& Configureer probleemoplossing in downloadbare ACL's op Catalyst 9800

Inhoud

Inleiding

Dit document beschrijft hoe u downloadbare ACL's (dACL's) op Catalyst 9800 draadloze LANcontroller (WLC) kunt configureren en problemen kunt oplossen.

Achtergrondinformatie

ACL's worden al vele jaren ondersteund in Cisco IOS® en IOS XE® switches. Een dACL verwijst naar het feit dat het netwerkapparaat dynamisch de ACL-vermeldingen van de RADIUS-server

downloadt wanneer verificatie plaatsvindt, in plaats van een lokale kopie van de ACL te hebben en gewoon de ACL-naam te krijgen. Er is een completer <u>voorbeeld van Cisco ISE-configuratie</u> beschikbaar. Dit document concentreert zich op Cisco Catalyst 9800 die dACL's voor centrale switching sinds de 17.10-release ondersteunt.

Voorwaarden

Het idee achter dit document is het gebruik van dACL's op Catalyst 9800 aan te tonen door middel van een eenvoudig voorbeeld van de SSID-configuratie, dat laat zien hoe deze volledig aanpasbaar kunnen zijn.

Op Catalyst 9800 draadloze controller zijn downloadbare ACL's

- Ondersteund vanaf de Cisco IOS XE Dublin 17.10.1 release.
- Alleen ondersteund voor gecentraliseerde controller met Local Mode Access points (of Flexconnect Central-switching). FlexConnect Local Switching ondersteunt geen dACL.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Catalyst draadloze 9800 configuratiemodel.
- Cisco IP-toegangscontrolelijsten (ACL's).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Catalyst 9800-CL (v. Dublin 17.12.03).
- ISE (v. 3.2).

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Door deze configuratiegids, zelfs als de methodes verschillend zijn (bijvoorbeeld WLAN-verificatie, beleidsconfiguratie, enzovoort), is het eindresultaat hetzelfde. In het hier weergegeven scenario worden twee gebruikersidentiteiten gedefinieerd als GEBRUIKER1 en GEBRUIKER2. Beiden krijgen toegang tot het draadloze netwerk. Aan elk van hen wordt, respectievelijk, ACL_USER1 en ACL_USER2 toegewezen die dACLs zijn die door Catalyst 9800 van ISE worden gedownload.

DACL's met 802.1x SSID's gebruiken

Netwerkdiagram



WLC-configuratie

Raadpleeg voor meer informatie over de configuratie en probleemoplossing van 802.1x SID's op Catalyst 9800 de configuratiehandleiding <u>Configure 802.1X verificatie op Catalyst 9800 Wireless</u> <u>Controller Series</u>.

Stap 1. Configureer de SSID.

Configureer een 802.1x geverifieerde SSID met ISE als RADIUS-server. In dit document is de SSID aangeduid als "DACL_DOT1X_SSID".

Via de GUI:

Navigeer naar Configuration > Tags & profielen > WLAN en maak een WLAN dat vergelijkbaar is met de hier weergegeven WLAN:

Cisco Cata	alyst 9800-CL Wireless Controller		Welcome admin	* * & B & B & B @ C	Search APs and Clients Q	idback 💒 Թ
Q: Search Menu Items	Configuration * > Tags & Profiles * > WLAM	4s				
Dashboard	+ Add × Delete Clone	Enable WLAN Disable WLAN				WLAN Wizard
Monitoring	Selected WLANs : 0					
🔾 Configuration 🔷 🔸	Status Y Name DACL_DOT1X_SSID	T ID	SSID DACL_DOT1X_SSID		6 GHz Security	Ŧ
Administration >	·∺ - 1 -					1 - 1 of 1 items
C Licensing						
X Troubleshooting						
Walk Me Through >						
	1					

Van de CLI:

WLC#configure terminal WLC(config)#wlan DACL_DOT1X_SSID 2 DACL_DOT1X_SSID WLC(config-wlan)#security dot1x authentication-list DOT1X WLC(config-wlan)#no shutdown

Stap 2. Configureer het beleidsprofiel.

Configureer het beleidsprofiel dat samen met de hierboven gedefinieerde SSID wordt gebruikt. Zorg er in dit beleidsprofiel voor dat AAA Override is geconfigureerd vanuit het tabblad "Geavanceerd", zoals wordt weergegeven in de screenshot. In dit document is het gebruikte beleidsprofiel "DACL-8021X".

Zoals in het gedeelte Voorwaarden wordt vermeld, worden dACL's alleen ondersteund voor centrale switching/verificatie-implementaties. Zorg ervoor dat het beleidsprofiel op die manier is geconfigureerd.

Via de GUI:

Navigeer naar Configuratie > Tags & profielen > Beleid, selecteer het gebruikte beleidsprofiel en configureer het zoals getoond.



Cisco Cisco Catal	yst 9800-CL Wireless Controller	Welcome admin	A & A B & B O	Search APs and Clients Q
Q. Search Menu Items	Configuration * > Tags & Profiles * > Policy	Edit Policy Profile		×
Dashboard	+ Add × Delete	A Disabling a Policy or	configuring it in 'Enabled' state, will result in Ic	ss of connectivity for clients associated with this Policy profile.
 ⊘ Monitoring →	Admin Y Associated O Y Status Policy Tags Policy Profile Name	General Access Policies	QOS and AVC Mobility Adv	anced
Configuration	DACL-8021X	WLAN Timeout		Fabric Profile
Administration	default-policy-profile	Session Timeout (sec)	28800	Link-Local Bridging
C Licensing		Idle Timeout (sec)	300	mDNS Service default-mdns-ser Clear
* Troubleshooting		Idle Threshold (bytes)	0	Hotspot Server Search or Select
		Client Exclusion Timeout (sec)	60	User Defined (Private) Network
		Guest LAN Session Timeout	0	Status 🖸
Walk Me Through)		DHCP		Drop Unicast
		IPv4 DHCP Required	0	DNS Layer Security
		DHCP Server IP Address		DNS Layer Security Not Configured
		Show more >>>		Flex DHCP Option ENABLED
		AAA Policy		Flex DNS Traffic
		Allow AAA Override		
		NAC State	0	WLAN FIEX POICY
		Policy Name	default-aaa-policy 🗙 💌 💋	VLAN Central Switching
			· · · · ·	Shir Mart and Search or Select
		D Cancel		Update & Apply to Device

Van de CLI:

```
WLC#configure terminal
WLC(config)#wireless profile policy DACL-8021X
WLC(config-wireless-policy)#aaa-override
WLC(config-wireless-policy)#vlan VLAN_1413
WLC(config-wireless-policy)#no shutdown
```

Stap 3. Wijs het beleidsprofiel en de SSID toe aan de gebruikte beleidstag.

Via de GUI:

Navigeren naar Configuratie > Tags & profielen > Tags. Maak (of selecteer) de gebruikte tag op het tabblad Policy en wijs er het WLAN- en beleidsprofiel aan toe dat tijdens stap 1-2 is gedefinieerd.



Van de CLI:

```
WLC#configure terminal
WLC(config)#wireless tag policy default-policy-tag
WLC(config-policy-tag)#description "default policy-tag"
WLC(config-policy-tag)#wlan DACL_DOT1X_SSID policy DACL-8021X
```

Stap 4. Sta leverancierspecifieke kenmerken toe.

Downloadbare ACL's worden via leverancierspecifieke kenmerken (VSA) doorgegeven in de RADIUS-uitwisseling tussen ISE en WLC. De ondersteuning van deze eigenschappen kan worden ingeschakeld op de WLC, met behulp van deze CLI opdracht.

Van de CLI:

```
WLC#configure terminal
WLC(config)#radius-server vsa send authentication
```

Stap 5. Standaardautorisatielijst configureren.

Wanneer het werken met dACL, moet de netwerkvergunning door RADIUS voor WLC worden afgedwongen om het even welke gebruiker te machtigen die aan 802.1x SSID wordt gevormd voor authentiek verklaart. Niet alleen de verificatie, maar ook de autorisatiefase wordt hier aan de kant van de RADIUS-server afgehandeld. Daarom is in dit geval een toelatingslijst vereist.

Zorg ervoor dat de standaardmethode voor netwerkautorisatie deel uitmaakt van de 9800configuratie.

Via de GUI:

Navigeer naar Configuratie > Beveiliging > AAA en creëer vanuit het tabblad AAA-methodelijst > Autorisatie een autorisatiemethode die vergelijkbaar is met de methode die wordt getoond.



Van de CLI:

```
WLC#configure terminal
WLC(config)#aaa authorization network default group radius
```

ISE-configuratie

Wanneer het uitvoeren van dACLs in draadloos milieu met ISE, zijn twee gemeenschappelijke configuraties mogelijk, om te weten:

- 1. Configuratie per gebruiker van dACL. Met dit, heeft elke bepaalde identiteit een dACL toegewezen dankzij een gebied van de douaneidentiteit.
- 2. Configuratie van dACL per resultaat. Terwijl het kiezen voor deze methode, wordt een

bepaalde dACL toegewezen aan een gebruiker die op het vergunningsbeleid wordt gebaseerd het op de gebruikte beleidsreeks aanpaste.

dACL's per gebruiker

Stap 1. Een aangepast dACL-gebruikerskenmerk definiëren

Om dACL aan een gebruikersidentiteit te kunnen toewijzen, moet eerst dit veld op de gecreëerde identiteit configureerbaar zijn. Standaard wordt op ISE het veld "ACL" niet gedefinieerd voor een nieuwe identiteit die wordt gemaakt. Om dit te overwinnen, kan men de "Custom User Attribute" gebruiken en een nieuw configuratieveld definiëren. Ga hiervoor naar Beheer > Identity Management > Instellingen > Aangepaste gebruikerskenmerken. Gebruik de knop "+" om een nieuw kenmerk toe te voegen dat gelijk is aan het kenmerk dat wordt weergegeven. In dit voorbeeld is de naam van het aangepaste kenmerk ACL.

≡ Cisco ISE		Administration • Identi	ty Management		License Warning	Q Q Q @
Identities Groups	External Identity Sources	Identity Source Sequence	ces Settings			
User Custom Attributes						all \sim $ \nabla$
User Authentication Settings	Mandat Attrib	ute Name	∧ Data Type			
Endpoint Purge Endpoint Custom Attributes	Firstna	me	String			
REST ID Store Settings	Lastna	me	String			
	 Name 		String			1
	Passw	ord (CredentialPassword)	String			
	✓ User Custom At	tributes				
	Attribute Name	Description	Data Type	Parameters	Default Value M	andatory
	ACL		String	 String Max length 	+	□ 🝵 +
					Save	Reset

Als dit is ingesteld, gebruikt u de knop "Opslaan" om de wijzigingen op te slaan.

Stap 2. Configureer de dACL

Navigeer naar Beleid > Beleidselementen > Resultaten > Autorisatie > Downloadbare ACL's om dACL op ISE te zien en te definiëren. Gebruik de knop "Toevoegen" om een nieuwe te maken.

■ Cisco ISE			Polic	y · Policy Elements	🔺 License Warning 🔍 ⊘ 💭 🐡
Dictionaries 0	Conditions	Results			
Authentication Authorization	>	Dow	vnloadable ACL:	S	Selected 0 Total 7 🦪 🚳
Downloadable ACLs		C Edit	+ Add Duplicate	Delete	NI $\sim~\lambda$
Profiling	>		ACL_USER1	ACL assigned to USER1	
Posture	>		DENY_ALL_IPV4_TRAFFIC	Deny all ipv4 traffic	
Client Provisioning	>		DENY_ALL_IPV6_TRAFFIC	Deny all ipv6 traffic	
			PERMIT_ALL_IPV4_TRAFFIC	Allow all ipv4 Traffic	
			PERMIT_ALL_IPV6_TRAFFIC	Allow all ipv6 Traffic	
			test-dacl-cwa		
			test-dacl-dot1x		

Hiermee opent u het configuratieformulier "Nieuwe downloadbare ACL". Configureer de volgende velden:

- Naam: de naam van de gedefinieerde dACL.
- Beschrijving (optioneel): een korte beschrijving over het gebruik van de gemaakte dACL.
- IP-versie: de IP-protocolversie die in de gedefinieerde dACL wordt gebruikt (versie 4, 6 of beide).
- DACL-inhoud: de inhoud van de dACL, zoals per Cisco IOS XE ACL-syntaxis

In dit document is de gebruikte dACL "ACL_USER1" en deze dACL staat elk verkeer toe behalve het verkeer dat bestemd is voor 10.48.39.186 en 10.48.39.13.

Zodra de velden geconfigureerd zijn, gebruikt u de knop "Indienen" om de dACL te maken.

Herhaal de stap om de dACL voor de tweede gebruiker, ACL_USER2, te definiëren zoals in de afbeelding.

■ Cisco ISE		Policy · Policy Elements			
Dictionaries Condit	ions	Results			
Authentication	>	Dow	nloadable ACLs		
Authorization	~			Selected 0 Total 8 🧭 🏘	
Downloadable ACLs		0 Edit	🕂 Add 🎦 Duplicate 🧻 Delete		All \sim $~$ λ
			Name	Description	
Profiling	>		ACL_USER1	ACL assigned to USER1	
Posture	>		ACL_USER2	ACL assigned to USER2	
Client Provisioning	>		DENY_ALL_IPV4_TRAFFIC	Deny all ipv4 traffic	
			DENY_ALL_IPV6_TRAFFIC	Openy all joy6 traffic Ceny all joy6 traffic	
			PERMIT_ALL_IPV4_TRAFFIC	Allow all ipv4 Traffic	
			PERMIT_ALL_IPV6_TRAFFIC	Allow all ipv6 Traffic	
			test-daci-cwa		
			test-dacl-dot1x		

Stap 3. Wijs de dACL toe aan een gemaakte identiteit

Nadat de dACL is gemaakt, kan deze aan elke ISE-identiteit worden toegewezen met behulp van de aangepaste gebruikerskenmerken die in Stap 1 zijn gemaakt. Ga hiervoor naar Beheer > Identity Management > Identity > Identities > Gebruikers. Gebruik zoals gebruikelijk de knop "Toevoegen" om een gebruiker aan te maken.

■ Cisco ISE		Administration • Identity M	lanagement	🛕 License W	arning Q 🖉 🔎 🐡
Identities Groups	External Identity Sources	Identity Source Sequences	Settings		
Users Latest Manual Network Scan Res	Network Ac	CCESS USERS	🛧 Export 🗸 🚦 Delete	✓ ID Duplicate	Selected 0 Total 1 📿 🏟
	Status	Username	First Name Last Name	Network Access Users	Admin
	Disabled	9 adminuser		admin-group	

Definieer op het configuratieformulier "Nieuwe gebruiker netwerktoegang" de gebruikersnaam en het wachtwoord voor de gemaakte gebruiker. Gebruik het aangepaste kenmerk "ACL" om de

dACL die in Stap 2 is gemaakt, aan de identiteit toe te wijzen. In het voorbeeld, wordt de identiteit USER1 die ACL_USER1 gebruikt bepaald.

E Cisco ISE		Administration - Identity Management	🔺 License Warning Q 🛞 💭
Identities Groups Exte	rnal Identity Sources Identity Source Sequences Settings		
Users Latest Manual Network Scan Res	Natwork Access Users List > USER1		
	✓ Network Access User		
	* Username USER1		
	Status 🔄 Enabled ~		
	Account Name Alias		
	Emai		
	✓ Passwords		
	Password Type: Internal Users		
	Password Lifetime:		
	 With Expiration () Password will expire in 53 days 		
	Never Expires		
	Password Re-Enter Password		
	* Login Password	Generate Password	
	Enable Password	Generate Password ③	
	Lier Information		
	> Account Ontions		
	Account Disable Policy		
	V User Custom Attributes		
	• • • • • • • • • • • • • • • • • • • •		
	ACL ACL_USER1		
	✓ User Groups		
	E Select an item 0		
			Save Reset

Zodra de velden goed zijn geconfigureerd kunt u de knop "Verzenden" gebruiken om de identiteit aan te maken.

Herhaal deze stap om USER2 te maken en ACL_USER2 hieraan toe te wijzen.

E Cisco ISE	Administration - Identity Management	🔺 License Warning Q 🖉 🐼 🖗
Identities Groups Ex	ternal Identity Sources Identity Source Sequences Settings	
Users Latest Manual Network Scan Res	Network Access Users	
		Selected 0 Tetal 3 📿 🔕
	P Em +Ad ⊗ Charge Standa V → Inspect → B Davies V □ Depleters	AI 🗸 🗸
	Status Username \wedge Description First Name Last Name Email Address User Identity Groups Admin	
	Olisabled 1 adminuer admin-group	
	B Enabled <u>1</u> USER1	
	If institute If USER2	
	Network Access Users	

Stap 4. Configureer het resultaat van het autorisatiebeleid.

Zodra de identiteit is geconfigureerd en de dACL is toegewezen, moet het autorisatiebeleid nog steeds worden geconfigureerd om het aangepaste gebruikerskenmerk "ACL" te matchen dat is gedefinieerd voor een bestaande autorisatie en gemeenschappelijke taak. Hiervoor navigeer je naar Policy > Policy Elements > Results > Authorisation > Authorisation Profiles. Gebruik de knop "Toevoegen" om een nieuw autorisatiebeleid te definiëren.

- Naam: de naam van het vergunningsbeleid, hier "9800-DOT1X-GEBRUIKERS".
- Toegangstype: het type toegang dat wordt gebruikt wanneer dit beleid wordt aangepast, hier ACCESS_ACCEPTEREN.
- Gemeenschappelijke taak: stem "DACL-naam" af op Interne Gebruiker:<naam van aangepaste attribuut gemaakt> voor interne gebruiker.Volgens de namen die in dit document worden gebruikt, wordt het profiel 9800-DOT1X-GEBRUIKERS geconfigureerd met de dACL geconfigureerd als Interne Gebruiker:ACL.

≡ Cisco ISE	Policy · Policy Elements	🔺 License Warning 🔍 💮 🗔 🕸
Dictionaries Conditions	Results	
Authentication	Authorization Profiles > New Authorization Profile	
Authorization \checkmark	Autorization Prome	
Authorization Profiles	* Name 9800-DOT1X-USERS	
Downloadable ACLs	Description Authorization profile for 802.1x users using dACLs.	
Profiling >		
Posture >	* Access Type ACCESS_ACCEPT ~	
Client Provisioning	Network Device Profile 🕮 Cisco 🗸 🐵	
	Service Template	
	Track Movement	
	Agentiess Pasture 🗌 🕠	
	Passive Identity Tracking 🔲 😗	
	✓ Common Tasks	
	DACL Name InternalUser:ACL	1
	D IPv6 DACL Name	
	ACL (Filter-ID)	
	C see much many mix	

Stap 5. Gebruik het autorisatieprofiel in de beleidsset.

Zodra het autorisatieprofiel correct is gedefinieerd, moet dit deel uitmaken van de beleidsset die wordt gebruikt voor het verifiëren en autoriseren van draadloze gebruikers. Navigeer naar Policy > Policy Sets en open de gebruikte policy set.

In dit geval komt de verificatieregel "Dot1X" overeen met elke verbinding die via bekabelde of draadloze 802.1x wordt gemaakt. De autorisatieregel "802.1x Gebruikers dACL" implementeert een voorwaarde op de gebruikte SSID (dat is Radius-Calling-ID bevat DACL_DOT1X_SSID). Als een autorisatie wordt uitgevoerd op het "DACL_DOT1X_SSID" WLAN, wordt het profiel "9800-DOT1X-GEBRUIKERS", gedefinieerd in stap 4, gebruikt om de gebruiker te autoriseren.

	Policy · Policy S	Sets	🔺 License Warning	Q (2) [0
olicy Sets→ Default			Reset Policyset Hitcount	ts	Sav
Status Policy Set Name	Description Conditions		Allowed Protocols / Serv	er Seque	nce
Q Search Default	Default policy set		Default Network Access	. 🛛 🗸	+
 Authentication Policy (2) 					
+ Status Rule Name	Conditions		Use	Hits	Actio
Q Search					
	Wired 802.1X		All_User_ID_Stores 🛛 🛇		
Oct1X	OR		> Options	65	ŝ
			All_User_ID_Stores 🛛 🛇		
Ø Default			> Options	10	贷
> Authorization Policy - Local	xceptions				
> Authorization Policy - Global	Exceptions				
 Authorization Policy (2) 		Results			
🕂 Status Rule Name	Conditions	Profiles	Security Groups	Hits	Actio
Q Search					
	ACL Radius-Called-Station-ID CONTAINS DACL_DOT1X_SSID	9800-DOT1X-USERS ×	Select from list	- 65	{ĝ
📀 802.1x Users d					

dACL's per resultaat

Om de enorme taak te vermijden om een bepaalde dACL aan elke identiteit toe te wijzen die op ISE wordt gemaakt, kan men kiezen voor het toepassen van dACL op een bepaald beleidsresultaat. Dit resultaat wordt vervolgens toegepast op basis van elke voorwaarde die wordt afgemeten aan de vergunningsregels uit de gebruikte beleidsreeks.

Stap 1. Configureer de dACL

Voer dezelfde stap 2 uit vanuit de <u>sectie Per-gebruiker dACL's</u> om de benodigde dACL's te definiëren. Hier, zijn dit ACL_USER1 en ACL_USER2.

Stap 2. Identiteiten maken

Ga naar Beheer > Identity Management > Identity > Gebruikers en gebruik de knop "Add" om een gebruiker aan te maken.



Definieer op het configuratieformulier "Nieuwe gebruiker netwerktoegang" de gebruikersnaam en het wachtwoord voor de gemaakte gebruiker.

≡ Cis	ico ISE				Administration - Identity M	anagement	📥 Licanse Warning	0.0	58 Ø
Identities	Groups	External Identity Sources	Identity Source Sequence	a Settings					
Users Latest Manual	Network Scan Res	Network Access Users L	Lint > New Network Access User						
		~ Network Acco	ess User			_			
		* Usemame	USER1						
		Status	🗧 Enabled 🗸						
		Account Name All	30	0					
		Ernall							
		✓ Passwords							
		Password Type:	Internel Users 💛						
		Password Lifetim	NG:						
		 With Expirate 	an (i)						
		 Never Expire 	. 0						
			Password	Re-Enter Password					
		* Login Password	d		Generate Password]			
		Enoble Password			Generate Password				
		> User Informa	ation						
		> Account Opt	tions						
		> Account Dis	able Policy						
		> User Custon	n Attributes						
		> User Groups	1						
							Submit	Carce	·

Herhaal deze stap om USER2 te maken.

= Cisco ISE	Administration - Identity Management	🔺 Ucerso Riverso 🔍 🛞 52 d)
Identities Groups E	ternal Identity Sources Identity Source Sequences Settings	
Users Latest Manual Network Scan Res	Network Access Users	
		Selected O Total 3 🜔 🔕
	/ Gill 🕂 Add 🛞 Diverge Danke 🗸 Ja Seguent 🛆 Elsevit 🗸 🖞 Delations	$m \sim -\Delta$
	Status Username A Description Finst Name Last Name Email Address User Identity Groups Admin	
	O Distates 1 convinser official distance of the dista	
	Metwork Access Ultern	

Stap 4. Configureer het resultaat van het autorisatiebeleid.

Zodra de identiteit en de dACL zijn geconfigureerd, moet het autorisatiebeleid nog steeds worden geconfigureerd om een bepaalde dACL toe te wijzen aan gebruiker die de voorwaarde aanpast om dit beleid te gebruiken. Hiervoor navigeer je naar Policy > Policy Elements > Results > Authorisation > Authorisation Profiles. Gebruik de knop "Toevoegen" om een nieuw autorisatiebeleid te definiëren en deze velden te voltooien.

- Naam: de naam van het vergunningsbeleid, hier "9800-DOT1X-USER1".
- Toegangstype: het type toegang dat wordt gebruikt wanneer dit beleid wordt aangepast, hier ACCESS_ACCEPTEERT.
- Gemeenschappelijke Taak: pas "DACL Naam"aan "ACL_USER1"voor interne gebruiker aan. Volgens de namen die in dit document worden gebruikt, wordt het profiel 9800-DOT1X-USER1 geconfigureerd met de dACL geconfigureerd als "ACL_USER1".

■ Cisco ISE	Policy - Policy Elements	A Lorence Warring	0. © 1	52 Ø
Dictionaries Conditions	Results			
Asthurdsartas > Asthurdsartas > Asthurdsartas > Downloadash Poties > Prelifing > Pasture > Claret Presistoring >	Addressed Profiles > Near Addressed on Profile * Norro 9800-00130-005811 Description			
	Advanced Attributes bettings Attributes Details Anne Type + KCDS, ACOPT DAD, + AD, ISSR	Submit	Cane	:el

Herhaal deze stap om het beleidsresultaat "9800-DOT1X-USER2" te maken en wijs "ACL_USER2" als DACL toe aan het.

Cisco ISE		Polic	zy - Policy Elements 🔺 Leaves Running Q, 🕲 (
Dictionaries Conditions	Results		
Asthenication	Standard Authorization Profi	iles	
Authorization \sim	For Policy Expert go to Administration > System > Backup & Pr	estore > Policy Export Page	
Authorization Profiles			Selected 8 Tatal 13 🦪
	/ Edit + Add Duplicate () Delete		# V
Profiling >	Name	Profile	
Pasture >	0000-0011X-USDN	m Cisco 🕕	
(East Resolutions	56880-2010-0086	# Cisco 🕡	
contributing /	9600-DOTIX-USDAS	# Ciaco 🕢	Authorization profile for 802.1s users using dACLs.
	Block_Windess_Access	m Cisco 🕧	Default profile used to block wireless devices. Ensure that you certigure a NULL ROUTE ACL on the Wireless LAN Controller
	Class_JP_Phones	# Cisco 🕕	Default profile used for Cloco Phones.
	Cisco_Temporal_Orboard	tti Cisco 🕕	Driboard the device with Cisco temporal agent
	Choo_WebArth	AL Cisco 🕧	Default Profile used to redirect users to the CWA portal.
	Internal User Attribute Test	# Ciaco 🕦	
	NSP_Onboard	m Cisco 🕕	Onboard the dovice with Native Supplicant Provisioning
	Non_Cisco_IP_Phones	AL Cisco 🕧	Default Profile used for Non Cisco Phones.
	U0N	± Ciaco 🕢	Default profile used for UDN.
	DenyAccess		Default Profile with access type as Access-Reject
	Permitancese		Default Profile with access type as Access-Accept

Stap 5. Gebruik autorisatieprofielen in de beleidsset.

Zodra het autorisatieprofiel correct is gedefinieerd, moet het nog steeds deel uitmaken van de beleidsset die wordt gebruikt voor het verifiëren en autoriseren van draadloze gebruikers. Navigeer naar Policy > Policy Sets en open de gebruikte policy set.

In dit geval komt de verificatieregel "Dot1X" overeen met elke verbinding die via bekabelde of draadloze 802.1X wordt gemaakt. De autorisatieregel "802.1X Gebruiker 1 dACL" implementeert

een voorwaarde op de gebruikte gebruikersnaam (dat is Interne Gebruiker-Naam BEVAT USER1). Als een autorisatie wordt uitgevoerd met de gebruikersnaam USER1, dan wordt het profiel "9800-DOT1X-USER1", gedefinieerd in Stap 4, gebruikt om de gebruiker te autoriseren en wordt dus ook de dACL uit dit resultaat (ACL_USER1) toegepast op de gebruiker. Hetzelfde wordt ingesteld voor de gebruikersnaam USER2, waarvoor "9800-DOT1X-USER1" wordt gebruikt.

licy Set	s→ D	Default			Reset Policyset Hitopunts	a r	54
Status	i Pal	licy Set Name	Description Conditions		Allowed Protocols / Server	/ Sequ	ence
Q See	arch						
•	•	Defeuit	Default policy set		Default Network Access		~+
Authenti	ication	Palicy (2)					
(-) 55	a0.45	Rule Name	Conditions		Use	Hits	Ao
0.9							
~						_	-
	_		montestation montestation		All_User_ID_Stores CE V		
	•	Der1X	CR Window, MAD		2 Options		Г
			E Wired_WAS				
					All_User_ID_Stores CI V		
	•	Defeat			> Options	10	0
Authoriz	ration F	Pelicy - Local Exceptions					
Authoriz	ration P	Palicy (3)	•				
				Results			
(a) 80	attas	Rule Name	Conditions	Profiles	Security Groups	Hits	a.
Q 9	earch						
	•	902.1x liser 2 dACL	1 Internal/over Name 2010/LS 1/1092	9800-DOT1X-USER2 × +	Select from list ~+	a	6
	•	992.1x liner 1 dAGL	1 Internal/Juar Roma EDURIS 1/0281	980D-DOT1X-USER1 ×	Select from list		4
	•	Defeat		DenyAccess ×	Select from list $\sim +$	a	{

Opmerkingen over het gebruik van dACL's met CWA-SSID's

Zoals beschreven in de <u>Configure Central Web Verification (CWA) op Catalyst 9800 WLC en ISE</u>configuratiehandleiding, maakt CWA gebruik van MAB en bepaalde resultaten om gebruikers te verifiëren en te autoriseren. Downloadbare ACL's kunnen aan de CWA-configuratie vanuit ISEzijde op dezelfde manier worden toegevoegd als wat hierboven is beschreven.



Waarschuwing: downloadbare ACL's kunnen alleen worden gebruikt als netwerktoegangslijst en worden niet ondersteund als pre-verificatie ACL's. Daarom moet elke pre-authenticatie ACL die gebruikt wordt in een CWA-workflow worden gedefinieerd in de WLC-configuratie.

Verifiëren

Om de gemaakte configuratie te controleren, kunnen deze opdrachten worden gebruikt.

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>
# show access-lists { acl-name }
```

Hier wordt verwezen naar het relevante deel van de WLC-configuratie die overeenkomt met dit voorbeeld.

```
aaa new-model
1
!
aaa group server radius authz-server-group
server name DACL-RADIUS
1
aaa authentication login default local
aaa authentication dot1x default group radius
aaa authentication dot1x DOT1X group radius
aaa authorization exec default local
aaa authorization network default group radius
ļ
ļ
aaa server radius dynamic-author
client <ISE IP>
ļ
aaa session-id common
I
[...]
vlan 1413
name VLAN_1413
T
[...]
radius server DACL-RADIUS
address ipv4 <ISE IP> auth-port 1812 acct-port 1813
key 6 aHaOSX[QbbEHURGW`cXiG^UE]CR]^PVANfcbROb
ï
I
[...]
wireless profile policy DACL-8021X
aaa-override
vlan VLAN_1413
no shutdown
[...]
wireless tag policy default-policy-tag
description "default policy-tag"
wlan DACL_DOT1X_SSID policy DACL-8021X
[...]
wlan DACL_DOT1X_SSID 2 DACL_DOT1X_SSID
security dot1x authentication-list DOT1X
no shutdown
```

De RADIUS-serverconfiguratie wordt weergegeven met de opdracht all in werking stellen-config van de show.

WLC#show running-config all | s radius-server radius-server attribute 77 include-in-acct-req radius-server attribute 11 default direction out radius-server attribute 11 default direction out radius-server attribute nas-port format a radius-server attribute wireless authentication call-station-id ap-macaddress-ssid radius-server dead-criteria time 10 tries 10 radius-server cache expiry 24 enforce hours radius-server transaction max-tries 8 radius-server timeout 5 radius-server timeout 5 radius-server ipc-limit in 10 radius-server vsa send accounting radius-server vsa send authentication

Problemen oplossen

Checklist

- Zorg ervoor dat de clients goed kunnen aansluiten op de 802.1X SSID die is geconfigureerd.
- Verzeker dat het RADIUS-toegangsverzoek/acceptatie de juiste attribuut-waarde paren (AVP's) bevat.
- Zorg ervoor dat clients het juiste WLAN/beleidsprofiel gebruiken.

WLC One Stop-Shop Reflex

Client Username : USER1

Om te controleren of de dACL correct aan een bepaalde draadloze client is toegewezen, kan men de opdracht **show wireless client mac-address** <**H.H.H> detail** gebruiken zoals getoond. Van daar, kan de verschillende nuttige het oplossen van probleeminformatie worden gezien, namelijk: de cliëntgebruikersbenaming, staat, beleidsprofiel, WLAN en, het belangrijkst hier, ACS-ACL.

<#root>

WLC#show wireless client mac-address 08be.ac14.137d detail Client MAC Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Address : 08be.ac14.137d Client MAC Type : Universally Administered Administered

AP MAC Address : f4db.e65e.7bc0 AP Name: AP4800-E Client State : Associated Policy Profile : DACL-8021X Wireless LAN Id: 2 WLAN Profile Name: DACL_DOT1X_SSID Wireless LAN Network Name (SSID): DACL_DOT1X_SSID BSSID : f4db.e65e.7bc0 Association Id : 1 Authentication Algorithm : Open System Client Active State : Client ACLs : None Policy Manager State: Run Last Policy Manager State : IP Learn Complete Client Entry Create Time : 35 seconds Policy Type : WPA2 I VLAN : VLAN_1413

```
[...] Session Manager: Point of Attachment : capwap_90000012 IIF ID : 0x90000012 Authorized : TRUE Sess
SM State : AUTHENTICATED
SM Bend State : IDLE Local Policies:
Service Template : wlan_svc_DACL-8021X_local (priority 254) VLAN : VLAN_1413 Absolute-Timer : 28800
Server Policies:
ACS ACL : xACSACLx-IP-ACL_USER1-65e89aab
Resultant Policies:
ACS ACL : xACSACLx-IP-ACL_USER1-65e89aab VLAN Name : VLAN_1413 VLAN : 1413 Absolute-Timer : 28800
[...]
```

WLC-opdrachten weergeven

Om alle ACL's te zien die momenteel deel uitmaken van de Catalyst 9800 WLC-configuratie, kunt u de opdracht **toegangslijsten tonen** gebruiken. Dit bevel maakt een lijst van alle plaatselijk bepaalde ACLs of dACLs die door WLC wordt gedownload. Om het even welke dACLs die van ISE door WLC wordt gedownload heeft het formaat xACSACLx-IP-<ACL_NAME>-<ACL_HASH>.



Opmerking: downloadbare ACL's blijven in de configuratie zolang een client is gekoppeld en gebruikt in de draadloze infrastructuur. Zodra de laatste client die gebruik maakt van de dACL de infrastructuur verlaat, wordt de dACL verwijderd uit de configuratie.

WLC#show access-lists Extended IP access list IP-Adm-V4-Int-ACL-global [...] Extended IP access list IP-Adm-V4-LOGOUT-ACL [...] Extended IP access list implicit_deny [...] Extended IP access list implicit_permit [...]

```
Extended IP access list meraki-fqdn-dns
[...]
Extended IP access list preauth-ise
[...]
Extended IP access list preauth_v4
[...]
Extended IP access list xACSACLx-IP-ACL_USER1-65e89aab
   1 deny ip any host 10.48.39.13
    2 deny ip any host 10.48.39.15
    3 deny ip any host 10.48.39.186
    4 permit ip any any (56 matches)
IPv6 access list implicit_deny_v6
[...]
IPv6 access list implicit_permit_v6
[...]
IPv6 access list preauth_v6
[...]
```

Voorwaardelijke debugging en radio actieve tracering

Tijdens het oplossen van problemen configuratie, kunt u <u>radioactieve sporen</u> verzamelen voor een client die verondersteld wordt te worden toegewezen met de gedefinieerde dACL. Hier worden de logboeken benadrukt die het interessante deel van de radioactieve sporen tijdens het proces van de cliëntenvereniging voor cliënt 08be.ac14.137d tonen.

<#root>

```
24/03/28 10:43:04.321315612 {wncd_x_R0-0}{1}: [client-orch-sm] [19620]: (note): MAC: 08be.ac14.137d Asso
```

```
2024/03/28 10:43:04.321414308 {wncd_x_R0-0}{1}: [client-orch-sm] [19620]: (debug): MAC: 08be.ac14.137d
```

```
2024/03/28 10:43:04.321464486 {wncd_x_R0-0}{1}: [client-orch-state] [19620]: (note): MAC: 08be.ac14.1376
```

[...]

2024/03/28 10:43:04.322185953 {wncd_x_R0-0}{1}: [dot11] [19620]: (note): MAC: 08be.ac14.137d Association

2024/03/28 10:43:04.322199665 {wncd_x_R0-0}{1}: [dot11] [19620]: (info): MAC: 08be.ac14.137d DOT11 state

[...]

2024/03/28 10:43:04.322860054 {wncd_x_R0-0}{1}: [client-orch-sm] [19620]: (debug): MAC: 08be.ac14.137d &

2024/03/28 10:43:04.322881795 {wncd_x_R0-0}{1}: [client-orch-state] [19620]: (note): MAC: 08be.ac14.1376

[...]

2024/03/28 10:43:04.323379781 {wncd_x_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Client-auth]

[...]

2024/03/28 10:43:04.330181613 {wncd_x_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Client-auth]

2024/03/28 10:43:04.353413199 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [19620]: (info): [08be.ac14.13 2024/03/28 10:43:04.353414496 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [19620]: (info): [08be.ac14.13 2024/03/28 10:43:04.353443674 {wncd_x_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Client-auth]

[...]

2024/03/28 10:43:04.381397739 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Send Access-Request to

2024/03/28 10:43:04.381411901 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: authenticator e9 8b e

2024/03/28 10:43:04.381425481 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: User-Name [1] 7 "USER

2024/03/28 10:43:04.381430559 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Service-Type [6] 6 Fr 2024/03/28 10:43:04.381433583 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 27 2024/03/28 10:43:04.381437476 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 21 " 2024/03/28 10:43:04.381440925 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Framed-MTU [12] 6 148 2024/03/28 10:43:04.381452676 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: EAP-Message [79] 12 . 2024/03/28 10:43:04.381466839 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Message-Authenticator 2024/03/28 10:43:04.381482891 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: EAP-Key-Name [102] 2 2024/03/28 10:43:04.381486879 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 49 2024/03/28 10:43:04.381489488 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 43 " 2024/03/28 10:43:04.381491463 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 20

2024/03/28 10:43:04.381494016 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 14 "r

2024/03/28 10:43:04.381495896 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 32 2024/03/28 10:43:04.381498320 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 26 " 2024/03/28 10:43:04.381500186 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 20

2024/03/28 10:43:04.381502409 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 14 "v

2024/03/28 10:43:04.381506029 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: NAS-IP-Address [4] 6 1

2024/03/28 10:43:04.381509052 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: NAS-Port-Type [61] 6 2024/03/28 10:43:04.381511493 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: NAS-Port [5] 6 3913 2024/03/28 10:43:04.381513163 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 39

2024/03/28 10:43:04.381515481 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 33 "c

2024/03/28 10:43:04.381517373 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 41

2024/03/28 10:43:04.381519675 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 35 "w

2024/03/28 10:43:04.381522158 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Called-Station-Id [30 2024/03/28 10:43:04.381524583 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Calling-Station-Id [3 2024/03/28 10:43:04.381532045 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Airespace [26 2024/03/28 10:43:04.381534716 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Airespace-WLAN-ID [1]

2024/03/28 10:43:04.381537215 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Nas-Identifier [32] 1

2024/03/28 10:43:04.381539951 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: wlan-group-cipher [18

2024/03/28 10:43:04.381542233 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: wlan-pairwise-cipher[2024/03/28 10:43:04.381544465 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: wlan-akm-suite [188] 2024/03/28 10:43:04.381619890 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Started 5 sec timeout [...]

2024/03/28 10:43:04.392544173 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Received from id 1812,

2024/03/28 10:43:04.392557998 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: authenticator 08 6d for 2024/03/28 10:43:04.392564273 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: State [24] 71 ... 2024/03/28 10:43:04.392615218 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: EAP-Message [79] 8 .. 2024/03/28 10:43:04.392628179 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Message-Authenticator 2024/03/28 10:43:04.392738554 {wncd_x_R0-0}{1}: [radius] [19620]: (info): Valid Response Packet, Free t 2024/03/28 10:43:04.726798622 {wncd_x_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap_9000001.

2024/03/28 10:43:04.726801212 {wncd_x_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap_90000012

2024/03/28 10:43:04.726896276 {wncd_x_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap_9000001

2024/03/28 10:43:04.726905248 {wncd_x_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap_90000012

[...]

2024/03/28 10:43:04.727138915 {wncd_x_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap_90000012

2024/03/28 10:43:04.727148212 {wncd_x_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap_9000

2024/03/28 10:43:04.727164223 {wncd_x_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap_9000 2024/03/28 10:43:04.727169069 {wncd_x_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap_9000

2024/03/28 10:43:04.727223736 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : use

2024/03/28 10:43:04.727233018 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : cl 2024/03/28 10:43:04.727234046 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : EA 2024/03/28 10:43:04.727234996 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : Me 2024/03/28 10:43:04.727236141 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : EA M\$®vf9∫Ø◊«? %ÿ0?ã@≤™ÇÑbWï6\Ë&\q.1U+QB-2®"≠∫JÑv?"

2024/03/28 10:43:04.727246409 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : Cis

[...]

2024/03/28 10:43:04.727509267 {wncd_x_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap_9000

2024/03/28 10:43:04.727513133 {wncd_x_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap_90000

2024/03/28 10:43:04.727607738 {wncd_x_R0-0}{1}: [svm] [19620]: (info): SVM_INFO: SVM Apply user profile 2024/03/28 10:43:04.728003638 {wncd_x_R0-0}{1}: [svm] [19620]: (info): SVM_INFO: Activating EPM feature

2024/03/28 10:43:04.728144450 {wncd_x_R0-0}{1}: [epm-misc] [19620]: (info): [08be.ac14.137d:capwap_9000

2024/03/28 10:43:04.728161361 {wncd_x_R0-0}{1}: [epm] [19620]: (info): [08be.ac14.137d:capwap_90000012] 2024/03/28 10:43:04.728177773 {wncd_x_R0-0}{1}: [epm] [19620]: (info): [08be.ac14.137d:capwap_90000012] 2024/03/28 10:43:04.728184975 {wncd_x_R0-0}{1}: [epm] [19620]: (info): [08be.ac14.137d:capwap_90000012]

2024/03/28 10:43:04.728218783 {wncd_x_R0-0}{1}: [epm-acl] [19620]: (info): [08be.ac14.137d:capwap_90000

2024/03/28 10:43:04.729005675 {wncd_x_R0-0}{1}: [epm] [19620]: (info): [08be.ac14.137d:capwap_90000012] 2024/03/28 10:43:04.729019215 {wncd_x_R0-0}{1}: [svm] [19620]: (info): SVM_INFO: Response of epm is ASY [...]

2024/03/28 10:43:04.729422929 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Send Access-Request to

2024/03/28 10:43:04.729428175 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: authenticator 20 06 3

2024/03/28 10:43:04.729432771 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: NAS-IP-Address [4] 6

2024/03/28 10:43:04.729435487 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: User-Name [1] 32 "#ACS

2024/03/28 10:43:04.729437912 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 32

2024/03/28 10:43:04.729440782 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 26 "a

2024/03/28 10:43:04.729442854 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 30

2024/03/28 10:43:04.729445280 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 24 "a

2024/03/28 10:43:04.729447530 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Message-Authenticator 2024/03/28 10:43:04.729529806 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Started 5 sec timeout

2024/03/28 10:43:04.731972466 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Received from id 1812,

2024/03/28 10:43:04.731979444 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: authenticator 2a 24 8

2024/03/28 10:43:04.731983966 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: User-Name [1] 32 "#ACS

2024/03/28 10:43:04.731986470 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Class [25] 75 ... 2024/03/28 10:43:04.732032438 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Message-Authenticator

2024/03/28 10:43:04.732048785 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 47

2024/03/28 10:43:04.732051657 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 41 ":

2024/03/28 10:43:04.732053782 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 47

2024/03/28 10:43:04.732056351 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 41 ":

2024/03/28 10:43:04.732058379 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 48

2024/03/28 10:43:04.732060673 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 42 "i

2024/03/28 10:43:04.732062574 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 36

2024/03/28 10:43:04.732064854 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 30 ":

2024/03/28 10:43:04.732114294 {wncd_x_R0-0}{1}: [radius] [19620]: (info): Valid Response Packet, Free t [...]

2024/03/28 10:43:04.733046258 {wncd_x_R0-0}{1}: [svm] [19620]: (info): [08be.ac14.137d] Applied User Pro

```
2024/03/28 10:43:04.733058380 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: M
2024/03/28 10:43:04.733064555 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: M
2024/03/28 10:43:04.733065483 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: e
2024/03/28 10:43:04.733066816 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: m
2024/03/28 10:43:04.733068704 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: c
2024/03/28 10:43:04.733069947 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: c
```

2024/03/28 10:43:04.733070971 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: us

```
2024/03/28 10:43:04.733079208 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: c
2024/03/28 10:43:04.733080328 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: E
M$®vf9∫Ø◊«? %ÿ0?ã@≤™ÇÑbWï6\Ë&\q·lU+QB-º®"≠∫JÑv?"
2024/03/28 10:43:04.733091441 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: e
```

2024/03/28 10:43:04.733092470 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile:Cis

[...]

2024/03/28 10:43:04.733396045 {wncd_x_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap_90000

2024/03/28 10:43:04.733486604 {wncd_x_R0-0}{1}: [client-auth] [19620]: (note): MAC: 08be.ac14.137d L2 A

2024/03/28 10:43:04.734665244 {wncd_x_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Client-auth]

2024/03/28 10:43:04.734894043 {wncd_x_R0-0}{1}: [client-keymgmt] [19620]: (info): MAC: 08be.ac14.137d E 2024/03/28 10:43:04.734904452 {wncd_x_R0-0}{1}: [client-keymgmt] [19620]: (info): MAC: 08be.ac14.137d C

2024/03/28 10:43:04.734915743 {wncd_x_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap_90000012

2024/03/28 10:43:04.740499944 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.742238941 {iosrp_R0-0}{1}: [og] [26311]: (info): OG_PI_ACL_INFO: ogacl_configured: A

2024/03/28 10:43:04.744387633 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= c

[...]

2024/03/28 10:43:04.745245318 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: epm acl]

2024/03/28 10:43:04.745294050 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Allocate

2024/03/28 10:43:04.745326416 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Index in

2024/03/28 10:43:04.751291844 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= 0

2024/03/28 10:43:04.751943577 {iosrp_R0-0}{1}: [og] [26311]: (info): OG_PI_ACL_INFO: ogacl_configured: A

2024/03/28 10:43:04.752686055 {wncd_x_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Client-auth]

2024/03/28 10:43:04.755505991 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.756746153 {wncd_x_R0-0}{1}: [mm-transition] [19620]: (info): MAC: 08be.ac14.137d MM 2024/03/28 10:43:04.757801556 {wncd_x_R0-0}{1}: [client-auth] [19620]: (note): MAC: 08be.ac14.137d ADD

2024/03/28 10:43:04.758843625 {wncd_x_R0-0}{1}: [client-orch-state] [19620]: (note): MAC: 08be.ac14.1376

2024/03/28 10:43:04.759064834 {wncd_x_R0-0}{1}: [client-iplearn] [19620]: (info): MAC: 08be.ac14.137d II

2024/03/28 10:43:04.761186727 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: epm acl]

2024/03/28 10:43:04.761241972 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Index in

2024/03/28 10:43:04.763131516 {wncd_x_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Client-auth]

2024/03/28 10:43:04.764575895 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.764755847 {iosrp_R0-0}{1}: [og] [26311]: (info): OG_PI_ACL_INFO: ogacl_configured: A

2024/03/28 10:43:04.769965195 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.770727027 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.772314586 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: epm acl]

2024/03/28 10:43:04.772362837 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Index in

2024/03/28 10:43:04.773070456 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.773661861 {iosrp_R0-0}{1}: [og] [26311]: (info): OG_PI_ACL_INFO: ogacl_configured: A

2024/03/28 10:43:04.775537766 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= o

2024/03/28 10:43:04.778756670 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: epm acl]

2024/03/28 10:43:04.778807076 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Index in

2024/03/28 10:43:04.778856100 {iosrp_R0-0}{1}: [mpls_ldp] [26311]: (info): LDP LLAF: Registry notificat:

2024/03/28 10:43:04.779401863 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.779879864 {iosrp_R0-0}{1}: [og] [26311]: (info): OG_PI_ACL_INFO: ogacl_configured: A

2024/03/28 10:43:04.786433419 {wncd_x_R0-0}{1}: [sisf-packet] [19620]: (info): RX: DHCPv4 from interfac 2024/03/28 10:43:04.786523172 {wncd_x_R0-0}{1}: [sisf-packet] [19620]: (info): TX: DHCPv4 from interfac 2024/03/28 10:43:04.787787313 {wncd_x_R0-0}{1}: [sisf-packet] [19620]: (info): RX: DHCPv4 from interfac 2024/03/28 10:43:04.788160929 {wncd_x_R0-0}{1}: [sisf-packet] [19620]: (info): TX: DHCPv4 from interfac 2024/03/28 10:43:04.788491833 {wncd_x_R0-0}{1}: [client-iplearn] [19620]: (info): TX: DHCPv4 from interfac 2024/03/28 10:43:04.788576063 {wncd_x_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap_9000 2024/03/28 10:43:04.788741337 {wncd_x_R0-0}{1}: [webauth-sess] [19620]: (info): Change address update, 2024/03/28 10:43:04.788761575 {wncd_x_R0-0}{1}: [auth-mgr-feat_acct] [19620]: (info): [08be.ac14.137d:c2 2024/03/28 10:43:04.78877999 {wncd_x_R0-0}{1}: [epm] [19620]: (info): [0000.0000.0000:unknown] HDL = 0

2024/03/28 10:43:04.789333126 {wncd_x_R0-0}{1}: [client-iplearn] [19620]: (info): MAC: 08be.ac14.137d II

2024/03/28 10:43:04.789410101 {wncd_x_R0-0}{1}: [client-orch-sm] [19620]: (debug): MAC: 08be.ac14.137d

2024/03/28 10:43:04.789622587 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): [Applied attribute : us

2024/03/28 10:43:04.789632684 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): [Applied attribute : c

2024/03/28 10:43:04.789642576 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): [Applied attribute :Cis

2024/03/28 10:43:04.789651931 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): [Applied attribute :bs

2024/03/28 10:43:04.789653490 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): [Applied attribute : t 2024/03/28 10:43:04.789735556 {wncd_x_R0-0}{1}: [ew]c-qos-client] [19620]: (info): MAC: 08be.ac14.137d 2024/03/28 10:43:04.789800998 {wncd_x_R0-0}{1}: [rog-proxy-capwap] [19620]: (debug): Managed client RUN

PacketCapture

Een andere interessante reflex is pakketopnamen van de RADIUS-stroom voor een clientassociatie te nemen en te analyseren. Downloadbare ACL's zijn afhankelijk van RADIUS, niet alleen om te worden toegewezen aan een draadloze client, maar ook om te worden gedownload door de WLC. Terwijl u pakketopname neemt voor het oplossen van problemen met de configuratie van dACL's, moet u daarom op de interface opnemen die door de controller wordt gebruikt om met de RADIUS-server te communiceren. Dit document toont hoe u gemakkelijk ingesloten pakketvastlegging op Catalyst 9800 kunt configureren, die zijn gebruikt om de in dit artikel geanalyseerde opname te verzamelen.

RADIUS-clientverificatie

U kunt de client-RADIUS-toegangsaanvraag zien die van de WLC naar de RADIUS-server wordt verzonden om de gebruiker USER1 (AVP-gebruikersnaam) op de DACL_DOT1X_SSID SSID (AVP NAS-Identifier) te verifiëren.



Wanneer de verificatie slaagt, antwoordt de RADIUS-server met een access-accept, nog steeds voor gebruiker USER1 (AVP-gebruikersnaam) en past de AAA-kenmerken toe, in het bijzonder de verkoper-specifieke AVP ACS:CiscoSecure-Defined-ACL die hier "#ACSACL#-IP-ACL_USER1-65e89aab" is.



DACL-download

Als dACL al deel uitmaakt van de WLC-configuratie, wordt deze simpelweg toegewezen aan de gebruiker en worden de RADIUS-sessies beëindigd. Anders downloadt de WLC de ACL, nog steeds met RADIUS. Om dit te doen, doet de WLC een RADIUS access-request, dit keer met behulp van de dACL naam ("#ACSACL#-IP-ACL_USER1-65e89aab") voor de AVP User-Name. Tegelijkertijd informeert de WLC de RADIUS-server dat deze access-acceptatie een ACL-download initieert met behulp van het Cisco AV-paar aaa:event=acl-download.



De RADIUS-toegang-acceptatie die is teruggestuurd naar de controller bevat de gevraagde dACL, zoals aangegeven op de afbeelding. Elke ACL-regel bevindt zich in een andere Cisco AVP van het type "ip:inacl# $<X>=<ACL_REGEL>$ ", waarbij <X> het regelnummer is.

					Packet:	Go to packet Cancel
No.	Length ID	Source	Destination	linfo		Protocol
8037	184 3	9 10.48.39.130	10.48.39.134	Access-Request id=81, Duplicate Request		RADIUS
+ 8038	369 3	9 10.48.39.134	10.48.39.130	Access-Accept id=81		RADIUS
> Frame > Ethern 000, 10	8038: 369	bytes on wire (2952 c: VMware_8d:01:ec (0	bits), 369 bytes captured (7 0:50:56:8d:01:ec), Dst: Cise	2952 bits) co_b2:fe:ff (00:1e:f6:b2:fe:ff)		
> Intern	et Proto	col Version 4, Src: 10	.48.39.134, Dst: 10.48.39.13	30		
User D ~ RADIUS	atagram F Protocol	rotocol, Src Port: 18	12, Dst Port: 63772			
Code	: Access-	Accept (2)				
Leng	th: 323	(1161: 0X51 (81)				
Auth	enticator s is a re	: 61342164ce39be06eed	828b3ce566ef5 n frame 80361			
[Tim	e from re	quest: 0.007995000 se	conds]			
> AV	P: t=User	-Name(1) l=32 val=#AC	SACL#-IP-ACL_USER1-65e89aab			
> AV > AV	P: t=Clas P: t=Mess	s(25) l=75 val=434143 age-Authenticator(80)	533a30613330323738366d624251 l=18 val=a3c4b20cd1e64785d9	L7239445259673447765f436554692f48737050 De0232511cd8b72		
~ AV	P: t=Vend	lor-Specific(26) l=47	vnd=ciscoSystems(9)			
	Length: 4	7				
	Vendor ID VSA: t=Ci	: ciscoSystems (9) .sco-AVPair(1) l=41 va	l=ip:inacl#1=denv ip anv hos	st 10.48.39.13		
~ AV	P: t=Vend	lor-Specific(26) l=47	vnd=ciscoSystems(9)			
	Length: 4	7				
	Vendor ID VSA: t=Ci	: ciscoSystems (9) .sco-AVPair(1) l=41 va	l=ip:inacl#2=denv ip anv hos	st 10.48.39.15		
~ AV	P: t=Vend	or-Specific(26) l=48	vnd=ciscoSystems(9)			
	Length: 4	8				
	Vendor ID VSA: t=Ci	: ciscoSystems (9) .sco-AVPair(1) l=42 va	l=ip:inacl#3=denv ip anv hos	t 10.48.39.186		
~ AV	P: t=Vend	lor-Specific(26) l=36	vnd=ciscoSystems(9)			
	Length: 3	6				
	Vendor ID VSA: t=Ci	: ciscoSystems (9) .sco-AVPair(1) l= <u>30 va</u>	l=ip:inacl#4=permit ip any a	any		
• 2 •	DILIS Protocol (re	dus). 323 bytes		- Parkar	ts: 43372 - Displayed: 2 (0.0%)	Profile: Default
	the second se				and the second sec	Provide: Delagan



Opmerking: Als de inhoud van een download ACL wordt gewijzigd nadat deze op de WLC is gedownload, wordt de wijziging voor deze ACL niet weergegeven tot een gebruiker die deze gebruikt opnieuw authenticeert (en de WLC voert opnieuw een RADIUS-verificatie uit voor zo'n gebruiker). Een wijziging in de ACL wordt weerspiegeld door een wijziging in het hashgedeelte van de ACL-naam. Daarom moet de volgende keer dat deze ACL aan een gebruiker wordt toegewezen, de naam anders zijn en moet de ACL dus geen deel uitmaken van de WLC-configuratie en moet worden gedownload. Clients die voor de wijziging op de ACL authenticeren, blijven echter de vorige gebruiken totdat ze volledig opnieuw worden geauthenticeerd.

ISE-functielogboeken

RADIUS-clientverificatie

De verrichtingslogbestanden tonen een succesvolle verificatie van de gebruiker "USER1", waarop de downloadbare ACL "ACL_USER1" wordt toegepast. Delen van belang voor het oplossen van problemen worden in rood weergegeven.

Cisco ISE

Overview	
Event	5200 Authentication succeeded
Username	USER1
Endpoint Id	08:BE:AC:14:13:7D ⊕
Endpoint Profile	Unknown
Authentication Policy	Default >> Dot1X
Authorization Policy	Default >> 802.1x User 1 dACL
Authorization Result	9800-DOT1X-USER1

Authentication Details	
Source Timestamp	2024-03-28 05:11:11.035
Received Timestamp	2024-03-28 05:11:11.035
Policy Server	ise
Event	5200 Authentication succeeded
Username	USER1
User Type	User
Endpoint Id	08:BE:AC:14:13:7D
Calling Station Id	08-be-ac-14-13-7d
Endpoint Profile	Unknown
Authentication Identity Store	Internal Users
Identity Group	Unknown
Identity Group Audit Session Id	Unknown 8227300A0000000B848ABE3F
Identity Group Audit Session Id Authentication Method	Unknown 8227300A0000000D848ABE3F dot1x
Identity Group Audit Session Id Authentication Method Authentication Protocol	Unknown 8227300A000000D848ABE3F dol1x PEAP (EAP-MSCHAPv2)
Identity Group Audit Session Id Authentication Method Authentication Protocol Service Type	Unknown 8227300A000000D848ABE3F dol1x PEAP (EAP-MSCHAPv2) Framed
Identity Group Audit Session Id Authentication Method Authentication Protocol Service Type Network Device	Unknown 8227300A000000D848ABE3F dot1x PEAP (EAP-MSCHAPv2) Framed gdefland-9800
Identity Group Audit Session Id Authentication Method Authentication Protocol Service Type Network Device Device Type	Unknown 8227300A0000000D848ABE3F det1x PEAP (EAP-MSCHAPv2) Framed gdefland-9800 All Device Types
Identity Group Audit Session Id Authentication Method Authentication Protocol Service Type Network Device Device Type Location	Unknown 8227300A000000D848ABE3F dot1x PEAP (EAP-MSCHAPv2) Framed gdefland-9800 All Device Types All Locations
Identity Group Audit Session Id Authentication Method Authentication Protocol Service Type Network Device Device Type Location NAS IPv4 Address	Unknown 8227300A000000D848ABE3F dot1x PEAP (EAP-MSCHAPv2) Framed gdefland-9800 All Device Types All Locations 10.48.39.130
Identity Group Audit Session Id Authentication Method Authentication Protocol Service Type Network Device Device Type Location NAS IPv4 Address NAS Port Type	Unknown 822730040000000D848ABE3F dot1x PEAP (EAP-MSCHAPv2) Framed gdefland-9800 All Device Types All Locations 10.48.39.130 Wireless - IEEE 802.11
Identity Group Audit Session Id Authentication Method Authentication Protocol Service Type Network Device Device Type Location NAS IPv4 Address NAS Port Type Authorization Profile	Unknown 8227300A0000000B48ABE3F dol1x PEAP (EAP-MSCHAPv2) Framed gdefland-9800 All Device Types All Locations 10.48.39.130 Wireless - IEEE 802.11 9800-DOT1X-USER1

S

Steps	
11001	Received RADIUS Access-Request
11017	RADIUS created a new session
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
11507	Extracted EAP-Response/Identity
12500	Prepared EAP-Request proposing EAP-TLS with challenge
12625	Valid EAP-Key-Name attribute received
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12301	Extracted EAP-Response/NAK requesting to use PEAP instead
12300	Prepared EAP-Request proposing PEAP with challenge
12625	Valid EAP-Key-Name attribute received
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12302	Extracted EAP-Response containing PEAP challenge- response and accepting PEAP as negotiated
12318	Successfully negotiated PEAP version 0
12800	Extracted first TLS record; TLS handshake started
12805	Extracted TLS ClientHello message
12806	Prepared TLS ServerHello message
12807	Prepared TLS Certificate message
12808	Prepared TLS ServerKeyExchange message
12810	Prepared TLS ServerDone message
12305	Prepared EAP-Request with another PEAP challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PEAP challenge- response
12305	Prepared EAP-Request with another PEAP challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PEAP challenge- response
12305	Prepared EAP-Request with another PEAP challenge

12305 Prepared EAP-Request with another PEAP challenge 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request 11018 RADIUS ir re-using an existing session 12304 Extracted EAP-Response containing PEAP challenge-response

12318 Successfully negotiated PEAP version 0

Other Attributes	
ConfigVersionId	73
DestinationPort	1812
Protocol	Radius
NAS-Port	3913
Framed-MTU	1485
State	37CPMSessionID=8227300A000000D848ABE3F;26SessionI D=ise/499610885/35;
undefined-186	00:0f:ac:04
undefined-187	00:0f:ac:04
undefined-188	00:0f:ac:01
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	ise/499610885/35
SelectedAuthenticationIden	Internal Users
SelectedAuthenticationIden	All_AD_Join_Points
SelectedAuthenticationIden	Guest Users
AuthenticationStatus	AuthenticationPassed
AuthenticationStatus IdentityPolicyMatchedRule	AuthenticationPassed Dot1X
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched	AuthenticationPassed Dot1X 802.1x User 1 dACL
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-BE-AC-14-13-7D
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-BE-AC-14-13-7D Default
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-BE-AC-14-13-7D Default Dot1X
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-BE-AC-14-13-7D Default Dot1X 515
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency ClientLatency	AuthenticationPassed Det1X 802.1x User 1 dACL 08-BE-AC-14-13-7D Default Det1X 515 147
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency ClientLatency TLSCipher	AuthenticationPassed Det1X 802.1x User 1 dACL 08-BE-AC-14-13-7D Default Dot1X 515 147 ECOHE-RSA-AES256-GCM-SHA384
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency ClientLatency TLSCipher TLSCipher TLSVersion	AuthenticationPassed Det1X 802.1x User 1 dACL 08-BE-AC-14-13-7D Default Dot1X 515 147 ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency ClientLatency TLSCipher TLSSversion DTLSSupport	AuthenticationPassed Det1X 802.1x User 1 dACL 08-BE-AC-14-13-7D Default Det1X 515 147 ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Unknown
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency CilentLatency TLSCipher TLSSversion DTLSSupport HostIdentityGroup	AuthenticationPassed Det1X 802.1x User 1 dACL 08-BE-AC-14-13-7D Default Det1X 515 147 ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Unknown Endpoint Identity Groups:Unknown
AuthenticationStatus identityPolicyMatchedRule AuthorizationPolicyMatchedL EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency ClientLatency TLSCipher TLSVersion DTLSSupport HostIdentityGroup Network Device Profile	AuthenticationPassed Det1X 802.1x User 1 dACL 08-BE-AC-14-13-7D Default Dot1X 515 147 ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Unknown Endpoint Identity Groups:Unknown Cisco
AuthenticationStatus identityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency ClientLatency TLSCipher TLSVersion DTLSSupport HostIdentityGroup Network Device Profile Location	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-8E-AC-14-13-7D Default Dot1X 515 147 ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Unknown Endpoint Identity Groups:Unknown Cisco Location#All Locations
AuthenticationStatus identityPolicyMatchedRule AuthorizationPolicyMatchedL EndPointMACAddress ISEPolicySetName identitySelectionMatchedRule TotalAuthenLatency ClientLatency TLSCipher TLSVersion DTLSSupport HostidentityGroup Network Device Profile Location Device Type	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-8E-AC-14-13-7D Default Dot1X 515 147 ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Unknown Endpoint Identity Groups:Unknown Cisco Locationt#All Locations Device Type#All Device Types
AuthenticationStatus identityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName identitySelectionMatchedRule TotalAuthenLatency ClientLatency TLSCipher TLSVersion DTLSSupport HostIdentityGroup Network Device Profile Location Device Type IPSEC	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-8E-AC-14-13-7D Default Dot1X 515 147 ECDHE-RSA-AES256-GCM-SHA384 TLSV1.2 Unknown Endpoint Identity Groups:Unknown Cisco LocationHAll Locations Device TypesHAII Device Types IPSECHIS IPSEC DeviceIINo

EnableFlag	Enabled
RADIUS Username	USER1
NAS-Identifier	DACL_DOT1X_SSID
Device IP Address	10.48.39.130
CPMSessionID	8227300A000000D848ABE3F
Called-Station-ID	10-b3-c6-22-99-c0:DACL_DOT1X_SSID
CiscoAVPair	service-type=Framed, audit-session-id=8227300A0000000B48A8E3F, method=doft1x, client-iif-id=2113931001, vlan-id=1413, clisco-wlan-ssid=DACL_DOT1X_SSID, wlan-profile-name=DACL_DOT1X_SSID, AuthenticationIdentityStore=Internal Users, FQSubjectName9273630-8c01-11e6-996c- 525400b48521Nuser1, UniqueSubjectID=94b3604f5b49b88ccfafe2f3a86c80d1979b 5c43
Result	

Class	CACS:8227300A0000000D848ABE3F:ise/499610885/35
EAP-Key-Name	19:66:05:40:45:8d:a0:0b:35:b3:a4:1b:ab:87:b8:72:94:16:e3:b 9:93:27:37:29:6b:c5:88:e3:b1:40:23:0a:b3:96:6f:85:82:04:0a:a 5:c5:05:d6:75:5b:11:24:62:d3:6b:e0:19:c1:46:a4:29:f0:ba:65:0 6:9c:e1:3e:91:f6
cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-ACL_USER1- 65e89aab
MS-MPPE-Send-Key	
MS-MPPE-Recv-Key	
LicenseTypes	Essential license consumed.
Session Events	
2024-03-28 05:11:11.035	Authentication succeeded

12810	Prepared TLS ServerDone message
12812	Extracted TLS ClientKeyExchange message
12803	Extracted TLS ChangeCipherSpec message
12804	Extracted TLS Finished message
12801	Prepared TLS ChangeCipherSpec message
12802	Prepared TLS Finished message
12816	TLS handshake succeeded
12310	PEAP full handshake finished successfully
12305	Prepared EAP-Request with another PEAP challenge
11005	Received RADIUS Access-Gnailenge
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PEAP challenge- response
12313	PEAP inner method started
11521	Prepared EAP-Request/Identity for inner EAP method
12305	Prepared EAP-Request with another PEAP challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PEAP challenge- response
11522	Extracted EAP-Response/Identity for inner EAP method
11806	Prepared EAP-Request for inner method proposing EAP- MSCHAP with challenge
12305	Prepared EAP-Request with another PEAP challenge
11006	Returned RADIUS Access-Challenge
11018	PADIUS is re-using an existing session
12304	Extracted EAP-Response containing PEAP challenge- response
11808	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP- MSCHAP as negotiated
15041	Evaluating Identity Policy
15048	Queried PIP - Normalised Radius.RadiusFlowType
22072	Selected identity source sequence - All_User_ID_Stores
15013	Selected Identity Source - Internal Users
24210	Looking up User in Internal Users IDStore - USER1
24212	Found User in Internal Users IDStore
22037	Authentication Passed
11824	EAP-MSCHAP authentication attempt passed
12305	Prepared EAP-Request with another PEAP challenge
11005	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
	Extracted EAP-Response containing PEAP challenge-
12304	response
11810	Extracted EAP-Response for inner method containing
11014	Incer EAD-MSCHAD authentication susceeded
11610	Prepared FAP-Success for incer FAP method
12314	PEAP inner method finished successfully
12305	Prepared EAP-Request with another PEAP challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PEAP challenge- response
24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory
15036	Evaluating Authorization Policy
24209	Looking up Endpoint in Internal Endpoints IDStore - USER1
24211	Found Endpoint in Internal Endpoints IDStore
15048	Queried PIP - Network Access.UserName
15048	Selected Authorization Profile - 9800-0071X-USEP1
11022	Added the dACL specified in the Authorization Profile

22081 Max sessions policy passed

- 22080 New accounting session created in Session cache
- 12306 PEAP authentication succeeded
- 11503 Prepared EAP-Success 11002 Returned RADIUS Access-Accept

DACL-download

De verrichtingslogboeken tonen een succesvolle download van ACL "ACL_USER1". Delen van belang voor het oplossen van problemen worden in rood weergegeven.

Cisco ISE

Overview			
Event	5232 DACL Download Succeeded		
Username	#ACSACL#-IP-ACL_USER1-65e89aab		
Endpoint Id			
Endpoint Profile			
Authorization Result			
Authentication Details			
Source Timestamp	2024-03-28 05:43:04.755		
Received Timestamp	2024-03-28 05:43:04.755		
Policy Server	ise		
Event	5232 DACL Download Succeeded		
Username	#ACSACL#-IP-ACL_USER1-65e89aab		
Network Device	gdefland-9800		
Device Type	All Device Types		
Location	All Locations		
NAS IPv4 Address	10.48.39.130		
Response Time	1 milliseconds		
Other Attributes			
ConfigVersionId	73		
DestinationPort	1812		
Protocol	Radius		
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c		
IsThirdPartyDeviceFlow	false		
AcsSessionID	ise/499610885/48		
TotalAuthenLatency	1		
ClientLatency	0		
DTLSSupport	Unknown		
Network Device Profile	Cisco		
Location	Location#All Locations		
Device Type	Device Type#All Device Types		
IPSEC	IPSECIIIs IPSEC Device#No		
RADIUS Username	#ACSACL#-IP-ACL_USER1-65e89aab		
Device IP Address	10.48.39.130		
CPMSessionID	0a302786pW4sgAjhERVzOW2a4lizHKqV4k4gukE1upAfdFbcs eM		
CiscoAVPair	aaa:service=ip_admission, aaa:event=acl-download		
Result			
Class	CACS:0a302786pW4sgAjhERVzOW2a4lizHKqV4k4gukE1upAfd FbcseM:lse/499610885/48		
cisco-av-pair	ip:inacl#1=deny ip any host 10.48.39.13		
cisco-av-pair	ip:inacl#2=deny ip any host 10.48.39.15		
cisco-av-pair	ip:inacl#3=deny ip any host 10.48.39.186		
cisco-av-pair	ip:inacl#4+permit ip any any		

Steps

11001	Received	RADIUS	Access-Request

- 11017 RADIUS created a new session 11117 Generated a new session ID 11102 Returned RADIUS Access-Accept

1

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.