Central Web Authentication on the WLC and ISE Configuration Example

TAC

Updated: July 3, 2017 **Document ID:** 115732

Contents

Introduction

This document describes a configuration example that is used in order to complete Central Web Authentication (CWA) on the Wireless LAN Controller (WLC).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- Cisco Identity Services Engine Software Release 2.0
- Cisco WLC Software Release 8.2.141.0

Configure

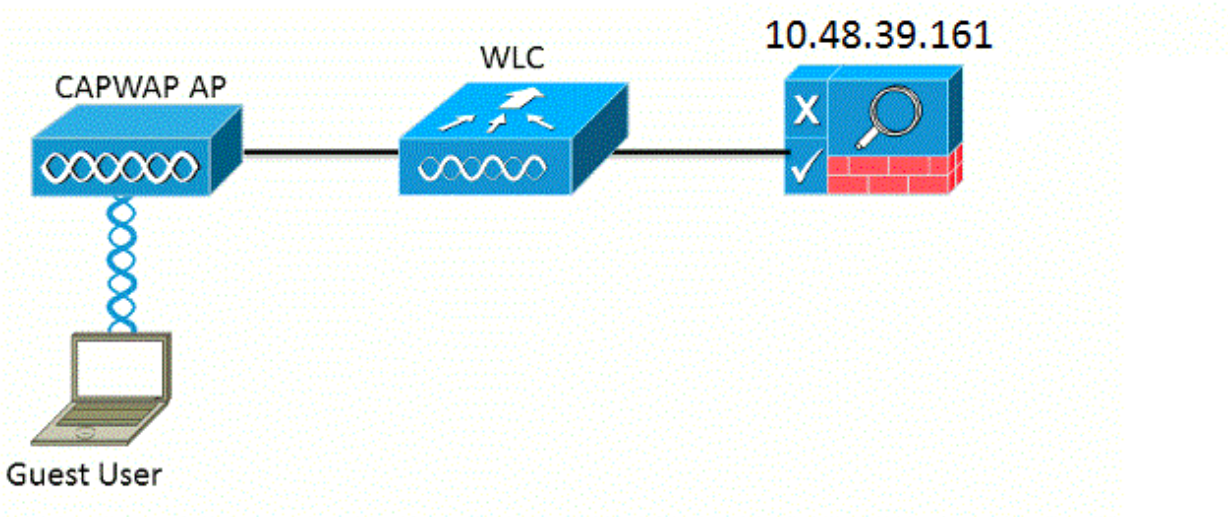
The first method of web authentication is local web authentication. In this case, the WLC redirects the HTTP traffic to an internal or external server where the user is prompted to authenticate. The WLC then fetches the credentials (sent back via an HTTP GET request in the case of an external server) and makes a RADIUS authentication. In the case of a guest user, an external server (such as Identity Services Engine (ISE) or NAC Guest Server (NGS)) is required because the portal provides features such as device registering and self-provisioning. The flow includes these steps:

1. The user associates to the web authentication Service Set Identifier (SSID).
2. The user opens the browser.
3. The WLC redirects to the guest portal (such as ISE or NGS) as soon as a URL is entered.
4. The user authenticates on the portal.
5. The guest portal redirects back to the WLC with the credentials entered.
6. The WLC authenticates the guest user via RADIUS.
7. The WLC redirects back to the original URL.

This flow includes several redirections. The new approach is to use CWA. This method works with ISE (versions later than 1.1) and WLC (versions later than 7.2). The flow includes these steps:

1. The user associates to the web authentication SSID, which is in fact open+macfiltering and no layer 3 security.
2. The user opens the browser.
3. The WLC redirects to the guest portal.
4. The user authenticates on the portal.
5. The ISE sends a RADIUS Change of Authorization (CoA - UDP Port 1700) to indicate to the controller that the user is valid, and eventually pushes RADIUS attributes such as the Access Control List (ACL).
6. The user is prompted to retry the original URL.

The setup used is:

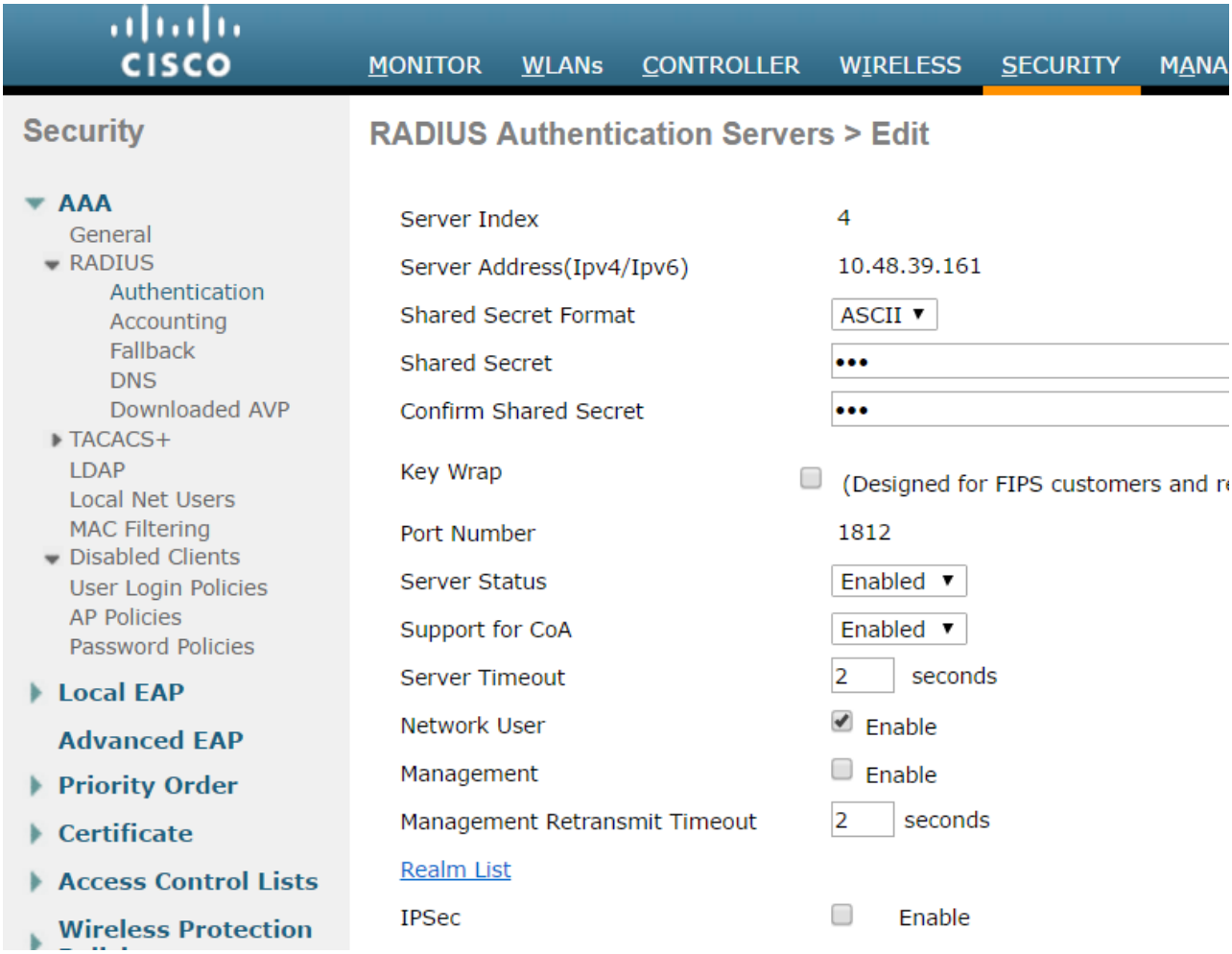


WLC Configuration

The WLC configuration is fairly straightforward. A **trick** is used (same as on switches) in order to obtain the dynamic authentication URL from the ISE (since it uses Change of Authorization (CoA), a session must be created and the session ID is part of the URL). The SSID is configured in order to use MAC filtering. The ISE is configured in order to return an access-accept even if the MAC address is not found, so that it sends the redirection URL for all users.

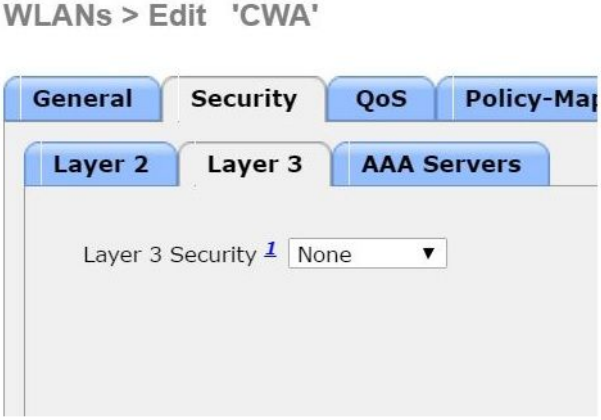
In addition to this, ISE Network Admission Control (NAC) and Authentication, Authorization, and Accounting (AAA) Override must be enabled. The ISE NAC allows the ISE to send a CoA request that indicates that the user is now authenticated and is able to access the network. It is also used for posture assessment, in which case the ISE changes the user profile based on the posture result.

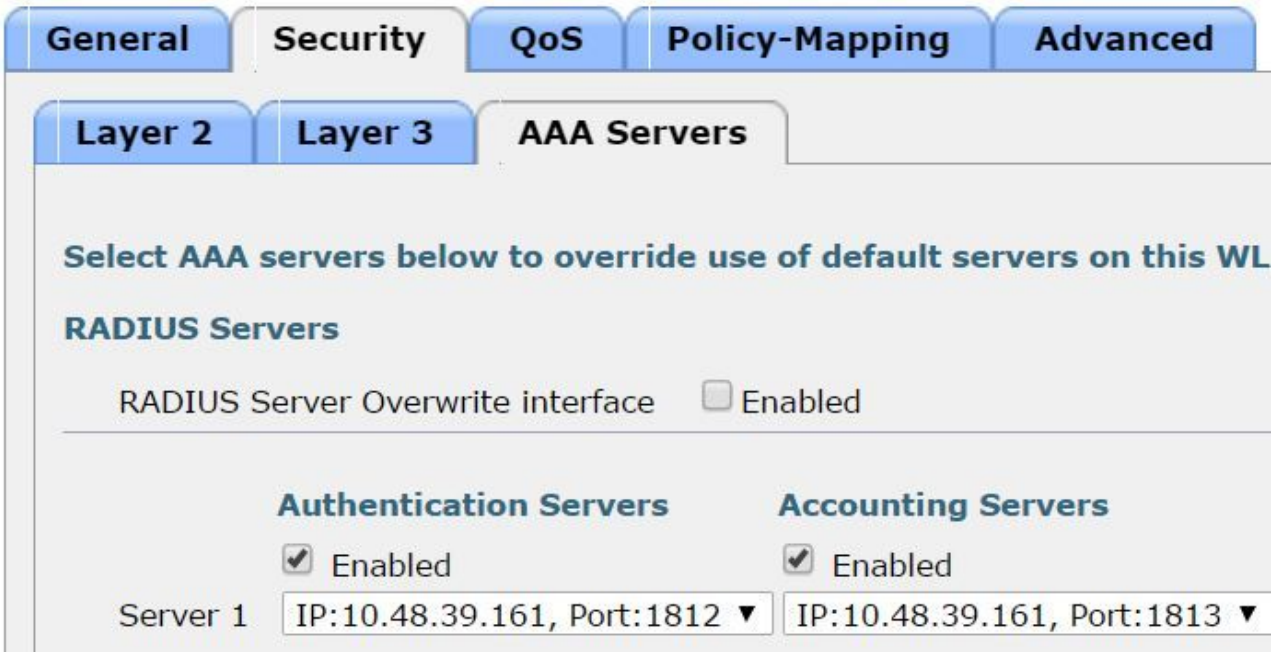
Ensure that the RADIUS server has " Support for CoA" enabled, which is by default.

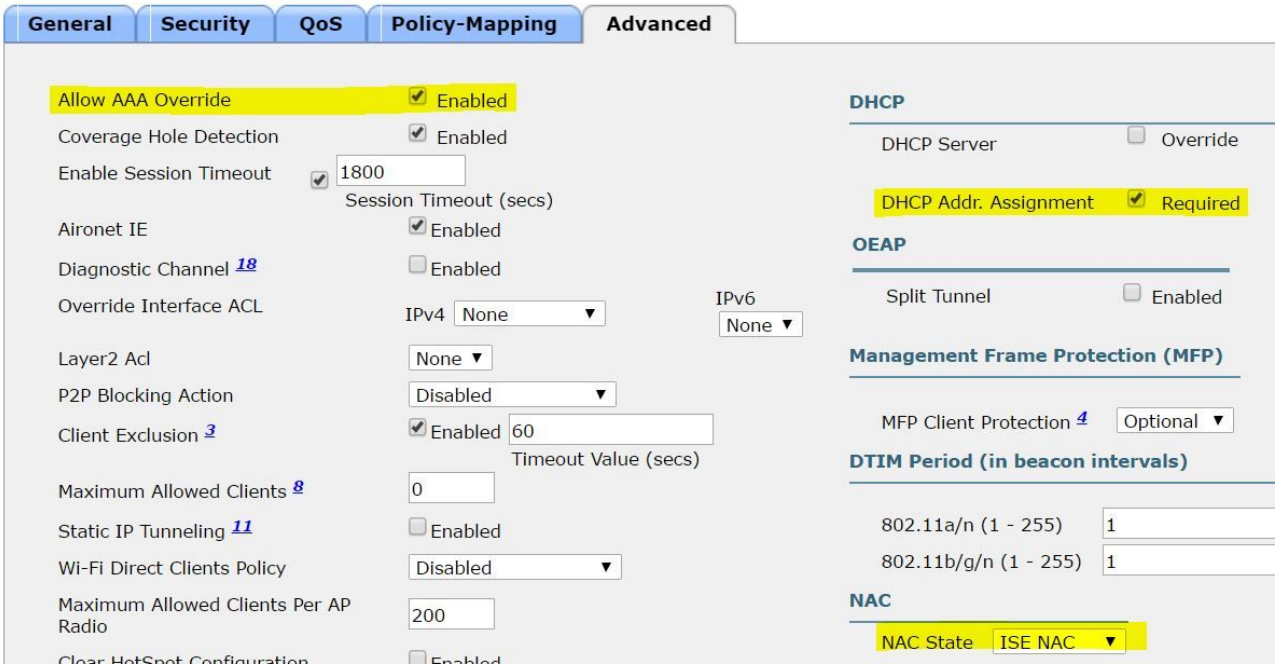

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANA
Security
AAA
General
RADIUS
Authentication
Accounting
Fallback
DNS
Downloaded AVP
TACACS+
LDAP
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Password Policies
Local EAP
Advanced EAP
Priority Order
Certificate
Access Control Lists
Wireless Protection
RADIUS Authentication Servers > Edit
Server Index 4
Server Address(Ipv4/Ipv6) 10.48.39.161
Shared Secret Format ASCII
Shared Secret
Confirm Shared Secret
Key Wrap (Designed for FIPS customers and r
Port Number 1812
Server Status Enabled
Support for CoA Enabled
Server Timeout 2 seconds
Network User Enable
Management Enable
Management Retransmit Timeout 2 seconds
Realm List
IPSec Enable


MONITOR WLANs CONTROLLER WIRELES
WLANs
WLANs
WLANs
Advanced
WLANs > New
Type WLAN
Profile Name CWA
SSID CWA
ID 1


WLANs > Edit 'CWA'
General
Security
QoS
Policy-Mapp
Layer 2
Layer 3
AAA Servers
Layer 2 Security 6 None
MAC Filtering9
Fast Transition
Fast Transition


WLANs > Edit 'CWA'
General
Security
QoS
Policy-Map
Layer 2
Layer 3
AAA Servers
Layer 3 Security 1 None





The final step is to create a redirect ACL. This ACL is referenced in the access-accept of the ISE and defines what traffic should be redirected (denied by the ACL) and what traffic should not be redirected (permitted by the ACL). Here you just prevent from redirection traffic towards the ISE. You might want to be more specific and only prevent traffic to/from the ISE on port 8443 (guest portal), but still redirect if a user tries to access the ISE on port 80/443.

> **Note**: Earlier versions of WLC software such as 7.2 or 7.3 did not require you to specify Domain Name System (DNS), but later code versions require you to permit DNS traffic on that redirect ACL.

General

Access List Name cwa_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	DNS	Any	Any	Any	836
2	Permit	0.0.0.0 0.0.0.0	/	0.0.0.0 0.0.0.0	/	UDP	Any	DNS	Any	Any	2072
3	Permit	0.0.0.0 0.0.0.0	/	10.48.39.161 255.255.255.255	/	Any	Any	Any	Any	Any	4895
4	Permit	10.48.39.161 255.255.255.255	/	0.0.0.0 0.0.0.0	/	Any	Any	Any	Any	Any	7160
5	Deny	0.0.0.0 0.0.0.0	/	0.0.0.0 0.0.0.0	/	Any	Any	Any	Any	Any	6587

Configuration is now complete on the WLC.

ISE Configuration

Create the Authorization Profile

On the ISE, the authorization profile must be created. Then, the authentication and authorization policies are configured. The WLC should already be configured as a network device.

In the authorization profile, enter the name of the ACL created earlier on the WLC.

1. Click **Policy**, and then click **Policy Elements**.

2. Click **Results**.

3. Expand **Authorization**, and then click **Authorization profile**.

4. Click the **Add** button in order to create a new authorization profile for central webauth.

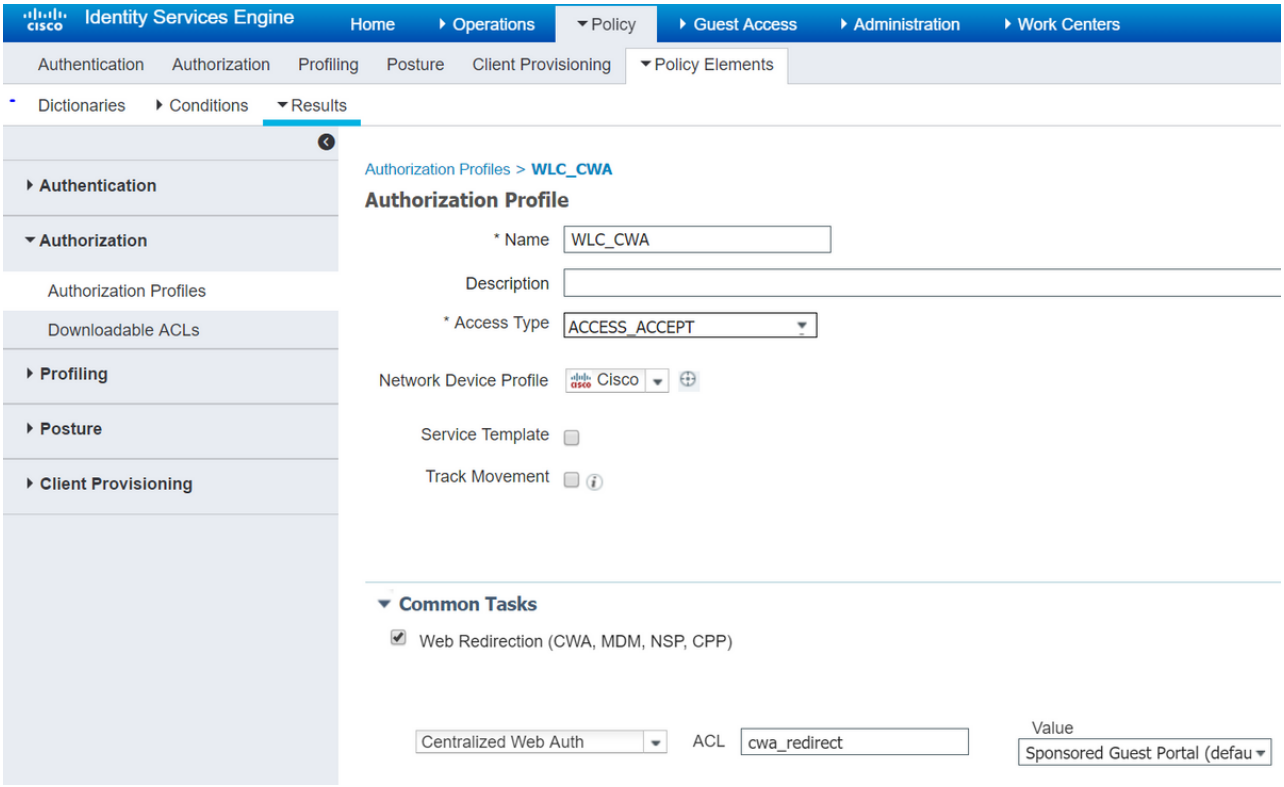
5. In the **Name** field, enter a name for the profile. This example uses **WLC_CWA**.

6. Choose **ACCESS_ACCEPT** from the Access Type drop-down list.

7. Check the **Web Redirection** check box, and choose **Centralized Web Auth** from the drop-down list.

8. In the ACL field, enter the name of the ACL on the switch that defines the traffic to be redirected. This example uses **cwa_redirect**.

9. In the value field, one can choose **Sponsored Guest Portal** or **Self-Registered Guest Portal** from the drop-down list. In sponsored guest portal, sponsors create guest accounts, and guests access the network using their assigned username and password while in self-registration guest portal, guests are allowed to create their own accounts and access the network using their assigned username and password. This example uses **Sponsored Guest Portal.**



Create an Authentication Rule

Ensure that the ISE accepts all of the MAC authentications from the WLC and make sure it will pursue authentication even if the user is not found.

Under the Policy menu, click **Authentication**.

The next image shows an example of how to configure the authentication policy rule. In this example, a rule is configured that triggers when MAB is detected.

1. Enter a name for your authentication rule. This example uses **MAB**, which already exists by default on ISE Version 1.2.

2. Select the plus (**+**) icon in the If condition field.

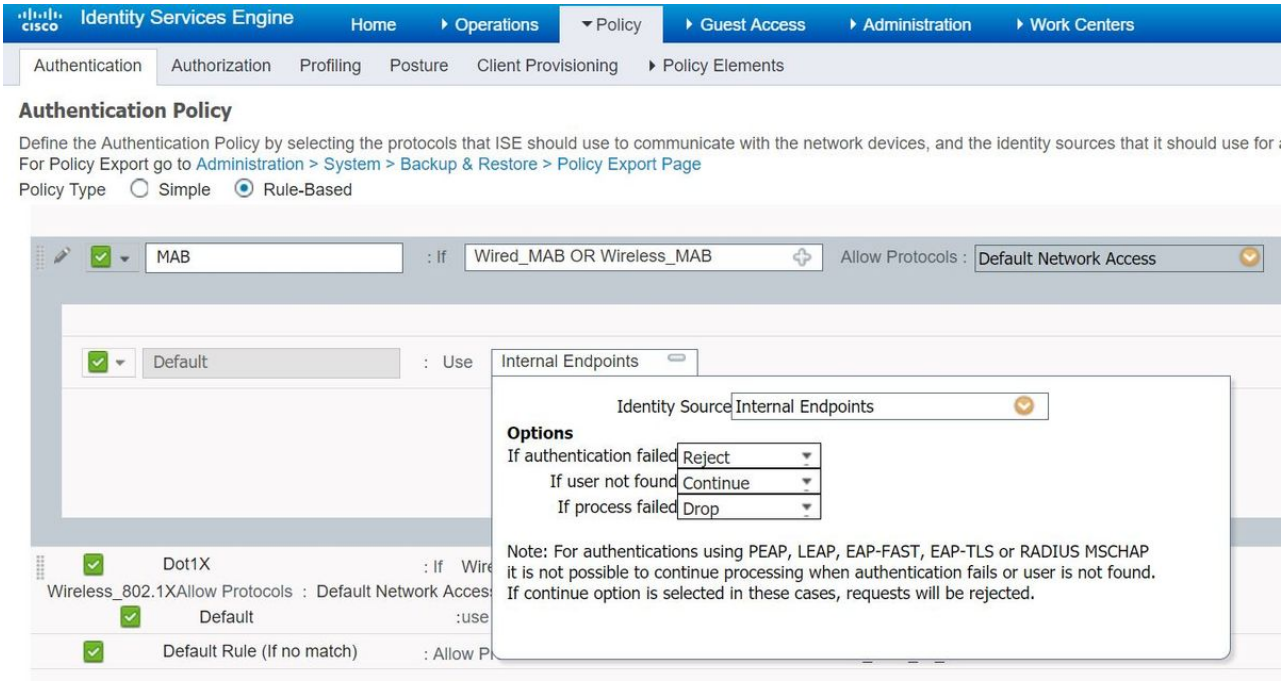
3. Choose **Compound condition**, and then choose **Wired_MAB OR Wireless_MAB**.

4. Click the arrow located next to **and ...** in order to expand the rule further.

5. Click the **+** icon in the Identity Source field, and choose **Internal endpoints**.

6. Choose **Continue** from the If user not found drop-down list.

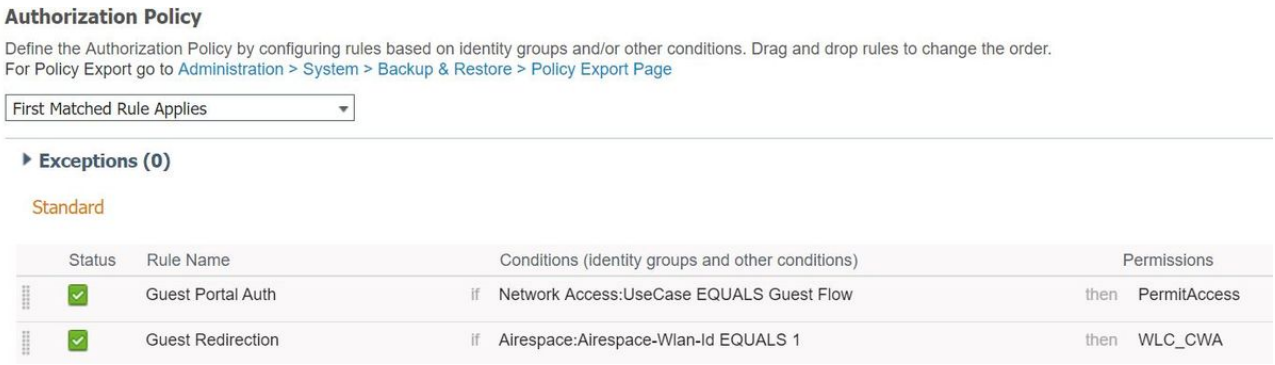
Note: Now there is a MAB authentication rule created on the ISE by default.



Create an Authorization Policy

Configure the authorization policy. One important point to understand is that there are two authentications/authorizations:

- The first is when the user associates to the SSID (" CWA" in this case) and the CWA profile is returned.
  In this example **Airespace-Wlan-Id** is used as a condition. When a client connects to the SSID, the RADIUS access request to ISE contains the Airespace-WLAN-ID attribute. This attribute is used to make policy decisions in ISE. So when an unknown client connects to SSID CWA, ISE sends an acceess-accept with redirect URL (web portal) and ACL. Use of the Airespace-Wlan-Id rule ensures that the portal page is presented to users that only connect to the CWA SSID.
- The second is when the user authenticates on the web portal. This one matches the default rule (internal users) in this configuration (it can be configured in order to meet your requirements). It is important that the authorization part does not match the CWA profile again. Otherwise, there will be a redirection loop. The **Network Access:UseCase Equals Guest Flow** attribute can be used in order to match this second authentication. The result looks like this:



Complete these steps in order to create the authorization rules as shown in the previous images:

1. Create a new rule, and enter a name. This example uses **Guest Redirection**.

2. Click the plus (**+**) icon in the condition field, and choose to create a new condition.

3. Expand the **Expression** drop-down list.

4. Choose **Airespace**, and expand it.

5. Click **Airespace-Wlan-Id--[1]**, and choose the **Equals** operator.

6. Enter the **WLAN ID** in the right-hand field, in this example 1.

7. On the General Authorization page, choose **WLC_CWA** (Authorization Profile) in the field to the right of the word **then**.

   This step allows the ISE to continue even though the user (or the MAC address) is not known when connected to **CWA** SSID and present them with the login portal.

8. Click the **Actions** button located at the end of the **Guest Redirection** rule, and choose to insert a new rule before it.

Note: It is very important that this new rule comes before the **Guest Redirection** rule.

---

9. Enter a name for the new rule. This example uses **Guest Portal Auth**.

0. In the condition field, click the plus **(+)** icon, and choose to create a new condition.

1. Choose **Network Access**, and click **UseCase**.

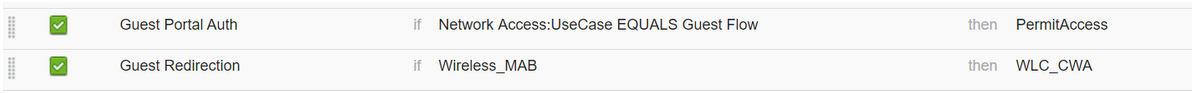
2. Choose **Equals** as the operator.

3. Choose **GuestFlow** as the right operand.

4. On the authorization page, click the plus (**+**) icon (located next to **then**) in order to choose a result for your rule.

   You can choose a **Permit Access** option or create a custom profile in order to return the VLAN or attributes that you like. Note that on top of **If GuestFlow**, you can add more conditions in order to return various authz profiles based on the user group. As mentioned in Step 7, this **Guest Portal Auth** rule matches upon the second MAC address authentication initiated after the successful portal login and after ISE sent a CoA in order to reauthenticate the client. The difference with this second authentication is that, instead of coming to ISE with simply its MAC address, ISE remembers the username given in the portal. You can make this authorization rule take into account the credentials entered a few milliseconds before in the guest portal.

Note: In a multi controller environment the WLAN-ID should be the same across the WLCs. If one does not want to use the Airespace-Wlan-Id attribute as a condition, then it is better to match Wireless_MAB (Built-in condition) requests.



Enable the IP Renewal (Optional)

If you assign a VLAN, the final step is for the client PC to renew its IP address. This step is achieved by the guest portal for Windows clients. If you did not set a VLAN for the **2nd AUTH** rule earlier, you can skip this step.

If you assigned a VLAN, complete these steps in order to enable IP renewal:

1. Click **Guest Access**, and then click **Configure**.
2. Click **Guest Portals**.
3. Click **Sponsored Guest Portal** (used in this example), and then expand **VLAN DHCP Release Page Settings**.
4. Click the **VLAN DHCP Release** check box.

Note: This option works only for Windows clients.

Anchor-Foreign Scenario

This setup can also work with the auto-anchor feature of the WLCs. The only catch is that since this web authentication method is Layer 2, you have to be aware that it will be the foreign WLC that does all of the RADIUS work. Only the foreign WLC contacts the ISE, and the redirection ACL must be present also on the foreign WLC.

Just like in other scenarios, the foreign WLC quickly shows the client to be in the **RUN** state, which is not entirely true. It simply means that traffic is sent to the anchor from there. The real client state can be seen on the anchor where it should display **CENTRAL_WEBAUTH_REQD**.

Here is the flow in an **anchor-foreign** setup:

1. The client connects to the SSID on the foreign WLC. The foreign WLC contacts the ISE server for MAB. ISE sends access-accept with the redirect URL and redirect ACL to the foreign.
2. Now the client is anchored to the anchor WLC where it gets an IP address and is put in CENTRAL_WEBAUTH_REQD.
3. When the client tries to access a website, the anchor WLC redirects the client to the ISE portal page. The client is presented with the login page.
4. After successful login, ISE sends a CoA to the foreign WLC.
5. The foreign WLC contacts the anchor WLC to let it know to put the client in the RUN state.
6. All the client traffic is forwarded from foreign to anchor, and goes out of the anchor WLC.

The firewall ports which are required to allow communication between the WLC and ISE are:

- UDP:1645, 1812 (RADIUS Authentication)
- UDP:1646, 1813 (RADIUS Accounting)
- UDP:1700 (RADIUS CoA)
- TCP:8443 Guest Portal or 8905 if you have Posturing.

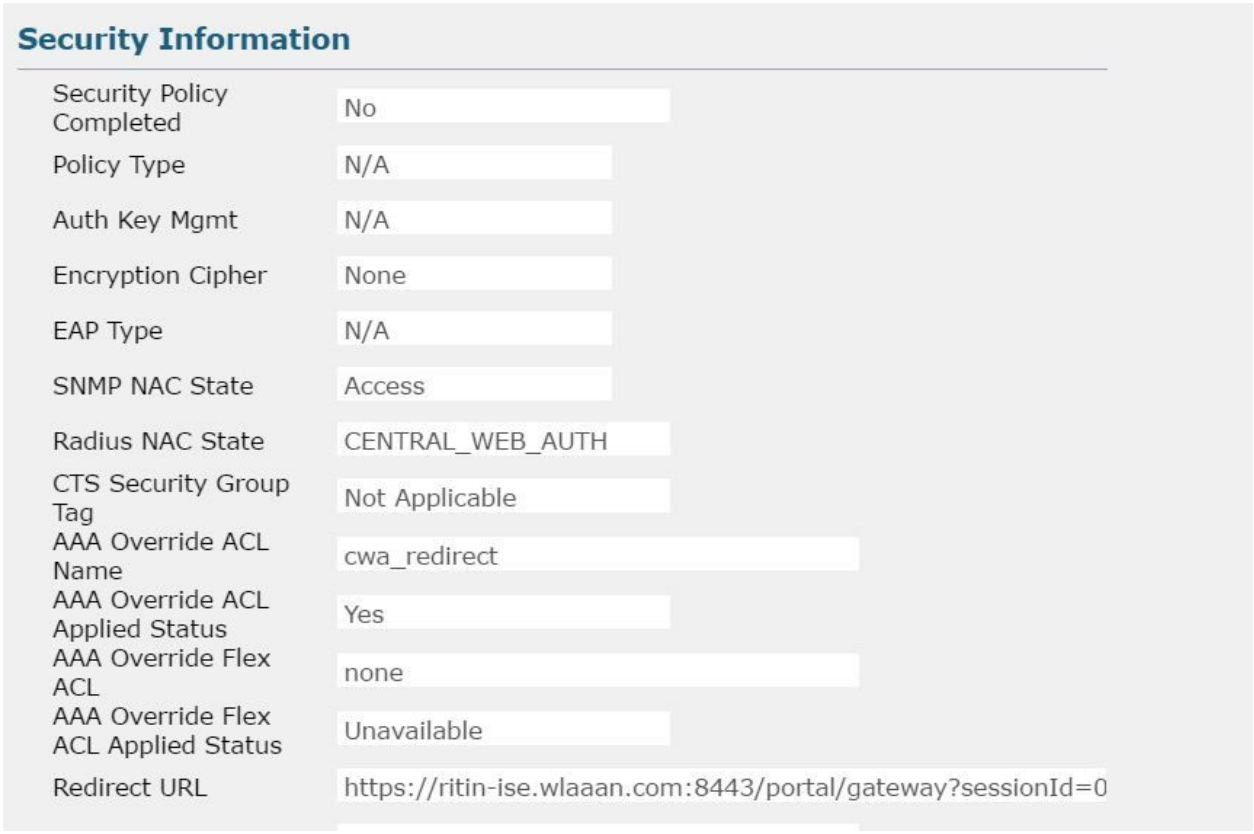
Note: The anchor-foreign setup with Central Web Authentication (CWA) only works in Releases 7.3 or later.

Note: Due to Cisco bug ID CSCuo56780 (even in versions that include fixes), you cannot run accounting on both anchor and foreign because it causes the profiling to become inaccurate due to a potential lack of IP-to-MAC binding. It also creates many issues with the session ID for guest portals. If you desire to configure accounting, then configure it on the foreign controller.

Verify

Use this section in order to confirm that your configuration works properly.

1. Once the user is associated to the SSID, WLC contacts the ISE (as MAC filtering is configured). ISE has been configured to return access accept with redirect URL and ACL. This is the first authentication.
   The client details in the WLC show that the redirection URL and ACL are applied.



In the WLC client and AAA all debug, you can see access accept with the redirect URL and ACL sent from the ISE.

```
*radiusTransportThread: 5c:c5:d4:b1:09:95 Access-Accept received from RADIU
*radiusTransportThread: AVP[04] Cisco / Url-Redirect-Acl.................cv
*radiusTransportThread: AVP[05] Cisco / Url-Redirect.....................DA

*apfReceiveTask: 5c:c5:d4:b1:09:95 Redirect URL received for client from RA
 Client will be moved to WebAuth_Reqd state to facilitate redirection. Skip
*apfReceiveTask: 5c:c5:d4:b1:09:95 AAA Override Url-Redirect-Acl 'cwa_redi:
```

The same thing can also be verified in the ISE. Choose **Operations** > **Radius livelogs**. Click the detail for that MAC.

You can see that for the first authentication (MAC filtering) ISE returns the AuthZ profile **WLC_CWA** as it hits the authentication rule **MAB** and authz policy **Guest Redirection**.

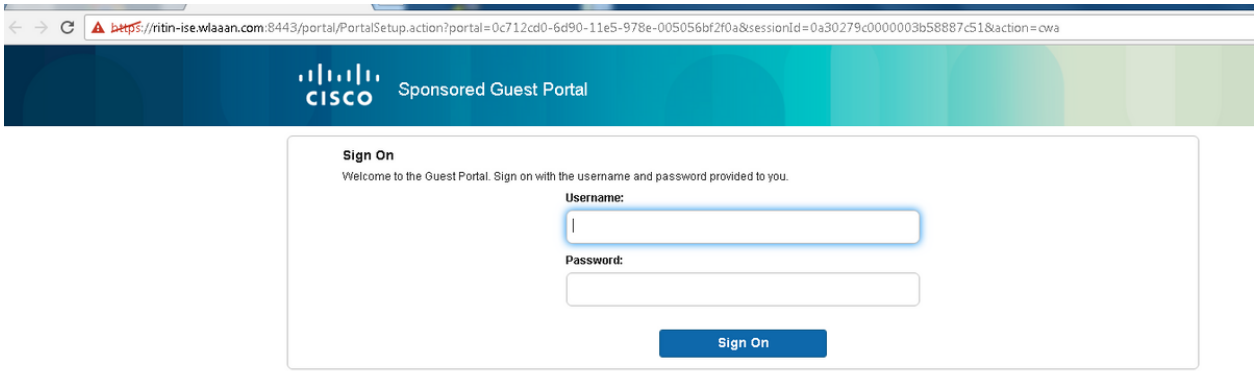
Authentication Policy	Default >> MAB >> Default
Authorization Policy	Default >> Guest Redirection
Authorization Result	WLC_CWA

22037 Authentication Passed
15036 Evaluating Authorization Policy
15004 Matched rule - Guest Redirection
15016 Selected Authorization Profile - WLC_CWA
11002 Returned RADIUS Access-Accept

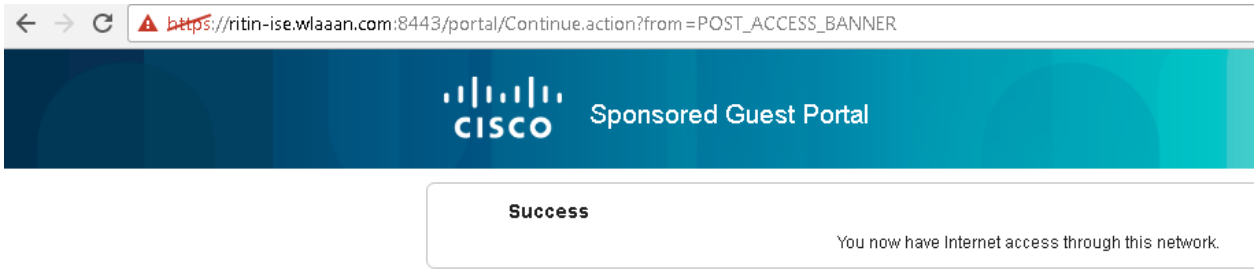
Result

UserName	5C:C5:D4:B1:09:95
User-Name	5C-C5-D4-B1-09-95
State	ReauthSession:0a30279c0000003b58887c51
Class	CACS:0a30279c0000003b58887c51:ritin-ise/274207619/279
cisco-av-pair	url-redirect-acl=cwa_redirect
cisco-av-pair	url-redirect=https://ritin-ise.wlaaan.com:8443/portal/gateway?sessionId=0a30279c0000003b58887c51&portal=0c712cd0-6d90-11e5-978e-005056bf2f0a&action=cwa&token=af5aad217cad23b7dd183792d728f196

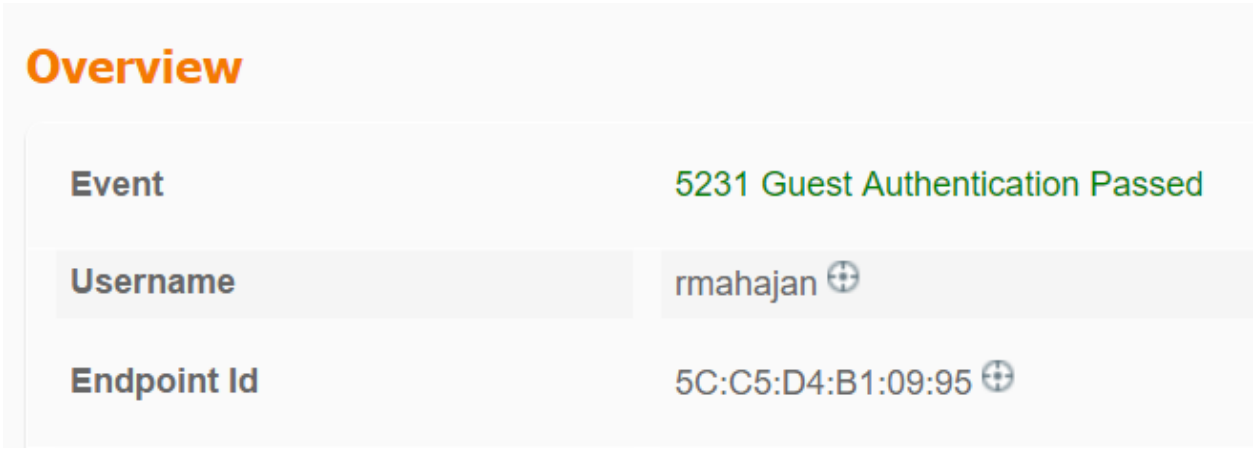
2. At this point the client gets an IP address. Now the client is in **CENTRAL_WEB_AUTH** state. When any address is opened on the client, the browser is redirected to the ISE. Ensure that the DNS is set up correctly.

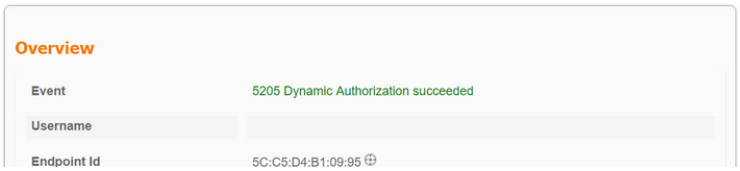


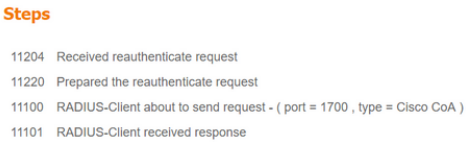
3. Once the correct credentials are entered, network access is granted. This is the second authentication.



When the credentials are entered, ISE authenticates the client and sends the CoA.







On the WLC this can be seen in AAA all debugs.

```
*radiusCoASupportTransportThread: audit session ID recieved in CoA = 0a302
*radiusCoASupportTransportThread: Received a 'CoA-Request' from 10.48.39.1

*radiusCoASupportTransportThread: CoA - Received IP Address : 10.48.39.156
*radiusCoASupportTransportThread: 5c:c5:d4:b1:09:95 Calling-Station-Id ---
*radiusCoASupportTransportThread: Handling a valid 'CoA-Request' regarding
*radiusCoASupportTransportThread: 5c:c5:d4:b1:09:95 Reauthenticating stati
*radiusCoASupportTransportThread: Sent a 'CoA-Ack' to 10.48.39.161
```

4. After this the client is reauthenticated and granted access to the network.

5. On the controller, the Policy Manager state and RADIUS NAC state changes from **CENTRAL_WEB_AUTH** to **RUN**.

> **Note**: In Release 7.2 or earlier, the state **CENTRAL_WEB_AUTH** was called **POSTURE_REQD.**

Note that the type of CoA returned by ISE evolved across versions. ISE 2.0 will request the WLC to re-run the authentication rather than plainly disconnect the client.

Example of ISE 2.0 CoA request :

```
▼ AVP: l=44 t=Vendor-Specific(26) v=ciscoSystems(9)
    AVP Type: 26
    AVP Length: 44
  ▶ VSA: l=38 t=Cisco-AVPair(1): subscriber:reauthenticate-type=rerun
▼ AVP: l=41 t=Vendor-Specific(26) v=ciscoSystems(9)
    AVP Type: 26
    AVP Length: 41
  ▼ VSA: l=35 t=Cisco-AVPair(1): subscriber:command=reauthenticate
      Cisco-AVPair: subscriber:command=reauthenticate
```

The WLC will then not send a disassociation frame to the client and will run a radius authentication again and apply the new result transparently to the client.

However, things are still different if a PSK is in use. Since 8.3, the WLC supports setting a WPA pre-shared key on a CWA SSID. In that kind of situation, upon reception of the same CoA from ISE as above, the WLC will have to trigger a new WPA key exchange again. Therefore in case of PSK, the WLC will have to send a disassociate frame to the client which will have to reconnect. In classical non-PSK scenarios, the WLC will not send a disassociate frame to the client and will simply apply the new authorization result. However an " association response" will be still sent ot the client although no " association request" was ever received from the client, which might seem curious when analyzing sniffer traces.

Troubleshoot

Complete these steps in order to troubleshoot or isolate a CWA problem:

1. Enter the **debug client <mac address of client>** command on the controller and monitor in order to determine whether the client reaches the **CENTRAL_WEBAUTH_REQD** state. A common problem is observed when the ISE returns a redirect ACL that does not exist (or is not properly input) on the WLC. If this is the case, then the client is deauthenticated once the **CENTRAL_WEBAUTH_REQD** state is reached, which causes the process to begin again.

2. If the correct client state can be reached, then navigate to **monitor > clients** on the WLC web GUI and verify that the correct redirect ACL and URL are applied for the client.

3. Verify that the correct DNS is used. The client should have the ability to resolve internet websites and the ISE hostname. You can verify this via nslookup.

4. Verify that all authentication steps occur on the ISE:

   - The MAC authentication should occur first, to which CWA attributes are returned.
   - The portal login authentication occurs.
   - The dynamic authorization occurs.
   - The final authentication is a MAC authentication that shows the portal username on the ISE, to which the final authorization results are returned (such as the final VLAN and ACL).

Special Considerations for Anchoring Scenarios

Consider these Cisco bug IDs that limit the efficiency of the CWA process in a mobility scenario (especially when accounting is configured):

- CSCuo56780 - ISE RADIUS Service Denial of Service Vulnerability
- CSCul83594 - Session-id is not synchronized across mobility, if the network is open