Konfigurieren von CWA mit FlexConnect APs auf einem WLC mit ISE

Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Hintergrundinformationen
Konfigurieren
Netzwerkdiagramm
WLC-Konfiguration
ISE-Konfiguration
Autorisierungsprofil erstellen
Erstellen einer Authentifizierungsregel
Erstellen einer Autorisierungsregel
Aktivieren der IP-Verlängerung (optional)
Datenverkehrsfluss
Überprüfung
Zugehörige Informationen

Einleitung

In diesem Dokument wird beschrieben, wie die zentrale Webauthentifizierung mit FlexConnect-APs auf einer WLC-ISE im lokalen Switching-Modus konfiguriert wird.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

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

- Cisco Identity Services Engine (ISE) Version 1.2.1
- Wireless LAN Controller (WLC)-Software, Version 7.4.100.0

• Access Points (AP)

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



Hinweis: Lokale Authentifizierung auf den FlexAPs wird für dieses Szenario derzeit nicht unterstützt.

Weitere Dokumente dieser Serie

- <u>Konfigurationsbeispiel für die zentrale Web-Authentifizierung mit Switch und Identity</u> <u>Services Engine</u>
- Zentrale Webauthentifizierung im Konfigurationsbeispiel für WLC und ISE

Konfigurieren

Es gibt mehrere Methoden, um die zentrale Webauthentifizierung auf dem Wireless LAN Controller (WLC) zu konfigurieren. Die erste Methode ist die lokale Web-Authentifizierung, bei der der WLC den HTTP-Datenverkehr an einen internen oder externen Server umleitet, wo der Benutzer zur Authentifizierung aufgefordert wird. Der WLC ruft dann die Anmeldeinformationen ab (im Fall eines externen Servers über eine HTTP GET-Anforderung zurückgesendet) und führt eine RADIUS-Authentifizierung durch. Bei einem Gastbenutzer ist ein externer Server (z. B. Identity Service Engine (ISE) oder NAC Guest Server (NGS)) erforderlich, da das Portal Funktionen wie die Geräteregistrierung und die benutzerseitige Bereitstellung bereitstellt. Dieser Prozess umfasst folgende Schritte:

- 1. Der Benutzer wird der Webauthentifizierungs-SSID zugewiesen.
- 2. Der Benutzer öffnet seinen Browser.
- 3. Der WLC leitet direkt nach Eingabe einer URL zum Gastportal (z. B. zur ISE oder zum NGS) weiter.
- 4. Der Benutzer authentifiziert sich im Portal.
- 5. Das Gastportal leitet mit den eingegebenen Anmeldeinformationen zurück zum WLC.
- 6. Der WLC authentifiziert den Gastbenutzer über RADIUS.
- 7. Der WLC kehrt zur ursprünglichen URL zurück.

Dieser Prozess beinhaltet eine Menge Umleitung. Der neue Ansatz besteht in der zentralen Web-Authentifizierung, die mit ISE (Versionen später als 1.1) und WLC (Versionen später als 7.2) funktioniert. Dieser Prozess umfasst folgende Schritte:

- 1. Der Benutzer wird der Webauthentifizierungs-SSID zugewiesen.
- 2. Der Benutzer öffnet seinen Browser.
- 3. Der WLC leitet zum Gastportal um.
- 4. Der Benutzer authentifiziert sich im Portal.
- 5. Die ISE sendet eine RADIUS-Autorisierungsänderung (CoA UDP-Port 1700), um dem Controller die Gültigkeit des Benutzers anzuzeigen, und überträgt schließlich RADIUS-Attribute wie die Zugriffskontrollliste (ACL).
- 6. Der Benutzer wird aufgefordert, die ursprüngliche URL erneut zu versuchen.

In diesem Abschnitt werden die erforderlichen Schritte zum Konfigurieren der zentralen Webauthentifizierung auf dem WLC und der ISE beschrieben.

Netzwerkdiagramm

Bei dieser Konfiguration wird folgende Netzwerkkonfiguration verwendet:



WLC-Konfiguration

Die WLC-Konfiguration ist relativ einfach. Es wird ein Trick verwendet (wie bei Switches), um die dynamische Authentifizierungs-URL von der ISE zu erhalten. (Da diese CoA verwendet, muss eine Sitzung erstellt werden, da die Sitzungs-ID Teil der URL ist.) Die SSID ist so konfiguriert, dass sie die MAC-Filterung verwendet, und die ISE ist so konfiguriert, dass sie eine Access-Accept-Nachricht zurückgibt, auch wenn die MAC-Adresse nicht gefunden wurde, sodass sie die Umleitungs-URL für alle Benutzer sendet.

Außerdem müssen RADIUS Network Admission Control (NAC) und AAA Override aktiviert sein. Mit RADIUS NAC kann die ISE eine CoA-Anforderung senden, die anzeigt, dass der Benutzer nun authentifiziert ist und auf das Netzwerk zugreifen kann. Es wird auch für Statusüberprüfungen verwendet, bei denen die ISE das Benutzerprofil basierend auf dem Statusergebnis ändert.

1. Stellen Sie sicher, dass auf dem RADIUS-Server standardmäßig RFC3576 (CoA) aktiviert ist.

cisco	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	TEEDBACK
Security	RADIUS	Authenti	cation Server	s > Edit					
 AAA General RADIUS Accounting Pallback TACACS+ LOAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Personord Policies Local EAP Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSiec SXOP Advanced 	Server In Server Ad Shared S Shared S Confirm S Key Wrap Port Num Server St Support f Server Ti Network I Managen JPSec	dex stress ecret: Forma ecret: Shared Secr b ber ber setus tor RPC 357 meout: User went:	et et	1 10.48.39.200 ASCII 8 (Designed fo 1812 Enabled 8 Enabled 9 Enable Enable Enable	r FIPS oustom	ers and requires a l	any wrap complia	nt RADIL	5 server)

RADIUS-Server hat RFC3576

2. Erstellen Sie ein neues WLAN. In diesem Beispiel wird ein neues WLAN mit dem Namen CWAFlex erstellt und vlan33 zugewiesen. (Beachten Sie, dass dies keine großen Auswirkungen hat, da sich der Access Point im lokalen Switching-Modus befindet.)

MONITOR WLANS CON	TROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
WLANs > Edit 'CWAF	lex'					
General Security	QoS	Advanced				
Profile Name	CWAFlex					
Туре	WLAN					
SSID	CWAFlex					
Status	🥑 Enable	d				
Security Policies	MAC Filt	erina				
	(Modificatio	ons done under	security tab v	vill appear after app	lying the change	is.)
Radio Policy	All	•]				
Interface/Interface	Luna 22					
Group(G)	VIBII33					
Multicast Vian Feature	Enabled	1				
Broadcast SSID	🗹 Enabled	1				
NAS-ID	WLC					

3. Aktivieren Sie auf der Registerkarte Sicherheit die Option MAC-Filterung als Layer-2-Sicherheit.

General	Security	QoS	Advanced
Layer 2	Layer 3	AAA S	ervers
	-		•
Layer 2	Security MA	one C Filtering	2 🗹
Fast Trans	ition		
Fast Transit	ion 🗌		

Neues WLAN erstellen

4. Stellen Sie auf der Registerkarte Layer 3 sicher, dass die Sicherheitsfunktion deaktiviert ist. (Wenn die Webauthentifizierung auf Layer 3 aktiviert ist, ist die lokale Webauthentifizierung aktiviert, nicht die zentrale Webauthentifizierung.)

General	Security	QoS	Advanced
Layer 2	Layer 3	AAA S	iervers
lavor 2	Security No	no. *	
Layer 5	Security INO	ne •	
🗆 We	b Policy ¹		

Stellen Sie sicher, dass die Sicherheitsfunktion deaktiviert ist.

5. Wählen Sie auf der Registerkarte AAA-Server den ISE-Server als Radius-Server für das WLAN aus. Optional können Sie es für die Buchhaltung auswählen, um detailliertere Informationen zur ISE zu erhalten.

Laura A	1								
Layer 2	Layer 3		ervers						_
Select AAA	servers belo	w to over	rice use of default se	rvers on this	WLAN				
Radius Ser	rvers						DAP Server	8	
Radius (Server Overwri	te interfac	e Enabled				Server 1	None	
			Authentication Ser	rvers	Accounting Servers		Server 2	None	
			Cinabled		Chabled		Server 3	None	
Server :	1		IP:10.48.39.208, 1	Port:1812 :	IP:10.48.39.208, Port:1813	4			
Server 2	2		None	÷	None				
Server 3	3		None	:	None	:			
Server -	4		None		None				
Server 3	5		None	•	None				
Server 6	6		None		None				
Radius Ser	rver Accounti	ng							
Interim	Update	8		Interim Inter	val 600				

6. Vergewissern Sie sich auf der Registerkarte Advanced, dass Allow AAA Override (AAA-Außerkraftsetzung zulassen) aktiviert ist und Radius NAC für NAC State (NAC-Status) ausgewählt ist.

General Security	QoS Advanced	
Allow AAA Override	S Enabled	DHCP
Coverage Hole Detection Enable Session Timeout	Chabled	DHCP Server Override
Aironet IE	Session Timeout (secs)	DHCP Addr. Assignment S Required Management Frame Protection (MFP)
Diagnostic Channel Override Interface ACL	Enabled IPv4 None IPv6 None IPv6	MFP Client Protection # Optional = 1
P2P Blocking Action Client Exclusion ²	Disabled : Cenabled 60 Timeout Value (secs)	802.11a/n (1 - 255) 1
Maximum Allowed Clients	0	802.11b/g/n (1 - 255) 1
Static IP Tunneling	Enabled	NAC State Sector NAC 1
Wi-Fi Direct Clients Policy	Disabled :	Load Balancing and Band Select
Per AP Radio	200	Client Load Balancing
Clear HotSpot Configuration	Enabled	Client Band Select

Stellen Sie sicher, dass AAA-Aufhebung zulassen aktiviert ist.

7. Erstellen Sie eine Umleitungszugriffskontrollliste.

Diese ACL wird in der Access-Accept-Nachricht der ISE referenziert und definiert, welcher Datenverkehr umgeleitet (von der ACL abgelehnt) und welcher Datenverkehr nicht umgeleitet werden darf (von der ACL zugelassen). Grundsätzlich müssen DNS und Datenverkehr zur/von der ISE zugelassen werden.



Achtung: Bei FlexConnect-APs müssen Sie eine FlexConnect-ACL erstellen, die von Ihrer normalen ACL getrennt ist. Dieses Problem ist in der Cisco Bug-ID <u>CSCue68065</u> dokumentiert und in Version 7.5 behoben. In WLC 7.5 und höher ist nur eine FlexACL erforderlich, und es ist keine Standard-ACL erforderlich. Der WLC erwartet, dass es sich bei der von der ISE zurückgegebenen Umleitungs-ACL um eine normale ACL handelt. Damit dies funktioniert, benötigen Sie jedoch dieselbe Zugriffskontrollliste wie die FlexConnect-Zugriffskontrollliste. (Nur registrierte Cisco Benutzer können auf interne Tools und Informationen von Cisco zugreifen.)

Dieses Beispiel zeigt, wie Sie eine FlexConnect-ACL mit dem Namen flexred erstellen:

TY
_

Erstellen einer FlexConnect-ACL mit dem Namen Flexred

a. Erstellen Sie Regeln, um DNS-Datenverkehr sowie Datenverkehr zur ISE zuzulassen und den Rest zu verweigern.

CISCO	MONI	TOR W	LANS <u>C</u> ONTRO	ILLE	R WIRELESS	S	ECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Wireless	Acc	ess Con	trol Lists > E	dit							
Access Points All APs Padios	Gene	eral									
802.11a/n 802.11b/g/n	Acces	s List Nam	e flexre	t							
Dual-Band Radios Global Configuration	Seq	Action	Source IP/Ma	ik	Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	
Advanced	1	Permit	0.0.0.0	/	10.48.39.208 255.255.255.255	5	Any	Any	Any	Any	
Mesh RF Profiles	2	Permit	10.48.39.208 255.255.255.25	/ 5	0.0.0.0 0.0.0.0	/	Any	Any	Any	Any	
FlexConnect Groups FlexConnect ACLs	3	Permit	0.0.0.0	/	0.0.0.0 0.0.0.0	/	UDP	Any	DNS	Any	
▶ 802.11a/n	.4	Permit	0.0.0.0	/	0.0.0.0 0.0.0.0	/	UDP	DNS	Any	Any	
 802.11b/g/n Media Stream 	5	Deny	0.0.0.0 0.0.0.0	/	0.0.0.0 0.0.0.0	/	Any	Any	Any	Any	

DNS-Datenverkehr zulassen

Wenn Sie die maximale Sicherheit wünschen, können Sie nur Port 8443 zur ISE zulassen. (Wenn Sie einen Status erhalten, müssen Sie typische Status-Ports hinzufügen, z. B. 8905.8906.8909.8910.)

 b. (Nur bei Code vor Version 7.5 aufgrund des Cisco Bugs <u>IDCSCue68065</u>) Wählen Sie Security > Access Control Lists (Sicherheit > Zugriffskontrolllisten), um eine identische ACL mit demselben Namen zu erstellen.

cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY
Security	Access (Control L	ists		
 AAA General RADIUS Authentication Accounting Fallback TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies 	Enable Co Name flexred	ounters		ד זז ז	ype 2v4 🔽
Local EAP					
Priority Order					
Certificate Access Control Lists Access Control Lists CPU Access Control Lists FlexConnect ACLs					
Identische ACL erstellen					

- c. Vorbereiten des jeweiligen FlexConnect AP Beachten Sie, dass Sie bei einer größeren Bereitstellung in der Regel FlexConnect-Gruppen verwenden und diese Elemente aus Gründen der Skalierbarkeit nicht auf AP-Basis ausführen.
 - 1. Klicken Sie auf Wireless, und wählen Sie den gewünschten Access Point aus.
 - 2. Klicken Sie auf die Registerkarte FlexConnect, und klicken Sie auf Externe Webauthentifizierungs-ACLs . (Vor Version 7.4 wurde diese Option als Webrichtlinien bezeichnet.)

cisco	MONITOR	WUANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	ELEOMOX
Wireless	All APs >	Details	for FlexAP1						
 Access Points Al APs 	General	Cred	entials Inte	rfaces H	igh Availabili	ty Inventor	y FlexCon	nect	Advanced
Radios 802.11a/n 802.11b/g/n Dual-Band Radios Global Configuration Advanced Mash	VLAN S Native PlexCo	iupport VLAN ID meet Grou	33 p Name	V Not Configured	AN Mappings	1			
RF Profiles	PreAuthe	ntication /	Locess Control L	ata					
FlexConnect Groups FlexConnect ACLs	External	WebAuther	tication ACLa						
> 802.11a/m	Contral	OmCP Proce	aning .						



3. Fügen Sie die ACL (in diesem Beispiel als flexred bezeichnet) zum Bereich für Webrichtlinien hinzu. Dadurch wird die ACL vorab an den Access Point übertragen. Sie wird noch nicht angewendet, aber der ACL-Inhalt wird an den Access Point übergeben, damit er bei Bedarf angewendet werden kann.

cisco	MONITOR	WLANS	CONTROLLER	WTRELESS	SECURITY	MANAGEMENT	COMMANDS
Wireless	All APs >	FlexAP	1 > ACL Mapp	oings			
All APs	AP Name		FlexAP1				
 Radios 802.11a/n 	Base Radio	MAC	00:1c:f9:c2:42:30)			
802.11b/g/n Dual-Band Radios Global Configuration	WLAN AC	L Mappi	ing				
Advanced	WLAN Id	0					
Mesh	WebAuth	ACL fie	wred +				
RF Profiles		Ad	56				
FlexConnect Groups RexConnect ACLs	WLAN Id	WLA	N Profile Name	WebA	with ACL	_	
▶ 802.11a/n		_					
▶ 802.11b/g/n	WebPolic	ies					
Media Stream	WebPolic	y ACL 👔	exred +				
Application Visibility And Control			66				
Country	WebPolicy	Access (Control Lists				
Timers	flexired						
Netflow							

ACL zum Webrichtlinienbereich hinzufügen

Die WLC-Konfiguration ist jetzt abgeschlossen.

ISE-Konfiguration

Gehen Sie wie folgt vor, um das Autorisierungsprofil zu erstellen:

- 1. Klicken Sie auf Richtlinie und dann auf Richtlinienelemente.
- 2. Klicken Sie auf Ergebnisse.
- 3. Erweitern Sie Autorisierung, und klicken Sie dann auf Autorisierungsprofil.
- 4. Klicken Sie auf die Schaltfläche Hinzufügen, um ein neues Autorisierungsprofil für die zentrale Webauthentifizierung zu erstellen.
- 5. Geben Sie im Feld Name einen Namen für das Profil ein. In diesem Beispiel wird CentralWebauth verwendet.
- 6. Wählen Sie ACCESS_ACCEPT aus der Dropdown-Liste "Access Type" aus.
- 7. Aktivieren Sie das Kontrollkästchen Web Authentication, und wählen Sie Centralized Web Auth aus der Dropdown-Liste aus.
- 8. Geben Sie im Feld ACL (ACL) den Namen der ACL auf dem WLC ein, die den umzuleitenden Datenverkehr definiert. In diesem Beispiel wird flexred verwendet.
- 9. Wählen Sie in der Dropdown-Liste "Redirect" die Option Default aus.

Das Redirect-Attribut definiert, ob die ISE das Standard-Webportal oder ein vom ISE-Administrator erstelltes benutzerdefiniertes Webportal erkennt. In diesem Beispiel löst die flexible ACL eine Umleitung des HTTP-Datenverkehrs vom Client an einen beliebigen Standort aus.

A Home Operations * Policy * Administ	tudion *
Automation 🕞 Autorization 🕞 Pri	affing 🗠 Pasture 🗽 Clerit Hostologing 🔄 Security Group Access 🌲 Parky Demons
Dictionaries Conditions Results	
Results (2) Qr • [10] (2) • • • • • • • • • • • • • • • • • • •	Authorization Profile * Name DantonNetouch Description
Contralindouth	Common Taska OAD, Name
Q PermitAcess	⊖ VAN
Q shariport Q sharipo	Uties Constin Permission
Downkaadable ACLa Downkaadable ACLa Downkaadable ACLa	of Veb Authentication Centralized * AOL fromed Redrect OrderA *

ACL löst eine Umleitung des HTTP-Datenverkehrs vom Client an einen beliebigen Standort aus

Führen Sie die folgenden Schritte aus, um die Authentifizierungsregel mithilfe des Authentifizierungsprofils zu erstellen:

1. Klicken Sie im Menü Richtlinie auf Authentifizierung.

Dieses Bild zeigt ein Beispiel für die Konfiguration der Authentifizierungsrichtlinienregel. In diesem Beispiel wird eine Regel konfiguriert, die ausgelöst wird, wenn eine MAC-Filterung erkannt wird.

wireless MAB	: 2	Wreless_MAB 🔷 allow protocols Allowed Protocol : Default Network and ,
MAB	: 14	Wred_MA8 🔷 allow protocols Allowed Protocol : Default Networ@ and
Dot1X	: #	Wred_802.1X 🔷 allow protocols Allowed Protocol : Default NetworQ and
Default Rule (If no match)	: 4	ow protocols Allowed Protocol : Default Networ: Internal Users

Konfigurieren der Policy-Regel

- 2. Geben Sie einen Namen für die Authentifizierungsregel ein. In diesem Beispiel wird Wireless MAB verwendet.
- 3. Wählen Sie das Plus-Symbol (+) im Feld If Bedingung.
- 4. Wählen Sie Compound condition (Zusammengesetzte Bedingung) und dann Wireless_MAB
- 5. Wählen Sie Standard-Netzwerkzugriff als zulässiges Protokoll aus.
- 6. Klicken Sie auf den Pfeil neben und ..., um die Regel zu erweitern.
- 7. Klicken Sie im Feld Identity Source (Identitätsquelle) auf das Symbol +, und wählen Sie Internal endpoints (Interne Endpunkte).
- 8. Wählen Sie in der Dropdown-Liste "Wenn Benutzer nicht gefunden" die Option Weiter aus.

wireless MAB : If Wirele	ss_MAB 🚸 allow protocols Allowed Protocol : D
Default : use	Internal Users 👄
	Identity Source Internal Endpoints
	Options
	If authentication failed Reject
MAB : If Wired	If user not found Continue *
	If process failed Drop *
Post V - If Mired	1



Diese Option ermöglicht die Authentifizierung eines Geräts (über Webauth), auch wenn dessen MAC-Adresse nicht bekannt ist. Dot1x-Clients können sich weiterhin mit ihren

Anmeldeinformationen authentifizieren und dürfen von dieser Konfiguration nicht betroffen sein.

Erstellen einer Autorisierungsregel

In der Autorisierungsrichtlinie müssen nun mehrere Regeln konfiguriert werden. Wenn der PC zugeordnet ist, durchläuft er die MAC-Filterung. Es wird davon ausgegangen, dass die MAC-Adresse nicht bekannt ist, sodass die Webauth- und ACL-Adresse zurückgegeben werden. Diese MAC-Regel ist im nächsten Bild dargestellt und in diesem Abschnitt konfiguriert.

	2	2nd AUTH	if.	Network Access:UseCase EQUALS Guest Flow	then	vlan34
L	*	IS-a-GUEST	if.	IdentityGroup:Name EQUALS Guest	then	PermitAccess
L		MAC not known	ľ	Network Access:AuthenticationStatus EQUALS UnknownUser	then	CentralWebauth

MAC nicht bekannt

Gehen Sie wie folgt vor, um die Autorisierungsregel zu erstellen:

- 1. Erstellen Sie eine neue Regel, und geben Sie einen Namen ein. In diesem Beispiel wird MAC unbekannt verwendet.
- 2. Klicken Sie im Bedingungsfeld auf das Pluszeichen (+), und wählen Sie eine neue Bedingung aus.
- 3. Erweitern Sie die Dropdownliste Ausdruck.
- 4. Wählen Sie Netzwerkzugriff aus, und erweitern Sie ihn.
- 5. Klicken Sie auf AuthenticationStatus, und wählen Sie den Operator Equals aus.
- 6. Wählen Sie im rechten Feld die Option UnbekannterBenutzer aus.
- 7. Wählen Sie auf der Seite "General Authorization" (Allgemeine Autorisierung) im Feld rechts neben dem Wort "Central Webauth" (<u>Autorisierungsprofil</u>) dann aus.

Mit diesem Schritt kann die ISE fortgesetzt werden, obwohl der Benutzer (oder die MAC-Adresse) nicht bekannt ist.

Unbekannte Benutzer werden nun mit der Anmeldeseite angezeigt. Nach Eingabe der Anmeldeinformationen wird ihnen jedoch erneut eine Authentifizierungsanforderung auf der ISE angezeigt. Daher muss eine andere Regel konfiguriert werden, die erfüllt ist, wenn es sich bei dem Benutzer um einen Gastbenutzer handelt. In diesem Beispiel entspricht UseridentityGroup Guestis used und es wird angenommen, dass alle Gäste zu dieser Gruppe gehören.

8. Klicken Sie auf die Aktionsschaltfläche am Ende der MAC-Regel nicht bekannt, und wählen Sie oben eine neue Regel aus.



Hinweis: Es ist sehr wichtig, dass diese neue Regel vor der MAC-Regel steht, die nicht bekannt ist.

- 9. Geben Sie im Namensfeld die zweite AUTH ein.
- 10. Wählen Sie eine Identitätsgruppe als Bedingung aus. In diesem Beispiel wurde Guest ausgewählt.
- 11. Klicken Sie im Bedingungsfeld auf das Plus-Symbol (+), und wählen Sie eine neue Bedingung aus.
- 12. Wählen Sie Network Access aus, und klicken Sie auf UseCase .
- 13. Wählen Sie als Operator Equals.
- 14. Wählen Sie GuestFlow als den richtigen Operanden aus. Das bedeutet, dass Sie nur dann Benutzer auffangen, die sich gerade auf der Webseite angemeldet haben und nach einer Autorisierungsänderung (der Gastfluss-Teil der Regel) wieder zurückkehren, wenn sie der Gast-Identitätsgruppe angehören.

15. Klicken Sie auf der Autorisierungsseite auf das Pluszeichen (+) (neben diesem Symbol), um ein Ergebnis für Ihre Regel auszuwählen.

In diesem Beispiel wird ein vorkonfiguriertes Profil (vlan34) zugewiesen; diese Konfiguration wird in diesem Dokument nicht dargestellt.

Sie können eine Option für Zugriffsrechte auswählen oder ein benutzerdefiniertes Profil erstellen, um das gewünschte VLAN oder die gewünschten Attribute zurückzugeben.



Vorsicht: In ISE Version 1.3 kann der Anwendungsfall "Guest Flow" je nach Webauthentifizierungstyp nicht mehr gefunden werden. Die Autorisierungsregel müsste dann als einzig mögliche Bedingung die Gastbenutzergruppe enthalten.

Aktivieren der IP-Verlängerung (optional)

Wenn Sie ein VLAN zuweisen, besteht der letzte Schritt darin, dass der Client-PC seine IP-Adresse erneuert. Dieser Schritt wird durch das Gastportal für Windows-Clients erreicht. Wenn Sie kein VLAN für die zweite AUTH-Regel zuvor festgelegt haben, können Sie diesen Schritt überspringen.

Beachten Sie, dass das VLAN bei FlexConnect-APs bereits auf dem AP selbst vorhanden sein muss. Wenn dies nicht der Fall ist, können Sie eine VLAN-ACL-Zuordnung auf dem Access Point selbst oder auf der Flex Group erstellen, bei der Sie keine ACL für das neue VLAN anwenden, das Sie erstellen möchten. Dadurch wird ein VLAN erstellt (ohne ACL).

Wenn Sie ein VLAN zugewiesen haben, führen Sie die folgenden Schritte aus, um die IP-Erneuerung zu aktivieren:

- 1. Klicken Sie auf Administration und dann auf Guest Management.
- 2. Klicken Sie auf Einstellungen.
- 3. Erweitern Sie Gast und dann Multi-Portal Configuration.
- 4. Klicken Sie auf DefaultGuestPortal oder den Namen eines von Ihnen erstellten benutzerdefinierten Portals.
- 5. Klicken Sie auf das Kontrollkästchen Vlan DHCP Release.



Hinweis: Diese Option funktioniert nur für Windows-Clients.

Settings	
General	Multi-Portal
Sponsor	
My Devices	General Operations Customization Authentication
* 🧰 Guest	U Every Lope
Details Policy	
Language Template	Enable Self-Provisioning Flow
Multi-Postal Configurations Multi-Postal Configurations Postal Policy Password Policy Time Profiles Username Policy	Allow guest users to change password Require guest users to change password at expiration and first login Guest users should download the posture client Guest users should be allowed to do self service Guest users should be allowed to do device registration Vian Dhcp Release (Note: Release should occur prior to the CoA. Renew should be set to occur after the CoA occurs). * Delay to Release seconds (Valid Range 1 to 200)

Aktivieren Sie das Kontrollkästchen VLAN DHCP Release.

Datenverkehrsfluss

In diesem Szenario ist es schwierig zu verstehen, welcher Datenverkehr wohin gesendet wird. Hier eine kurze Zusammenfassung:

- Der Client sendet eine Zuordnungsanforderung per Funk für die SSID.
- Der WLC übernimmt die MAC-Filterauthentifizierung mit der ISE (wo er die Umleitungsattribute empfängt).
- Der Client erhält eine assoc-Antwort erst, nachdem die MAC-Filterung abgeschlossen ist.
- Der Client sendet eine DHCP-Anfrage, die vom Access Point LOKAL umgeschaltet wird, um eine IP-Adresse des Remote-Standorts zu erhalten.
- Im Status "Central_webauth" wird der Datenverkehr, der in der Umleitungs-ACL als "deny" (Verweigern) markiert ist (also HTTP in der Regel), ZENTRAL geswitcht. Die Umleitung übernimmt also nicht der WAP, sondern der WLC. Wenn der Client beispielsweise nach einer Website fragt, sendet der WAP diese an den CAPWAP-gekapselten WLC, und der WLC spiegelt die IP-Adresse der Website vor und leitet sie zur ISE um.
- Der Client wird an die ISE-Umleitungs-URL umgeleitet. Dieser wird LOKAL wieder geschaltet (weil er auf "Zulassen" auf der Flex Redirect ACL trifft).
- Sobald der Datenverkehr im Status "RUN" ist, wird er lokal geswitcht.

Überprüfung

Sobald der Benutzer mit der SSID verknüpft ist, wird die Autorisierung auf der ISE-Seite angezeigt.

Apr 09,13 11:49:27.179 AM			No	00101021-2010	nicowic	vier34	Guest	NoNapplicable	
Apr 08,13 11:49:27.174 APR		-0			nicowie				Dynamic Author
Apr 09,13 11:48:58.372 AM	10	.0	No	001330212013			Guest		Guest Authoritic.
Ar 00,0 1142 15425 AM			00.13.10.21.70.13	001330217013	nicowie	CertraWebauth		Pending	Authentication

Autorisierung wird angezeigt

Von unten nach oben sehen Sie die Authentifizierung durch MAC-Adressfilterung, die die CWA-Attribute zurückgibt. Als Nächstes müssen Sie sich beim Portal mit dem Benutzernamen anmelden. Die ISE sendet dann eine CoA an den WLC, und die letzte Authentifizierung ist eine Layer-2-MAC-Filterauthentifizierung auf der WLC-Seite. Die ISE erinnert sich jedoch an den Client und den Benutzernamen und wendet das in diesem Beispiel konfigurierte VLAN an.

Wenn eine beliebige Adresse auf dem Client geöffnet wird, wird der Browser zur ISE umgeleitet. Stellen Sie sicher, dass das Domain Name System (DNS) richtig konfiguriert ist.

🛋 — heige //www.energe.order 🕷 the play stands — 🔛 stand	an con BHC (pareporta/Lop Chapter 1 🗎 2001 🗎 2	arten hauren die 161 Met Met Met 1913	U.S.	+ Coopie	1/1 MIL
	cisco Guest P	rtal			
		Username: Pasaword	sus Type On Otenget Pressond]	



Umleitung zur ISE

Der Netzwerkzugriff wird gewährt, nachdem der Benutzer die Richtlinien akzeptiert hat.



Signed on successfully You can now type in the original URL in the browser's address bar.

You can now type in the original URL in the browser's address bar.



Auf dem Controller werden der Status des Richtlinien-Managers und der RADIUS NAC-Status von POSTURE_REQD in RUN geändert.

Zugehörige Informationen

<u>Technischer Support und Downloads von Cisco</u>

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.