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

Table des matières

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 Conventions relatives aux conseils techniques Cisco.

Informations générales

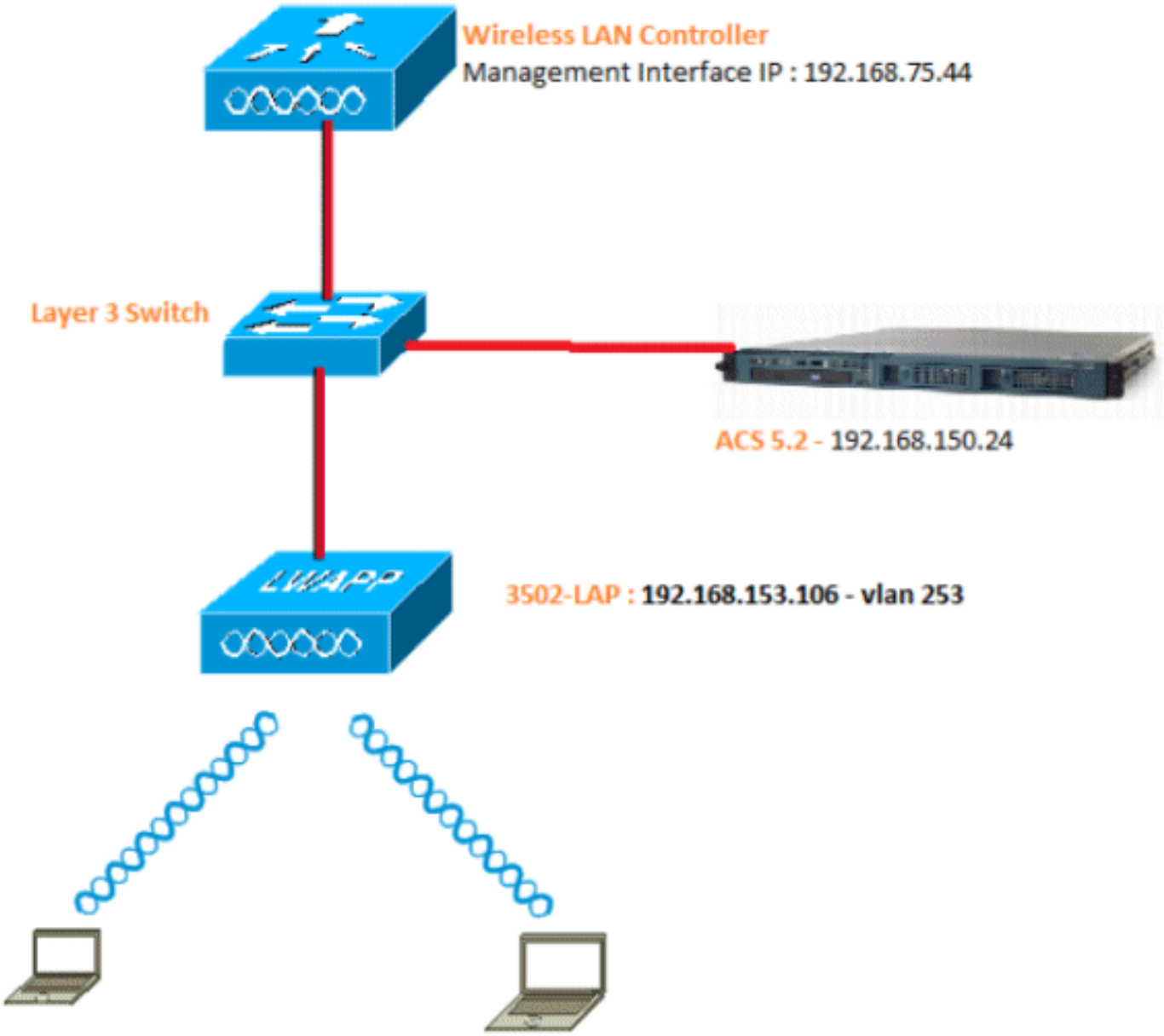
Les LAP ont installé en usine des certificats X.509 - signés par une clé privée - qui sont gravés dans le périphérique au moment de la fabrication. Les LAP utilisent ce certificat afin de s'authentifier auprès du WLC lors du processus de jointure. Cette méthode décrit une autre façon d'authentifier les 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.

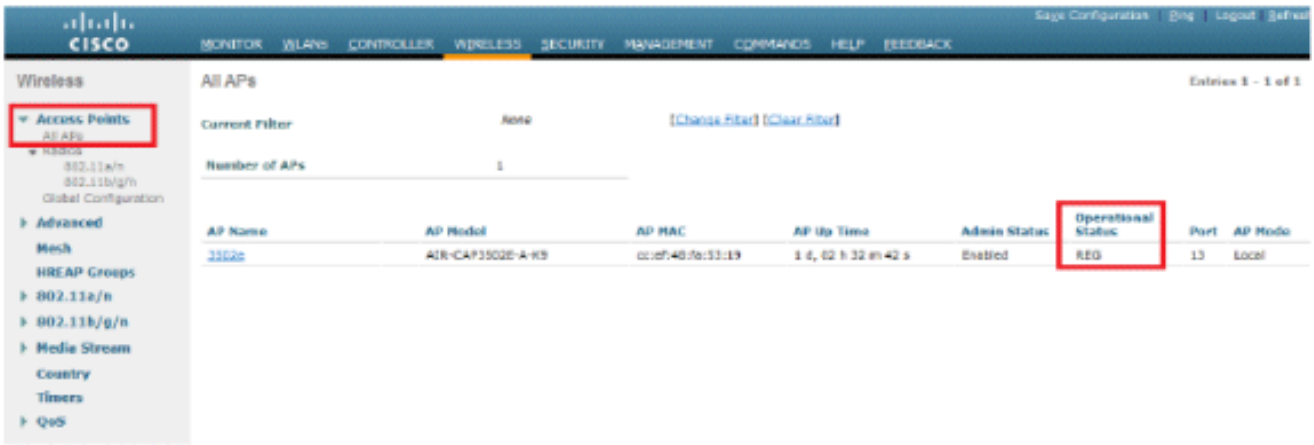
Configurer le LAP

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.

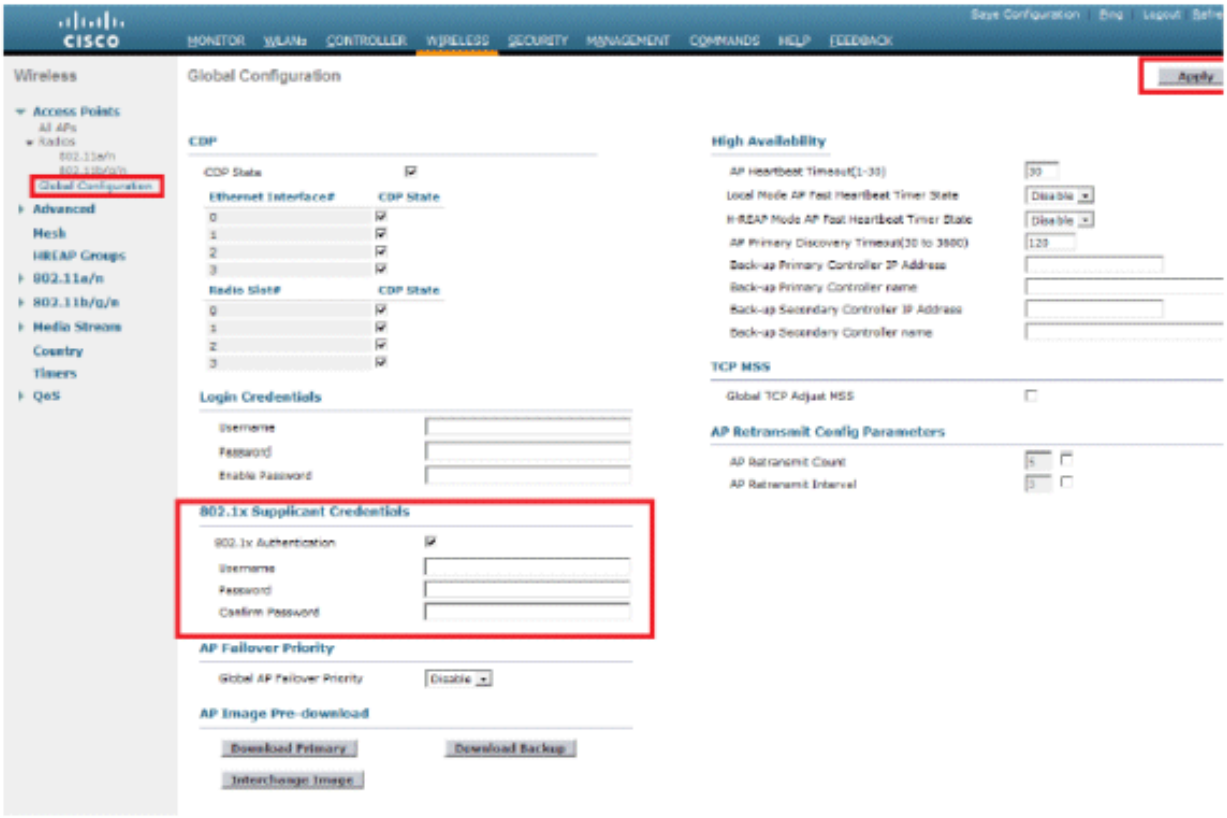


2. Vous pouvez configurer les informations d'identification 802.1x (nom d'utilisateur/mot de passe) pour tous les LAP de deux manières :

   - 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.

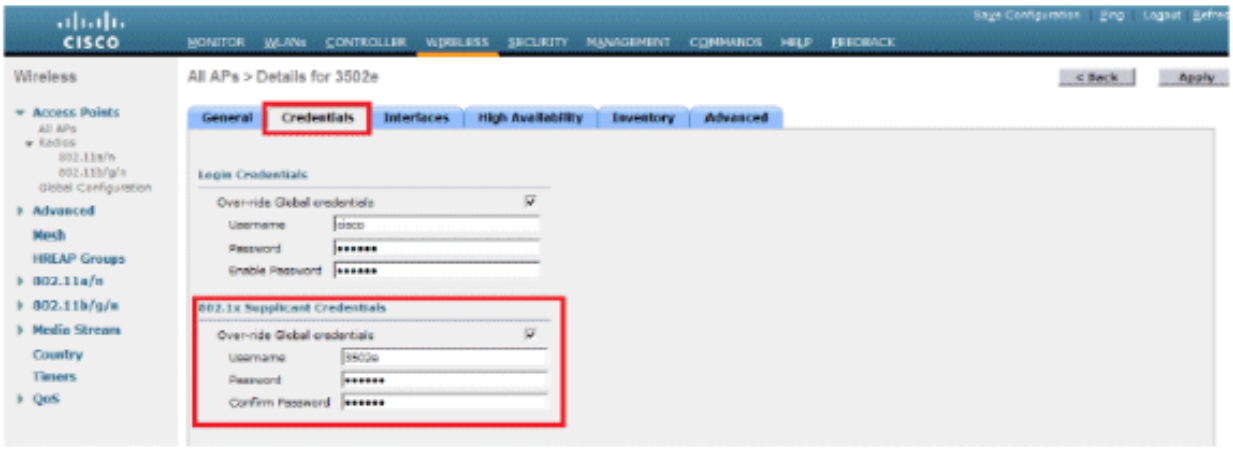


- Individuellement

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

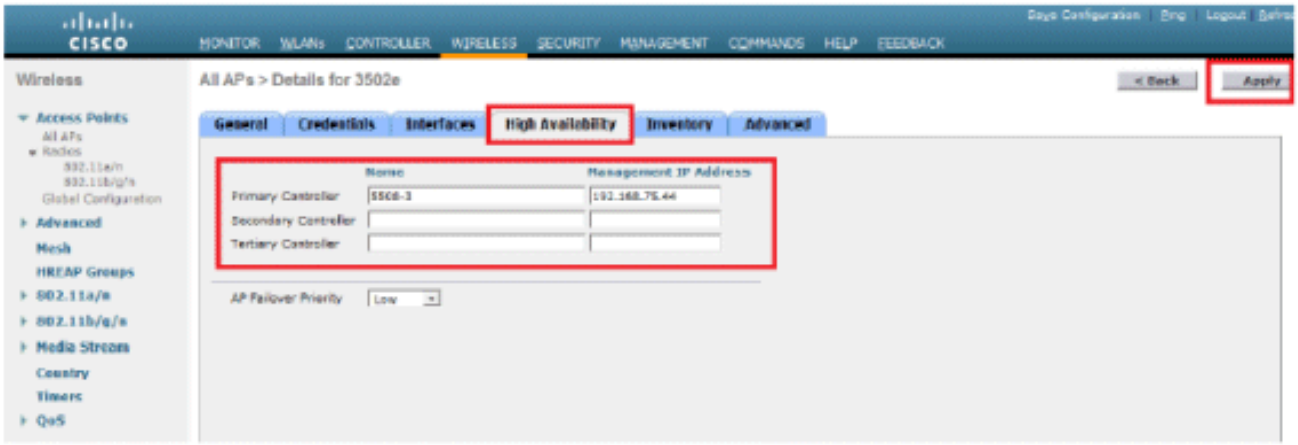
  a. Accédez à Wireless > All APs, et sélectionnez le point d'accès concerné.

  b. Ajoutez le nom d'utilisateur et le mot de passe dans les champs 802.1x Supplicant Credentials.



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.



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#lwapp 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. Configurer les ressources réseau
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®.

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.

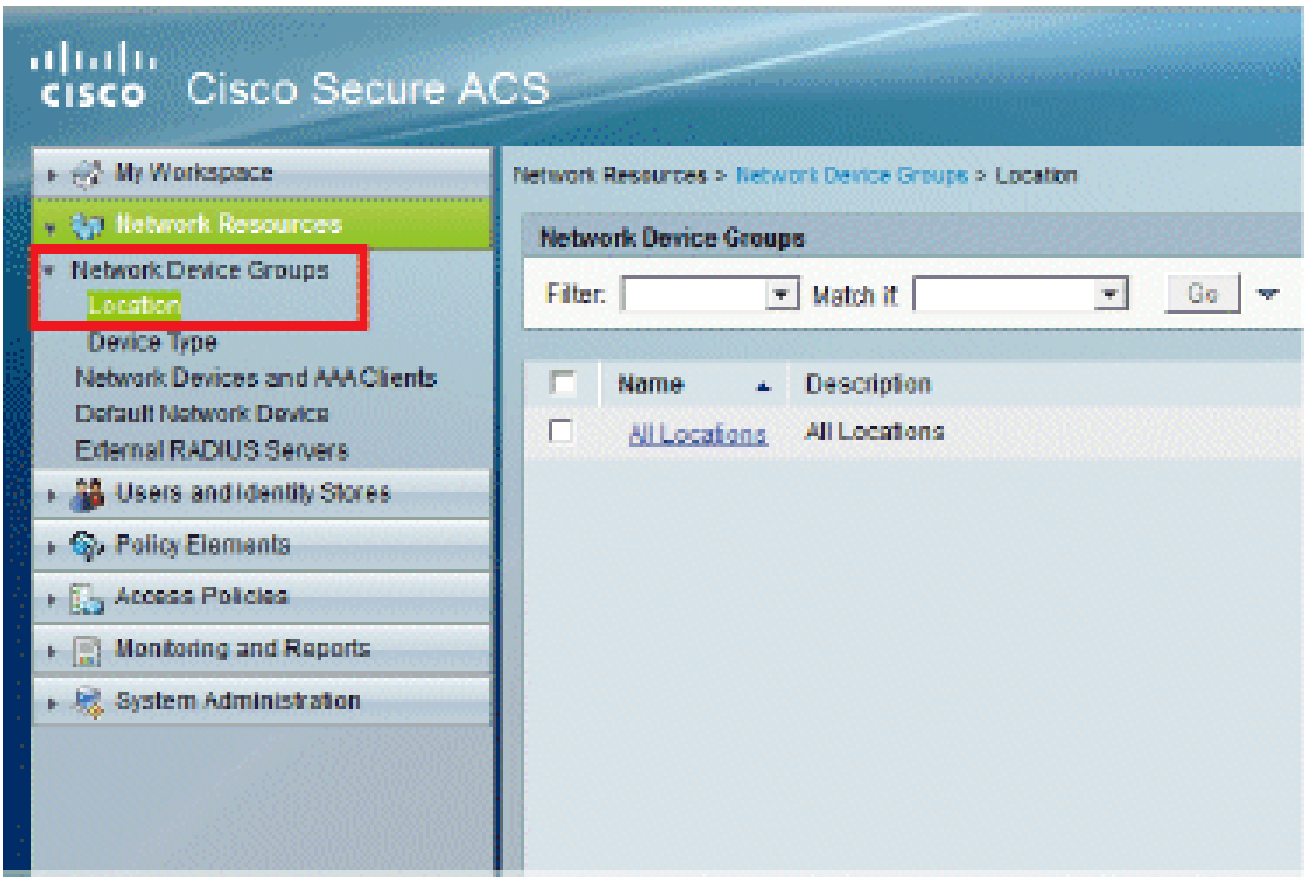
Cette procédure explique comment ajouter le commutateur en tant que client AAA sur le serveur RADIUS afin que le commutateur puisse transmettre les informations d'identification de l'utilisateur du LAP au serveur RADIUS.

Procédez comme suit :

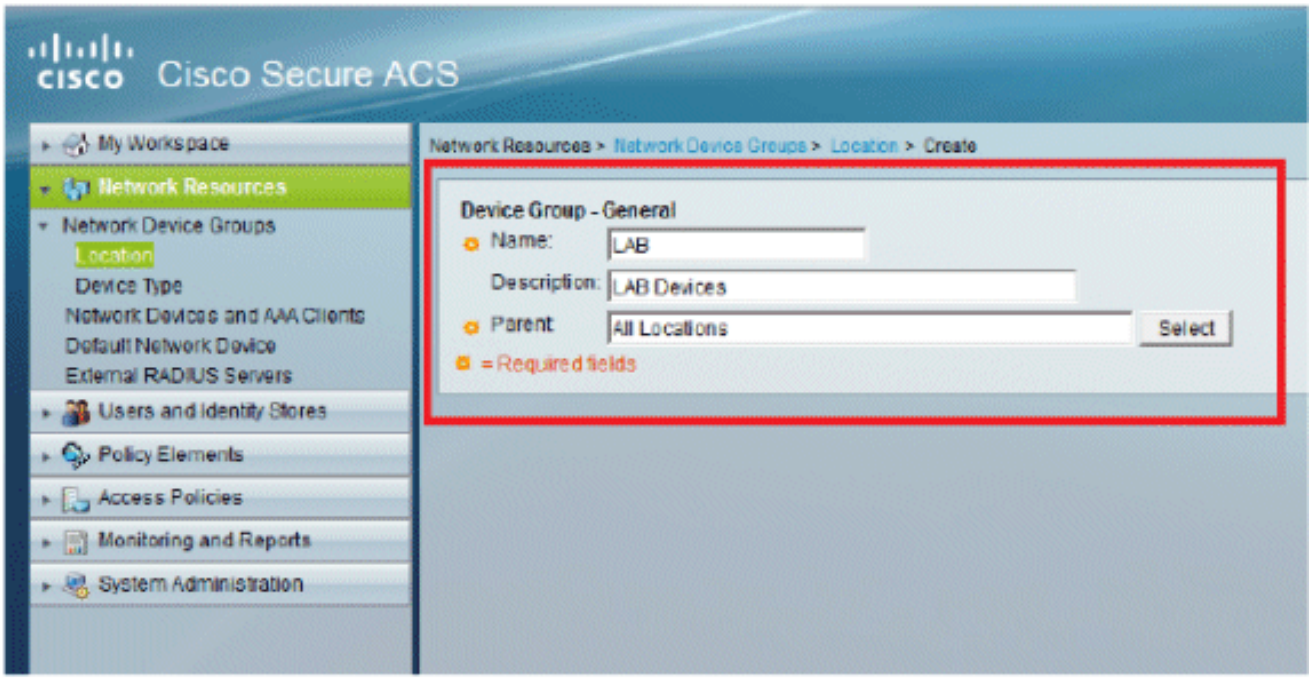
1. Dans l'interface graphique utilisateur ACS, cliquez sur Network Resources.

2. Cliquez sur Network Device Groups.

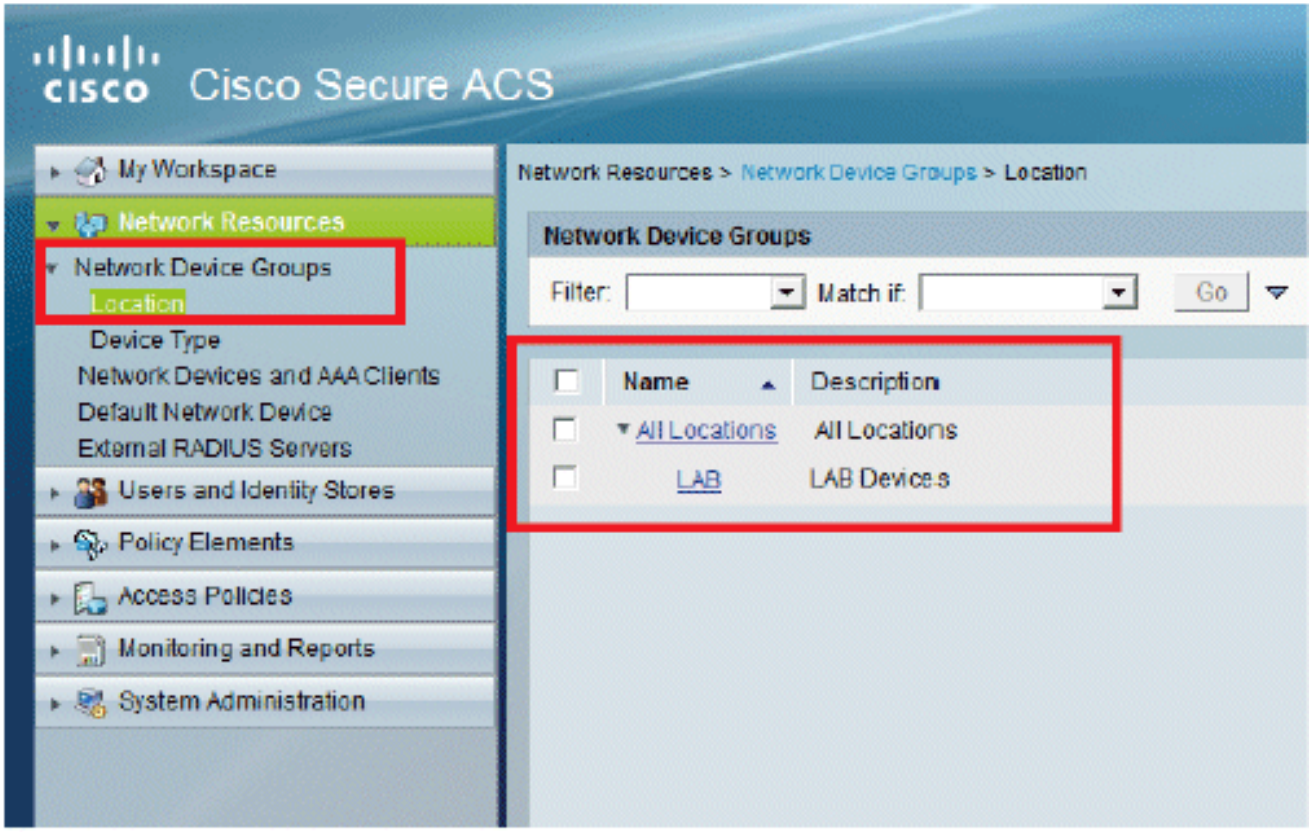
3. Accédez à Location > Create (en bas).



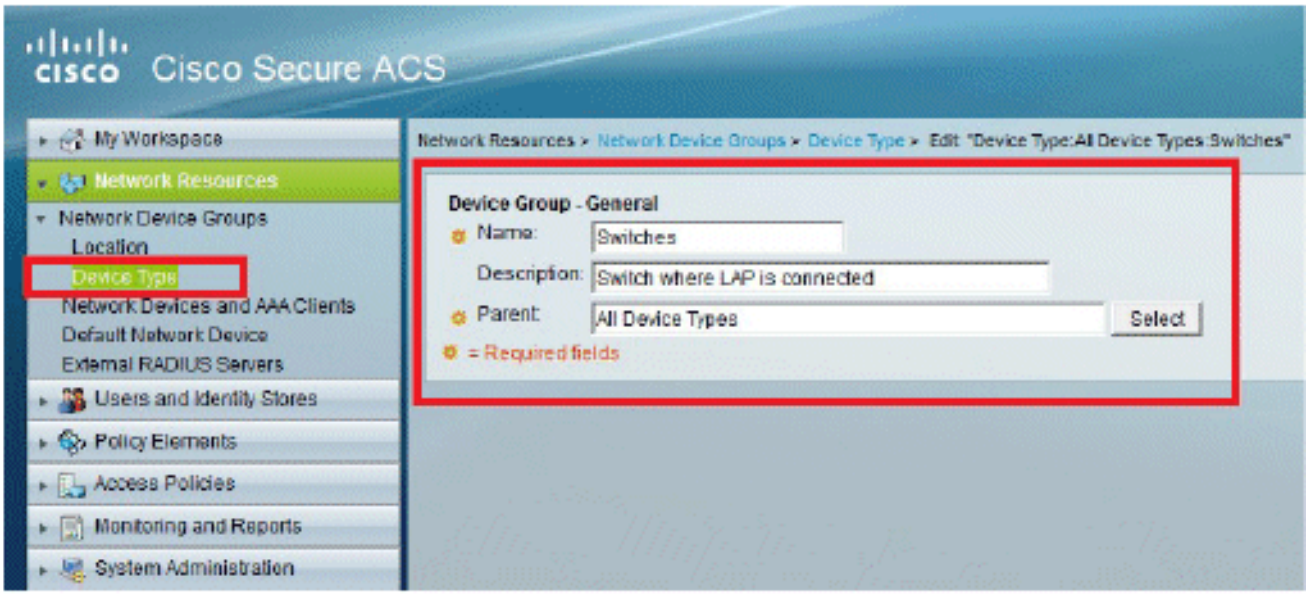
4. Ajoutez les champs requis et cliquez sur Submit.



5. La fenêtre est actualisée :



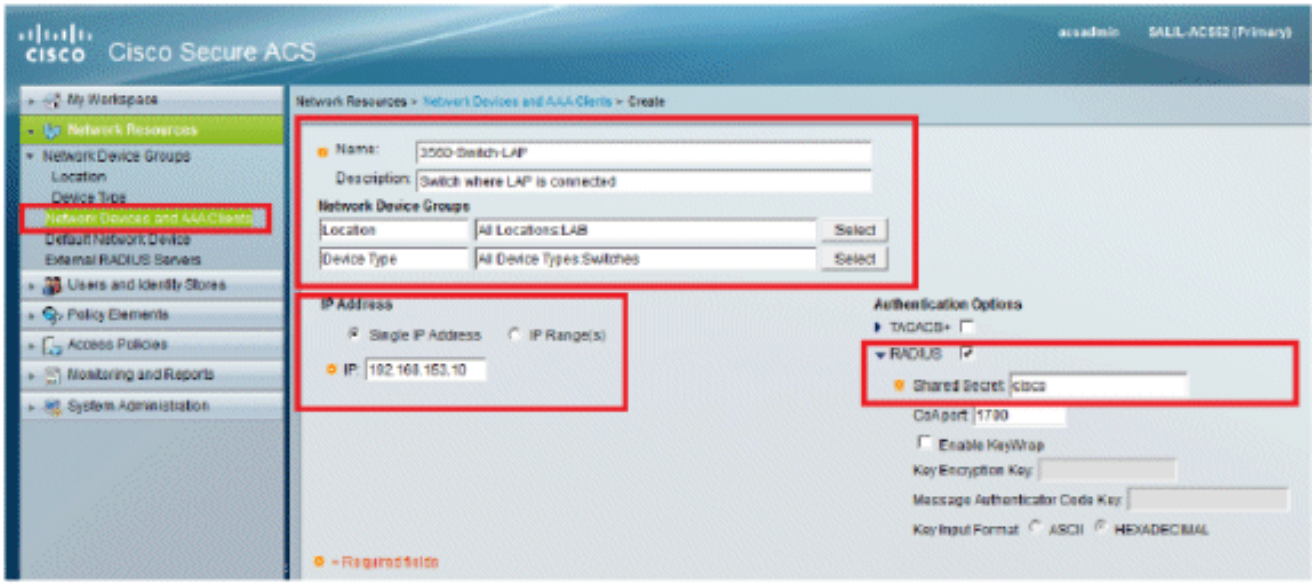
6. Cliquez sur Device Type > Create.



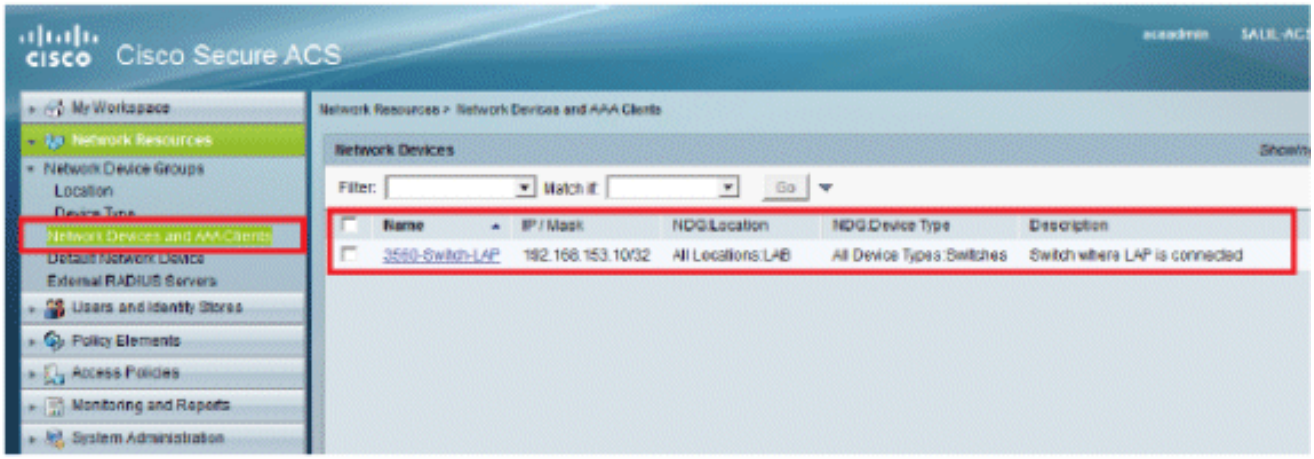
7. Cliquez sur Submit. Une fois terminée, la fenêtre est actualisée :

8. Accédez à Ressources réseau > Périphériques réseau et clients AAA.

9. Cliquez sur Create, et remplissez les détails comme indiqué ici :



10. Cliquez sur Submit. La fenêtre est actualisée :

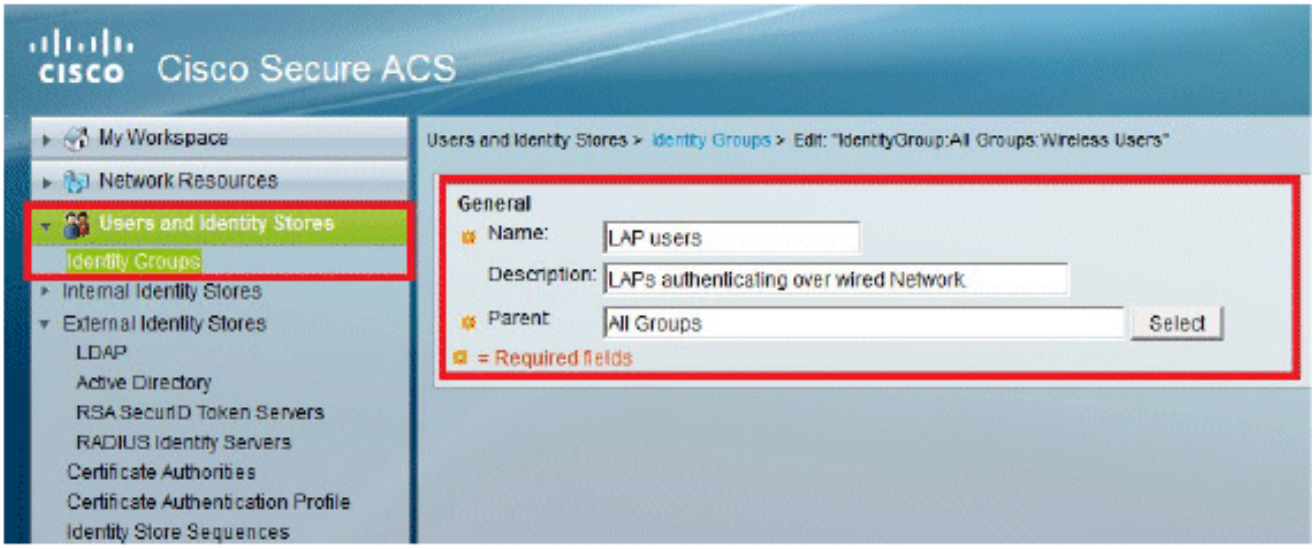


Configurer des utilisateurs

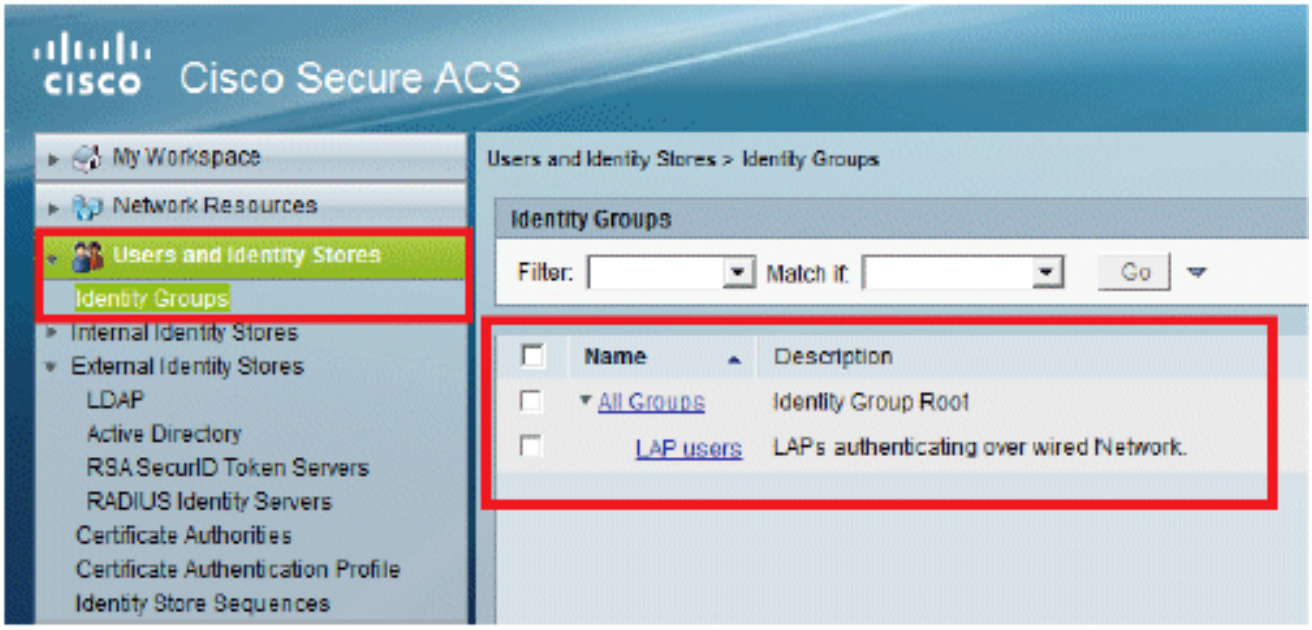
Dans cette section, vous allez voir comment créer un utilisateur sur l'ACS configuré précédemment. Vous attribuerez l'utilisateur à un groupe appelé « utilisateurs LAP ».

Procédez comme suit :

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

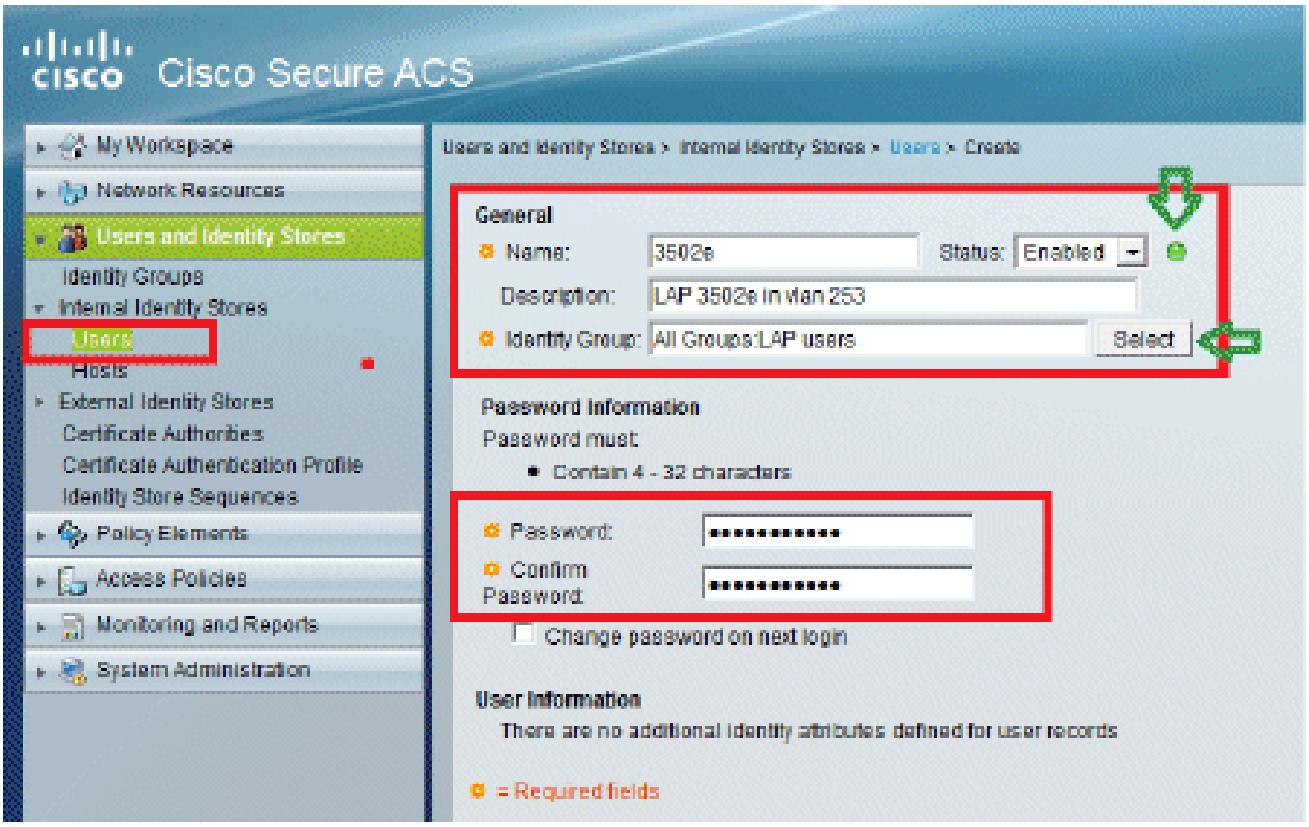


2. Cliquez sur Submit.

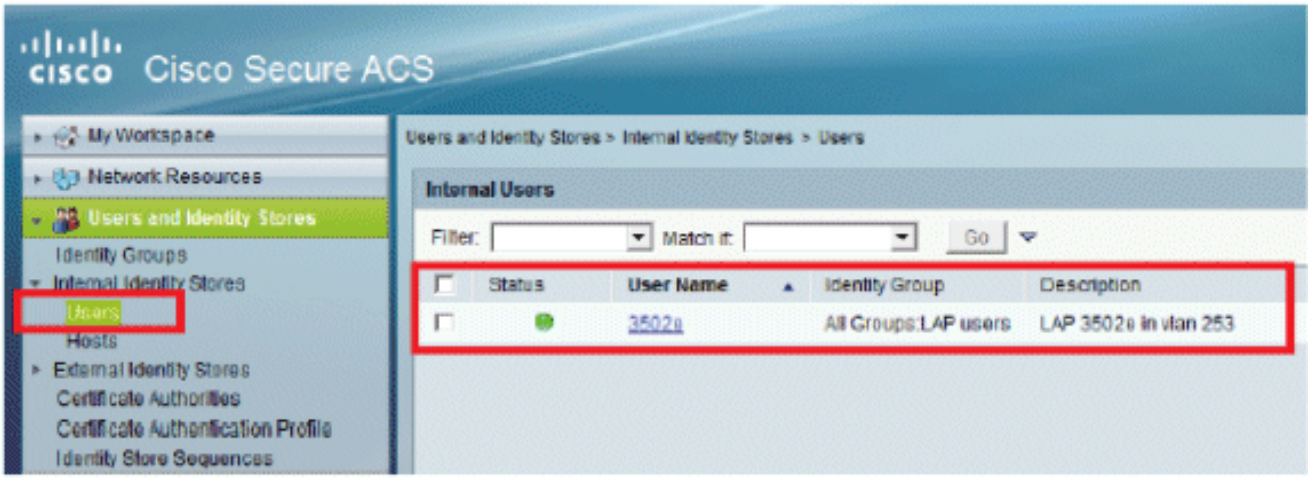


3. Créez 3502e et attribuez-le au groupe « Utilisateurs LAP ».

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

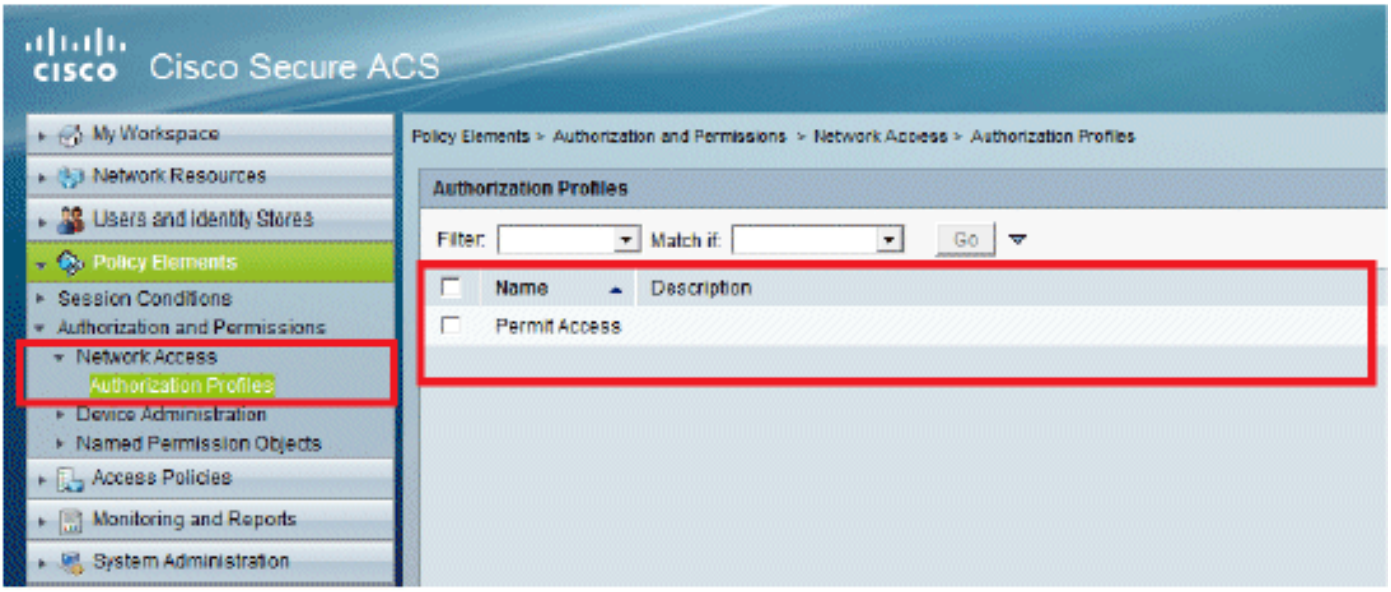


5. Vous verrez les informations mises à jour :



Définir des éléments de stratégie

Vérifiez que Permit Access est défini.

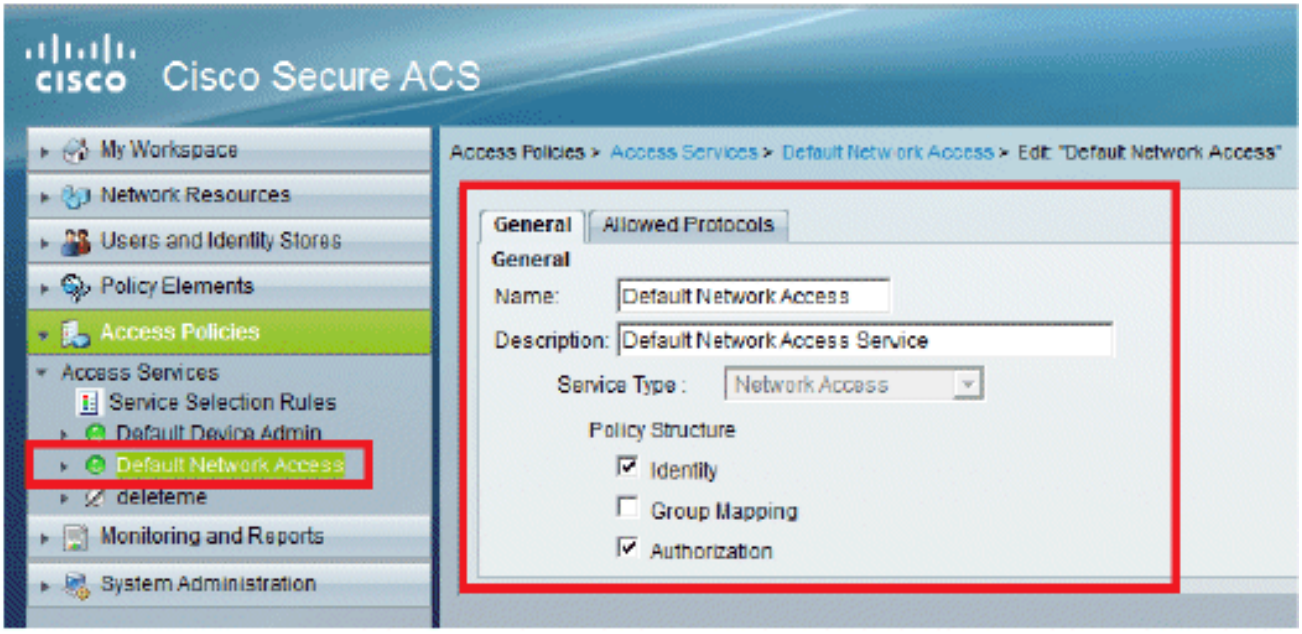


Appliquer les stratégies d'accès

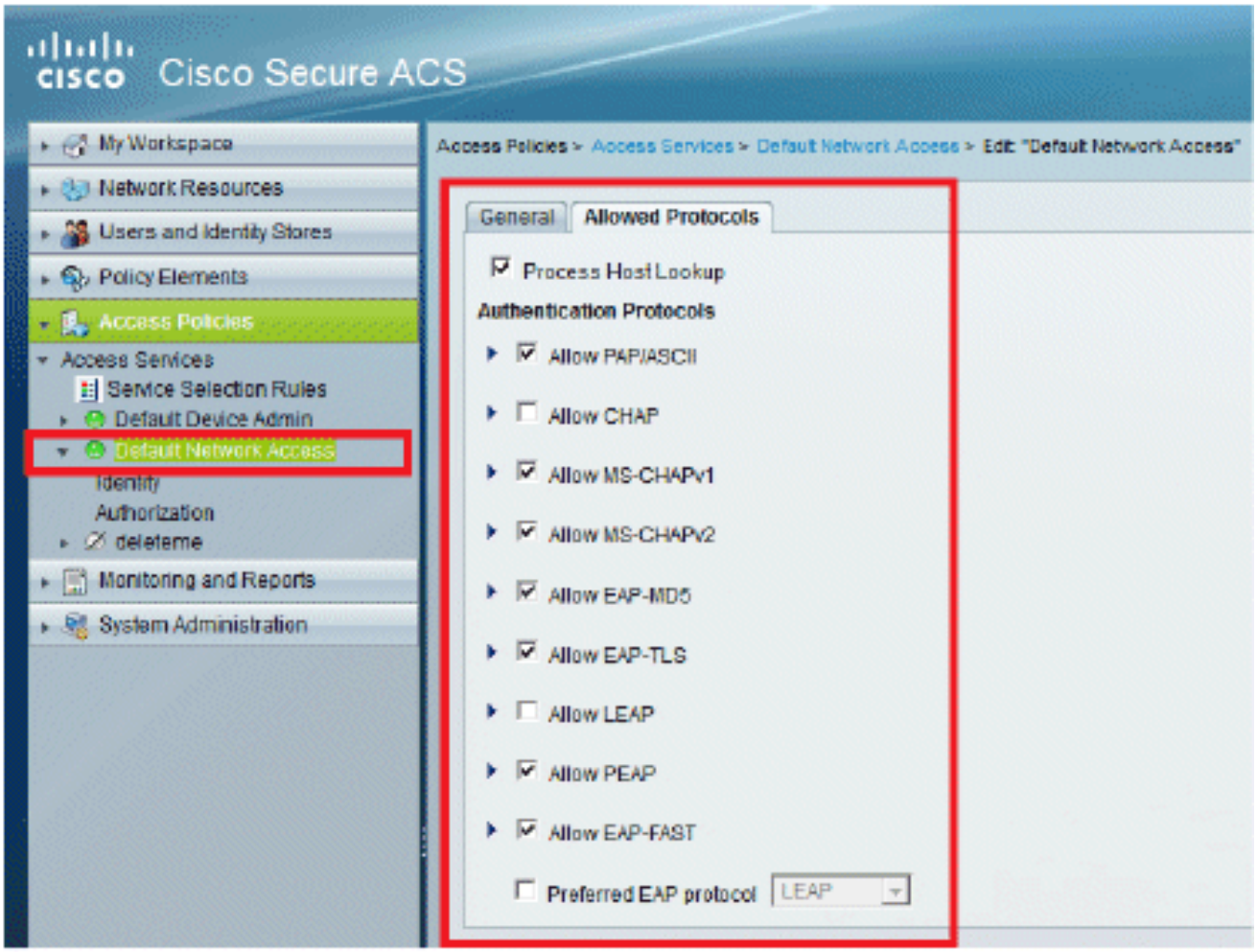
Dans cette section, vous allez sélectionner EAP-FAST comme méthode d'authentification utilisée pour les LAP afin de s'authentifier. Vous allez ensuite créer des règles basées sur les étapes précédentes.

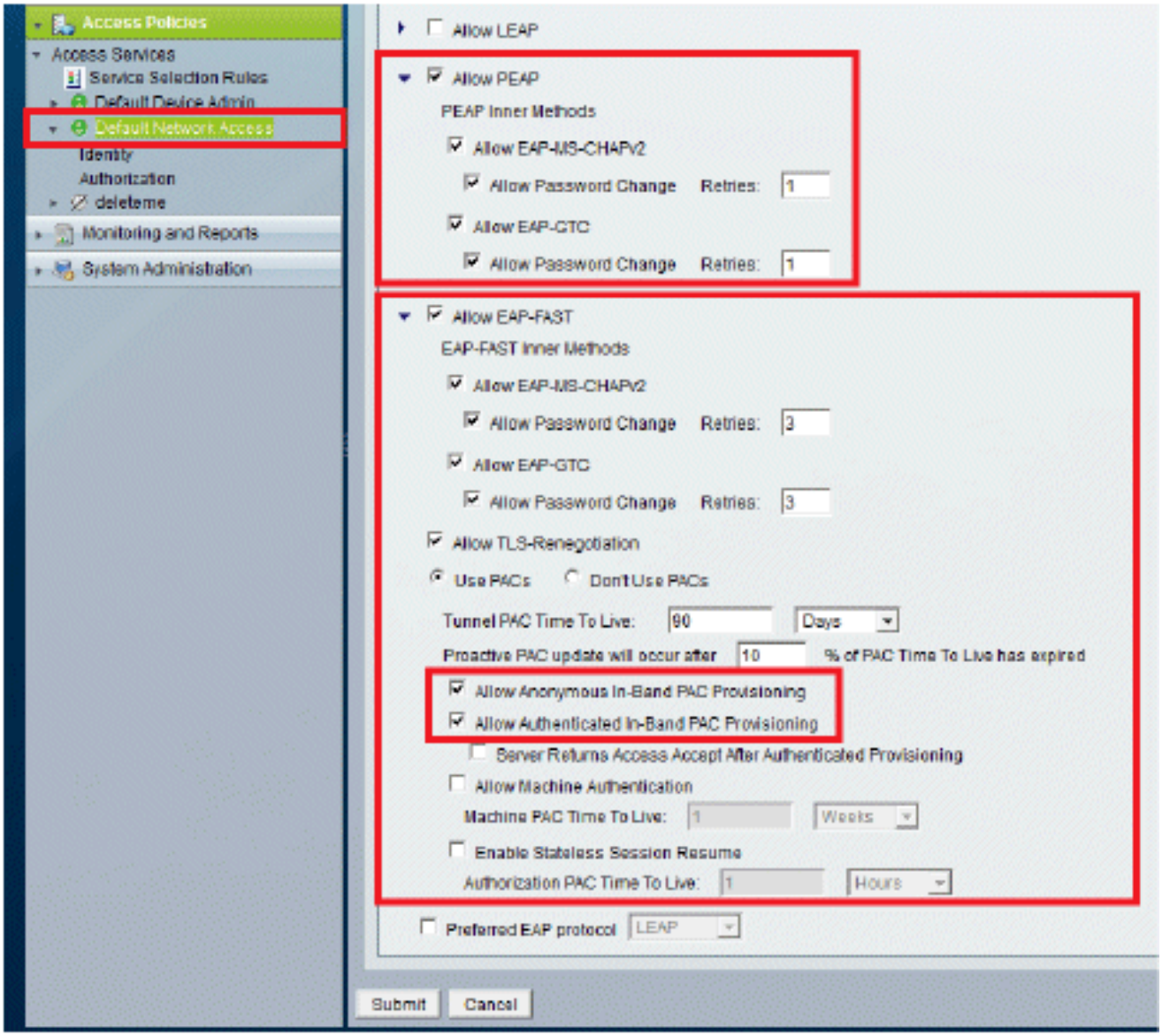
Procédez comme suit :

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



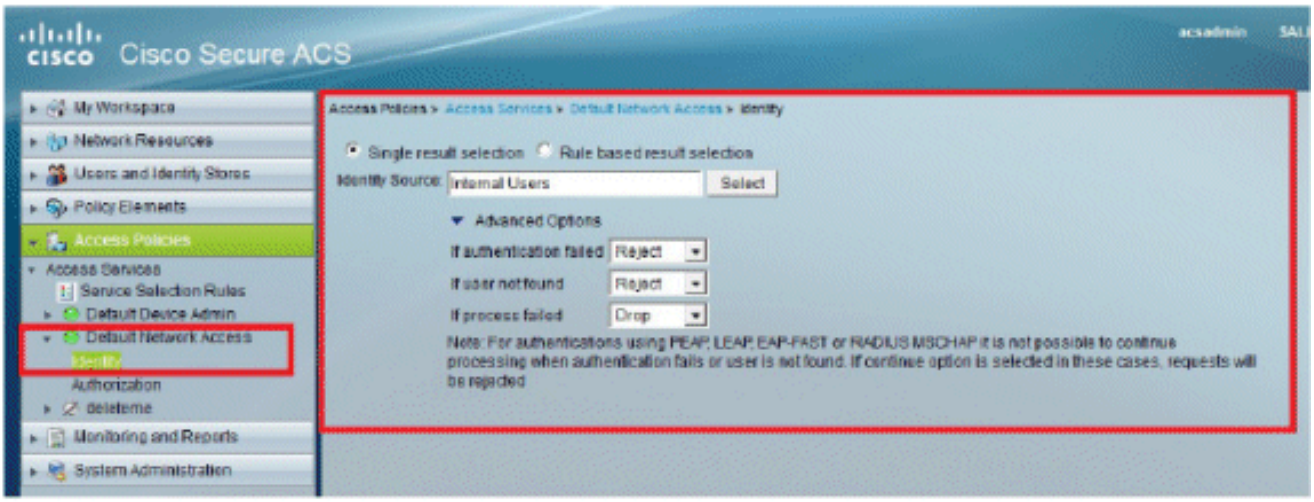
2. Assurez-vous que vous avez activé EAP-FAST et Anonymous In-Band PAC Provisioning.





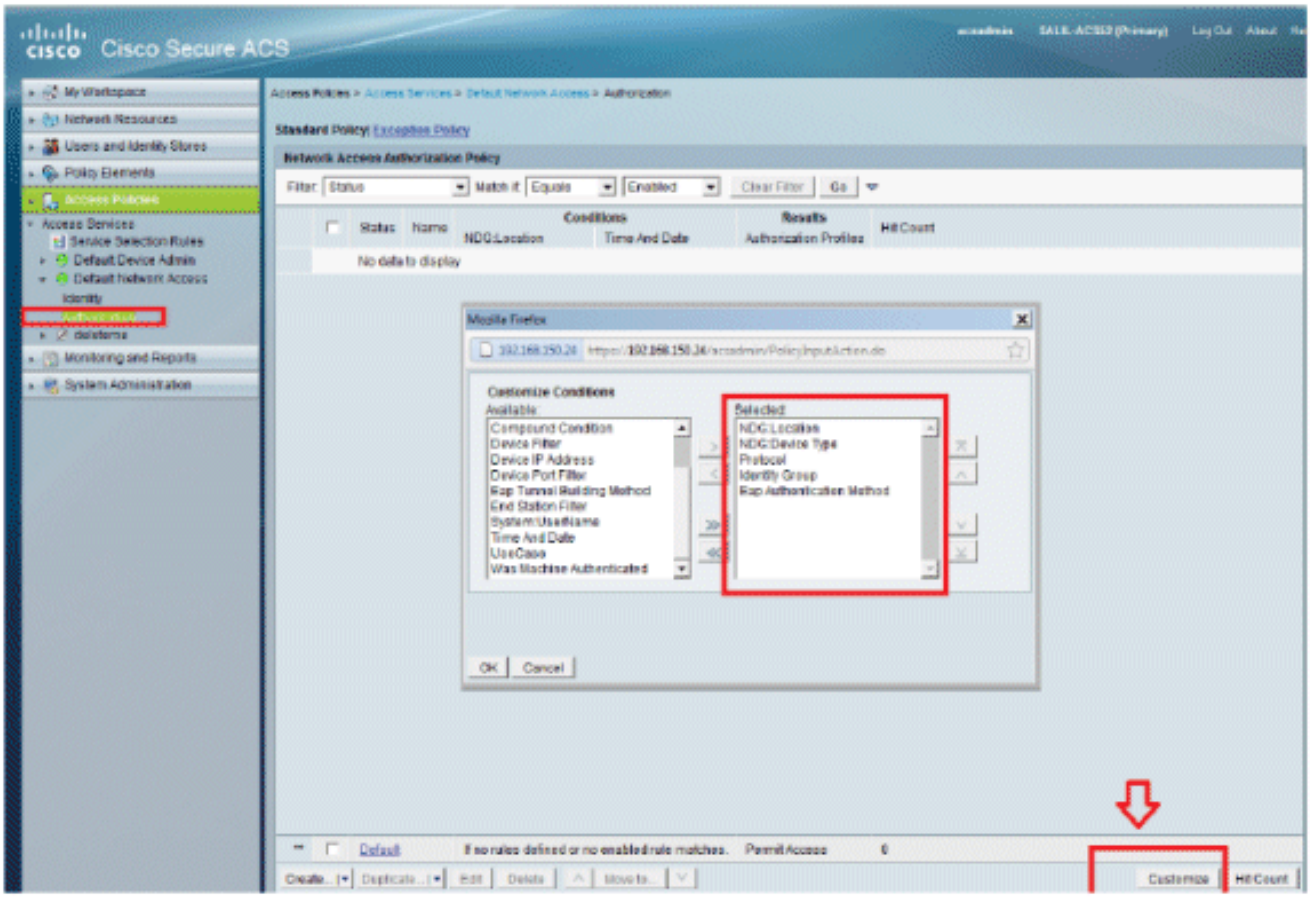
3. Cliquez sur Submit.

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.



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

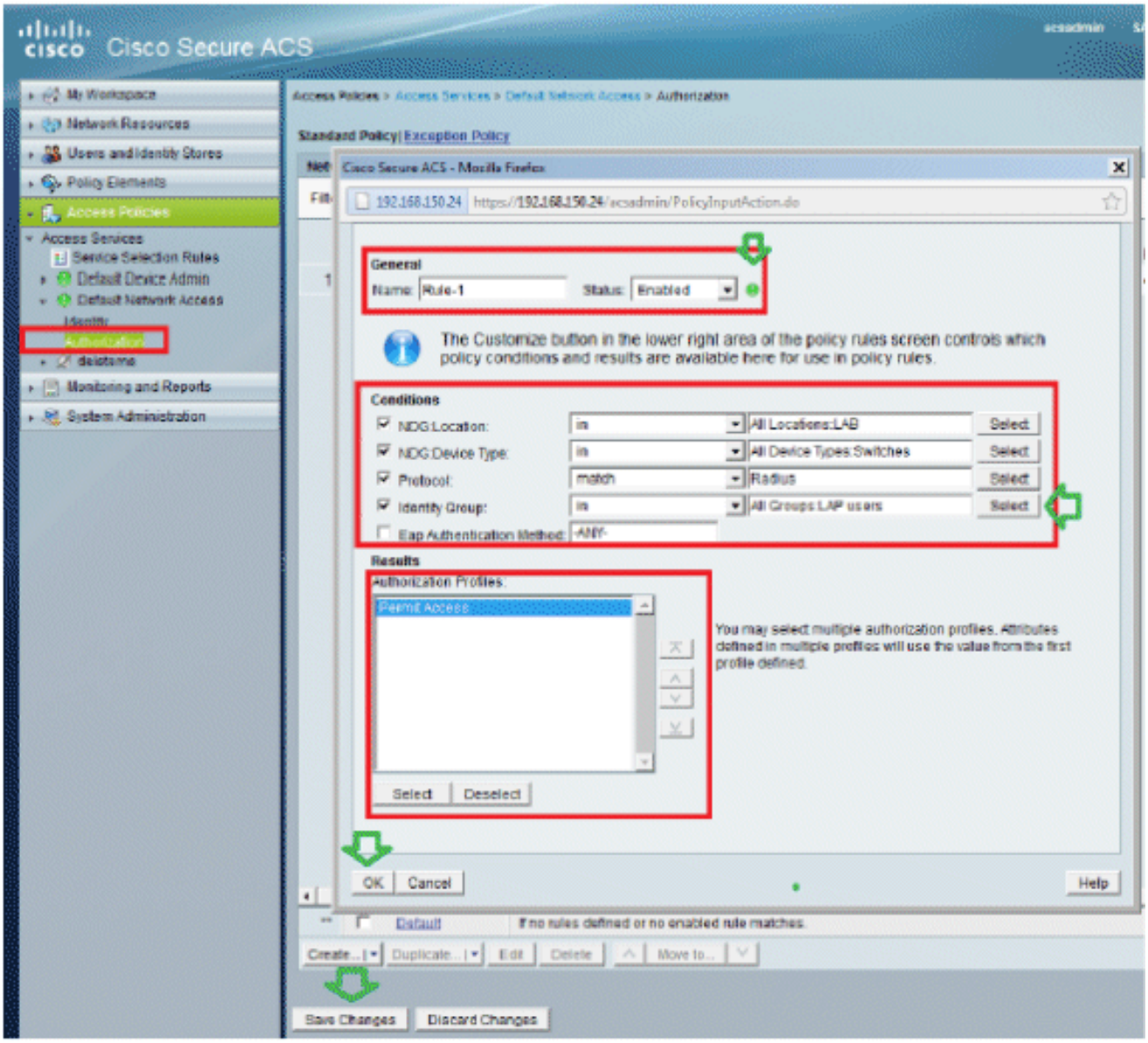
   Vous pouvez personnaliser dans quelles conditions vous autorisez un utilisateur à accéder au réseau et quel profil d'autorisation (attributs) vous passerez une fois authentifié. Cette granularité est uniquement disponible dans ACS 5.x. Dans cet exemple, les options Emplacement, Type de périphérique,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



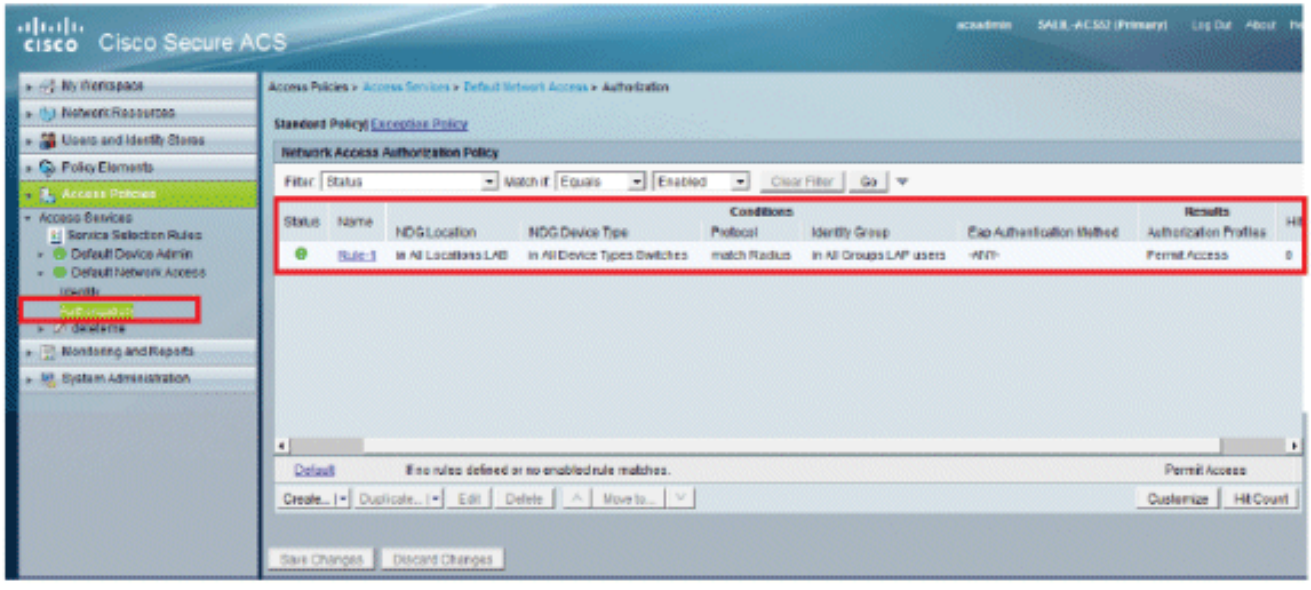
6. Cliquez sur OK, puis sur Save Changes.

7. L'étape suivante consiste à créer une règle. Si aucune règle n'est définie, l'accès LAP est autorisé sans aucune condition.

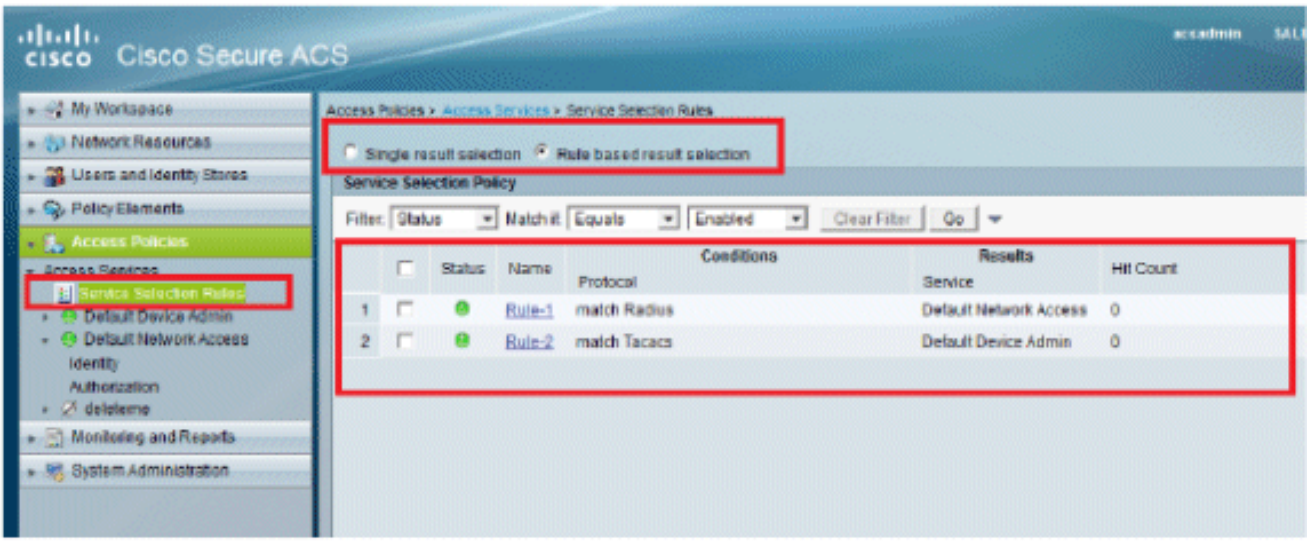
8. Cliquez sur Create > Rule-1. Cette règle s'applique aux utilisateurs du groupe « Utilisateurs LAP ».



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 ».



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 :



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>

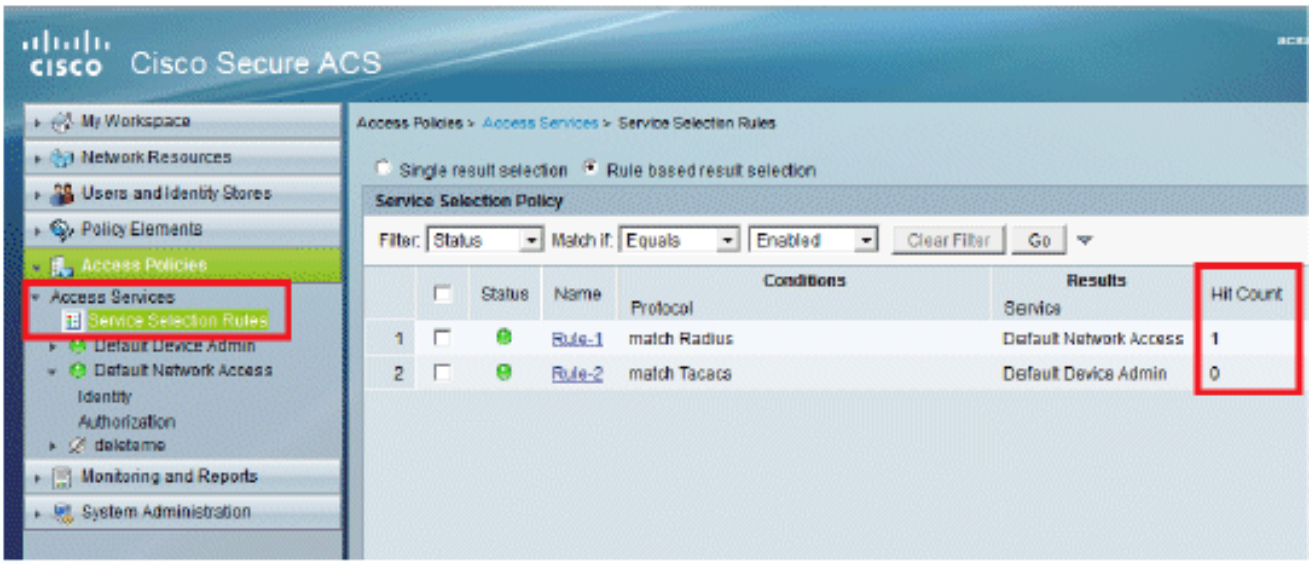
```
*Jan 29 09:10:24.048: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
   192.168.75.44:5246
*Jan 29 09:10:27.049: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
   192.168.75.44:5247

!--- 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 Dot11Radio0, 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
```

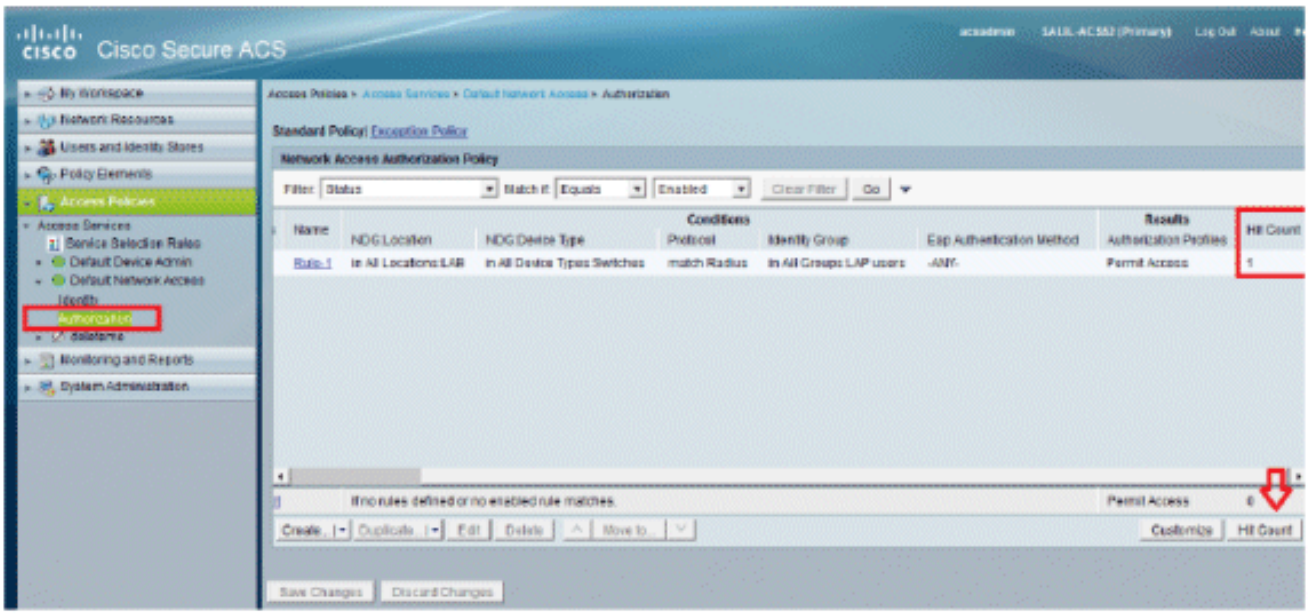
```
*Jan 29 09:11:05.927: %DOT1X_SHIM-6-AUTH_OK: Interface GigabitEthernet0 authenticated [EAP-FAST] *Jan 29

!--- 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 Dot11Radio0, 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 :

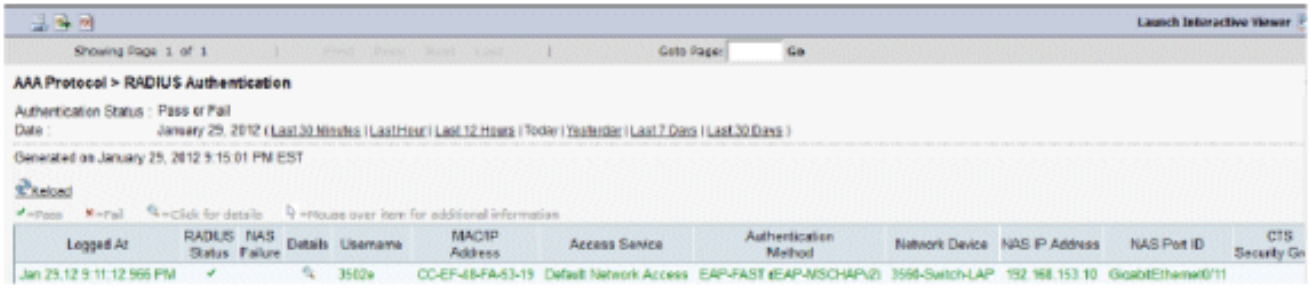
1. Affichez le nombre d'occurrences :

   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.





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.



Dépannage

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

Informations connexes

- Système de contrôle d’accès sécurisé (ACS) de Cisco
- Assistance et documentation techniques - Cisco Systems

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.