Exemple de configuration de TACACS+ sur un point d'accès Aironet pour l'authentification de la connexion à l'aide de l'interface utilisateur graphique

Contenu

Introduction

Ce document explique comment activer les services TACACS Plus (TACACS+) sur un point d'accès Cisco Aironet afin d'effectuer l'authentification de connexion à l'aide d'un serveur TACACS+.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Connaissance de la configuration des paramètres de base sur les points d'accès Aironet
- Connaissance de la configuration d'un serveur TACACS+ tel que Cisco Secure Access Control Server (ACS)
- Connaissance des concepts TACACS+

Pour plus d'informations sur le fonctionnement de TACACS+, référez-vous à la section *Comprendre TACACS+* de Configuration des serveurs RADIUS et TACACS+.

Components Used

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

- Points d'accès Aironet Cisco Aironet 1240/1140
- ACS qui exécute la version logicielle 4.1
- ACS qui exécute la version 5.2 du logiciel

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 à Conventions relatives aux conseils techniques Cisco.

Configuration

Cette section explique comment configurer le point d'accès Aironet et le serveur TACACS+ (ACS) pour l'authentification de connexion TACACS+.

Cet exemple de configuration utilise les paramètres suivants :

- Adresse IP de l'ACS—172.16.1.1/255.255.0.0
- Adresse IP de l'AP—172.16.1.30/255.255.0.0
- Clé secrète partagée utilisée sur l'AP et le serveur TACACS+—**Exemple**

Voici les informations d'identification de l'utilisateur que cet exemple configure sur ACS :

- Nom d'utilisateur : **Utilisateur1**
- Mot de passe : **Cisco**
- Groupe : **AdminUsers**

Vous devez configurer les fonctionnalités TACACS+ pour valider les utilisateurs qui tentent de se connecter au point d'accès soit par l'interface Web soit par l'interface de ligne de commande (CLI). Pour effectuer cette configuration, vous devez effectuer les tâches suivantes :

1. Configurez le serveur TACACS+ pour l'authentification de connexion.
2. Configurez l'AP Aironet pour l'authentification TACACS+.

Remarque : Utilisez l'outil de recherche de commandes (clients inscrits seulement) pour en savoir plus sur les commandes figurant dans le présent document.

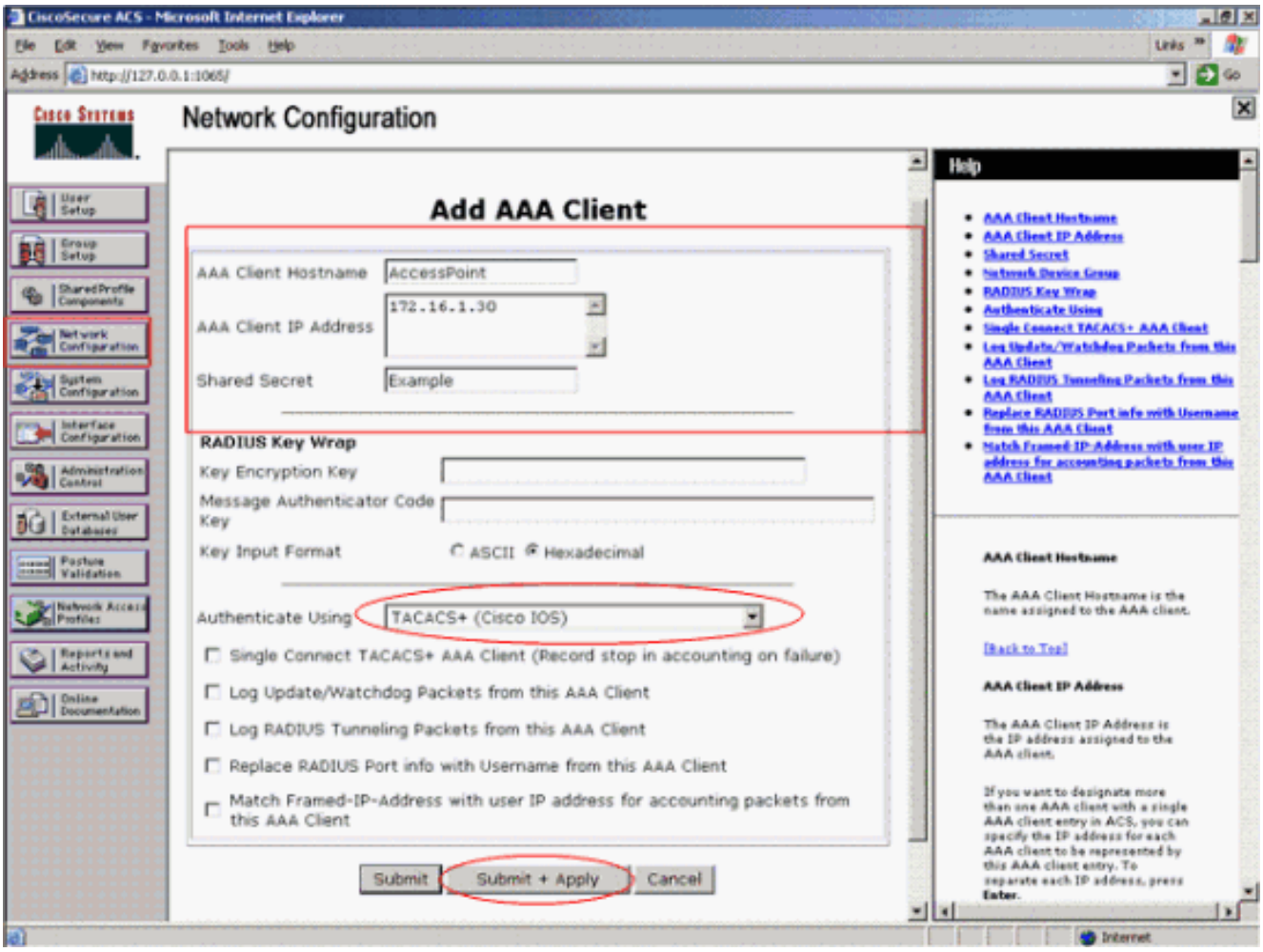
Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Configuration du serveur TACACS+ pour l'authentification de connexion - Utilisation d'ACS 4.1

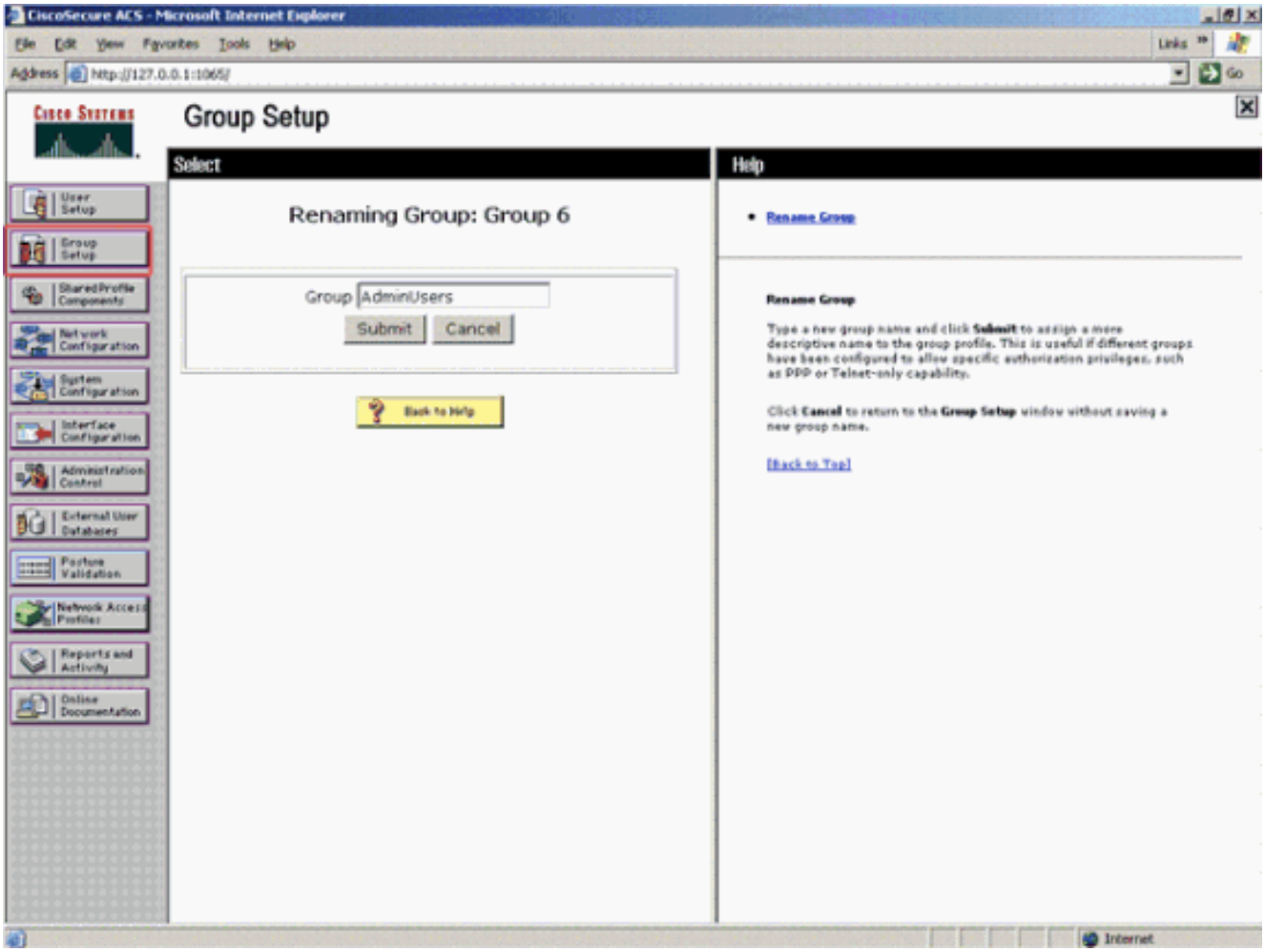
La première étape consiste à configurer un démon TACACS+ pour valider les utilisateurs qui tentent d'accéder au point d'accès. Vous devez configurer ACS pour l'authentification TACACS+ et créer une base de données utilisateur. Vous pouvez utiliser n'importe quel serveur TACACS+. Cet exemple utilise ACS comme serveur TACACS+. Procédez comme suit :

1. Complétez ces étapes afin d'ajouter le point d'accès en tant que client AAA (Authentication, Authorization, and Accounting) :Dans l'interface utilisateur graphique ACS, cliquez sur l'onglet **Configuration réseau**.Sous Clients AAA, cliquez sur **Ajouter une entrée**.Dans la fenêtre Add AAA Client, saisissez le nom d'hôte AP, l'adresse IP de l'AP et une clé secrète partagée.Cette clé secrète partagée doit être identique à la clé secrète partagée que vous configurez sur l'AP.Dans le menu déroulant Authentifier à l'aide, sélectionnez **TACACS+ (Cisco IOS)**.Cliquez sur **Soumettre + Redémarrer** afin d'enregistrer la configuration.Voici un exemple
:

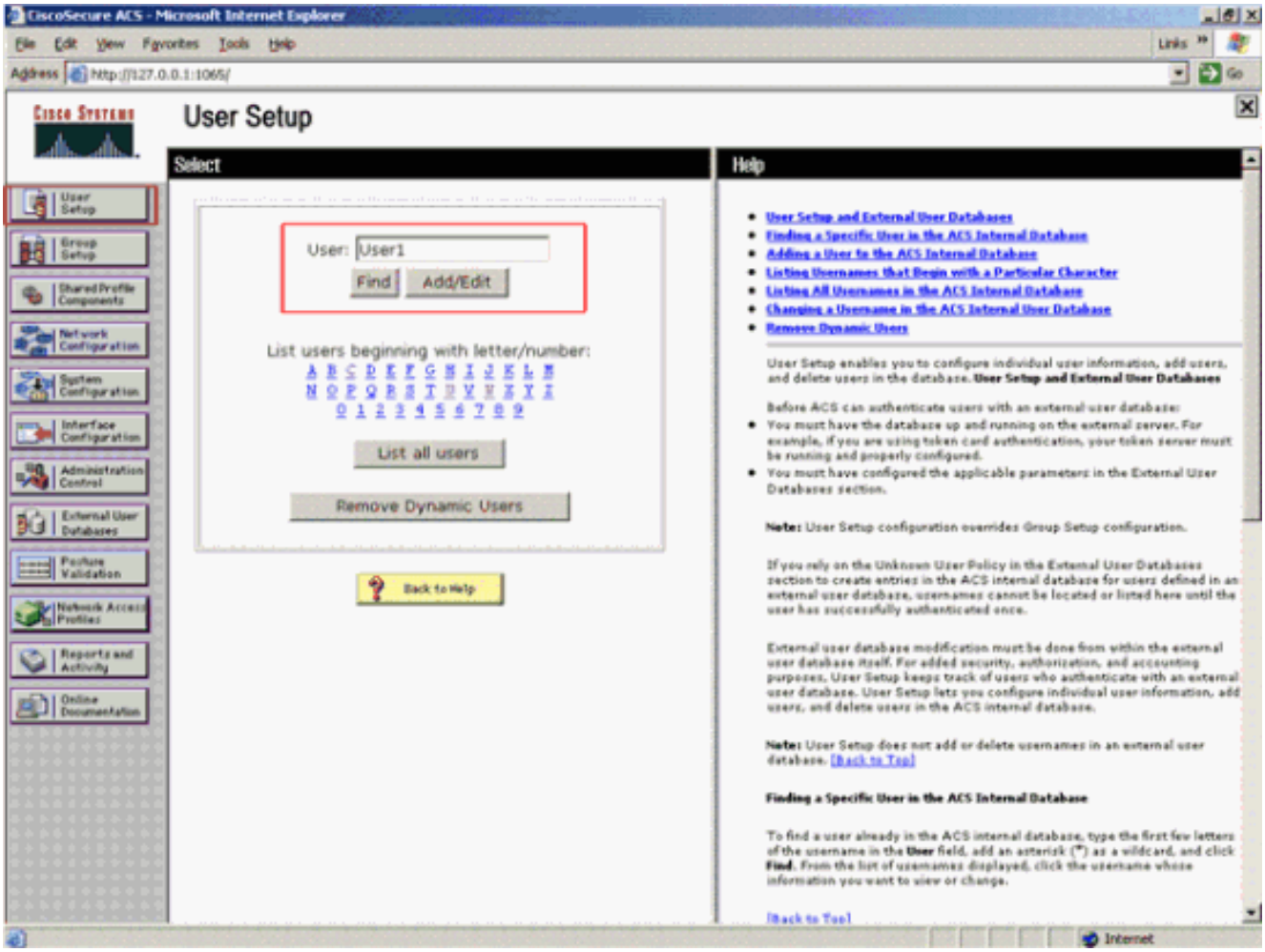


Cet exemple utilise :Nom d'hôte du client AAA **AccessPoint**Adresse **172.16.1.30/16** en tant qu'adresse IP du client AAA**Exemple** de clé secrète partagée

2. Complétez ces étapes afin de créer un groupe qui contient tous les utilisateurs administratifs (admin) :Cliquez sur **Configuration du groupe** dans le menu de gauche.Une nouvelle fenêtre apparaît.Dans la fenêtre Configuration du groupe, sélectionnez un groupe à configurer dans le menu déroulant et cliquez sur **Renommer le groupe**.Cet exemple montre comment sélectionner le groupe 6 dans le menu déroulant et renommer le groupe AdminUsers.Cliquez sur Submit.Voici un exemple
:

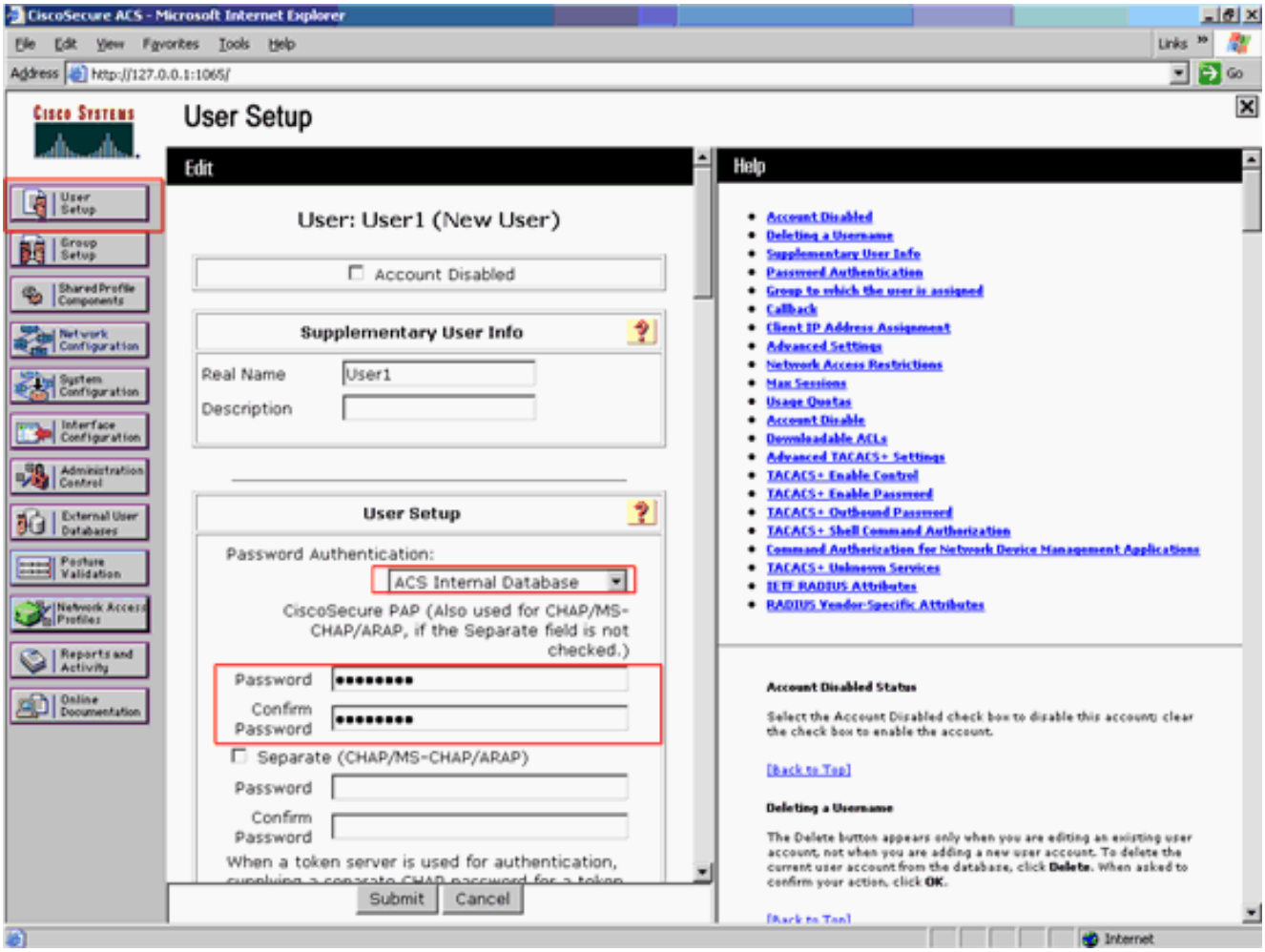


3. Complétez ces étapes afin d'ajouter les utilisateurs à la base de données TACACS+ :Cliquez sur l'onglet **Configuration utilisateur**.Afin de créer un nouvel utilisateur, entrez le nom d'utilisateur dans le champ Utilisateur et cliquez sur **Ajouter/Modifier**.Voici un exemple qui crée **User1**
:

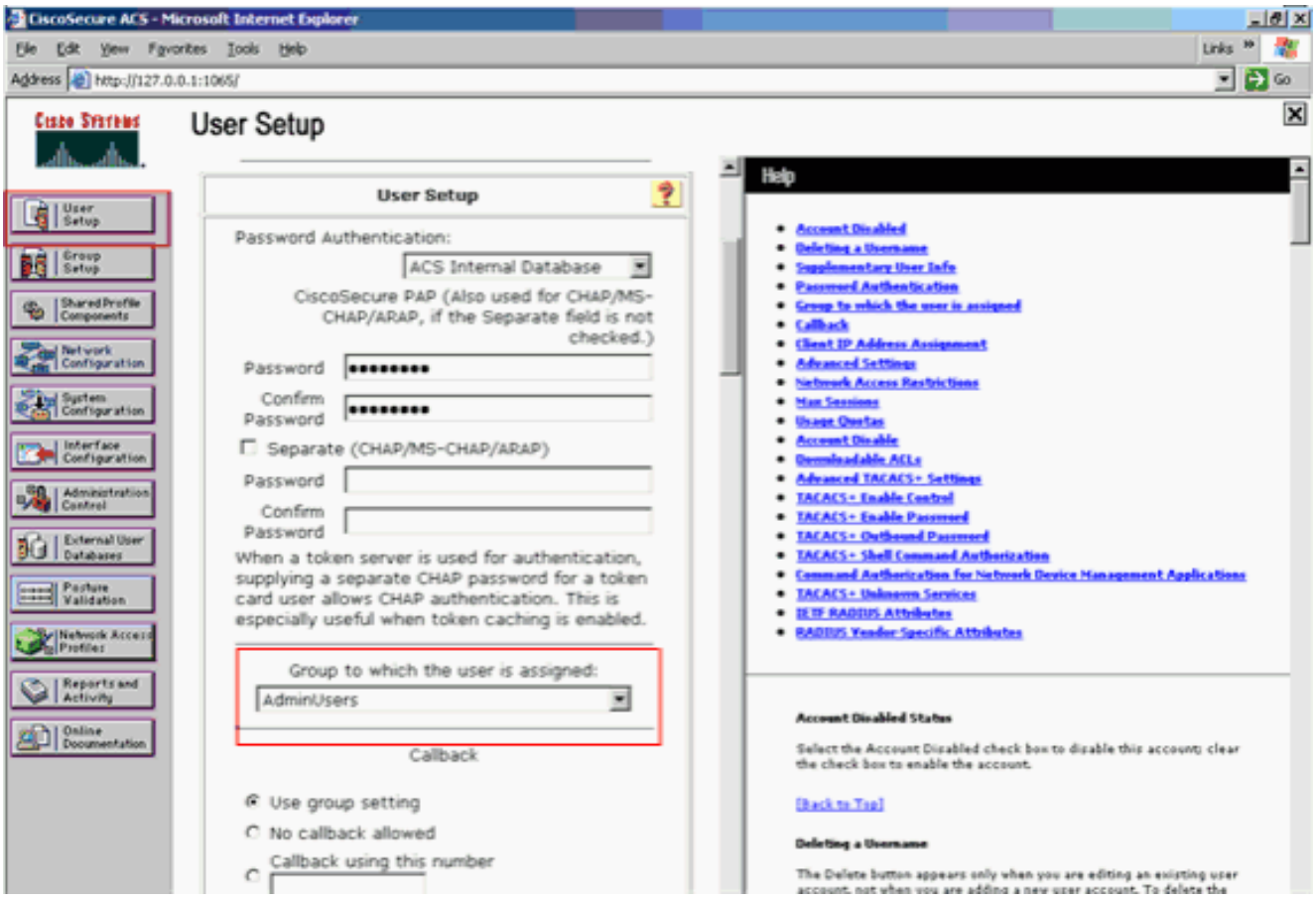


Après avoir cliqué sur Ajouter/Modifier, la fenêtre Ajouter/Modifier de cet utilisateur apparaît.

4. Entrez les informations d'identification propres à cet utilisateur et cliquez sur **Submit** afin d'enregistrer la configuration.Les informations d'identification que vous pouvez saisir comprennent :Informations supplémentaires sur l'utilisateurConfiguration utilisateurGroupe auquel l'utilisateur est affectéVoici un exemple
:



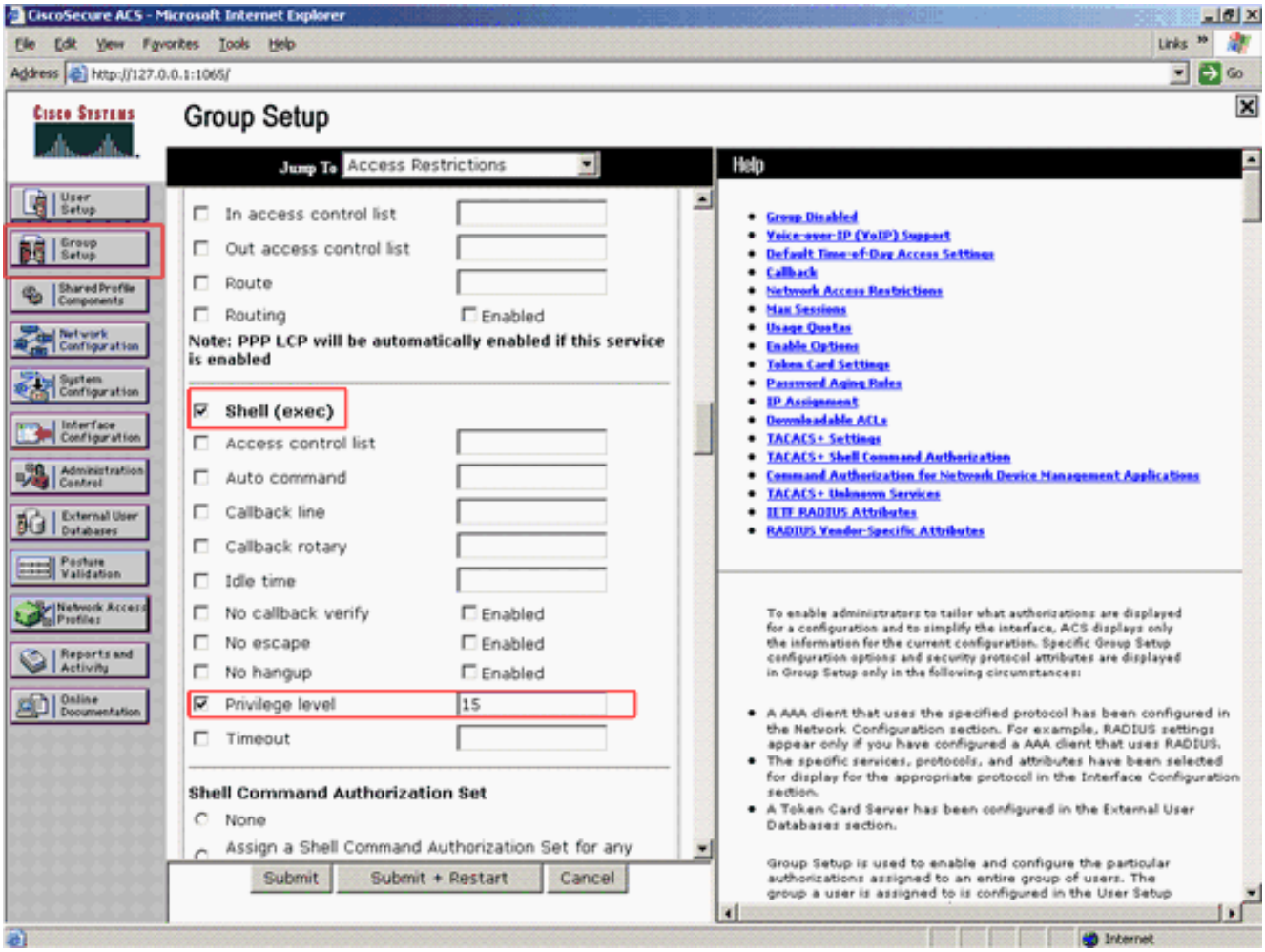
Vous pouvez voir que cet exemple ajoute l'utilisateur User1 au groupe AdminUsers.



Remarque : Si vous ne créez pas de groupe spécifique, les utilisateurs sont affectés au

groupe par défaut.

5. Complétez ces étapes afin de définir le niveau de privilège :Cliquez sur l'onglet **Configuration du groupe**.Sélectionnez le groupe que vous avez précédemment affecté à cet utilisateur et cliquez sur **Modifier les paramètres**.Cet exemple utilise le groupe AdminUsers.Sous Paramètres TACACS+, cochez la case **Shell (exec)** et cochez la case **Niveau de privilège** dont la valeur est 15.Cliquez sur **Soumettre + Redémarrer**.



Remarque : Le niveau de privilège 15 doit être défini pour l'interface utilisateur graphique et Telnet afin d'être accessible en tant que niveau 15. Sinon, par défaut, l'utilisateur ne peut accéder qu'au niveau 1. Si le niveau de privilège n'est pas défini et que l'utilisateur tente de passer en mode enable sur l'interface de ligne de commande (avec l'utilisation de Telnet), l'AP affiche ce message d'erreur :

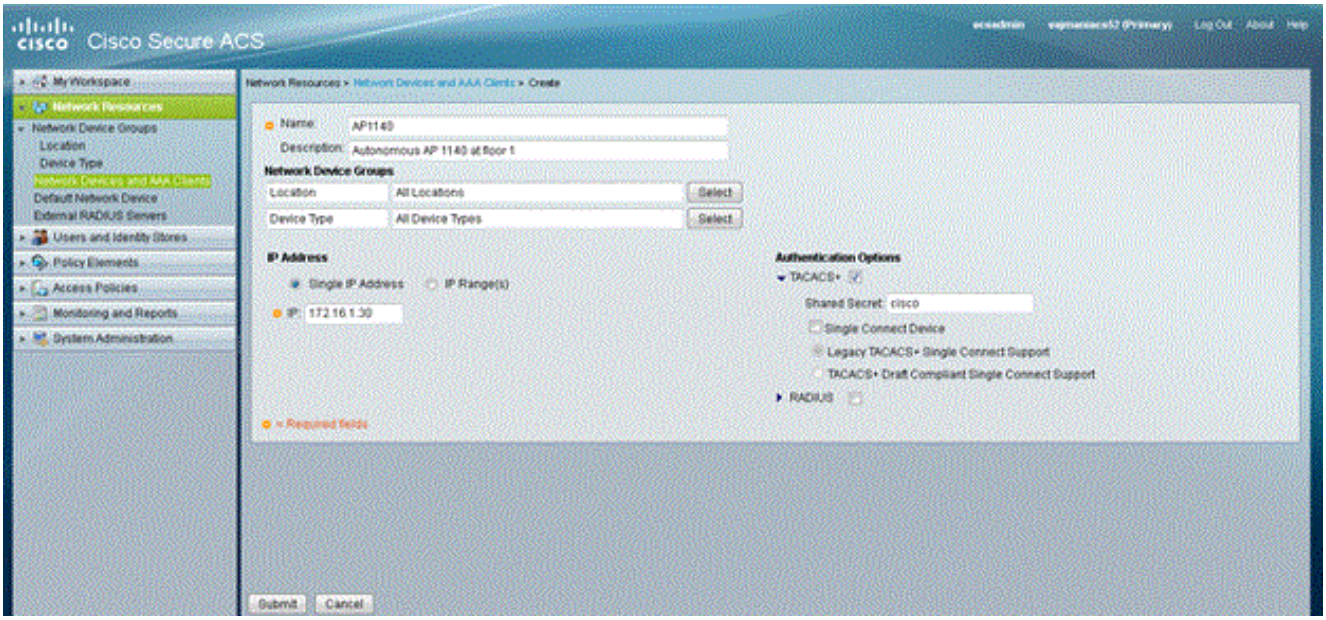
```
AccessPoint>enable
% Error in authentication
```

Répétez les étapes 2 à 4 de cette procédure si vous souhaitez ajouter d'autres utilisateurs à la base de données TACACS+. Une fois ces étapes terminées, le serveur TACACS+ est prêt à valider les utilisateurs qui tentent de se connecter au point d'accès. Maintenant, vous devez configurer l'AP pour l'authentification TACACS+.

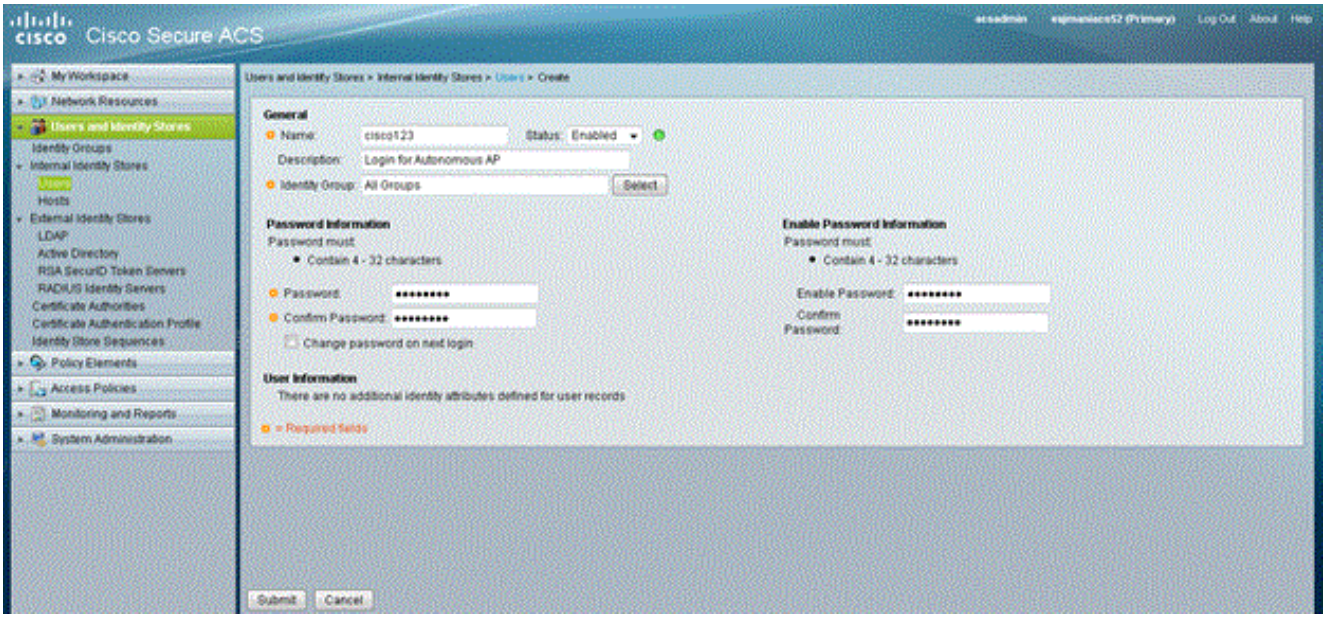
Configuration du serveur TACACS+ pour l'authentification de connexion - Utilisation d'ACS 5.2

La première étape consiste à ajouter le point d'accès en tant que client AAA dans l'ACS et à créer une stratégie TACACS pour la connexion.

1. Complétez ces étapes afin d'ajouter AP en tant que client AAA :Àpartir de l'interface utilisateur graphique ACS, cliquez sur **Ressources réseau**, puis sur **Périphériques réseau et clients AAA**.Sous Périphériques réseau, cliquez sur **Créer**.Entrez le nom d'hôte du point d'accès dans **Name**, et fournissez une description du point d'accès.Sélectionnez l'**emplacement** et le **type de périphérique** si ces catégories sont définies.Comme un seul point d'accès est configuré, cliquez sur **Adresse IP unique**. Vous pouvez ajouter la plage d'adresses IP de plusieurs points d'accès en cliquant sur **Plage(s) d'adresses IP**. Saisissez ensuite l'adresse IP du point d'accès.Sous **Options d'authentification**, cochez la case **TACACS+** et entrez le **secret partagé**.Voici un exemple
:

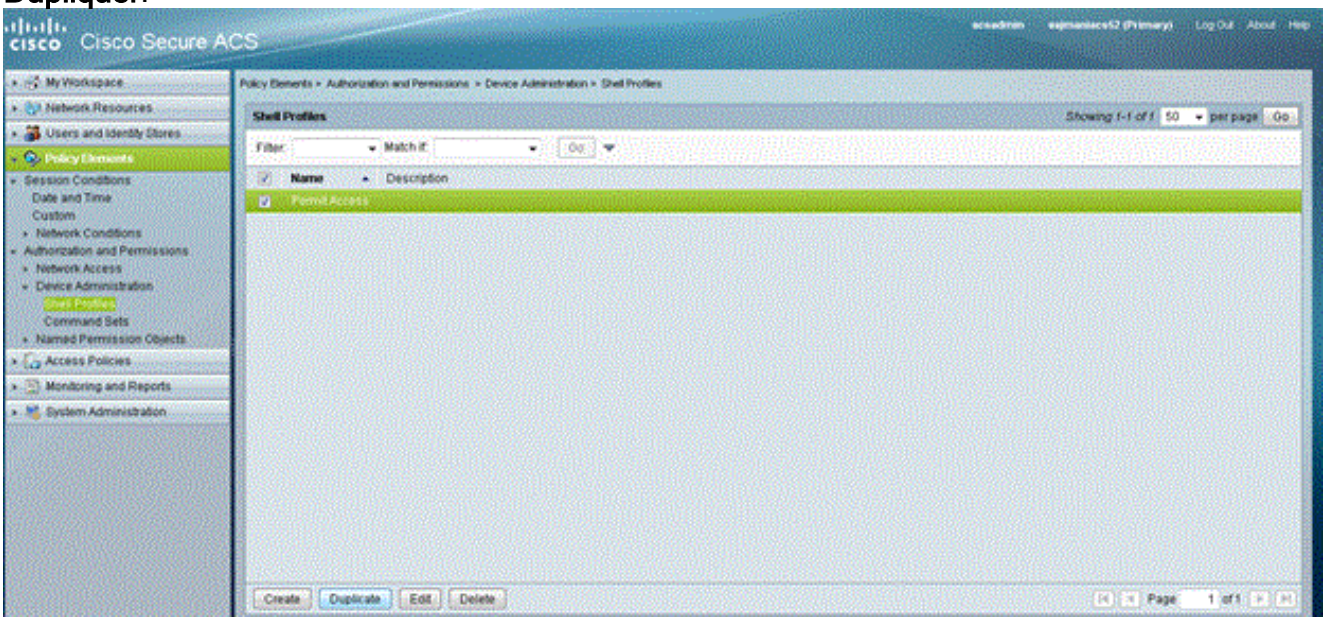


2. L'étape suivante consiste à créer un nom d'utilisateur et un mot de passe de connexion :Cliquez sur **Utilisateurs et magasins d'identité**, puis sur **Utilisateurs**.Click **Create**.Donnez le nom d'utilisateur sous **Nom** et fournissez une description.Sélectionnez le **groupe d'identités**, le cas échéant.Entrez le mot de passe dans la zone de texte **Mot de passe**, puis saisissez à nouveau dans la zone **Confirmer le mot de passe**.Vous pouvez modifier le mot de passe enable en entrant un mot de passe sous **Mot de passe enable**. Saisissez à nouveau pour confirmer.Voici un exemple
:

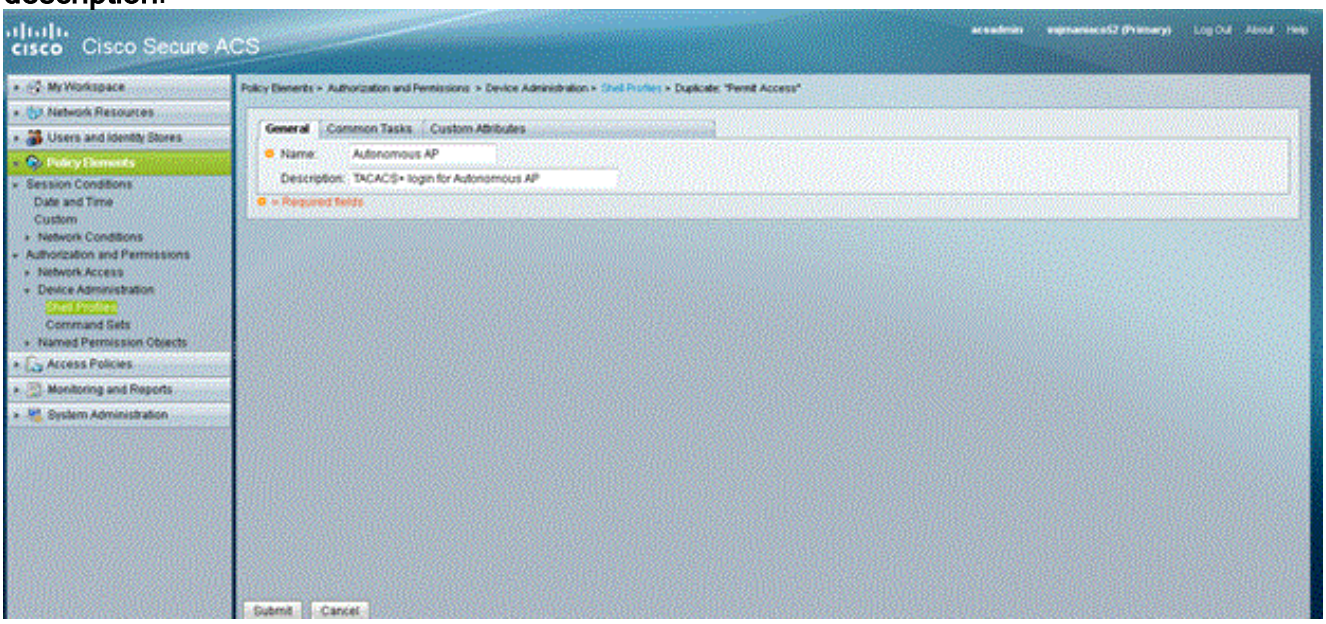


3. Complétez ces étapes afin de définir le niveau de privilège :Cliquez sur **Eléments de**

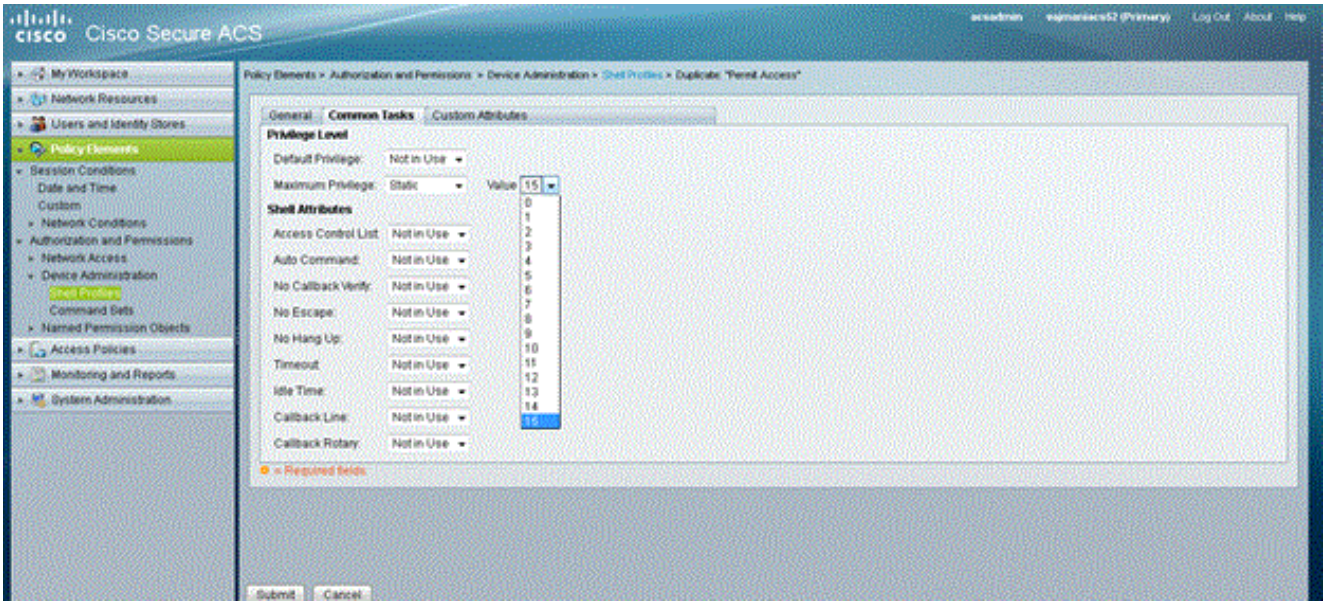
stratégie > Autorisations et autorisations > Administration des périphériques > Profils Shell.Cochez la case **Autoriser l'accès** et cliquez sur **Dupliquer**.



Entrez le **nom** et la **description**.

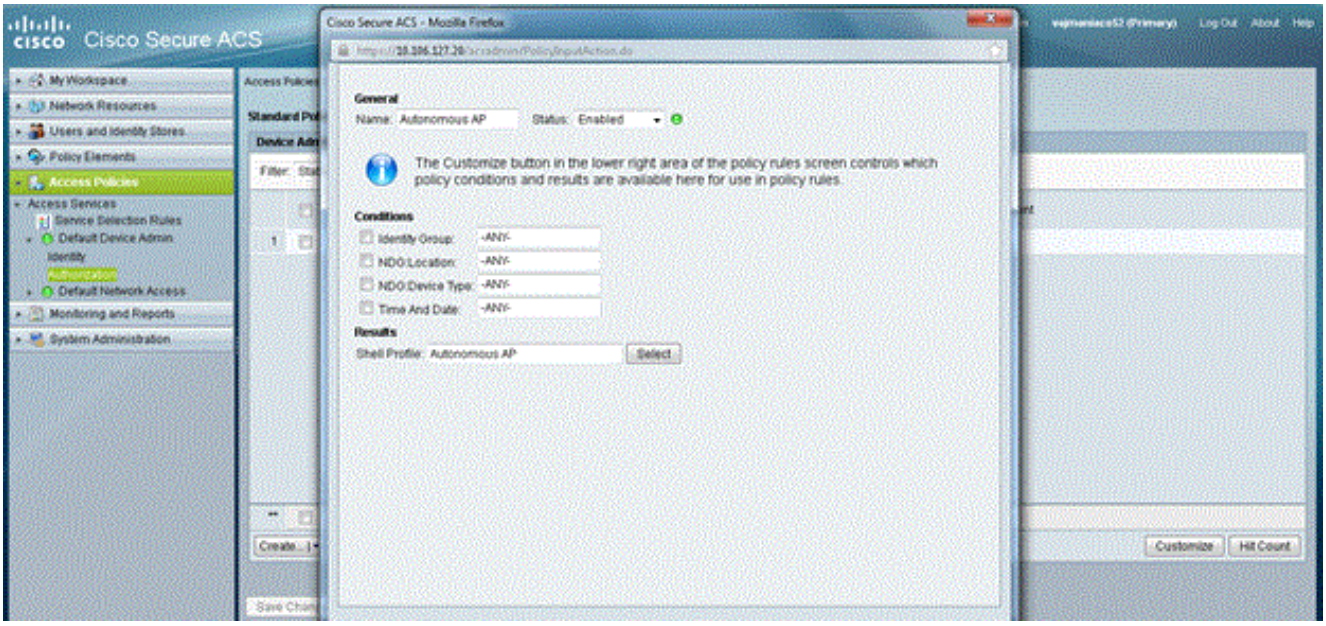


Sélectionnez l'onglet Tâches communes et choisissez **15** pour le privilège maximal.

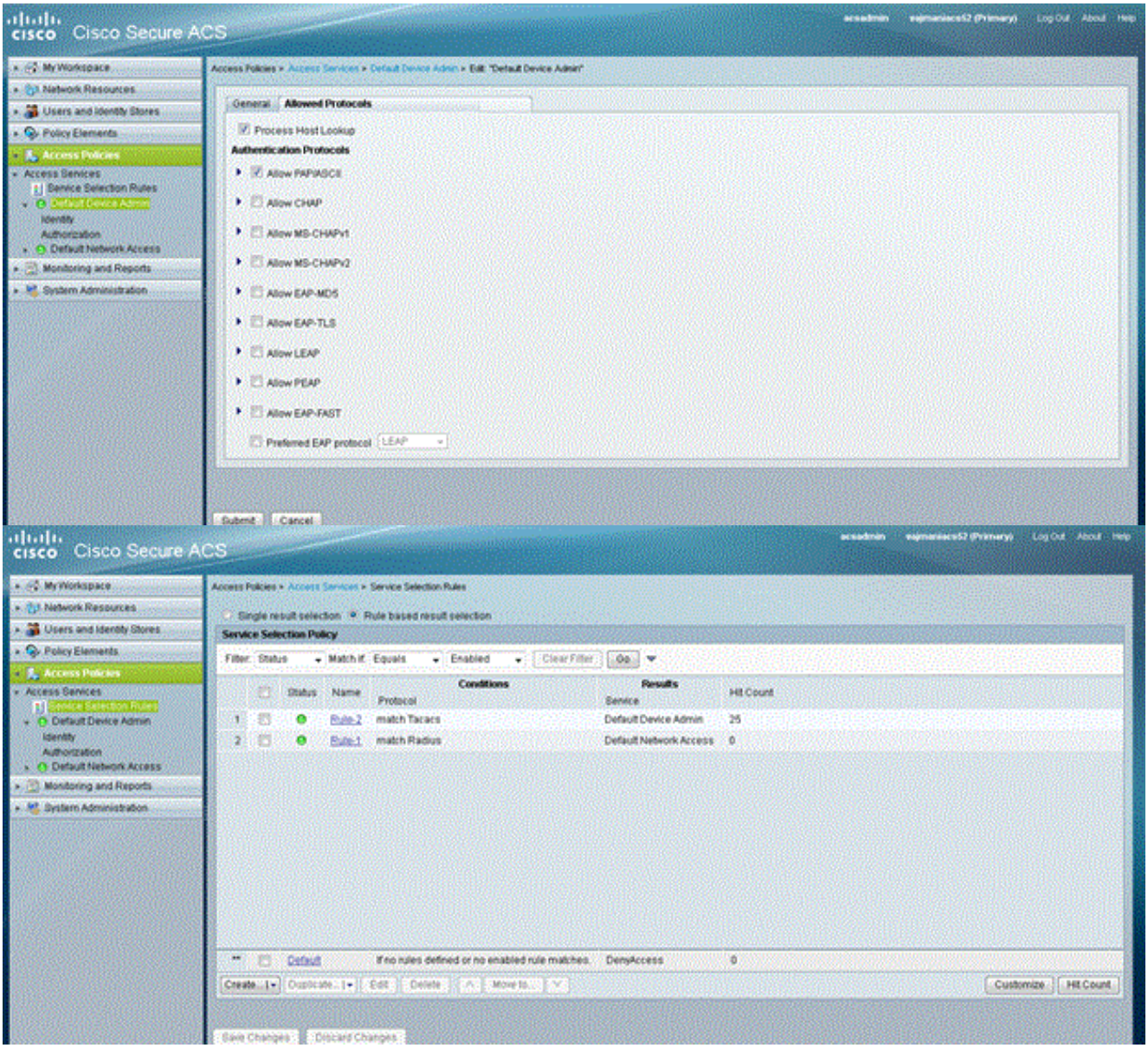


Cliquez sur Submit.

4. Complétez ces étapes afin de créer une stratégie d'autorisation :Cliquez sur **Access Policies > Access Services > Default Device Admin > Authorization**.Cliquez sur **Créer** afin de créer une nouvelle stratégie d'autorisation.Une nouvelle fenêtre contextuelle apparaît pour créer les règles de la stratégie d'autorisation.Sélectionnez le **groupe d'identités**, l'**emplacement**, etc. pour le nom d'utilisateur spécifique et le client AAA (AP), le cas échéant.Cliquez sur **Sélectionner** pour le profil Shell pour choisir le profil créé AP autonome.



Une fois cette opération effectuée, cliquez sur **Enregistrer les modifications**.Cliquez sur **Default Device Admin** , puis sur **Allowed Protocols**.Cochez **Autoriser PAP/ASCII**, puis cliquez sur **Envoyer**.Cliquez sur **Règles de sélection de service** pour vous assurer qu'il existe une règle correspondant à TACACS et pointant vers Admin. périphérique par défaut.

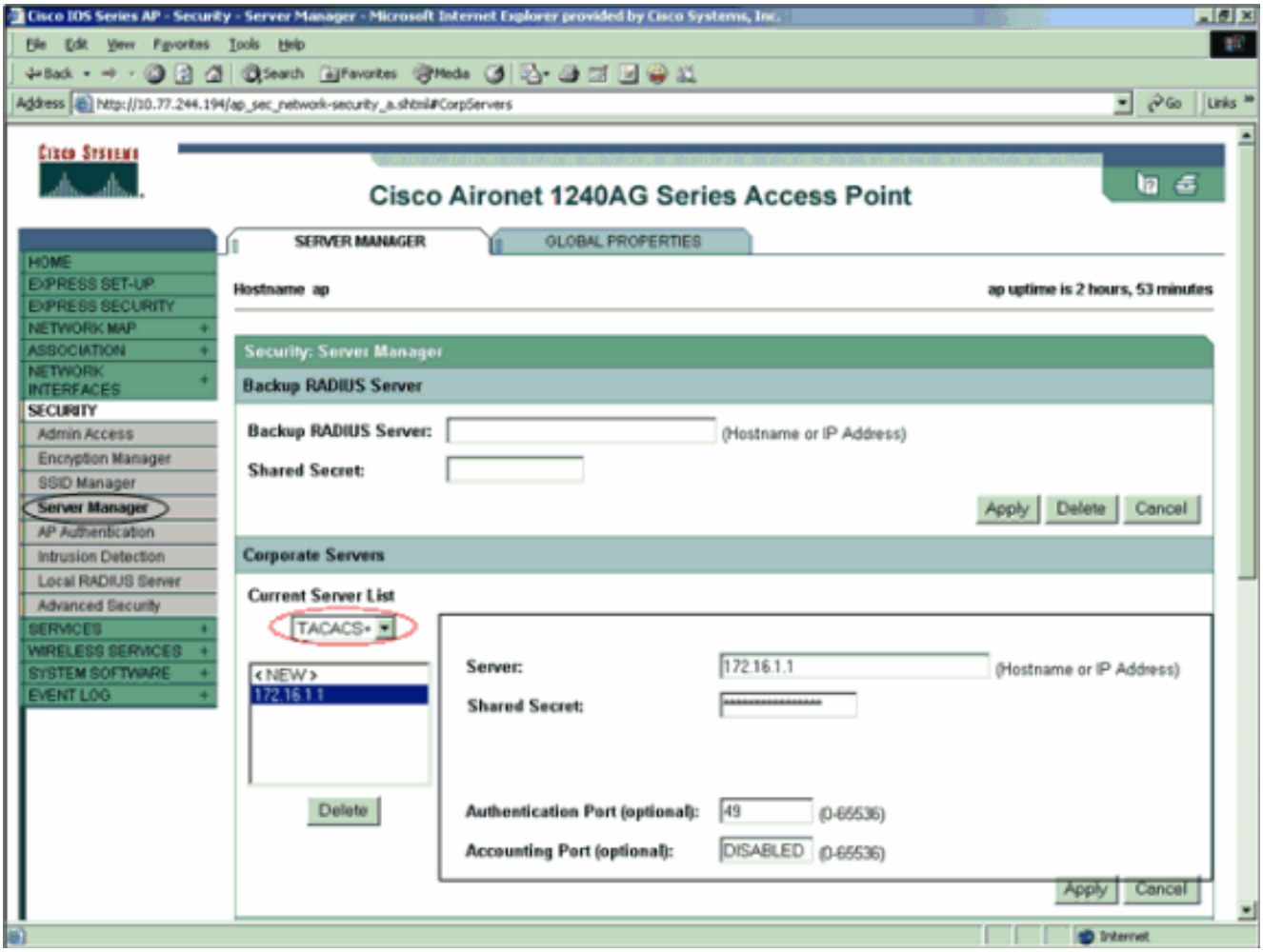


Configurer le point d'accès Aironet pour l'authentification TACACS+

Vous pouvez utiliser CLI ou GUI afin d'activer les fonctionnalités TACACS+ sur l'AP Aironet. Cette section explique comment configurer l'AP pour l'authentification de connexion TACACS+ avec l'utilisation de l'interface utilisateur graphique.

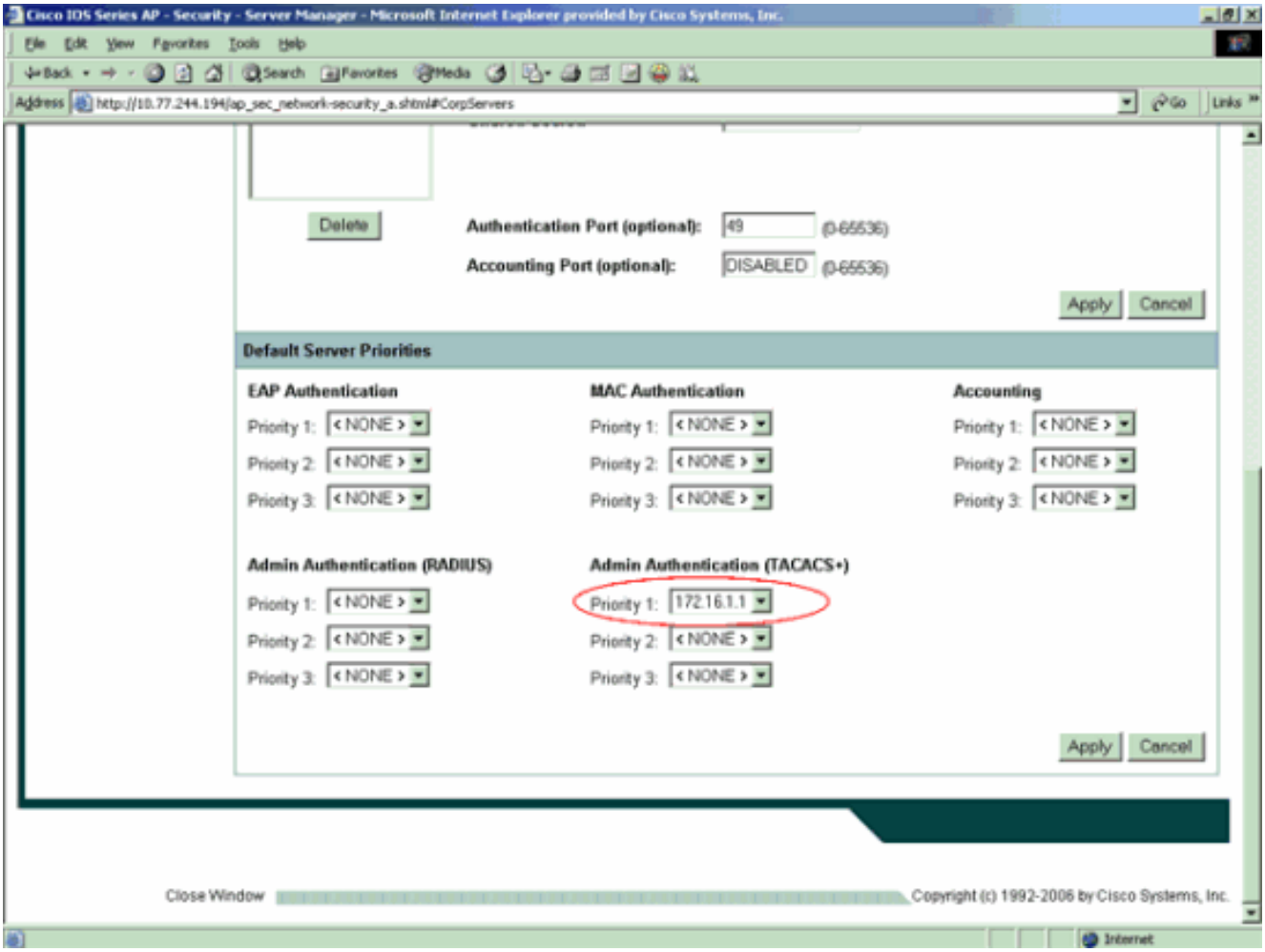
Complétez ces étapes afin de configurer TACACS+ sur l'AP avec l'utilisation de l'interface utilisateur graphique :

1. Complétez ces étapes afin de définir les paramètres du serveur TACACS+ :Dans l'interface utilisateur graphique du point d'accès, sélectionnez **Security > Server Manager**.La sécurité : La fenêtre Gestionnaire de serveur s'affiche.Dans la zone Corporate Servers, sélectionnez **TACACS+** dans le menu déroulant Current Server List.Dans cette même zone, saisissez l'adresse IP, le secret partagé et le numéro de port d'authentification du serveur TACACS+.Cliquez sur Apply.Voici un exemple
   :

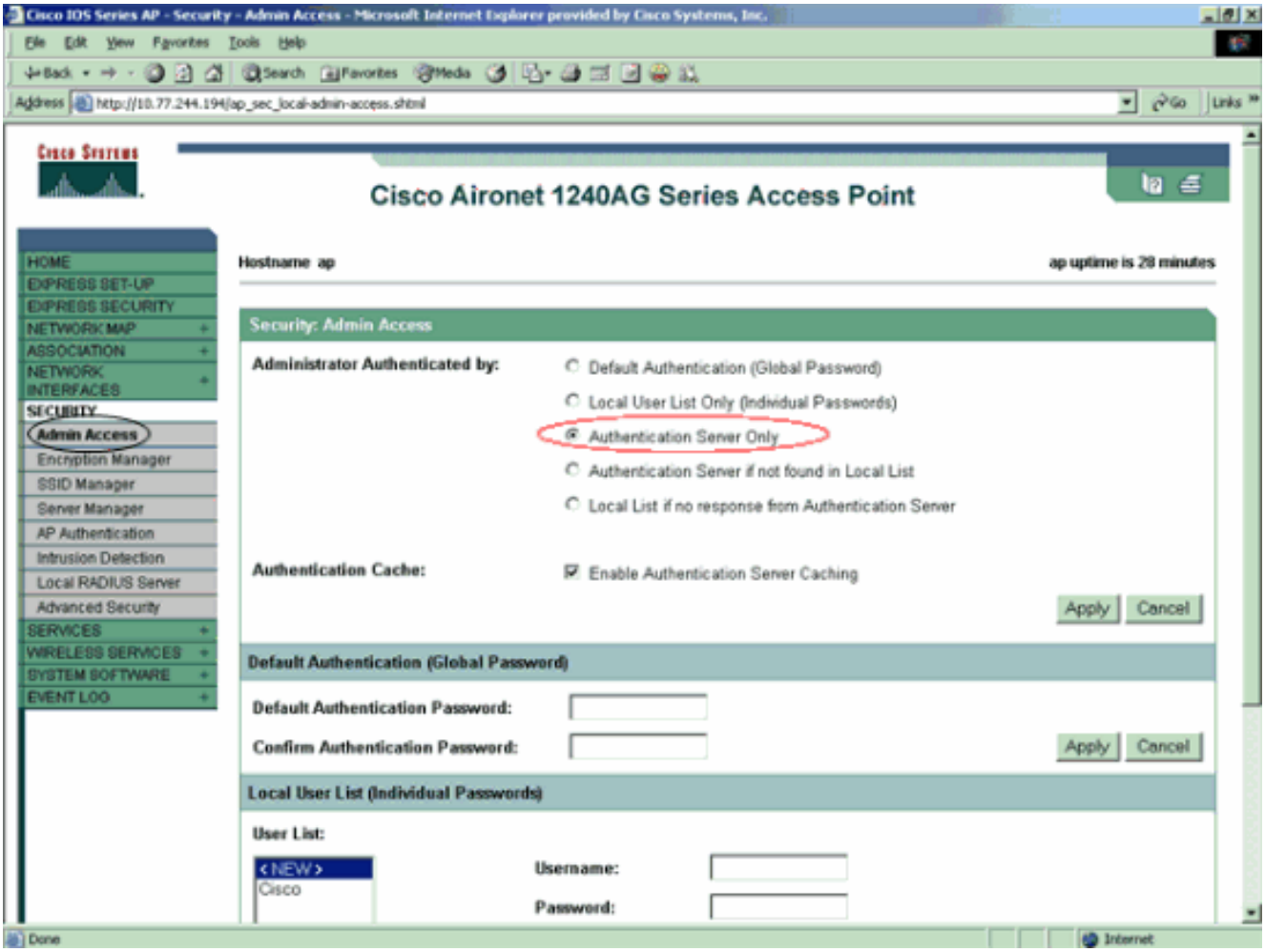


Remarque : Par défaut, TACACS+ utilise le port TCP 49.**Remarque :** La clé secrète partagée que vous configurez sur ACS et le point d'accès doit correspondre.

2. Choisissez **Default Server Priority > Admin Authentication (TACACS+)**, sélectionnez dans le menu déroulant Priority 1 l'adresse IP du serveur TACACS+ que vous avez configurée, puis cliquez sur **Apply**.Voici un exemple
:



3. Choisissez **Security > Admin Access** et, pour Administrator Authenticated by :, sélectionnez **Authentication Server Only** et cliquez sur **Apply**.Cette sélection garantit que les utilisateurs qui tentent de se connecter au point d'accès sont authentifiés par un serveur d'authentification.Voici un exemple
:



Voici la configuration CLI de l'exemple de configuration :

Point d'accès

```
AccessPoint#show running-config

Current configuration : 2535 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname AccessPoint
!
!
ip subnet-zero
!
!
aaa new-model
!--- Enable AAA. ! ! aaa group server radius rad_eap !
aaa group server radius rad_mac ! aaa group server
radius rad_acct ! aaa group server radius rad_admin
cache expiry 1 cache authorization profile admin_cache
cache authentication profile admin_cache ! aaa group
server tacacs+ tac_admin
!--- Configure the server group tac_admin. server
172.16.1.1
!--- Add the TACACS+ server 172.16.1.1 to the server
group. cache expiry 1
```

```
!--- Set the expiration time for the local cache as 24
hours. cache authorization profile admin_cache
 cache authentication profile admin_cache
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default group tac_admin
!--- Define the AAA login authentication method list to
use the TACACS+ server. aaa authentication login
eap_methods group rad_eap aaa authentication login
mac_methods local aaa authorization exec default group
tac_admin
!--- Use TACACS+ for privileged EXEC access
authorization !--- if authentication was performed with
use of TACACS+. aaa accounting network acct_methods
start-stop group rad_acct aaa cache profile admin_cache
all ! aaa session-id common ! ! username Cisco password
7 00271A150754 ! bridge irb ! ! interface Dot11Radio0 no
ip address no ip route-cache shutdown speed basic-1.0
basic-2.0 basic-5.5 basic-11.0 station-role root bridge-
group 1 bridge-group 1 subscriber-loop-control bridge-
group 1 block-unknown-source no bridge-group 1 source-
learning no bridge-group 1 unicast-flooding bridge-group
1 spanning-disabled ! interface Dot11Radio1 no ip
address no ip route-cache shutdown speed station-role
root bridge-group 1 bridge-group 1 subscriber-loop-
control bridge-group 1 block-unknown-source no bridge-
group 1 source-learning no bridge-group 1 unicast-
flooding bridge-group 1 spanning-disabled ! interface
FastEthernet0 no ip address no ip route-cache duplex
auto speed auto bridge-group 1 no bridge-group 1 source-
learning bridge-group 1 spanning-disabled ! interface
BVI1 ip address 172.16.1.30 255.255.0.0 no ip route-
cache ! ip http server ip http authentication aaa
!--- Specify the authentication method of HTTP users as
AAA. no ip http secure-server ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/ea ip radius source-interface BVI1 ! tacacs-server
host 172.16.1.1 port 49 key 7 13200F13061C082F tacacs-
server directed-request radius-server attribute 32
include-in-access-req format %h radius-server vsa send
accounting ! control-plane ! bridge 1 route ip ! ! !
line con 0 transport preferred all transport output all
line vty 0 4 transport preferred all transport input all
transport output all line vty 5 15 transport preferred
all transport input all transport output all ! end
```

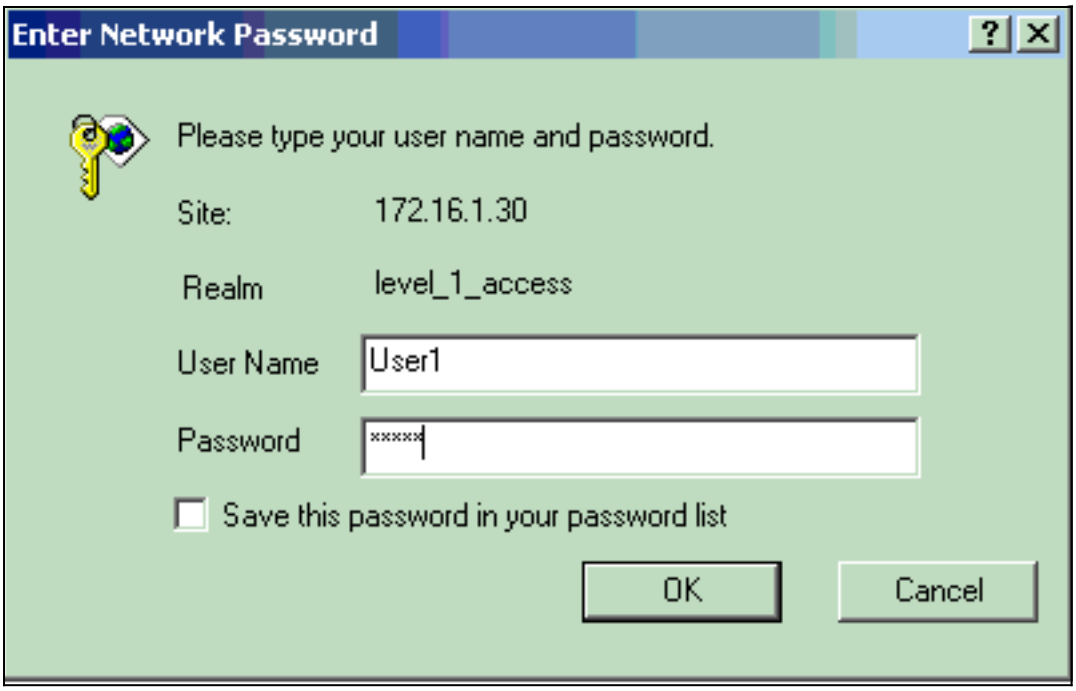
Remarque : Vous devez disposer du logiciel Cisco IOS Version 12.3(7)JA ou ultérieure pour que toutes les commandes de cette configuration fonctionnent correctement. Toutes ces commandes peuvent ne pas être disponibles dans une version antérieure du logiciel Cisco IOS.

Vérification

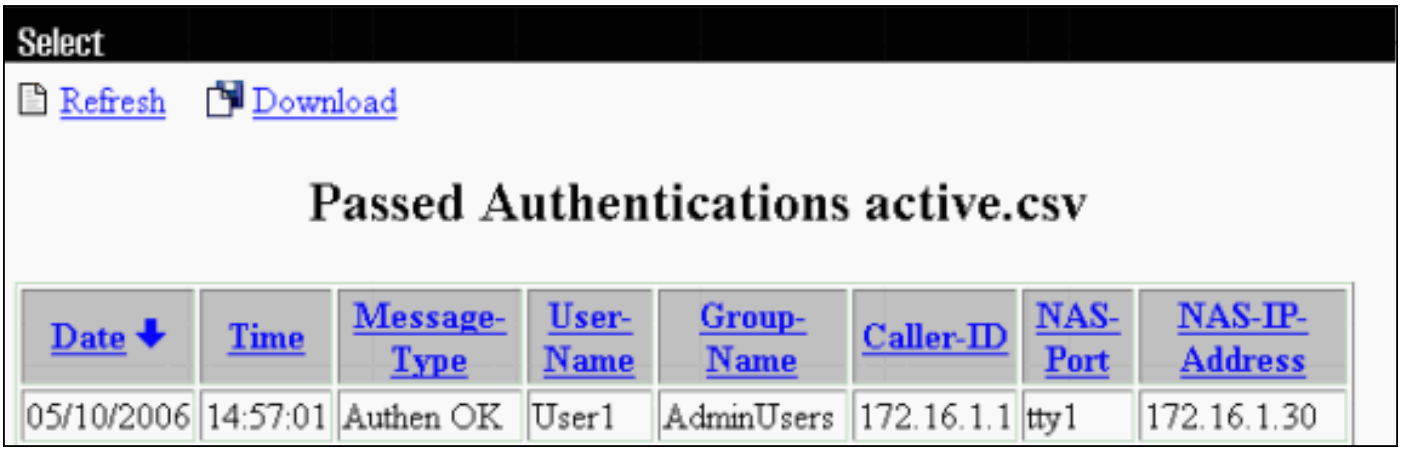
Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

Afin de vérifier la configuration, essayez de vous connecter au point d'accès à l'aide de l'interface utilisateur graphique ou de l'interface de ligne de commande. Lorsque vous essayez d'accéder au point d'accès, le point d'accès vous demande un nom d'utilisateur et un mot de passe.



Lorsque vous fournissez les informations d'identification de l'utilisateur, le point d'accès transfère les informations d'identification au serveur TACACS+. Le serveur TACACS+ valide les informations d'identification sur la base des informations disponibles dans sa base de données et fournit l'accès au point d'accès lors d'une authentification réussie. Vous pouvez choisir **Rapports et Activité > Authentification passée** sur ACS et utiliser le rapport Authentification passée afin de vérifier si l'authentification de cet utilisateur a réussi. Voici un exemple :



Vous pouvez également utiliser la commande **show tacacs** afin de vérifier la configuration correcte du serveur TACACS+. Voici un exemple :

```
AccessPoint#show tacacs

Tacacs+ Server            : 172.16.1.1/49
              Socket opens:         348
             Socket closes:         348
             Socket aborts:           0
             Socket errors:           0
          Socket Timeouts:            0
   Failed Connect Attempts:           0
```

```
        Total Packets Sent:        525
        Total Packets Recv:        525
```

Vérification pour ACS 5.2

Vous pouvez vérifier les tentatives d'échec/de réussite des informations d'identification de connexion à partir de ACS 5.2 :

1. Cliquez sur **Monitoring and Reports > Launch Monitoring and Report Viewer**.Une nouvelle fenêtre contextuelle s'ouvre avec le tableau de bord.
2. Cliquez sur **Authentications-TACACS-Today**. Affiche les détails des tentatives échouées/passées.

Dépannage

Vous pouvez utiliser ces commandes de débogage sur l'AP afin de dépanner votre configuration :

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **debug tacacs events** - Cette commande affiche la séquence des événements qui se produisent pendant l'authentification TACACS. Voici un exemple du résultat de cette commande :

```
*Mar  1 00:51:21.113: TPLUS: Queuing AAA Authentication request 0 for
processing
*Mar  1 00:51:21.113: TPLUS: processing authentication start request id 0
*Mar  1 00:51:21.113: TPLUS: Authentication start packet created for 0(User1)
*Mar  1 00:51:21.114: TPLUS: Using server 172.16.1.1
*Mar  1 00:51:21.115: TPLUS(00000000)/0/NB_WAIT/C6DC40: Started 5 sec timeout
*Mar  1 00:51:21.116: TPLUS(00000000)/0/NB_WAIT: socket event 2
*Mar  1 00:51:21.116: TPLUS(00000000)/0/NB_WAIT: wrote entire 25 bytes request
*Mar  1 00:51:21.116: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:51:21.117: TPLUS(00000000)/0/READ: Would block while reading
*Mar  1 00:51:21.120: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:51:21.120: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect
16 bytes data)
*Mar  1 00:51:21.120: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:51:21.120: TPLUS(00000000)/0/READ: read entire 28 bytes response
*Mar  1 00:51:21.121: TPLUS(00000000)/0/C6DC40: Processing the reply packet
*Mar  1 00:51:21.121: TPLUS: Received authen response status GET_PASSWORD (8)
*Mar  1 00:51:21.121: TPLUS: Queuing AAA Authentication request 0 for processing
*Mar  1 00:51:21.121: TPLUS: processing authentication continue request id 0
*Mar  1 00:51:21.122: TPLUS: Authentication continue packet generated for 0
*Mar  1 00:51:21.122: TPLUS(00000000)/0/WRITE/C6DC40: Started 5 sec timeout
*Mar  1 00:51:21.122: TPLUS(00000000)/0/WRITE: wrote entire 22 bytes request
*Mar  1 00:51:21.178: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:51:21.178: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect
6 bytes data)
*Mar  1 00:51:21.178: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:51:21.178: TPLUS(00000000)/0/READ: read entire 18 bytes response
*Mar  1 00:51:21.179: TPLUS(00000000)/0/C6DC40: Processing the reply packet
*Mar  1 00:51:21.179: TPLUS: Received authen response status PASS (2)
```

- **debug ip http authentication** - Utilisez cette commande pour résoudre les problèmes d'authentification HTTP. La commande affiche la méthode d'authentification que le routeur a tenté et les messages d'état spécifiques à l'authentification.

- **debug aaa authentication** - Cette commande affiche des informations sur l'authentification AAA TACACS+.

Si l'utilisateur entre un nom d'utilisateur qui n'existe pas sur le serveur TACACS+, l'authentification échoue. Voici la sortie de commande **debug tacacs authentication** pour une authentification ayant échoué :

```
*Mar  1 00:07:26.624: TPLUS: Queuing AAA Authentication request 0 for processing
*Mar  1 00:07:26.624: TPLUS: processing authentication start request id 0
*Mar  1 00:07:26.624: TPLUS: Authentication start packet created for 0(User3)
*Mar  1 00:07:26.624: TPLUS: Using server 172.16.1.1
*Mar  1 00:07:26.625: TPLUS(00000000)/0/NB_WAIT/A88784: Started 5 sec timeout
*Mar  1 00:07:26.626: TPLUS(00000000)/0/NB_WAIT: socket event 2
*Mar  1 00:07:26.626: TPLUS(00000000)/0/NB_WAIT: wrote entire 25 bytes request
*Mar  1 00:07:26.627: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:07:26.627: TPLUS(00000000)/0/READ: Would block while reading
*Mar  1 00:07:26.631: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:07:26.632: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 16
bytes data)
*Mar  1 00:07:26.632: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:07:26.632: TPLUS(00000000)/0/READ: read entire 28 bytes response
*Mar  1 00:07:26.632: TPLUS(00000000)/0/A88784: Processing the reply packet
*Mar  1 00:07:26.632: TPLUS: Received authen response status GET_PASSWORD (8)
*Mar  1 00:07:26.632: TPLUS: Queuing AAA Authentication request 0 for processing
*Mar  1 00:07:26.633: TPLUS: processing authentication continue request id 0
*Mar  1 00:07:26.633: TPLUS: Authentication continue packet generated for 0
*Mar  1 00:07:26.634: TPLUS(00000000)/0/WRITE/A88784: Started 5 sec timeout
*Mar  1 00:07:26.634: TPLUS(00000000)/0/WRITE: wrote entire 22 bytes request
*Mar  1 00:07:26.688: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:07:26.688: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 6
bytes data)
*Mar  1 00:07:26.689: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:07:26.689: TPLUS(00000000)/0/READ: read entire 18 bytes response
*Mar  1 00:07:26.689: TPLUS(00000000)/0/A88784: Processing the reply packet
*Mar  1 00:07:26.689: TPLUS: Received authen response status FAIL (3)
```

Vous pouvez choisir **Rapports et Activité > Echec de l'authentification** afin de voir la tentative d'authentification échouée sur ACS. Voici un exemple :

Date ↓	Time	Message-Type	User-Name	Group-Name	Caller-ID	Authen-Failure-Code	Author-Failure-Code	Author-Data	NAS-Port
05/17/2006	19:40:14	Authen failed	User3	..	..	CS user unknown	..	..	..

Si vous utilisez une version du logiciel Cisco IOS sur l'AP antérieure à la version 12.3(7)JA du logiciel Cisco IOS, vous pouvez frapper un bogue chaque fois que vous essayez de vous connecter à l'AP avec l'utilisation de HTTP. L'ID de bogue Cisco est CSCeb52431 (clients enregistrés uniquement).

L'implémentation HTTP/AAA du logiciel Cisco IOS nécessite l'authentification indépendante de chaque connexion HTTP distincte. L'interface utilisateur graphique du logiciel Cisco IOS sans fil comprend la référence de dizaines de fichiers distincts dans une seule page Web (par exemple Javascript et GIF). Ainsi, si vous chargez une seule page dans l'interface utilisateur graphique du logiciel Cisco IOS sans fil, des dizaines et des dizaines de demandes d'authentification/autorisation distinctes peuvent atteindre le serveur AAA.

Pour l'authentification HTTP, utilisez RADIUS ou l'authentification locale. Le serveur RADIUS est toujours soumis aux demandes d'authentification multiples. Mais RADIUS est plus évolutif que TACACS+, et il est donc probable qu'il ait un impact moins négatif sur les performances.

Si vous devez utiliser TACACS+ et que vous disposez d'un Cisco ACS, utilisez le mot clé **single-connection** avec la commande **tacacs-server**. L'utilisation de ce mot clé avec la commande évite à ACS la majeure partie de la surcharge de configuration/désactivation de la connexion TCP et est susceptible de réduire la charge sur le serveur dans une certaine mesure.

Pour les versions du logiciel Cisco IOS 12.3(7) JA et ultérieures sur l'AP, le logiciel inclut une correction. Le reste de cette section décrit le correctif.

Utilisez la fonctionnalité de cache d'authentification AAA afin de mettre en cache les informations renvoyées par le serveur TACACS+. La fonctionnalité de cache et de profil d'authentification permet au point d'accès de mettre en cache les réponses d'authentification/autorisation pour un utilisateur, de sorte que les demandes d'authentification/autorisation suivantes ne doivent pas être envoyées au serveur AAA. Afin d'activer cette fonctionnalité avec l'interface de ligne de commande, utilisez ces commandes :

```
cache expiry
cache authorization profile
cache authentication profile
aaa cache profile
```

Pour plus d'informations sur cette fonctionnalité et les commandes, référez-vous à la section *Configuration du cache et du profil d'authentification* de l'administration du point d'accès.

Afin d'activer cette fonctionnalité sur l'interface utilisateur graphique, sélectionnez **Security > Admin Access** et cochez la case **Enable Authentication Server Caching**. Comme ce document utilise le logiciel Cisco IOS Version 12.3(7)JA, le document utilise le correctif, comme le montrent les configurations.

Informations connexes

- Configuration des serveurs RADIUS et TACACS+
- Avis sur le champ : Le point d'accès IOS protège le serveur TACACS+ avec des requêtes
- Authentification EAP avec le serveur RADIUS
- Assistance produit sans fil
- Support et documentation techniques - Cisco Systems