Configurar & Solucionar Problemas de ACLs Baixáveis no Catalyst 9800

Contents

Introdução
Informações de Apoio
Pré-requisitos
Requisitos
Componentes Utilizados
Configurar
Usando dACLs com SSIDs 802.1x
Diagrama de Rede
Configuração de WLC
Configuração do ISE
dACLs por usuário
dACLs por resultado
Observações sobre o uso de dACLs com SSIDs do CWA
Verificar
Troubleshooting
Lista de verificação
Reflexo de One Stop-Shop da WLC
Comandos show da WLC
Depuração condicional e rastreamento radioativo
Captura do pacote
Autenticação de cliente RADIUS
Download de DACL
Logs de operação do ISE
Autenticação de cliente RADIUS
Download de DACL

Introdução

Este documento descreve como configurar e solucionar problemas de ACLs para download (dACLs) no Catalyst 9800 Wireless LAN Controller (WLC).

Informações de Apoio

Os dACLs têm sido suportados por muitos anos nos switches Cisco IOS® e IOS XE®. Um dACL se refere ao fato de que o dispositivo de rede faz o download dinâmico das entradas ACL do

servidor RADIUS quando ocorre a autenticação, em vez de ter uma cópia local da ACL e apenas receber o nome da ACL. Um <u>exemplo de configuração do Cisco ISE</u> mais completo está disponível. Este documento concentra-se no Cisco Catalyst 9800 que suporta dACLs para switching central desde a versão 17.10.

Pré-requisitos

A ideia por trás deste documento é demonstrar o uso de dACLs no Catalyst 9800 através de um exemplo de configuração básica de SSID, mostrando como eles podem ser totalmente personalizáveis.

No controlador sem fio Catalyst 9800, as ACLs para download são

- Suportado a partir do Cisco IOS XE Dublin versão 17.10.1.
- Compatível com controlador centralizado com pontos de acesso no modo Local apenas (ou comutação central Flexconnect). O FlexConnect Local Switching não é compatível com dACL.

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Modelo de configuração do Catalyst Wireless 9800.
- Listas de controle de acesso (ACLs) IP da Cisco.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Em todo este guia de configuração, mesmo que os métodos sejam diferentes (por exemplo, autenticação WLAN, configuração de política, etc.), o resultado final é o mesmo. No cenário exposto aqui, duas identidades de usuário são definidas como USER1 e USER2. Ambos recebem acesso à rede sem fio. A cada um deles é atribuído, respectivamente, ACL_USER1 e ACL_USER2 sendo dACLs baixados pelo Catalyst 9800 do ISE.

Usando dACLs com SSIDs 802.1x

Diagrama de Rede



Configuração de WLC

Para obter detalhes sobre a configuração e a solução de problemas de SSIDs 802.1x no Catalyst 9800, consulte o guia de configuração <u>Configurar a Autenticação 802.1X no Catalyst 9800</u> <u>Wireless Controller Series</u>.

Etapa 1. Configure o SSID.

Configure um SSID 802.1x autenticado, usando o ISE como servidor RADIUS. Neste documento, o SSID foi nomeado como "DACL_DOT1X_SSID".

<u>Na GUI:</u>

Navegue para Configuration > Tags & Profiles > WLAN e crie uma WLAN semelhante à mostrada aqui:

Cisco Catal	ilyst 9800-CL Wireless Controller		Welcome admin		Search APs and Clients Q	eedback _K * ()
Q: Search Menu Items	Configuration * > Tags & Profiles * > WLA	Ns				
Dashboard	+ Add × Delete	Enable WLAN Disable WLAN				WLAN Wizard
Monitoring >	Selected WLANs : 0					
🖏 Configuration	Status T Name DACL_DOT1X_SSID	T ID	SSID DACL_DOT1X_SSID	2.4/5 GHz Security [WPA2](802.1x)[AES]	F 6 GHz Security	T
Administration	14 d 1 k d 1					1 - 1 of 1 items
C Licensing						
💥 Troubleshooting						
waik me incode a						

Na 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

Etapa 2. Configure o perfil de política.

Configure o perfil de política que é usado junto com o SSID definido acima. Neste perfil de política, certifique-se de que AAA Override esteja configurado na guia "Advanced", como mostrado na captura de tela. Neste documento, o perfil de política usado é "DACL-8021X".

Conforme indicado na seção de pré-requisitos, os dACLs são suportados apenas para implantações de switching/autenticação central. Certifique-se de que o perfil de política esteja configurado dessa maneira.

<u>Na GUI:</u>

Navegue até Configuration > Tags & Profiles > Policy, selecione o perfil de política usado e configure-o como mostrado.



Cisco Cisco Catal	yst 9800-CL Wireless Controller	Welcome admin	A & A B & B O	Search APs and Clients Q EFeedback	2.0
Q: Search Menu Items	Configuration * > Tags & Profiles * > Policy	Edit Policy Profile			,
Dashboard	+ Add × Delete	Disabling a Policy or	configuring it in 'Enabled' state, will result in lo	oss of connectivity for clients associated with this Policy profile	ie.
Monitoring >	Admin T Associated O T Policy Trags Policy Profile Name	General Access Policies	QOS and AVC Mobility Adv	ranced	
Configuration	DACL-8021X	WLAN Timeout		Fabric Profile Search or Select 👻 🖬	0
		Session Timeout (sec)	28800	Link-Local Bridging	
C Licensing		Idie Timeout (sec)	300	mDNS Service default-mdns-ser v 2 Policy Clear	
* Troubleshooting		Idle Threshold (bytes)	Ū.	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 Parameter Map Clear	
		Show more >>>		Flex DHCP Option ENABLED	
		AAA Policy		Flex DNS Traffic IGNORE	
		Allow AAA Override		WI AN Eley Dolloy	
		NAC State	0		
		Policy Name	default-aaa-policy 🛪 👻 💋	VLAN Central Switching	
		D Cancel		Shit Mart and E Search or Select • 10	o Device

Na 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
```

Etapa 3. Atribua o perfil de política e o SSID à tag de política usada.

Na GUI:

Navegue até Configuração > Marcas e perfis > Marcas. Na guia Policy tags (Marcas de política), crie (ou selecione) a marca usada e atribua a ela o perfil de WLAN e de política definido durante as etapas 1 a 2.



Na 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
```

Etapa 4. Permitir Atributo Específico Do Fornecedor.

As ACLs para download são passadas através de atributos específicos do fornecedor (VSA) na troca RADIUS entre o ISE e a WLC. O suporte a esses atributos pode ser habilitado na WLC, usando esses comandos da CLI.

Na CLI:

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

Etapa 5. Configurar Lista de Autorização Padrão.

Ao trabalhar com dACL, a autorização de rede através do RADIUS deve ser imposta para que a WLC autorize qualquer usuário que se autentique no SSID 802.1x configurado. De fato, não apenas a autenticação, mas a fase de autorização, é tratada aqui no lado do servidor RADIUS. Por conseguinte, a lista de autorização é necessária neste caso.

Verifique se o método de autorização de rede padrão faz parte da configuração do 9800.

<u>Na GUI:</u>

Navegue até Configuration > Security > AAA e, na guia AAA Method List > Authorization, crie um método de autorização semelhante ao mostrado.



Na CLI:

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

Configuração do ISE

Ao implementar dACLs em um ambiente sem fio com ISE, duas configurações comuns são possíveis, para saber:

- 1. Configuração de dACL por usuário. Com isso, cada identidade específica tem um dACL atribuído graças a um campo de identidade personalizado.
- 2. Configuração de dACL por resultado. Ao optar por esse método, um determinado dACL é atribuído a um usuário com base na política de autorização que ele correspondeu no

conjunto de políticas usado.

dACLs por usuário

Etapa 1. Definir um Atributo de Usuário Personalizado dACL

Para poder atribuir um dACL a uma identidade de usuário, primeiro esse campo deve ser configurável na identidade criada. Por padrão, no ISE, o campo "ACL" não é definido para nenhuma nova identidade criada. Para superar isso, é possível usar o "Atributo de usuário personalizado" e definir um novo campo de configuração. Para fazer isso, navegue até Administração > Gerenciamento de identidades > Configurações > Atributos personalizados do usuário. Use o botão "+"para adicionar um novo atributo semelhante ao mostrado. Neste exemplo, o nome do atributo personalizado é ACL.

≡ Cisco ISE		Administration · Identity M	lanagement		🔺 License Warning 🛛 🔾	\$ \$ \$
Identities Groups	External Identity Sources	Identity Source Sequences	Settings			
User Custom Attributes						${\rm All} \lor \nabla$
User Authentication Settings	Mandat Attrib	ute Name	Data Type			
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 Mandato	ory
	ACL		String ~	String Max length	+	B +
					Save	Reset

Depois de configurada, use o botão "Salvar" para salvar as alterações.

Etapa 2. Configurar o dACL

Navegue até Policy > Policy Elements > Results > Authorization > Downloadable ACLs para ver e definir o dACL no ISE. Use o botão "Adicionar" para criar um novo.

≡ Cisco ISE		Policy · Policy Elements		🔺 License Warning 🔍 ⊘ 🔎	
Dictionaries C	Conditions	Results			
Authentication	>	Dow	nloadable AC ↓	Ls	Selected 0 Total 7 🦪 🚳
Authorization Profiles		🖉 Edit	+ Add Duplicate	Delete	\sim γ
			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		

Isso abre o formulário de configuração "Nova ACL para download". Neste, configure estes campos:

- Nome: o nome do dACL definido.
- Descrição (opcional): uma breve descrição sobre o uso do dACL criado.
- Versão IP: a versão do protocolo IP usada no dACL definido (versão 4, 6 ou ambos).
- Conteúdo da DACL: o conteúdo da dACL, conforme a sintaxe da ACL do Cisco IOS XE.

Neste documento, o dACL usado é "ACL_USER1" e este dACL permite qualquer tráfego, exceto aquele destinado a 10.48.39.186 e 10.48.39.13.

Depois que os campos estiverem configurados, use o botão "Submit" (Enviar) para criar o dACL.

Repita a etapa para definir o dACL para o segundo usuário, ACL_USER2, como mostrado na figura.

■ Cisco ISE		Policy · Policy Elements			🔺 License Warning 🔍 ⊘ 💭 🐡	
Dictionaries Condit	ions	Results				
Authentication	ation Downloadable ACLs					
Authorization	~				Selected 0 Total 8 🧭 🏟	
Downloadable ACLs		/ Edit	+ Add Duplicate Delete	0	All \sim γ	
			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	Denv. all. iov6. traffic Denv. all. iov6 traffic Denv. all.iov6 traffic		
			PERMIT_ALL_IPV4_TRAFFIC	Allow all ipv4 Traffic		
			PERMIT_ALL_IPV6_TRAFFIC	Allow all ipv6 Traffic		
			test-dacl-cwa			
			test-dacl-dot1x			

Etapa 3. Atribuir o dACL a uma identidade criada

Depois que o dACL é criado, é possível atribuí-lo a qualquer identidade do ISE usando os atributos personalizados do usuário criados na etapa 1. Para fazer isso, navegue até Administração > Gerenciamento de identidades > Identidades > Usuários. Como de costume, use o botão "Adicionar" para criar um usuário.

■ Cisco ISE		Administration · Identity N	lanagement	🔺 License W	iarning Q 💮 🕫 🐡
Identities Groups	External Identity Sources	Identity Source Sequences	Settings		
Users Latest Manual Network Scan Res	Network Ac	cess Users			
	C Edit + Add	्रे Change Status \vee 🕁 Import	🛧 Export \vee 🛛 🚦 Delete	∨ ID Duplicate	Selected 0 Total 1 💭 🌚
	Status	Username \wedge Description	First Name Last Name	Network Access User Identity Groups	Admin
	Disabled	2 adminuser		admin-group	

No formulário de configuração "Novo usuário de acesso à rede", defina o nome de usuário e a senha para o usuário criado. Use o atributo personalizado "ACL" para atribuir o dACL criado na

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	Network Access Users Elist > USER1		
	✓ Network Access User		
	* Username USER1		
	Status 🖉 Enabled 🛩		
	Account Name Alias		
	Email		
	V Passwords		
	Password type: menna overs		
	Password Lifetime:		
	Password will expire in 53 days O Never Expires ①		
	Password Re-Enter Password		
	* Login Password	Generate Password	
	Enable Password	Generate Password	
	> User Information		
	> Account Ontions		
	Account Disable Policy		
	V Liser Oustern Attributes		
	· User Custom Attributes	-	
	ACL * ACL_USER1		
	V User Grouns		
	🗄 Select an item 🗸 💿 🛑		
			Save

Etapa 2 à identidade. No exemplo, a identidade USER1 usando ACL_USER1 é definida.

Quando os campos estiverem configurados corretamente, use o botão "Enviar" para criar a identidade.

Repita esta etapa para criar USER2 e atribuir ACL_USER2 a ele.

E Cisco ISE	E Cisco ISE Administration - Identity Management							
Identities Groups Ext	Identities Groups External Identity Sources Identity Source Sequences Settings							
Users	Network Access Users							
Latest Manual Network Scan Res		Selected 0 Total 3 🦪 🍈						
	Ø 681 + Add 🛞 Charge Status ∨ 👍 Japan 🕁 Egent ∨ 🚦 Danista	AL V V						
	Status Username -> Description First Name Last Name Email Address User Identity Groups Admin							
	© Disabled 1 adminuser admin-group							
	B Enabled 1 USER1							
	Exabled 1 USER2							
	Network Access Users							

Etapa 4. Configurar resultado da política de autorização.

Depois que a identidade for configurada e o dACL atribuído a ela, a política de autorização ainda deverá ser configurada para corresponder ao atributo de usuário personalizado "ACL" definido para uma tarefa comum de autorização existente. Para fazer isso, navegue até Política > Elementos de política > Resultados > Autorização > Perfis de autorização. Use o botão "Adicionar" para definir uma nova política de autorização.

- Nome: o nome da política de autorização, aqui "9800-DOT1X-USERS".
- Tipo de acesso: o tipo de acesso usado quando esta política é correspondida, aqui ACCESS_ACCEPT.
- Tarefa comum: associe "DACL Name" a InternalUser:<name of custom attribute created> para usuário interno.De acordo com os nomes usados neste documento, o perfil 9800-DOT1X-USERS é configurado com o dACL configurado como InternalUser:ACL.

E Cisco ISE	Policy - Policy Elements				
Dictionaries Conditions	Results				
Authentication >	Authorization Profiles > New Authorization Profile				
Authorization \sim	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 🚓 Cisco 🗸 😑				
	Service Template				
	Track Movement				
	Agentiess Posture				
	Passive Identity Tracking 🗋 🕕				
	Common Tasks				
	DACL Name InternalUser:ACL				
	IPv6 DACL Name				
	ACL (Filter-ID)				
	(7) S.R. 10. P. Phys. 103				

Etapa 5. Usar perfil de autorização no conjunto de políticas.

Depois que o resultado do perfil de autorização for definido corretamente, ele ainda precisará fazer parte do conjunto de políticas usado para autenticar e autorizar usuários sem fio. Navegue para Política > Conjuntos de políticas e abra o conjunto de políticas usado.

Aqui, a regra de política de autenticação "Dot1X" corresponde a qualquer conexão feita via 802.1x com ou sem fio. A regra de política de autorização "802.1x Users dACL" implementa uma condição no SSID usado (isto é, Radius-Called-Station-ID CONTAINS DACL_DOT1X_SSID). Se uma autorização for executada na WLAN "DACL_DOT1X_SSID", o perfil "9800-DOT1X-USERS" definido na Etapa 4 será usado para autorizar o usuário.

		Policy · Policy Sets			A License Warning	Q (0)	,a
olicy Sets→	Default			Reset	Reset Policyset Hitcounts		Save
Status P	Policy Set Name	Description Conditions			Allowed Protocols / Serve	r Sequer	ice
© Search	Default	Default policy set			Default Network Access	<u> </u>	+ 3
✓ Authentication	on Policy (2)						
+ Status	Rule Name	Conditions		Use		Hits	Actio
Q Search	h						
		Wired_802.1X		All_Us	er_ID_Stores 🛛 🛛 🗸		
0	Dot1X	OR Wireless_802.1X		> Opt	ions	65	{ĝ}
				All_Us	er_ID_Stores 🛛 🛇 🗸		
۲	Default			> Opt	ions	10	(2)
> Authorization	n Policy - Local Exceptions						
> Authorization	Policy - Global Exception	5					
 Autionzation 	Policy (2)		Results				
🕣 Status	Rule Name	Conditions	Profiles	Security	Groups	Hits	Actio
Q Search	h						
	202 to Hears dACI	Radius-Called-Station-ID CONTAINS DACL DOT1X SSID	9800-DOT1X-USERS ×	Select	from list ~+	65	{ô}
	DOZ.TX OSETS DAGE						-4-

dACLs por resultado

Para evitar a enorme tarefa de atribuir um dACL específico a cada identidade criada no ISE, pode-se optar por aplicar o dACL a um resultado de política específico. Esse resultado é então aplicado com base em qualquer condição correspondida nas regras de autorização do conjunto de políticas usado.

Etapa 1. Configurar o dACL

Execute a mesma Etapa 2 da <u>seção dACLs por usuário</u> para definir os dACLs necessários. Aqui, eles são ACL_USER1 e ACL_USER2.

Etapa 2. Criar identidades

Navegue até Administração > Gerenciamento de identidades > Identidades > Usuários e use o botão "Adicionar" para criar um usuário.



No formulário de configuração "Novo usuário de acesso à rede", defina o nome de usuário e a senha para o usuário criado.

≡ Cisco ISE		Administration - Identity Management	🔺 Likanse Warring 🔍 🕥 💯 🔅
Identities Groups Ext	ernal Identity Sources Identity Source Sequences Settings		
Users Latest Manual Network Scan Res	Network Access Users Litz: > New Network Access User		
	V Network Access User		
	* Usemame USER1		
	Status 📴 Enabled 🗸		
	Account Name Allas		
	Ernal		
	✓ Passwords		
	Password Type: Internel Users 🗸		
	Dannanet i Perima		
	With Expiration ()		
	Never Expines ①		
	Password Re-Enter Password		
	* Login Password	Generate Password	
	Enoble Password	Generate Password	
	> User Information		
	> Account Options		
	> Account Disable Policy		
	> User Custom Attributes		
	> User Groups		
			Submit
			Submit

Repita esta etapa para criar USER2.

E Cisco ISE	Administration - Identity Management	🔺 Ucerse Rummy C, O 52 @
Identities Groups	xternal Identity Sources Identity Source Sequences Settings	
Users Latest Manual Network Scan Res	Network Access Users	
		Selected O Total 3 🛛 🔕
	/ EAL + Add 🛞 Change Bollan 🗸 do legent 🛆 Edgent 🗸 🗍 Delate 🗸 🔘 Deplace	м ~
	Status Username A Description First Name Last Name Email Address User Identity Groups Admin	
	Ossibel 1 edinineser admin-group	
	Network Access Users	

Etapa 4. Configurar o resultado da política de autorização.

Depois que a identidade e o dACL forem configurados, a política de autorização ainda deverá ser configurada para atribuir um determinado dACL ao usuário que corresponder à condição para usar essa política. Para fazer isso, navegue até Política > Elementos de política > Resultados > Autorização > Perfis de autorização. Use o botão "Adicionar" para definir uma nova política de autorização e preencher esses campos.

- Nome: o nome da política de autorização, aqui "9800-DOT1X-USER1".
- Tipo de acesso: o tipo de acesso usado quando esta política é correspondida, aqui ACCESS_ACCEPT.
- Tarefa comum: associar "DACL Name" a "ACL_USER1" para o usuário interno. De acordo com os nomes usados neste documento, o perfil 9800-DOT1X-USER1 está configurado com o dACL configurado como "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

Repita esta etapa para criar o resultado da política "9800-DOT1X-USER2" e atribuir "ACL_USER2" como DACL a ele.

Clsco ISE		Polic	y - Policy Elements A License Remay Q	0 53
Dictionaries Conditions	Results			
Authoritation >	Standard Authorization Prof	iles		
Authorization \sim	For Policy Expert ge to Administration > System > Backup & F	Restore > Policy Export Page		
Authorization Profiles			Selected 0 Tatal	13 🧭 🍕
Development Acca	🖉 EAR 🕂 ADD 🗍 Displayers 🛞 Delete			мү 7
Profiling >	Neme	Profile	∧ Description	
Pasture	9800-0011X-USDN	m Cisco 🕕		
Cont Development .	9800-0011X-03592	# Cisco 🕡		
contributing /	9000-DOTIX-USERS	# Ciaco 🕜	Authorization profile for 802.1x 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	
	Cisco_JP_Phones	# Cisco 🕥	Default profile used for Disco Phones.	
	Cisco_Temporal_Onboard	tt Cisco 🕕	Onboard the dovice with Gisco temporal agent	
	Choo_WebJach	AL Cisco 🕧	Default Profile used to redirect users to the CMMA portal.	
	Internal OverAtt/Date Test	# Ciaco 🕕		
	DISP_Onboard	m Cisco 🕕	Oriboard the dorkse with Nativo Supplicant Provisioning	
	Non_Cisco_IP_Promes	📇 Cisco 🕧	Default Profile used for Non Cisco Phones.	
	UDN	# Cisco 🕠	Default profile used for UDN.	
	DenyAccess		Default Profile with access type as Access-Reject	
	Permithecess		Default Profile with access type as Access-Accept	

Etapa 5. Usar perfis de autorização no conjunto de políticas.

Depois que o perfil de autorização for definido corretamente, ele ainda precisará fazer parte do conjunto de políticas usado para autenticar e autorizar usuários sem fio. Navegue para Política > Conjuntos de políticas e abra o conjunto de políticas usado.

Aqui, a regra de política de autenticação "Dot1X" corresponde a qualquer conexão feita via 802.1X com ou sem fio. A regra de política de autorização "802.1X Usuário 1 dACL" implementa

uma condição no nome de usuário usado (ou seja, InternalUser-Name CONTAINS USER1). Se uma autorização for executada usando o nome de usuário USER1, o perfil "9800-DOT1X-USER1" definido na Etapa 4 será usado para autorizar o usuário e, portanto, o dACL desse resultado (ACL_USER1) também será aplicado ao usuário. O mesmo é configurado para o nome de usuário USER2, para o qual "9800-DOT1X-USER1" é usado.

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	{

Observações sobre o uso de dACLs com SSIDs do CWA

Conforme descrito no guia de configuração <u>Configurar a autenticação da Web central (CWA) no</u> <u>Catalyst 9800 WLC e ISE</u>, o CWA depende do MAB e de resultados específicos para autenticar e autorizar usuários. As ACLs para download podem ser adicionadas à configuração do CWA do lado do ISE de forma idêntica à descrita acima.



Aviso: ACLs para download podem ser usadas apenas como lista de acesso de rede e não são suportadas como ACLs de pré-autenticação. Portanto, qualquer ACL de pré-autenticação usada em um fluxo de trabalho do CWA deve ser definida na configuração da WLC.

Verificar

Para verificar a configuração feita, esses comandos podem ser usados.

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 }
```

Aqui é feita referência à parte relevante da configuração da WLC correspondente a este exemplo.

```
aaa new-model
!
Т
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
I
T
aaa server radius dynamic-author
client <ISE IP>
!
aaa session-id common
1
[...]
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
!
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
[\ldots]
wlan DACL_DOT1X_SSID 2 DACL_DOT1X_SSID
 security dot1x authentication-list DOT1X
 no shutdown
```

A configuração do servidor RADIUS é apresentada, exibida com o comando 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

Troubleshooting

Lista de verificação

- Verifique se os clientes podem se conectar corretamente ao SSID 802.1X configurado.
- Certifique-se de que a solicitação de acesso/aceitação do RADIUS contenha os pares atributo-valor apropriados (AVPs).
- Certifique-se de que os clientes usem o perfil de WLAN/política apropriado.

Reflexo de One Stop-Shop da WLC

Client Username : USER1

Para verificar se o dACL está atribuído corretamente a um cliente sem fio específico, é possível usar o comando **show wireless client mac**address <H.H.H> detail como mostrado. A partir daí, diferentes informações úteis de solução de problemas podem ser vistas, ou seja: o nome de usuário do cliente, o estado, o perfil de política, a WLAN e, mais importante aqui, o 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
[...]
```

Comandos show da WLC

Para ver todas as ACLs que atualmente fazem parte da configuração da WLC do Catalyst 9800, você pode usar o comando **show access-lists**. Esse comando lista todas as ACLs definidas localmente ou dACLs baixadas pela WLC. Qualquer dACL baixado do ISE pelo WLC tem o formato xACSACLx-IP-<ACL_NAME>-<ACL_HASH>.



Observação: as ACLs para download permanecem na configuração enquanto um cliente estiver associado e o utiliza na infraestrutura sem fio. Assim que o último cliente que usa o dACL deixa a infraestrutura, o dACL é removido da configuração.

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
[...]
```

Depuração condicional e rastreamento radioativo

Durante a solução de problemas de configuração, você pode coletar <u>rastreamentos radioativos</u> para um cliente que deve ser atribuído com o dACL definido. Aqui estão destacados os registros mostrando a parte interessante dos traços radioativos durante o processo de associação de cliente para o cliente 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 10:43:04.353443674 {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

Captura do pacote

Outro reflexo interessante é capturar e analisar capturas de pacotes do fluxo RADIUS para uma associação de cliente. As ACLs para download dependem do RADIUS, não apenas para serem atribuídas a um cliente sem fio, mas também para serem baixadas pela WLC. Ao fazer a captura de pacotes para solucionar problemas de configuração de dACLs, você deve, portanto, capturar na interface usada pelo controlador para se comunicar com o servidor RADIUS. Este documento mostra como configurar a captura de pacotes facilmente incorporados no Catalyst 9800, que foram usados para coletar a captura analisada neste artigo.

Autenticação de cliente RADIUS

Você pode ver a solicitação de acesso RADIUS do cliente enviada do WLC para o servidor RADIUS para autenticar o usuário USER1 (AVP User-Name) no SSID DACL_DOT1X_SSID (AVP NAS-Identifier).



Quando a autenticação é bem-sucedida, o servidor RADIUS responde com um access-accept, ainda para o usuário USER1 (AVP User-Name) e aplicando os atributos AAA, em particular o ACS AVP específico do fornecedor: CiscoSecure-Defined-ACL estar aqui "#ACSACL#-IP-ACL_USER1-65e89aab".



Download de DACL

Se o dACL já faz parte da configuração da WLC, ele é simplesmente atribuído ao usuário e a sessão RADIUS termina. Caso contrário, a WLC fará o download da ACL, ainda usando o RADIUS. Para fazer isso, a WLC faz uma solicitação de acesso RADIUS, desta vez usando o nome dACL ("#ACSACL#-IP-ACL_USER1-65e89aab") para o Nome de Usuário do AVP. Junto com isso, a WLC informa ao servidor RADIUS que esse access-accept inicia um download de ACL usando o par Cisco AV aaa:event=acl-download.



A aceitação de acesso RADIUS enviada de volta ao controlador contém o dACL solicitado, como mostrado. Cada regra de ACL está contida dentro de um AVP Cisco diferente do tipo "ip:inacl#<X>=<ACL_RULE>", <X> sendo o número da regra.

					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, Sr	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	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	dius). 323 bytes		- Parkar	ts: 43372 - Displayed: 2 (0.0%)	Profile: Default
	the second se				and the second sec	Provide: Delagan



Observação: se o conteúdo de uma ACL de download for modificado depois de ter sido baixado na WLC, a alteração para essa ACL não será refletida até que um usuário usando essa ACL reautentique (e a WLC execute uma autenticação RADIUS para esse usuário novamente). De fato, uma alteração na ACL é refletida por uma alteração na parte de hash do nome da ACL. Portanto, na próxima vez que essa ACL for atribuída a um usuário, seu nome deverá ser diferente e, portanto, a ACL não deverá fazer parte da configuração da WLC e deverá ser baixada. No entanto, os clientes que se autenticam antes da alteração na ACL continuam a usar o anterior até que se reautentiquem completamente.

Logs de operação do ISE

Autenticação de cliente RADIUS

Os registros de operação mostram uma autenticação bem-sucedida do usuário "USER1", ao qual a ACL "ACL_USER1" que pode ser baixada é aplicada. As partes de interesse para solução de problemas estão em vermelho.

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=8227300A0000000B48ABE3F, method=dot1x, client-id=2113931001, vlan-id=1433, clisco-wlan-ssid=DACL_DOT1X_SSID, wlan-profile-name=DACL_DOT1X_SSID, AuthenticationIdentifyStore=Internal Users, FQSubjectName=927a630-8c01-116e-996c- S25400b48521Nuser1, UniqueSubjectID=94b3604f5b49b88ccfafe2f3a86c80d1979b Sc43
Result	

Class	CACS:8227300A000000D848ABE3F:ise/499610885/35
EAP-Key-Name	19:66:05:40:45:8d:a0:0b:35:b3:a4:1b:ab:87:b8:72:94:16:a3:b 9:93:27:37:29:6b:c5:88:e3:b1:40:23:0a:b3:96:67:85:82:04:0a:c 5:c5:05:d6:57:5b:11:24:62:d3:6b:e0:19:cf:46:a4:29:f0:ba:65:0 6:9c:ef:3e:9f: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 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

Download de DACL

Os registros de operação mostram um download bem-sucedido da ACL "ACL_USER1". As partes de interesse para solução de problemas estão em vermelho.

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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.