Configure Central Web Authentication with Anchor on Catalyst 9800

Contents

Introduction
<u>Prerequisites</u>
Requirements
Components Used
Configure a Catalyst 9800 anchored to another Catalyst 9800
Network Diagram
Configure AAA on both 9800s
Configure the WLANs on the WLCs
Create the Policy Profile and Policy Tag on the Foreign WLC
Create the Policy Profile on the Anchor WLC
Redirect ACLConfig on both 9800s
Configure ISE
Configure a Catalyst 9800 Anchored to an AireOS WLC
Catalyst 9800 Foreign Configuration
AAA Configs on the Anchor AireOS WLC
WLAN Config on the AireOS WLC
Redirect ACL on the AireOS WLC
Configure ISE
Differences in Config when the AireOS WLC is the Foreign and the Catalyst 9800 is the Anchor
<u>Verify</u>
Troubleshoot
Catalyst 9800 troubleshooting information
<u>Client Details</u>
Embedded Packet Capture
RadioActive Traces
AireOS Troubleshooting information
<u>Client Details</u>
Debugs from the CLI
Related Information

Introduction

This document describes how to configure and troubleshoot a CWA on the Catalyst 9800 pointing to another WLC as a mobility anchor.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Central Web Authentication (CWA)
- Wireless LAN Controller (WLC)
- 9800 WLC
- AireOS WLC
- Cisco ISE

It is assumed that before you start the CWA anchor config you have already brought up the mobility tunnel between the two WLCs. This is outside of the scope of this config example. If you need help with this, consult the document titled <u>Configuring Mobility Topologies on 9800</u>

Components Used

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

- 9800 17.2.1
- 5520 8.5.164 IRCM image
- ISE 2.4

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 a Catalyst 9800 anchored to another Catalyst 9800

Network Diagram



Configure AAA on both 9800s

On both the anchor and the foreign you need to first add the RADIUS server and make sure that CoA is enabled. To do so, navigate to the menu **Configuration** > **Security** > **AAA** > **Servers/Groups** > **Servers**. Then, click on the **Add** button.

Cisco Cata	lyst 9800-L Wireless Controller		Welcome admin Last login Fit, May 15 2020 16 56 51
Q Search Menu Items	Configuration * > Security * > AAA + AAA Wizard	J	
	Servers / Groups AAA Method Lis	AAA Advanced	
Configuration	+ Add × Delete		
	RADIUS	Servers Server Groups	
C Licensing	TACACS+	Name ~ Address	V Auth Port
X Troubleshooting	LDAP Create AAA Radius Server		×
	Name*	CLUS-Server	
	Server Address*	XXXX	
	PAC Key		
	Кеу Туре	Clear Text	
	Key*		
	Confirm Key*		
	Auth Port	1812	
	Acct Port	1813	
	Server Timeout (seconds)	1-1000	
	Retry Count	0-100	
	Support for CoA	ENABLED	
	Cancel		Apply to Device

You now need to create a Server group and place the server you just configured into that group. To do so, navigate to **Configuration > Security > AAA > Servers/Groups > Server Groups > +Add**.

Cisco Catalyst 9800-L Wireless Controller						
Q Search Menu Items	Configuration > Security	· > AAA				
Dashboard	+ AAA Wizard					
Monitoring >	Servers / Groups AAA	Method List AAA Ad	lvanced			
Configuration	+ Add × Delete					
Administration	RADIUS	Servers	Server Groups			
© Licensing	TACACS+	Nar		v cor		
X Troubleshooting	LDAP Create AAA Padius Serve			× 38		
	Create AAA Radius Serve			~		
	Name*	CLUS-Server-Group				
	Group Type	RADIUS				
	MAC-Delimiter	none 🔻				
	MAC-Filtering	none 🔻				
	Dead-Time (mins)	1-1440				
	Available Servers	Assigned	d Servers			
		CLUS-Serve	er 🔹	 × × 		
	Cancel			Apply to Device		

Now, create an authorization method list (an authentication method list is not required for CWA) where the type is network and the group type is group. Add the server group from the previous action to this method list.

To do so, navigate to **Configuration > Security > AAA > Servers/AAA Method List > Authorization > +Add**.

Cisco Catal	yst 9800-L Wirele	ess Controller	
Q Search Menu Items	Configuration > S	Security * > AAA	
📰 Dashboard	+ AAA Wizard		
Monitoring >	Servers / Groups	AAA Method List AAA Advanced	
Configuration	Authentication		
Administration	Authorization		
C Licensing	Quick Setup: AAA A	Authorization	Group Type
💥 Troubleshooting	Method List Name*	CLUS-AuthZ-Meth-List	
	Туре*	network 🗸	
	Group Type	group 🔹	
	Fallback to local		
	Authenticated Available Server Groups	s Assigned Server Groups	
	radius Idap tacacs+ ISE1	CLUS-Server-Group	
	Cancel		Apply to Device

(Optional) Create an accounting method list using the same server group as the authorization method list. To create the accounting list, navigate to **Configuration** > **Security** > **AAA** > **Servers/AAA Method List** > **Accounting** > +**Add**.

Cisco Cata	alyst 9800-L Wirele	ess Controller			
Q Search Menu Items	Configuration * > S	Security * > AAA			
📻 Dashboard	+ AAA Wizard				
Monitoring >	Servers / Groups	AAA Method List	AAA Advanced		
Configuration	Authentication				
Administration	Authorization		+ Add ×		
C Licensing	Quick Setup: AAA	Accounting	Name	√. Туре	Croup1
₩ Troubleshooting	Method List Name*	CLUS-	Acct-Meth-List		
	Type*	identity	•		
	Available Server Groups	3	Assigned Server Gr	oups	
	radius Idap tacacs+ ISE1		> CLUS-Serv	er-Group	× ×
	Cancel				Apply to Device

Configure the WLANs on the WLCs

Create and configure the WLANs on both the WLCs. The WLANs must match on both. The security type must be mac filtering and the authorization method list from the previous step must be applied. To configure this, navigate to **Configuration > Tags & Profiles > WLANs > +Add**.

Cisco Catalyst 9800-L Wireless Controller						
Q Search Menu Items	Configuration * > Tag	s & Profiles * > WLANs				
Dashboard	+ Add × Dele					
Monitoring >	Number of WLANs selected	:0				
	Status - Nam	e	~ ID		~	
	Add WLAN				×	
	General Security	Advanced				
C Licensing	Profile Name*	CLUS-WLAN-Name	Radio Policy	All]	
X Troubleshooting	SSID*	CLUS-SSID	Broadcast SSID	ENABLED		
	WLAN ID*	2				
	Status					
)			
	D Cancel				Apply to Device	

Cisco Cata	alyst 9800-L Wireless Controller	
Q Search Menu Items	Configuration * > Tags & Profiles * > WLANs	
Dashboard	+ Add × Delete Enable WLAN Disable WLAN	
Monitoring	Number of WLANs selected : 0 Image: Status of the selected of the sel	~
	Add WLAN General Security Advanced	×
C Licensing	Layer2 Layer3 AAA	
X Troubleshooting	Layer 2 Security Mode None Kone Kone Kone	
	OWE Transition Mode Over the DS Authorization List* CLUS-AuthZ-Meth-l	
	Cancel	

Create the Policy Profile and Policy Tag on the Foreign WLC

Navigate to the foreign WLC web UI. To create the policy profile navigate to **Configuration > Tags & Profiles > Policy > +Add**. When anchoring you have to use central switching.

Cisco Catalys	st 9800-L Wireless Contr	roller		
Q Search Menu Items	Configuration * > Tags & Pro	files* > Policy		
Configuration	Status V Policy Profile t dd Policy Profile	Name		 Description
(O) Administration (C) Licensing	Access Policies	QOS and AVC Mobility	Advanced of connectivity for clients associated with	this profile.
Council of the second s	Name*	CLUS-Policy-Profile	WLAN Switching Policy	
	Status		Central Switching Central Authentication	
	Passive Client	DISABLED	Central DHCP Central Association	
	CTS Policy Inline Tagging		Hex NAT/PAT	DISABLED
	SGACL Enforcement	2-65519		
	Cancel			Apply to Device

On the **Advanced** tab, the AAA override and **RADIUS** NAC are mandatory for CWA. Here you can also apply the accounting method list if you chose to make one.

Q Search Menu Items	Configuration * > Tags & Pro	ofiles* > Policy		
Dashboard	+ Add × Delete			
Monitoring >	Status \vee Policy Profile	Name		 Description
	Add Policy Profile			×
Configuration >	General Access Policies	QOS and AVC Mobility	Advanced	
Administration	WLAN Timeout		Fabric Profile	Search or Select
C Licensing	Session Timeout (sec)	1800	mDNS Service	Search or Select
X Troubleshooting	Idle Timeout (sec)	300	Hotspot Server	Search or Select
	Idle Threshold (bytes)	0	User Private Networ	k
	Client Exclusion Timeout (sec)	60	Status	
			Status	
	Guest LAN Session Timeout		Drop Unicast	
	DHCP		Umbrella	
	IPv4 DHCP Required		Umbrella Parameter Map	Not Configured
	DHCP Server IP Address			Clear
	Show more >>>		Flex DHCP Option for DNS	ENABLED
	AAA Policy		DNS Traffic Redirect	IGNORE
	Allow AAA Override		WLAN Flex Policy	
	NAC State		VLAN Central Switchin	ng 🔲
	NAC Type	RADIUS	Split MAC ACL	Search or Select
	Policy Name	default-aaa-policy 🗙 🔻	Air Time Fairness Po	blicies
	Accounting List	CLUS-Acct-Meth-L	2.4 GHz Policy	Search or Select 🗸

On the **Mobility** tab **DO NOT** check the **Export Anchor** checkbox but rather add the anchor WLC to the anchor list. Make sure to enter **Apply to Device**. As reminder, this assumes you already have a mobility tunnel setup between the two controllers

Cisco Cat	alyst 9800-L Wireless Controller			
Q, Search Menu Iteme	Configuration * > Tags & Profiles * >	Policy		
Monitoring >	Add Policy Profile			×
Configuration	General Access Policies QOS an	Id AVC Mobility	Advanced	
C Administration	Mobility Anchors			
 Licensing Troubleshooting 	Expart Anchor Static IP Mobility Acting Mobility Acting Mobility Anchors will cause the erobled deable and may result in loss of connectivity for Drag and Drop/double click/click on the arro	DEABLED WLANs to momentarily aome chents. w to add/remove Anchons		
	Available (0)	Selected (1)		
	Anchor IP	Anchor IP	Anchor Priority	
	No anchors available	192.168.160.18	B Primary (1)	• •
	Cancel			Apply to Device

In order for the APs to use this policy profile, you need to create a policy tag and apply it to the APs you

wish to use.

To create the policy tag, navigate to **Configuration > Tags & Profiles > Tags?Policy > +Add**.

Cisco Cata	alyst 9800-L Wireles	ss Controller		
Q Search Menu Items	Configuration > Ta	ags & Profiles * > Tags		
📷 Dashboard	Policy Site F	RF AP		
C Monitoring	+ Add ×			
Configuration >	Policy Tag Na	me		
Administration	Add Policy Tag	CLUS-Policy-Tag		×
© Licensing	Description	Policy Tag for CLUS		
X Troubleshooting	V WLAN-POLIC	Y Maps: 0		
	+ Add × De	lete		
	WLAN Profile		 Policy Profile 	~
		10 🔻 items per page		No items to display
	Map WLAN and Pol	licy		
	WLAN Profile*	CLUS-WLAN-Name 🗸	Policy Profile*	CLUS-Policy-Profile
		×		
	RLAN-POLICY	′ Maps: 0		
	Cancel			Apply to Device

To add this to multiple APs at the same time, navigate to **Configuration > Wireless Setup > Advanced > Start Now**. Click on the bullet bars next to **Tag APs** and add the tag to the APs you choose.

¢	Cisco Catalyst 9800-L Wireless Controller										
Q 8	Search Menu Iten	ns	Configuration * >	Wireless Setup *	> Adv	vance	d				
	Dashboard		Start			*	+	- Tag APs			
	Monitoring	>		Tags & Profiles			Numb Selec	er of APs: 3 ted Number of APs	: 3		
Z,		>	6	WLAN Profile				AP Name	~ AP Model ~	AP MAC ~	AP × A Mode S
ැරු		>	0	Policy Profile				Jays2800	AIR-AP2802I- B-K9	002a.10f3.6b60	Local E
Ô	icensing		0	Policy Tag 🛛 🧳				Jays3800	AIR-AP3802I- B-K9	70b3.1755.0520	Local E
								AP0062.ec20.122	AIR-CAP2702I- B-K9	cc16.7e6c.3cf0	Local D
X	Troubleshootir	ng	0	AP Join Profile			14	≪ 1 ⊳	10 v items per		
			0	Flex Profile		+	Tag	APs			×
			A	Site Tag 🛛 🥒		+	Та	gs			
			Ť				Po	licy CL	US-Policy-Tag 🗸		
			0	RF Profile		+	Sit	e Se	arch or Select 🔻		
			0	RF Tag 🛛 🥏		+	RF	Se	arch or Select 🔻		
				Apply			Ch	anging AP Tag(s) w	vill cause associated A	P(s) to reconnect	
			ð	Tag APs			0	Cancel			to Device

Create the Policy Profile on the Anchor WLC

Navigate to the anchor WLC web UI. Add the Policy Profile on the anchor 9800 under **Configuration** > **Tags & Profiles** > **Tags** > **Policy** > +**Add**. Make sure this matches the Policy Profile made on the foreign except for the mobility tab and the accounting list.

Here you do not add an anchor but you do check the **Export Anchor** checkbox. Do not add the accounting list here. This assumes you already have a mobility tunnel setup between the two controllers.



Note: There is no reason to associate this profile to a WLAN in a policy tag. This creates problems if you do. If you want to use the same WLAN for APs on this WLC create another policy profile for it.

Cisco Cisco Cata	lyst 9800-L Wireless Controller			
Q Search Menu Items	Configuration * > Tags & Profiles * >	Policy		
Dashboard	+ Add × Delete			
Monitoring	Add Policy Profile			×
Configuration	General Access Policies QOS and	d AVC Mobility	Advanced	
Administration	Mobility Anchors			
C Licensing	Export Anchor			
X Troubleshooting	Adding Mobility Anchors will cause the enabled V disable and may result in loss of connectivity for s	VLANs to momentarily some clients.		
	Available (1)	Selected (0)		
	Anchor IP	Anchor IP	Anchor Priority	
			Anchors not assigned	
	D Cancel			Apply to Device

Redirect ACL Config on both 9800s

Next, you need to create the redirect ACL config on both 9800s. The entries on the foreign does not matter because it is the anchor WLC applying the ACL to the traffic. The only requirement is that it is there and has some entry. The entries on the anchor have to deny access to ISE on port 8443 and permit everything else. This ACL is only applied to traffic coming in from the client so rules for the return traffic are not needed. DHCP and DNS pass through without entries in the ACL.

Cisco Cata	lyst 9800-L Wireless Co	ontroller			Welcome admin
Q Search Menu Items	Configuration * > Security	· > ACL			
Dashboard	+ Add × Delete Add ACL Setup	Associate Interfaces			×
Monitoring >	ACL Name*	CLUS-ACL	ACL Type	IPv4 Extended	
Configuration	Rules				
Administration	Sequence*		Action	permit 🔹	
© Licensing	Source Type	any 🔻			
X Troubleshooting	Destination Type	any 🔻			
	Protocol	ahp 🔹			
	Log	0	DSCP	None	
	+ Add × Delete				
	Sequence ~ Action	<pre>Source ∨ Source ∨ Vildcard</pre>	Destination V Destination Wildcard	Protocol v Port	Destination ~ Port DSCP ~ Log ~
	10 deny	any	192.168.160.99	tcp None	eq 8443 None Disabled
	100 permit	any	any	ip None	None None Disabled
		10 🔻 items per page			1 - 2 of 2 items
	Cancel				Apply to Device

Configure ISE

The last step is to configure ISE for CWA. There are a ton of options for this but this example sticks to the basics and use the default self-registered guest portal.

On ISE, you need to create an authorization profile, a policy set with an authentication policy and an authorization policy that uses the authorization profile, add the 9800(foreign) to ISE as a network device, and create a username and password to log into the network.

To create the authorization profile, navigate to **Policy > Policy Elements > Authorization > Results > Authorization Profiles**, then click **Add**. Ensure the access type returned is **ACCESS_ACCEPT**, and then set the attribute-value pairs (AVPs) that you want to send back. For CWA the redirect ACL and redirect URL are mandatory but you can also send back things like VLAN ID and session timeout. It is important that the ACL name matches the name of the redirect ACL on both the foreign and the anchor 9800.

$\leftarrow \rightarrow C$ A Not secure 19	2.168.160.99/admin/#policy/p	olicy_elements/policy	_elements_permissions/p	olicy_elements_permi	ssions_authorization/pol	icy_element
dentity Services Engine	Home	Operations Performed and the second	olicy Administration	Work Centers		
Policy Sets Profiling Posture Cl	ient Provisioning 🔽 Policy Eleme	ents				
Dictionaries	5					
Authentication Authorization Authorization Authorization Profiles Downloadable ACLs Profiling Posture Client Provisioning	Authorization Profiles > test Authorization Profile * Name C Description * Access Type A Network Device Profile Service Template Track Movement Passive Identity Tracking	LUS-AuthZ-Profile-ISE CCESS_ACCEPT the Cisco ▼ ⊕ () ()				
	Common Tasks Voice Domain Permission Web Redirection (CWA, Centralized Web Auth	n MDM, NSP, CPP) (j)	ACL CLUS-ACL	Vali	Je Self-Registered Guest Po	ortal (c 🗸

You then need to configure a way to apply the authorization profile you just created to the clients that go through CWA. To achieve this, one way is to create a policy set that bypasses authentication when using MAB and apply the authorization profile when using the SSID sent in the called station ID. Again, there are a lot of ways to accomplish this so if you need something more specific or more secure, that fine, this is just the most simple way of doing it.

To create the policy set go to **Policy > Policy Sets** and click the + button on the left side of the screen. Name the new policy set and make sure it is set to **Default Network Access** or any allowed protocol list that allows **Process Host Lookup** for MAB (to check the allowed protocol list go to **Policy > Policy Elements > Results > Authentication > Allowed Protocols**). Now, click the + sign in the middle of the new policy set you created.

dude Identity Services Engine Home	Context Visibility	Policy Administration	Work Centers				U	cense Warning 🤞	<u>а</u>	0 C	0
Policy Sets Profiling Posture Client Provisionin	ng						Click here to do vit	sibility setup Do no	ot show this	again.	×
Policy Sets							Re	setAll Hitcount	s R	eset	Save
+ Status Policy Set Name	Description	Conditions				Allov	ved Protocols / Sen	ver Sequence	Hits	Actions	View
Search						_					
O <u>CLUS-CWA-Policy-Set</u>				+		Def	ault Network Access	** +		٥	>
Default	Default policy set					Def	ault Network Access	×* +	0	٥	>
									R	eset	Save

For this policy set every time MAB is used in ISE it goes through this policy set. Later you can make authorization policies that match on the called station ID so that different results can be applied depending on the WLAN that is being used. This process is very customizable with a lot of things you can match on.

Conditions Studio		
Library	Editor	
mab ♥ 尋 □ # ⊕ 및 및 중 ऌ ₰ ₫ © ₰ ♥ ₺ ♥	Wireless_MAB Set to 'Is not'	<i>i</i>)
Wired_MAB ()		
Wireless_MAB ()	+ New AND OR	

Inside the policy set, create the policies. The authentication policy can again match on MAB but you need to change the ID store to use internal endpoints and need to change the options to continue for **Auth Fail** and **User Not Found**.

Policy Sets Profiling Posture Client Provisioning + Policy Elements		Click here to do visibility setup Do not show this again.	×
Policy Sets + CLUS-CWA-Policy-Set		ResetAll Hitcounts Reset	Save
Status Policy Set Name Description Condition	ns	Allowed Protocols / Server Sequence	Hits
Search			
CLUS-CWA-Policy-Set	reless_MAB	Default Network Access 🔹 👻 🕈	0
✓ Authentication Policy (2)			
+ Status Rule Name Conditions		Use Hits /	Actions
Search	_		
		Internal Endpoints * *	
		✓ Options	
		If Auth fail	
		CONTINUE * *	~
		If User not found	~
		CONTINUE * *	
		If Process fail	
		DROP × *	
Defend	-	All_User_ID_Stores * *	~
U Desaust		> Options	¥
Authorization Policy - Local Exceptions			
Authorization Policy - Global Exceptions			
> Authorization Policy (1)			

Once the authentication policy is set, you need to create two rules in the authorization policy. This policy reads like an ACL so the order needs to have the **Post-Auth** rule on top and the **Pre-Auth** rule on the bottom. The **Post-Auth** rule matches users that have already gone through guest-flow. This is to say, if they already signed in they can reach the rule and must stop there. If they have not signed in, they continue down the list and reach the **Pre-Auth** rule and then are redirected. It is a good idea to match the authorization policy rules with the called station ID ending with the SSID so that it only reaches the WLANs that are configured to do so.

Policy Sets +	CLUS-CWA-Policy-Set							ResetAll Hitcounts
Status	Policy Set Name	Descripti	tion	Con	litions			Allowed Protocols / Server S
Search								
0	CLUS-CWA-Policy-Set				Wireless_MAB			Default Network Access
> Authentication	n Policy (2)							
> Authorization	Policy - Local Exceptions							
> Authorization	Policy - Global Exceptions							
✓ Authorization	Policy (4)							
+ Status	Rule Name	Condition	ions			Results Profiles	Security G	iroups
Search			_	-			`	
ø	Post-CWA	AND	E Network Access-U	UseCa ation-I	se EQUALS Guest Flow	+ CLUS-Post-Auth	Select fro	n list 🔹 🕇
ø	MAE on WLAN	AND	Radius Called-Sta	ation-I	D ENDS_WITH CLUS-SSID	CLUS-AuthZ-Profile-ISE	Select fro	n list 🔹 🕈
Ø	Flex AuthZ	₽	Radius-Called-Station-ID E	ends,	WITH FLEX-CWA	(×CLUS-Flex_CWA)	Select tro	n list 🔹 🕈
0	Default					* DenyAccess	Select fro	n list 🔹 🕇

Now that the policy set is configured, you need to inform ISE about the 9800 (foreign) in order for ISE to trust it as an authenticator. This can be done by navigating to **Admin > Network Resources > Network Device >** +. You need to name it, set the IP address (or in this case the whole admin subnet), enable RADIUS, and set the shared secret. The shared secret on ISE has to match the shared secret on the 9800 or this process fails. After the config is added click the **Submit** button to save it.

altala cisco	Identity Services Engine	Home	Context Visibility	 Operations 	Policy	→ Admir	nistration	Work Centers			
► Sy	stem 🔹 Identity Management	✓ Networ	rk Resources 🕽 🕨 Devic	e Portal Management	pxGrid S	ervices	Feed Service	 Threat Centric 	NAC		
✓ Ne	twork Devices Network Device	Groups	Network Device Profiles	External RADIUS	Servers F	RADIUS S	erver Sequences	s NAC Managers	External MDM	Location Services	
Networ Default Device	& Devices t Device Security Settings	Netwo	ork Devices List > JAysh work Devices	* Name CLU	5_Net-Device	4					
			IP Address 🔻	* IP : 192.168.160).0			/ 24			
			* Network Device Group Location All Locatio IPSEC No Device Type All Device	Device Profile de C Model Name fitware Version S ons S S Types S	et To Default et To Default et To Default						
				tion Settings							
			RADIUS UDP Sett	ings	2	at a start of the					
					Shared S	Secret		Show	v		
				Use Seco	ond Shared S	Secret 🗌] ()		_		
								Show	v		
					Co/	A Port 1	700	Set	To Default		
			RADIUS DTLS Set	ttings (j)							

Finally, you need to add the username and password that the client is going to enter into the log in page in

order to validate that they must have access to the network. To do this, navigate to **Admin > Identity Management > Identity > Users > +Add** and click **Submit** after you add it. Like everything else with ISE, this is customizable and does not have to be a user stored locally but again, it is the easiest config.

cisco	dentity Service	s Engine	Home	Context Visibi	ility ► Ope	erations	Policy	- Administra	ation • W	ork Centers	
System	em 🔽 Identity I	Vanagement	Network F	Resources F	Device Portal M	lanagement	pxGrid §	Services F	eed Service	Threat Centric NAC	
✓Ident	iities Groups	External Identit	y Sources	Identity Source	Sequences	 Settings 					
Users Latest M	anual Network Sc	Can Results	Network Net Nar Stat Em Pas Cha Cha Cha Subr	Access Users Lis work Access I ne CLUS-User us Enable ail asswords sword Type: pgin Password ble Password ble Password chame ble Password ble Passwo	st > New Netw User Internal Users Password Password Internal Users Password Internal Users Internal Users Internal Users Internal Users Internal Users Internal Users Internal Usersword Internal Users Internal Usersword Internal Users Internal Use	rork Access 1	Jser	Re-Enter Passv	vord	Generate Pa Generate Pa	essword () essword ()

Configure a Catalyst 9800 Anchored to an AireOS WLC



Catalyst 9800 Foreign Configuration

Do the same, previous steps, skipping the Create the policy profile on the anchor WLC section.

AAA Configs on the Anchor AireOS WLC

Add the server to the WLC by going to **Security** > **AAA** > **RADIUS** > **Authentication** > **New**. Add the server IP address, shared secret, and support for CoA.



WLAN Config on the AireOS WLC

To create the WLAN navigate to WLANs > Create New > Go.

Configure the **Profile Name**, WLAN ID, and SSID then click **Apply**.



This must take you to the WLAN configuration. On the **General** tab, you can add the interface you want the clients to use if you are not going to configure ISE to send it in the AVPs. Next navigate to the **Security** > **Layer2** tab and match the **Layer 2 Security** config you used on the 9800 and enable **MAC Filtering**.



Now move over to the **Security > AAA Servers** tab and set the ISE server as the **Authentication Servers**. **Do Not** set anything for the **Accounting Servers**. Uncheck the **Enable** box for accounting.

ahaha		Sage Configuration Ping	Logout Befresh
cisco	Monitor Munie Controller Wireless security Management Commands Help feedback		🔒 Home
WLANs	WLANs > Edit 'CLUS-WLAN-Name'	< Back	Apply
VILANS	General Security QoS Policy-Mapping Advanced		
Advanced	Layer 2 Layer 3 AAA Servers		î.
	Select AAA servers below to override use of default servers on this WLAN EAOLUS Server RADUX Servers RADUX Servers RADUX Servers RADUX Servers Reserver 1 Prior None None None None None None None None		

While still in the WLAN configs, move over to the **Advanced** tab and enable **Allow AAA Override** as well as change the **NAC State** to **ISE NAC**.

WLANS WLANS > Edit: 'CLUS-WLAN-Name' Central WLANS General Security QoS Policy-Mapping Advanced Difc? WLANS More Add Override Enabled WLANS More add Override Enabled Jamestic Barley Enabled Difc? Difc? Berver Override Enabled Difc? Berver Override Enabled Override Information Enabled OLCP Override Information Enabled OLLP Override Information Enabled OLLING (ICLS) Informatin Allowed Cleafts Pride Pade OLLING (ICLS) </th <th></th> <th>MONITOR WIANS CONTROLLER WI</th> <th>IRFLESS SECURITY MANAGEMENT (</th> <th>MMANDS HELP FEEDBACK</th> <th>Sage Configuration Bing Logout Befresh</th>		MONITOR WIANS CONTROLLER WI	IRFLESS SECURITY MANAGEMENT (MMANDS HELP FEEDBACK	Sage Configuration Bing Logout Befresh
WLARS WLARS Centeral Socurity QoS Policy-Mapping Advanced Mutanization Advanced Costage Co	WLANs	WLANs > Edit 'CLUS-WLAN-Nam	16'		< Back Apply
> Advanced Inovide Enabled Overrage Hole Detection Enabled DHCP Coverage Hole Detection Enabled DHCP detection Arower HE Enabled DHCP Addx. Assignment Required Arower HE Enabled OcAP Dagnotic Channel HE Enabled OcAP Deprotic Channel HE Intel® None ♥ URL ACL IPv4 [Brone ♥ IPv6 [Brone ♥ URL ACL None ♥ Management Frame Protection (HFP) URL ACL None ♥ MPP Clent Pervotection # Optional ♥ Clent Endugin Atian Detabled DTTM Period (means) Teneout Value (lents) # 0 002.11aln (1 - 255) 1 Static IP Tunneling HE Enabled 002.11aln (1 - 255) 1 Hainoum Allowed Clents # 0 0 Viri-B Dret Cleints Paley 0 0 Wir-B Cret Cleints Paley 0 0 Hainoum Allowed Clents # 0 0 Uri-B Cret Cleints Paley 0 0 Hainoum Allowed Clents # 0 0 Uri-B Cret Cleints Paley	✓ WLANS WLANS	General Security QoS Pol	licy-Mapping Advanced		
	Advanced	Allow AAA Override Coverage Hole Detection Enable Session Timeout Aironet IE Diagnotic Channel II Override Interfete ACL Laver2 Acl URL ACL P2P Biocking Action Client Exclusion I Maximum Allowed Clients II Static IP Tunneling II Wirh Forett Clients Pirky Hanimum Allowed Clients Per AP Radio Client HotSpot Configuration	C trabled C trabled Tenebic (see) Cabled IN4 (None	DHCP DHCP Server DHCP Adds. Assignment DHCP	

The last thing is to anchor it to itself. For this, navigate back to **WLANs** page and hover over the blue box on the right of the **WLAN > Mobility Anchors**. Set **Switch IP Address (Anchor)** to local and click the

Mobility Anchor Create button. It must then show up with priority 0 anchored local.

սիսիս cisco	MONITOR V	<u>V</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>o</u> mmands	HELP	<u>F</u> EEDBACK		
WLANs	WLANs										
VLANs	Current Filter:	Nor	ne	[Change Filte	er] [Clear Filter]					Create New	Go
Advanced	U WLAN ID	Туре	Profi	e Name		WLAN SSI	D		Admin Status	Security Policies	
		WLAN	CLUS	WLAN-Name		CLUS-SSID			Enabled	MAC Filtering	Pamera
											Mobility Anchors
											Foreign Maps
											Service Advertisements
											Hotspot 2.0

Redirect ACL on the AireOS WLC

This is the final config needed on the AireOS WLC. To create the redirect ACL navigate to **Security** > **Access Control Lists** > **Access Control Lists** > **New**. Enter the ACL name (this must match what is sent in the AVPs) and click **Apply**.

ahaha		age Configuration Bing Logout Befresh
cisco	Monitor Wilang Controller Wireless Security Management Commands Help Feedback	A Home
Security	Access Control Lists > New	< Back Apply
General RADIUS	Access Control List Name CLUS-ACL	
Authentication Accounting Fallback	ACLType IPv4 OIPv6	
DNS Downloaded AVP TACACS+		

Now click the name of the ACL you just created. The click the **Add New Rule** button. Unlike the 9800 controller, on the AireOS WLC, you configure a permit statement for traffic that is allowed to reach ISE without being redirected. DHCP and DNS are allowed by default.

սիսիս								~						Sa <u>v</u> e Co	nfiguration	Ping	Logout	Refrest
CISCO	MONT	TOR <u>W</u> L	ANs :	CONTROLLER	WIREL	ESS	SECURITY	M	1 <u>A</u> NAGEMENT	COMMANDS	HELP	FEEDBACK					6	<mark>I</mark> ome
Security	Acce	ess Cont	rol Lis	sts > Edit										[< Back	A	dd New R	Rule
AAA General RADIUS Authentication Accounting Fallback	Gene Access	e ral E List Name		CLUS-ACL					_									
DNS Downloaded AVR	Deny	counters		·														_
▶ TACACS+	Seq	Action	Sourc	ce IP/Mask	D	estinat	ion IP/Ma	sk	Protocol	Source Po	rt	Dest Port	DSCP	Direction	Number	of Hits		
LDAP Local Net Users	т	Permit	0.0.0.	.0 .0	/ 19	2.168.1	160.99 255.255	/	ТСР	Any		8443	Any	Any	273			
MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	2	Permit	192.1 255.2	68.160.99 55.255.255	/ 0.	0.0.0 0.0.0		/	ТСР	8443		Any	Any	Any	566			J
Local EAD																		
Advanced FAD																		
Advanced EAP																		
Priority Order																		
Certificate																		
Access Control Lists Access Control Lists CPU Access Control																		

Configure ISE

The last step is to configure ISE for CWA. There are several options for this but this example uses the basics and the default self-registered guest portal. On ISE, you need to create an authorization profile, a policy set with an authentication policy and an authorization policy that uses the authorization profile. Add the 9800(foreign) to ISE as a network device and create a username and password to log into the network.

To create the authorization profile go to**Policy > Policy Elements > Authorization > Results > Authorization Profiles > +Add**. Make sure the access type returned is **ACCESS_ACCEPT**, and then set the AVPs that you want to send back. For CWA the redirect ACL and redirect URL are mandatory but you can also send back like VLAN ID, for example, and session timeout. It is important that the ACL name matches the name of the redirect ACL on both the foreign and the anchor WLC.

$\leftarrow \rightarrow C$ A Not secure 19	2.168.160.99/admin/#policy/policy_elements/policy_elements_permissions/policy_elements_permissions_authorization/policy	/_element
dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	
Policy Sets Profiling Posture Cl	ant Provisioning Policy Elements	
Dictionaries		
Authentication Authorization Authorization Profiles Downloadable ACLs Profiling Posture Client Provisioning	Authorization Profiles > test Authorization Profile * Name CLUS-AuthZ-Profile-ISE Description * Access Type ACCESS_ACCEPT Network Device Profile Cisco]
	Common Tasks Voice Domain Permission Web Redirection (CWA, MDM, NSP, CPP) ACL CLUS-ACL Value Self-Registered Guest Porta	al (c 🗸

You then need to configure a way to apply the authorization profile you just created to the clients that go through CWA. To achieve this, one way is to create a policy set that bypasses authentication when using MAB and apply the authorization profile when using the SSID sent in the called station ID. Again, there are a lot of ways to accomplish this so if you need something more specific or more secure, that fine, this is just the most simple way of doing it. To create the policy set go to**Policy > Policy Sets** and click the **+** button on the left side of the screen. Name the new policy set and make sure it is set to **Default Network Access** or any allowed protocol list that allows **Process Host Lookup** for MAB (to check the allowed protocol list go to **Policy > Policy Elements > Results > Authentication > Allowed Protocols**). Now click the **+** sign in the middle of the new policy set you created.

dude Identity Services Engine Home + Context Visibility + Operations	Policy Administration Work Centers	License Warning 🔺 🔍 🔍 🔘 🔘
Policy Sets Profiling Posture Client Provisioning + Policy Elements	—	Click here to do visibility setup Do not show this again.
Policy Sets		ResetAll Hitcounts Reset Save
+ Status Policy Set Name Description	Conditions	Allowed Protocols / Server Sequence Hits Actions View
Search		
O <u>CLUS-CWA-Policy-Set</u>	+	Default Network Access * * + 🌣 🔉
Default Default Default		Default Network Access ** + 0 🗘 >
		Durt Con

For this policy set every time MAB is used in ISE it can go through this policy set. Later you can make authorization policies that match on the called station ID so that different results can be applied depending on the WLAN that is being used. This process is very customizable with a lot of things you can match on

Inside the policy set, create the policies. The authentication policy can again match on MAB but you need to change the ID store to use **Internal Endpoints** and you need to change the options to continue for **Auth Fail** and **User Not Found**.

Policy Sets Profiling Posture Client Provisioning Policy Elements			Click here to do visibility setup Do not show this	again.	×
Policy Sets → CLUS-CWA-Policy-Set			ResetAll Hitcounts R	eset	Save
Status Policy Set Name Description Con	nditions		Allowed Protocols / Server Se	quence	Hits
Search					
CLUS-CWA-Policy-Set	Wireless_MAB		Default Network Access	+	0
Authentication Policy (2)					
Status Rule Name Conditions			Use	Hits	Actions
✓ ⊘ <u>CLUS MAB</u> -Condition Wireless_MAB		(Internal Endpoints Coptions If Auto Ital CONTINUE CONTINUE CONTINUE If User of bund CONTINUE If Process tal DROP		¢
⊘ Default			Al_User_ID_Stores * * > Options	۰	٥
Authorization Policy - Local Exceptions					
Authorization Policy - Global Exceptions					
> Authorization Policy (1)					

Once the authentication policy is set, you need to create two rules in the authorization policy. This policy reads like an ACL so the order needs to have the **Post-Auth** rule on top and the **Pre-Auth** rule on the bottom. The **Post-Auth** rule matches users that have already gone through guest-flow. This is to say if they already signed in they reacg that rule and stop there. If they have not signed in they continue down the list and hit the **Pre-Auth** rule getting the redirect. It is a good idea to match the authorization policy rules with the called station ID ending with the SSID so that it only hits for WLANs that are configured to do so.

Policy Sets +	CLUS-CWA-Policy-Set								Reset	All Hitcounts
Status	Policy Set Name	Descripti	tion	Con	itions				Allowed	Protocols / Server S
Search										
0	CLUS-CWA-Policy-Set				Wireless_MAB				Default	Network Access
> Authentication	n Policy (2)									
> Authorization	Policy - Local Exceptions									
> Authorization	Policy - Global Exceptions									
✓ Authorization	Policy (4)									
+ Status	Rule Name	Condition	ions				Results Profiles	Se	ecurity Groups	
0	Post-CWA	AND	E Network Access Image: Control of the second	s-UseCa Station-I	se EQUALS Guest Flow D ENDS_WITH CLUS-SSID		CLUS-Post-Auth	+	Select from list	- +
ø	MAS on WLAN	AND	Radius Called-St	Station-I	D END\$_WITH CLUS-SSID		CLUS-AuthZ-Profile-ISE	+	Select from list	• •
Ø	Flex AuthZ	₽	Radius-Called-Station-ID	ENDS,	WITH FLEX-CWA		CLUS-Flex_CWA	+ 8	Select from list	- +
Ø	Default						* DenyAccess	+ 8	Select from list	- +

Now that the policy set is configured, you need to inform ISE about the 9800 (foreign) in order for ISE to trust it as an authenticator. This can be done atAdmin > Network Resources > Network Device > +. You need to name it, set the IP address (or in this case the whole admin subnet), enable RADIUS, and set the shared secret. The shared secret on ISE has to match the shared secret on the 9800 or this process fails. After the config is added hit the submit button to save it.

dentity Services Engine	Home	Operations Policy	- Administration	Work Centers		
System Identity Management	Network Resources) Device	Portal Management pxGri	Services Feed Service	Threat Centric N	IAC	
Network Devices Network Device Gro	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers	External MDM	Location Services
System Identity Management Vetwork Devices Network Devices Network Devices Default Device Device Security Settings	Network Resources) Device Pups Network Device Profiles Network Devices List > JAysNe Network Devices IP Address	Portal Management pxGrid External RADIUS Servers t * Name CLUS_Net-Der Description * IP : 192.168.160.0 Device Profile dtt Cisco Model Name ware Version s S Set To Defa Set To Defa	Service RADIUS Server Sequences ADIUS Server Sequences ADIUS ADIUS Protocol RADIUS A Secret ADIUS A Secret A ADIUS A ADIUS A ADIUS A ADIUS A ADIUS A ADIUS A	Threat Centric N NAC Managers	VAC External MDM	Location Services
			Cod Bad	Show		
			1700	Set T	o Default	

Finally, you need to add the username and password that the client is going to enter into the log in page in order to validate that they must have access to the network. This is done underAdmin > Identity Management > Identity > Users > +Addand make sure to click **Submit** after you add it. Like everything else with ISE, this is customizable and does not have to be user stored locally but again, it is the easiest config.

altalta cisco	Identity Servic	es Engine	Home •	Context Visibility	▸ Operations	• Policy	 Administration 	m 🕨 Work	Centers	
► Sy	stem 🔽 Identity	Management	Network Res	ources	e Portal Management	pxGrid §	Services + Feed	d Service	Threat Centric NAC	
▼ Ide	entities Groups	External Identit	y Sources Io	dentity Source Sec	quences F Settings					
Users Latest	Identity Servic	Anagement External Identi Con Results	Home Network Result Sources Network Acco Change	Context Visibility ources → Devic dentity Source Sec cess Users List > ork Access User CLUS-User CLUS-Use	Operations Poperations Poperations Settings New Network Access	Policy pxGrid S User	Re-Enter Passwor	n + Work	Centers Threat Centric NAC Generate Password Generate Password	
			 ✓ Acco □ Di ✓ User iii Select Submit 	unt Disable Po isable account if d Groups : an item Cancel	licy ate exceeds 2020-0	7-17		(yyyy-mm-dd)		

Differences in Config when the AireOS WLC is the Foreign and the Catalyst 9800 is the Anchor

If you want the AireOs WLC to be the foreign controller the config is the same as previously described with a few differences.

- 1. AAA accounting is never done on the anchor so the 9800 would not have an accounting method list and the AireOS WLC would have accounting enabled and pointing to ISE.
- 2. The AireOS would need to anchor to the 9800 instead of itself. In the Policy Profile, the 9800 would not have an anchor selected but would have the **Export Anchor** box checked.
- 3. It is important to note that when AireOS WLCs export the client to the 9800 there is no concept of policy profiles. It only sends the WLAN Profile Name. Therefore, the 9800 applies the WLAN Profile Name sent from AireOS to both the WLAN Profile Name and the Policy Profile Name. When anchoring from an AireOS WLC to a 9800 WLC the WLAN Profile Name on both WLCs, and Policy Profile Name on the 9800, must match.

Verify

To verify the configs on the 9800 WLC run these commands:

• AAA:

Show Run | section aaa|radius

• WLAN:

Show wlan id <wlan id>

• Policy Profile:

Show wireless profile policy detailed <profile name>

• Policy Tag:

Show wireless tag policy detailed <policy tag name>

• ACL:

Show IP access-list <ACL name>

• Verify mobility is up with the anchor:

Show wireless mobility summary

To verify the configs on the AireOS WLC run the commands.

• AAA:

Show radius summary



Note: RFC3576 is the CoA config.

• WLAN:

Show WLAN <wlan id>

• ACL:

Show acl detailed <acl name>

• Verify mobility is up with the foreign:

Troubleshoot

Troubleshooting looks different depending on what point in the process the client stops. For example, if the WLC never gets a response from ISE on MAB, the client would be stuck in the **Policy Manager State: Associating** and would not be exported to the anchor. In this situation, you would only troubleshoot on the foreign and you would need to collect an RA trace and a packet capture for traffic between the WLC and ISE. Another example would be that MAB has passed successfully but the client does not receive the redirect. In this case, you need to make sure the foreign received the redirect in the AVPs and applied it to the client. You also need to check the anchor to make sure the client is there with the correct ACL. This scope of troubleshooting is outside of the design of this article (check the Related Information for a generic client troubleshooting guidelines).

For more help with troubleshooting CWA on the 9800 WLC please see the Cisco Live! presentation DGTL-TSCENT-404.



Note: Only registered Cisco users have access to internal Cisco tools and information.

Catalyst 9800 troubleshooting information

Client Details

show wireless client mac-address <client mac> detail

Here you must look at the Policy Manager State, Session Manager > Auth Method, Mobility Role.

You can also find this information in the GUI under **Monitoring > Clients**.

Embedded Packet Capture

From the CLI the command starts **#monitor capture <capture name>** then the options come after that.

From the GUI go to **Troubleshoot > Packet Capture > +Add**.

RadioActive Traces

From the CLI:

```
debug wireless mac|ip <client mac|ip>
```

Use the no form of the command to stop it. This is logged to a file in bootflash named **ra_trace** then the client MAC or IP address and the date and time.

From the GUI navigate to **Troubleshoot > Radioactive Trace > +Add**. Add the client mac or ip address, click **Apply**, then hit start. After you have gone through the process a few times stop the trace, generate the log, and download it to your device.

AireOS Troubleshooting information

Client Details

From the CLI, show client details <client mac>.

From the GUI, **Monitor > Clients**.

Debugs from the CLI

Debug client <client mac>

Debug mobility handoff

Debug mobility config

Related Information

- Building Mobility Tunnels with 9800 Controllers
- Wireless Debugging and Log Collection on 9800
- <u>Cisco Technical Support & Downloads</u>