# Configuration du & Dépannage des ACL téléchargeables sur Catalyst 9800

# Table des matières

Introduction
Informations générales
Conditions préalables
Exigences
Composants utilisés
Configurer
Utilisation de dACL avec des SSID 802.1x
Diagramme du réseau
Configuration WLC
Configuration ISE
dACL par utilisateur
dACL par résultat
Remarques sur l'utilisation des dACL avec les SSID CWA
Vérifier
<u>Dépannage</u>
Liste de vérification
WLC One Stop-Shop Reflex
Commandes show du WLC
Débogage conditionnel et traçage Radio Active
Capture de paquets
Authentification du client RADIUS
Téléchargement DACL
Journaux des opérations ISE
Authentification du client RADIUS
Téléchargement DACL

# Introduction

Ce document décrit comment configurer et dépanner les ACL téléchargeables (dACL) sur le contrôleur LAN sans fil (WLC) Catalyst 9800.

# Informations générales

Les dACL sont prises en charge depuis de nombreuses années dans les commutateurs Cisco IOS® et IOS XE®. Une dACL fait référence au fait que le périphérique réseau télécharge

dynamiquement les entrées de la liste de contrôle d'accès à partir du serveur RADIUS lors de l'authentification, plutôt que d'avoir une copie locale de la liste de contrôle d'accès et d'être simplement affecté au nom de la liste de contrôle d'accès. Un <u>exemple</u> de <u>configuration Cisco ISE</u> plus complet est disponible. Ce document se concentre sur le Cisco Catalyst 9800 qui prend en charge les dACL pour la commutation centrale depuis la version 17.10.

# Conditions préalables

L'idée derrière ce document est de démontrer l'utilisation des dACL sur Catalyst 9800 à travers un exemple de configuration SSID de base, montrant comment ceux-ci peuvent être entièrement personnalisables.

Sur le contrôleur sans fil Catalyst 9800, les ACL téléchargeables sont

- Pris en charge <u>à partir de la</u> version<u>17.10.1 de Cisco IOS XE Dublin</u>.
- Prise en charge pour contrôleur centralisé avec points d'accès en mode local uniquement (ou commutation centrale Flexconnect). La commutation locale FlexConnect ne prend pas en charge dACL.

# Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Modèle de configuration Catalyst Wireless 9800.
- Listes de contrôle d'accès IP (ACL) Cisco.

# Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

# Configurer

Tout au long de ce guide de configuration, même si les méthodes sont différentes (par exemple, authentification WLAN, configuration des politiques, etc.), le résultat final est le même. Dans le scénario présenté ici, deux identités d'utilisateur sont définies, USER1 et USER2. Tous deux ont accès au réseau sans fil. À chacun d'eux est attribué, respectivement, ACL\_USER1 et ACL\_USER2 étant des dACL téléchargées par le Catalyst 9800 depuis ISE.

# Utilisation de dACL avec des SSID 802.1x

# Diagramme du réseau



# **Configuration WLC**

Pour plus d'informations sur la configuration des SSID 802.1x et le dépannage sur le Catalyst 9800, veuillez vous reporter au guide de configuration <u>Configurer l'authentification 802.1x sur le contrôleur sans fil Catalyst 9800</u>.

Étape 1. Configurez le SSID.

Configurez un SSID authentifié 802.1x, en utilisant ISE comme serveur RADIUS. Dans ce document, le SSID a été nommé "DACL\_DOT1X\_SSID".

### À partir de la GUI :

Accédez à Configuration > Tags & Profiles > WLAN et créez un WLAN semblable à celui montré ici :

Cisco Cata	lyst 9800-CL Wireless Controller		Welcome admin	* * 4 8 4 8 0 2	Search APs and Clients Q	₹ ⊕
Q: Search Menu Items	Configuration * > Tags & Profiles * > WLAN:	S				
Dashboard	+ Add × Delete	Enable WLAN Disable WLAN			WLAN	Wizard
Monitoring ,	Selected WLANs : 0					
🖏 Configuration 💦 🔸	Status Y Name DACL_DOT1X_SSID	▼ ID 2	SSID     DACL_DOT1X_SSID	2.4/5 GHz Security     [WPA2][802.1x][AES]	Y 6 GHz Security	Ŧ
Administration >	H - 1 - H - 10 -				1 - 1 o	f 1 items
C Licensing						
X Troubleshooting						
Walk Me Through >						

# À partir de la 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

Étape 2. Configurez le profil de stratégie.

Configurez le profil de stratégie utilisé avec le SSID défini ci-dessus. Sur ce profil de stratégie, assurez-vous que AAA Override est configuré à partir de l'onglet « Advanced », comme indiqué dans la capture d'écran. Dans ce document, le profil de stratégie utilisé est « DACL-8021X ».

Comme indiqué dans la section des conditions préalables, les dACL sont uniquement prises en charge pour les déploiements de commutation/d'authentification centralisés. Assurez-vous que le profil de stratégie est configuré de cette façon.

### À partir de la GUI :

Accédez à Configuration > Tags & Profiles > Policy, sélectionnez le profil de stratégie utilisé et configurez-le comme indiqué.



CISCO CISCO Catal	yst 9800-CL wireless Controller	Welcome some Market	C Search Ar's and Cleris Q Carebound P. (4
Q. Search Menu Items	Configuration * > Tags & Profiles * > Policy	Edit Policy Profile	ж
Dashbaard	+ Add X Delete	A Disabling a Policy or configuring it in 'Enabled' state, will result in lo	ss of connectivity for clients associated with this Policy profile.
Mashboard	Admin Y Associated O Y Status Policy Taos Policy Profile Name	Canadal Assace Delicing OOS and AVC Mability Advan	
() Monitoring >		General Access Policies QCS and AVC Mobility Adve	inced
🔧 Configuration 💦 🔸	default-policy-profile	WLAN Timeout	Fabric Profile Search or Select 🗸 🖉
(Ô) Administration	18 4 <b>1 b</b> 81 <b>10 </b>	Session Timeout (sec) 28800	Link-Local Bridging
C Licensing		Idle Timeout (sec) 300	mDNS Service default-mdns-ser   Clear
💥 Troubleshooting		Idle Threshold (bytes)	Hotspot Server Search or Select
		Client Exclusion Timeout (sec) 00 60	User Defined (Private) Network
		Guest LAN Session Timeout	Status
Walk Me Through >		DHCP	Drop Unicast
		IPv4 DHCP Required	DNS Layer Security
		DHCP Server IP Address	DNS Layer Security Not Configured
		Show more >>>	Flex DHCP Option ENABLED
		AAA Policy	Flex DNS Traffic IGNORE
		Allow AAA Override	Redirect
		NAC State	WLAN Flex Policy
		Policy Name default-aaa-policy × •	VLAN Central Switching
			Shit Marc and Search or Select - D
		D Cancel	Update & Apply to Device

### À partir de la 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
```

Étape 3. Attribuez le profil de stratégie et le SSID à la balise de stratégie utilisée.

À partir de la GUI :

Accédez à Configuration > Tags & Profiles > Tags. Dans l'onglet Balises de stratégie, créez (ou sélectionnez) la balise utilisée et attribuez-lui le WLAN et le profil de stratégie définis au cours des étapes 1 et 2.



À partir de la 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
```

Étape 4. Autoriser un attribut spécifique au fournisseur.

Les listes de contrôle d'accès téléchargeables sont transmises via des attributs spécifiques au fournisseur (VSA) dans l'échange RADIUS entre ISE et le WLC. La prise en charge de ces attributs peut être activée sur le WLC, à l'aide de ces commandes CLI.

À partir de la CLI :

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

Étape 5. Configurez la liste d'autorisations par défaut.

Lors de l'utilisation d'une dACL, l'autorisation réseau via RADIUS doit être appliquée pour que le WLC autorise tout utilisateur s'authentifiant sur le SSID 802.1x configuré. En effet, non seulement l'authentification mais aussi la phase d'autorisation sont gérées du côté du serveur RADIUS ici. Par conséquent, la liste d'autorisation est requise dans ce cas.

Assurez-vous que la méthode d'autorisation de réseau par défaut fait partie de la configuration du 9800.

### À partir de la GUI :

Accédez à Configuration > Security > AAA et à partir de la liste de méthodes AAA > Authorization tab, créez une méthode d'autorisation similaire à celle indiquée.



# À partir de la CLI :

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

# **Configuration ISE**

Lors de la mise en oeuvre de dACL dans un environnement sans fil avec ISE, deux configurations communes sont possibles, à savoir :

- 1. Configuration dACL par utilisateur. Ainsi, une dACL est attribuée à chaque identité particulière grâce à un champ d'identité personnalisé.
- 2. Configuration dACL par résultat. En optant pour cette méthode, une dACL particulière est

attribuée à un utilisateur en fonction de la stratégie d'autorisation qu'elle a mise en correspondance avec le jeu de stratégies utilisé.

### dACL par utilisateur

Étape 1. Définir un attribut utilisateur personnalisé dACL

Pour pouvoir attribuer une dACL à une identité d'utilisateur, ce champ doit d'abord être configurable sur l'identité créée. Par défaut, sur ISE, le champ « ACL » n'est pas défini pour toute nouvelle identité créée. Pour remédier à cela, on peut utiliser l'"Attribut Utilisateur Personnalisé" et définir un nouveau champ de configuration. Pour ce faire, accédez à Administration > Identity Management > Settings > User Custom Attributes. Utilisez le bouton "+" pour ajouter un nouvel attribut similaire à celui affiché. Dans cet exemple, le nom de l'attribut personnalisé est ACL.

≡ Cisco ISE		Administration · Identity N	lanagement		🔺 License Warning	\$ 0 p \$
Identities Groups	External Identity Sources	Identity Source Sequences	Settings			
User Custom Attributes						All $\sim$ $\nabla$
User Authentication Settings	Mandat Attrib	ute Name	Data Type			
Endpoint Purge						
Endpoint Custom Attributes	Firstn	ame	String			
REST ID Store Settings	Lastna	ime	String			
	Name		String			1
	Passw	ord (CredentialPassword)	String			
	✓ User Custom A	tributes				
	Attribute Name	Description	Data Type	Parameters	Default Value Ma	andatory
	ACL		String ~	String Max length	+	🗆 🍙 +
					Save	Reset

Une fois cette configuration effectuée, utilisez le bouton « Enregistrer » pour enregistrer les modifications.

Étape 2. Configurer la dACL

Accédez à Policy > Policy Elements > Results > Authorization > Downloadable ACLs pour afficher et définir dACL sur ISE. Utilisez le bouton Ajouter pour en créer un nouveau.

≡ Cisco ISE		Policy · Policy Elements			🔺 License Warning 🔍 🎯 💭 🐡
Dictionaries C	onditions	Results			
Authentication Authorization Authorization Profiles	>	Dow		LS Delete	Selected 0 Total 7 😅 🚳
000000000000000000000000000000000000000			Name	Description	
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		

L'écran de configuration « Nouvelle liste de contrôle d'accès téléchargeable » s'affiche. Sur celuici, configurez ces champs :

- Name : nom de la dACL définie.
- Description (facultatif) : brève description de l'utilisation de la dACL créée.
- IP version : version du protocole IP utilisée dans la dACL définie (version 4, 6 ou les deux).
- DACL Content : contenu de la dACL, conformément à la syntaxe de la liste de contrôle d'accès Cisco IOS XE.

Dans ce document, la dACL utilisée est "ACL\_USER1" et cette dACL autorise tout trafic sauf celui destiné à 10.48.39.186 et 10.48.39.13.

Une fois les champs configurés, utilisez le bouton « Submit » pour créer la dACL.

Répétez l'étape pour définir la dACL pour le deuxième utilisateur, ACL\_USER2, comme indiqué dans la figure.

≡ Cisco ISE			Policy · Po	🔺 License Warning 🔍 💮 💭 🐡							
Dictionaries Con	ditions	Results									
Authentication	>	Downloadable ACLs									
Authorization Authorization Profiles	~	🖉 Edit	Selected 0 Total 8 😴								
Downloadable ACLs			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	Deny all lov6 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								

Étape 3. Attribuer la dACL à une identité créée

Une fois la dACL créée, vous pouvez l'attribuer à n'importe quelle identité ISE à l'aide des attributs personnalisés utilisateur créés à l'étape 1. Pour ce faire, accédez à Administration > Identity Management > Identities > Users. Comme d'habitude, utilisez le bouton Ajouter pour créer un utilisateur.

■ Cisco ISE		Administration · Identity M	lanagement	🔺 License Wi	aming Q 🖉 🔎 🐡
Identities Groups E	xternal Identity Sources	Identity Source Sequences	Settings		
Users Latest Manual Network Scan Res	Network Ac	ccess Users			
		🛞 Change Status 🗸 🕁 Import	🛧 Export 🗸 🚦 Delete	✓ ☐ Duplicate	All $\sim$ $\nabla$
	Status	Username $\wedge$ Description	First Name Last Name	Email Address User Identity Groups	Admin
	Disabled	🧕 adminuser		admin-group	

Dans le formulaire de configuration « Nouvel utilisateur d'accès au réseau », définissez le nom d'utilisateur et le mot de passe de l'utilisateur créé. Utilisez l'attribut personnalisé « ACL » pour

affecter la dACL créée à l'étape 2 à l'identité. Dans l'exemple, l'identité USER1 utilisant ACL\_USER1 est définie.

E Cisco ISE		Administration - Identity Management	🔺 License Warning Q 💿 🗔 🔘
Identities Groups	xternal identity Sources Identity Source Sequences Settings		
Users Latest Manual Network Scan Res	Network Access Users List > USER1		
	~ Network Access User		
	* Username USER1		
	Status 🖉 Enabled ~	—	
	Account Name Alias		
	Email		
	✓ Passwords		
	Password Type: Internal Users ~		
	Password Lifetime:		
	With Expiration      Password will expire in 53 days		
	O Never Expires ()		
	Password Re-Enter Password		
	* Login Password	Generate Password	
	Enable Password	Generate Password	
	> Liser Information		
	> Account Options		
	> Account Disable Policy		
	✓ User Custom Attributes		
		7	
	HARE HARE OFFICE		
	✓ User Groups		
	🗄 Select an item 🗸 🔞 🔵		
			Save

Une fois les champs correctement configurés, utilisez le bouton « Submit » pour créer l'identité.

Répétez cette étape pour créer USER2 et lui attribuer ACL\_USER2.

E Cisco ISE	Administration - Identity Management	🔺 License Warning 🔍 🛞 💭
Identities Groups Ext	ernal Identity Sources Identity Source Sequences Settings	
Users Latest Manual Network Scan Res	Network Access Users	
		Selected O Total 3 🧷 💮
	🖉 Elli 🕂 Add 🛞 Change Status V 😀 Baport 🕲 Deport V 🔹 Deport V 🔹 Deport V	ALV V
	Status Username 🔿 Description First Name Last Name Email Address User Identity Groups Admin	
	© Disabled 1 adminuser admin-group	
	E Enabled _1_USER1	
	D Enabled 1 USER2	
	Network Access Users	

Étape 4. Configurez le résultat de la stratégie d'autorisation.

Une fois l'identité configurée et la dACL qui lui est attribuée, la stratégie d'autorisation doit toujours être configurée afin de faire correspondre l'attribut d'utilisateur personnalisé « ACL » défini à une tâche commune d'autorisation existante. Pour ce faire, accédez à Policy > Policy Elements > Results > Authorization > Authorization Profiles. Utilisez le bouton « Ajouter » pour définir une nouvelle stratégie d'autorisation.

- Name : nom de la stratégie d'autorisation, ici « 9800-DOT1X-USERS ».
- Access Type : type d'accès utilisé lorsque cette stratégie est mise en correspondance, ici ACCESS\_ACCEPT.
- Tâche courante : faites correspondre « Nom de la liste de contrôle d'accès » à InternalUser : <nom de l'attribut personnalisé créé> pour l'utilisateur interne.Selon les noms utilisés dans ce document, le profil 9800-DOT1X-USERS est configuré avec la liste de contrôle d'accès configurée comme InternalUser : ACL.

≡ Cisco ISE	Policy - Policy Elements	🔺 License Warring 🔍 🛞 💭 🕼
Dictionaries Conditions	Results	
Authentication >	Authorization Profiles > New Authorization Profile Authorization Profile	
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 🗰 Claco 🗸 🕀	
	Service Template	
	Track Movement	
	Agentiess Posture	
	Passive Identity Tracking 🗋 📀	
	✓ Common Tasks	
	Z DACL Name InternalUser:ACL ~	1
	IPv6 DACL Name	
	ACL (Filter-ID)	
	The sense only devices and	

Étape 5. Utiliser le profil d'autorisation dans le jeu de stratégies.

Une fois le résultat du profil d'autorisation correctement défini, il doit toujours faire partie du jeu de stratégies utilisé pour authentifier et autoriser les utilisateurs sans fil. Accédez à Policy > Policy Sets et ouvrez le jeu de stratégies utilisé.

Ici, la règle de stratégie d'authentification « Dot1X » correspond à toute connexion établie via la norme 802.1x filaire ou sans fil. La règle de stratégie d'autorisation « 802.1x Users dACL » implémente une condition sur le SSID utilisé (c'est-à-dire Radius-Called-Station-ID CONTAINS DACL\_DOT1X\_SSID). Si une autorisation est effectuée sur le WLAN "DACL\_DOT1X\_SSID", le profil "9800-DOT1X-USERS" défini à l'étape 4 est utilisé pour autoriser l'utilisateur.

Cisco ISE	Policy · Policy Sets			🔺 License Warning	Q (0)	6
olicy Sets→ Default			Reset	Reset Policyset Hitcounts		Save
Status Policy Set Name	Description Conditions			Allowed Protocols / Serve	r Sequer	nce I
Default	Default policy set			Default Network Access	∞ ~	+ :
$\sim$ Authentication Policy (2)						
🛨 Status Rule Name	Conditions		Use		Hits	Actio
Q Search						
	E Wired_802.1X		All_Us	ser_ID_Stores 🛛 🛛 🗸		
Oct1X	OR E Wireless_802.1X		> Opt	tions	65	¢
			All_Us	ser_ID_Stores 🛛 🛛 🗸		
Default			> Opt	tions	10	(¢}
> Authorization Policy - Local Exceptions						
> Authorization Policy - Global Exceptions						
Authorization Policy (2)		Results				
+ Status Rule Name	Conditions	Profiles	Security	y Groups	Hits	Actio
Q Search						
1 Soc.1x Users dACL	Radius-Called-Station-ID CONTAINS DACL_DOT1X_SSID	9800-DOT1X-USERS ×	v+ Select	t from list $\sim$ +	65	{¢}
O Default		DenyAccess ×	~+ Select	t from list $\sim+$	0	<b>(</b> \$}

### dACL par résultat

Pour éviter l'énorme tâche d'assigner une dACL particulière à chaque identité créée sur ISE, on peut choisir d'appliquer la dACL à un résultat de stratégie particulier. Ce résultat est ensuite appliqué en fonction de toute condition correspondant aux règles d'autorisation du jeu de stratégies utilisé.

Étape 1. Configurer la dACL

Exécutez la même étape 2 à partir de la <u>section Per-user dACLs</u> afin de définir les dACL nécessaires. Ici, il s'agit de ACL\_USER1 et ACL\_USER2.

Étape 2. Créer des identités

Accédez à Administration > Identity Management > Identities > Users et utilisez le bouton « Add » pour créer un utilisateur.



Dans le formulaire de configuration « Nouvel utilisateur d'accès au réseau », définissez le nom d'utilisateur et le mot de passe de l'utilisateur créé.

Cisco ISE				Administration - Identity Ma	negement	🔺 License Warning	0.0	¢ 52 ¢
Identities Groups	External Identity Sources	Identity Source Sequence	s Settings					
Users Latest Manual Network Scan Res	Network Access Users Lis	2 3 New Network Access User						
	~ Network Acces	ss User			_			
	* Usemame U	USER1						
	Status	🛢 Enabled 🗸			-			
	Account Name Allar		0					
	Email							
	✓ Passwords							
	Password Type:	Internel Users 🗸 🗸						
	- Password Lifetime							
	O With Expiration	0						
	<ul> <li>Never Expires</li> </ul>	0						
		Password	Re-Enter Password					
	* Login Password			Generate Password ()	1			
	Enoble Password			Generate Password	•			
	> User Informat	ion						
	> Account Optic	ons						
	> Account Disal	ble Policy						
	> User Custom	Attributes						
	> User Groups							
						Submit	Ca	ncel

Répétez cette étape pour créer USER2.

= Cisco ISE	Administration - Identity Management	🔺 Loanse Warming 🔍 🛞 💭 🏟
Identities Groups	ternal Identity Sources Identity Source Sequences Settings	
Users Latest Manual Network Scan Res	Network Access Users	
		Selected O Total 3 🜔 🔇
	🖉 tell 🕂 Add 🛞 Change Status 🗸 👍 Ingent 🛆 Expert 🗸 🖞 Delices 🗸 🗍 Delices	$u \sim - \nabla$
	Status Username 🔨 Description First Name Last Name Email Address User Identity Groups Admin	
	Ofisabled 1 adminuser     admin-group	
	GEnabled 1.05ER1	
	Bernarde Yogene	
	Metaoric Access Uners	

Étape 4. Configurez le résultat de la stratégie d'autorisation.

Une fois l'identité et la dACL configurées, la stratégie d'autorisation doit toujours être configurée afin d'attribuer une dACL particulière à l'utilisateur correspondant à la condition d'utilisation de cette stratégie. Pour ce faire, accédez à Policy > Policy Elements > Results > Authorization > Authorization Profiles. Utilisez le bouton « Ajouter » pour définir une nouvelle stratégie d'autorisation et renseignez ces champs.

- Name : nom de la stratégie d'autorisation, ici « 9800-DOT1X-USER1 ».
- Access Type : type d'accès utilisé lorsque cette stratégie est mise en correspondance, ici ACCESS\_ACCEPT.
- Tâche courante : faites correspondre « DACL Name » à « ACL\_USER1 » pour l'utilisateur interne. Selon les noms utilisés dans ce document, le profil 9800-DOT1X-USER1 est configuré avec la dACL configurée comme « ACL\_USER1 ».

E Cisco ISE	Policy - Policy Elements	A License Warning	Q	0 21	۲
Dictionaries Conditions	Results				
Asthurdsarbas     >       Asthurdsarbas     >       Asthurdsarbas     >       Downloadain Profiles     >       Profiles     >       Profiles     >       Clarit Provisioning     >	Authorization Profile         * Nomo       900-D0T1x-USEN1         Description				
	Common Tasks      DACL Name     ACL_USER1      O     HYS DACL Name     ACL (Harr-D)     ACL (Harr-D)     ACL (Harr-ID)				U
	Advanced Attributes Settings     Attributes Details     Astributes Details     Astributes Details     Astributes Details     Astributes Details	Submit		Cancel	

Répétez cette étape pour créer le résultat de stratégie « 9800-DOT1X-USER2 » et lui attribuer « ACL\_USER2 » comme DACL.

Cisco ISE		Policy	- Policy Elements 🔺 Literes Ruring Q (0) 53
Dictionaries Conditions	Results		
Authentication >	Standard Authorization Pro	ofiles	
Authorization ~	For Policy Facest as to Administration > System > Backup	8. Restore > Policy Export Page	
Authorization Profiles		a manager - I and Calent I also	Selected 8 Tatal 13 🦪 🤅
Development ACCI	🖉 Edit 🕂 Add 📋 Duplicate 🌒 Delete		ж ч т Т
rolling >	C Neme	Profile	∧ Description
contract of the second	9000-D011X-USD11	m Cisco 🕕	
Gast Resolution .	000-0011X-US612	tta Gisco 🕥	
	9000-DOTIX-USDAS	# Claca 🕠	Authorization profile for 802.1x users using dAGLs.
	Block_Miniess_Access	m Cisco 🕕	Default profile used to block wireless devices. Ensure that you configure a NULL ROUTE ACL on the Wireless LAN Controller
	Cisco_JP_Phones	# Cisco 🕕	Default profile used for Cloco Phones.
	Cisco_Temporal_Onboard	# Cisca 🕕	Onboard the device with Gisco temporal agent
	Chen_WebArth	AL Cisco 🕕	Default Profile used to redirect users to the CWA portal.
	Internal User Attribute Text	# Cisco 🕕	
	NSP_Onboard	m Cisco 🕕	Onboard the dovice with Nativo Supplicant Provisioning
	Non_Cisco_IP_Phones	📇 Cisco 🕧	Default Profile used for Non Cisco Phones.
	UDN	# Cisco 🕕	Default profile used for UDN.
	DenyAccess		Default Profile with access type as Access-Reject
	Permithecese		Default Profile with access type as Access-Accept

Étape 5. Utiliser des profils d'autorisation dans un ensemble de stratégies.

Une fois le profil d'autorisation correctement défini, il doit toujours faire partie du jeu de stratégies utilisé pour authentifier et autoriser les utilisateurs sans fil. Accédez à Policy > Policy Sets et ouvrez le jeu de stratégies utilisé.

Ici, la règle de stratégie d'authentification « Dot1X » correspond à toute connexion établie via la norme 802.1X filaire ou sans fil. La règle de stratégie d'autorisation « 802.1X User 1 dACL »

implémente une condition sur le nom d'utilisateur utilisé (c'est-à-dire InternalUser-Name CONTAINS USER1). Si une autorisation est effectuée à l'aide du nom d'utilisateur USER1, alors le profil "9800-DOT1X-USER1" défini à l'étape 4 est utilisé pour autoriser l'utilisateur et donc, la dACL de ce résultat (ACL\_USER1) est également appliquée à l'utilisateur. Il en va de même pour le nom d'utilisateur USER2, pour lequel « 9800-DOT1X-USER1 » est utilisé.

Leve Co		Default				(	a (	
may se	KS→ L	perault			Reset	Reset Policyset Hitcourts		- 24
State	an Pai	licy Set Name	Description Conditions			Allowed Protocols / Serve	r Sequr	ence
Q 9	earch							
	•	Defeat	Default policy set			Default Network Access		<u>+</u>
- Author	tication	Palicy (2)						
⊙ 8	itatus	Rule Name	Conditions		Use		Hits	Act
0	Search							
			Word_MD.XX		All_User	_D_Stores 00 V		Γ
	•	Det1X	CR Wite/suc_002.1X		> Optio	ns		H
			E Wood_MAR					
					AIL_User,	_iD_Stores 01 V		
	•	Defeat			> Optio	ns	10	0
Author	ization I	Pelicy - Local Exceptions						
Author	ization I	Policy - Global Exception	9					
- Author	instion 1	Palicy (3)						
				Results				
⊙ 8	itatus	Rule Name	Conditions	Profiles	Security G	roups	Hits	Ao
Q. 3	Search						_	
	•	#82.1x liter 2 dACL	1 Internativer Name 2008LS USER2	9800-DOT1X-USER2 ×	Select fr	om list ~+	0	{
	•	992.1x liter 1 dACL	1 Internativer Name 1008LS V3281	9600-DOT1X-USER1 ×	Select fr	om list 🔍 +	86	{
	•	Defeat		DenyAccess ×	Soloct fr	om list $\sim+$	٥	{

# Remarques sur l'utilisation des dACL avec les SSID CWA

Comme décrit dans le guide de configuration <u>Configure Central Web Authentication (CWA) on</u> <u>Catalyst 9800 WLC and ISE</u>, CWA se base sur MAB et sur un résultat particulier pour authentifier et autoriser les utilisateurs. Les listes de contrôle d'accès téléchargeables peuvent être ajoutées à la configuration CWA du côté ISE de la même manière que ce qui a été décrit ci-dessus.



Avertissement : les listes de contrôle d'accès téléchargeables peuvent uniquement être utilisées comme listes d'accès réseau et ne sont pas prises en charge comme listes de contrôle d'accès de pré-authentification. Par conséquent, toute liste de contrôle d'accès de pré-authentification utilisée dans un workflow CWA doit être définie dans la configuration WLC.

# Vérifier

Pour vérifier la configuration effectuée, ces commandes peuvent être utilisées.

# 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 }
```

Voici référencé la partie pertinente de la configuration WLC correspondant à cet exemple.

```
aaa new-model
1
!
aaa group server radius authz-server-group
server name DACL-RADIUS
!
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
!
Т
aaa server radius dynamic-author
client <ISE IP>
I
aaa session-id common
!
[...]
vlan 1413
name VLAN_1413
L
[...]
radius server DACL-RADIUS
address ipv4 <ISE IP> auth-port 1812 acct-port 1813
key 6 aHaOSX[QbbEHURGW`cXiG^UE]CR]^PVANfcbROb
!
T
[...]
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
```

La configuration du serveur RADIUS est présentée, affichée à l'aide de la commande show running-config all.

WLC#show running-config all | s radius-server radius-server attribute 77 include-in-acct-req radius-server attribute 77 include-in-access-req 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

Dépannage

Liste de vérification

- Vérifiez que les clients peuvent se connecter correctement au SSID 802.1X configuré.
- Assurez-vous que la requête d'accès/acceptation RADIUS contient les paires attribut-valeur (AVP) appropriées.
- Assurez-vous que les clients utilisent le profil WLAN/de stratégie approprié.

### WLC One Stop-Shop Reflex

Client Username : USER1

Pour vérifier si la dACL est correctement assignée à un client sans fil particulier, on peut utiliser la commande **show wireless client mac**address <H.H.H>detail comme montré. De là, différentes informations de dépannage utiles peuvent être vues, à savoir : le nom d'utilisateur du client, l'état, le profil de politique, le WLAN et, plus important encore, ici, l'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 | 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
[...]
```

Commandes show du WLC

Pour afficher toutes les listes de contrôle d'accès qui font actuellement partie de la configuration du WLC Catalyst 9800, vous pouvez utiliser la commande **show access-lists**. Cette commande répertorie toutes les ACL définies localement ou les dACL téléchargées par le WLC. Toutes les dACL téléchargées depuis ISE par le WLC ont le format xACSACLx-IP-<ACL\_NAME>-<ACL\_HASH>.



**Remarque** : les listes de contrôle d'accès téléchargeables restent dans la configuration tant qu'un client est associé et l'utilise dans l'infrastructure sans fil. Dès que le dernier client utilisant la dACL quitte l'infrastructure, la dACL est supprimée de la configuration.

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 implicit\_permit

```
[...]
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
[...]
```

### Débogage conditionnel et traçage Radio Active

Lors du dépannage de la configuration, vous pouvez collecter des traces radioactives pour un client supposé être affecté avec la dACL définie. Voici les journaux montrant la partie intéressante des traces radioactives pendant le processus d'association client pour le client 08be.ac14.137d.

<#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 10:43:04.353438621 {wncd\_x\_R0-0}{1}: [client-auth] [19620]: (note): MAC: 08be.ac14.137d L2 Au

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 "

2024/03/28 10:43:04.381506029 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: NAS-IP-Address [4] 6

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 "d

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 "v

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 f 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\_90000

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\_90000

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 10:43:04.729005675 {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 "i

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 "i

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 ":

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 "i

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:	n
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:	i

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\_9000

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= o

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= 0

[...]

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= o

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= of the set of the

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= o

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= o

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 10:43:04.777154567 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= c

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 10:43:04.780510740 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= c

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]: (note): MAC: 08be.ac14.137d C
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:c
2024/03/28	10:43:04.788877999	$wncd_x_R0-0$ {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

2024/03/28 10:43:04.789886011 {wncd\_x\_R0-0}{1}: [client-orch-state] [19620]: (note): MAC: 08be.ac14.1376

### Capture de paquets

Un autre réflexe intéressant est de prendre et d'analyser les captures de paquets du flux RADIUS pour une association client. Les listes de contrôle d'accès téléchargeables dépendent de RADIUS, non seulement pour être attribuées à un client sans fil, mais également pour être téléchargées par le WLC. Lors de la capture de paquets pour le dépannage de la configuration des dACL, vous devez donc effectuer la capture sur l'interface utilisée par le contrôleur pour communiquer avec le serveur RADIUS. <u>Ce document</u> montre comment configurer facilement la capture de paquets intégrée sur le Catalyst 9800, qui ont été utilisés pour collecter la capture analysée dans cet article.

### Authentification du client RADIUS

Vous pouvez voir la demande d'accès RADIUS du client envoyée du WLC au serveur RADIUS afin d'authentifier l'utilisateur USER1 (Nom d'utilisateur AVP) sur le SSID DACL\_DOT1X\_SSID (Identificateur NAS AVP).



Lorsque l'authentification réussit, le serveur RADIUS répond avec un access-accept, toujours pour l'utilisateur USER1 (AVP User-Name) et en appliquant les attributs AAA, en particulier l'AVP ACS:CiscoSecure-Defined-ACL spécifique au fournisseur étant ici "#ACSACL#-IP-ACL\_USER1-65e89aab".



### **Téléchargement DACL**

Si la dACL fait déjà partie de la configuration du WLC, alors elle est simplement assignée à l'utilisateur et la session RADIUS se termine. Sinon, le WLC télécharge la liste de contrôle d'accès, toujours en utilisant RADIUS. Pour ce faire, le WLC effectue une demande d'accès RADIUS, cette fois en utilisant le nom dACL ("#ACSACL#-IP-ACL\_USER1-65e89aab") pour le nom d'utilisateur AVP. Parallèlement, le WLC informe le serveur RADIUS que cette acceptation d'accès initie un téléchargement de liste de contrôle d'accès à l'aide de la paire AV Cisco aaa:event=acl-download.



Le message d'acceptation d'accès RADIUS renvoyé au contrôleur contient la dACL demandée, comme illustré. Chaque règle ACL est contenue dans un protocole Cisco AVP différent de type « ip : inacl#<X>=<ACL\_RULE> », <X> étant le numéro de la règle.

					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 et II, Su	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 s				and the second sec	Provide: Delagan



**Remarque** : si le contenu d'une ACL de téléchargement est modifié après qu'elle a été téléchargée sur le WLC, la modification pour cette ACL n'est pas reflétée jusqu'à ce qu'un utilisateur utilisant cette ACL se réauthentifie ( et le WLC effectue une authentification RADIUS pour un tel utilisateur à nouveau). En effet, une modification de la liste de contrôle d'accès se traduit par une modification de la partie hachée du nom de la liste. Par conséquent, la prochaine fois que cette liste de contrôle d'accès est attribuée à un utilisateur, son nom doit être différent et par conséquent, la liste de contrôle d'accès ne doit pas faire partie de la configuration du WLC et doit être téléchargée. Cependant, les clients qui s'authentifient avant la modification de la liste de contrôle d'accès contrôle d'accès continuent à utiliser la précédente jusqu'à ce qu'ils s'authentifient à nouveau complètement.

### Journaux des opérations ISE

### Authentification du client RADIUS

Les journaux d'opérations affichent une authentification réussie de l'utilisateur "USER1", auquel la liste de contrôle d'accès téléchargeable "ACL\_USER1" est appliquée. Les éléments intéressants pour le dépannage sont encadrés en rouge.

#### 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	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-8227300A0000000D848ABE3F, method=dot1x, client-iif-id=2113931001, vlan-id=1413, clisco-wlan-ssid=DACL_DOT1X_SSID, wlan-profile-name=DACL_DOT1X_SSID, AuthenticationIdentityStore=Internal Users, FQSubjectName=927a620-8c01-11e6=996c- 525400b48521Huser1, UniqueSubjectID=94b3604f5b49b88ccfafe2f3a86c80d1979b 5c43
Result	

Session Events	
LicenseTypes	Essential license consumed.
MS-MPPE-Recv-Key	
MS-MPPE-Send-Key	
cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-ACL_USER1- 65e89aab
EAP-Key-Name	19:66:05:40:45:8d:a0:0b:35:b3:a4:1b:ab:87:b8:72:94:16:93:b 9:93:27:37:29:6b:c5:88:e3:b1:40:23:0a:b3:96:6f:85:82:04:0a:c 5:c5:05:d6:75:b5:11:24:24:3:6b:e0:19:cf:46:a4:29:f0:ba:65:0 6:9c:ef:3e:9f:f6
Class	CACS:8227300A000000D848ABE3F:ise/499610885/35

#### 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 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 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 11001 Received RADIUS Access-Request 11018 RADIUS is re-using an existing session 12304 Extracted EAP-Response containing PEAP challengeresponse Extracted EAP-Response containing EAP-MSCHAP 11808 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 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request 11018 RADIUS is re-using an existing sessio 12304 Extracted EAP-Response containing PEAP challenge-11810 Extracted EAP-Response for inner method containing MSCHAP challenge-response 11814 Inner EAP-MSCHAP authentication succeeded 11519 Prepared EAP-Success for inner EAP 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 challengeresponse 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 Queried PIP InternalUser.Name
- 15016 Selected Authorization Profile 9800-DOT1X-USER1
- 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

### **Téléchargement DACL**

Les journaux des opérations indiquent que le téléchargement de la liste de contrôle d'accès « ACL\_USER1 » a réussi. Les éléments intéressants pour le dépannage sont encadrés en rouge.

#### 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:ise/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

### À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.