Configurer ISE en tant qu'authentification externe pour l'interface utilisateur DNAC

Table des matières

Introduction								
Conditions préalables								
Exigences								
Composants utilisés								
Avant de commencer								
Configurer								
(Option 1) Configurez l'authentification externe DNAC à l'aide de RADIUS								
(Option 1) Configuration d'ISE pour RADIUS								
(Option 2) Configurer l'authentification externe DNAC à l'aide de TACACS+								
(Option 2) Configuration d'ISE pour TACACS+								
Vérifier								
Vérification de la configuration RADIUS								
Vérification de la configuration TACACS+								
<u>Dépannage</u>								
Références								

Introduction

Ce document décrit comment configurer Cisco Identity Services Engine (ISE) en tant qu'authentification externe pour l'administration de l'interface utilisateur graphique de Cisco DNA Center.

Conditions préalables

Exigences

Cisco vous recommande d'avoir connaissance des sujets suivants :

- Protocoles TACACS+ et RADIUS.
- Intégration de Cisco ISE avec Cisco DNA Center.
- Évaluation de la politique Cisco ISE.

Composants utilisés

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

- Cisco Identity Services Engine (ISE) Version 3.4 Patch1.
- Cisco DNA Center version 2.3.5.5

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.

Avant de commencer

- Assurez-vous qu'au moins un serveur d'authentification RADIUS est configuré sur System > Settings > External Services > Authentication and Policy Servers.
- Seul un utilisateur avec des autorisations SUPER-ADMIN-ROLE sur DNAC peut effectuer cette procédure.
- Activez le fallback d'authentification externe.
- Mise en garde : Dans les versions antérieures à 2.1.x, lorsque l'authentification externe est activée, Cisco DNA Center revient aux utilisateurs locaux si le serveur AAA est inaccessible ou si le serveur AAA rejette un nom d'utilisateur inconnu. Dans la version actuelle, Cisco DNA Center ne reviendra pas aux utilisateurs locaux si le serveur AAA est inaccessible ou si le serveur AAA rejette un nom d'utilisateur inconnu. Lorsque le secours d'authentification externe est activé, les utilisateurs externes et les administrateurs locaux peuvent se connecter à Cisco DNA Center.

Pour activer la reprise d'authentification externe, établissez une connexion SSH avec l'instance Cisco DNA Center et entrez la commande this CLI (magctl rbac external_auth_fallback enable).

Configurer

(Option 1) Configurez l'authentification externe DNAC à l'aide de RADIUS

Étape 1. (Facultatif) Définissez des rôles personnalisés.

Configurez vos rôles personnalisés en fonction de vos besoins. Vous pouvez utiliser les rôles d'utilisateurs par défaut. Pour ce faire, accédez à l'onglet System > Users & Roles > Role Based Access Control.

Procédure

a. Créer un nouveau rôle.

Create a User Role

2

Create a New Role

Define the name of the role, and then provide an optional description. To make it easier to assign roles down the road, describe the role as clearly as possible.

]
_

Exit

Nom du rôle DevOps

b. Définissez l'accès.

≡ Cisco Di	NA Center				Create a User Role	Q @ & A				
De	efine the	Acce	SS							
0	These permissions enable different capabilities in Cisco DNA Center, some of which are inter-dependent. Before making the selections, please ensure you understand the details of what each of these X permissions allow. Click here to Learn More.									
Def a ro	fine the DevOps - ole is configured	-Role role with Deny 1	. Custom r permissic	oles permit or on, all related c	restrict user access to certain Cisco DNA Center functions. By default, roles are configured with Read permission, which is an Observer role. If ontent for that capability is removed from the GUI.					
	Access •	Permission			Description					
	> Assurance	O Deny	○ Read	O Write	Assure consistent service levels with complete visibility across all aspects of your network.					
	> Network Analytics	O Deny	Read	O Write	Access to Network Analytics related components.					
	> Network Design	O Deny	O Read	() Write	Set up network hierarchy, update your software image repository, and configure network profiles and settings for managing your sites and network devices.					
	> Network Provision	O Deny	O Read	O Write	Configure, upgrade, provision and manage your network devices.					
	> Network Services	O Deny	O Read	O Write	Configure additional capabilities on the network beyond basic network connectivity and access.					
	> Platform	O Deny	O Read	O Write	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.					
	> Security	O Deny	O Read	O Write	Manage and control secure access to the network.					
C						2				
Exit					Review Back	Next				

Accès au rôle DevOps

c. Créez le nouveau rôle.

■ Cisco DNA Center	Create a User Role	Q @ 4
Summary Review the DevOps-Role role. Make su	Ire all the details are as you expect them to be. If you need to change something, clicking edit will take you back to that section	
v Role Name & Description Edit		
Role Name DevOps-Role		
Role Description		
 Role Capability Edit 		
ASSURANCE		
Monitoring and Troubleshooting	Deny	
Monitoring Settings	Deny	
Troubleshooting Tools	Deny	
NETWORK ANALYTICS		
Data Access	Read	
NETWORK DESIGN		
Advanced Network Settings	Deny	
Image Repository	Deny	
Network Hierarchy	Deny	1
Network Profiles	Deny	
Network Settings	Deny	
Virtual Network	Dany	
- Exit	В	lack Create Role

Récapitulatif des rôles DevOps

■ Cisco DNA Center		Create a User Role	Q @ & A
Network Device	Deny		
Port Management	Deny		
Topology	Deny		
License	Deny		
Network Telemetry	Deny		
PnP	Deny		
Provision	Deny		
NETWORK SERVICES			
App Hosting	Deny		
Bonjour	Deny		
Stealthwatch	Deny		
Umbrella	Deny		
PLATFORM			
APIs	Write		
Bundles	Write		
Events	Write		
Reports	Write		
SECURITY			
Group-Based Policy	Deny		
IP Based Access Control	Deny		
Security Advisories	Deny		1
SYSTEM			
Machine Reasoning	Deny		1
Suntan Managament	Domi		
Exit		Back	Create Role

Vérifier et créer un rôle DevOps

Étape 2 : configuration de l'authentification externe à l'aide de RADIUS Pour ce faire, accédez à l'onglet System > Users & Roles > External Authentication.

Procédure

a. Pour activer l'authentification externe dans Cisco DNA Center, cochez la case Enable External User.

b. Définissez les attributs AAA.

Saisissez Cisco-AVPair dans le champ AAA attributes.

c. (Facultatif) Configurez les serveurs AAA principal et secondaire.

Assurez-vous que le protocole RADIUS est activé sur le serveur AAA principal au moins, ou sur les serveurs principal et secondaire.

E Cisco DNA Center		System / Users & Roles	Q @ C A
User Management Role Based Access Control External Authentication	External Authentication Cisco DNA Center supports external servers fr name of the AAA attribute chosen on the AAA The value of the AAA attribute to be configure configuration inside Authorization profile would An example configuration in the case of manu Enable External User	authentication and authorization of External Users. Use the fields in this window to create. erver: The default attribute expected is Cisco-AVPair, but if the user chooses to change it t for authorization on AAA server would be in the format of "Role-role1". On ISE server, choo look like "cisco-av-pair" Role-SUPER-ADMIN-ROLE" ly defining the AAA attribute would be "Cisco-AVPair+Role+SUPER-ADMIN-ROLE".	update and delete AAA Servers. The AAA Attribute here on Cisco DNA Center is the to any other AAA attribute, it needs to be configured here on Cisco DNA Center. see the cisco-av-pair attribute from cisco specific AAA attributes list. A sample
b	AAA Attribute: Cisco-AVPair Reset to Default Updat		
c	Primary AAA Server P Address ISE Server 1 IP Shared Secret ***** Infe Hide Advanced Settings O RADIUS O TACACS Authentication Port 1812	Secondary AAA Server P Address ISE Server 2 IP Shared Secret Info Hide Advanced Settings AADIUS O TACACS Authentication Port 1812	

Étapes de configuration de l'authentification externe (RADIUS)

(Option 1) Configuration d'ISE pour RADIUS

Étape 1 : ajout d'un serveur DNAC en tant que périphérique réseau sur ISE

Pour ce faire, accédez à l'onglet Administration > Network Resources > Network Devices.

- a. Définissez le nom et l'adresse IP du périphérique réseau (DNAC).
- b. (Facultatif) Classez le type de périphérique pour la condition Jeu de stratégies.
- c. Activez les paramètres d'authentification RADIUS.
- d. Définissez le secret partagé RADIUS.

≡	deale Identity Services I	Engine		Administration / Network Resources	Q	۵	0	۹ ۶
н	Bookmarks	Network Devices	Network De	evice Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences External MDM pxGrid Direct Connectors				
11 日 × 日 14 日 15 ①	Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Help	Network Device Default Device Device Security Setting	a	Interest Devices Name Description				
				Software Version Network Device Group Location All Locations Version Set To Default IPSEC No Version Set To Default				
			b	Device Type DNAC-Servers V Set To Default				
			с	ADIUS Authentication Settings RADIUS UOP Settings Pretocal RADIUS C Shared Secret Dus Second Shared Secret Secret				

Périphérique réseau ISE (DNAC) pour RADIUS

Étape 2 : création de profils d'autorisation RADIUS

Vous pouvez le faire à partir de l'onglet Stratégie > Éléments de stratégie > Résultats > Autorisation > Profils d'autorisation.

Nemarque : Créez trois profils d'autorisation RADIUS, un pour chaque rôle d'utilisateur.

Procédure

a. Cliquez sur Add et définissez le nom du profil d'autorisation RADIUS.

b. Saisissez la paire Cisco : cisco-av-dans les paramètres d'attributs avancés et remplissez le rôle d'utilisateur approprié.

- Pour le rôle d'utilisateur (DecOps-Role), entrez ROLE=DevOps-Role.
- Pour le rôle d'utilisateur (NETWORK-ADMIN-ROLE), entrez ROLE=NETWORK-ADMIN-ROLE.
- Pour le rôle d'utilisateur (SUPER-ADMIN-ROLE), entrez ROLE=SUPER-ADMIN-ROLE.
- c. Consultez les détails des attributs.
- d. Cliquez sur Save.

$\equiv rac{\mathrm{dede}}{\mathrm{dsc}}$ Identity Services	Engine	Policy / Policy Elements	
II Bookmarks 문전 Dashboard 년 Context Visibility 약 Operations II Policy 표 ₀ Administration	Dictionaries Conditions R Asthemication / Advect Protection Autorecidente Protection Downloadable ACLs Prefiling >	Authorization Profile a	
, Mork Centers	Plastare > Client Provisioning >	* Access Type ACCESS_ACCEPT Network Device Profile Casco Service Template Image: Casco Track Movement Image: Casco Agentiess Posture Image: Casco Passive Identity Tracking Image: Casco > Common Tasks	
		Advanced Attributes Settings b If Ciscocitsco-sv-pair * ROLE-DevOps-Rote + C * * * * * Attributes Details * * * Mexme Mget + KOSRA KOSP * * *	d Carcel

Créer un profil d'autorisation

Étape 3 : création d'un groupe d'utilisateurs

Pour ce faire, accédez à l'onglet Administration > Identity Management > Groups > User Identity Groups.

- a. Cliquez sur Add et définissez le nom du groupe d'identités
- b. (Facultatif) Définissez la description.
- c. Cliquez sur Envoyer.



Créer un groupe d'identités utilisateur

Étape 4 : création d'un utilisateur local

Pour ce faire, accédez à l'onglet Administration > Identity Management > Identities > Users.

- a. Cliquez sur Add et définissez le nom d'utilisateur.
- b. Définissez le mot de passe de connexion.
- c. Ajoutez l'utilisateur au groupe d'utilisateurs associé.
- d. Cliquez sur Submit.

=	dentity Services E	Engine			Administration / Identity Management	Q	۵ (D (9 S
н	Bookmarks	Identities	Groups	External	al Identity Sources Identity Source Sequences Settings				
15	Dashboard Context Visibility	Users Latest Manual Results	I Network Scan		Network Access Users List > New Network Access User				
×	Operations				V Network Access User				
0	Policy			a	a Username DerOps_User				
20	Administration				Status Enabled V				
-fil	Work Centers				Account Name Alias				
(?)	Interactive Help				tmai				
					Passwords Descent Tune Understitling				
					Descent Linitary				
					Vith Expiration ①				
					Password will expire in 60 days Never Expires ①				
					Plassword Re-Enter Plassword				
					* Login Password Generate Password				
					Enable Password O				
					~ User Information				
					First Name				
					Last Name				

Créer un utilisateur local 1-2

= -deade-	Identity Services E	Engine			Admini	istration / Identity Manageme	ent			, Q	۵	0	٥	A
III Bookm Bill Dashb Idi Context V Operating III Policy III Policy IIII Work C Interact	aarks ooard xt Viaibility tions istration Centers ctive Help	Users Latest Mara Results	Groups aal Network Scan	External Identity Sources	Identity Source Sequences	Settings ne-Cites reasonau	Generate Password	 ○ ○ 						
				 ✓ Account Disal Disable acco ✓ User Groups 	ble Policy unt if date exceeds 2025-03-20 C	(yyyy-mm-dd)			(d		Canc	cel	

Créer un utilisateur local 2-2

Étape 5. (Facultatif) Ajouter un jeu de stratégies RADIUS.

Pour ce faire, accédez à l'onglet Policy > Policy Sets.

Procédure

a. Cliquez sur Actions et choisissez (Insérer une nouvelle ligne ci-dessus).

b. Définissez le nom du jeu de stratégies.

c. Définissez la condition du jeu de stratégies sur Sélectionner le type de périphérique précédemment créé (Étape 1 > b).

- d. Définissez les protocoles autorisés.
- e. Cliquez sur Save.

f. Cliquez sur (>) Policy Set View pour configurer les règles d'authentification et d'autorisation.

=	disco Identity Services Engin	ne	Policy / Policy Sets	Q & @ Q A
Щ	Bookmarks	Status Policy Set Name	Description Conditions	Allowed Protocols / Server Sequence Hits Actions View
:::: :년	Context Visibility	Q Search b	C DEVICE Device Type RQUALS All Device TypesIBDNAC-Servers	Default Network Access @ >+) 0 @ (3)
×	Operations Policy	Default	Default policy set	Default Network Access 🖉 + • 🚳 🕨
a. Ai	Administration Work Centers			Reset
?	Interactive Help			_

Ajouter un ensemble de stratégies RADIUS

Étape 6 : configuration de la stratégie d'authentification RADIUS

Pour ce faire, sélectionnez l'onglet Policy > Policy Sets > Click (>).

- a. Cliquez sur Actions et choisissez (Insérer une nouvelle ligne ci-dessus).
- b. Définissez le nom de la stratégie d'authentification.
- c. Définissez la condition de stratégie d'authentification et sélectionnez le type de périphérique que vous avez créé précédemment (Étape 1 > b).
- d. Définissez l'option Authentication Policy Use for Identity source.
- e. Cliquez sur Save.

≡	dentity Services Eng	ine Policy / Policy Sets		۵ ۵	0	Q 8	٩
Щ	Bookmarks	Policy Sets-+ DNAC - Policy	Reset	Reset Policy Set Hit Counts		Save	
	Dashboard	Status Policy Set Name Description Conditions		Allowed Protocols / Serve	r Seque	nce Hits	
명	Context Visibility	Q Search					
×	Operations	DIALC - Pullov DIALC - Pullov DIALC - Pullov DIALC - Pullov		Default Network Access		+ 0	
્ણ	Policy						
20	Administration	VAuthentication Policy(2)					
ri.	Work Centers	Status Rule Name Conditions	Use		Hits	Actions	
(?)	Interactive Help	Q, Search		d			
		DINAC - Authentication C DINAC - Authentication DEVICE Device Type EQUALS All Device TypesROMAC-Servers	> Opt	l Users	0	ø	
		Defauit	AI_Us	ons	2	ø	
		>Authorization Policy - Local Exceptions					
		>Authorization Policy - Global Exceptions					
		>Authorization Policy(1)					
				Reset	(e Save)

Ajouter une stratégie d'authentification RADIUS

Étape 7 : configuration de la stratégie d'autorisation RADIUS

Pour ce faire, accédez à l'onglet Policy > Policy Sets > Click (>).

Cette étape permet de créer une stratégie d'autorisation pour chaque rôle d'utilisateur :

- RÔLE DE SUPER-ADMINISTRATEUR
- RÔLE-ADMINISTRATEUR-RÉSEAU
- Rôle DevOps

Procédure

a. Cliquez sur Actions et choisissez (Insérer une nouvelle ligne ci-dessus).

b. Définissez le nom de la stratégie d'autorisation.

c. Définissez la condition de stratégie d'autorisation et sélectionnez le groupe d'utilisateurs que vous avez créé à l' (étape 3).

d. Définissez les résultats/profils de stratégie d'autorisation et sélectionnez le profil d'autorisation que vous avez créé à l' (étape 2).

e. Cliquez sur Save.

≡	dentity Services Eng	ine Policy / Policy Sets	Q & 0	9 Q A
н	Bookmarks	Policy Sets-+ DNAC - Policy	Reset Reset Policy Set Hit Counts	Save
	Dashboard	Status Policy Set Name Description Conditions	Allowed Protocols / Server Sequ	vence Hits
18	Context Visibility	Q Search		
~	Operations	O DNAC - Policy 🖳 DEVICE Device Type EQUALS All Device TypesillON	NAC-Servers Default Network Access	0 + o
	Policy			
al o	Administration	> Authentication Policy(2)		
-fili	Work Centers	> Authorization Policy - Local Exceptions		
		> Authorization Policy - Global Exceptions		
3	Interactive Help	VAuthorization Policy(4)		
			Results	
		Status Rule Name Conditions	Profiles Security Groups Hits	Actions
		Q Search b C	d	а
		Super Admin Ri IdentityGroup Name EQUALS User Identity Groups:SUPER-ADMIN	Super-Admin_Role_Pr_ × V + Select from list 🖉 + o	
		Network Admin Pi, IdentityGroup Name EQUALS User Identity Groups.NETWORK-ADMIN	Network-Admin_Role × v + Select from list	٨
		DevOps R. IdentityGroup Name EQUALS User Identity Groups:DevOps	DevOps-Profile	٢
		O Default	DenyAccess / + Select from list / + •	ŵ
				~
				÷
			Reset	Save

(Option 2) Configurer l'authentification externe DNAC à l'aide de TACACS+

Étape 1. (Facultatif) Définissez des rôles personnalisés.

Configurez vos rôles personnalisés en fonction de vos besoins. Vous pouvez utiliser les rôles d'utilisateurs par défaut. Pour ce faire, accédez à l'onglet System > Users & Roles > Role Based Access Control.

Procédure

a. Créer un nouveau rôle.

Ajouter une stratégie d'autorisation

Create a User Role

Create a New Role

Define the name of the role, and then provide an optional description. To make it easier to assign roles down the road, describe the role as clearly as possible.

	Role Name*			
	SecOps-Role	_]		
	Describe the role (antional)			
	or a cite the tare (opposition)			
		4		
				0
				2
				\frown
Exit				Next
-				
L				

Nom du rôle SecOps

b. Définissez l'accès.

⊟ Cisc	o DNA Center				Create a User Role	Q @ 🛎 🗘			
	Define the Access								
	These permissions enable different capabilities in Cisco DNA Center, some of which are inter-dependent. Before making the selections, please ensure you understand the details of what each of these permissions allow. Click here to Learn More.								
	Define the SecOl a role is configure	r restrict user access to certain Cisco DNA Center functions. By default, roles are configured with Read permission, which is an Observer role. If content for that capability is removed from the GUI.							
	> Network Analytics	O Deny	O Read	O Write	Access to Network Analytics related components.				
	> Network Design	O Deny	O Read	() Write	Set up network hierarchy, update your software image repository, and configure network profiles and settings for managing your sites and network devices.				
	> Network Provision	O Deny	○ Read	 Write 	Configure, upgrade, provision and manage your network devices.				
	> Network Services	O Deny	⊖ Read	⊖ Write	Configure additional capabilities on the network beyond basic network connectivity and access.				
	> Platform	 Deny 	O Read	 Write 	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.				
	> Security	() Deny	◯ Read	O Write	Manage and control secure access to the network.				
	> System	O Deny	○ Read	O Write	Centralized administration of your Cisco DNA Center, which includes configuration management, network connectivity, software upgrades, and more.				
	> Utilities	Deny	Read	Write	One-stop-shop productivity resource for the most commonly used troubleshooting tools and services.				
						2			
🕣 Exit					Review Back	Next			

Accès au rôle SecOps

c. Créez le nouveau rôle.

■ Cisco DNA Center		Create a User Role	
Summary Review the SecOps-Role role Make s	ure all the details are as you expect them t	o be. If you need to change something, clicking edit will take you back to that section	
 Role Name & Description Edit 			
Role Name SecOps-Role Role Description			
~ Role Capability Edit			
ASSURANCE			
Monitoring and Troubleshooting	Deny		
Monitoring Settings	Deny		
Troubleshooting Tools	Deny		
NETWORK ANALYTICS			
Data Access	Write		
NETWORK DESIGN			
Advanced Network Settings	Deny		
Image Repository	Deny		
Network Hierarchy	Deny		
Network Profiles	Deny		
Network Settings	Deny		
Virtual Network	Denv		
- Exit			Back Create Role

Résumé du rôle SecOps

■ Cisco DNA Center		Create a User Role	Q @ C A
PnP	Deny		
Provision	Deny		
NETWORK SERVICES			
App Hosting	Deny		
Bonjour	Deny		
Stealthwatch	Deny		
Umbrella	Deny		
PLATFORM			
APIs	Write		
Bundles	Deny		
Events	Deny		
Reports	Deny		
SECURITY			
Group-Based Policy	Write		
IP Based Access Control	Write		
Security Advisories	Write		
SYSTEM			
Machine Reasoning	Deny		
System Management	Deny		
UTILITIES			
Audit Log	Deny		
Event Viewer	Read		
Network Reasoner	Read		1
€ Exit			Back Create Role

Vérifier et créer un rôle SecOps

Étape 2 : configuration de l'authentification externe à l'aide de TACACS+ Pour ce faire, accédez à l'onglet System > Users & Roles > External Authentication.

a. Pour activer l'authentification externe dans Cisco DNA Center, cochez la case Enable External User.

b. Définissez les attributs AAA.

Saisissez Cisco-AVPair dans le champ AAA attributes.

c. (Facultatif) Configurez les serveurs AAA principal et secondaire.

Assurez-vous que le protocole TACACS+ est activé sur le serveur AAA principal au moins, ou sur les serveurs principal et secondaire.

E Cisco DNA Center	System / Users & Roles Q 💿 🔿 🗸	0
User Management Role Based Access Control	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 delete AAA Servers. The AAA Attribute here 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 chooses to change it to any other AAA attribute, it needs to be configured here on Cisco DNA Center.	e
a a	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 cisco-av-pair attribute from cisco specific AAA attributes list. A sample configuration inside Authorization profile would look like "cisco-av-pairs Role=SUPER-ADMIN-ROLE".	
b	AAA Attribute AAA Attribute Cisco-AVPair	
С	Reset to Default Update V AAA Server(s) Primary AAA Server Secondary AAA Server P Address IP Address ISE Server 1 IP V Shared Secret Shared Secret Imp Into Hide Advanced Settings Hide Advanced Settings Port Ag9	

(TACACS+) Étapes de configuration de l'authentification externe

(Option 2) Configuration d'ISE pour TACACS+

Étape 1 : activation du service d'administration des périphériques

Pour ce faire, accédez à l'onglet Administration > System > Deployment > Edit (ISE PSN Node) > Check Enable Device Admin Service.

=	dealer Identity Services	Engine						Administration	System				۵ ۵	0	0 A
JI.	Bookmarks	Deployr	ment Licensing	Certificate	s Logging	Maintenance	Upgrade & Rollback	Health Checks	Backup & Restore	Admin Access	Settings				
- 22	Dashboard														
15	Context Visibility				Adm	inistration									
*	Operations														
-0	Policy					Monitoring									
20	Administration				Ro	e Pi	RIMARY	Ŷ							
ñ	Work Centers				Ot	her Monitoring Node									
						Dedicated MnT (
C	Interactive Help														
					— × 1	Policy Service									
					2 ×	Enable Session Se	rvices 🕠								
						Include Node in No	ode Group None		~ 0						
		L			🛃 Er	able Profiling Service	• 🖸								
					Er	able Threat Centric P	VAC Service 🕕								
						Enable SXP Service	• (1)								
					1 6										
						able Device Admin :	service ()								
					_ E	able Passive Identity	y Service 🕕								
					— ~ 1	oxGrid ()									
					E E	able pxGrid Cloud)								
														2	
												Reset		Save	

Étape 2 : ajout d'un serveur DNAC en tant que périphérique réseau sur ISE

Pour ce faire, accédez à l'onglet Administration > Network Resources > Network Devices.

Procédure

- a. Définissez le nom et l'adresse IP du périphérique réseau (DNAC).
- b. (Facultatif) Classez le type de périphérique pour la condition Jeu de stratégies.
- c. Activez les paramètres d'authentification TACACS+.
- d. Définissez le secret partagé TACACS+.

\equiv dealer identity Services	Engine	Administration / Network Resources	Q & @ Q	۹
JII Bookmarks	Network Devices	Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences External MDM pxGrid Direct Connectors		
Dashbaard Context Visibility Context Visibility Operations Policy Administration R Work Centers Triteractive Help	Vetant Device Drivel Device Device Security Settings	A A A A A A A A A A A A A A A A A A A		
		C No Set To Default D Device Type DNAC-Servers C C Authentication Settings C C Shared Secret D Envice Single Connect Mode C C C Connect Mode C Single Connect Mode C Connect Single Connect Support		

Périphérique réseau ISE (DNAC) pour TACACS+

Étape 3 : création de profils TACACS+ pour chaque rôle DNAC

Pour ce faire, accédez à l'onglet Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles.

Remarque : Créez 3 profils TACACS+, un pour chaque rôle d'utilisateur.

- a. Cliquez sur Add et définissez le nom du profil TACACS.
- b. Cliquez sur l'onglet Affichage brut.
- c. Saisissez Cisco-AVPair=ROLE= et remplissez le rôle d'utilisateur approprié.
 - Pour le rôle d'utilisateur (SecOps-Role), saisissez Cisco-AVPair=ROLE=SecOps-Role.

- Pour le rôle d'utilisateur (NETWORK-ADMIN-ROLE), entrez Cisco-AVPair=ROLE=NETWORK-ADMIN-ROLE.
- Pour le rôle d'utilisateur (SUPER-ADMIN-ROLE), saisissez Cisco-AVPair=ROLE=SUPER-ADMIN-ROLE.

Remarque : Souvenez-vous que la valeur AVPair (Cisco-AVPair=ROLE=) est sensible à la casse et assurez-vous qu'elle correspond au rôle d'utilisateur DNAC.

d. Cliquez sur Save.

≡	dentity Services	Engine		Wor	k Centers / Device Ac			٩	۵	0	φΙ.	<u>م</u>	
Л	Bookmarks	Overview Identities	User Identity (roups Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	Reports	Settings				
	Dashboard	Conditions	TACACS	Profiles > New									
망	Context Visibility	Network Conditions	TACA	S Profile									
- ×	Operations	Results	 Name SecOp 	_Role									
	Policy	TACACS Command Sets	_										
40	Administration	TACACS Profiles	Descript	on									
- Ali	Work Centers												
0	Interactive Help		C Profile C Cisco-	hibute View Attributes Attributes AVPP#r=ROLE=SecOps-Role	Cancel	d Save							

Créer un profil TACACS (SecOps_Role)

Étape 4 : création d'un groupe d'utilisateurs

Pour ce faire, accédez à l'onglet Work Centers > Device Administration > User Identity Groups.

- a. Cliquez sur Add et définissez le nom du groupe d'identités.
- b. (Facultatif) Définissez la description.
- c. Cliquez sur Envoyer.

≡	ahada Identity Services	Engine			Work	Centers / Device Ad	ministration			٩	۵	0	¢	A
Л	Bookmarks	Overview	Identities User	Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	Reports	Settings				
51	Dashboard			User Ide	tity Groups > New User Ide	ntity Group								
1d	Context Visibility	Identity (Groups	Identit	y Group									
×	Operations	<	1	• a	e SecOps									
0	Policy	> E	Endpoint Identity Gro	ups ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	SecOps-Role	<──								
20	Administration	> 0	User Identity Groups	b Desc	iption									
đ	Work Centers)								
•	Interactive Help									C		C	incel	

Créer un groupe d'identités utilisateur

Étape 5 : création d'un utilisateur local

Pour ce faire, accédez à l'onglet Work Centers > Device Administration > Identities > Users.

- a. Cliquez sur Add et définissez le nom d'utilisateur.
- b. Définissez le mot de passe de connexion.
- c. Ajoutez l'utilisateur au groupe d'utilisateurs associé.
- d. Cliquez sur Submit.

≡	dentity Services	Engine				Work	Centers / De	evice Adm	inistration			٩	۵ ۵	р Ф	A
Л	Bookmarks	Overview	Identities	User Identity G	roups	Ext Id Sources	Network Res	sources	Policy Elements	Device Admin Policy	Sets Reports	Settings			
53	Dashboard	Users		Network	Access Users I	List > New Network Ac	cess User								
15	Context Visibility														
×	Operations			V Net	work Acc	ess User									
-0	Policy			a 🕛	rname	SecOps_User	_								
8.	Administration			Statu	s	Z Enabled 🗸	_								
đ	Work Centers			Acco	unt Name Ali	ias		0							
				Emai											
?	Interactive Help														
				∨ Pa	sswords										
				Pas	sword Type:	Internal Users	~								
				Pas	word Lifetim	ne:									
				•	With Expiration	on ① expire in 60 days									
				0	Never Expire	s 🛈									
				6											
				h		Password		Re-Enter	Password]					
				·Le	gin Passwor	d				Generate Password	0				
				Enal	ble Password	d				Generate Password	0				
				∨ Us	er Informa	ation									

Créer un utilisateur local 1-2

≡	alada Identity Services	Engine			Work	Centers / Device Ad	ministration			q	۵ ۵	0 Q A
н	Bookmarks	Overview	Identities	User Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	Reports	Settings		
	Dashboard	Users		✓ User Information	nation							
1d	Context Visibility			First Name								
*	Operations			Last Name								
-0	Policy			- Cast Hollie								
8.	Administration			× Account C	otions							
đ	Work Centers			Description	,							
?	Interactive Help			Change passv	rord on next login							
				✓ Account D	isable Policy							
				Disable a	ccount if date exceed	s 2025-03-20	(yyyy-mm-dd)					
					С							
				✓ User Grou	ps							
				: SecOpe		<u>~</u> (1) 🕤						
										d		
										Submit		Dancel

Créer un utilisateur local 2-2

Étape 6. (Facultatif) Ajoutez un jeu de stratégies TACACS+.

Pour ce faire, accédez à l'onglet Work Centers > Device Administration > Device Admin Policy Sets.

Procédure

a. Cliquez sur Actions et choisissez (Insérer une nouvelle ligne ci-dessus).

b. Définissez le nom du jeu de stratégies.

c. Définissez la condition Jeu de stratégies sur Sélectionner le type de périphérique précédemment créé (Étape 2 > b).

- d. Définissez les protocoles autorisés.
- e. Cliquez sur Save.

f. Cliquez sur (>) Policy Set View pour configurer les règles d'authentification et d'autorisation.

≡	dentity Services Er	ngine		Policy / Policy Sets	Q & @ Q A
Щ	Bookmarks	Policy Sets			Reset Policy Set Hit Counts Save
	Dashboard	Status Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence Hits Actions View
15	Context Visibility	Q Search		0	d (
- %	Operations	D			
0	Policy	Unave - Peney		E DEVICE DANCE TYPE EQUALS AL DANCE TYPESHUMAC-Servers	
8.	Administration	Oefault	Default policy set		Default Network Access 🖉 🕂 o 🍪 🕨
di.	Work Centers				e
					Resot Save
?	Interactive Help				

Ajouter un ensemble de stratégies TACACS+

Étape 7 : configuration de la stratégie d'authentification TACACS+

Pour ce faire, accédez à l'onglet Work Centers > Device Administration > Device Admin Policy Sets > Cliquez sur (>).

Procédure

a. Cliquez sur Actions et choisissez (Insérer une nouvelle ligne ci-dessus).

b. Définissez le nom de la stratégie d'authentification.

c. Définissez la condition de stratégie d'authentification et sélectionnez le type de périphérique que vous avez créé précédemment (Étape 2 > b).

- d. Définissez l'option Authentication Policy Use for Identity source.
- e. Cliquez sur Save.

$\equiv \frac{\mathrm{diab}}{\mathrm{cisco}}$ Identity Servic	es Engine Work Centers / Device Administration		9 A
II Bookmarks	Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements	Device Admin Policy Sets Reports Settings	
E Dashboard	Policy Sets→ DNAC - Policy	Reset Reset Policy Set Hit Counts	e
1-1 Context Visibility			
ℜ Operations	Status Policy Set Name Description Conditions	Allowed Protocols / Server Sequence	Hits
Dolicy	Q. Search		
Administration	DNAC - Pelicy DEVICE Device Type EQUALS All Device Typest0NAC	Default Device Admin	0
Work Centers			
	VAuthentication Policy(2)		
Interactive Help	Status Rule Name Conditions	Use Hits Ac	tions
	Q, Search	d	
	b	Internal Users	
	DNAC - Authentication E DEVICE-Device Type EQUALS All Device TypesIIDNAC-Servers	> Options • §	<u>څ</u>
		All_User_ID_Stores	
	O Default:	> Options 0 A	\$ ³
	> Authorization Policy - Local Exceptions		
	>Authorization Policy - Global Exceptions		
	>Authorization Policy(4)		

Ajouter une stratégie d'authentification TACACS+

Étape 8 : configuration de la stratégie d'autorisation TACACS+

Pour ce faire, accédez à l'onglet Work Centers > Device Administration > Device Admin Policy Sets > Cliquez sur (>).

Cette étape permet de créer une stratégie d'autorisation pour chaque rôle d'utilisateur :

- RÔLE DE SUPER-ADMINISTRATEUR
- RÔLE-ADMINISTRATEUR-RÉSEAU
- Rôle SecOps

Procédure

a. Cliquez sur Actions et choisissez (Insérer une nouvelle ligne ci-dessus).

b. Définissez le nom de la stratégie d'autorisation.

c. Définissez la condition de stratégie d'autorisation et sélectionnez le groupe d'utilisateurs que vous avez créé à l' (étape 4).

d. Définissez les profils Shell de stratégie d'autorisation et sélectionnez le profil TACACS que vous avez créé à l' (étape 3).

e. Cliquez sur Save.

≡	ahala Identity Services I	Engine				Wa	ork Center	s / Device Ad	ministratio	n			Q	۵	0	Q A
Щ	Bookmarks	Overview	Identi	ties User Identity	Groups	Ext Id Sources	s Netwo	rk Resources	Policy El	ements Device	Admin Policy Set	s Reports	Settings			
22	Dashboard	0	Q Search													
망	Context Visibility		0	DNAC - Policy			DEVICE	Device Type EQUAL	S All Device Ty	pes#DNAC		D	efault Device Ad	min	0	+ 0
~%	Operations															
-0	Policy	> A1	uthentication	Policy(2)												
80	Administration	> A1	uthorization F	folicy - Local Exceptions												
đ	Work Centers	> A1	uthorization F	folicy - Global Exceptions												
		VAL	uthorization F	olicy(1)												
?	Interactive Help									Results						
		0	Status	Rule Name	Condit	lions				Command Sets		Shell Profiles			Hits	Actions
			Q Search					1	l							
	SUPER-ADMIN	I-ROLE	•	Super Admin	8.4	dentityGroup-Name EQ	QUALS User Iden	ntity Groups:SUPER-	ADMIN	Select from list	0 +	SUPER_ADMI	N_ROLE 🛛	· ~+		(3)
	NETWORK-ADM	IN-ROLE	0	Network Admin	8.1	dentityGroup-Name EQ	UALS User Ide	ntity Groups:NETWO	RK-ADMIN	Select from list	0 +	NETWORK_AD	MIN_ROLE 🤕	×+		
	SecOps-Rol	е	•	SecOps	8.1	dentityGroup-Name EQ	QUALS User Ide	ntity Groups:SecOps		Select from list	0 +	SecOps_Role	æ	~+		(2)
			۰	Default						DenyAllCommands	0 +	Deny All Shell	Profile	0+	0	(2)
																0
															6	
														Reset	C	Save

Ajouter une stratégie d'autorisation

Vérifier

Vérification de la configuration RADIUS

1- DNAC - Afficher les utilisateurs externes Système > Utilisateurs et rôles > Authentification externe > Utilisateurs externes.

Vous pouvez afficher la liste des utilisateurs externes qui se sont connectés via RADIUS pour la première fois. Les informations affichées incluent leurs noms d'utilisateur et leurs rôles.

■ Cisco DNA Center	System	/ Users & Roles		Q @ @ \$
User Management Role Based Access Control External Authentication	External Authentication Cisco DNA Center supports external servers for authentication and authorization of name of the AAA attribute chosen on the AAA server. The default attribute expecte The value of the AAA attribute to be configured for authorization on AAA server we configuration inside Authorization profile would look like "cisco-av-pairs" Role-SUP An example configuration in the case of manually defining the AAA attribute would Cable External User AAA Attribute AAA Attribute Cisco-AVPair	External Users Use the fields in this window to create, update and delete AAA Servers. In Gisco-AVPair, but if the user chooses to change it to any other AAA attribute, it needs id be in the format of "Role=role1". On ISE server, choose the cisco-av-pair attribute fror R-ADMIN-ROLE?	e AAA Attribute here on C s to be configured here on n cisco specific AAA attrib	isco DNA Center is the Cisco DNA Center. utes list. A sample
	Reset to Default Update			
	 ✓ External Users \[\Vec{Filter} \] 		∃Q, Find	
	Username •	Role	Action	
	devops_user	DevOps-Role	Delete	
		Showing 1 of 1		

2. DNAC - Confirmez l'accès utilisateur.

Cisco DNA Center		۵	04
Jag Workflows Tools > Platform > Explore >	Overview Manage Developer Toolkit Runtime Dashboard	enter with the adoption journey map. time to value, as you guide your organization on its	Explore
▲ devops_user 《			

3.a ISE - RADIUS Live-Logs Operations > RADIUS > Live-Logs.

=	dentity Services	Engine	o	perations / RADIUS		A & @ & A
1	Bookmarks	Live Logs Live Sessions				
=: .(2	Context Visibility	Misconfigured Supplicants 💿	Misconfigured Network Devices 📀	RADIUS Drops 🕕	Client Stopped Responding 📀	Repeat Counter 🕕
*	Operations	0	0	5761	0	0
U	Policy				Refresh Show	Within
2	Administration	🖉 📁 Reset Repeat Counts 🖞 Export To			Never V Latest 20 reco	Filter V O
-	Work Centers	Time Status	Details Repea Identity En	dpoint ID Endpoint Profile Authentication Polic	cy Authorization Policy Author	ization Profiles IP Addre
(?	Interactive Help	X AuthN	x Identity En	dpoint ID Endpoint Profile Authentication Policy	Authorization Policy Authori	zation Profiles IP Addres
		Jan 19, 2025 11:19:18.1	OevOps_User	DNAC - Policy >> DNAC	C - Authentication DNAC - Policy >> DevOps	Profile
		Last Updated: Sun Jan 19 2025 23:19:5	7 GMT+0100 (Central European Standard Time)			Records Shown: 1

Journaux en direct RADIUS

3.b ISE - RADIUS Live-Logs Operations > RADIUS > Live-Logs > Click (Details) for Authorization log.

Accès utilisateur limité



Steps		
Step ID	Description	Latency
11001	Received RADIUS Access-Request	
11017	RADIUS created a new session	0
11015	An Access-Request MUST contain at least a NAS-IP- Address, NAS-IPv6-Address, or a NAS-Identifier; Continue processing	1
11117	Generated a new session ID	2
15049	Evaluating Policy Group	1
15008	Evaluating Service Selection Policy	1
15048	Queried PIP - DEVICE.Device Type	2
15041	Evaluating Identity Policy	3
15048	Queried PIP - DEVICE.Device Type	4
15013	Selected Identity Source - Internal Users	3
24210	Looking up User in Internal Users IDStore - DevOps_User	0
24212	Found User in Internal Users IDStore	8
22037	Authentication Passed	1
15036	Evaluating Authorization Policy	1
15016	Selected Authorization Profile - DevOps-Profile	5
22081	Max sessions policy passed	1
22080	New accounting session created in Session cache	1
11002	Returned RADIUS Access-Accept	0

(ms)

Journaux en direct détaillés RADIUS 1-2

Cisco ISE	
IdentityPolicyMatchedRule	DNAC - Authentication
AuthorizationPolicyMatchedR ule	DevOps
ISEPolicySetName	DNAC - Policy
IdentitySelectionMatchedRule	DNAC - Authentication
TotalAuthenLatency	35
ClientLatency	0
DTLSSupport	Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types#DNAC-Servers
IPSEC	IPSEC#Is IPSEC Device#No
Name	User Identity Groups:DevOps
EnableFlag	Enabled
RADIUS Username	DevOps_User
Device IP Address	
CPMSessionID	0a301105o95d4kCbV7kMBCoFkesRirFcDiXec0uEqPPr8RtG/ WY
CiscoAVPair	AuthenticationidentityStore-Internal Users, FQSubjecName=9273E03-8c01-11e6-996c- 525400be85784eevoos_user, UniqueSubjectD+9b4d28083db66a1f8bcc98565c8f5eaa5de df467
Result	
Class	CACS:0a301105o95d4kCbV7kMBCoFkesRirFcDiXec0uEqPPr8R tG/WY:ise34/526422220/15433
cisco-av-pair	ROLE=DevOps-Role

Journaux en direct détaillés RADIUS 2-2

Vérification de la configuration TACACS+

1- DNAC - Afficher les utilisateurs externes Système > Utilisateurs et rôles > Authentification externe > Utilisateurs externes.

Vous pouvez afficher la liste des utilisateurs externes qui se sont connectés via TACACS+ pour la première fois. Les informations affichées incluent leurs noms d'utilisateur et leurs rôles.

■ Cisco DNA Center		System / Users & Roles		Q @ 4
User Management Role Based Access Control External Authentication	 AAA Attribute AAA Attribute Cisco-AVPair Reset to Default Upd 	ate		
	 AAA Server(s) Primary AAA Server P Address Shared Secret Imfo View Advanced Settings Update 	Secondary AAA Server IP Address Shared Secret Internet Secret Internet Secret Internet Secret Internet Secret Internet Secret Internet Secret Secret Internet Secret Secre		
	 ✓ External Users ▽ Filter Usemame + 	Role	Action	EQ Find
	secops_user	SecOps-Role Showing 1 of 1	Delete	

Utilisateurs externes

2. DNAC - Confirmez l'accès utilisateur.

Cisco DNA Center			Q (0)
Policy	Group-Based Access Control		C Explore
- Workflows	IP & URL Based Access Control	enter with the adoption journey map.	×
💥 Tools		time to value, as you guide your organization on its	
Platform			
Activities			
Explore			
<u>β</u> secops_user		Job Network Bug identifier Identify bugs in the network	

Accès utilisateur limité

3.a ISE - Centres de travail TACACS+ Live-Logs > Administration des périphériques > Présentation > TACACS Livellog.

≡	dentity Services	Engine		Operations / TACACS		Q & @ Q A
н	Bookmarks	Live Logs				
50	Dashboard					
망	Context Visibility				Refresh	Show Within
*	Operations				Never 🗸	Latest 20 records v Last 60 Secondsv
0	Policy	Ø ⊥ Export To ∨				Filter 🗸 🔘
20	Administration	Logged Time	Status Details Identity	Type Authentication Policy	Authorization Policy Shell Profile	Device Type Lo
đ	Work Centers	×	Identity	Authentication Policy	Authorization Policy Shell Profile	Device Type Lo
		Jan 19, 2025 05:12:4	SecOps_User	Authorization	DNAC - Policy >> SecOps SecOps_Role	Device Type#All Device Types#DNAC Loc
?	Interactive Help	Jan 19, 2025 05:12:4	2025 17:16:38 GMT+0100 (Central Europe	Authentication DNAC - Policy >> DNAC - Authentication		Device TypeIIAII Device TypesIIDNAC Loc Records Shown: 2
		Last opdated. Suit san 197		an standard rinney		Records Shown. 2

Journaux TACACS en direct

3.b ISE - détails TACACS+ Live-Logs Work Centers > Device Administration > Overview > TACACS Livellog > Click (Details) for Authorization log.

1	taté Cisco ISE									
	Overview		Steps							
	Request Type	Authorization	Step ID	Description	Latency (ms)					
	Status	Pass	13005	Received TACACS+ Authorization Request						
			15049	Evaluating Policy Group	1					
	Session Key	ise34/526427220/13958	15008	Evaluating Service Selection Policy	1					
	Message Text	Device-Administration: Session Authorization succeeded	15048	Queried PIP - DEVICE.Device Type	4					
	Username	SecOps_User	15041	Evaluating Identity Policy	7					
			15013	Selected Identity Source - Internal Users	5					
	Authorization Policy	DNAC - Policy >> SecOps	24210	Looking up User in Internal Users IDStore	1					
	Shell Profile	SecOps_Role	24212	Found User in Internal Users IDStore	4					
	Matched Command Set		22037	Authentication Passed	0					
	0			Evaluating Authorization Policy	0					
	Command From Device		15048	Queried PIP - Network Access.UserName	10					
			15048	Queried PIP - IdentityGroup.Name	2					
			15017	Selected Shell Profile	2					
	Authorization Details		22081	Max sessions policy passed	1					
	Generated Time	2025-01-19 17:12:43.368 +1:00	22080	New accounting session created in Session cache	0					
			13034	Returned TACACS+ Authorization Reply	•					
	Logged Time	2025-01-19 17:12:43.368								
	Epoch Time (sec)	1737303163								
	ISE Node	ise34								
	Message Text	Device-Administration: Session Authorization succeeded								
	Failure Reason									
	Resolution									
	Root Cause									
	Username	SecOps_User								
	Network Device Name	DNAC								

Journaux en direct détaillés TACACS+ 1-2

dinde Cisco ISE	
.160	riterioniconom
Service-Argument	cas-service
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	Lookup
SelectedAccessService	Default Device Admin
RequestLatency	38
IdentityGroup	User Identity Groups:SecOps
SelectedAuthenticationIdentit yStores	Internal Users
AuthenticationStatus	AuthenticationPassed
UserType	User
CPMSessionID	13004827410.62.150.14628131Authorization130048274
IdentitySelectionMatchedRule	DNAC - Authentication
StepLatency	1=1;2=1;3=4;4=7;5=5;6=1;7=4;8=0;9=0;10=10;11=2;12=2;1 3=1;14=0;15=0
TotalAuthenLatency	38
ClientLatency	0
Network Device Profile	Cisco
IPSEC	IPSEC#Is IPSEC Device#No
Name	User Identity Groups:SecOps
EnableFlag	Enabled
Response	{Author-Reply-Status=PassAdd; AVPair=Cisco- AVPair=ROLE=SecOps-Role; }

Journaux en direct détaillés TACACS+ 2-2

Dépannage

Aucune information de diagnostic spécifique n'est actuellement disponible pour cette configuration.

Références

- <u>Guide d'administration de Cisco Identity Services Engine, version 3.4 > Device</u>
 <u>Administration</u>
- Guide de l'administrateur de Cisco DNA Center, version 2.3.5
- Cisco DNA Center: Contrôle d'accès basé sur les rôles avec authentification externe

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.