# Configurer ACS 5.2 pour l'authentification basée sur les ports avec un LAP

## Table des matières

Introduction Conditions préalables **Exigences** Composants utilisés **Conventions** Informations générales Configurer Diagramme du réseau **Hypothèses Configuration Steps Configurer le LAP** Configurer le commutateur Configuration du serveur RADIUS Configuration des ressources réseau Configurer des utilisateurs Définir des éléments de stratégie Appliquer les stratégies d'accès Vérifier **Dépannage** Informations connexes

# Introduction

Ce document décrit comment configurer un point d'accès léger (LAP) en tant que demandeur 802.1x afin de s'authentifier auprès d'un serveur RADIUS tel qu'un serveur de contrôle d'accès (ACS) 5.2.

# Conditions préalables

## Exigences

Assurez-vous que vous remplissez ces conditions avant d'essayer cette configuration :

- Posséder des connaissances de base sur le contrôleur LAN sans fil (WLC) et les LAP.
- Avoir une connaissance fonctionnelle du serveur AAA.

 Avoir une connaissance complète des réseaux sans fil et des problèmes liés à la sécurité sans fil.

### Composants utilisés

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

- WLC Cisco 5508 exécutant la version de microprogramme 7.0.220.0
- LAP de la gamme Cisco 3502
- Cisco Secure ACS exécutant la version 5.2
- Commutateur de la série Cisco 3560

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. If your network is live, make sure that you understand the potential impact of any command.

### Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux <u>Conventions relatives aux conseils techniques Cisco.</u>

# Informations générales

Les LAP ont installé en usine des certificats X.509 - signés par une clé privée - qui sont gravés dans le périphérique au moment de la fabrication. Les LAP utilisent ce certificat afin de s'authentifier auprès du WLC lors du processus de jointure. Cette méthode décrit une autre façon d'authentifier les LAP. Avec le logiciel WLC, vous pouvez configurer l'authentification 802.1x entre un point d'accès (AP) Cisco Aironet et un commutateur Cisco. Dans ce cas, le point d'accès agit comme demandeur 802.1x et est authentifié par le commutateur sur un serveur RADIUS (ACS) qui utilise EAP-FAST avec approvisionnement PAC anonyme. Une fois configuré pour l'authentification 802.1x, le commutateur n'autorise aucun trafic autre que le trafic 802.1x à traverser le port tant que le périphérique connecté au port ne s'authentifie pas correctement. Un point d'accès peut être authentifié soit avant qu'il ne rejoigne un WLC, soit après qu'il ait rejoint un WLC, auquel cas vous configurez 802.1x sur le commutateur après que le LAP ait rejoint le WLC.

# Configurer

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

#### Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Voici les détails de configuration des composants utilisés dans ce diagramme :

- L'adresse IP du serveur ACS (RADIUS) est 192.168.150.24.
- L'adresse d'interface de gestion et de gestionnaire AP du WLC est 192.168.75.44.
- L'adresse des serveurs DHCP est 192.168.150.25.
- Le LAP est placé dans le VLAN 253.
- VLAN 253 : 192.168.153.x/24. Passerelle : 192.168.153.10
- VLAN 75 : 192.168.75.x/24. Passerelle : 192.168.75.1

#### Hypothèses

• Les commutateurs sont configurés pour tous les VLAN de couche 3.

- Une étendue DHCP est attribuée au serveur DHCP.
- La connectivité de couche 3 existe entre tous les périphériques du réseau.
- Le LAP est déjà joint au WLC.
- Chaque VLAN possède un masque /24.
- Un certificat auto-signé est installé sur ACS 5.2.

## **Configuration Steps**

Cette configuration est divisée en trois catégories :

- 1. Configurez LAP.
- 2. Configurez le commutateur.
- 3. Configurez le serveur RADIUS.

Configurer le LAP

Hypothèses :

LAP est déjà enregistré sur le WLC en utilisant l'option 43, DNS, ou IP d'interface de gestion WLC configurée statiquement.

Procédez comme suit :

1. Accédez à Wireless > Access Points > All APs afin de vérifier l'enregistrement LAP sur le WLC.

uluili. cisco	MONITOR MLANS	CONTROLLER WIRELESS SECURITY	Management op	MMANOS HELP (EEDBAC	Sag X	e Configuration	Bing   La	gout i Befred
Wireless	All APs						Entrie	s 1 - 1 of 1
Access Points     All APs	Current Filter	Rone	Change Fite	() [Clear. Filter]				
* NB008 802.11a/n 802.11b/g/h Global Configuration	Number of APs	1						
> Advanced	AP Name	AP Model	AP MAC	AP Up Time	Admin Status	Operational Statuc	Port	AP Mode
Mesh	3502e	AIR-CAP3502E-A-K9	00:0748:78:53:19	1 d, d2 h 32 m 42 s	Enabled	REG	13	Local
HaEAP Groups ▶ 802.11a/n								
▶ 902.11b/g/n								
Hedia Stream								
Country								
Timers								
+ QoS								

- 2. Vous pouvez configurer les informations d'identification 802.1x (nom d'utilisateur/mot de passe) pour tous les LAP de deux manières :
  - Mondialement

Pour un LAP déjà joint, vous pouvez définir les informations d'identification

globalement de sorte que chaque LAP joignant le WLC hérite de ces informations d'identification.

cisco	MONETOR MLAND CONTROLLE	R WIRELESS SECURETY M	иулласмент с	OMMANDS HELP	EEEDENCK	Says Configuration   B	ne i Legout Betre
Wireless	Global Configuration						Apply
CISCO Wireless * Access Points Al APs * Radios #02.336/1 Exclusion Recard Hesh Hesh Hesh Hesh Hesh Hesh Distanced Hesh Hesh Hesh Streams Country Timers > QoS	CDP  CDP  CDP  CDP  CDP  CDP  CDP  CDP	P P State State Coable •		High Availability Af Heartbest Til Lood Mole AF Te HISAP Mole AF Te HISAP Mole AF Te HISAP Mole AF AF Primary Disc Back-up Primary Back-up Pri	LLLDOOD heavt(1-33) st Heartheat Timer State Faut Heartheat Timer State Faut Heartheat Timer State very Timeout(30 to 3600) Controller 39 Address any Controller anne any Controller name t HSS bonfig Parameters bant tarval	5 5 5 5 5 5 7 7 7 7 7 7 7 7 7 7 7 7 7 7	
	Download Primary	Download Backup					

• Individuellement

Configurez des profils 802.1 x par AP. Dans notre exemple, nous allons configurer les informations d'identification par AP.

- a. Accédez à Wireless > All APs, et sélectionnez le point d'accès concerné.
- b. Ajoutez le nom d'utilisateur et le mot de passe dans les champs 802.1x Supplicant Credentials.

ı. cısco	MONITOR MLANE S	CONTROLLER	wpeness	SECURITY	NANGEMENT	COMMINDS	HELP	BERGRACK	Sage Configuration 2ng	Logout   Befree
Wireless	All APs > Details for	3502e							< Beck	Apply
Access Points     All APs     * Rodies     802.118/n     002.118/n     002.118/n     fobbl carfiguration     Advanced     Mesh     HRLAP Groups     b 200.116/n	General Credentials Desin Credentials Over-ride Glebal ere Userneme Pessword Enable Password	sdoritiols	laces   Hilg	ir Aveilebill	y Inventory	Advanced				
<ul> <li>002.11b/g/n</li> <li>Media Stream Country Timers</li> <li>QoS</li> </ul>	802.1x Supplicant Cr Over-ride Global ore Username Peaneord Confirm Password	edentials dentials 3800e 		2						

Remarque : les identifiants de connexion sont utilisés pour établir une connexion Telnet, SSH ou console au point d'accès.

3. Configurez la section Haute disponibilité et cliquez sur Apply.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MUNAGEMENT COMMANDS HELP EEEDBACK	Bays Configuration   Bing   Logout Being
Wireless	All APs > Details for 3502e	< Beck Apply
<ul> <li>Access Points         All APs         S32.116/n         S32.116/n         S32.116/n         S32.116/n         S32.116/n         S0541Configuration         Advanced         Mesh         HREAP Groups         S02.116/n         S02.116/n         S02.116/n         Media Stream         Country         Timers         QoS         </li> </ul>	General     Credentials     Interfaces     High Availability     Investory     Advanced       Name     Name     Name     Name     Name       Primary Castrollar     5566-3     192.168.75.44     Secondary Castrollar       Secondary Castrollar     Tertiary Castrollar     Interfaces	

Remarque : une fois enregistrées, ces informations d'identification sont conservées sur le WLC et l'AP redémarre. Les informations d'identification changent uniquement lorsque le LAP rejoint un nouveau WLC. Le LAP utilise le nom d'utilisateur et le mot de passe qui ont été configurés sur le nouveau WLC.

Si l'AP n'a pas encore rejoint un WLC, vous devez vous connecter au LAP en mode console afin de définir les informations d'identification. Exécutez cette commande CLI en mode enable :

LAP#Iwapp ap dot1x username <username> password <password>

ou

LAP#capwap ap dot1x username <username> password <password>

Remarque : cette commande est disponible uniquement pour les points d'accès qui exécutent l'image de récupération.

Le nom d'utilisateur et le mot de passe par défaut du LAP sont respectivement cisco et Cisco.

#### Configurer le commutateur

Le commutateur agit comme un authentificateur pour le LAP et authentifie le LAP sur un serveur RADIUS. Si le commutateur ne dispose pas du logiciel compatible, mettez-le à niveau. Dans l'interface de ligne de commande du commutateur, émettez ces commandes afin d'activer l'authentification 802.1x sur un port de commutateur :

<#root>
switch#
configure terminal
switch(config)#
dot1x system-auth-control

switch(config)#

aaa new-model

!--- Enables 802.1x on the Switch.

switch(config)#

aaa authentication dot1x default group radius

switch(config)#

radius server host 192.168.150.24 key cisco

!--- Configures the RADIUS server with shared secret and enables switch to send !--- 802.1x information

switch(config)#

ip radius source-interface vlan 253

!--- We are sourcing RADIUS packets from VLAN 253 with NAS IP: 192.168.153.10.

switch(config)interface gigabitEthernet 0/11
switch(config-if)switchport mode access
switch(config-if)switchport access vlan 253
switch(config-if)mls qos trust dscp
switch(config-if)spanning-tree portfast

!--- gig0/11 is the port number on which the AP is connected.

switch(config-if)dot1x pae authenticator

!--- Configures dot1x authentication.

switch(config-if)dot1x port-control auto

!--- With this command, the switch initiates the 802.1x authentication.

Remarque : si vous avez d'autres AP sur le même commutateur et que vous ne voulez pas qu'ils utilisent 802.1x, vous pouvez laisser le port non configuré pour 802.1x ou émettre cette commande :

<#root>

switch(config-if)authentication port-control force-authorized

#### Configuration du serveur RADIUS

Le LAP est authentifié avec EAP-FAST. Vérifiez que le serveur RADIUS que vous utilisez prend en charge cette méthode EAP si vous n'utilisez pas Cisco ACS 5.2. La configuration du serveur RADIUS se divise en quatre étapes :

- 1. <u>Configurer les ressources réseau</u>
- 2. Configurer les utilisateurs.
- 3. Définir des éléments de stratégie.
- 4. Appliquer des stratégies d'accès

ACS 5.x est un ACS basé sur des politiques. En d'autres termes, ACS 5.x utilise un modèle de stratégie basé sur des règles au lieu du modèle basé sur des groupes utilisé dans les versions 4.x.

Le modèle de politique basé sur des règles ACS 5.x offre un contrôle d'accès plus puissant et plus flexible que l'ancienne approche basée sur des groupes.

Dans l'ancien modèle basé sur les groupes, un groupe définit une stratégie car il contient et lie trois types d'informations :

- Informations d'identité Ces informations peuvent être basées sur l'appartenance à des groupes AD ou LDAP ou sur une affectation statique pour les utilisateurs ACS internes.
- Autres restrictions ou conditions : restrictions temporelles, restrictions de périphérique, etc.
- Autorisations VLAN ou niveaux de privilège Cisco IOS<sup>®</sup>.

Le modèle de stratégie ACS 5.x est basé sur des règles de la forme suivante :

Si la condition se produit

Par exemple, nous utilisons les informations décrites pour le modèle basé sur les groupes :

Si identity-condition, restriction-condition puis authorization-profile.

Par conséquent, cela nous donne la flexibilité de limiter les conditions dans lesquelles l'utilisateur est autorisé à accéder au réseau et aussi quel niveau d'autorisation est autorisé lorsque des conditions spécifiques sont remplies.

#### Configuration des ressources réseau

Dans cette section, nous allons configurer le client AAA pour le commutateur sur le serveur RADIUS.

Cette procédure explique comment ajouter le commutateur en tant que client AAA sur le serveur RADIUS afin que le commutateur puisse transmettre les informations d'identification de l'utilisateur du LAP au serveur RADIUS.

Procédez comme suit :

1. Dans l'interface graphique utilisateur ACS, cliquez sur Network Resources.

- 2. Cliquez sur Network Device Groups.
- 3. Accédez à Location > Create (en bas ).

cisco Cisco Secure A	cs
+ 😚 My Workspace	Network Resources > Network Device Groups > Location
👻 🕼 Network Resources	Network Device Groups
Network Device Groups     Location	Filter: 💌 Match it 💌 Go 🛩
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Name      Description     All Locations
🕨 👪 Users and Identity Stores	
+ Sp. Policy Elements	
+ 🔂 Access Policies	
+ 📄 Monitoring and Reports	
🔸 🍇 System Administration	

4. Ajoutez les champs requis et cliquez sur Submit.

cisco Cisco Secure A	CS
+ 🛞 My Workspace	Network Resources > Network Device Groups > Location > Create
Apple Hetwork Resources     Network Device Groups     Location     Device Type     Notwork Devices and AAA Clients     Default Network Device     External RADIUS Servers	Device Group - General         o Name:       LAB         Description:       LAB Devices         o Parent       All Locations         B = Required fields
38 Users and Identity Stores	
Policy Elements	
Access Policies	
Monitoring and Reports	
System Administration	

5. La fenêtre est actualisée :

cisco Cisco Secure ACS							
► 💮 My Workspace	Network Resources > Network Device Groups > Location						
🗴 🛵 Network Resources	Network Device Groups						
<ul> <li>Network Device Groups</li> <li>Location</li> </ul>	Filter: ■ Match if: ■ Go マ						
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Name      Description     * <u>All Locations</u> All Locations						
Users and Identity Stores	LAB LAB Devices						
Policy Elements							
Access Policies							
Monitoring and Reports							
System Administration							

6. Cliquez sur Device Type > Create.

cisco Cisco Secure A	ICS	
+ 🛃 My Workspace	Network Resources > Network Device Groups > Device Type > Edit "Device Type:Al Device Types:Switch	ies"
Kan Network Resources     Network Device Groups     Location	Device Group - General v Name: Switches	
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Parent All Device Types     Select     Select	
Busers and Identity Stores		
Policy Elements		
Access Policies		
Monitoring and Reports	1 1. A. M.	
🖌 🍓 System Administration		

7. Cliquez sur Submit. Une fois terminée, la fenêtre est actualisée :

Cisco Secure ACS						
🕨 🏐 My Workspace	Network Resources > Network Device Groups > Device Type					
🔹 🚛 Network Resources	Network Device Groups					
<ul> <li>Network Device Groups Location</li> </ul>	Filter. Match if. Go 🗢					
Device Type						
Default Network Device	Name A Description					
External RADIUS Servers	All Device Types All Device Types					
Users and Identity Stores	I <u>Switches</u> Switch where LAP is connected					
Sp. Policy Elements						
Access Policies						
Monitoring and Reports						
🕨 🍇 System Administration						

- 8. Accédez à Ressources réseau > Périphériques réseau et clients AAA.
- 9. Cliquez sur Create, et remplissez les détails comme indiqué ici :

cisco Cisco Secure A	cs	acsadmin SALUL-ACSS2 (Primary)
	Network Resources > Network Devices and AAA Clarits > Create o Name: 2500-Seebby LAP Description: Device shares LAD is connected.	
Device Tros Notwork Devices and AAAChents Default Nativork Device External RADIUS Servers 91 Unace and Medite Torses	Network Device Groups Location Al Locations LAB Device Type Al Device Types Switches	Select Select
Group Dements     Group Dements     Group Construction     Group Construction     Group Construction     Group Construction     Group Construction	P Address P Single IP Address C IP Range(s) • IP: 102-168-153.10	Authentication Options
<ul> <li>Ng System Administration</li> </ul>		CoApert  1790 Enable KeyWrap Key Encryption Key Massage Authenticator Cede Key Key Ingut Format C ASCII (* HEXADECIMA).
	O - Regurad felds	

10. Cliquez sur Submit. La fenêtre est actualisée :

cisco Cisco Secure A	CS	economic SALIL-ACI
+ 🔂 Mr Workspace	Network Resources > Network Devices and AAA Clients	
<ul> <li>An Network Resources</li> </ul>	Retwork Devices	Showin
Network Device Groups     Location	Filter: Vilatch it. V Go V	
Network Devices and AM-Clients	Rame - IP/Mask NDGLocation NDGDevice Type	Description
Detault Network Device External RADIUS Servera	Step-Switch-LAP 192.168.153.10/32 All Locations:LAB All Device Types:Bwitches	Switch withere LAP is connected
+ 🎒 Lisers and identity Stores		
+ 🚱 Policy Elements		
» 💭 Access Policies		
Monitoring and Reports		
+ 🥂 System Administration		

Configurer des utilisateurs

Dans cette section, vous allez voir comment créer un utilisateur sur l'ACS configuré précédemment. Vous attribuerez l'utilisateur à un groupe appelé « utilisateurs LAP ».

Procédez comme suit :

1. Accédez à Utilisateurs et magasins d'identités > Groupes d'identités > Créer.

	cisco Cisco Secure A	CS
	▶ 💮 My Workspace	Users and identity Stores > identity Groups > Edit: "identityGroup:All Groups:Wireless Users"
	Network Resources	Canadral
	Weers and identity Stores     Identity Groups     Internal Identity Stores     External Identity Stores     LDAP	Vame: LAP users     Description: LAPs authenticating over wired Network     Parent All Groups Select
the set of	Active Directory RSA SecuriD Token Servers RADIUS Identity Servers Certificate Authorities Certificate Authorities Identity Store Sequences	

2. Cliquez sur Submit.

Cisco Secure A	CS
<ul> <li>► 😚 My Workspace</li> <li>► 🎲 Network Resources</li> </ul>	Users and Identity Stores > Identity Groups
<ul> <li>Stores</li> <li>Identity Groups</li> </ul>	Filter: 💽 Match if: 💽 Go 🔫
<ul> <li>Internal Identity Stores</li> <li>External Identity Stores         <ul> <li>LDAP</li> <li>Active Directory</li> <li>RSA SecurID Token Servers</li> <li>RADIUS Identity Servers</li> <li>Certificate Authorities</li> <li>Certificate Authentication Profile</li> <li>Identity Store Sequences</li> </ul> </li> </ul>	Name       Description         * All Groups       Identity Group Root         LAP users       LAPs authenticating over wired Network.

- 3. Créez 3502e et attribuez-le au groupe « Utilisateurs LAP ».
- 4. Accédez à Utilisateurs et magasins d'identités > Groupes d'identités > Utilisateurs > Créer.

cisco Cisco Secure Ad	cs
🕨 🔆 My Workspace	Users and identity Stores > Internal identity Stores > Users > Create
In the second	Canaral
🔹 👸 Users and Identity Stores	Name: 3502e Status: Enabled - G
Identity Groups	Description: LAP 3502e in Vian 253
Users	Identity Group: All Groups:LAP users     Select
Hosts <ul> <li>External Identity Stores</li> <li>Certificate Authorities</li> <li>Certificate Authentication Profile</li> <li>Identity Store Sequences</li> </ul>	Password Information Password must Contain 4 - 32 characters
Policy Elements	Password:
Access Policies	O Confirm Password
<ul> <li>Monitoring and Reports</li> </ul>	Change password on next login
🕨 🍓 System Administration	User information There are no additional identity attributes defined for user records • = Required fields

5. Vous verrez les informations mises à jour :

Wetwork Resources      Metwork Resources      Identity Stores      Identity Groups      Identity Stores      Identity Stores					s > Internal identity 5	id Identity Store	Users an	My Workspace
Users and Identity Stores         Filter:         Match it:         G0 ♥           Identity Groups         Filter:         Identity Groups         G0 ♥		Internal Users						
Identity Groups						-	Filler	😘 Users and Identity Stores
Distanti disati Casa di Santa di S					→ Match II:	- 1	Filler	Identity Groups
identity Group Description		Description	Identity Group		User Name	Status		ntemai identity Stores
I I I All Groups:LAP users LAP 3502e in v	in vian 253	LAP 3502e in via	All Groups:LAP users		<u>3502e</u>			Users

Définir des éléments de stratégie

Vérifiez que Permit Access est défini.

cisco Cisco Secure ACS					
+ 💮 My Workspace	Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles				
Network Resources	Authorization Profiles				
Users and identity Stores	Filter That h if the second se				
🗸 🚱 Policy Elements	There Description				
<ul> <li>Session Conditions</li> <li>Authorization and Permissions</li> </ul>	Permit Access				
<ul> <li>Network Access Authorization Profiles</li> </ul>					
Device Administration     Named Permission Objects					
+ 🔂 Access Policies					
Monitoring and Reports					
🕨 🦓 System Administration					

#### Appliquer les stratégies d'accès

Dans cette section, vous allez sélectionner EAP-FAST comme méthode d'authentification utilisée pour les LAP afin de s'authentifier. Vous allez ensuite créer des règles basées sur les étapes précédentes.

Procédez comme suit :

1. Accédez à Politiques d'accès > Services d'accès > Accès réseau par défaut > Modifier : "Accès réseau par défaut".

cisco Cisco Secure ACS					
🕞 😚 My Workspace	Access Policies > Access Services > Default Network Access > Edit "Default Network Access"				
+ 🍪 Network Resources					
Busers and Identity Stores	General Allowed Protocols				
Policy Elements	Name: Default Network Access				
🖌 🅵 Access Policies	Description: Default Network Access Service				
Access Services     Access Service Selection Rules     O Default Device Admin	Service Type : Network Access				
Oefault Network Access	Identity				
▶ 🖉 deleterne	Group Mapping				
Monitoring and Reports	Authorization				
<ul> <li>System Administration</li> </ul>					

2. Assurez-vous que vous avez activé EAP-FAST et Anonymous In-Band PAC Provisioning.

cisco Cisco Secure ACS						
+ 💮 My Workspace	Access Policies > Access Services > Default Network Access > Edit "Default Network Acces					
Network Resources     Webwork Resources     Users and Identity Stores     Users and Identity Stores     Policy Elements     Access Policies     Access Services     Service Selection Rules     Service Selection Rules     O Default Device Admin     O Default Network Access     Identity     Authorization     Ø deleteme     Monitoring and Reports     System Administration	General       Allowed Protocols         Image: Process Host Lookup         Authentication Protocols         Image: Allow PAP/ASCII         Image: Allow CHAP         Image: Allow MS-CHAPv1         Image: Allow MS-CHAPv2         Image: Allow EAP-IND5         Image: Allow EAP-TLS         Image: Allow EAP-FAST         Image: Preferred EAP protocol					

• 🛼 Access Policies	► Allow LEAP
Access Services     Service Selection Rules     G Default Device Admin     O Default Device Admin     O Default Network Access     Identity     Authorization     Ø deleteme     Monitoring and Reports     Ø System Administration	Allow PEAP     PEAP Inner Methods     P Allow EAP-MS-CHAPV2     P Allow Password Change Retries: 1     P Allow EAP-GTC     P Allow Password Change Retries: 1
	<ul> <li>Allow EAP-FAST</li> <li>EAP-FAST Inner Methods</li> <li>Allow EAP-MS-CHAPV2</li> <li>Allow EAP-GTC</li> <li>Allow Password Change Retries: 3</li> <li>Allow TLS-Renegotiation</li> <li>Use PACs © Don't Use PACs</li> <li>Tunnel PAC Time To Live: 90</li> <li>Poactive PAC update will occur after 10</li> <li>% of PAC Time To Live has expired</li> <li>Allow Authenticated In-Band PAC Provisioning</li> <li>Server Returns Access Accept After Authenticated Provisioning</li> <li>Berver Returns Access Accept After Authenticated Provisioning</li> <li>Allow Nachine Authentication</li> <li>Machine PAC Time To Live: 1</li> <li>Hours </li> </ul>
	Submit Cancel

- 3. Cliquez sur Submit.
- 4. Vérifiez le groupe d'identités que vous avez sélectionné. Dans cet exemple, utilisez Internal Users (qui a été créé sur ACS) et enregistrez les modifications.

cisco Cisco Secure Al	csadmin SAI
▶ 🚭 My Workspace	Access Policies > Access Services > Default Network Access > Mently
+ ity Network Resources	9 Single result selection C Bule based result selection.
+ 🐉 Users and Identity Stores	Identity Source: Internal Users Select
Policy Elements	· Advanced Centers
🖌 🕵 Access Policies	t a mentication failed Read
Access Services     E Service Selection Rules     O Detault Device Admin	if user not found Reject  If process failed Drop
Option Network Access	Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP it is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests will
Authorization	be rejected
<ul> <li>Monitoring and Reports</li> </ul>	
🕨 🥞 System Administration	

5. Accédez à Access Policies > Access Services > Default Network Access > Authorization afin de vérifier le profil d'autorisation.

Vous pouvez personnaliser dans quelles conditions vous autorisez un utilisateur à accéder au réseau et quel profil d'autorisation (attributs) vous passerez une fois authentifié. Cette granularité est uniquement disponible dans ACS 5.x. Dans cet exemple, les options Emplacement, Type de périphérique, Protocole, Groupe d'identités et Méthode d'authentification EAP sont sélectionnées.

CISCO DECURE ALS	
Apress Folkers > Apress Territors > Default Network Access > Automotion	
+ (h Anthendi Resources	
Standard Procey     Stores     Stores	
So Policy Elements     Instance Access Authorization Precy	
Filer Status Matter Equals ClearFilter Ga V	
Access Benices     States Name     States Name     ND01_acation     Time And Date     Authorization Profiles     Hit Count	
O Default Device Admin     No defaits display	
Advantage     Mosile Firefox     X	
Ci Monitoring and Reports	
System Administration	
Cadast Eservice defined or no enabled rule matches. Permit Access 0	_
Cesate(* Depticate(* Edit Delots A Move1e V Cester	HE Count

- 6. Cliquez sur OK, puis sur Save Changes.
- 7. L'étape suivante consiste à créer une règle. Si aucune règle n'est définie, l'accès LAP est autorisé sans aucune condition.
- 8. Cliquez sur Create > Rule-1. Cette règle s'applique aux utilisateurs du groupe « Utilisateurs LAP ».

cisco Cisco Secure Al	CS	economie) S
+ 🕀 My Workspace	Access Policies > Access Services > Definit Network Access > Authorization	
+ 🎲 Network Resources	Standard Balleyi Evention Deller	
+ 🎎 Users and identity Stores		
Policy Elements	Net Caco Secure ACS - Moralis Finetica	×
- 🅵 Access Policies	Fin 192.168.150.24 https://192.168.150.24/acsadmin/PolicyInputAction.do	<u>.</u>
Access Services     Service Selection Rules     O Default Device Admin     O Default Network Access     Identity     Access     delotant	Image: The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.	n
+ 📳 Monitoring and Reports	Conditione	<b>-</b>
+ 🥂 System Administration	PINDGLocator: in PIAILocators:LAB Select	
	In a select in a select select select	i
	Protocol: match - Radius Select	i L
	✓ Identity Group: In ▲ All Groups LAP users Select	
	Eap Authentication Method: AMA	
	Authoritzation Profiles:         Permit Access         You may select multiple authorization profiles. Attributed fined in multiple profiles will use the value from the profile defined.         Select       Deselect	/es e first
	OK Cancel	Help
	Default     Eno seles defined or no enabled rule matches	
	CreateI DuplicateI Edit Delete A Move to	
	Save Changes Discard Changes	

9. Cliquez sur Enregistrer les modifications. Si vous souhaitez que les utilisateurs ne répondant pas aux conditions soient refusés, modifiez la règle par défaut pour dire « Refuser l'accès ».

cisco Cisco Secure A	CS	iadmin SALIX-ACSS2(Primary) Log Dat About In						
Ally Meritspace     My Meritspace     More Resources     Multi-Resources     Multi-Resources     Policy Elements	ISBADO ISBADO Access Policies > Access Services > Default lietwork Access > Authorization ISBADO IS							
Access Bences     Access Bences     Access Bences     Bences     Bences     Default Device Admin     Device Admin	Status         Non-training         Conditions           Image: Imag	Results Hill So Authenitication Method Authonization Profiles N/IP Permit Access Permi						
	Save Changes Discard Changes							

10. La dernière étape consiste à définir des règles de sélection des services. Utilisez cette page pour configurer une stratégie simple ou basée sur des règles afin de déterminer le service à appliquer aux demandes entrantes. Exemple :

A My Workspace	AC	cess P									
(3) Network Resources		Single result selection Rule based result selection									
🖀 Users and identity Stores											
Sy Policy Elements		Filter	Stat	us *	Natchilt	Equals V Enabled V Clear Fi	iter   Go   -				
👗 Access Policies						Conditions	Bocalts				
Annoss Reninss				Status	Name	Protocol	Service	Hit Count			
Default Device Admin		1			Rule-1	match Radius	Default Network Access	0			
O Detault Network Access		2	Г		Rule-2	match Tacacs	Default Device Admin	0			
Identity Authorization											
<ul> <li>Ø deleterne</li> </ul>	11										
The state of the sector											

## Vérifier

Une fois que la norme 802.1x est activée sur le port du commutateur, tout le trafic, à l'exception du trafic 802.1x, est bloqué par le port. Le LAP, qui est déjà enregistré sur le WLC, est dissocié. Un autre trafic n'est autorisé à transiter qu'après une authentification 802.1x réussie. L'enregistrement réussi du LAP sur le WLC après que le 802.1x est activé sur le commutateur indique que l'authentification LAP est réussie.

Console AP :

#### <#root>

```
*Jan 29 09:10:24.048: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
   192.168.75.44:5246
*Jan 29 09:10:27.049: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
   192.168.75.44:5247
!--- AP disconnects upon adding dot1x information in the gig0/11.
*Jan 29 09:10:30.104: %WIDS-5-DISABLED: IDS Signature is removed and disabled.
*Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
*Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
*Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11RadioO, changed state to
   administratively down
*Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
   administratively down
*Jan 29 09:10:30.186: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
   reset
*Jan 29 09:10:30.201: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Jan 29 09:10:30.211: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:10:30.220: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
   reset
Translating "CISCO-CAPWAP-CONTROLLER"...domain server (192.168.150.25)
*Jan 29 09:10:36.203: status of voice_diag_test from WLC is false
```

*!---* Authentication is successful and the AP gets an IP.

Translating "CISCO-CAPWAP-CONTROLLER.Wlab"...domain server (192.168.150.25) \*Jan 29 09:11:37.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer\_ip: 192.168.75.44 peer\_port: 5246 \*Jan 29 09:11:37.000: %CAPWAP-5-CHANGED: CAPWAP changed state to \*Jan 29 09:11:37.575: %CAPWAP-5-DTLSREQSUCC: DTLS connection created successfully peer\_ip: 192.168.75.44 peer\_port: 5246 \*Jan 29 09:11:37.578: %CAPWAP-5-SENDJOIN: sending Join Request to 192.168.75.44 \*Jan 29 09:11:37.578: %CAPWAP-5-CHANGED: CAPWAP changed state to JOIN \*Jan 29 09:11:37.748: %CAPWAP-5-CHANGED: CAPWAP chan wmmAC status is FALSEged state to CFG \*Jan 29 09:11:38.890: %LINK-3-UPDOWN: Interface Dot11RadioO, changed state to down \*Jan 29 09:11:38.900: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset \*Jan 29 09:11:38.900: %CAPWAP-5-CHANGED: CAPWAP changed state to UP \*Jan 29 09:11:38.956: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller 5508-3 \*Jan 29 09:11:39.013: %CAPWAP-5-DATA\_DTLS\_START: Starting Data DTLS handshake. Wireless client traffic will be blocked until DTLS tunnel is established. \*Jan 29 09:11:39.013: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up \*Jan 29 09:11:39.016: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[0] \*Jan 29 09:11:39.028: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to down \*Jan 29 09:11:39.038: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to reset \*Jan 29 09:11:39.054: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up \*Jan 29 09:11:39.060: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to down \*Jan 29 09:11:39.069: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset \*Jan 29 09:11:39.085: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up \*Jan 29 09:11:39.135: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[1]DTLS keys are plumbed successfully. \*Jan 29 09:11:39.151: %CAPWAP-5-DATA\_DTLS\_ESTABLISHED: Data DTLS tunnel established. \*Jan 29 09:11:39.161: %WIDS-5-ENABLED: IDS Signature is loaded and enabled

!--- AP joins the 5508-3 WLC.

Journaux ACS :

1. Affichez le nombre d'occurrences :

Si vous vérifiez les journaux dans les 15 minutes qui suivent l'authentification, assurez-vous d'actualiser le nombre d'accès. Sur la même page, en bas, vous avez un onglet Nombre de visites.

cisco Cisco Secure A	CS										
+ 🛞 My Workspace	Access Policies > Access Services > Service Selection Rules										
+ 🎲 Network Resources	Single result selection     Rule based result selection     Service Selection Policy										
Users and Identity Stores											
Policy Elements	Filter	Filter, Status • Match if, Equals • Enabled • Clear Filter Go •									
<ul> <li>Access Policies</li> </ul>	-				Conditions	Results					
<ul> <li>Access Services</li> </ul>			Status	Name	Protocol	Service	Hit Count				
El Service Selección Roles     O Default Device Admin     O Default Network Access	1			Bule-1	match Radius	Default Network Access	1				
	2			Rule-2	match Tacaca	Default Device Admin	0				
Identity Authorization > 2 deleterne											
+ 📳 Monitoring and Reports											
+ 🍓 System Administration											



2. Cliquez sur Surveillance et rapports et une nouvelle fenêtre contextuelle s'affiche. Cliquez sur Authentications -RADIUS -Today. Vous pouvez également cliquer sur Details afin de vérifier quelle règle de sélection de service a été appliquée.

							* * * * * * * * * * * * *	Launch Interact	live Thewar
Showing Page	1 of 1			I Gata i	Page: Go				
AAA Protocol > RADIL	US Authentication								
Authentication Status : P Date : J	Pass of Pail January 29, 2012 ( <u>Last 30 Ni</u>	naha i LastHouri	Last 12 Hours   To	day i <u>Yesferdar i Last 7 Das</u>	s (Last 30 Davs )				
Generated on January 25	2012 9:15:01 PM EST								
Reload	-Cick for details 9 -rea	as over item for	additional informat	úan .					
Logged At	RADUS NAS Status Failure Dataits	Usemame	MACIP Address	Access Service	Authentication Method	Network Device	NAS IP Address	NAS Port ID	CTS Security Gr
Jan 29.12 9:11:12 966 P	w v a	3502e CC	CEF-68-FA-53-19	Default Network Access	EAP-FAST (EAP-NSCHAP\2)	3560-Switch-LAP	192.168.153.10	GigablEthemet0/11	1.1.1.1.1.1

# Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

# Informations connexes

- Système de contrôle d'accès sécurisé (ACS) de Cisco
- <u>Assistance et documentation techniques Cisco Systems</u>

#### 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.