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 permettre à TACACS plus les services (TACACS+) sur un Point d'accès de Cisco Aironet (AP) afin d'exécuter l'authentification de connexion avec l'utilisation d'un serveur TACACS+.

Conditions préalables

Conditions requises

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

- La connaissance de la façon configurer des paramètres de base sur l'Aironet aps
- La connaissance de la façon configurer un serveur TACACS+ comme le Cisco Secure Access Control Server (ACS)
- La connaissance des concepts TACACS+

Pour les informations sur la façon dont les travaux TACACS+, se rapportent *compréhension derrière la* section *TACACS+ de* configurer des serveurs de RADIUS et TACACS+.

Composants utilisés

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

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Configurer

Cette section explique comment configurer l'Aironet AP et le serveur TACACS+ (ACS) pour l'authentification de connexion TACACS+-based.

Cet exemple de configuration utilise ces paramètres :

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

Ce sont les qualifications de l'utilisateur que cet exemple configure sur l'ACS :

- Nom d'utilisateur — **User1**
- Mot de passe cisco
- Groupe — **AdminUsers**

Vous devez configurer des caractéristiques TACACS+ pour valider les utilisateurs qui essayent de se connecter à AP par l'interface web ou par l'interface de ligne de commande (CLI). Afin d'accomplir cette configuration, vous devez effectuer ces tâches :

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

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour trouver plus d'informations sur les commandes utilisées dans ce document.

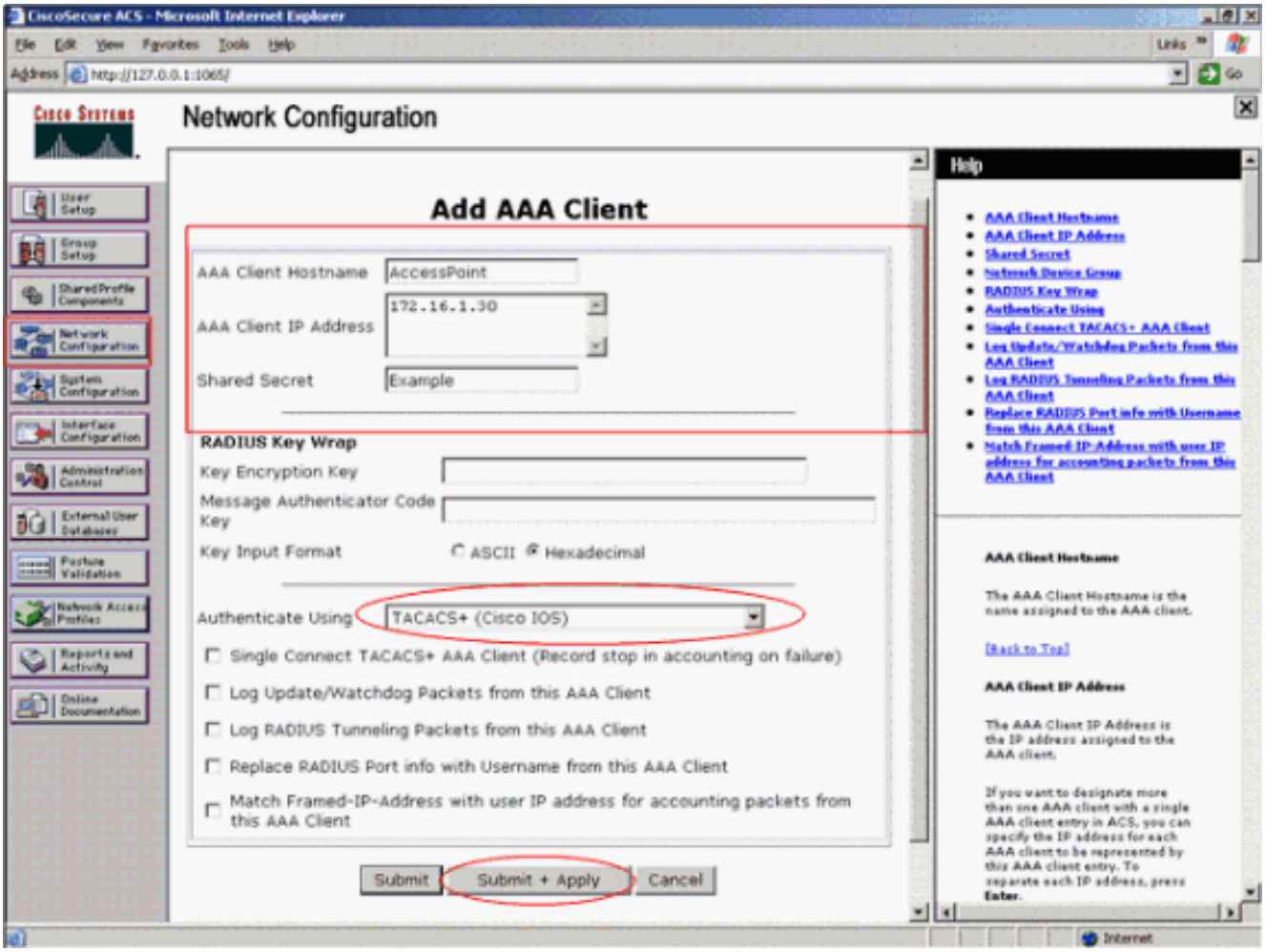
Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Configurez le serveur TACACS+ pour l'authentification de connexion - Utilisant ACS 4.1

La première étape est d'installer un démon TACACS+ pour valider les utilisateurs qui essayent d'accéder à AP. Vous devez installer l'ACS pour l'authentification TACACS+ et créer une base de données utilisateur. Vous pouvez utiliser n'importe quel serveur TACACS+. Cet exemple utilise l'ACS en tant que serveur TACACS+. Procédez comme suit :

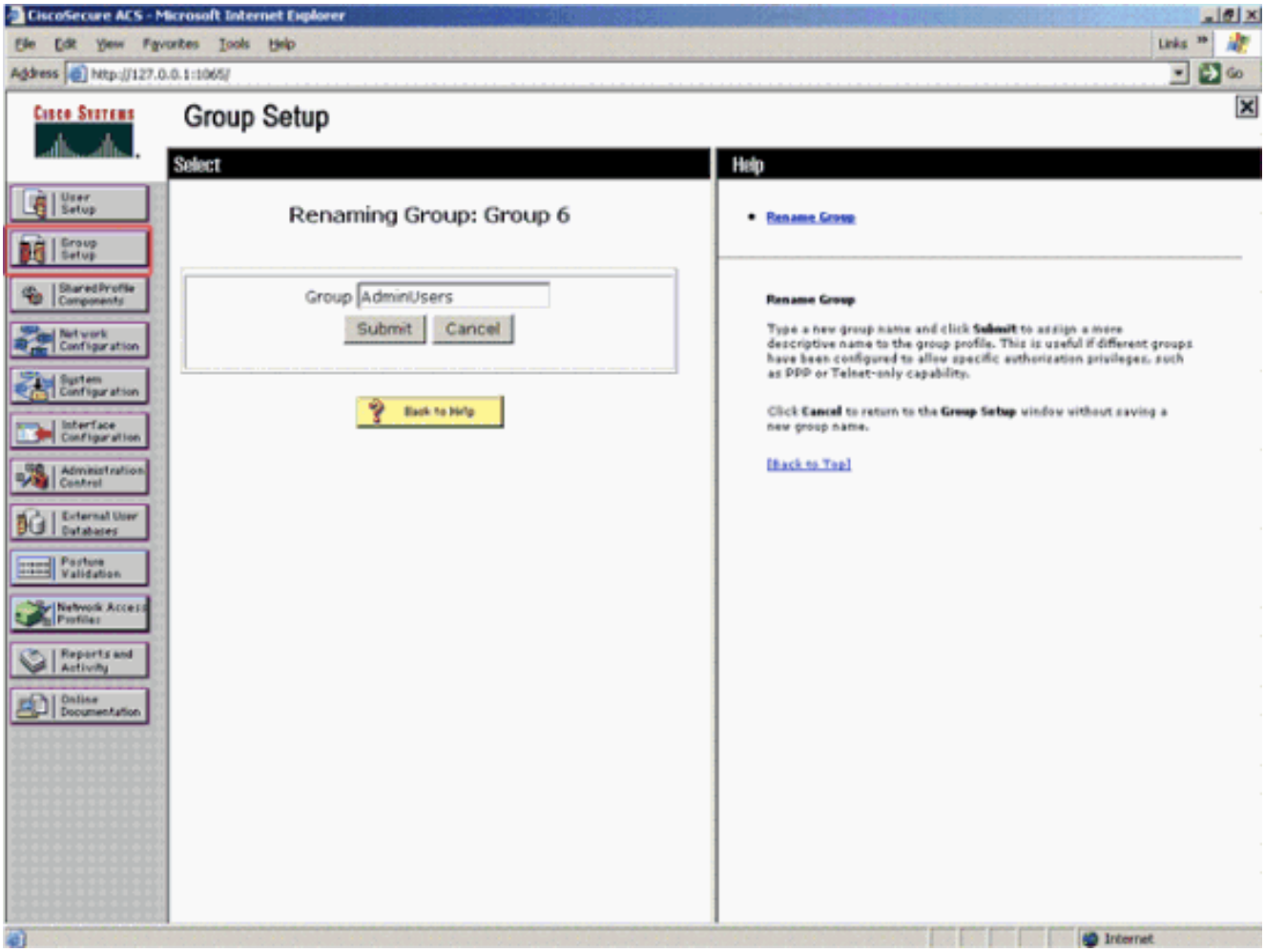
1. Terminez-vous ces étapes afin d'ajouter AP en tant que client d'Authentification, autorisation et comptabilité (AAA) :Du GUI ACS, cliquez sur l'onglet de **configuration réseau**.Sous des clients d'AAA, cliquez sur Add l'**entrée**.Dans la fenêtre de client d'AAA d'ajouter, introduisez le nom d'hôte AP, l'adresse IP d'AP, et une clé secrète partagée.Ceci clé secrète partagée doit être identique que la clé secrète partagée que vous configurez sur AP.De l'authentifier utilisant le menu déroulant, **TACACS+** choisi **(Cisco IOS)**.Cliquez sur Submit **+ reprise** afin de sauvegarder la configuration.Voici un exemple
:



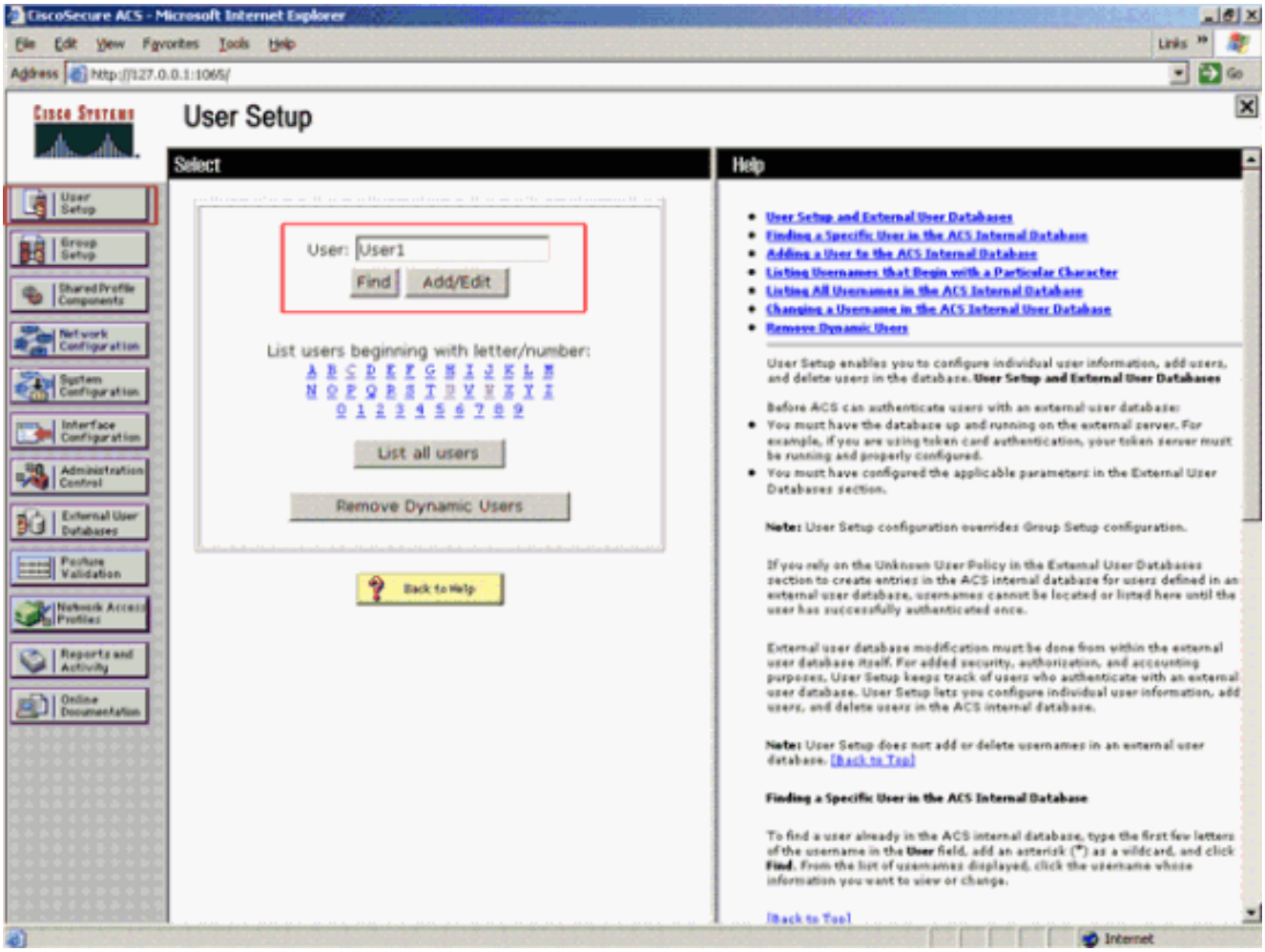
Cet exemple l'utilise :L'adresse Internet **AccessPoint de** client d'AAAL'adresse

172.16.1.30/16 comme adresse IP de client d'AAA**L'exemple** principal secret partagé

2. Terminez-vous ces étapes afin de créer un groupe qui contient tous les utilisateurs administratifs (d'admin) :Cliquez sur le **Group Setup du** menu du côté gauche.Une nouvelle fenêtre apparaît.Dans la fenêtre de Group Setup, sélectionnez un groupe pour configurer du menu déroulant et le clic **renomment le groupe**.Cet exemple sélectionne le groupe 6 du menu déroulant et renomme le groupe AdminUsers.Cliquez sur **Submit**.Voici un exemple :

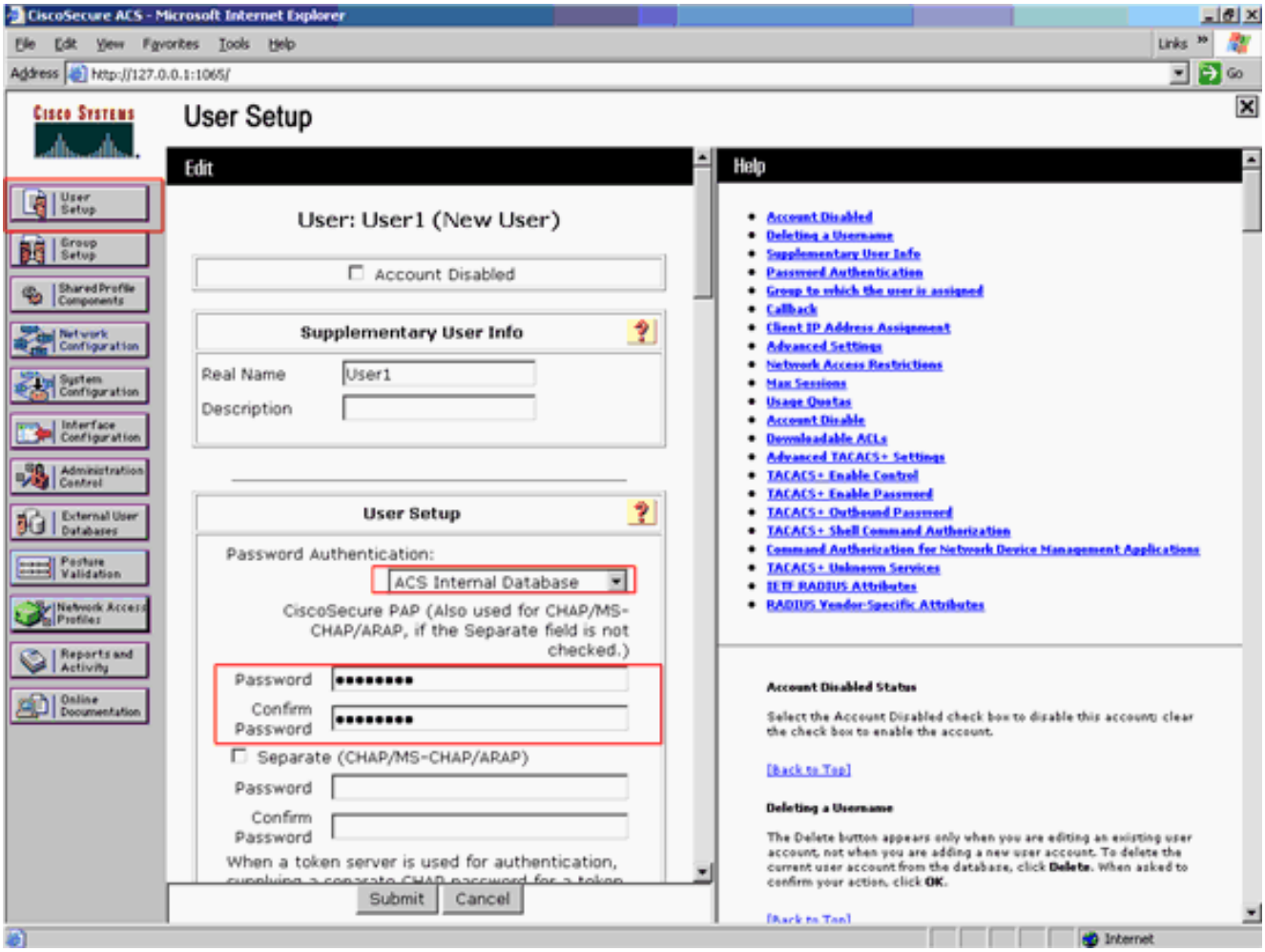


3. Terminez-vous ces étapes afin d'ajouter les utilisateurs à la base de données TACACS+ :Cliquez sur l'onglet d'**installation utilisateur**.Afin de créer un nouvel utilisateur, écrire le nom d'utilisateur dans le domaine d'utilisateur et cliquer sur Add**/éditez**.Voici un exemple, qui crée **User1** :

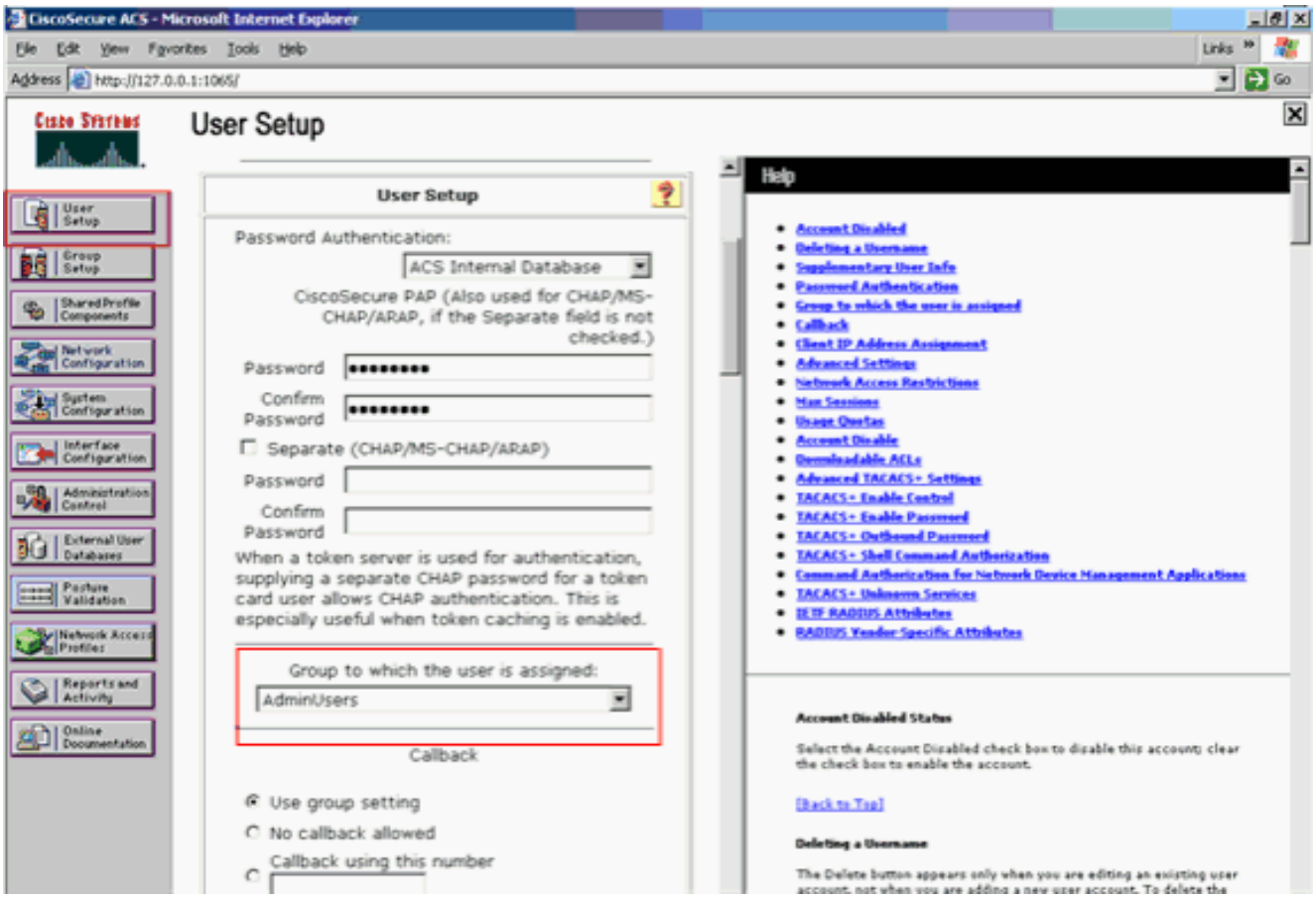


Après que vous cliquiez sur Add/éditez, la fenêtre d'Add/Edit pour cet utilisateur apparaît.

4. Entrez dans les qualifications qui sont spécifiques à cet utilisateur et cliquez sur Submit afin de sauvegarder la configuration.Les qualifications que vous pouvez entrer dans incluent :Les informations utilisateur supplémentairesInstallation utilisateurLe groupe auquel l'utilisateur est assignéVoici un exemple
:



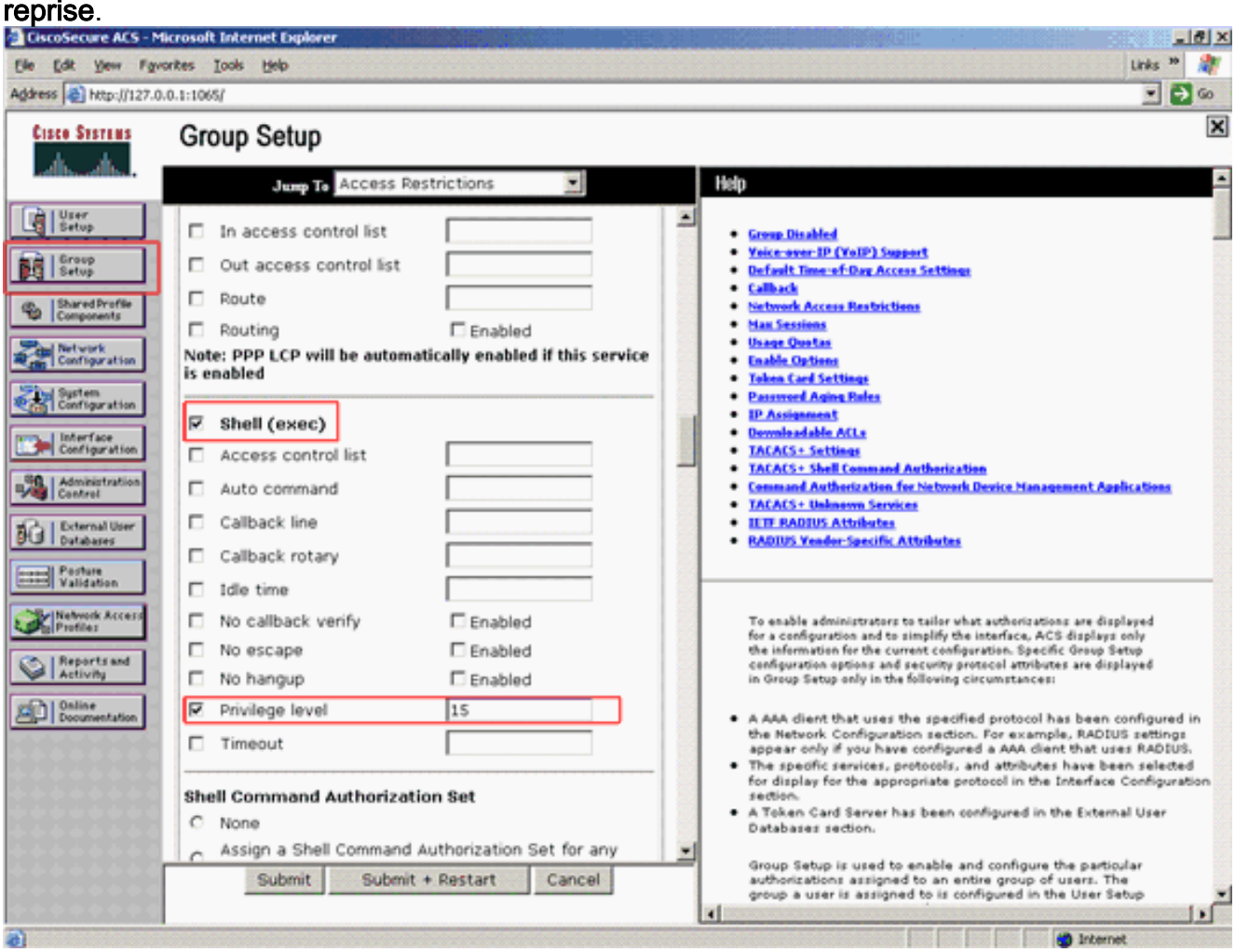
Vous pouvez voir que cet exemple ajoute l'utilisateur User1 au groupe AdminUsers.



Remarque: Si vous ne créez pas un groupe spécifique, les utilisateurs sont assignés au

groupe par défaut.

5. Terminez-vous ces étapes afin de définir le niveau de privilège :Cliquez sur l'onglet de **Group Setup**.Sélectionnez le groupe que vous avez précédemment assigné à cet utilisateur et cliquez sur Edit des **configurations**.Cet exemple utilise le groupe AdminUsers.Sous des configurations TACACS+, cochez la case de **shell (exécutif)** et cochez la case de **niveau de privilège** qui a une valeur de 15.Cliquez sur Submit **+ reprise**.



Remarque: Le niveau de privilège 15 doit être défini pour le GUI et le telnet afin d'être accessible comme niveau 15. Autrement, par défaut, l'utilisateur peut seulement accéder à comme niveau 1. Si le niveau de privilège n'est pas défini et les essais d'utilisateur pour écrire le mode enable sur le CLI (avec l'utilisation du telnet), AP affiche ce message d'erreur :

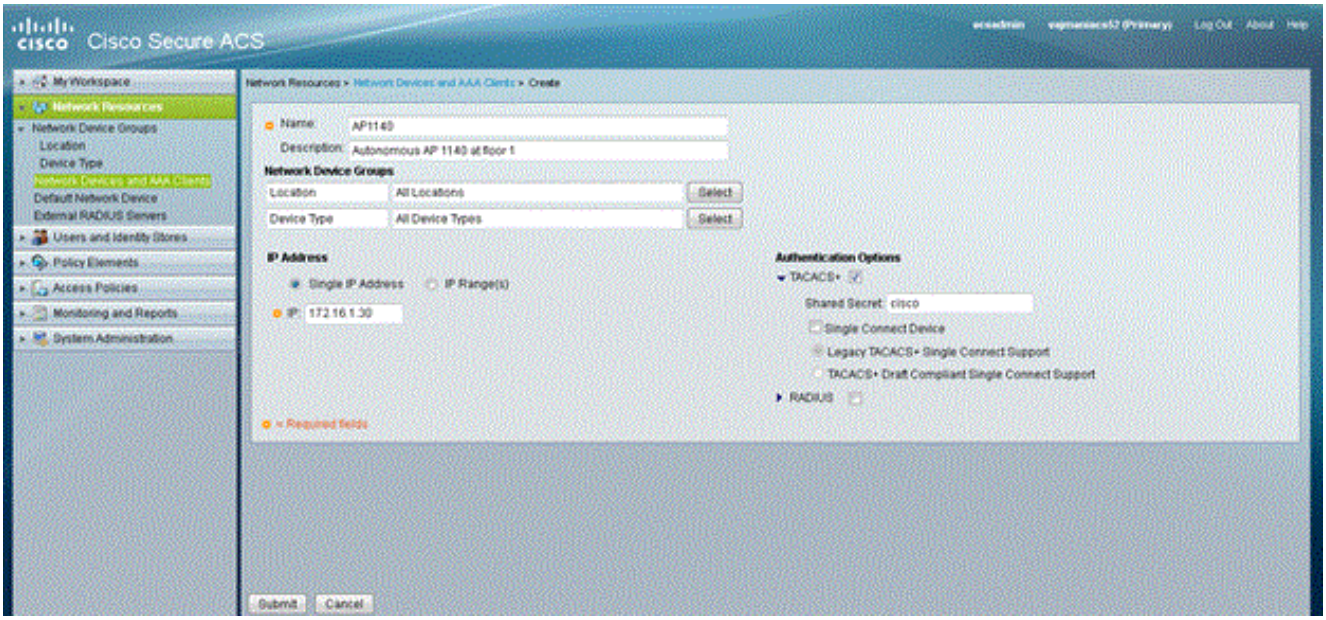
```
AccessPoint>enable
% Error in authentication
```

Répétez les étapes 2 à 4 de cette procédure si vous voulez ajouter plus d'utilisateurs à la base de données TACACS+. Après que vous vous soyez terminé ces étapes, le serveur TACACS+ est prêt à valider les utilisateurs qui essayent d'ouvrir une session à AP. Maintenant, vous devez configurer AP pour l'authentification TACACS+.

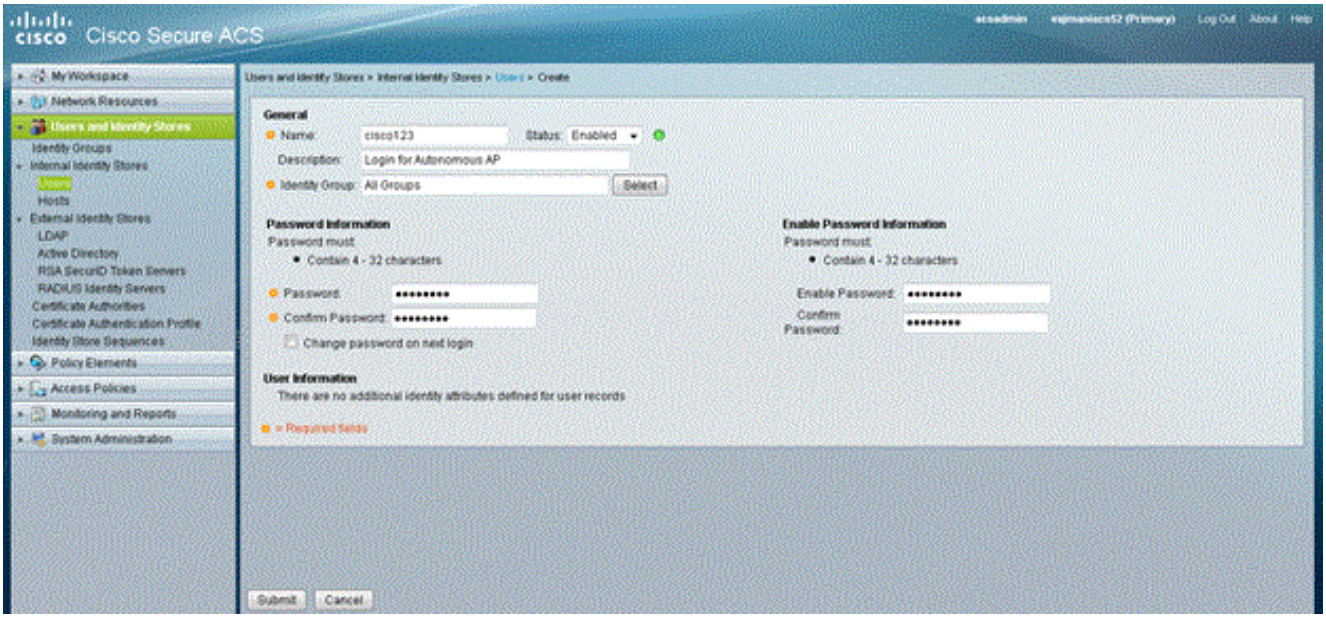
Configurez le serveur TACACS+ pour l'authentification de connexion - Utilisant ACS 5.2

La première étape est d'ajouter AP en tant que client d'AAA dans l'ACS et de créer une stratégie TACACS pour la procédure de connexion.

1. Terminez-vous ces étapes afin d'ajouter AP en tant que client d'AAA :Du GUI ACS, les **ressources de réseau en** clic, cliquent sur alors des **périphériques de réseau et des clients d'AAA**.Sous des périphériques de réseau, le clic **créent**.Entrez dans l'adresse Internet d'AP dans le **nom**, et fournissez une description au sujet d'AP.Sélectionnez l'**emplacement** et le **type de périphérique** si ces catégories sont définies.Puisque seulement AP simple est configuré, cliquez sur l'**adresse IP simple**. Vous pouvez ajouter la plage des adresses IP pour le multiple aps en cliquant sur des **plages IP**. Puis, écrivez l'adresse IP d'AP.Sous des **options d'authentification**, cochez la case **TACACS+** et écrivez le **secret partagé**.Voici un exemple
:

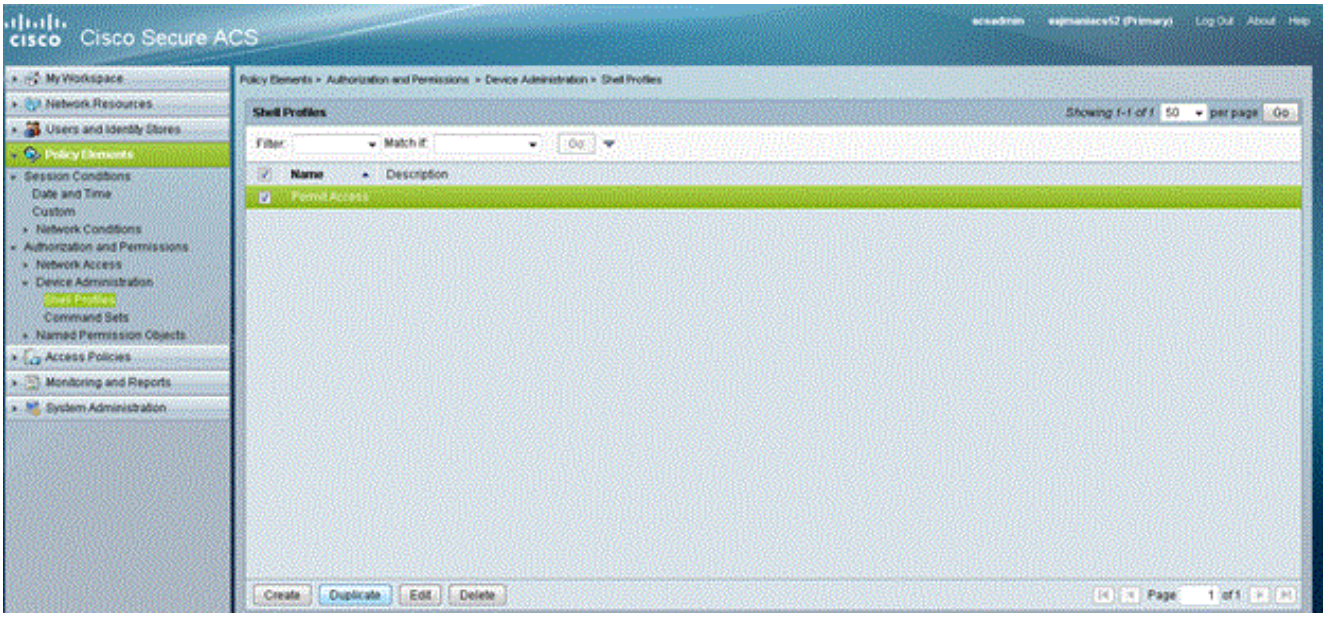


2. L'étape suivante est de créer un nom d'utilisateur et mot de passe de procédure de connexion :Cliquez sur les **utilisateurs et les mémoires d'identité**, puis cliquez sur les **utilisateurs**.Cliquez sur **Create**.Donnez le nom d'utilisateur sous le **nom**, et fournissez une description.Sélectionnez le **groupe d'identité** éventuel.Entrez le mot de passe sous la zone de texte de **mot de passe**, et le ressaisissez sous la **confirmation du mot de passe**.Vous pouvez modifier le mot de passe d'enable en écrivant un mot de passe sous le **mot de passe d'enable**. Confirmation à confirmer.Voici un exemple
:

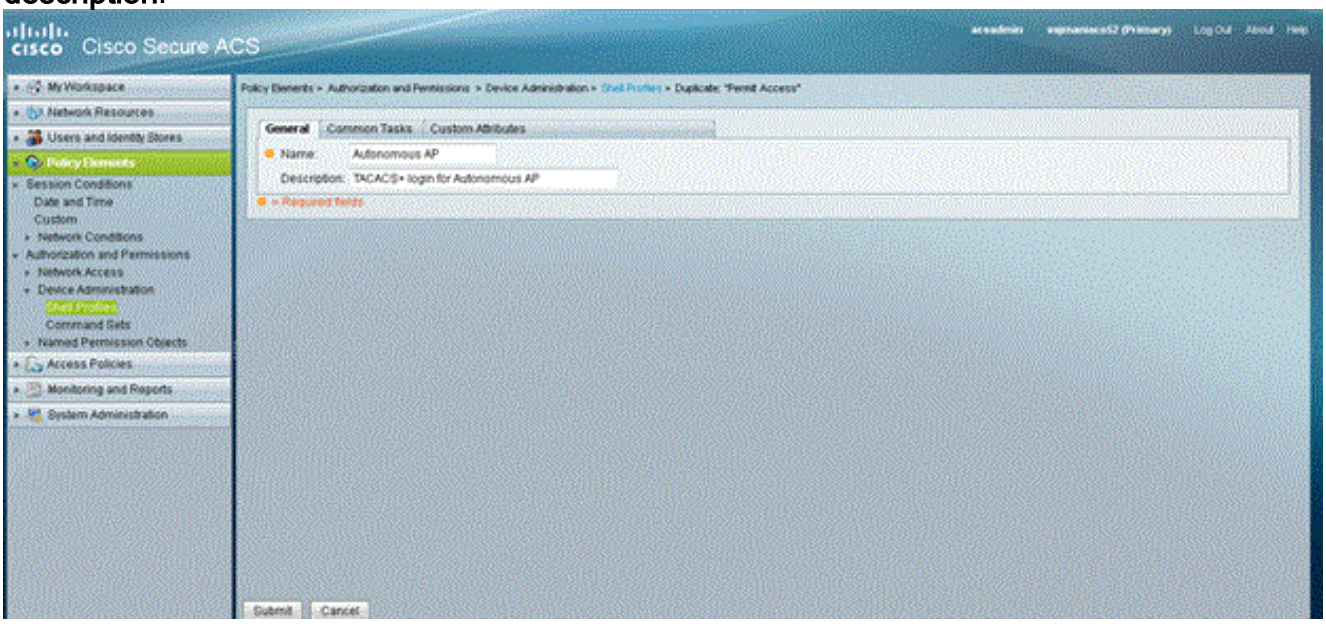


3. Terminez-vous ces étapes afin de définir le niveau de privilège :**Éléments de stratégie de** clic

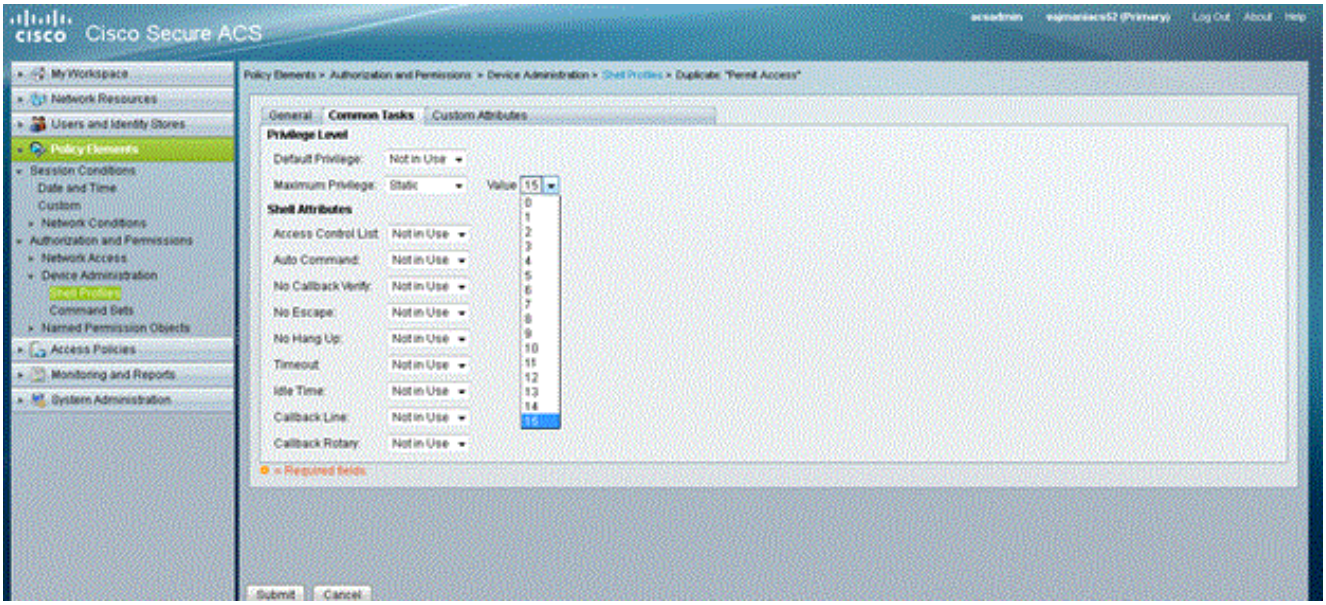
> **autorisations et autorisations** > **profils de gestion** > de **shell de périphérique**.Cochez la case d'**Access d'autorisation** et cliquez sur le **doublon**.



Écrivez le **nom** et la **description**.

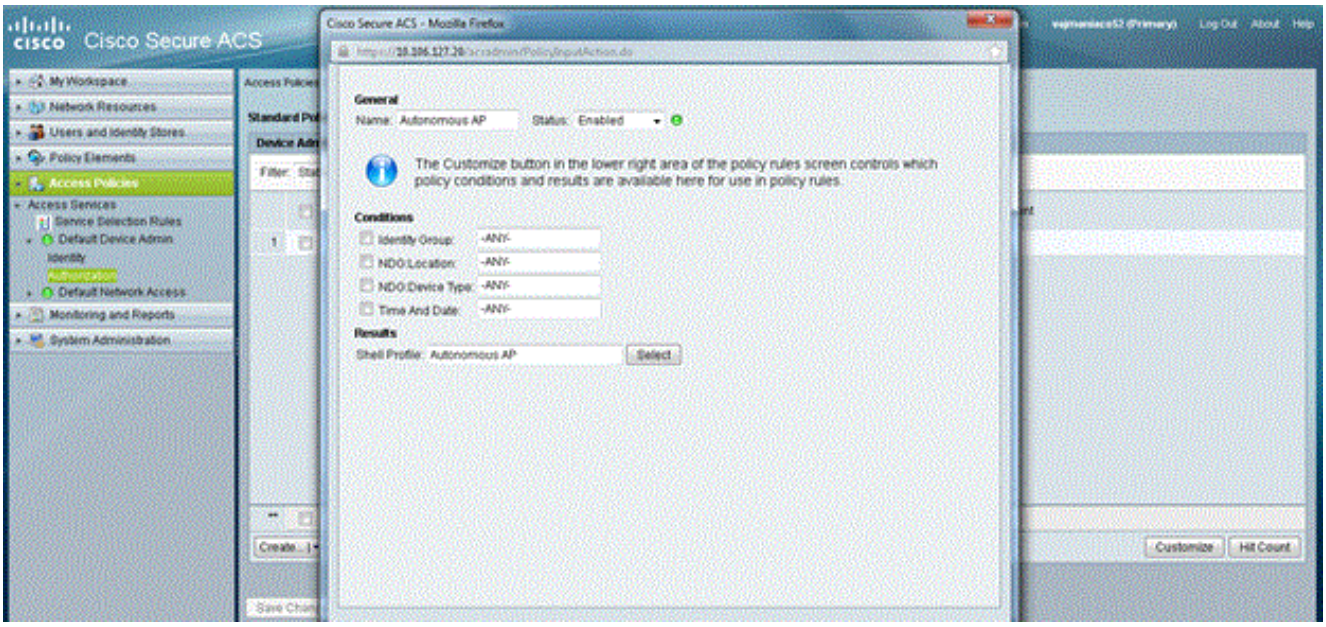


Sélectionnez l'onglet de fonctionnalités usuelles et choisissez **15** pour le privilège maximum.

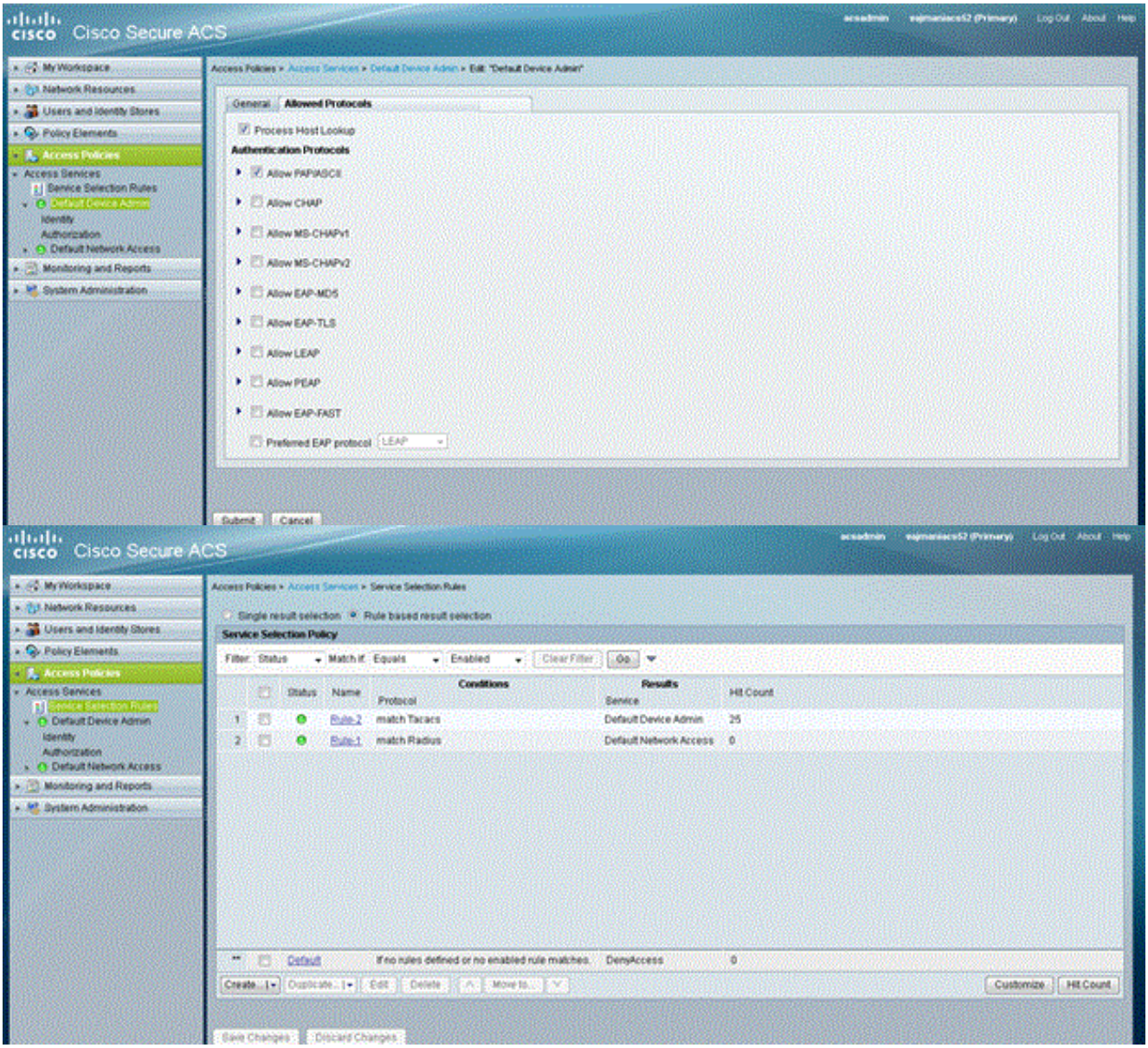


Cliquez sur **Submit**.

4. Terminez-vous ces étapes afin de créer une stratégie d'autorisation :**Stratégies d'Access de** clic **> services d'accès > admin > autorisation de périphérique de par défaut**.Le clic **créent** afin de créer une nouvelle stratégie d'autorisation.Un nouveau s'affiche semble créer les règles pour la stratégie d'autorisation.En sélectionnez le **groupe d'identité**, l'**emplacement** etc. pour le nom d'utilisateur et le client spécifiques d'AAA (AP), si.Le clic **choisi** pour que le profil de shell choisisse le profil a créé AP autonome.



Une fois que ceci est fait, la **sauvegarde de** clic **change**.Cliquez sur l'**admin par défaut de périphérique**, puis cliquez sur les **protocoles permis**.Le contrôle **permettent PAP/ASCII**, puis cliquent sur Submit.**Les règles de sélection de service de** clic de s'assurer il y a une règle appariant TACACS et se dirigeant pour transférer l'admin de périphérique.

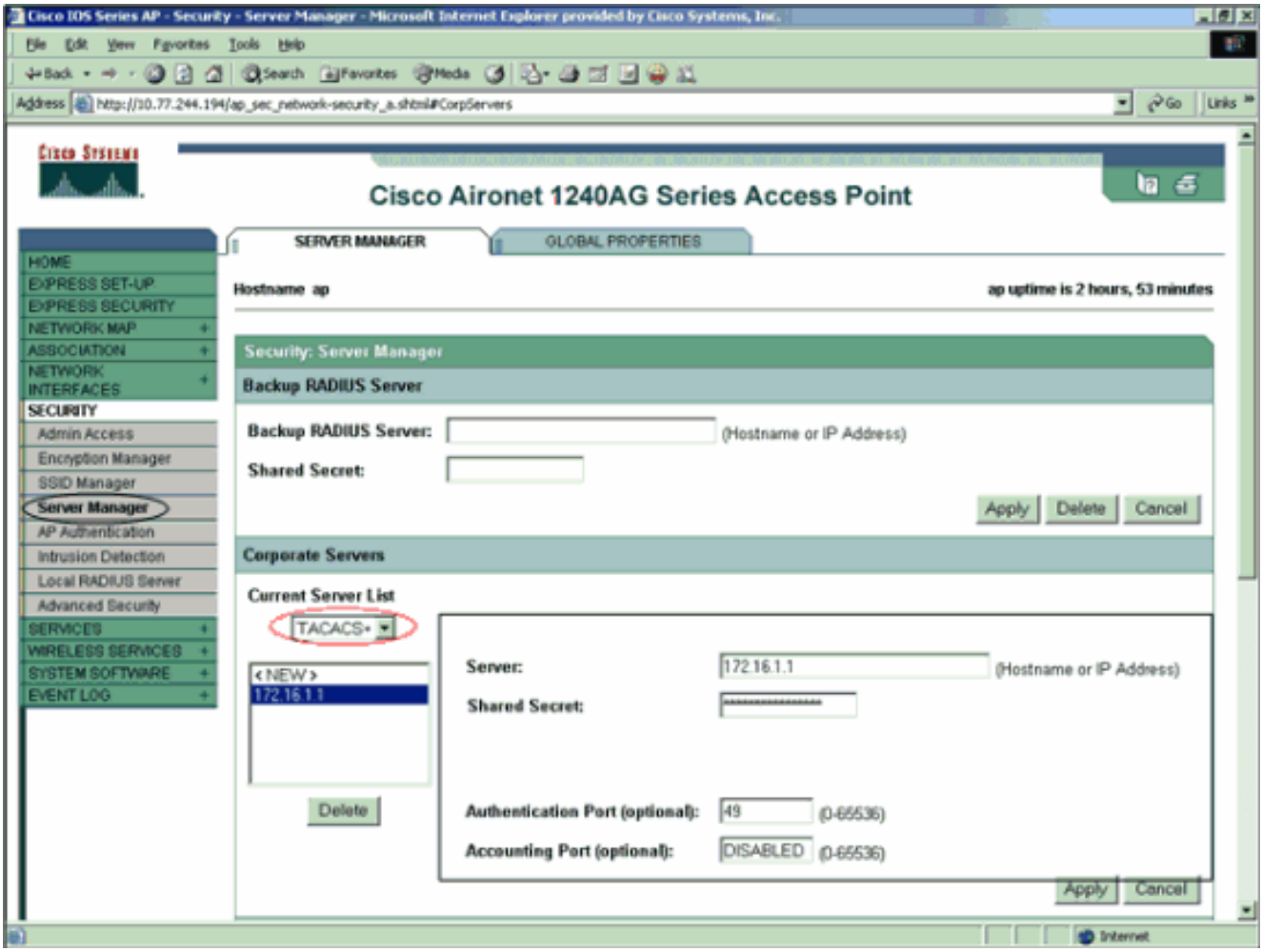


Configurez l'Aironet AP pour l'authentification TACACS+

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

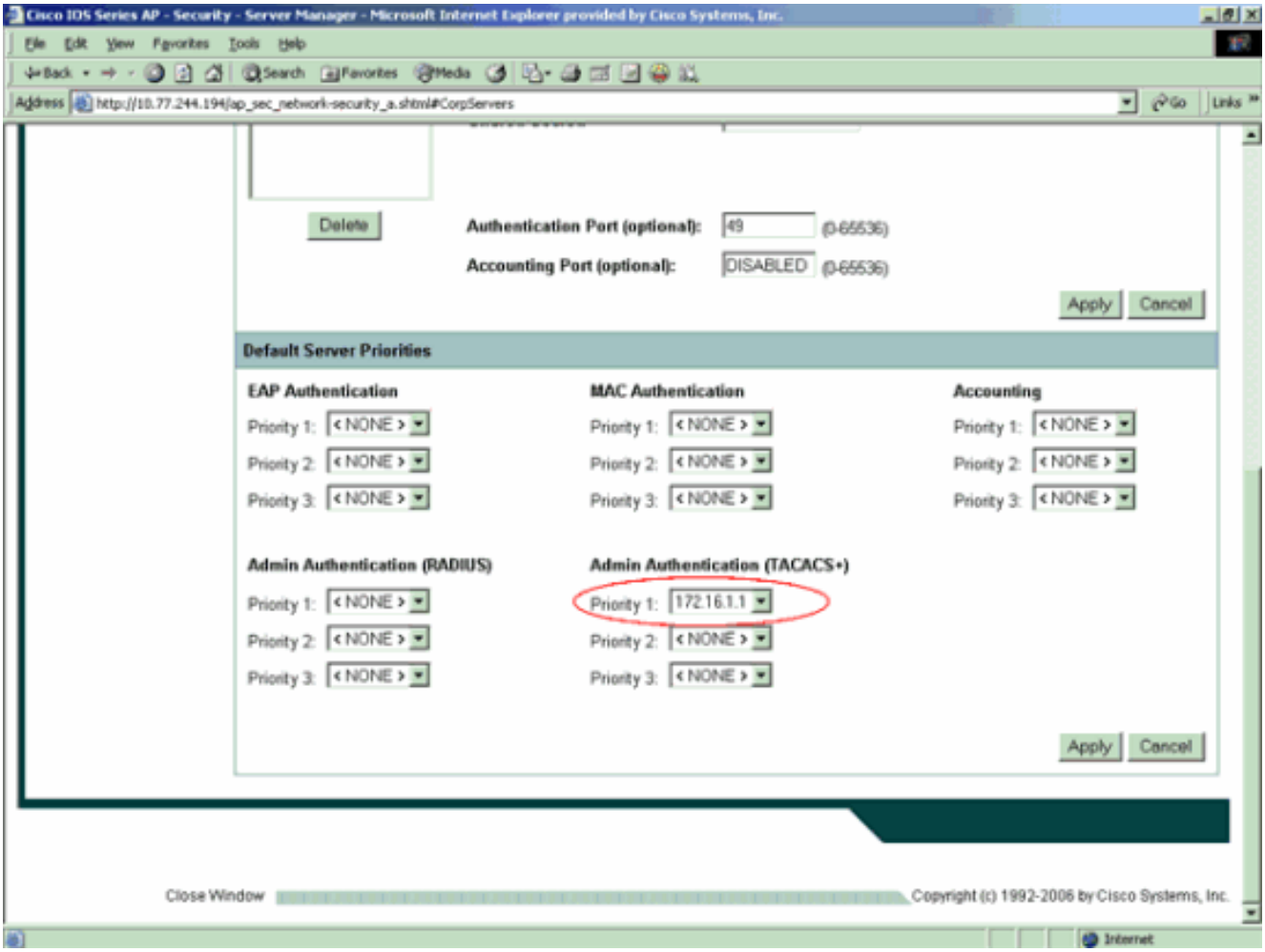
Terminez-vous ces étapes afin de configurer TACACS+ sur AP avec l'utilisation du GUI :

1. Terminez-vous ces étapes afin de définir les paramètres de serveur TACACS+ :Du GUI AP, choisissez le **Security > Server Manager**.La Sécurité : La fenêtre du gestionnaire de serveur apparaît.Dans la région entreprise de serveurs, **TACACS+** choisi du menu déroulant en cours de liste de serveur.Dans cette même zone, introduisez l'adresse IP, le secret partagé, et le numéro de port d'authentification du serveur TACACS+.Cliquez sur **Apply**.Voici un exemple
   :

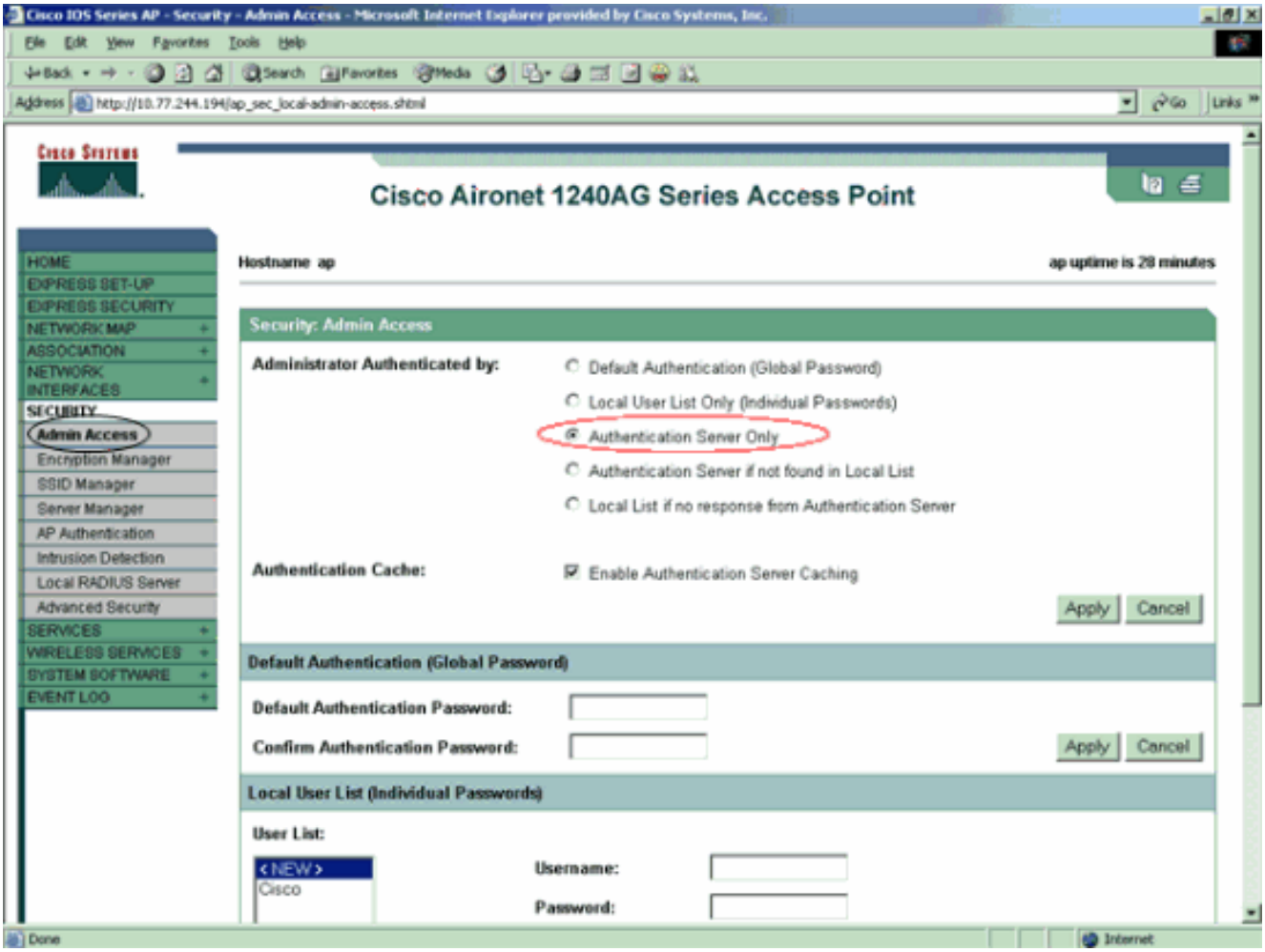


Remarque: Par défaut, TACACS+ utilise le port TCP 49.**Remarque:** La clé secrète partagée que vous configurez sur l'ACS et l'AP doit s'assortir.

2. Choisissez le **Default Server Priorities > l'authentification d'admin (TACACS+)**, choisissez parmi le menu déroulant prioritaire 1 l'adresse IP du serveur TACACS+ que vous avez configurée, et cliquez sur Apply.Voici un exemple
:



3. Choisissez la **Sécurité > l'admin Access** et, parce que l'administrateur authentifié par : , choisissez le **serveur d'authentification seulement** et cliquez sur Apply.Cette sélection s'assure que des utilisateurs qui essayent d'ouvrir une session à AP sont authentifiés par un serveur d'authentification.Voici un exemple
:



C'est la configuration CLI pour l'exemple de configuration :

AccessPoint

```
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
```

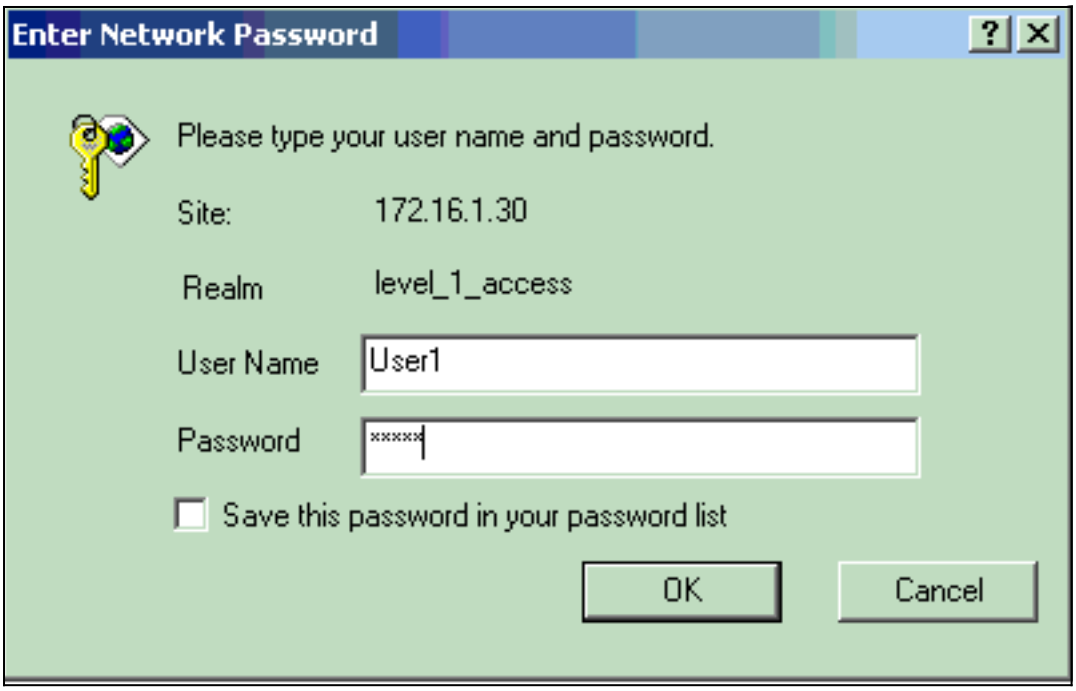
Remarque: Vous devez avoir la version du logiciel Cisco IOS 12.3(7)JA ou plus tard afin de toutes les commandes dans cette configuration de fonctionner correctement. Une version logicielle plus tôt de Cisco IOS ne pourrait pas avoir toutes ces commandes disponibles.

Vérifier

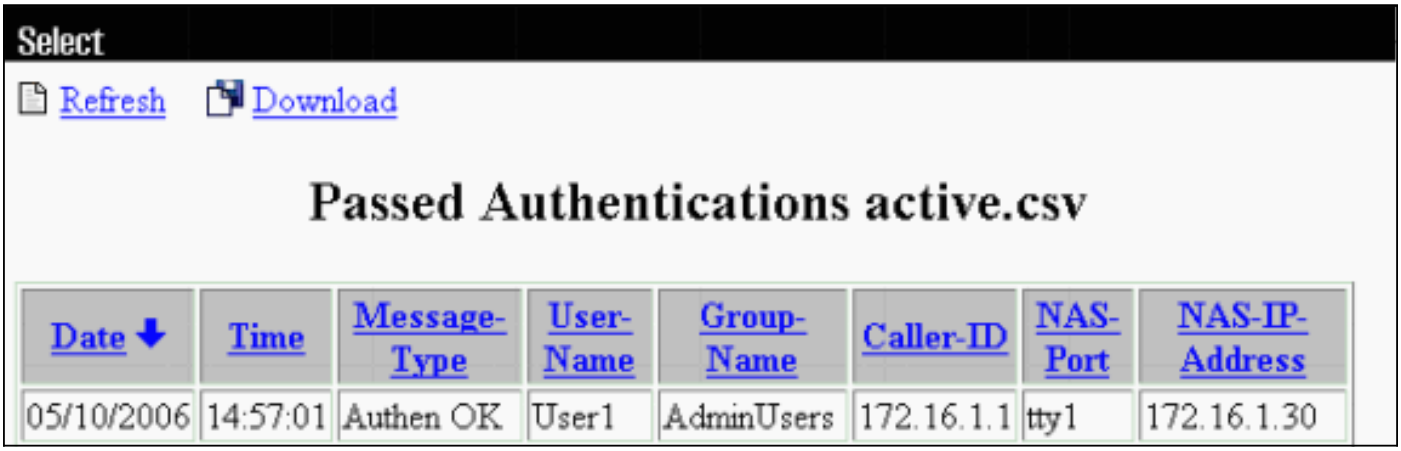
Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

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, l'essai pour ouvrir une session à AP avec l'utilisation du GUI ou le CLI. Quand vous essayez d'accéder à AP, AP vous incite pour un nom d'utilisateur et mot de passe.



Quand vous fournissez les identifiants utilisateurs, AP en avant les qualifications au serveur TACACS+. Le serveur TACACS+ valide les qualifications sur la base de l'information qui est disponible dans sa base de données et permet d'accéder à AP sur l'authentification réussie. Vous pouvez choisir des **états et l'activité > authentification passée** sur l'ACS et employer l'état passé d'authentification afin de vérifier l'authentification réussie pour cet utilisateur. Voici un exemple :



Vous pouvez également utiliser le **show tacacs** commandez 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 tentatives défectueuses/passées pour des qualifications de procédure de connexion de l'ACS 5.2 :

1. **Surveillance de** clic **et états > surveillance et visionneuse de rapports de lancement**.Un nouveau s'affiche s'ouvre avec le tableau de bord.
2. **Authentifications-TACACS-aujourd'hui de** clic. Ceci affiche les détails de tentatives défectueuses/passées.

Dépanner

Vous pouvez employer ces commandes de débogage sur AP afin de dépanner votre configuration :

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **événements de debug tacacs** — Cette commande affiche la séquence d'opérations qui se produisent pendant l'authentification TACACS. Voici un exemple de la sortie 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 de dépanner des problèmes d'authentification HTTP. La commande affiche la méthode d'authentification que le routeur ont tentée et les messages d'état d'authentification-particularité.

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

Si l'utilisateur écrit un nom d'utilisateur qui n'existe pas sur le serveur TACACS+, l'authentification échoue. Voici l'**authentication command de debug tacacs** sortie pour une authentification défaillante :

```
*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 des **états et l'activité > l'authentification défaillante** afin de voir la tentative d'authentification défaillante sur l'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 logicielle de Cisco IOS sur AP qui est plus tôt que la version du logiciel Cisco IOS 12.3(7)JA, vous pouvez frapper une bogue chaque fois que vous essayez d'ouvrir une session à AP avec l'utilisation du HTTP. L'ID de bogue Cisco est CSCeb52431 (clients enregistrés seulement).

L'implémentation du logiciel HTTP/AAA de Cisco IOS exige l'authentification indépendante de chacun connexion HTTP distincte. Le GUI Sans fil de logiciel de Cisco IOS implique la référence de beaucoup de douzaines de fichiers séparés dans une page Web simple (par exemple Javascript et GIF). Ainsi si vous chargez un d'une seule page dans le GUI Sans fil de logiciel de Cisco IOS, des douzaines et des douzaines d'authentification/de demandes d'autorisation distinctes peut frapper le serveur d'AAA.

Pour l'authentification HTTP, l'utilisation RADIUS ou l'authentification locale. Le serveur de RADIUS est encore soumis aux plusieurs demandes d'authentification. Mais RADIUS est plus extensible que TACACS+, et ainsi il est susceptible de fournir une incidence des performances moins-défavorable.

Si vous devez utiliser TACACS+ et vous avez Cisco ACS, utilisez le mot clé de **single-connection** avec l'ordre de **serveur TACACS**. L'utilisation de ce mot clé avec la commande épargne l'ACS plus de la connexion TCP installée/de temps système de désinstallation et est susceptible de réduire le chargement sur le serveur dans une certaine mesure.

Pour des versions du logiciel Cisco IOS 12.3(7) JA et plus tard AP, le logiciel inclut une difficulté. Le reste de cette section décrit la difficulté.

Employez la caractéristique de cache d'authentification d'AAA afin de cacher les informations que le serveur TACACS+ renvoie. La caractéristique de cache et de profil d'authentification permet à AP pour cacher les réponses d'authentification/autorisation pour un utilisateur de sorte que l'authentification/demandes d'autorisation ultérieures n'ait pas besoin d'être envoyée au serveur d'AAA. Afin d'activer cette caractéristique avec le CLI, utilisez ces commandes :

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

Pour plus d'informations sur cette caractéristique et les commandes, référez-vous à *configurer la* section de *cache et de profil d'authentification de* gérer le Point d'accès.

Afin d'activer cette caractéristique sur le GUI, choisir la **Sécurité > l'admin Access** et cocher la case de **mise en cache de serveur d'authentification d'enable**. Puisque ce document utilise la version du logiciel Cisco IOS 12.3(7)JA, le document utilise la difficulté, car les configurations illustrent.

Informations connexes

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