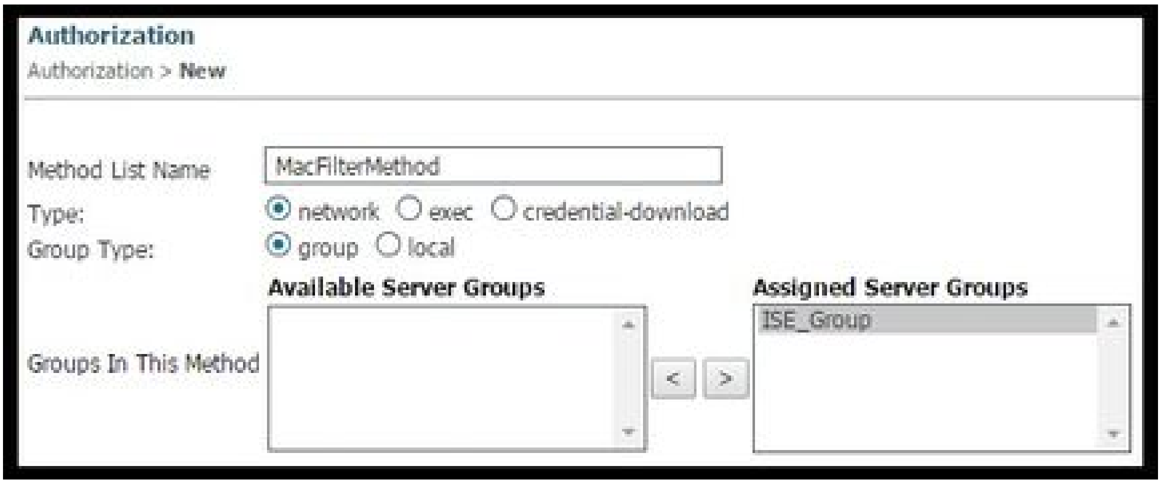
Available Server Groups:

Assigned Server Groups: ISE_Group

5. **Create the authorization MAC-filter method**.

This is called from the SSID settings later.

- Navigate to **Configuration> AAA > Method Lists > Authorization** and click **New**.
- Enter the **Method List Name**. Chose **Type = Network** and **Group Type Group**.
- Add ISE_Group to the Assigned Server Groups field.



Method List Name: MacFilterMethod

Type: ● network ○ exec ○ credential-download

Group Type: ● group ○ local

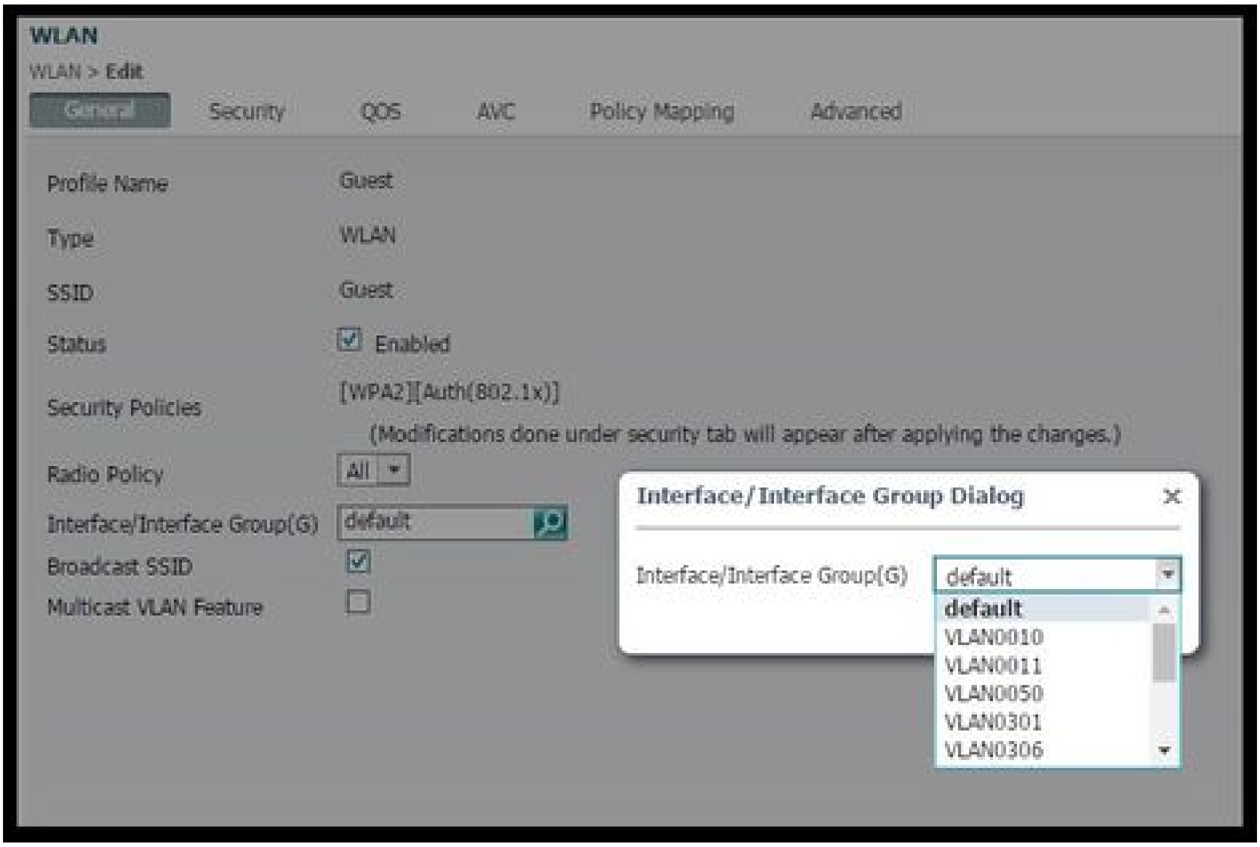
Groups In This Method

Available Server Groups	Assigned Server Groups
	ISE_Group

SSID configuration

1. **Create the Guest SSID**

- Navigate to **Configuration > Wireless > WLANs** and click **New**
- Enter WLAN ID, SSID and Profile Name and click Apply.
- Once in the SSID settings under Interface / Interface Group select the Guest VLAN Layer 3 interface.

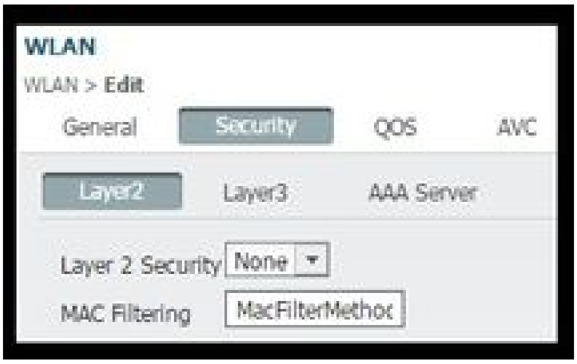


Profile Name	Guest
Type	WLAN
SSID	Guest
Status	☑ Enabled
Security Policies	[WPA2][Auth(802.1x)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	default
Broadcast SSID	☑
Multicast VLAN Feature	□

Interface/Interface Group(G): default

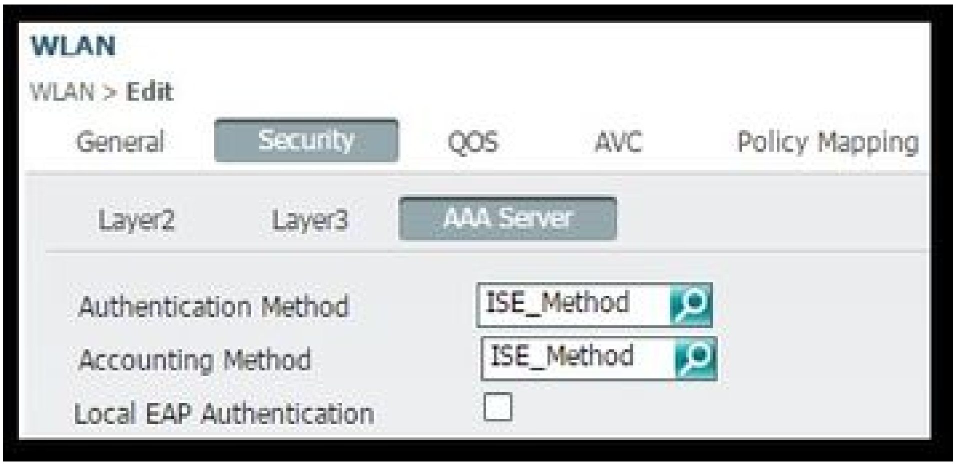
default
VLAN0010
VLAN0011
VLAN0050
VLAN0301
VLAN0306

- Under **Security** > **Layer 2** select **None** and next to **Mac Filtering** enter the Mac Filter Method List Name you previously configured (MacFilterMethod).
- Under **Security** > **AAA Server** Tab select the proper Authentication and Accounting methods lists (ISE_Method).



Layer 2 Security: None

MAC Filtering: MacFilterMethoc

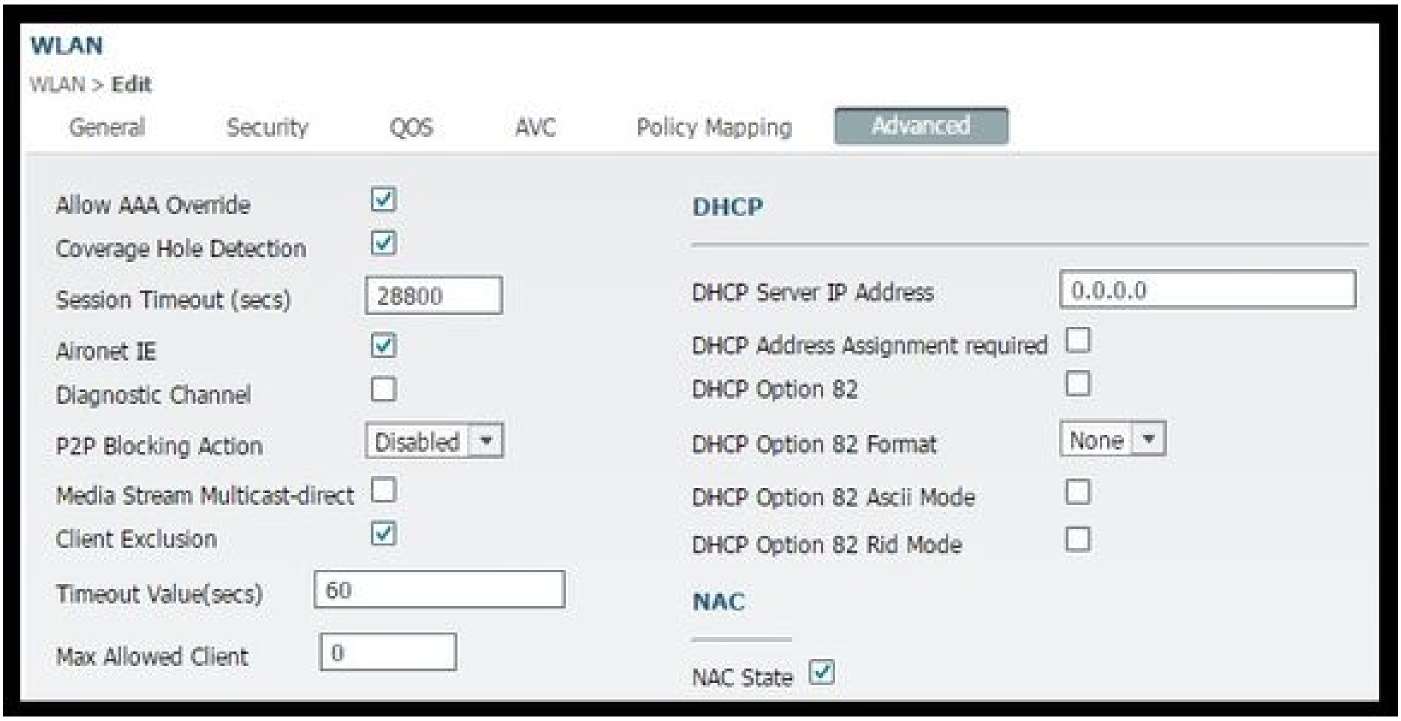


Authentication Method: ISE_Method

Accounting Method: ISE_Method

Local EAP Authentication: □

- Under **Advanced** Tab enable **Allow AAA Override** and **NAC state.** The rest of the settings must be adjusted as per each deployment requirements (session timeout, Client Exclusion, Support for Aironet Extensions).



Allow AAA Override: ☑

Coverage Hole Detection: ☑

Session Timeout (secs): 28800

Aironet IE: ☑

Diagnostic Channel: □

P2P Blocking Action: Disabled

Media Stream Multicast-direct: □

Client Exclusion: ☑

Timeout Value(secs): 60

Max Allowed Client: 0

DHCP

DHCP Server IP Address: 0.0.0.0

DHCP Address Assignment required: □

DHCP Option 82: □

DHCP Option 82 Format: None

DHCP Option 82 Ascii Mode: □

DHCP Option 82 Rid Mode: □

NAC

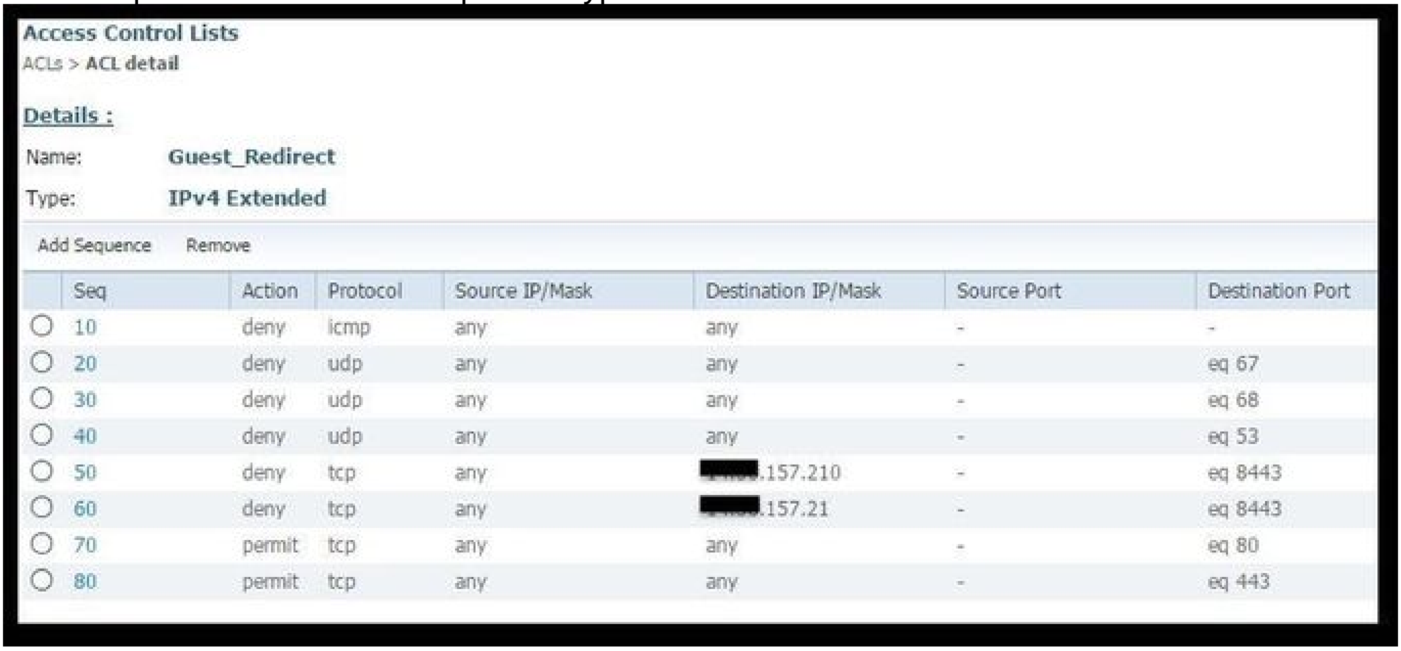
NAC State: ☑

- Navigate to the General Tab set the Status to Enabled. Then hit **Apply.**

Redirect ACL configuration

This ACL is referenced by ISE later in the access-accept in response to the initial MAB request. The NGWC uses it to determine what traffic to redirect and what traffic must be allowed through.

- Navigate to **configuration > security > ACL > Access Control Lists** and click **Add New**.
- Select Extended and enter the ACL Name.
- This picture shows an example of a typical Redirect ACL:



Access Control Lists

ACLs > ACL detail

Details :

Name: Guest_Redirect

Type: IPv4 Extended

	Seq	Action	Protocol	Source IP/Mask	Destination IP/Mask	Source Port	Destination Port
○	10	deny	icmp	any	any	-	-
○	20	deny	udp	any	any	-	eq 67
○	30	deny	udp	any	any	-	eq 68
○	40	deny	udp	any	any	-	eq 53
○	50	deny	tcp	any	[redacted].157.210	-	eq 8443
○	60	deny	tcp	any	[redacted].157.21	-	eq 8443
○	70	permit	tcp	any	any	-	eq 80
○	80	permit	tcp	any	any	-	eq 443

Note: Line 10 is optional. This is usually added for troubleshooting proposes. This ACL must allow access to DHCP, DNS services and also to ISE servers port TCP 8443(Deny ACEs). HTTP and HTTPS traffic gets redirected (Permit ACEs).

Command-Line interface (CLI) configuration

All the configuration discussed in previous steps can also be applied through the CLI.

802.1x Globally enabled

```
dot1x system-auth-control
```

Global AAA configuration

```
aaa new-model
!
aaa authentication dot1x ISE_Method group ISE_Group
aaa authorization network ISE_Method group ISE_Group
aaa authorization network MacFilterMethod group ISE_Group
aaa accounting Identity ISE_Method start-stop group ISE_Group
!
aaa server radius dynamic-author
 client 172.16.157.210 server-key *****
 client 172.16.157.21 server-key *****
 auth-type any
!
radius server ISE1
 address ipv4 172.16.157.210 auth-port 1812 acct-port 1813
 timeout 5
 retransmit 2
 key *****
!
radius server ISE2
```

```
 address ipv4 172.16.157.21 auth-port 1812 acct-port 1813
 timeout 5
 retransmit 2
 key *****
!
!
aaa group server radius ISE_Group
 server name ISE2
 server name ISE1
 deadtime 10
 mac-delimiter colon
!
```

Wlan Configuration

```
 wlan Guest 1 Guest
 aaa-override
 accounting-list ISE_Method
 client vlan VLAN0301
 mac-filtering MacFilterMethod
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security dot1x authentication-list ISE_Method
 no security ft over-the-ds
 session-timeout 28800
 no shutdown
```

Redirect ACL Example

```
3850#show ip access-lists Guest_Redirect
Extended IP access list Guest_Redirect
    10 deny icmp any any
    20 deny udp any any eq bootps
    30 deny udp any any eq bootpc
    40 deny udp any any eq domain
    50 deny tcp any host 172.16.157.210 eq 8443
    60 deny tcp any host 172.16.157.21 eq 8443
    70 permit tcp any any eq www
    80 permit tcp any any eq 443
```

HTTP and HTTPS support

```
3850#show run | inc http
ip http server
ip http secure-server
```

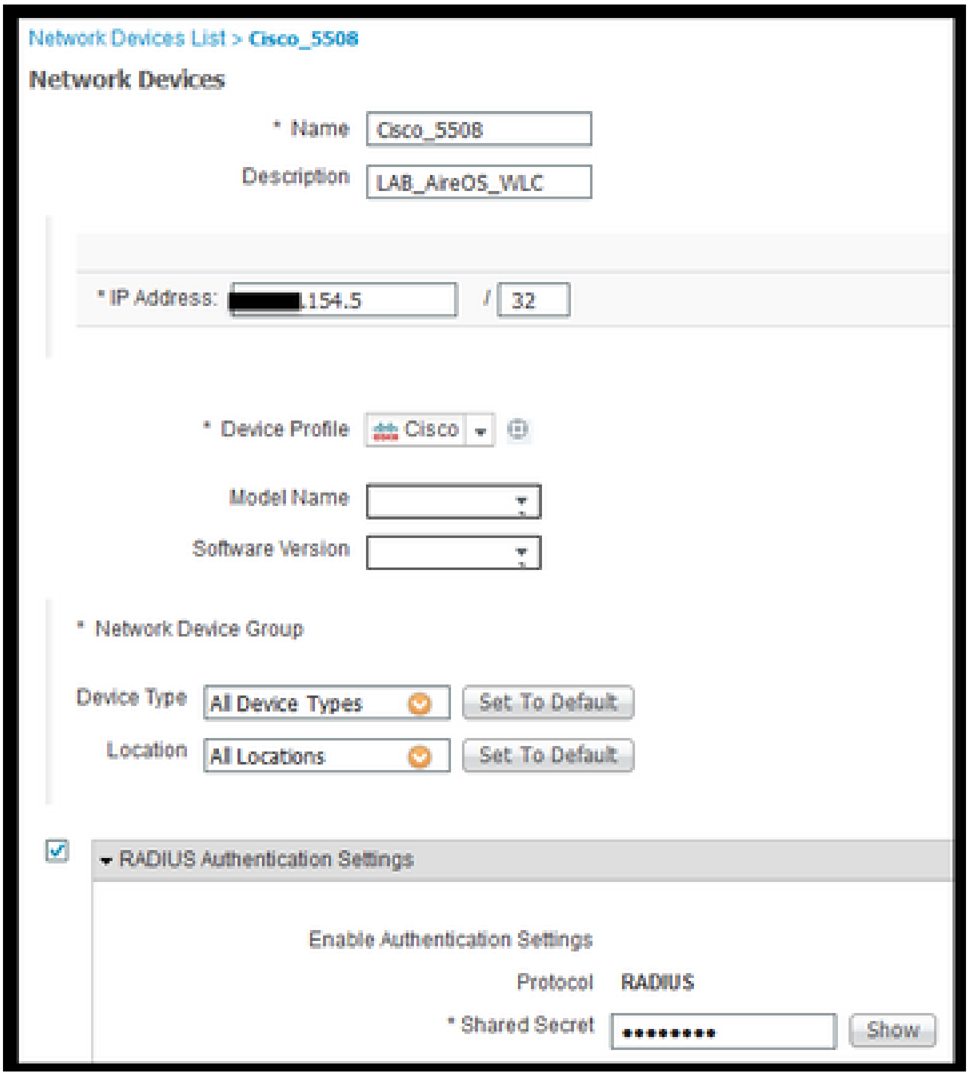
Note: If you apply an ACL to restrict access to the WLC over HTTP, it affects redirection.

Configure ISE

This section describes the configuration required on ISE to support the all uses cases discussed in this document.

Common ISE configuration tasks

1. Login to ISE and navigate to **Administration > Network Resources > Network Devices** and click **Add**
2. Enter the **Name** associated to the WLC and the device **IP address**.
3. Check the **RADIUs authentication settings** box and type the **Shared Secret** configured on the WLC side. Then click **Submit**.



Network Devices List > Cisco_5508

Network Devices

* Name: Cisco_5508
Description: LAB_AireOS_WLC

* IP Address: [redacted].154.5 / 32

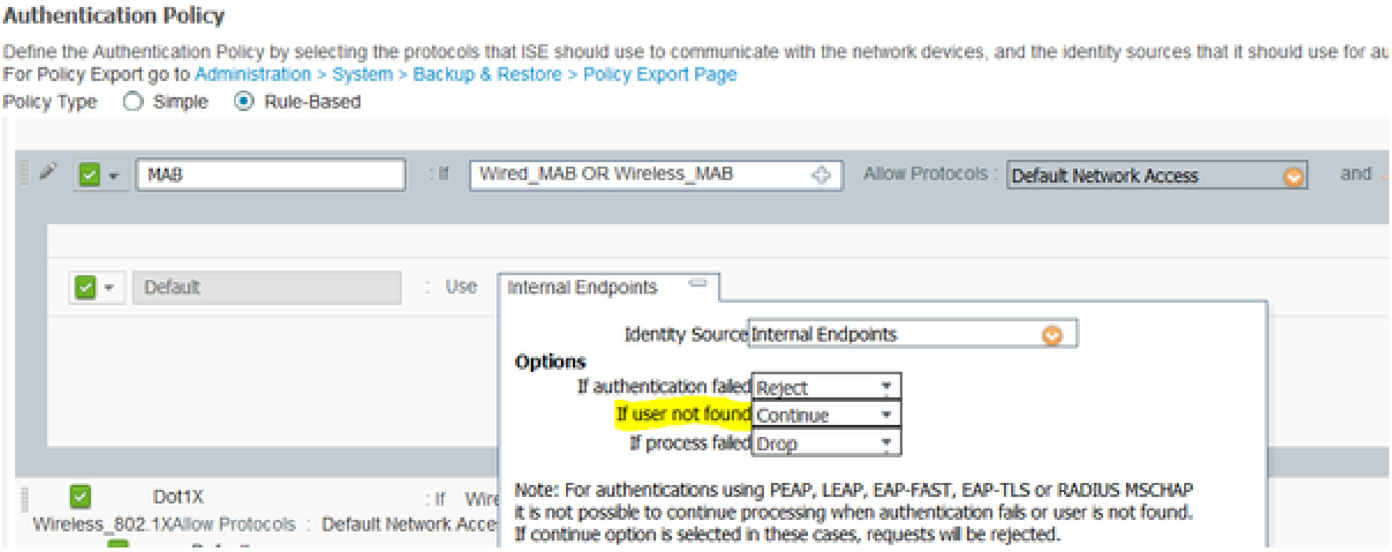
* Device Profile: Cisco
Model Name:
Software Version:

* Network Device Group
Device Type: All Device Types
Location: All Locations

☑ RADIUS Authentication Settings

Enable Authentication Settings
Protocol: RADIUS
* Shared Secret: •••••••••

4. Navigate to **Policy > Authentication** and under **MAB** click **Edit** and ensure that under **Use: Internal Endpoints** the option I**f user is not found** is set to **Continue** (It must be there by default).



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 should use for au

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB OR Wireless_MAB Allow Protocols : Default Network Access 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, EAP-TLS 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 Wire

Wireless_802.1XAllow Protocols : Default Network Acce

Use case 1: CWA With Guest Authentication in every user connection

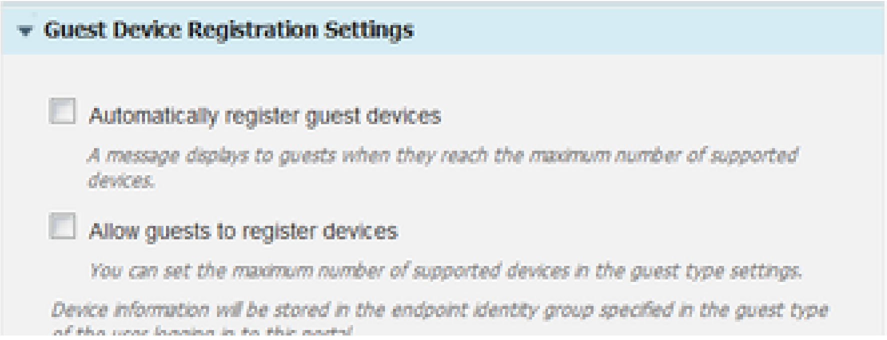
Flow Overview

1. Wireless user connects to the Guest SSID.
2. WLC authenticates the endpoint based on its MAC address on ISE as AAA server.
3. ISE returns back and access-accept with two Attribute Value Pairs (AVPs): url-redirect and url-redirect-acl. Once the WLC applies this AVPs to the endpoint session, the station transitions to DHCP-Required and once it grabs an IP address it stays in CENTRAL_WEB_AUTH. At this step the WLC is ready to start redirecting the client's http / https traffic.
4. The End User opens up the web browser and once HTTP or HTTPS traffic is generated, the WLC redirects the user to ISE guest portal.
5. Once the user gets to the Guest Portal it prompts to enter guest credentials (sponsor-created in this case).
6. Upon credentials validation ISE displays the AUP page and once the client accepts, a Dynamic CoA type Re-authenticate is sent out to the WLC.
7. The WLC re-processes the MAC filtering authentication without issuing a de-authenticate to the mobile station. This must be seamless to the endpoint.
8. Once the re-authentication event happens ISE re-evaluates Authorization policies and this time the endpoint is given a Permit access since there was a previous successful guest authentication event.

This process repeats itself every time the user connects to the SSID.

Configuration

1. Navigate to ISE and navigate to **Work Centers > Guest Access > Configure > Guest Portals** > Select **Sponsored Guest Portal** (or create a new portal type Sponsored-Guest).
2. Under **Guest Device Registration** settings uncheck all options and click **Save**.



▾ Guest Device Registration Settings

□ Automatically register guest devices

A message displays to guests when they reach the maximum number of supported devices.

□ Allow guests to register devices

You can set the maximum number of supported devices in the guest type settings.

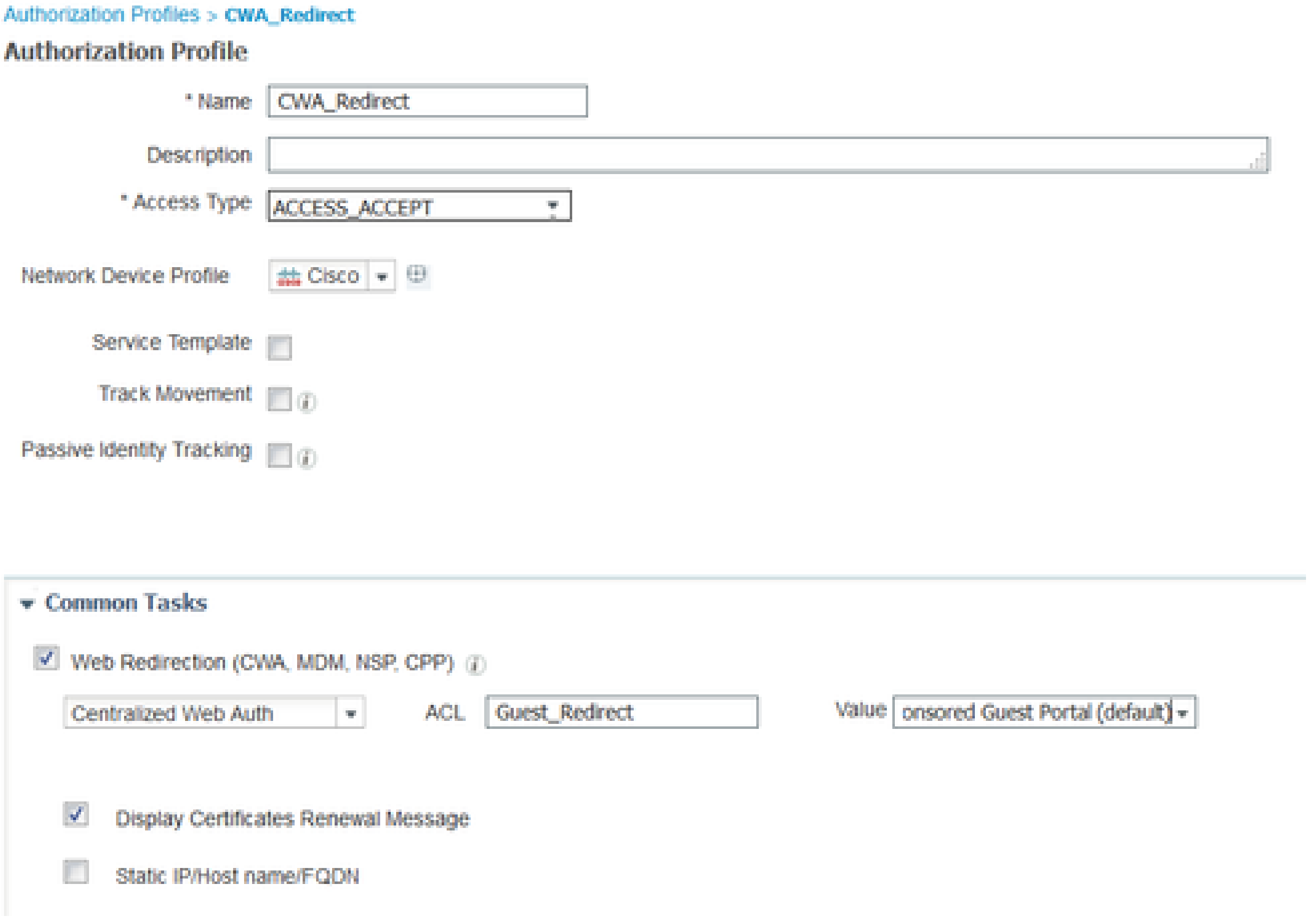
Device information will be stored in the endpoint identity group specified in the guest type of the user logging in to this portal

3. Navigate to **Policy > Policy Elements > Results > Authorization > Authorization Profiles**. Click **Add**.

4. This profile is pushed down to the WLC the **Redirect-URL** and the **Redirect-URL-ACL** in response to the initial Mac authentication bypass (MAB) request.

- Once the **Web redirection (CWA, MDM, NSP, CPP)** checked select **Centralized Web Auth**, then Type the Redirect ACL name under **ACL** field and under **Value** select the **Sponsored Guest Portal(default)**(or any other specific portal created in previous steps).

The Profile must look similar the one in this picture. Then click **Save**.



Authorization Profiles > CWA_Redirect

Authorization Profile

* Name: CWA_Redirect

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

▾ Common Tasks

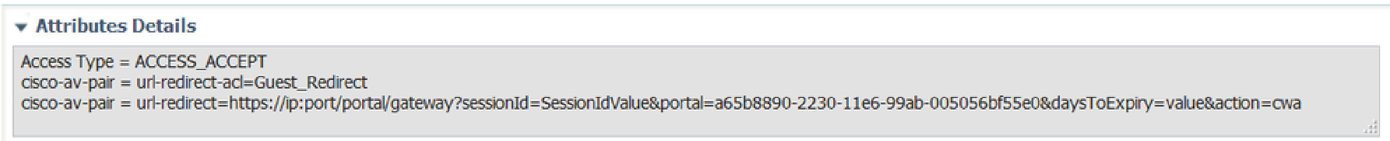
☑ Web Redirection (CWA, MDM, NSP, CPP)

Centralized Web Auth   ACL: Guest_Redirect   Value: onsored Guest Portal (default)

☑ Display Certificates Renewal Message

□ Static IP/Host name/FQDN

Attribute Details at the bottom of the page the Attribute Value Pairs(AVPs) as they are be pushed to the WLC



Attributes Details

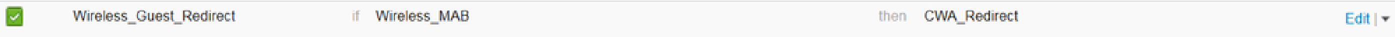
```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=Guest_Redirect
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=a65b8890-2230-11e6-99ab-005056bf55e0&daysToExpiry=value&action=cwa
```

5. Navigate to **Policy > Authorization** and insert a new rule. This rule is the one that triggers the redirect process in response to the initial MAC authentication request from WLC. (In this case called **Wireless_Guest_Redirect**).

6. Under **Conditions** choose **Select Existing Condition from Library**, then under **condition name** select **Compound condition**. Select a pre-defined compound condition called **Wireless_MAB**.

> **Note**: This condition consists of 2 Radius Attributes expected in the Access Request originated form the WLC (NAS-Port-Type= IEEE 802.11 <present in all wireless requests> and Service-Type = Call Check< which refers to an specific request for a mac authentication bypass>)

7. Under results, select **Standard** > **CWA_Redirect** (Authorization profile created in previous step). Then click **Done** and **Save**

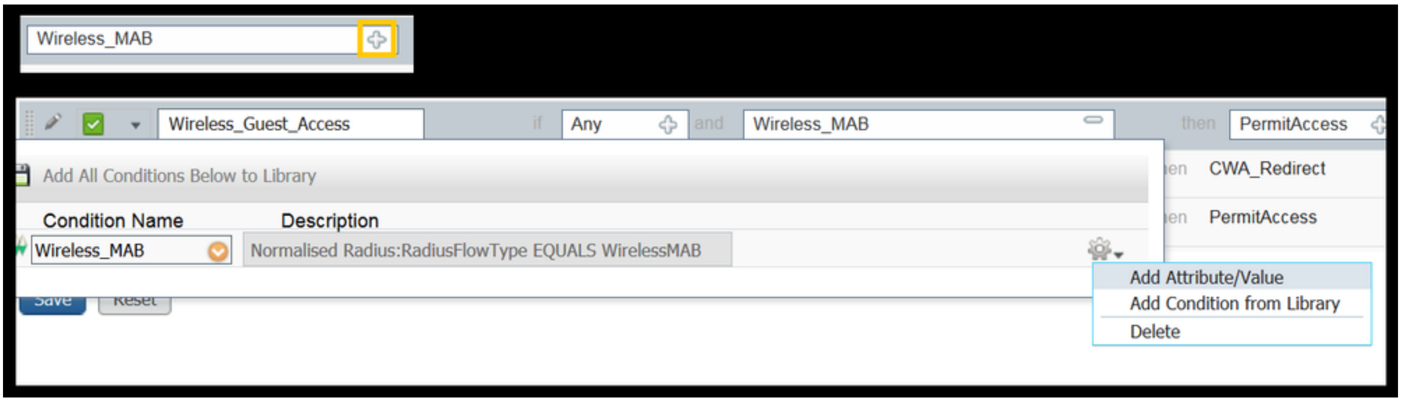


Wireless_Guest_Redirect if Wireless_MAB then CWA_Redirect

8. Navigate to the end of the **CWA_Redirect** rule and click the arrow next to **Edit**. Then select **duplicate above**.

9. Modify the name as this is the policy that the endpoint matches once the session is re-authenticated upon ISE's CoA (In this case Wireless_Guest_Access).

10. Next to **Wireless_MAB** compound condition click the **+** symbol to expand the conditions and by the end of the **Wireless_MAB** condition click **Add Attribute/Value**.



Wireless_MAB

Wireless_Guest_Access if Any and Wireless_MAB then PermitAccess

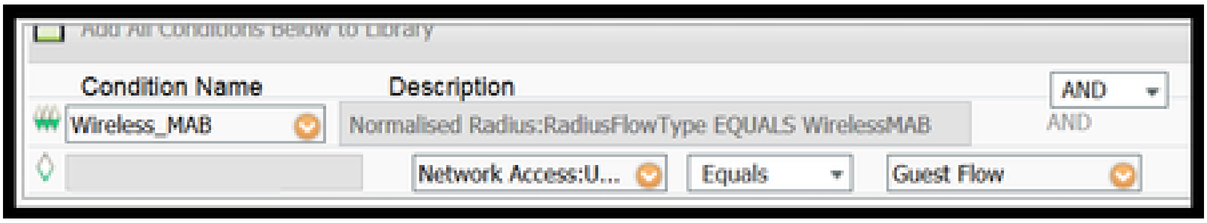
then CWA_Redirect

then PermitAccess

Add All Conditions Below to Library

Condition Name	Description
Wireless_MAB	Normalised Radius:RadiusFlowType EQUALS WirelessMAB

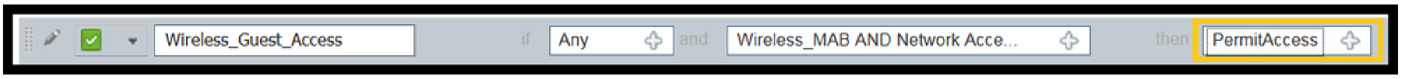
11. Under "Select Attribute" chose **Network Access > UseCase Equals Guest flow**



Add All Conditions Below to Library

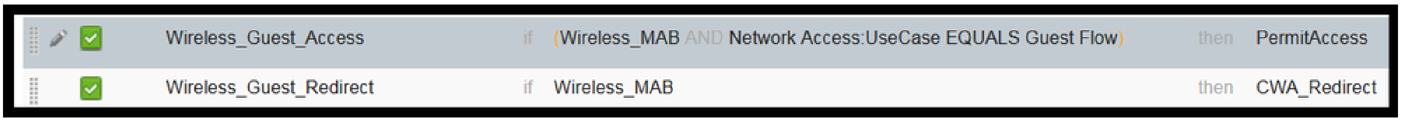
Condition Name	Description	
Wireless_MAB	Normalised Radius:RadiusFlowType EQUALS WirelessMAB	AND
	Network Access:U... Equals Guest Flow	

12. Under **Permissions** select **PermitAccess**. Then click **Done** and **Save**



Wireless_Guest_Access if Any and Wireless_MAB AND Network Acce... then PermitAccess

The two policies must look similar to this:



☑	Wireless_Guest_Access	if	(Wireless_MAB AND Network Access:UseCase EQUALS Guest Flow)	then PermitAccess
☑	Wireless_Guest_Redirect	if	Wireless_MAB	then CWA_Redirect

Use case 2: CWA with Device Registration enforcing guest authentication once a day.

Flow Overview

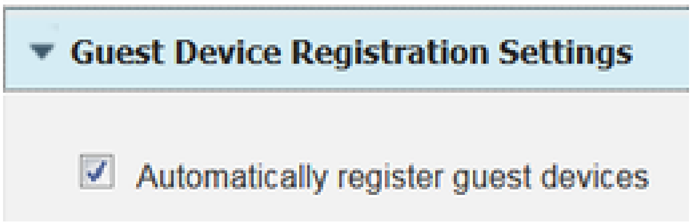
1. Wireless user connects to the Guest SSID.
2. WLC authenticates the endpoint based on its MAC address onISE as AAA server.
3. ISE returns back and access-accept with two Attribute Value Pairs (AVPs) (url-redirect and url-redirect-acl).
4. Once the WLC applies this AVPs to the endpoint session, the station transitions to DHCP-Required and once it grabs an IP address it stays in CENTRAL_WEB_AUTH. At this step the WLC is ready to start redirecting the client's http / https traffic.
5. The End User opens up the web browser and once HTTP or HTTPS traffic is generated, the WLC redirects the user to ISE guest portal.
6. Once the user gets to the Guest Portal, he gets prompted to enter sponsor-created credentials.
7. Upon credentials validation ISE adds this endpoint to a specific (pre-configured) Endpoint Identity Group (Device Registration).
8. AUP page is displayed and once the client accepts, a Dynamic CoA type Re-authenticate. Is sent out to the WLC.
9. The WLC to re-process the MAC filtering authentication without issuing a de-authenticate to the mobile station. This must be seamless to the endpoint.
10. Once the re authentication event happens ISE re-evaluates Authorization policies. This time since the endpoint is member of the right Endpoint Identity Group ISE returns an access accept with no restrictions.
11. Since the endpoint has been registered in step 6, each time that the user comes back, he is allowed on the network until it is removed manually from ISE, or an Endpoint Purge Policy runs flushing the endpoints meeting the criteria.

In this lab scenario, authentication is enforced once a day. Re-authentication trigger is Endpoint Purge Policy that removes all the endpoints of the used Endpoint Identity Group every day.

> **Note**: It is possible to enforce the guest authentication event based on Elapsed time since last AUP acceptance. This canbe an option if you need to enforce Guest Logon more often that once a day (in example every 4 hours).

Configuration

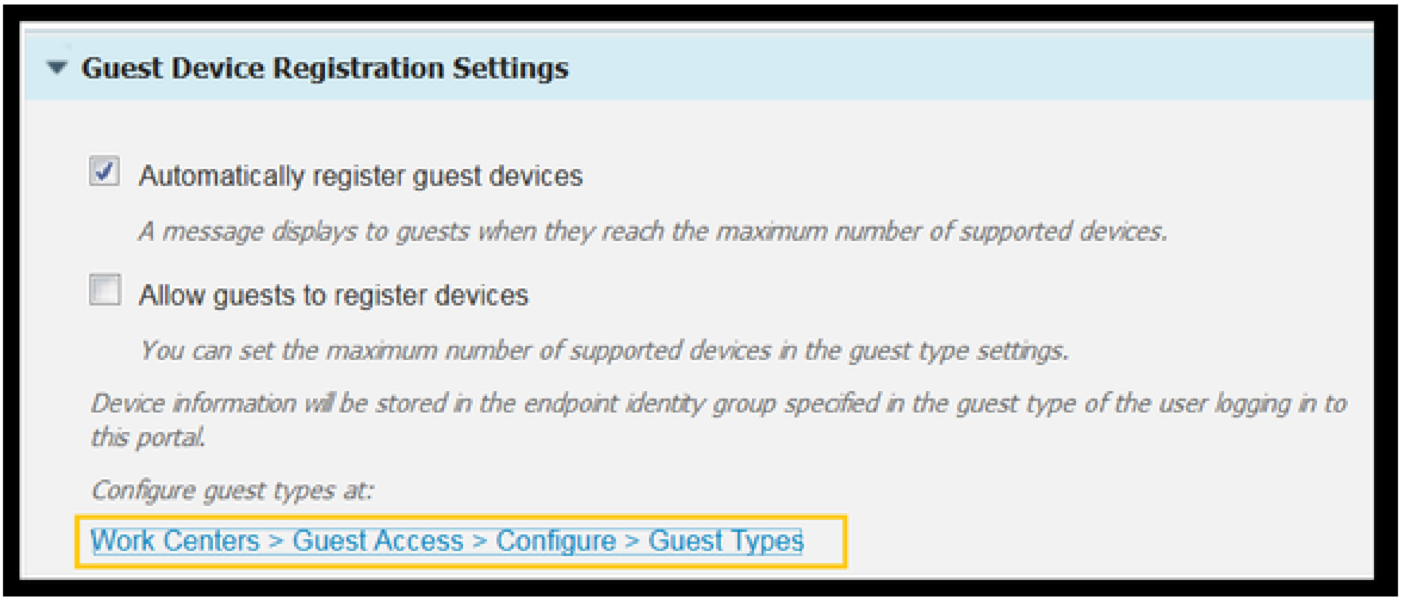
1. On ISE navigate to **Work Centers > Guest Access > Configure > Guest Portals** > Select **Sponsored Guest Portal** (or create a new portal type Sponsored-Guest).
2. Under **Guest Device Registration** settings verify that option **Automatically register guest devices** is checked. Click **Save**.



▾ Guest Device Registration Settings

☑ Automatically register guest devices

3. Navigate to **Work center > Guest Access > Configure > Guest Types** or just click on the shortcut specified under Guest Device Registration Settings in the portal.



▾ Guest Device Registration Settings

☑ Automatically register guest devices

A message displays to guests when they reach the maximum number of supported devices.

□ Allow guests to register devices

You can set the maximum number of supported devices in the guest type settings.

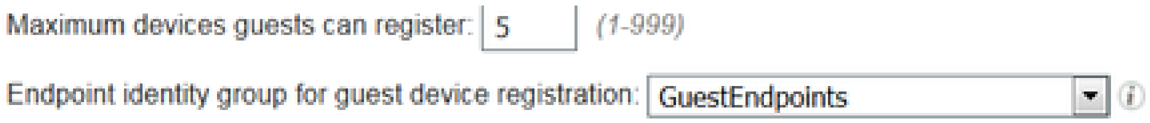
Device information will be stored in the endpoint identity group specified in the guest type of the user logging in to this portal.

Configure guest types at:

Work Centers > Guest Access > Configure > Guest Types

4. When the Sponsor User creates a guest account, he assigns a guest type to it. Each individual Guest Type can have a registered endpoint that belongs to a different Endpoint Identity Group.To assign the Endpoint Identity Group the device must be added to, select the Guest Type the sponsor uses for these guest users (This use case is based on Weekly (default)).

5. Once in the guest type, under **Login Options** select the Endpoint Group from the drop down menu **Endpoint Identity group for guest device registration**



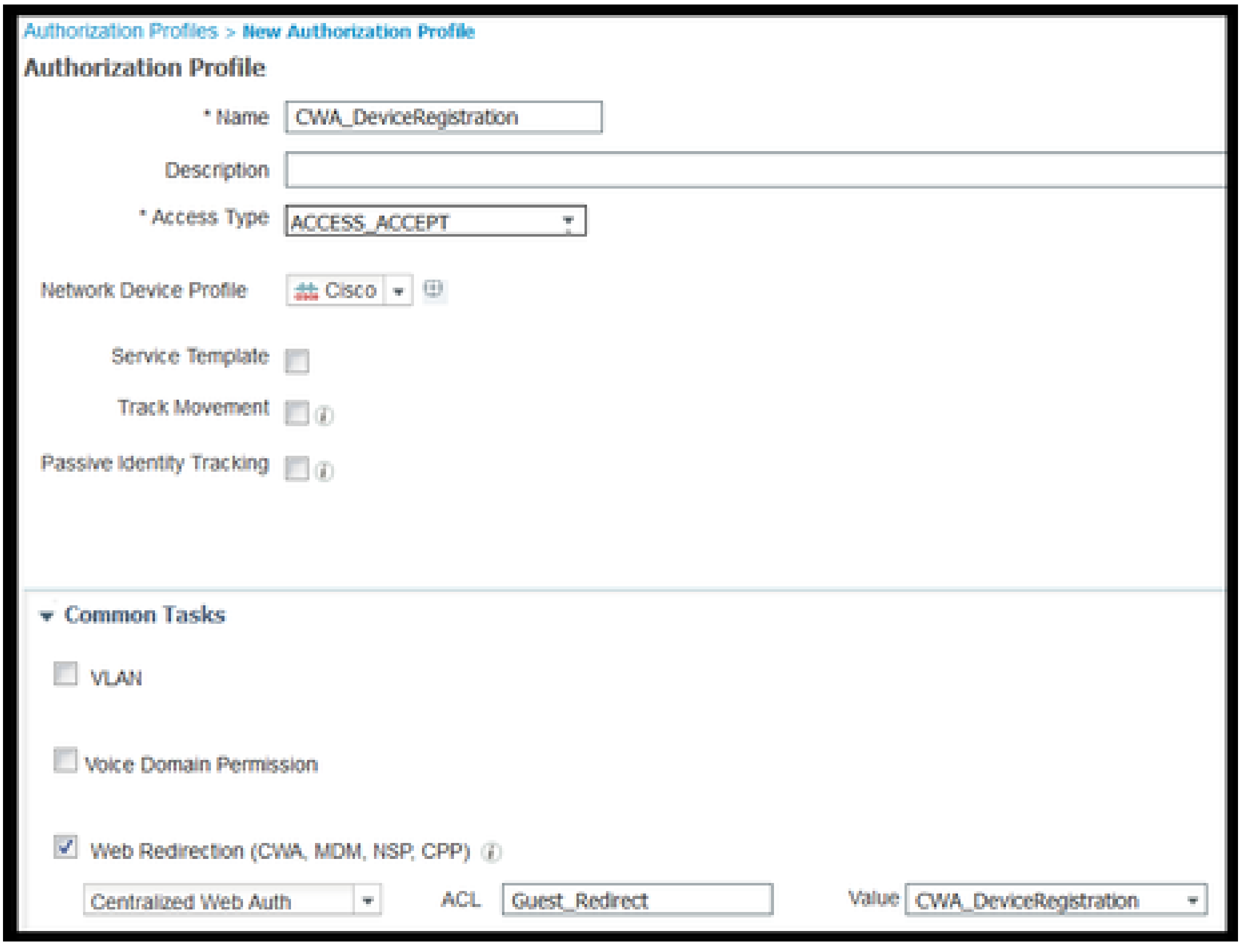
Maximum devices guests can register: 5 *(1-999)*

Endpoint identity group for guest device registration: GuestEndpoints

6. Navigate to **Policy > Policy Elements > Results > Authorization > Authorization Profiles**. Click **Add**.

7. This profile is pushed down to the WLC the **Redirect-URL** and the **Redirect-URL-ACL** in response to the initial Mac authentication bypass (MAB) request.

- Once the **Web redirection (CWA, MDM, NSP, CPP)** checked select **Centralized Web Auth**, then Type the Redirect ACL name under **ACL** field and under **Value** select the portal created for this flow (**CWA_DeviceRegistration**).


Authorization Profiles > New Authorization Profile

Authorization Profile

* Name: CWA_DeviceRegistration

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

Common Tasks

□ VLAN

□ Voice Domain Permission

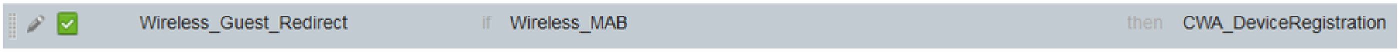
☑ Web Redirection (CWA, MDM, NSP, CPP)

Centralized Web Auth — ACL: Guest_Redirect — Value: CWA_DeviceRegistration

8. Navigate to **Policy > Authorization** and insert a new rule. This rule is the one that triggers the redirect process in response to the initial MAC authentication request from WLC. (In this case called **Wireless_Guest_Redirect**).

9. Under **Conditions** chose **Select Existing Condition from Library**, then under **condition name** select **Compound condition**. Select a pre-defined compound condition called **Wireless_MAB**.

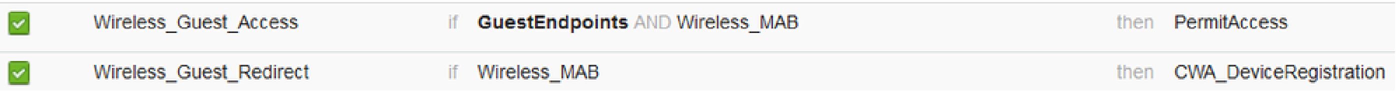
10. Under results, select **Standard** > **CWA_DeviceRegistration** (Authorization profile created in previous step). Then click **Done** and **Save**


☑ Wireless_Guest_Redirect if Wireless_MAB then CWA_DeviceRegistration

11. Duplicate the policy above, modify its name as this is the policy the endpoint hits after it returns from the re-authentication event (called Wireless_Guest_Access).

12. Under **Identity Group Details** box, select **Endpoint Identity Group** and select the group you referenced under the Guest Type(GuestEndpoints).

13. Under Results select **PermitAccess**. Click **Done** and **Save** the changes.


☑ Wireless_Guest_Access if **GuestEndpoints** AND Wireless_MAB then PermitAccess

☑ Wireless_Guest_Redirect if Wireless_MAB then CWA_DeviceRegistration

14. Create and endpoint purge policy that clears the GuestEndpoint Group daily.

- Navigate to **Administration** > **Identity management** > **Settings** > **Endpoint Purge**

- Under **Purge** rules there must be one by default that triggers GuestEndpoints deletion if Elapsed Time is greater than 30 days.
- Modify the existing policy for GuestEndpoints or create a new one (in case the default has been removed). Note that the purge policies run every day a defined time.

In this case the condition is Members of GuestEndpoints with Elapsed Days less than 1 day

Use case 3: HostSpot portal

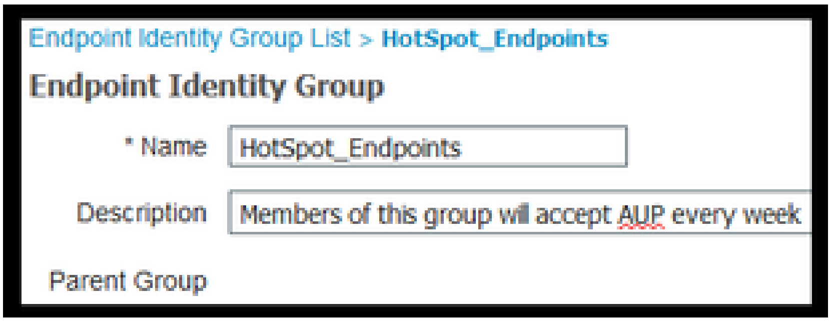
Flow Overview

1. Wireless user connects to the Guest SSID.
2. WLC authenticates the endpoint based on its MAC address using ISE as AAA server.
3. ISE returns back an access-accept with two Attribute Value Pairs (AVPs): url-redirect and url-redirect-acl.
4. Once the WLC applies this AVPs to the endpoint session, the station transitions to DHCP-Required and once it grabs an IP address it stays in CENTRAL_WEB_AUTH. At this step the WLC is ready to redirect the client's http / https traffic.
5. The End User opens up the web browser and once HTTP or HTTPS traffic is generated, the WLC redirects the user to ISE HotSpot Portal.
6. Once in the portal the user is prompted to accept an Acceptable Use Policy.
7. ISE adds the endpoint MAC address (Endpoint ID) into the configured Endpoint Identity group.
8. The Policy Services Node (PSN) that processes the request issues a Dynamic CoA type **Admin-Reset** to the WLC.
9. Once the WLC finishes processing the incoming CoA, it issues a de-authenticate to the client(connection is loss for time it takes for the client to come back).
10. Once the client reconnects, a new session is created so there is no session continuity on ISE side. It means that the authentication is processed as a new thread.
11. Since the endpoint is added to the configured Endpoint Identity Group, and there is an Authorization policy that checks if the endpoint is part of that group, the new authentication matches this policy. The result is full access to the Guest network.
12. The user must not have to accept the AUP again unless the Endpoint Identity Object is purged from ISE database as a result of an endpoint purge policy.

Configuration

1. Create a New Endpoint Identity Group to move these devices to upon registration. Navigate to **Work Centers > Guest Access > Identity Groups > Endpoint Identity Groups** and click ✚Add .

- Enter a group name (In this case HotSpot_Endpoints). Add a description and no Parent Group is needed.



Endpoint Identity Group List > HotSpot_Endpoints

Endpoint Identity Group

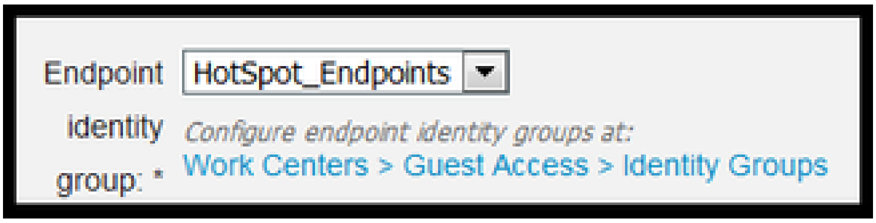
* Name: HotSpot_Endpoints

Description: Members of this group will accept AUP every week

Parent Group

2. Navigate to **Work Centers > Guest Access > Configure > Guest Portals** > select **Hotspot Portal (default**).

3. Expand Portal Settings and under Endpoint Identity Group select **HostSpot_Endpoints** group under **Endpoint Identity Group.** This sends the registered devices to the specified group.



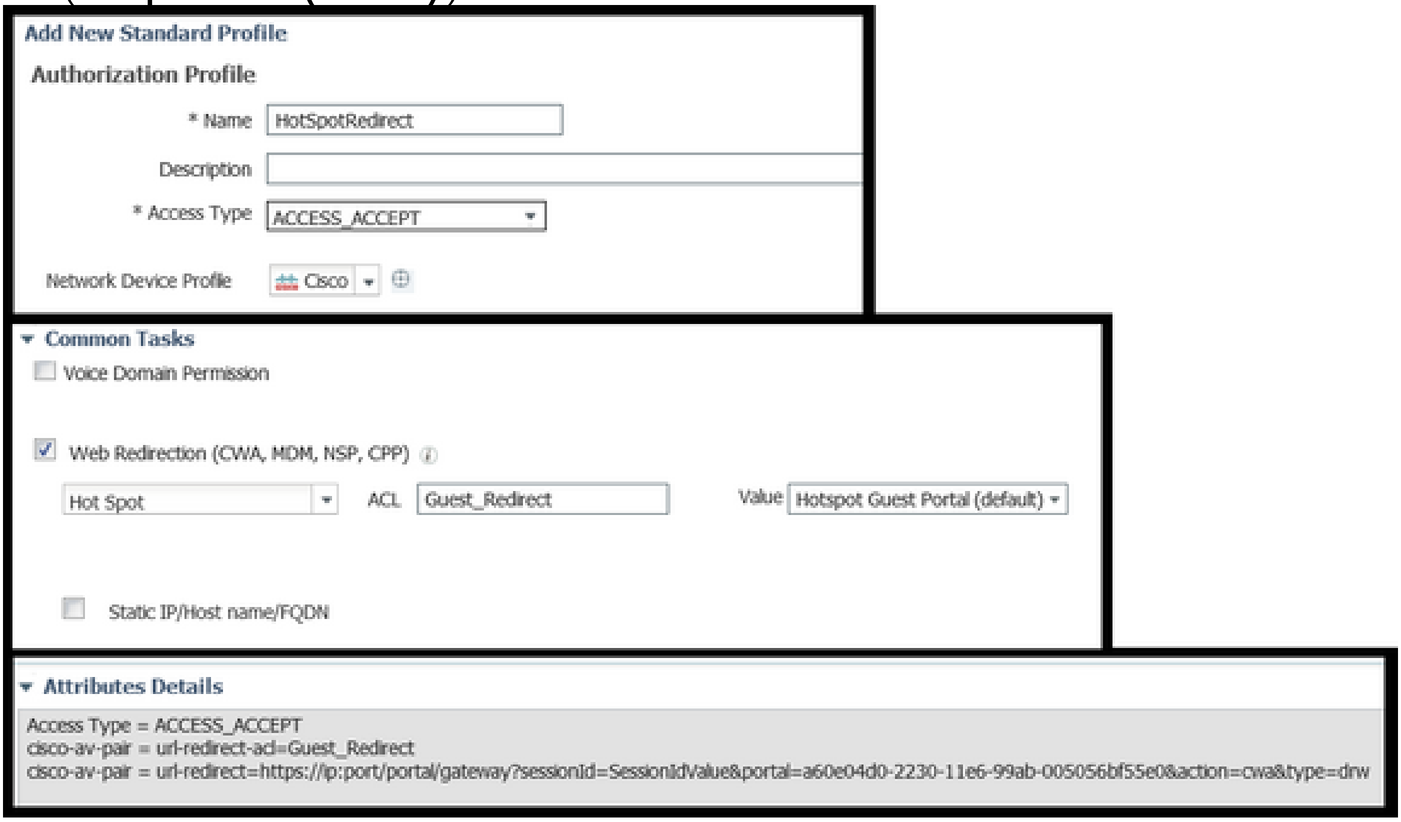
Endpoint identity group: * HotSpot_Endpoints

Configure endpoint identity groups at:
Work Centers > Guest Access > Identity Groups

4**. Save** the changes.

5. Create the Authorization profile that calls the HotSpot Portal upon MAB authentication originated by the WLC.

- Navigate to **Policy > Policy elements > Results > authorization > Authorization Profiles** and create one (HotSpotRedirect).
- Once the **Web redirection (CWA, MDM, NSP, CPP)** is checked select **Hot Spot**, then type the Redirect ACL name in ACL field (Guest_Redirect) and as a Value select correct portal (**Hotspot Portal (default)**).



Add New Standard Profile

Authorization Profile

* Name: HotSpotRedirect

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Common Tasks

□ Voice Domain Permission

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

Hot Spot — ACL: Guest_Redirect — Value: Hotspot Guest Portal (default)

□ Static IP/Host name/FQDN

Attributes Details

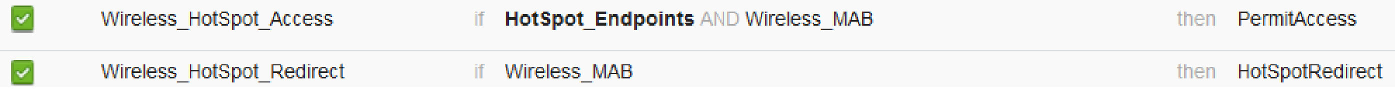
```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=Guest_Redirect
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=a60e04d0-2230-11e6-99ab-005056bf55e0&action=cwa&type=drw
```

6. Create the Authorization Policy that triggers the HotSpotRedirect result upon initial MAB request from WLC.

- Navigate to **Policy > Authorization** and insert a new rule. This rule is the one that triggers the redirect process in response to the initial MAC authentication request from WLC. (In this case called **Wireless_HotSpot_Redirect**).
- Under **Conditions** choose **Select Existing Condition from Library**, then under **condition name** select **Compound condition**
- Under results, select **Standard** > **HotSpotRedirect** (Authorization profile created in previous step). Then click **Done** and **Save**

7. Create the second Authorization Policy.

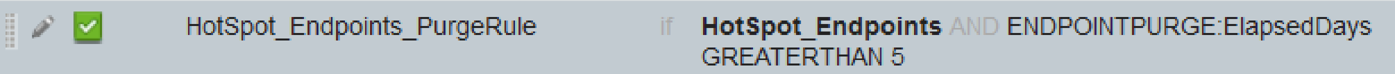
- Duplicate the policy above, modify its name as this is the policy the endpoint hits after it returns from the re-authentication event (called Wireless_HotSpot_Access).
- Under **Identity Group Details** box, select **Endpoint Identity Group** and then the group you created earlier (**HotSpot_Endpoints**).
- Under Results select **PermitAccess**. Click **Done** and **Save** the changes.



☑	Wireless_HotSpot_Access	if	**HotSpot_Endpoints** AND Wireless_MAB	then	PermitAccess
☑	Wireless_HotSpot_Redirect	if	Wireless_MAB	then	HotSpotRedirect

8. Configure the purge policy that clears endpoints with an Elapsed time greater than 5 days.

- Navigate to **Administration > Identity Management > Settings > Endpoint Purge** and under Purge rules create a new one.
- Under **Identity Group Details** box select **Endpoint Identity Group > HotSpot_Endpoints**
- Under **conditions** click **Create New Condition (Advanced Option)** .
- Under Select Attribute choose *ENDPOINTPURGE : ElapsedDays GREATERTHAN* 5 days

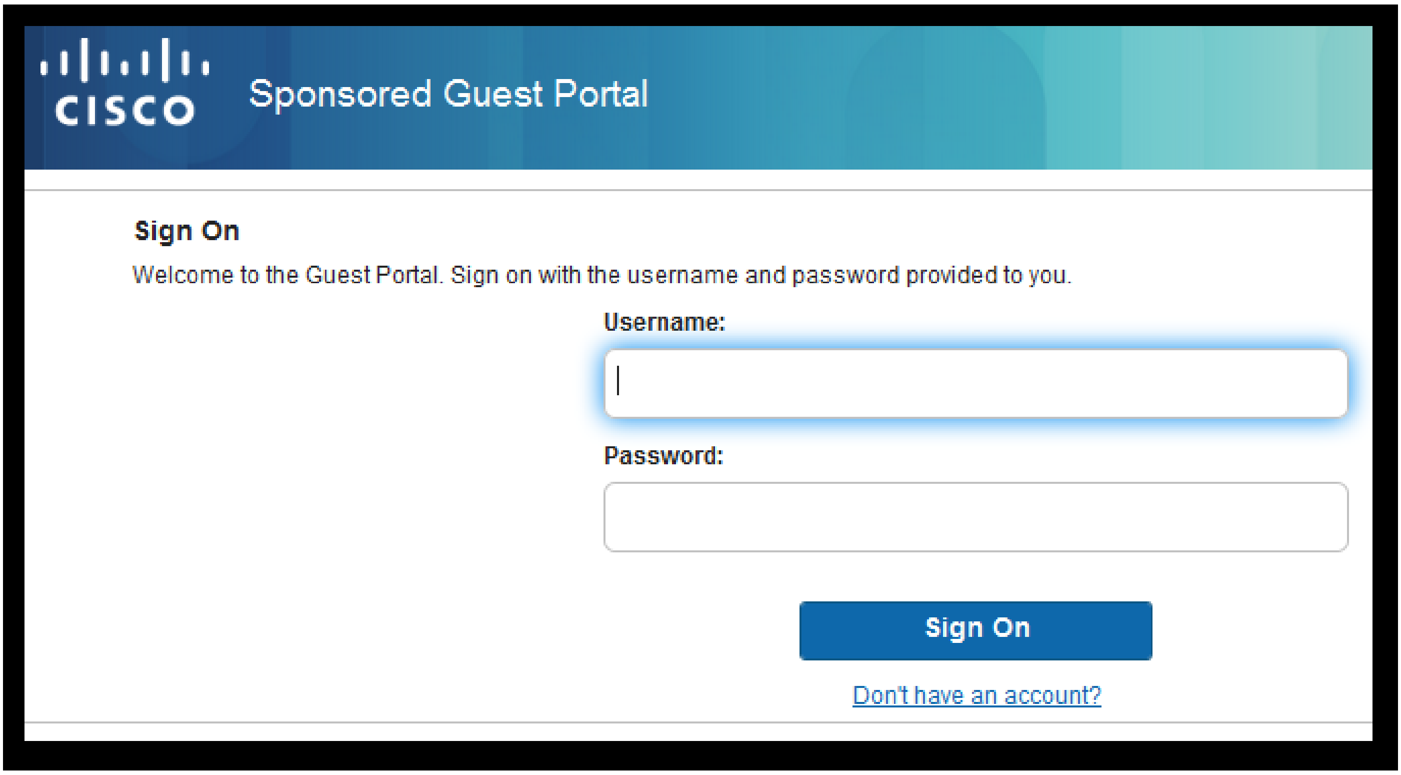


☑	HotSpot_Endpoints_PurgeRule	if	**HotSpot_Endpoints** AND ENDPOINTPURGE:ElapsedDays GREATERTHAN 5

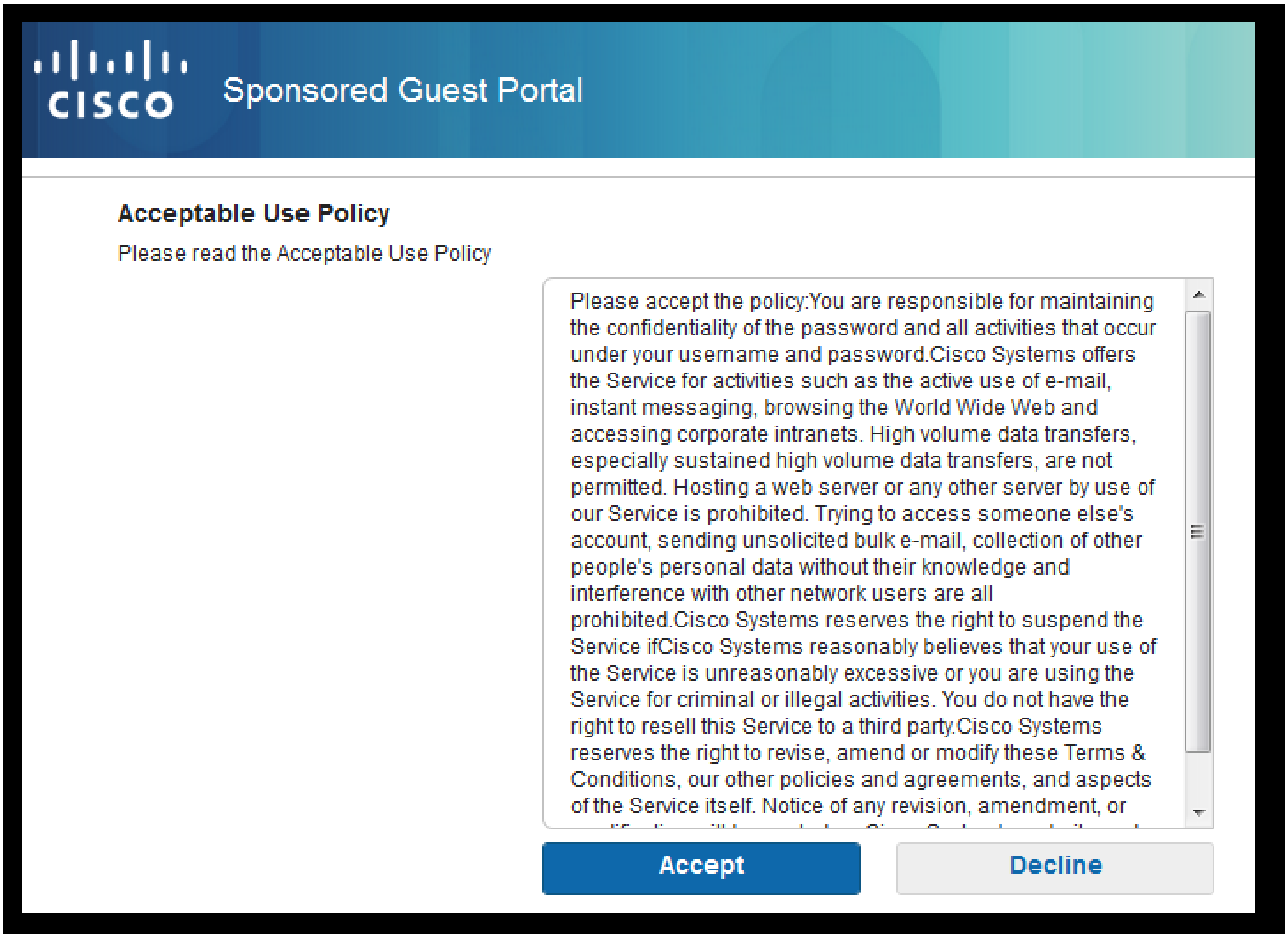
Verify

Use Case 1

1. User connects to the Guest SSID.
2. He opens the browser and as soon as HTTP traffic is generated, the guest portal is displayed.
3. Once the guest user authenticates and accepts the AUP, a success page is displayed.
4. A Re-authenticate CoA is sent out (transparent to the client).
5. The endpoint session is re-authenticated with full access to the network.
6. Any subsequent guest connection has to pass the guest authentication before gaining access to the network.

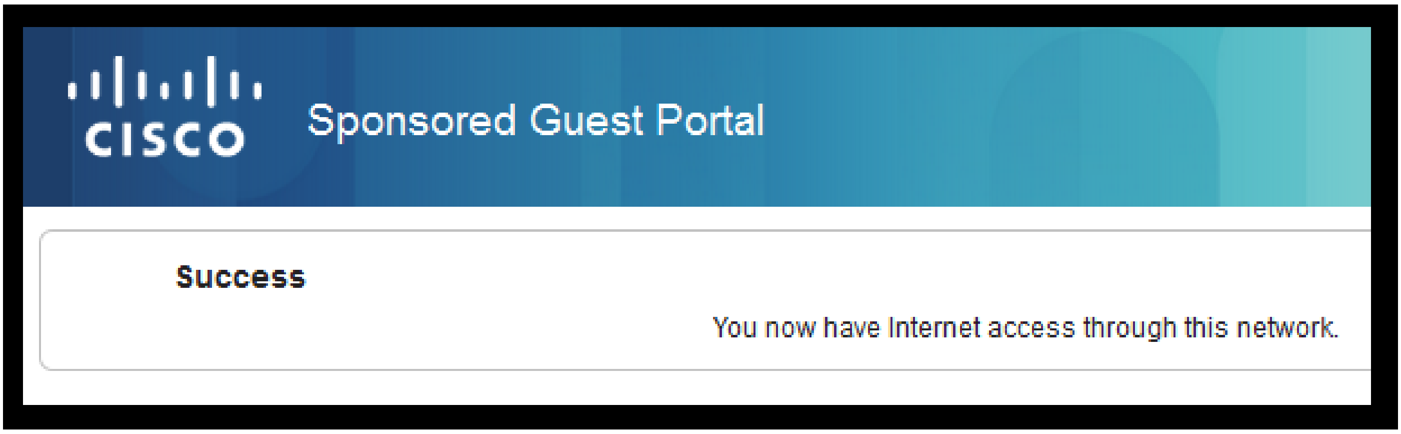


Welcome to the Guest Portal. Sign on with the username and password provided to you.



Please read the Acceptable Use Policy

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited.Cisco Systems reserves the right to suspend the Service ifCisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party.Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or

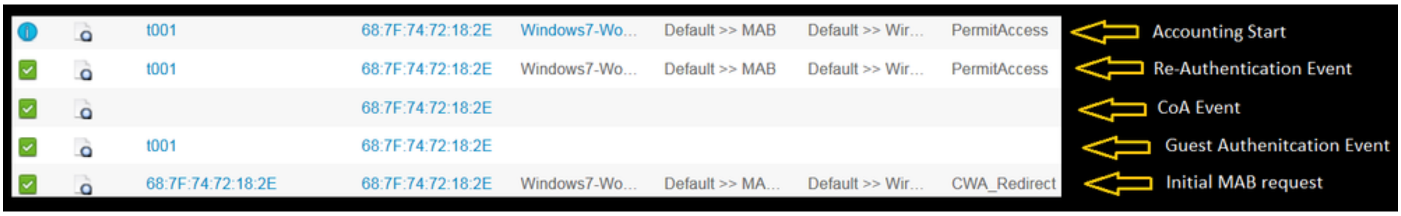


Sponsored Guest Portal

Success

You now have Internet access through this network.

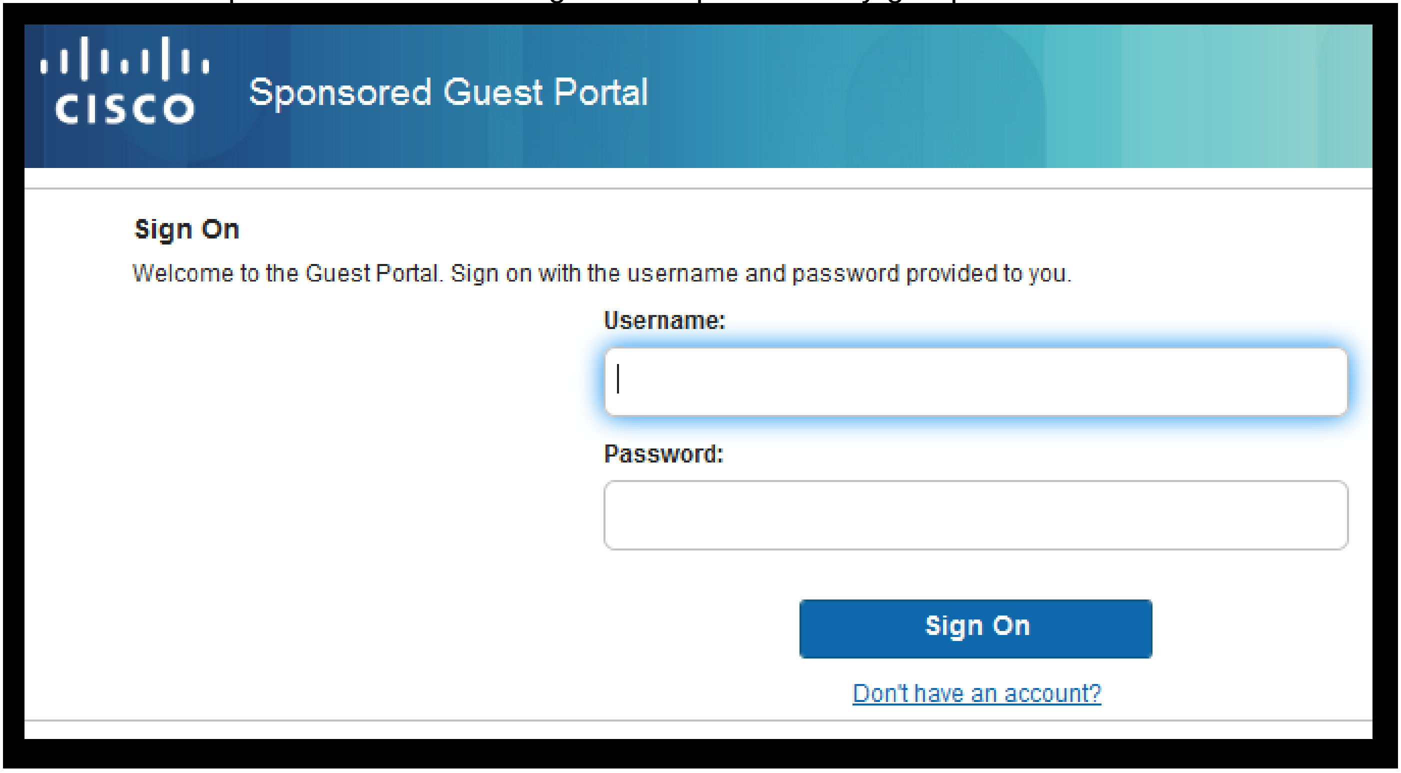
Flow from ISE RADIUS Live logs:



ⓘ	t001	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MAB	Default >> Wir...	PermitAccess	⇦	Accounting Start
☑	t001	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MAB	Default >> Wir...	PermitAccess	⇦	Re-Authentication Event
☑		68:7F:74:72:18:2E					⇦	CoA Event
☑	t001	68:7F:74:72:18:2E					⇦	Guest Authenitcation Event
☑	68:7F:74:72:18:2E	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MA...	Default >> Wir...	CWA_Redirect	⇦	Initial MAB request

Use Case 2

1. User connects to the Guest SSID.
2. He opens the browser and as soon as HTTP traffic is generated, the guest portal is displayed.
3. Once the guest user authenticates and accepts the AUP, the device is registered.
4. A success page is displayed and a Re-authenticate CoA is sent out (transparent to the client).
5. The endpoint session is re-authenticated with full access to the network.
6. Any subsequent gust connection 9s allowed without enforcing guest authentication as long as the endpoint is still in the configured Endpoint Identity group.



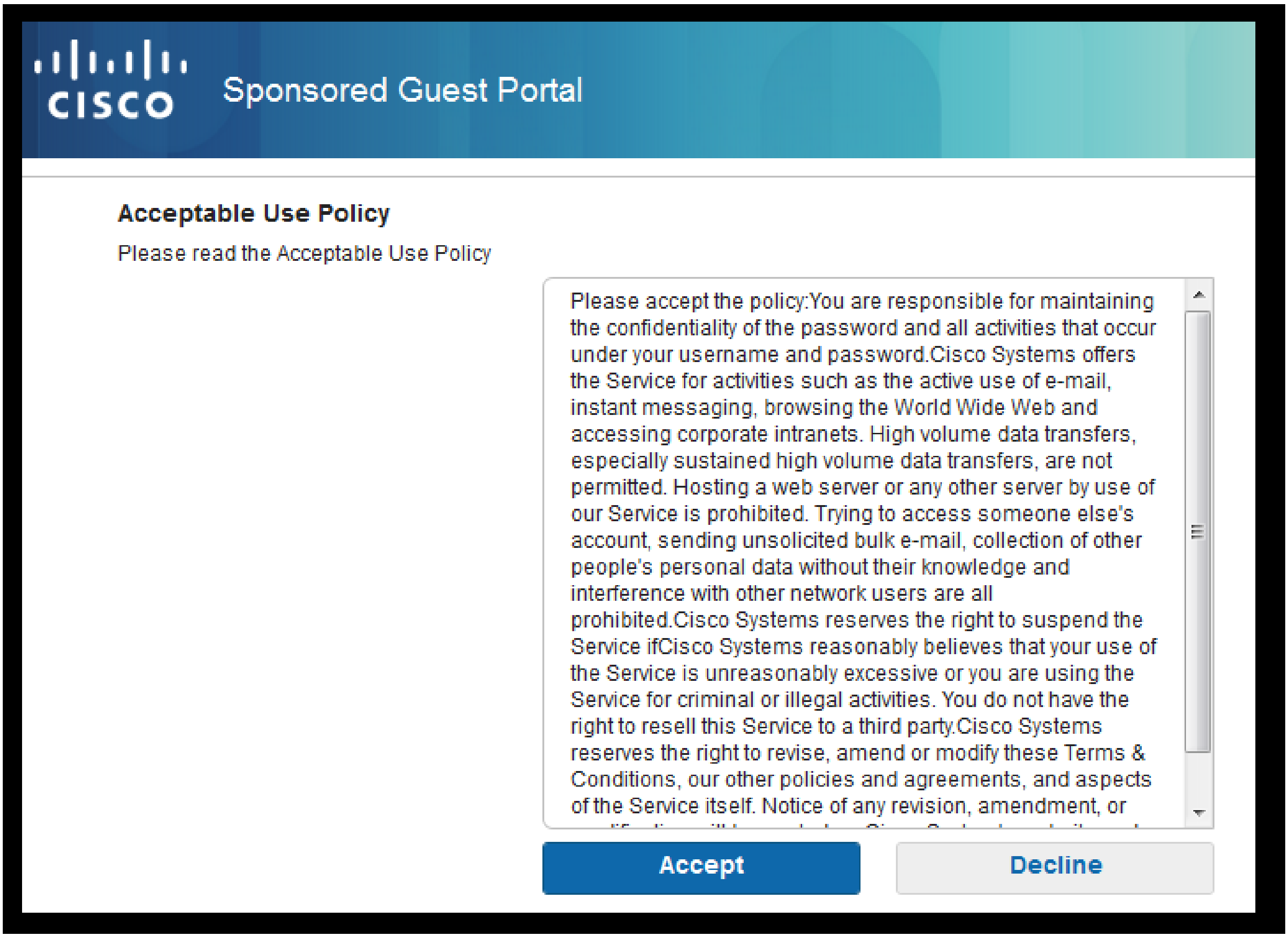
Sponsored Guest Portal

Sign On

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

Username:

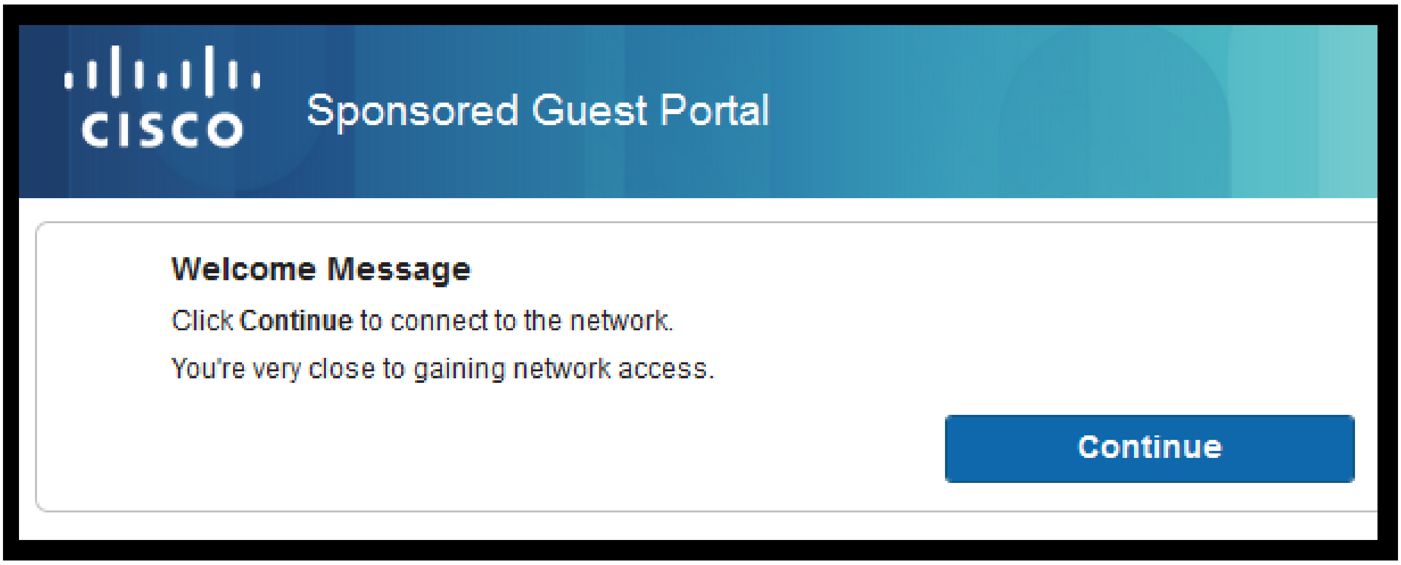
Password:



Acceptable Use Policy

Please read the Acceptable Use Policy

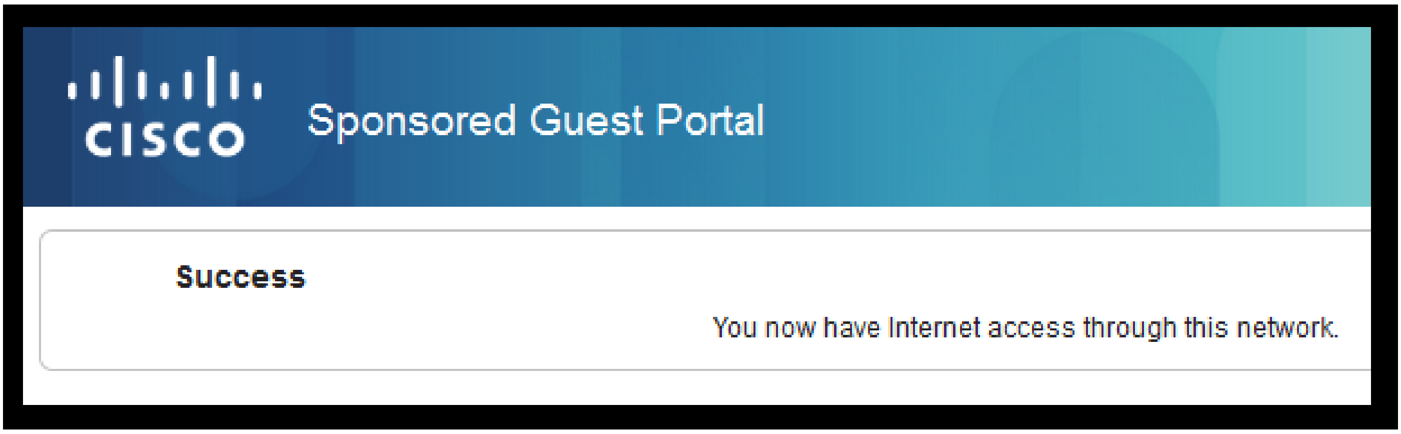
Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited.Cisco Systems reserves the right to suspend the Service ifCisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party.Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or



Welcome Message

Click **Continue** to connect to the network.

You're very close to gaining network access.

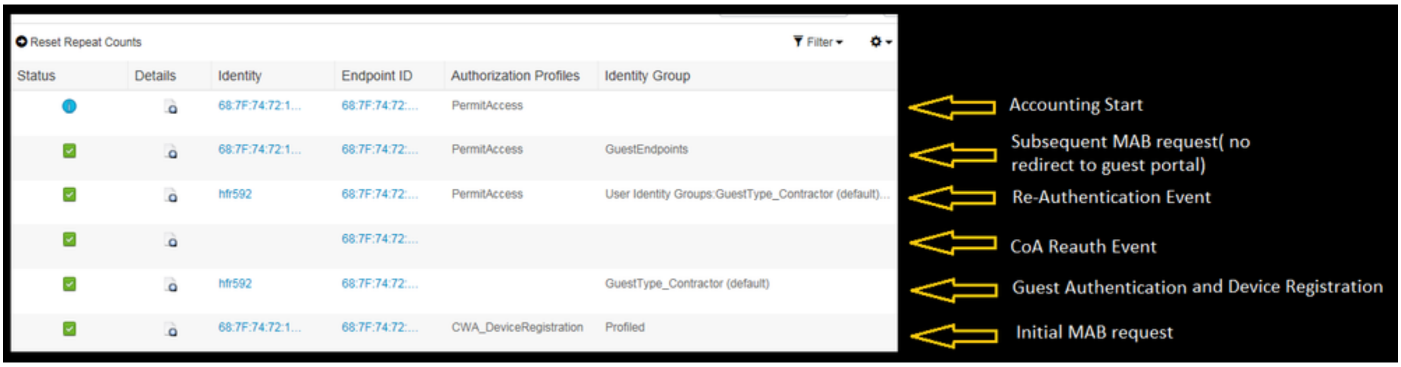


Sponsored Guest Portal

Success

You now have Internet access through this network.

Flow from ISE RADIUS Live logs:



Status	Details	Identity	Endpoint ID	Authorization Profiles	Identity Group
●		68:7F:74:72:1...	68:7F:74:72:...	PermitAccess	
✓		68:7F:74:72:1...	68:7F:74:72:...	PermitAccess	GuestEndpoints
✓		hfr592	68:7F:74:72:...	PermitAccess	User Identity Groups:GuestType_Contractor (default)...
✓			68:7F:74:72:...		
✓		hfr592	68:7F:74:72:...		GuestType_Contractor (default)
✓		68:7F:74:72:1...	68:7F:74:72:...	CWA_DeviceRegistration	Profiled

Accounting Start

Subsequent MAB request(no redirect to guest portal)

Re-Authentication Event

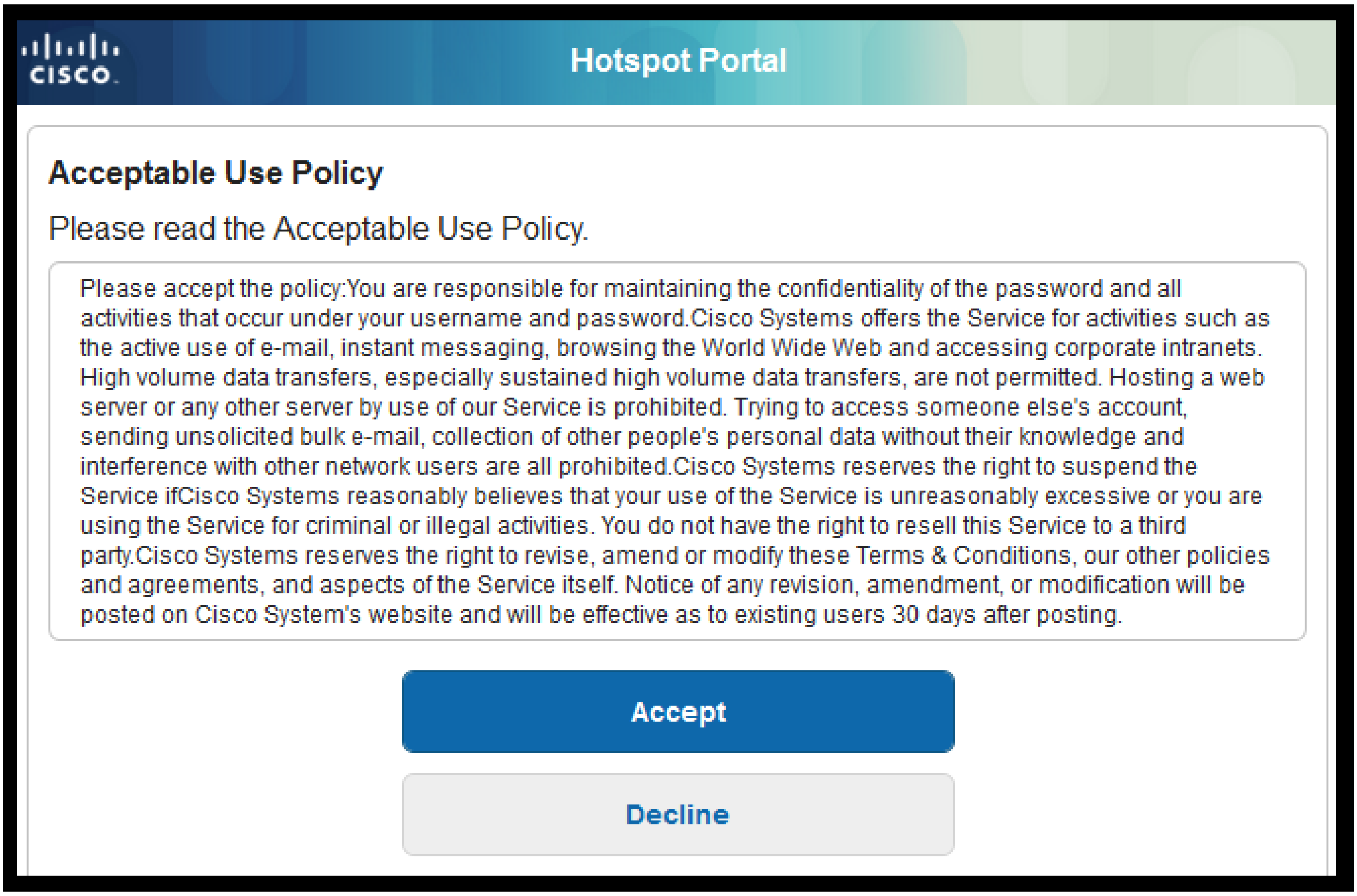
CoA Reauth Event

Guest Authentication and Device Registration

Initial MAB request

Use Case 3

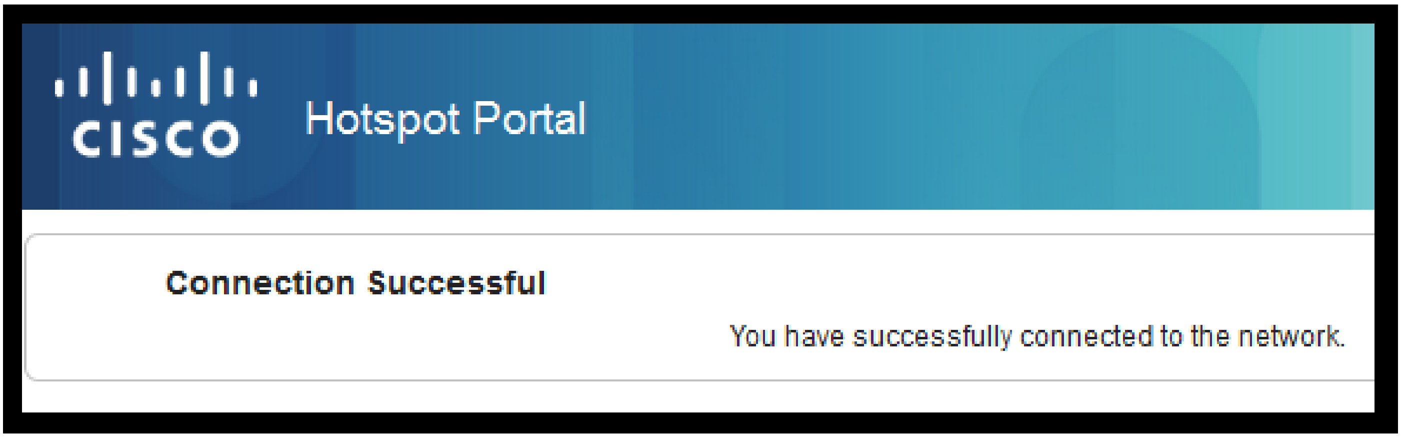
1. User connects to the Guest SSID.
2. He opens the browser and as soon as HTTP traffic is generated, an AUP page is displayed.
3. Once the guest user accepts the AUP, the device is registered.
4. A success page is displayed and an Admin-Reset CoA is sent out (transparent to the client).
5. The endpoint re-connects with full access to the network.
6. Any subsequent gust connection is allowed without enforcing AUP acceptance (unless otherwise is configured) for as long as the endpoint remains in the configured Endpoint Identity group.



Acceptable Use Policy

Please read the Acceptable Use Policy.

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited.Cisco Systems reserves the right to suspend the Service ifCisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party.Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.



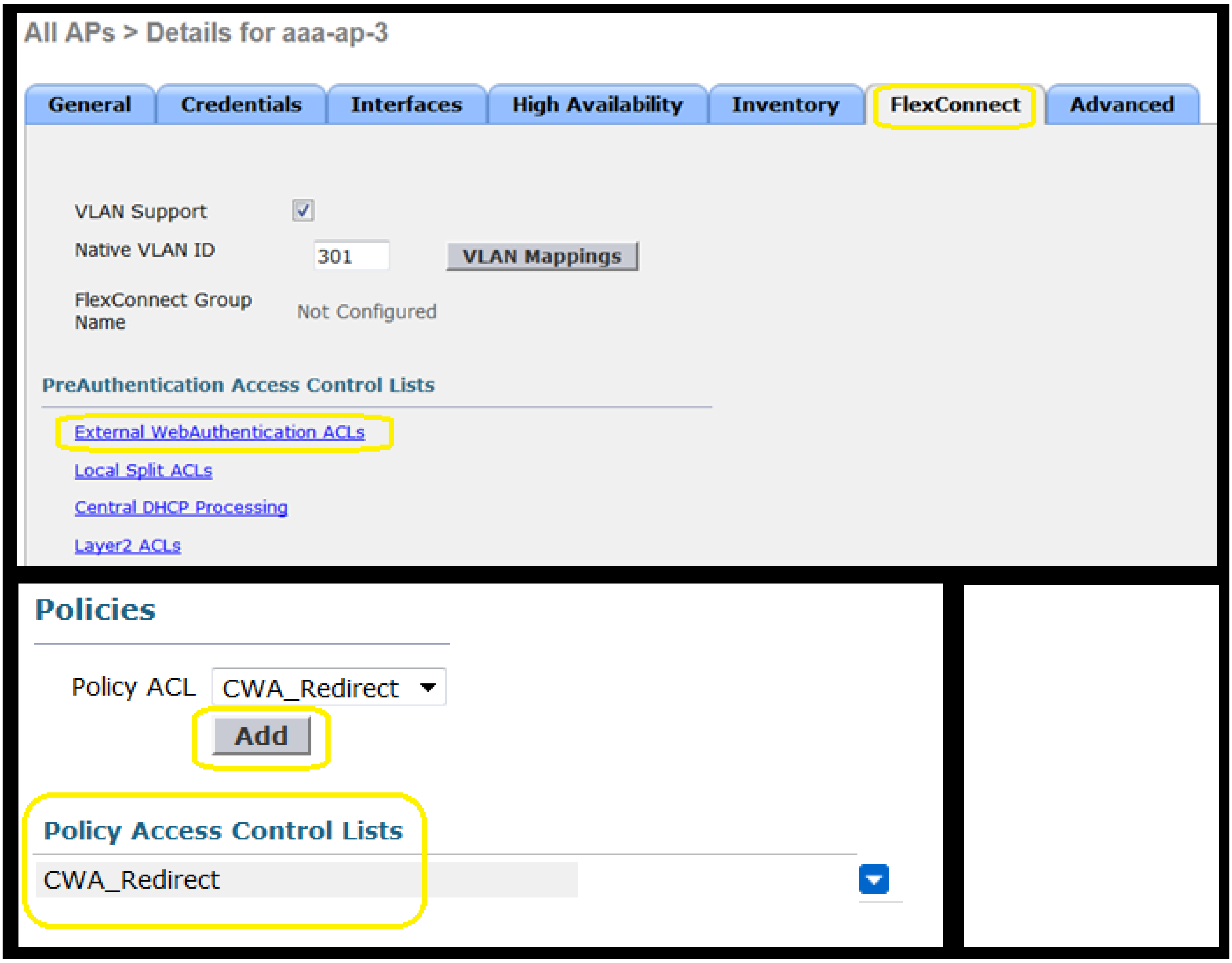
Connection Successful

You have successfully connected to the network.

FlexConnect Local switching in AireOS

When FlexConnect local switching is configured the Network Admin needs to ensure that:

- Redirect ACL is configured as a FlexConnect ACL.
- Redirect ACL has been applied as a policy either way through The AP itself under **FlexConnect** Tab > **External WebAuthentication ACLs** > **Policies** > Select Redirect ACL and click **Apply**



All APs > Details for aaa-ap-3

VLAN Support ☑

Native VLAN ID 301

FlexConnect Group Name Not Configured

PreAuthentication Access Control Lists

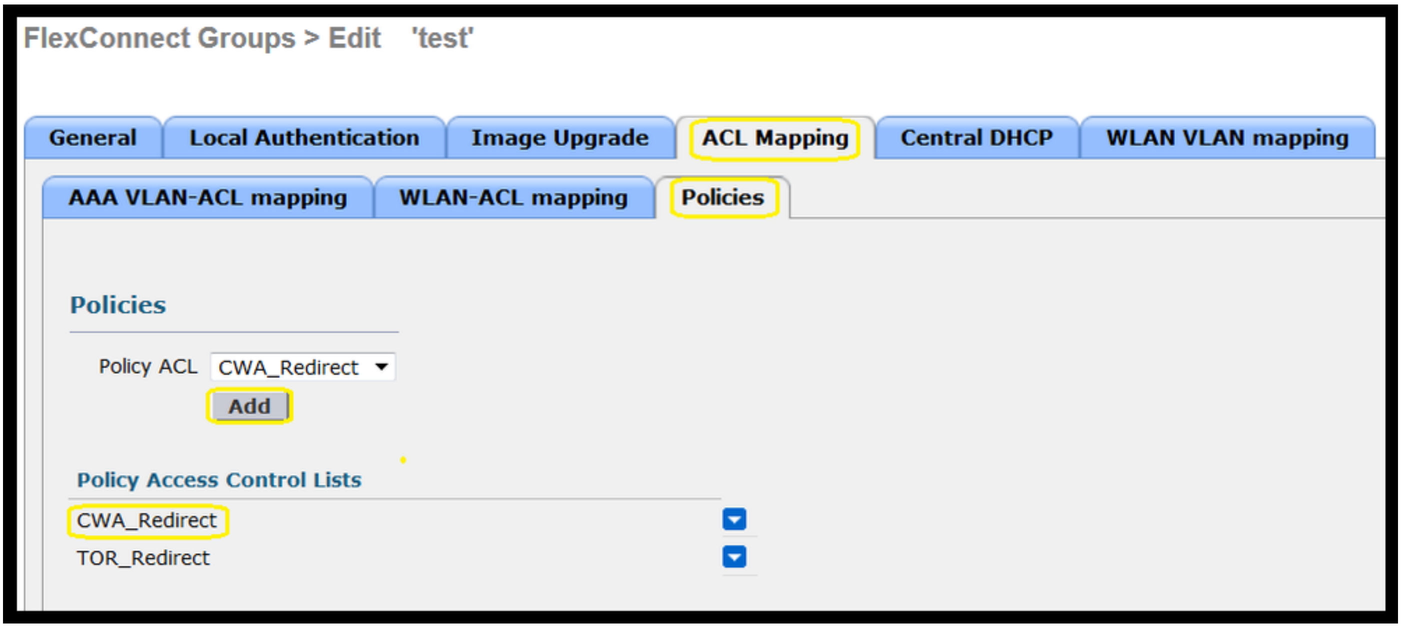
Policies

Policy ACL CWA_Redirect

Policy Access Control Lists

CWA_Redirect

Or by adding the Policy ACL to the FlexConnect Group belongs to (**Wireless > FlexConnect Groups >** Select the correct group > **ACL Mapping > Policies** Select the Redirect ACL and click Add)



FlexConnect Groups > Edit 'test'

Policies

Policy ACL CWA_Redirect

Policy Access Control Lists

CWA_Redirect

TOR_Redirect

Policy ACL addition triggers the WLC to push configured ACL down to the AP(s) members of the FlexConnect Group. Failure to do this results in a web redirect issue.

Foreign-Anchor Scenario

In auto-anchor (Foreign–Anchor) scenarios it is important to highlight these facts:

- Redirect ACL needs to be defined on both the Foreign and the Anchor WLC. Even when it is only enforced on the Anchor.
- Layer 2 Authentication is always handled by the Foreign WLC. This is critical during design phases (also for troubleshooting) as all the RADIUS authentication and accounting traffic occurs between ISE and the foreign WLC.

- Once the Redirect AVPs are applied to the client session the Foreign WLC updates the client session in the Anchor through a mobility handoff message.
- At this point the Anchor WLC starts to enforce the Redirect using the Redirect-ACL that has been pre-configured.
- Accounting must be completely turned off on the Anchor WLC SSID to avoid accounting updates towards ISE (referencing the same authentication event) coming both from the Anchor and Foreign.
- URL based ACLs are not supported in Foreign-Anchor scenarios.

Troubleshoot

Common broken states on both AireOS and Converged Access WLC

1. **Client is unable to join the Guest SSID**

A "**show client detailed xx:xx:xx:xx:xx:xx**" reveals that the client is stuck in **START**. Usually this is an indicator of the WLC unable to apply an attribute that the AAA server returns.

Verify that the Redirect ACL name pushed by ISE matches exactly the name of the pre-defined ACL on the WLC.

The same principle applies to any other attribute that you have configured ISE to push down to the WLC (VLAN IDs, Interface Names, Airespace-ACLs). The client must then transition to DHCP and then CENTRAL_WEB_AUTH.

2. **Redirect AVPs are applied to the client's session but redirect is not working**

Verify that the client's policy manager state is CENTRAL_WEB_AUTH with a valid IP address aligned to the configured dynamic interface for the SSID and also that the Redirect ACL and URL-Redirect attributes are applied to the client's session.

Redirect ACL

In AIreOS WLCs the redirect ACL must explicitly allow the traffic that must not be redirected, like DNS and ISE on TCP Port 8443 in both directions and the implicit deny ip any any triggers the rest of the traffic to be redirected.

In Converged access the logic is the opposite. Deny ACEs bypasses redirect while permit ACEs triggers the redirect. This is why it is recommended to explicitly permit TCP port 80 and 443.

Verify access to ISE over port 8443 from guest VLAN. If everything looks good from configuration perspective the easiest way to move forward is to grab a capture behind the client's wireless adapter and verify where the redirect breaks.

- Does DNS resoultion happen?
- Is TCP 3 way handshake finished against the requested page?
- Does the WLC return a redirect action after client initiates the GET?
- Is the TCP 3 way handshake against ISE over 8443 completed?

3. **Client is unable to access the network after ISE pushed a VLAN change at the end of the guest flow**

Once the client grabbed an IP address at the beginning of the flow (Pre Redirect state), if a VLAN change is pushed down after Guest authentication happens (post CoA re-authenticate), the only way to force a DHCP release / renew in Guest flow (without posture agent) is through a java applet that in mobile devices do not work.

This leaves the client black-holed in VLAN X with an IP address of VLAN Y. This must be considered while planning the solution.

4. **ISE shows “HTTP 500 Internal error, Radius session not found” message in Guest client's browser during redirect**

This is usually an indicator of session loss on ISE (session has been terminated). The most common reason for this is accounting configured on the Anchor WLC when Foreign-Anchor has been deployed. To fix this disable accounting on the Anchor and leave the Foreign handle Authentication and Accounting.

5. **Client disconnects and remains disconnected or connects to a different SSID after accepting AUP in ISE’s HotSpot portal.**

This canbe expected in HotSpot due to the Dynamic Change of Authorization (CoA) involved in this flow (CoA Admin Reset) that causes the WLC to issue a deauth to the wireless station. The majority of wireless endpoints do not have any issues to come back to the SSID after the de-authenticate happens, but in some cases the client connects to another preferred SSID in response to the de-authenitcate event. Nothing can be done from ISE or WLC to prevent this as it is up to the wireless client to stick to the original SSID, or to connect to another available (preferred) SSID.

In this case the wireless user must manually connect back to the HotSpot SSID.

AireOS WLC

```
(Cisco Controller) >debug client <MAC addr>
```

Debug client sets to DEBUG a set of components involved in Client State Machine changes.

```
(Cisco Controller) >show debug

MAC Addr 1.................................. AA:AA:AA:AA:AA:AA

Debug Flags Enabled:
  dhcp packet enabled.
  dot11 mobile enabled.
  dot11 state enabled
  dot1x events enabled.
  dot1x states enabled.
  mobility client handoff enabled.
  pem events enabled.
  pem state enabled.
  802.11r event debug enabled.
  802.11w event debug enabled.
  CCKM client debug enabled.
```

Debug AAA components

```
(Cisco Controller) >debug aaa {events, detail and packets} enable
```

This canbe impact resources depending on the amount of users that connect through MAB or Dot1X SSID. These components in DEBUG level record AAA transactions between WLC and ISE and print the RADIUS packets on the screen.

This is critical if you that ISE cannot deliver the expected attributes, or if the WLC does not process them correctly.

Web-Auth redirect

```
(Cisco Controller) >debug web-auth redirect enable mac aa:aa:aa:aa:aa:aa
```

This can be used to verify that the WLC is successfully triggering the redirect. This is an example of how the redirect must look like from debugs:

```
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e-  parser host is 10.10.10.10
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- parser path is /
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- added redirect=, URL is now
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-005056a15f11&action=cwa&to
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- str1 is now
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-005056a15f11&action=cwa&token=c455b075d20c
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- clen string is Content-Length: 430


*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- Message to be sent is
 HTTP/1.1 200 OK
Location:
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-0050
```

NGWC

Debug client sets to DEBUG a set of components involved in Client State Machine changes.

```
3850#debug client mac-address <client MAC>
```

This component prints the RADIUS packets (Authentication and Accounting) on the screen. This is handy when you need to verify that ISE delivers the right AVPs and also to verify that CoA is sent and processed correctly.

```
3850#debug radius
```

This will all AAA transitions (authentication, authorization and accounting) where wireless clients are involved. This is critical to verify that WLC parses correctly the AVPs and applies them to the client session.

```
3850#debug aaa wireless all
```

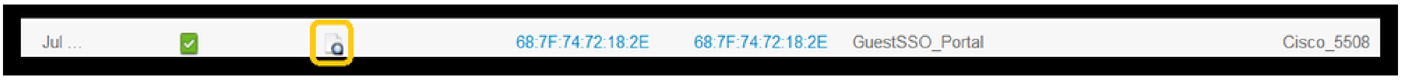
This can enabled when you suspect a redirect issue on the NGWC.

```
3850#debug epm plugin redirect all
3850#debug ip http transactions
3850#debug ip http url
```

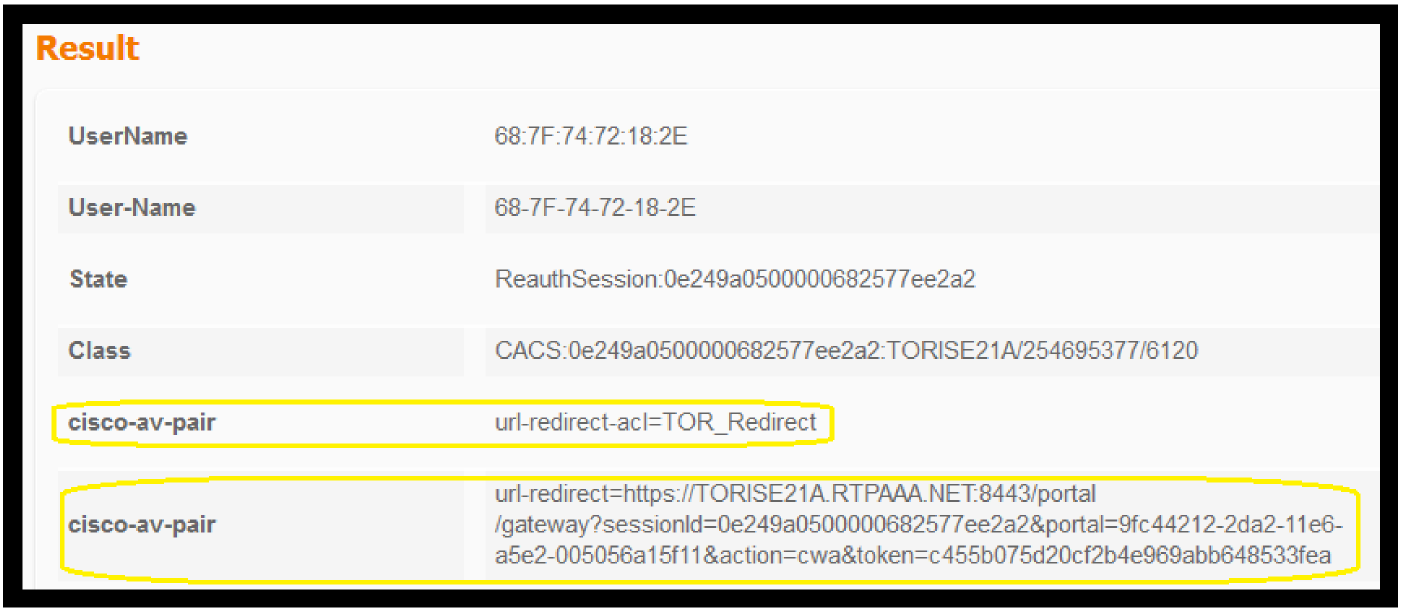
ISE

RADIUS Live logs

Verify initial MAB request has been processed correctly in ISE and that ISE pushes back the expected attributes. Navigate to **Operations > RADIUS > Live logs** and filter the output using the client MAC under **Endpoint ID**. Once the authentication event is found, click on details and then verify the Results pushed as part of the accept.



Jul ...	✓		68:7F:74:72:18:2E	68:7F:74:72:18:2E	GuestSSO_Portal	Cisco_5508



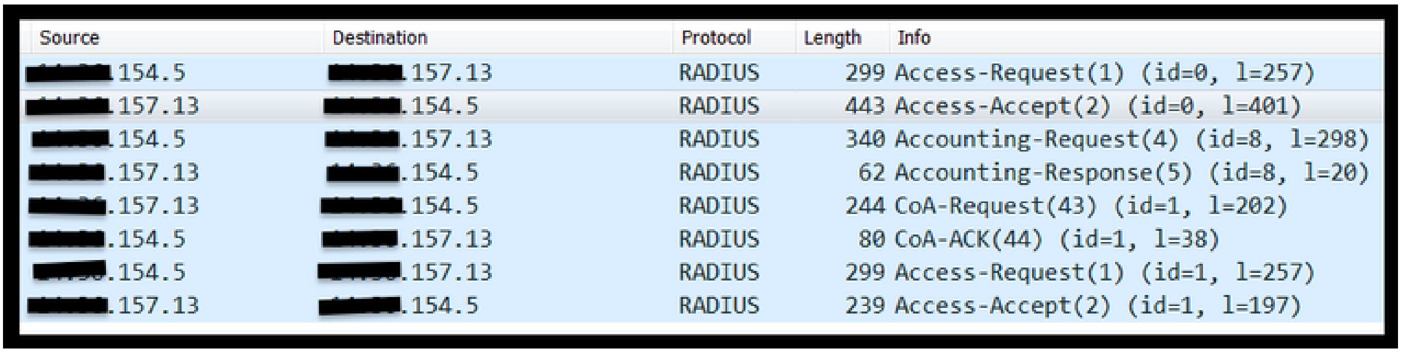
Result

UserName	68:7F:74:72:18:2E
User-Name	68-7F-74-72-18-2E
State	ReauthSession:0e249a0500000682577ee2a2
Class	CACS:0e249a0500000682577ee2a2:TORISE21A/254695377/6120
cisco-av-pair	url-redirect-acl=TOR_Redirect
cisco-av-pair	url-redirect=https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44212-2da2-11e6-a5e2-005056a15f11&action=cwa&token=c455b075d20cf2b4e969abb648533fea

TCPDump

This feature can be used when a deeper look into the RADIUS packet exchange between ISE and the WLC is needed. This way you can prove that ISE sends the correct attributes in the access-accept without the need to enable debugs on the WLC side. To start a capture using TCDDump navigate to **Operations > Troubleshoot > Diagnostic Tools >General Tools > TCPDump.**

This is an example of a correct flow captured through TCPDump



Source	Destination	Protocol	Length	Info
[redacted].154.5	[redacted].157.13	RADIUS	299	Access-Request(1) (id=0, l=257)
[redacted].157.13	[redacted].154.5	RADIUS	443	Access-Accept(2) (id=0, l=401)
[redacted].154.5	[redacted].157.13	RADIUS	340	Accounting-Request(4) (id=8, l=298)
[redacted].157.13	[redacted].154.5	RADIUS	62	Accounting-Response(5) (id=8, l=20)
[redacted].157.13	[redacted].154.5	RADIUS	244	CoA-Request(43) (id=1, l=202)
[redacted].154.5	[redacted].157.13	RADIUS	80	CoA-ACK(44) (id=1, l=38)
[redacted].154.5	[redacted].157.13	RADIUS	299	Access-Request(1) (id=1, l=257)
[redacted].157.13	[redacted].154.5	RADIUS	239	Access-Accept(2) (id=1, l=197)

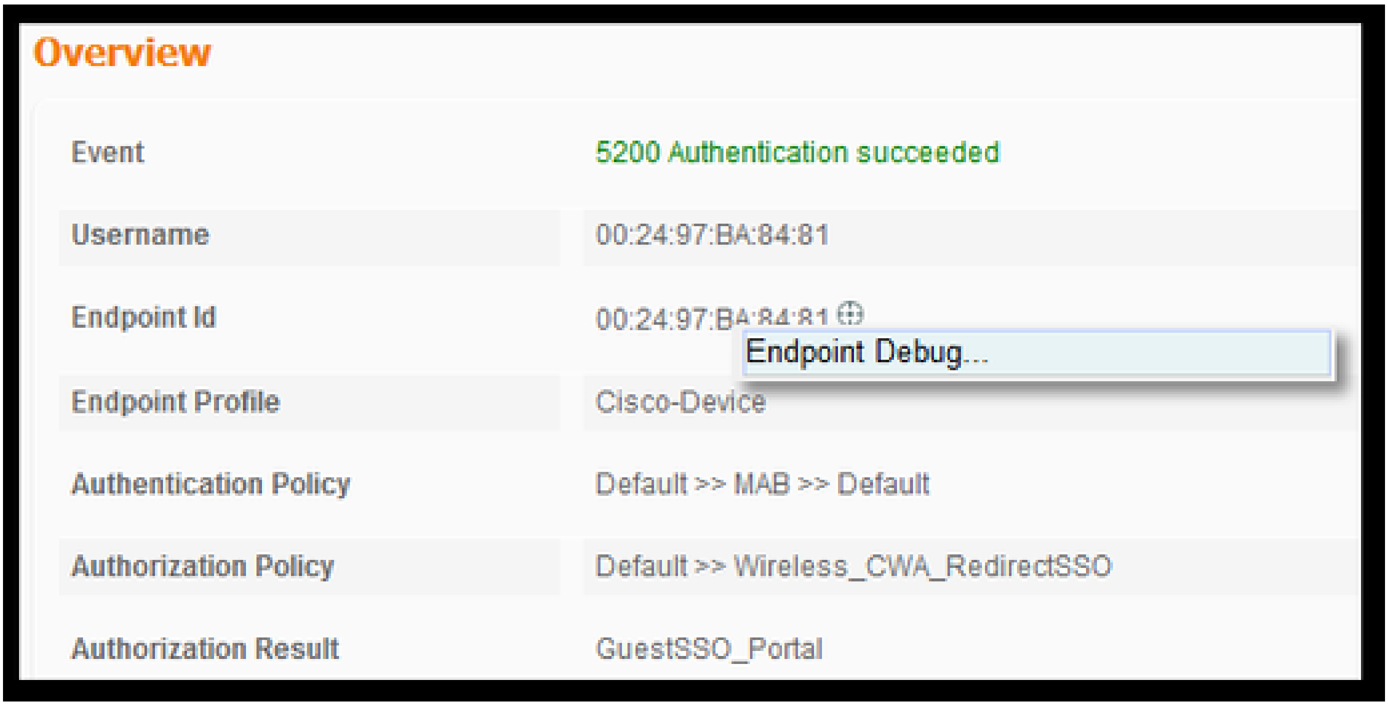
Here are the AVPs sent in response to the initial MAB request (second packet in the screenshot above).

```
RADIUS Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x0 (0)
    Length: 401
    Authenticator: f1eaaffcfaa240270b885a9ba8ccd06d
    [This is a response to a request in frame 1]
    [Time from request: 0.214509000 seconds]
    Attribute Value Pairs
        AVP: l=19 t=User-Name(1): 00-05-4E-41-19-FC
        AVP: l=40 t=State(24): 52656175746853657373696f6e3a30653234396130353030...
        AVP: l=55 t=Class(25): 434143533a30653234396130353030303030616130353536...
        AVP: l=37 t=Vendor-Specific(26) v=ciscoSystems(9)
            VSA: l=31 t=Cisco-AVPair(1): url-redirect-acl=Gues_Redirect
        AVP: l=195 t=Vendor-Specific(26) v=ciscoSystems(9)
            VSA: l=189 t=Cisco-AVPair(1): url-
redirect=https://ise21a.rtpaaa.net:8443/portal/gateway?sessionId=0e249a0500000aa05565e1c9&portal
=194a5780-5e4e-11e4-b905-005056bf2f0a&action=cwa&token=c6c8a6b0d683ea0c650282b4372a7622
        AVP: l=35 t=Vendor-Specific(26) v=ciscoSystems(9)
```

Endpoint Debugs:

If you need to dive deeper into ISE processes that involve policy decisions, portal selection, guest authentication, CoA handling the easiest way to approach this is to enable **Endpoit Debugs** instead of having to set complete components to debug level.

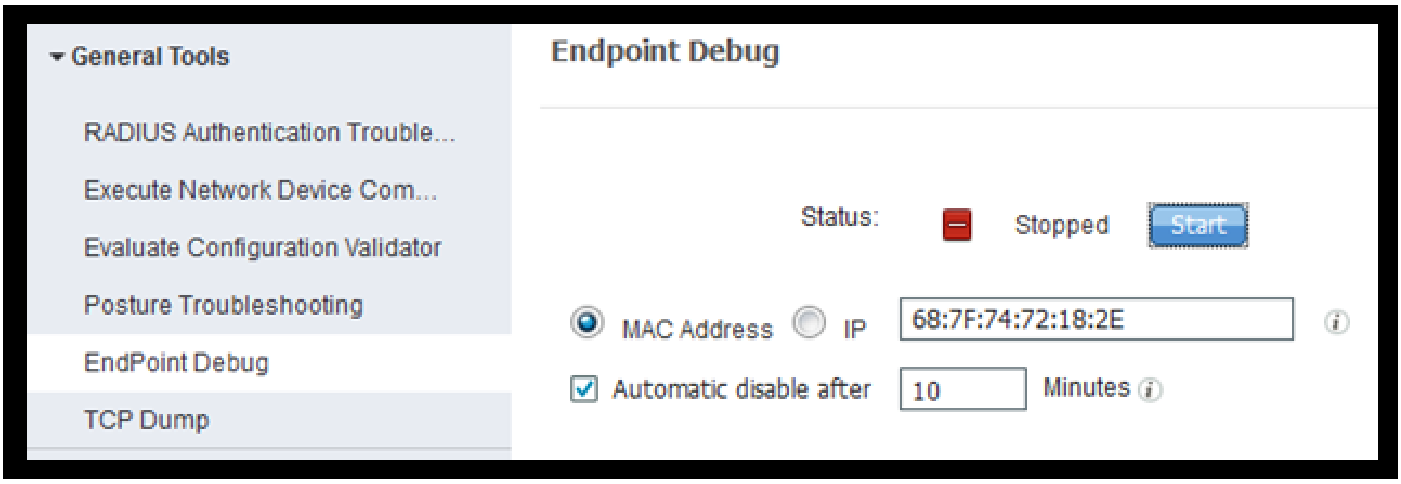
To enable this, navigate to **Operations > Troubleshooting > DiagnosticTools > General Tools** > **EndPoint Debug.**



Overview

Event	5200 Authentication succeeded
Username	00:24:97:BA:84:81
Endpoint Id	00:24:97:BA:84:81
Endpoint Profile	Cisco-Device
Authentication Policy	Default >> MAB >> Default
Authorization Policy	Default >> Wireless_CWA_RedirectSSO
Authorization Result	GuestSSO_Portal

Once in the Endpoint debug page, enter the endpoint MAC address and click start when ready to recreate the issue.



General Tools
RADIUS Authentication Trouble...
Execute Network Device Com...
Evaluate Configuration Validator
Posture Troubleshooting
EndPoint Debug
TCP Dump
Start

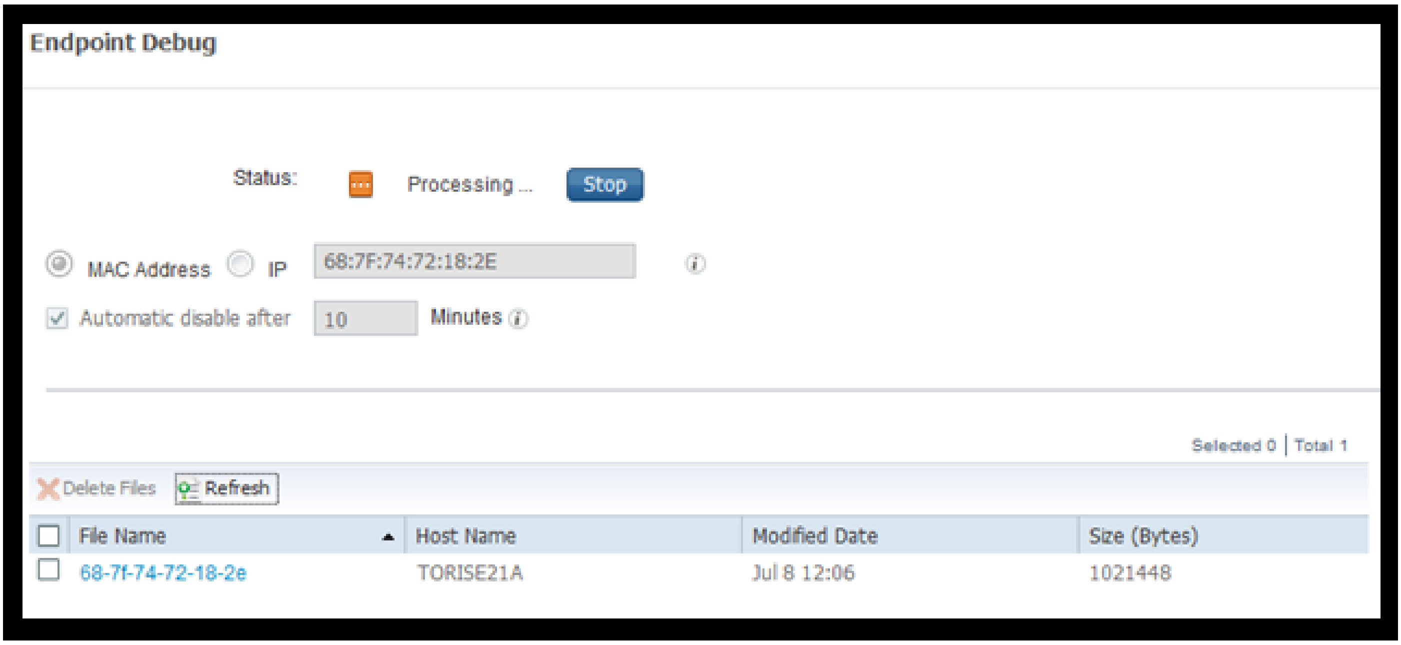
Endpoint Debug

Status: Stopped

● MAC Address ○ IP 68:7F:74:72:18:2E

☑ Automatic disable after 10 Minutes

Once the debug has been stopped click on the link that identifies the endpoint ID to download the debug output.



Endpoint Debug

Status: Processing ...

● MAC Address ○ IP 68:7F:74:72:18:2E

☑ Automatic disable after 10 Minutes

Selected 0 | Total 1

□	File Name	Host Name	Modified Date	Size (Bytes)
□	68-7f-74-72-18-2e	TORISE21A	Jul 8 12:06	1021448

Related Information

TAC Recommended AireOS Builds

Cisco Wireless Controller Configuration Guide, Release 8.0.

Cisco Identity Services Engine Administrator Guide, Release 2.1

Universal NGWC Wireless Configuration with Identity services Engine