Konfigurieren von Central Web Authentication (CWA) auf Catalyst 9800 WLC und ISE

Inhalt

Einleitung
<u>Voraussetzungen</u>
Anforderungen
Verwendete Komponenten
<u>Hintergrundinformationen</u>
Konfigurieren
Netzwerkdiagramm
AAA-Konfiguration auf dem 9800 WLC
WLAN-Konfiguration
Richtlinienprofilkonfiguration
Richtlinien-Tag-Konfiguration
Richtlinien-Tag-Zuweisung
Umleiten der ACL-Konfiguration
Umleitung für HTTP oder HTTPS aktivieren
ISE-Konfiguration
Hinzufügen von 9800 WLC zu ISE
Neuen Benutzer auf ISE erstellen
Erstellen des Autorisierungsprofils
Konfiguration der Authentifizierungsregel
Konfiguration der Authentifizierungsregeln
NUR Flexconnect Local Switching Access Points
Zertifikate
Überprüfung
Fehlerbehebung
Checkliste
Service-Port-Unterstützung für RADIUS
Debuggen sammeln
Beispiele

Einleitung

In diesem Dokument wird die Konfiguration eines CWA Wireless LAN auf einem Catalyst 9800 WLC und der ISE beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie mit der Konfiguration der 9800 Wireless LAN Controller (WLC) vertraut sind.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- 9800 WLC Cisco IOS® XE Gibraltar v17.6.x
- Identity Service Engine (ISE) v3.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Der CWA-Prozess ist hier dargestellt. Hier sehen Sie den CWA-Prozess eines Apple-Geräts als Beispiel:



Konfigurieren

Netzwerkdiagramm



AAA-Konfiguration auf dem 9800 WLC

Schritt 1: Fügen Sie den ISE-Server der 9800 WLC-Konfiguration hinzu.

Navigieren Sie zu den RADIUS-Serverinformationen, Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add und geben Sie sie wie in den Bildern dargestellt ein.

Q Search Menu Items	Configuration • > S	Security > AAA	
Dashboard	+ AAA Wizard		
Monitoring	> Servers / Groups	AAA Method List A	AA Advanced
	+ Add ×	Delete	
O Administration	RADIUS	Servers Se	erver Groups
C Licensing	TACACS+	Name	Y Address
K Troubleshooting	LDAP	0	▶ ▶ 10 ▼ items per page

Stellen Sie sicher, dass die Unterstützung für CoA aktiviert ist, wenn Sie zukünftig Central Web Authentication (oder irgendeine Art der Sicherheit, die CoA erfordert) verwenden möchten.

Create AAA Radius Server				×
Name*	ISE-server	Support for CoA (i)	ENABLED	
Server Address*	10.00101101	CoA Server Key Type	Clear Text 🔻	
PAC Key	0	CoA Server Key (i)		
Кеу Туре	Clear Text 🔻	Confirm CoA Server Key		
Key* (i)		Automate Tester	0	
Confirm Key*				
Auth Port	1812			
Acct Port	1813			
Server Timeout (seconds)	1-1000			
Retry Count	0-100			
Cancel				Apply to Device



Hinweis: Achten Sie bei Version 17.4.x und höher darauf, den CoA-Serverschlüssel auch zu konfigurieren, wenn Sie den RADIUS-Server konfigurieren. Verwenden Sie denselben Schlüssel wie den gemeinsamen geheimen Schlüssel (bei ISE sind sie standardmäßig identisch). Optional soll ein anderer Schlüssel für CoA als der gemeinsame geheime Schlüssel konfiguriert werden, wenn dies der Grund ist, für den der RADIUS-Server konfiguriert wurde. In Cisco IOS XE 17.3 wurde für die Webbenutzeroberfläche lediglich derselbe gemeinsame geheime Schlüssel wie für den CoA-Schlüssel verwendet.

Schritt 2: Erstellen Sie eine Liste mit Autorisierungsmethoden.

 $Navigieren \ Sie \ Configuration > Security > AAA > \ AAA \ Method \ List > Authorization > + \ Add \ wie \ im \ Bild \ dargestellt \ zu.$

Q Search Menu Items	Authentication Authoriza	ition and Accounting			
 Dashboard Monitoring > 	AAA Method List	Servers / Groups	AAA Advanced		
Configuration	General Authentication	+ Add × Delete			
Troubleshooting	Authorization	Name default Image: state	Type v network 0 v items per page	Group Type local	V Group

Quick Setup: AAA Authorization

Method List Name*	CWAauthz		
Type*	network	v	
Group Type	group	v	
Fallback to local			
Authenticated			
Available Server Groups	Assi	gned Server Groups	
ldap tacacs+	> < »	radius	

Schritt 3. (Optional) Erstellen Sie eine Abrechnungsmethodenliste, wie im Bild dargestellt.



Hinweis: CWA funktioniert nicht, wenn Sie sich aufgrund der Cisco Bug-ID <u>CSCvh03827</u> für den Lastenausgleich (über die CLI-Konfiguration von Cisco IOS XE) Ihrer Radius-Server entscheiden. Der Einsatz externer Load Balancer ist in Ordnung. Stellen Sie jedoch sicher, dass Ihr Load Balancer auf Client-Basis funktioniert, indem Sie das RADIUS-Attribut der anrufenden Station-ID verwenden. Die Verwendung eines UDP-Quell-Ports ist kein unterstützter Mechanismus zum Ausgleichen von RADIUS-Anfragen vom 9800.

Schritt 4: (Optional) Sie können die AAA-Richtlinie so definieren, dass der SSID-Name als Attribut "Called-Station-ID" gesendet wird. Dies kann nützlich sein, wenn Sie diese Bedingung später im Prozess auf der ISE nutzen möchten.

Navigieren Sie zu Configuration > Security > Wireless AAA Policy der standardmäßigen AAA-Richtlinie, und bearbeiten Sie sie, oder erstellen Sie eine neue Richtlinie.



Sie können Option 1 auswählenSSID. Beachten Sie, dass die angerufene Stations-ID auch dann die AP-MAC-Adresse an den SSID-Namen anhängt, wenn Sie nur SSID auswählen.

Edit Wireless AAA Policy

Policy Name*	default-aaa-policy
Option 1	SSID
Option 2	Not Configured 🔻
Option 3	Not Configured

WLAN-Konfiguration

Schritt 1: WLAN erstellen.



Schritt 2: Geben Sie die allgemeinen WLAN-Informationen ein.

Add WLAN			×
General Security	Advanced		
Profile Name*	cwa-ssid	Radio Policy (i)	
SSID*	cwa-ssid	Show slot configuration	
WLAN ID*	4	5 GHz ENABLED	
Status		2.4 GHZ	
Broadcast SSID	ENABLED	802.11b/g Policy 802.11b/g 🔻	

Schritt 3: Navigieren Sie zur Security Registerkarte, und wählen Sie die gewünschte Sicherheitsmethode aus. In diesem Fall werden nur die MAC-Filterung und die AAA-Autorisierungsliste (die Sie in Schritt 2 im AAA Configuration Abschnitt erstellt haben) benötigt.

Add WLAN			×
General Security	Advanced		
Layer2 Layer3 A	AA		
Layer 2 Security Mode	None 🗸	Lobby Admin Access	
MAC Filtering		Fast Transition	
OWE Transition Mode	O	Over the DS Reassociation Timeout	20
Authorization List*	CWAauthz 🔻 (i)		

CLI:

#config t
(config)#wlan cwa-ssid 4 cwa-ssid
(config-wlan)#mac-filtering CWAauthz
(config-wlan)#no security ft adaptive
(config-wlan)#no security wpa
(config-wlan)#no security wpa wpa2

(config-wlan)#no security wpa wpa2 ciphers aes (config-wlan)#no security wpa akm dot1x (config-wlan)#no shutdown

Richtlinienprofilkonfiguration

In einem Richtlinienprofil können Sie den Clients neben anderen Einstellungen (wie Zugriffskontrolllisten (ACLs), Quality of Service (QoS), Mobility Anchor, Timer usw.) festlegen, welchem VLAN sie zugewiesen werden sollen.

Sie können entweder Ihr Standardrichtlinienprofil verwenden oder ein neues erstellen.

GUI:

Schritt 1: Erstellen Sie eine neue Policy Profile.

Navigieren Sie zu, Configuration > Tags & Profiles > Policy und konfigurieren Sie Ihr, default-policy-profile oder erstellen Sie ein neues.

Q Search Menu Items		Policy Profile		
n Dashboard		+ Add X Delete		
 Monitoring 	>	Policy Profile Name	\sim	Description
		voice		
Configuration	>	default-policy-profile		default policy profile
S Administration	>	Image: Image of the second		

Stellen Sie sicher, dass das Profil aktiviert ist.

Edit Policy Profile			×
Disabling a Policy or co	nfiguring it in 'Enabled' state, will re	sult in loss of connectivity for clients associ	ated with this Policy profile.
General Access Policies	QOS and AVC Mobility	Advanced	
Name*	default-policy-profile	WLAN Switching Policy	
Description	default policy profile	Central Switching	
Status		Central Authentication	
Passive Client	DISABLED	Central DHCP	ENABLED
Encrypted Traffic Analytics	DISABLED	Flex NAT/PAT	DISABLED
CTS Policy			
Inline Tagging	D		
SGACL Enforcement	O		
Default SGT	2-65519		

Schritt 2: Wählen Sie das VLAN aus.

Navigieren Sie zur Access Policies Registerkarte, und wählen Sie im Dropdown-Menü den VLAN-Namen aus, oder geben Sie die VLAN-ID manuell ein. Konfigurieren Sie keine ACL im Richtlinienprofil.

dit Policy Profile			
Disabling a Policy or cont	figuring it in 'Enabled' state, will result in loss of com	nectivity for clients as	ssociated with this Policy profil
General Access Policies	QOS and AVC Mobility Advanced		
RADIUS Profiling	D	WLAN ACL	
HTTP TLV Caching		IPv4 ACL	Search or Select 🗸
DHCP TLV Caching	D	IPv6 ACL	Search or Select 🔻
WLAN Local Profiling		URL Filters	
Global State of Device Classification	Disabled (i)	Pre Auth	Search or Select 🗸
Local Subscriber Policy Name	Search or Select	Post Auth	Search or Select 🔹
VLAN			
VLAN/VLAN Group	VLAN1416 🔻		
Multicast VLAN	Enter Multicast VLAN		

Schritt 3: Konfigurieren Sie das Richtlinienprofil so, dass es ISE-Überschreibungen (Allow AAA Override) und Change of Authorization (CoA) (NAC State) zulässt. Sie können optional auch eine Abrechnungsmethode angeben.

Edit Policy Profile

Disabling a Policy or co	nfiguring it in 'Enabled' state, will result in I	oss of connectivity for clier	nts associated with this Policy profile.
General Access Policies	QOS and AVC Mobility	Advanced	
WLAN Timeout		Fabric Profile	Search or Select
Session Timeout (sec)	1800	Link-Local Bridging	0
Idle Timeout (sec)	300	mDNS Service Policy	default-mdns-ser
Idle Threshold (bytes)	0	Hotspot Server	Search or Select 🚽
Client Exclusion Timeout (sec)	60	User Defined (Priva	te) Network
Guest LAN Session Timeout	0	Status	0
DHCP		Drop Unicast	0
IPv4 DHCP Required	0	DNS Layer Security	1
DHCP Server IP Address		DNS Layer Security Parameter Map	Not Configured Clear
AAA Policy		Flex DHCP Option for DNS	
Allow AAA Override		Flex DNS Traffic Redirect	IGNORE
NAC State		WLAN Flex Policy	
NAC Type	RADIUS	VLAN Central Switchi	ing 🖸
Policy Name	default-aaa-policy × 👻	Split MAC ACL	Search or Select 🔹
Accounting List	CWAacct 🗸 (i) 🗙	Air Time Fairness P	olicies
WGB Parameters		2.4 GHz Policy	Search or Select 🗸
Broadcast Tagging		5 GHz Policy	Search or Select
WGB VLAN	0	EoGRE Tunnel Profi	les
Policy Proxy Settings		Tunnel Profile	Search or Select
ARP Proxy	DISABLED		

IPv6 Proxy

None

•

config # wireless profile policy <policy-profile-name> # aaa-override
nac
vlan <vlan-id_or_vlan-name>
accounting-list <acct-list>

no shutdown

Richtlinien-Tag-Konfiguration

Sie verbinden Ihre SSID innerhalb des Richtlinien-Tags mit Ihrem Richtlinienprofil. Sie können entweder ein neues Richtlinien-Tag erstellen oder das Standard-Richtlinien-Tag verwenden.

Hinweis: Das default-policy-Tag ordnet dem default-policy-Profil automatisch alle SSIDs mit einer WLAN-ID zwischen 1 und 16 zu.
 Es kann nicht geändert oder gelöscht werden. Wenn Sie über ein WLAN mit der ID 17 oder höher verfügen, kann das default-policy-Tag nicht verwendet werden.

GUI:

Navigieren Sie zu Configuration > Tags & Profiles > Tags > Policy und fügen Sie ggf. ein neues hinzu, wie im Bild gezeigt.

Со	nfigu	ration → Tags & Profiles → Tags		
Po	licy	Site RF AP		
	+	Add × Delete		
		Policy Tag Name	T	Description
		default-policy-tag		default policy-tag
		local-site-policy-tag		
	M	 ■ 1 ■ 10 ■ items per page 		

Verknüpfen Sie Ihr WLAN-Profil mit dem gewünschten Richtlinienprofil.

Add Policy Tag			×
Name*	cwa-policy-tag		
Description	Enter Description		
V WLAN-POLIC	Y Maps: 1		
+ Add X Dela	ete		
WLAN Profile		▼ Policy Profile	T
Cwa-ssid		default-policy-profile	
K ≪ 1 ⊨ E	10 V items per page		1 - 1 of 1 items
RLAN-POLICY	Maps: 0		
Cancel			Apply to Device

CLI:

config t # wireless tag policy <policy-tag-name> # wlan <profile-name> policy <policy-profile-name>

Richtlinien-Tag-Zuweisung

Weisen Sie den erforderlichen APs das Richtlinien-Tag zu.

GUI:

Um das Tag einem AP zuzuweisen, navigieren Sie zu, Configuration > Wireless > Access Points > AP Name > General Tags nehmen Sie die erforderliche Zuweisung vor, und klicken Sie dann auf Update & Apply to Device.

Edit AP								
General	Interfaces	High Availability	Inventory	/ ICap	Advanced	Support Bundle		
General				Tags				
AP Name*				A Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is				
Location	ĸ	default location		not allowed while changing lags.				
Base Rad	dio MAC	1010 0x10 0x00						
Ethernet	MAC	with 667 yrst		Policy		cwa-policy-tag		
Admin St	atus	ENABLED		Site		default-site-tag		
AP Mode		Local 🗸		RF		default-rf-tag 🔻		
Operation Status		Reaistered		Write Tag Cor	nfig to AP	i		

W Hinweis: Beachten Sie, dass nach dem Ändern des Richtlinien-Tags an einem AP die Verknüpfung mit dem 9800 WLC verloren geht und die Verbindung innerhalb von ca. 1 Minute wiederhergestellt wird.

Um dieselbe Policy Tag (Richtlinien-Tag) mehreren APs zuzuweisen, navigieren Sie zu Configuration > Wireless > Wireless Setup > Advanced > Start Now.



Configuration • > Wireless Setup • > Advanced	d Show M	le How 📀								
« Start	+ Tag APs Number of APs: 2									
Tags & Profiles	Selected Number	of APs: 2								
🚯 WLAN Profile 🔠 +-	AP T Name	AP T Model		Serial Y Number	AP T Mode	Admin Y Status	Operation Y Status	Policy Y Tag	Site T ag	RF Tag
Policy Profile		AIR- AP1815I- E-K9	****	-	Flex	Disabled	Registered	local- site- policy-tag	flex- site-tag	defa rf-ta
● Policy Tag ● III +		AIR- AP1815I- E-K9	-		Local	Enabled	Registered	default- policy-tag	default- site-tag	defa rf-ta
AP Join Profile H	R 4 1	▶ ►	10 🔻 items per	page				1 - 2 c	of 2 items	¢
 Policy Tag		AIR- AP1815I- E-K9	10 y items per	page	Local	Enabled	Registered	default- policy-tag 1 - 2 c	default- site-tag	defa rf-ta

Wählen Sie den gewünschten Tag aus und klicken Sie wie im Bild dargestellt aufSave & Apply to Device.

l	Tag APs		×
	Tags		
	Policy	cwa-policy-tag	
	Site	Search or Select	
	RF	Search or Select	
	Changing AP Tag connected client	g(s) will cause associated AP(s) to rejoin and disrupt (s)	
	Cancel	Apply to Devi	ce

CLI:

Umleiten der ACL-Konfiguration

Schritt 1: Navigieren Sie zu, Configuration > Security > ACL > + Add um eine neue ACL zu erstellen.

Add ACL Setup				×
ACL Name*	REDIRECT	ACL Type	IPv4 Extended v	
Rules				
Sequence*	1	Action	deny	
Source Type	any 🔻			
Destination Type	Host	Host Name*	<ise-ip></ise-ip>	eld is mandatory
Protocol	ip 🔹			
Log		DSCP	None v	
+ Add × Delete				
Sequence 😒	Source V Source Wildcard	Destination v Destination IP Wildcard	V Source V Destination Protocol V Port Port	DSCP v Log v
H 4 0 > H 1	0 🔻 items per page			No items to display
Cancel				Apply to Device

Sie müssen den Traffic zu Ihren ISE-PSNs-Knoten sowie DNS verweigern und den Rest zulassen. Bei dieser Umleitungs-ACL handelt es sich nicht um eine Sicherheits-ACL, sondern um eine Punkt-ACL, die festlegt, welcher Datenverkehr zur Weiterbehandlung (z. B. Umleitung) an die CPU weitergeleitet wird (bei entsprechender Berechtigung) und welcher Datenverkehr auf der Datenebene verbleibt (bei Ablehnung), um eine Umleitung zu vermeiden.

Die ACL muss wie folgt aussehen (ersetzen Sie in diesem Beispiel 10.48.39.28 durch Ihre ISE-IP-Adresse):

	Sequence ~	Action ~	Source v IP	Source v Wildcard	Destination ~ IP	Destination Wildcard	Protoc	ol ~	Source ~ Port	Destination Port	× DS	SCP ~	Log ~
	10	deny	any		10.48.39.28		ip				No	ne	Disabled
	20	deny	10.48.39.28		any		ip				No	ne	Disabled
	30	deny	any		any		udp			eq domain	No	ne	Disabled
	40	deny	any		any		udp		eq domain		No	ne	Disabled
	50	permit	any		any		tcp			eq www	No	ne	Disabled
 4	∢ 1 →	▶ 10	▼ items per p	bage								1 - 5 of	5 items

Hinweis: Bei der Umleitungs-ACL ist diedeny Aktion als Umleitung verweigern (Datenverkehr nicht verweigern) und die permit Aktion als Umleitung zulassen zu betrachten. Der WLC untersucht nur den Datenverkehr, den er umleiten kann (standardmäßig die Ports 80 und 443). ip access-list extended REDIRECT deny ip any host <ISE-IP> deny ip host<ISE-IP> any deny udp any any eq domain deny udp any eq domain any permit tcp any any eq 80

Hinweis: Wenn Sie die ACL mit einem permit ip any any anstatt mit einer Genehmigung auf Port 80 beenden, leitet der WLC auch HTTPS um, was oft unerwünscht ist, da er sein eigenes Zertifikat bereitstellen muss und immer eine Zertifikatverletzung verursacht. Dies ist die Ausnahme zu der vorherigen Aussage, die besagt, dass Sie im Fall von CWA kein Zertifikat auf dem WLC benötigen: Sie benötigen ein Zertifikat, wenn HTTPS-Interception aktiviert ist, es jedoch ohnehin nie als gültig angesehen wird.

Sie können die ACL verbessern, indem Sie dem ISE-Server nur den Gast-Port 8443 vorenthalten.

Umleitung für HTTP oder HTTPS aktivieren

Die Konfiguration des Web-Admin-Portals ist mit der Konfiguration des Web-Authentifizierungsportals verknüpft und muss Port 80 überwachen, um eine Umleitung zu ermöglichen. Daher muss HTTP aktiviert sein, damit die Umleitung ordnungsgemäß funktioniert. Sie können entweder wählen, ob die Funktion global aktiviert werden soll (mit dem Befehl ip http server) oder ob HTTP nur für das Web-Authentifizierungsmodul aktiviert werden soll (mit dem Befehl webauth-http-enable unter der Parameterzuordnung).



Hinweis: Die Umleitung des HTTP-Verkehrs erfolgt innerhalb von CAPWAP, selbst bei FlexConnect Local Switching. Da der WLC die Abfangarbeit erledigt, sendet der WAP die HTTP(S)-Pakete innerhalb des CAPWAP-Tunnels und empfängt die Umleitung vom WLC zurück in den CAPWAP

intercept-https-enable

Wenn Sie beim Zugriff auf eine HTTPS-URL umgeleitet werden möchten, fügen Sie den Befehl unter der Parameterzuordnung hinzu, beachten Sie jedoch, dass dies keine optimale Konfiguration ist, sich auf die WLC-CPU auswirkt und trotzdem Zertifikatfehler generiert:

<#root>

parameter-map type webauth global

intercept-https-enable

trustpoint xxxxx

Sie können dies auch über die GUI mit der Option 'Web Auth abfangen HTTPS' in der Parameter Map (Configuration > Security > Web Auth).

Q. Search Menu Items	Con	figuration •	> Secu	urity • > N	Web Auth	Edit Web Auth Parameter	
		- Add		e		Maximum HTTP connections	100
Dashboard						Init-State Timeout(secs)	120
		Parameter	Map Nam	e			
Monitoring >		global				Туре	webauth 🔻
Configuration >	Ν	۹ ا	F F	10 🔻) items per page	Virtual IPv4 Address	
Image: Color Image: Administration						Trustpoint	Select •
C Licensing						Virtual IPv6 Address	XIXIXIX
						Web Auth intercept HTTPs	0
S Houbleshooting						Captive Bypass Portal	O



Hinweis: Browser verwenden standardmäßig eine HTTP-Website, um den Umleitungsprozess zu starten. Wenn HTTPS-Umleitung erforderlich ist, muss Web Auth HTTPS abfangen aktiviert werden. Diese Konfiguration wird jedoch nicht empfohlen, da sie die CPU-Auslastung erhöht.

ISE-Konfiguration

Hinzufügen von 9800 WLC zu ISE

Schritt 1: Öffnen Sie die ISE-Konsole, und navigieren SieAdministration > Network Resources > Network Devices > Add zu, wie im Bild dargestellt.

≡ Cisco ISE	Administration · Network Resources	🛕 Evaluation Mode 85 Days 🔍 🕜 🕫 🚳
Network Devices	Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences	NAC Managers More \sim
Network Devices Default Device	Network Devices	
Device Security Settings	🖉 Edit 🕂 Add 🚺 Duplicate 🥁 Import 🛧 Export 🗸 🔒 Generate PAC 🏮 Delete 🗸	Selected 0 Total 1 🤌 🏟
	Name \land IP/Mask Profile Name Location Type	Description
	9800-WLC 10.48.38.86/ 🇰 Cisco 🕕 All Locations All Device Types	

Schritt 2: Konfigurieren des Netzwerkgeräts

Optional kann es sich um einen angegebenen Modellnamen, eine angegebene Softwareversion und eine Beschreibung handeln sowie Netzwerkgerätegruppen basierend auf Gerätetyp, Standort oder WLCs zuweisen.

Die IP-Adresse entspricht dabei der WLC-Schnittstelle, die die Authentifizierungsanforderungen sendet. Standardmäßig ist dies die Management-Schnittstelle, wie im Bild gezeigt:

E Cisco ISE	Administration ·	Network Resources		A Evaluation Mode 24 D	ays Q Ø 📈	0
Network Devices Network De	vice Groups Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers	More \smallsetminus	
Network Devices Network Devices Default Device Device Security Settings	vice Groups Network Device Profiles Network Devices List > nschyns-WLC Network Devices Name WLC Description P Address * Device Profile Cisco Model Name Yestion * Network Device Group Software Version Location All Locations IPSEC No Device Type All Device Types V RADIUS Authentication Settir	External RADIUS Servers	RADIUS Server Sequences	NAC Managers	More ~	
	RADIUS UDP Settings Protocol RADIUS * Shared Secret	Show				

Weitere Informationen zu Netzwerk-Gerätegruppen finden Sie im ISE Admin Guide Chapter: Manage Network Devices: <u>ISE - Network Device</u> <u>Groups</u>.

Neuen Benutzer auf ISE erstellen

Schritt 1: Navigieren Sie Administration > Identity Management > Identities > Users > Add wie im Bild dargestellt zu.

■ Cisco ISE	Administration - Identity Management	A Evaluation Mode 85 Days Q 🕜 🕫 🚳
Identities Groups	External Identity Sources Identity Source Sequences Settings	
Users Latest Manual Network Scan Res	Network Access Users	
	🖉 Edit 🕂 Add 🛞 Change Status 🗸 🥁 Import 🏠 Export 🗸 📋 Delete 🗸 🚺 Duplicate	Selected 0 Total 0 😥 🚱
	Status Name	User Identity Grou Ad
	No data available	

Schritt 2: Geben Sie die Informationen ein.

In diesem Beispiel gehört dieser Benutzer zu einer Gruppe namens ALL_ACCOUNTS, kann aber, wie im Bild gezeigt, nach Bedarf angepasst werden.

≡	Cisco IS	SE		Administration · Identity I	Management		4	Evaluation Mode 85 Days	Q	0	Ø	Ø
lde	entities	Groups	External Identity Sources	Identity Source Sequences	Settings							
Users	Manual Networ	k Scan Res	Network Access Users List	> New Network Access User								
			 Vetwork Acces * Name user1 Status Status 	s User		-						
			Email									
			Passwords Password Type: In Password Type: Password T	ternal Users V	Re-Enter Password]						
			* Login Password			Generate Pa	ssword	0				
			Enable Password			Generate Pa	ssword	6				
			> User Informati	on								
			> Account Optio	ons								
			> Account Disab	ble Policy								
			✓ User Groups									
			ALL_ACCOU	UNTS (default) 🗸 🗕 🕂								

Erstellen des Autorisierungsprofils

Das Richtlinienprofil ist das Ergebnis, das einem Client basierend auf dessen Parametern zugewiesen wird (z. B. MAC-Adresse, Anmeldeinformationen, verwendetes WLAN usw.). Sie kann spezifische Einstellungen wie VLAN (Virtual Local Area Network), Zugriffskontrolllisten (ACLs), URL-Umleitungen usw. zuweisen.

Beachten Sie, dass in aktuellen Versionen der ISE bereits ein Autorisierungsergebnis von Cisco_Webauth vorhanden ist. Hier können Sie es

bearbeiten und den Namen der Umleitungs-ACL so ändern, dass er mit der Konfiguration im WLC übereinstimmt.

Schritt 1: Navigieren Sie zu Policy > Policy Elements > Results > Authorization > Authorization Profiles. Klicken Sie add hier, um Ihr eigenes Standardergebnis zu erstellen oder zu bearbeitenCisco_Webauth.

E Cisco ISE	Policy · Policy Elements	🔺 Evaluation Mode 24 Days Q 💮 🗔 🔅				
Dictionaries Condition	s Results					
Authentication	Standard Authorization Profiles					
Authorization Authorization Profiles	For Policy Export go to Administration > System > Backup & Restore > Policy Export Page	Selected 0 Total 11 🧷 🐵				
Downloadable ACLs	🖉 Edit 🕂 Add 🗋 Duplicate 🔋 Delete	γ in				
Profiling	Name Profile	∧ Description				
Posture	Blackhole_Wireless_Access ## Cisco	Default profile used to blacklist wireless devices. Ensure that you \mbox{confi}_{ξ}				
Posture	Cisco_IP_Phones ## Cisco ()	Default profile used for Cisco Phones.				
Client Provisioning	Cisco_Temporal_Onboard ## Cisco ()	Onboard the device with Cisco temporal agent				
	Cisco_WebAuth #* Cisco	Default Profile used to redirect users to the CWA portal.				

Schritt 2: Geben Sie die Weiterleitungsinformationen ein. Stellen Sie sicher, dass der ACL-Name mit dem Namen übereinstimmt, der auf dem 9800 WLC konfiguriert wurde.

Ξ Cisco ISE			A Evaluation Mode 24 Days	Q	0	6	٥	
Dictionaries Co	onditions	Results						
Authentication	>	Authorization Profiles > Ci Authorization Profi	sco_WebAuth					
Authorization Profiles		* Name	Cisco_WebAuth					
Downloadable ACLs		Description	Default Profile used to redirect users to the CWA portal.					
Profiling	>	* Access Type	ACCESS_ACCEPT ~					
Posture	>	Network Device Profile	\Rightarrow Cisco $\sim \oplus$					
Client Provisioning	>	Service Template						
		Track Movement						
		Agentless Posture						
		Passive Identity Tracking						
		Common Tasks Web Redirection (C Centralized Web Aut Display Certificate Message Static IP/Host nam	WA, MDM, NSP, CPP) () A CL_REDIRECT Value Self-Registered Guest Portal (c s Renewal he/FQDN	,				

Konfiguration der Authentifizierungsregel

Schritt 1: Ein Richtliniensatz definiert eine Sammlung von Authentifizierungs- und Autorisierungsregeln. Um einen zu erstellen, navigieren Sie zuPolicy > Policy Sets, klicken Sie auf das Zahnrad des ersten Richtliniensatzes in der Liste, und Insert new row wählen Sie oder klicken Sie auf den blauen Pfeil rechts, um den Standard-Richtliniensatz auszuwählen.

≡ Cisco ISE	Policy · Policy Sets	▲ Evaluation Mode 24 Days Q ⑦ 50 @
Policy Sets		Reset Policyset Hitcounts Save
+ Status Policy Set Name Description	Conditions	Allowed Protocols / Server Sequence Hits Actions View
Q Search		
	+	
Default Default policy set		Default Network Access 🛛 🗸 + 70

Schritt 2: Erweitern Sie Authentication die Richtlinien. Erweitern Sie dieMAB Regel (Übereinstimmung auf kabelgebundenem oder Wireless-MAB), Optionsund wählen Sie die CONTINUE Option, falls "If User not found" (Benutzer nicht gefunden) angezeigt wird.

\sim Authentication Policy (3)								
(+) S	itatus R	tule Name	Cond	itions	Use	Hits	Actions	
Q	Search							
	O N	МАВ	OR	Wired_MAB Wireless_MAB	Internal Endpoints (X) ~ ~ Options If Auth fail REJECT (X) ~ If User not found CONTINUE (X) ~ If Process fail DROP (X) ~	0	¢\$	

Schritt 3: Klicken Sie Save auf, um die Änderungen zu speichern.

Konfiguration der Authentifizierungsregeln

Die Autorisierungsregel bestimmt, welche Berechtigungen (welches Autorisierungsprofil) auf den Client angewendet werden.

Schritt 1: Schließen Sie auf derselben Seite mit dem Richtliniensatz die Authentication Policy, und erweitern Sie sie, Authorziation Policy wie im Bild dargestellt.

Policy	/ Sets-	→ Default		Reset	Reset Policyset Hitcounts	Save				
ę	Status	Policy Set Name	Description	Conditions			Allowed Protocols / Server Sequen	e Hits		
C	Q Search									
	0	Default	Default policy set				Default Network Access 🛛 🗸 -	- 70		
> Au	thentica	tion Policy (3)								
> Au	thorizati	on Policy - Local Except	tions							
> Au	> Authorization Policy - Global Exceptions									
∨ Au	V Authorization Policy (13)									

Schritt 2: Die aktuellen ISE-Versionen beginnen mit einer vorgefertigten Regel namens Wifi_Redirect_to_Guest_Login "Precreated Rule", die

größtenteils unseren Anforderungen entspricht. Drehen Sie das graue Schild auf der linken Seite nach enable.

	Wi- Fi_Redirect_to_Guest_Login	-	Wireless_MAB	${\sf Cisco_WebAuth} \ \times$	~+	Select from list	~+	0	ŝ
--	-----------------------------------	---	--------------	---------------------------------	----	------------------	----	---	---

Schritt 3: Diese Regel stimmt nur mit Wireless_MAB überein und gibt die CWA-Umleitungsattribute zurück. Jetzt können Sie optional eine kleine Wendung hinzufügen und festlegen, dass diese nur mit der spezifischen SSID übereinstimmt. Wählen Sie die Bedingung (ab sofort Wireless_MAB), damit das Bedingungsstudio angezeigt wird. Fügen Sie rechts eine Bedingung hinzu, und wählen Sie das Radius Wörterbuch mit dem Called-Station-ID Attribut aus. Passen Sie es an Ihren SSID-Namen an. Validieren Sie mit derUse unten im Bildschirm, wie im Bild dargestellt.

Conditions Studio				0
Library	Editor			
Search by Name		E Wire	less_MAB	\otimes
	99 ()		Radius Called-Station-ID	8
BYOD_is_Registered	AND	₽	Contains 🧹 cwa-ssid	
Catalyst_Switch_Local_Web_Aut				
Compliance_Unknown_Devices			NEW AND OR	
Compliant_Devices		Set to 'Is	not'	Duplicate Save
E MAC_in_SAN				
				Close Use

Schritt 4: Sie benötigen jetzt eine zweite Regel, die mit einer höheren Priorität definiert wird und mit der Guest Flow Bedingung übereinstimmt, um Netzwerkzugriffsdetails zurückzugeben, sobald sich der Benutzer im Portal authentifiziert hat. Sie können die Wifi Guest Access Regel verwenden, die standardmäßig auch für die neuesten ISE-Versionen erstellt wurde. Sie müssen dann die Regel nur mit einer grünen Markierung auf der linken Seite aktivieren. Sie können die Standardeinstellung "PermitAccess" zurückgeben oder präzisere Zugriffslisteneinschränkungen konfigurieren.

0	Wi-Fi_Guest_Access	AND	-	Guest_Flow Wireless_MAB	PermitAccess ×	<u>~</u> +	Guests	<u> </u>	0	\$
	Wi-		-	Wireless_MAB						
0	Fi_Redirect_to_Guest_Login	AND	₽	Radius-Called-Station-ID CONTAINS cwa-ssid	+	Select from list	+	0	\$ <u>\$</u> }	

Schritt 5: Speichern Sie die Regeln.

NUR Flexconnect Local Switching Access Points

Was ist, wenn Sie über lokale Flexconnect Switching Access Points und WLANs verfügen? Die vorherigen Abschnitte sind weiterhin gültig. Sie benötigen jedoch einen zusätzlichen Schritt, um die Umleitungszugriffskontrollliste im Voraus an die APs zu senden.

Navigieren Sie zu Configuration > Tags & Profiles > Flex, und wählen Sie Ihr Flex-Profil aus. Navigieren Sie anschließend zur Policy ACL Registerkarte.

Klicken Sie Add wie im Bild dargestellt.

Edit Flex Profi	le				
General	Local Authent	ication	Policy ACL	VLAN	DNS Layer Security
+ Add	× Delete				
ACL Name		▼ Cen	tral Web Auth	URL Filter	T
₩ ≪ 0	► ► 10 ·	items pe	er page	No items to	display

Wählen Sie den Namen der Umleitungszugriffskontrollliste aus, und aktivieren Sie die zentrale Webauthentifizierung. Dieses Kontrollkästchen invertiert automatisch die ACL auf dem Access Point selbst (da eine "deny"-Anweisung bedeutet, dass auf dem WLC in Cisco IOS XE keine Umleitung zu dieser IP erfolgt). Auf dem AP bedeutet die "deny"-Anweisung jedoch das Gegenteil. Daher tauscht dieses Kontrollkästchen automatisch alle Berechtigungen aus und verweigert sie, wenn es den Push zum AP durchführt. Sie können dies mit einem aus dershow ip access list AP-CLI überprüfen).

Hinweis: In einem lokalen Flexconnect Switching-Szenario muss die ACL explizit Rückgabeanweisungen angeben (was im lokalen Modus nicht unbedingt erforderlich ist). Stellen Sie daher sicher, dass alle ACL-Regeln beide Datenverkehrsarten (z. B. zur und von der ISE) abdecken.

Vergessen Sie nicht zu schlagen Save und dann Update and apply to the device.

Edit Flex Profile									
	General	Local Authenticatio	n Policy ACL	VLAN	DNS Layer	Security			
+	Add	× Delete							
A	CL Name	Ŧ	Central Web Auth	URL Filter	▼ <				
N	< 0	▶ ▶ 10 ▼ ite	ms per page	No items to	display	ACL Name*	REDIRECT	×	
						Central Web Auth			
						URL Filter	Search or Select	v	
						✓ Save		Cancel	

Zertifikate

Damit der Client dem Web-Authentifizierungszertifikat vertrauen kann, ist es nicht erforderlich, ein Zertifikat auf dem WLC zu installieren, da das einzige vorgelegte Zertifikat das ISE-Zertifikat ist (das vom Client als vertrauenswürdig eingestuft werden muss).

Überprüfung

Sie können diese Befehle verwenden, um die aktuelle Konfiguration zu überprüfen.

<#root>

show run wlan # show run aaa # show aaa servers # show ap config general # show ap name <ap-name> config general

- # show ap tag summary
- # show ap name <AP-name> tag detail
- $\# \ show \ wlan \ \{ \ summary \ | \ id \ | \ nme \ | \ all \ \}$
- # show wireless tag policy detailed <policy-tag-name>
- # show wireless profile policy detailed <policy-profile-name>

Nachfolgend der relevante Teil der Konfiguration des WLC, der diesem Beispiel entspricht:

<#root>

aaa new-model ! aaa authorization network CWAauthz group radius aaa accounting identity CWAacct start-stop group radius ! aaa server radius dynamic-author client <ISE mac-filtering CWAauthz no security ft adaptive no security wpa no security wpa wpa2 no security wpa wpa2 ciphers aes no security wpa akm dot1x no shutdown ip http server (or "webauth-http-enable" under the parameter map) ip http secure-server

Fehlerbehebung

Checkliste

Stellen Sie sicher, dass der Client eine Verbindung herstellt und eine gültige IP-Adresse erhält.

• Wenn die Umleitung nicht automatisch erfolgt, öffnen Sie einen Browser, und versuchen Sie eine zufällige IP-Adresse. Beispiel: 10.0.0.1. Wenn die Umleitung funktioniert, liegt möglicherweise ein DNS-Auflösungsproblem vor. Stellen Sie sicher, dass Sie über DHCP einen gültigen DNS-Server bereitgestellt haben und dass dieser Hostnamen auflösen kann.

• Stellen Sie sicher, dass der Befehl ip http server für die Umleitung auf HTTP konfiguriert ist. Die Konfiguration des Web-Admin-Portals ist mit der Konfiguration des Web-Authentifizierungsportals verknüpft und muss auf Port 80 aufgeführt werden, um eine Umleitung zu ermöglichen. Sie können entweder wählen, ob die Funktion global aktiviert werden soll (mit dem Befehl ip http server) oder ob HTTP nur für das Web-Authentifizierungsmodul aktiviert werden soll (mit dem Befehl webauth-http-enable unter der Parameterzuordnung).

• Wenn Sie beim Zugriff auf eine HTTPS-URL nicht umgeleitet werden und dies erforderlich ist, stellen Sie sicher, dass der Befehl unter der Parameterzuordnung vorhandenintercept-https-enable ist:

<#root>

parameter-map type webauth global type webauth

intercept-https-enable

trustpoint xxxxx

Sie können auch über die GUI überprüfen, ob die Option 'Web Auth intercept HTTPS' in der Parameterzuordnung aktiviert ist:

Q. Search Menu Items	Configuration • > Security • > Web Auth	Edit Web Auth Parameter	
	+ Add × Delete	Maximum HTTP connections	100
Dashboard	Parameter Man Name	Init-State Timeout(secs)	120
Monitoring >	global	Туре	webauth 🔻
Configuration >	I I I I I I I I I I I I I I I I I I I	Virtual IPv4 Address	
Administration		Trustpoint	Select 🔻
C Licensing		Virtual IPv6 Address	X:X:X:X:X
		Web Auth intercept HTTPs	
Nousieshooting		Captive Bypass Portal	0

Service-Port-Unterstützung für RADIUS

Der Cisco Catalyst Wireless Controller der Serie 9800 verfügt über einen Service-Port, der als GigabitEthernet 0Port bezeichnet wird. Ab Version 17.6.1 wird RADIUS (einschließlich CoA) über diesen Port unterstützt.

Wenn Sie den Service-Port für RADIUS verwenden möchten, benötigen Sie folgende Konfiguration:

<#root>

aaa server radius dynamic-author client 10.48.39.28

vrf Mgmt-intf

server-key cisco123

interface GigabitEthernet0

vrf forwarding Mgmt-intf

ip address x.x.x.x x.x.x.x

!if using aaa group server: aaa group server radius group-name server name nicoISE

ip vrf forwarding Mgmt-intf

ip radius source-interface GigabitEthernet0

Debuggen sammeln

WLC 9800 bietet ALWAYS-ON-Tracing-Funktionen (immer aktiv). So wird sichergestellt, dass alle verbindungsbezogenen Fehler, Warnungen und Benachrichtigungen auf Client-Ebene ständig protokolliert werden und Sie nach einem Vorfall oder Fehler Protokolle anzeigen können.

Hinweis: Sie können in den Protokollen einige Stunden bis mehrere Tage zurückgehen, dies hängt jedoch von der Menge der generierten Protokolle ab.

Um die Traces anzuzeigen, die der 9800 WLC standardmäßig erfasst, können Sie sich über SSH/Telnet mit dem 9800 WLC verbinden und diese Schritte ausführen (stellen Sie sicher, dass Sie die Sitzung in einer Textdatei protokollieren).

Schritt 1: Überprüfen Sie die aktuelle WLC-Zeit, damit Sie die Protokolle bis zum Zeitpunkt des Problems nachverfolgen können.

<#root>

show clock

Schritt 2: Erfassen Sie die Syslogs aus dem WLC-Puffer oder dem externen Syslog gemäß der Systemkonfiguration. Dadurch erhalten Sie einen kurzen Überblick über den Systemzustand und etwaige Fehler.

<#root>

show logging

Schritt 3: Überprüfen Sie, ob Debug-Bedingungen aktiviert sind.

<#root>

show debugging Cisco IOS XE Conditional Debug Configs: Conditional Debug Global State: Stop Cisco IOS XE Packet Tracing Configs: Packet Infra d

Hinweis: Wenn eine Bedingung aufgeführt wird, bedeutet dies, dass die Ablaufverfolgungen für alle Prozesse, bei denen die aktivierten Bedingungen auftreten (MAC-Adresse, IP-Adresse usw.) protokolliert werden. Dadurch erhöht sich die Anzahl der Protokolle. Es wird daher empfohlen, alle Bedingungen zu löschen, wenn Sie das Debuggen nicht aktiv durchführen.

Schritt 4: Unter der Annahme, dass die zu testende MAC-Adresse in Schritt 3. nicht als Bedingung aufgeführt wurde, werden die Nachverfolgungen auf permanenter Benachrichtigungsebene für die spezifische MAC-Adresse erfasst.

<#root>

show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-<FILENAME.txt>

Sie können entweder den Inhalt der Sitzung anzeigen oder die Datei auf einen externen TFTP-Server kopieren.

<#root>

more bootflash:always-on-<FILENAME.txt>
or
copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>

Bedingtes Debugging und Radio Active Tracing

Wenn die stets verfügbaren Ablaufverfolgungen nicht genügend Informationen bereitstellen, um den Auslöser für das zu untersuchende Problem zu ermitteln, können Sie das bedingte Debuggen aktivieren und die Radio Active (RA)-Ablaufverfolgung erfassen, die Ablaufverfolgungen auf Debugebene für alle Prozesse bereitstellt, die mit der angegebenen Bedingung interagieren (in diesem Fall Client-MAC-Adresse). Um das bedingte Debuggen zu aktivieren, gehen Sie wie folgt vor. Schritt 5: Stellen Sie sicher, dass keine Debugbedingungen aktiviert sind.

<#root>

clear platform condition all

Schritt 6: Aktivieren Sie die Debug-Bedingung für die MAC-Adresse des Wireless-Clients, die Sie überwachen möchten.

Mit diesen Befehlen wird die angegebene MAC-Adresse 30 Minuten (1800 Sekunden) lang überwacht. Sie können diese Zeit optional auf bis zu 2085978494 Sekunden erhöhen.

<#root>

debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}

W Hinweis: Führen Sie den Befehl debug wireless mac <aaaa.bbbb.cccc> pro MAC-Adresse aus, um mehr als einen Client gleichzeitig zu überwachen.

W Hinweis: Die Ausgabe der Client-Aktivität wird in der Terminal-Sitzung nicht angezeigt, da alles intern gepuffert wird, um später angezeigt zu werden.

Schritt 7". Reproduzieren Sie das Problem oder Verhalten, das Sie überwachen möchten.

Schritt 8: Stoppen Sie die Debugs, wenn das Problem reproduziert wird, bevor die standardmäßige oder konfigurierte Monitoring-Zeit abgelaufen ist.

<#root>

no debug wireless mac <aaaa.bbbb.cccc>

Wenn die Überwachungszeit abgelaufen ist oder das Wireless-Debugging beendet wurde, generiert der 9800 WLC eine lokale Datei mit dem Namen:

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Schritt 9: Sammeln Sie die Datei der MAC-Adressaktivität. Sie können das auf einen externen Server kopierenra trace .log oder die Ausgabe direkt auf dem Bildschirm anzeigen.

Überprüfen Sie den Namen der RA-Tracing-Datei.

<#root>

dir bootflash: | inc ra_trace

Datei auf externen Server kopieren:

<#root>

copy bootflash: ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.d/ra-FILENAME.txt

Inhalt anzeigen:

<#root>

more bootflash: ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Schritt 10. Wenn die Ursache immer noch nicht offensichtlich ist, sammeln Sie die internen Protokolle, die eine ausführlichere Ansicht der Protokolle auf Debugebene darstellen. Sie müssen den Client nicht noch einmal debuggen, da wir nur einen weiteren detaillierten Blick auf Debug-Protokolle werfen, die bereits gesammelt und intern gespeichert wurden.

<#root>

show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file ra-internal-<FILENAME>.txt

Hinweis: Diese Befehlsausgabe gibt Ablaufverfolgungen f
ür alle Protokollstufen f
ür alle Prozesse zur
ück und ist sehr umfangreich. Wenden Sie sich an das Cisco TAC, um diese Traces zu analysieren. Sie können das auf einen externen Server kopierenra-internal-FILENAME.txt oder die Ausgabe direkt auf dem Bildschirm anzeigen.

Datei auf externen Server kopieren:

<#root>

copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt

Inhalt anzeigen:

<#root>

more bootflash:ra-internal-<FILENAME>.txt

Schritt 11. Entfernen Sie die Debug-Bedingungen.

<#root>

clear platform condition all



Hinweis: Stellen Sie sicher, dass die Debug-Bedingungen nach einer Fehlerbehebungssitzung immer entfernt werden.

Beispiele

Wenn das Authentifizierungsergebnis nicht Ihren Erwartungen entspricht, müssen Sie zur ISE-Seite navigierenOperations > Live logs und die Details zum Authentifizierungsergebnis abrufen.

Sie erhalten den Grund für den Fehler (falls ein Fehler vorliegt) und alle Radius-Attribute, die von der ISE empfangen wurden.

Im nächsten Beispiel hat ISE die Authentifizierung abgelehnt, da keine Autorisierungsregel zutraf. Der Grund hierfür ist, dass das Attribut "Called-Station-ID" als an die MAC-Adresse des AP angehängter SSID-Name gesendet wird, während die Autorisierung genau mit dem SSID-Namen übereinstimmt. Es wird mit der Änderung dieser Regel auf 'enthält' anstelle von 'gleich' korrigiert.

Event	5400 Authentication failed
Failure Reason	15039 Rejected per authorization profile
Resolution	Authorization Profile with ACCESS_REJECT attribute was selected as a result of the matching authorization rule. Check the appropriate Authorization policy rule- results.
Root cause	Selected Authorization Profile contains ACCESS_REJECT attribute
Username	E8:36:17:1F:A1:62

 15048
 Queried PIP - Radius.NAS-Port-Type

 15048
 Queried PIP - Network Access.UserName

 15048
 Queried PIP - IdentityGroup.Name (2 times)

 15048
 Queried PIP - EndPoints.LogicalProfile

 15048
 Queried PIP - Radius.edited_station_ID

 15048
 Queried PIP - Network Access.AuthenticationStatus

 15016
 Selected Authorization Profile - DenyAccess

 15039
 Rejected per authorization profile

 11003
 Returned RADIUS Access-Reject

Other Attributes

ConfigVersionId	140	
Device Port	58209	
DestinationPort	1812	
RadiusPacketType	AccessRequest	
Protocol	Radius	
NAS-Port	71111	
Framed-MTU	1485	
OriginalUserName	e836171fa162	
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c	
IsThirdPartyDeviceFlow	false	
AcsSessionID	nicolse26/356963261/1	
UseCase	Host Lookup	
SelectedAuthenticationIdentityStores	Internal Endpoints	
IdentityPolicyMatchedRule	MAB	
AuthorizationPolicyMatchedRule	Default	
EndPointMACAddress	E8-36-17-1F-A1-62	
ISEPolicySetName	Default	
IdentitySelectionMatchedRule	MAB	
DTLSSupport	Unknown	
Network Device Profile	Cisco	
Location	Location#All Locations	
Device Type	Device Type#All Device Types	
IPSEC	IPSEC#Is IPSEC Device#No	
RADIUS Username	E8:36:17:1F:A1:62	
NAS-Identifier	cwa-ssid	
Device IP Address	10.48.71.120	
CPMSessionID	7847300A0000012DFC227BF1	
Called-Station-ID	00-27-e3-8f-33-a0:cwa-ssid	
CiscoAVPair	service-type=Call Check, audit-session-id=7847300A0000012DFC227BF1, method=mab, client-iif-id=3003124185, vlan-id=1468, cisco-wid=cura-seid	

Q. Search Menu Items		Troubleshooting - > Radioactive Trace			
🚃 Dashboard		Conditional Debug Global State: Stopped			
Monitoring	>	+ Add X Delete	Stop		
	>	MAC/IP Address	Trace file		
Administration	>	e836.171f.a162 H	debugTrace_e836.171f.a162.txt 📥	► Generate	
X Troubleshooting					

In diesem Fall liegt das Problem darin, dass Sie einen Tippfehler gemacht haben, als Sie den ACL-Namen erstellt haben und dieser nicht mit dem ACL-Namen übereinstimmt, der von den ISEs zurückgegeben wurde, oder der WLC beklagt, dass es keine ACL gibt, die der von der ISE angeforderten entspricht:

<#root>

2019/09/04 12:00:06.507 {wncd_x_R0-0}{1}: [client-auth] [24264]: (ERR): MAC: e836.171f.a162 client authz result: FAILURE 2019/09/04 12:00:06.51

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.