# Configuración de la autenticación externa RADIUS en DNA Center e ISE 3.1

# Contenido

ntroducción	
Prerequisites	
Requirements	
Componentes Utilizados	
Configurar	
/erificación	
<u>lás funciones</u>	

# Introducción

Este documento describe cómo configurar la autenticación externa RADIUS en Cisco DNA Center mediante un servidor Cisco ISE que ejecute la versión 3.1.

# Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

 Cisco DNA Center y Cisco ISE ya están integrados y la integración se encuentra en estado activo.

### **Componentes Utilizados**

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco DNA Center 2.3.5.x Release.
- Cisco ISE versión 3.1.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

# Configurar

Paso 1. Inicie sesión en la GUI de Cisco DNA Center y navegue hastaSystem > Settings >

Authentication and Policy Servers.

Verifique que el protocolo RADIUS esté configurado y que el estado de ISE sea Activo para el servidor de tipo de ISE.

Settings / External Services

#### Authentication and Policy Servers

Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

⊕ Add ∨ ⊥ Export				As of: Jul 19, 2023 4:38 PM 🛛 🧭
IP Address	Protocol	Туре	Status	Actions
	RADIUS_TACACS	AAA	ACTIVE	
52 (MPR) /	RADIUS	ISE	ACTIVE	
A second of the second se	RADIUS	AAA	ACTIVE	
10 C 10 C 10 C	RADIUS	AAA	ACTIVE	
	RADIUS_TACACS	AAA	ACTIVE	



Nota: El tipo de protocolo RADIUS\_TACACS funciona para este documento.



Advertencia: en caso de que el servidor ISE no esté en estado activo, primero debe corregir la integración.

Paso 2. En ISE Server, navegue hasta Administration > Network Resources > Network Devices, haga clic en el icono Filter, escriba la dirección IP de Cisco DNA Center y confirme si existe una entrada. Si es así, vaya al paso 3.

Si falta la entrada, debe ver el mensaje No hay datos disponibles.

#### Network Devices

										Selected 0 Total 0	C 🕸
🖉 Edit	$+ \operatorname{Add}$	C	) Duplicate	Import ريلي	📤 Export 🖂	Generate PAC	📋 Delete	$\sim$		Quick Filter	~ 7
	Name	^	IP/Mask	Profile N	lame	Location		Туре	Descripti	on	
			x.x.x.x	_							
No data	available										

En este caso, debe crear un dispositivo de red para Cisco DNA Center, así que haga clic en el botón Add.

Network Devi	ices						
						Selected 0 Total 0	9 Ø
🖉 Edit 🕂 Add 🗓 Du	iplicate 🕁 Import 🏦	Export 🖂 🔒 Generate PAG	Delete 🗸			Quick Filter $\vee$	V
Name $\land$ IP	P/Mask	Profile Name	Location	Туре	Description		
x							
No data available							

Configure el nombre, la descripción y la dirección IP (o direcciones) desde Cisco DNA Center; el resto de las configuraciones se establecen en los valores predeterminados y no son necesarias para los fines de este documento.

Network Devices List > New Network Device

## Network Devices

<ul> <li>Name</li> </ul>	mxc-dna	ic5			
Description	Cisco DN	A Cente	1		
IP Ad	dress 🗸 * IP :	-		/32	ŵ•
Device Profile	tta Cisco	<b>∨</b> ⊕			
Model Name		~			
Software Versio	n	~			
* Network De	vice Group				
Location	All Locations	$\mathbf{v}$	Set To (	Default	
IPSEC	Is IPSEC Device	~	Set To [	Default	
Device Type	All Device Types	~	Set To I	Default	

Desplácese hacia abajo y habilite RADIUS Authentication Settings haciendo clic en su casilla de verificación y configure un Shared Secret.



RADIUS UDP Settings





Sugerencia: este secreto compartido se necesitará más adelante, así que guárdelo en otro lugar.

Solo entonces, haga clic en Submit.

Paso 3. En el servidor ISE, vaya a Policy > Policy Elements > Results, para crear el perfil de autorización.

Asegúrese de que se encuentra en Authorization > Authorization Profiles, luego seleccione la opción Add.

E Cisco ISE				Policy · Policy Eler	ments		1 Q Ø	Ø 0
Dictionaries Condition	ns Res	sults						
Authentication Allowed Protocols	~	Stan For Policy E	dard Authoriza xport go to Administration > System > B	tion Profiles ackup & Restore > Policy Export Page				~ *
Authorization	× A	/ Edit	+ Add Duplicate	Dolete			Selected 0 Total 20	"~ γ
Downloadable ACLs			Name	Profile	^	Description		
			APs_19.5.0	🗯 Cisco 🕕		172_19_5_0-INFRA_VN		
Profiling	>		AuthTemplate	🗰 Cisco 🕕				
Posture	>		Blackhole_Wireless_Access	🗯 Cisco 🕕		Default profile used to blacklist wireless devices. Ensure that yo	u configure a BLACKHOLE AC	3L on the
Client Provisioning	>		CY_CAMPUS_MAC	🗮 Cisco 🕕		CY_CAMPUS_MAC		
	1		CV Quest profile	the Circos		CV Quart profile		

Configure Name, agregue una Description sólo para mantener un registro del nuevo perfil y asegúrese de que el Access Type esté configurado en ACCES\_ACCEPT.

Results	
Authorization Profiles > Ne	w Authorization Profile
Authorization Prom	e
* Name	DNAC_AUTH_PROFILE
Description	External Authentication for Cisco DNA Center
* Access Type	ACCESS_ACCEPT ~
Network Device Profile	tic Cisco ∨⊕
Service Template	
Track Movement	
Agentless Posture	
Passive Identity Tracking	

Desplácese hacia abajo y configure Advanced Attributes Settings (Parámetros de atributos avanzados).

En la columna izquierda, busque la opción cisco-av-pair y selecciónela.

En la columna derecha, escriba manualmente Role=SUPER-ADMIN-ROLE.

Una vez que se parezca a la imagen de abajo, haga clic en Submit.

÷	Cisco:cisco-av-pair	~	=	Role=SUPER-ADMIN-ROLE	~	_	4
∕ Att	ributes Details						

Paso 4. En el servidor ISE, navegue hasta Centros de trabajo > Profiler > Conjuntos de políticas, para configurar la política de autenticación y autorización.

Identifique la política Default y haga clic en la flecha azul para configurarla.

≡	Cisco	ISE		Work Cer	nters • Profi	iler			0	Q (2)	P	⊚
Over	view	Ext Id Sources	Network Devices	Endpoint Classif	ication	Node Config	Feeds	Manual Scans	More	• ~		
Poli	cy Sets						Reset	Reset Policyset	Hitcounts		Save	
0	Status	s Policy Set Name	Description	Con	ditions	Alle	owed Protocols	s / Server Sequen	ce Hits	Actions	vie	w
(	Q Searc	ch										)
	$\otimes$	Wire-dot1x		=	Wired_802.1	IX intern	al_user	<u> </u>	0	£Ç}	>	
	$\otimes$	МАВ		=	Wired_MAB	Defau	It Network Acc	ess $\propto$ $\sim$ +	0	ŝ	>	
	0	Default	Default policy s	et		Defau	It Network Acc	ess 🛛 🗸 +	180517	ŝ	>	]
									Reset		Save	

Dentro del Conjunto de políticas predeterminadas, expanda la Política de autenticación y en la sección Predeterminado, expanda las Opciones y asegúrese de que coincidan con la siguiente configuración.

Overview       Ext ld Sources       Network Devices       Endpoint Classification       Node Config       Feeds       Manual Scans       Policy Elements       Profiling Policies       More         Policy Sets-+       Default       Reset	≡ 0	Cisco IS	E				Work Centers •	Profiler			Q	Q (	) ,a ¢
Policy Sets-> Default     Reset     Reset Policyset Hitcourts     Same       Status     Policy Set Name     Description     Conditions     Allowed Protocols / Server Sequence     H       Image: Search     Image: Search     Image: Search     Image: Search     Image: Search       Image: Status     Rote Name     Conditions     Use     Hits     Action       Image: Status     Rote Name     Conditions     Image: Status     Image: Status <td< th=""><th>Overvie</th><th>ew E</th><th>xt Id Sources</th><th>Network Devic</th><th>es Endp</th><th>oint Classification</th><th>Node Config</th><th>Feeds</th><th>Manual Scans</th><th>Policy Elements</th><th>Profiling Policies</th><th>More ~</th><th></th></td<>	Overvie	ew E	xt Id Sources	Network Devic	es Endp	oint Classification	Node Config	Feeds	Manual Scans	Policy Elements	Profiling Policies	More ~	
Status       Policy Set Name       Description       Conditions       Allowed Protocols / Server Sequence       H <ul> <li>Status</li> <li>Default</li> <li>Default</li></ul>	Policy	Sets→	Default							Reset	Reset Policyset Hitcou	nts	Save
Q Search       Default Network Access Q ~ + 19887         ✓ Authentication Policy (3)       Use       Hits       Action         Q Search       Internal Endpoints       Q ~ + 19887         Image: Search       Image: Search       Image: Search       Image: Search         Image: Search       Image: Search       Image: Search       Image: Search       Image: Search         Image: Search       Image: Search       Image: Search       Image: Search       Image: Search       Image: Search         Image: Search       Image: Search       Image: Search       Image: Search       Image: Search <td< th=""><th>s</th><th>tatus P</th><th>olicy Set Name</th><th>Descrip</th><th>tion</th><th>Conditions</th><th></th><th></th><th></th><th></th><th>Allowed Protocols / Se</th><th>rver Seque</th><th>ence Hits</th></td<>	s	tatus P	olicy Set Name	Descrip	tion	Conditions					Allowed Protocols / Se	rver Seque	ence Hits
Default       Default policy set       Default policy (3)         Image: Status       Rule Name       Conditions       Use       Hits       Action         Image: Status       Rule Name       Image: Status       Rule Name       Image: Status       <	(0	Search											
✓ Authentication Policy (3)         ③ Status       Rule Name       Conditions       Use       Hits       Action         ④ Sarch       ● MAB       OR       ● Wired_MAB       ● Options       4556       @         ● MAB       OR       ● Wired_B02.1X       ● Options       0       @         ● Detaxt       OR       ● Wired_B02.1X       ● Options       0       @         ● Detaxt       OR       ● Wired_B02.1X       ● Options       0       @         ● Detaxt       OR       ● Wired_B02.1X       ● Options       0       @         ● Detaxt       OR       ● Wired_B02.1X       ● Options       0       @         ● Detaxt       OR       ● Wired_B02.1X       ● Options       0       @         ● Detaxt       OR       ● Wired_B02.1X       ● Options       0       @         ● Detaxt       OR       ● Wired_B02.1X       ● Options       0       @         ● Detaxt       ● REJECT       © Satis       © Options       %       @       @       @		0	Default	Default	policy set					D	efault Network Access	<u>a ~</u> +	180617
i Status       Rule Name       Conditions       Use       Hits       Action         Image: Search       Imag	∨ Aut	thenticatio	n Policy (3)										
Q Search       MAB       OR       Internal Endpoints       Internal Endpoin	Ð	Status	Rule Name	Con	ditions					Use		Hits	Actions
MAB       MAB       MAB       Internal Endpoints       MAB         Image: MAB       Internal Endpoints       Image: MAB       Image: MAB       Image: MAB         Image: MAB       Image: MAB       Image: MAB       Image: MAB       Image: MAB       Image: MAB         Image: MAB       Image: Mab       Ima       Ima       Ima	C	Q Search	1										
Image: MAB       OR       Image: MAB       > Options       4556       Image: MAB         Image: Detail       Det1X       OR       Image: Mired_802.1X       Im					Wired	MAB				Internal En	dpoints 🛛 🗸 🗸		
Image: Default       Default       Image: Nired_802.1X       All_User_ID_Stores (R) > Options       Image: Default		0	MAB	OR	E Wireles	ss_MAB				> Options	3	4556	錼
OR       Image: Second se					E Wired	802.1X				All_User_I	D_Stores 🛛 🗸		
Default       Image: Default     All_User_ID_Stores     Image: Default       Image: Default     Image: Default     Image: Default       Image: Default     Image: Default     Image: Default		0	Dot1X	OR	E Wireles	ss_802.1X				> Options	6	0	錼
Default     D										All_User_II	D_Stores 🛛 🗸		
Default										✓ Options	3		
Default      Default      If User not found      REJECT      If Process fail      DROP      K      V										If Auth fa	ii T 🛛 🐼 🗸		
If Process fail		0	Default							If User no	ot found T 🛛 🙁 🗸	62816	¢
										If Process	s fail 🛛 🛛 🛛		



Sugerencia: el RECHAZO configurado en las 3 opciones también funciona

Dentro del Conjunto de directivas predeterminado, expanda la Directiva de autorización y seleccione el icono Agregar para crear una nueva Condición de autorización.

≡ Cisco	ISE			Work Centers - F	Profiler			C	Q (0	) ja (j
Overview	Ext Id Sources	Network Devices	Endpoint Classification	Node Config	Feeds	Manual Scans	Policy Elements	Profiling Policies	More ~	
Policy Sets	→ Default						Reset	Reset Policyset Hitcou	nts	Save
Status	Policy Set Name	Description	Conditions					Allowed Protocols / Se	rver Seque	nce Hits
Q Sear	ch									
٢	Default	Default policy	set					Default Network Access	<u>a</u> ~+	180617
> Authentic	ation Policy (3)									
> Authoriza	tion Policy - Local Ex	ceptions								
> Authorizat	tion Policy - Global E	xceptions								
$\sim$ Authorizat	tion Policy (25)									
					Result	s				
🕒 Stat	tus Rule Name	Conditions	1		Profile	15	Security	Groups	Hits	Actions
Q Sea	arch									

Configure un nombre de regla y haga clic en el icono Add (Agregar) para configurar la condición.

≡	Cisco	ISE			Work Centers - I	Profiler				1 Q	0 7	0 ©
Overv	riew	Ext Id Sources	Network Devices	Endpoint Classification	Node Config	Feeds	Manual Scans	Policy Elements	Profiling Policies	More	~	
Polic	y Sets-	→ Default						Reset	Reset Policyset Hitco	ounts	Sav	ve
	Status	Policy Set Name	Description	Conditions					Allowed Protocols / S	Gerver Sequ	ience	Hits
0	Q Sear	ch										$\supset$
	ø	Default	Default policy	set				_	Default Network Access	<u>a</u> ~+	180	617
> A	uthentica	ation Policy (3)										
> A	uthorizat	tion Policy - Local Exc	eptions									
> A	uthorizat	tion Policy - Global Ex	ceptions									
~ A	uthorizat	tion Policy (26)										
						Results						
e	Stat	us Rule Name	Conditions	1		Profiles		Security	Groups	Hits	Acti	ons
(	Q Sea	arch										)
	0	DNAC-SUPER-ADM	MIN-ROLE	*		Select from	list	~+ Select fro	om list 🗸 🗸		\$	}

Como parte de la Condición, asóciela a la Dirección IP del Dispositivo de Red configurada en el Paso 2.

## Conditions Studio

Search by Name     Image: Search by Nam     Image: Search by Name </th <th>Library</th> <th>Editor</th> <th></th> <th></th> <th></th> <th>0</th>	Library	Editor				0
Image: Contract of the set of the s	Search by Name		Network Access Device IP Addr	ress		
Image: BYOD_is_Registered   Image: Catalyst_Switch_Local_Web_Aut   Image: Catalyst_Switch_Local_Web_Aut   Image: Compliance_Unknown_Devices   Image: Compliant_Devices   Image: Compliantert </th <th></th> <th>₽</th> <th>Equals ~ 10.88.2</th> <th>44.151</th> <th></th> <th></th>		₽	Equals ~ 10.88.2	44.151		
III III   III III   III IIII   IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	:: E BYOD_is_Registered		Set to 'Is not'		Duplicate	Save
III III   III III   III IIII   IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	:: E Catalyst_Switch_Local_Web_Aut		NE	W AND OR		
III IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	:: E Compliance_Unknown_Devices					
III	:: E Compliant_Devices					
III III CY_CAMPUS_MAC   III III CY_Campus_voice   III III CY_Guest   III III CY_GUEST <th>: E CY_Campus</th> <th></th> <th></th> <th></th> <th></th> <th></th>	: E CY_Campus					
Image: CY_Campus_voice   Image: CY_Guest   Image: Comparison   Image: CY_Guest   Image: Comparison   Image: Comparison   Image: Comparison	E CY_CAMPUS_MAC					
Image: CY_Guest   Image: EAP-MSCHAPv2   Image: Close   Image: Close   Use	:: E CY_Campus_voice					
E EAP-MSCHAPv2 () Close Use	: E CY_Guest					
Close Use	EAP-MSCHAPv2					
Close Use	"					
					Close	Use

Haga clic en Guardar.

Guárdelo como una nueva Condición de Biblioteca, y nombrelo como desee, en este caso se nombra comoDNAC.

# Save condition

O Save as existing Library Condition (replaces current version and impact all policies that use this condition

×

Select from list		$\sim$
Save as a new Library Cor	dition	
DNAC	Description (optional) Condition Description	<i>"</i>
	Close	Save

### Por último, configure el perfil creado en el paso 3.

≡ Cisco	ISE			Work Centers - I	Profiler			0	9	
Overview	Ext Id Sources	Network Devices	Endpoint Classification	Node Config	Feeds	Manual Scans	Policy Elements	Profiling Policies	More	•
Policy Sets	→ Default						Reset	Reset Policyset Hitcount	ts	Save
Status	Policy Set Name	Description	Conditions					Allowed Protocols / Serv	ver Seque	nce Hits
Q Sear	ch									
٢	Default	Default policy	set					Default Network Access 🤇	<b>x</b> ~ +	180617
> Authentic	ation Policy (3)									
> Authorizat	tion Policy - Local Ex	ceptions								
> Authorizat	tion Policy - Global E	xceptions								
$\sim$ Authorizat	tion Policy (25)									
					Results					
🕂 Stat	tus Rule Name	Conditions			Profiles		Security	Groups	Hits	Actions
Q Sea	arch									
٩	DNAC-SUPER-AD	MIN-ROLE E DNAC			DNAC_AU	TH_PROFILE ×	✓ + Select from	m list $\sim$ +		<u>لې</u>

Haga clic en Guardar.

Paso 5. Inicie sesión en la GUI de Cisco DNA Center y navegue hastaSistema > Usuarios y funciones > Autenticación externa.

Haga clic en la opción Enable External User y establezca el atributo AAA como Cisco-AVPair.

#### ■ Cisco DNA Center

Jser Management		
-----------------	--	--

Role Based Access Control

External Authentication

#### **External Authentication**

Cisco DNA Center supports external servers for authentication and authorization of External Users.Use the fields in this window to create, update and on Cisco DNA Center is the name of the AAA attribute chosen on the AAA server. The default attribute expected is Cisco-AVPair, but if the user choo it needs to be configured here on Cisco DNA Center.

The value of the AAA attribute to be configured for authorization on AAA server would be in the format of "Role=role1". On ISE server, choose the cisc attributes list. A sample configuration inside Authorization profile would look like "cisco-av-pair= Role=SUPER-ADMIN-ROLE".

An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE".





Nota: El servidor ISE utiliza el atributo Cisco-AVPair en el servidor, por lo que la

configuración del paso 3 es válida.

Desplácese hacia abajo para ver la sección de configuración AAA Server(s). Configure la dirección IP del servidor ISE en el paso 1 y la clave secreta compartida configurada en el paso 3.

A continuación, haga clic en Ver configuración avanzada.

e.	Secondary A	AA Server
	V Address	
SHOW	Shared Secret	SHOW
Info		Info
	View Advanced S	ettings
	SHOW	SHOW Info

Compruebe que la opción RADIUS esté seleccionada y haga clic en el botón Update (Actualizar) en ambos servidores.

AAA Server(s)

Primary AAA Server	Secondary AAA Server			
IP Address		IP Address		
1 (1 (1 (1 (1 (1 (1 (1 (1 (1 (1 (1 (1 (1	~	$(1,1,\ldots,n)$	1	
Shared Secret		Shared Secret		
	SHOW			SHOW
	Info			Info
Hide Advanced Settings		Hide Advanced	Settings	
O TACACS		O RADIUS	O TACACS	
Authentication Port		Authentication P	ort	
1812		1812		
Accounting Port		Accounting Port		
1813		1813		
Retries		Retries		
3		3		
Timeout (seconds)		Timeout (second	is)	
4		4		

Debe ver un mensaje de Confirmación para cada uno.



Ahora puede iniciar sesión con cualquier identidad de ISE creada en el menú de ISE > Administración > Gestión de identidad > Identidades > Usuarios.

En caso de que no haya creado ninguno, inicie sesión en ISE, navegue hasta la ruta anterior y agregue un nuevo usuario de acceso a la red.

Cisco ISE	Administration - Identity Management	0 0 59 4
Identities Groups	External Identity Sources Identity Source Sequences Settings	
Users Latest Manual Network Scan Res	Network Access Users	
	🖉 Edit 🕂 Add 🛞 Change Status 🗸 🕁 Import 🔿 Export 🗸 👩 Delete 🗸 🕦 Duplicate	Selected 0 Total 24 🧭 🚳

## Verificación

Cargar la GUI de Cisco DNA Center e inicie sesión con un usuario de las identidades de ISE.

	ılıılı cısco	
X YX XX XX XX YX XX	Cisco DNA Center The bridge to possible	
A NUMBER OF STREET	✓ Success!	
	Username test	
	Password	
	Log In	

Inicio de sesión en DNA Center



Nota: cualquier usuario con identidades ISE puede iniciar sesión ahora. Puede agregar más granularidad a las reglas de autenticación en el servidor ISE.

Una vez que el inicio de sesión se haya realizado correctamente, el nombre de usuario se muestra en la GUI del Cisco DNA Center



# Welcome, test

Pantalla de bienvenida

## Más funciones

Puede repetir estos pasos para cada rol en Cisco DNA Center, como opción predeterminada que tenemos: SUPER-ADMIN-ROLE, NETWORK-ADMIN-ROLE y OBSERVER-ROLE.



En este documento utilizamos el ejemplo de rol SUPER-ADMIN-ROLE; sin embargo, puede configurar un perfil de autorización en ISE para cada rol en Cisco DNA Center, la única consideración es que el rol configurado en el paso 3 debe coincidir exactamente (distingue entre mayúsculas y minúsculas) con el nombre del rol en Cisco DNA Center.

#### Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).