TACACS+ op een Aironet access point voor loginverificatie met gebruik van het GUI-configuratievoorbeeld

Inhoud

Inleiding

Dit document legt uit hoe u TACACS Plus (TACACS+) services kunt inschakelen op een Cisco Aironet Access Point (AP) om inlogverificatie met gebruik van een TACACS+ server uit te voeren.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Kennis van de manier waarop u fundamentele parameters op Aironet APs kunt configureren
- Kennis van de manier waarop u een TACACS+ server kunt configureren zoals Cisco Secure Access Control Server (ACS)
- Kennis van TACACS+-concepten

Raadpleeg voor informatie over de manier waarop TACACS+ werkt het *begrip TACACS+* gedeelte van RADIUS- en TACACS+ servers configureren.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Aironet Cisco Aironet 1240/1140 Series access points
- ACS dat softwareversie 4.1 uitvoert
- ACS dat softwareversie 5.2 uitvoert

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Configureren

Deze sectie legt uit hoe u Aironet AP en de TACACS+ server (ACS) moet configureren voor TACACS+-gebaseerde aanmelding-verificatie.

Dit configuratievoorbeeld gebruikt deze parameters:

- IP-adres van de ACS-172.16.1.1/255.255.0.0
- IP-adres van AP-172.16.1.30/255.255.0.0
- Gedeelde geheime sleutel die op AP en TACACS+ server-**Voorbeeld** wordt gebruikt

Dit zijn de referenties van de gebruiker die dit voorbeeld op ACS vormt:

- Gebruikersnaam—**Gebruiker1**
- Wachtwoord—**Cisco**
- Groep-**Admin-gebruikers**

U dient de functies TACACS+ te configureren om de gebruikers te valideren die proberen verbinding te maken met de AP via de webinterface of via de opdrachtregel interface (CLI). Om deze configuratie te kunnen uitvoeren, dient u deze taken uit te voeren:

1. Configureer de TACACS+ server voor inlogverificatie.
2. Configureer de Aironet AP voor TACACS+ verificatie.

N.B.: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

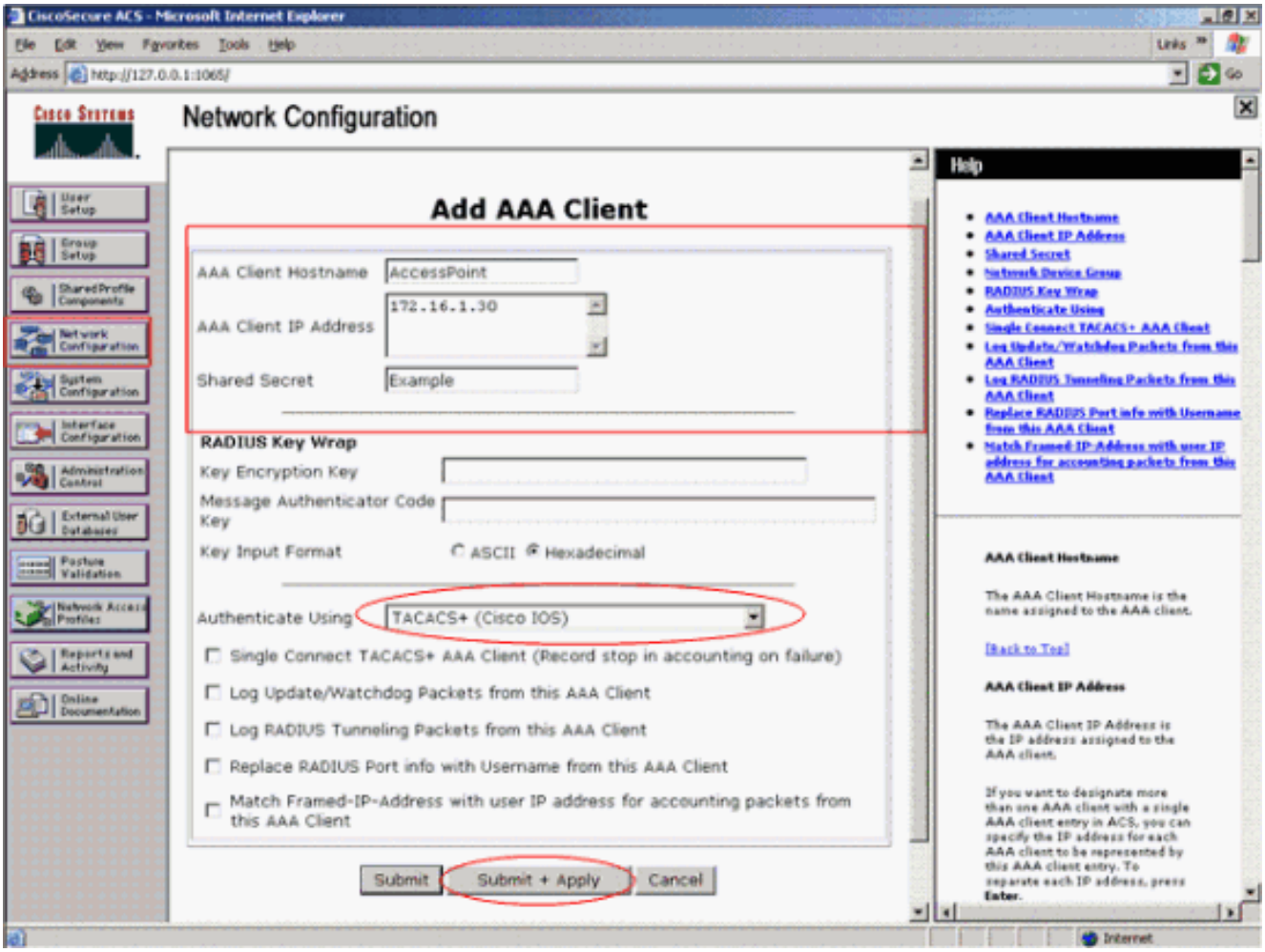
Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:

Configureer de TACACS+ server voor inlogverificatie - met behulp van ACS 4.1

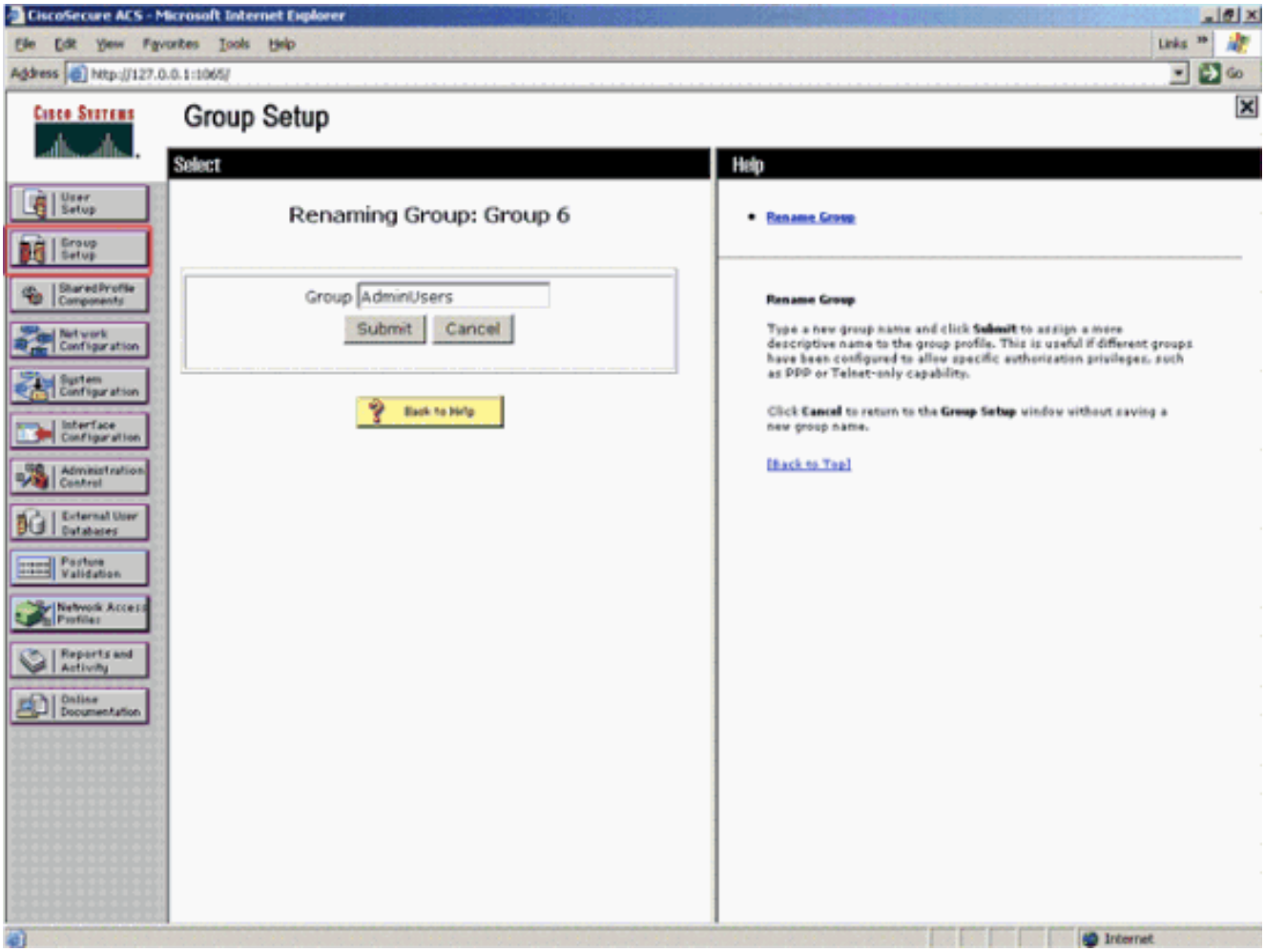
De eerste stap is het instellen van een TACACS+-daemon om de gebruikers te valideren die proberen toegang te krijgen tot de AP. U moet de ACS voor TACACS+ verificatie instellen en een gebruikersdatabase maken. U kunt elke TACACS+ server gebruiken. Dit voorbeeld gebruikt ACS als de TACACS+ server. Voer de volgende stappen uit:

1. Voltooi deze stappen om het AP toe te voegen als een verificatie-, autorisatie- en boekhoudcliënt (AAA):Klik vanuit de ACS-GUI op het tabblad **Netwerkconfiguratie**.Klik onder AAA-clients op **Toevoegen**.Voer in het venster Add AAA Client de AP host-naam, het IP-adres van de AP en een gedeelde geheime sleutel in.Deze gedeelde geheime sleutel moet dezelfde zijn als de gedeelde geheime sleutel die u op de AP vormt.Selecteer in het vervolgkeuzemenu Verifiëren met behulp van **TACACS+ (Cisco IOS)**.Klik op **Indienen + Herstart** om de configuratie op te slaan.Hierna volgt een voorbeeld:

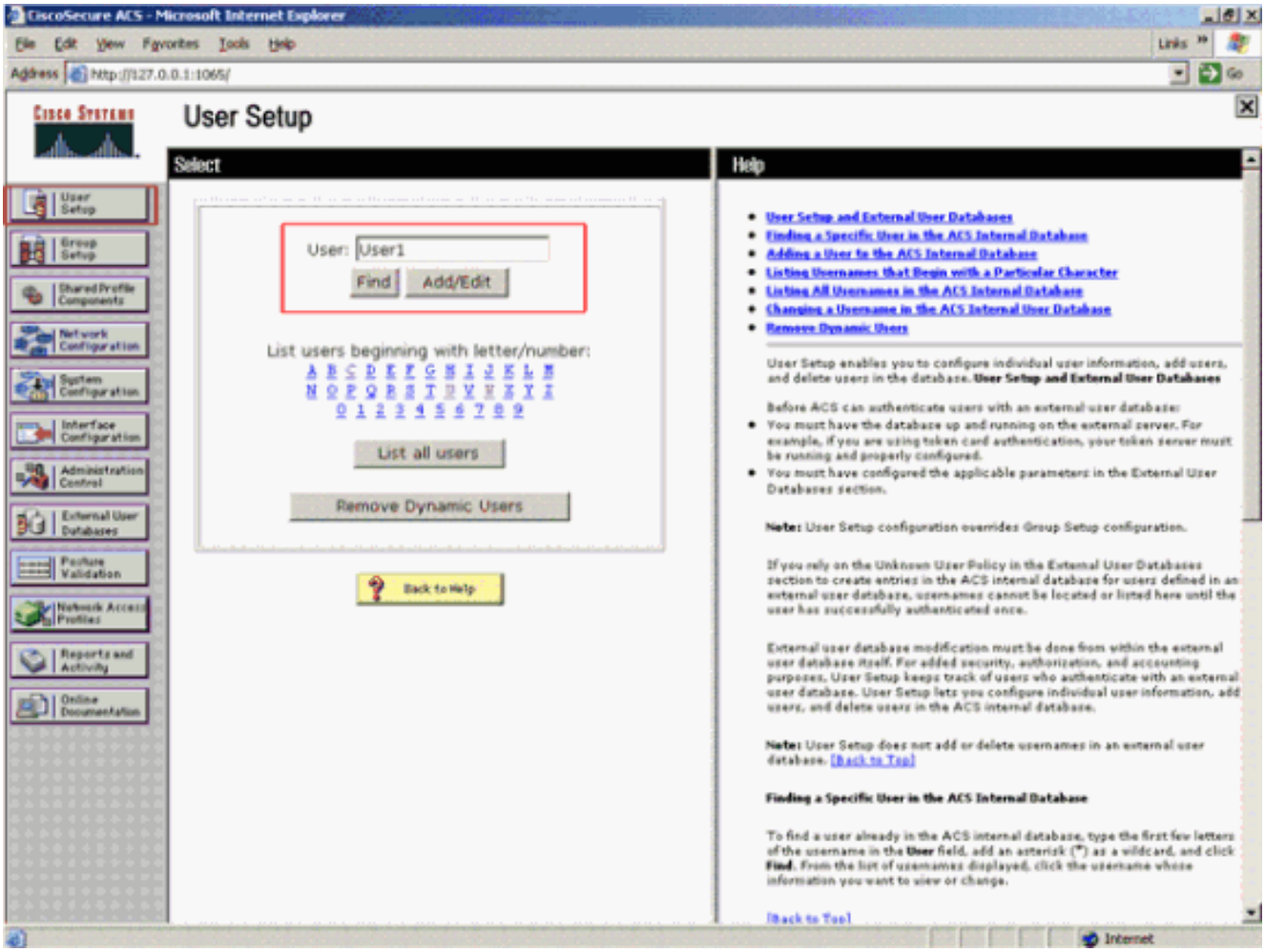


In dit voorbeeld wordt gebruik gemaakt van:Het AAA-**clientadapterpunt**Het adres **172.16.1.30/16** als het AAA-client-IP-adresHet gedeelde geheime sleutelvoorbeeld

2. Voltooi deze stappen om een groep te maken die alle administratieve (admin) gebruikers bevat:Klik op **Groepsinstelling** in het menu links.Er verschijnt een nieuw venster.Selecteer in het venster Groepsinstallatie een groep die u in het vervolgkeuzemenu wilt configureren en klik op **Hernoemen**.Dit voorbeeld selecteert Groep 6 in het vervolgkeuzemenu en geeft de groep AdminGebruikers een andere naam.Klik op **Inzenden**.Hierna volgt een voorbeeld:

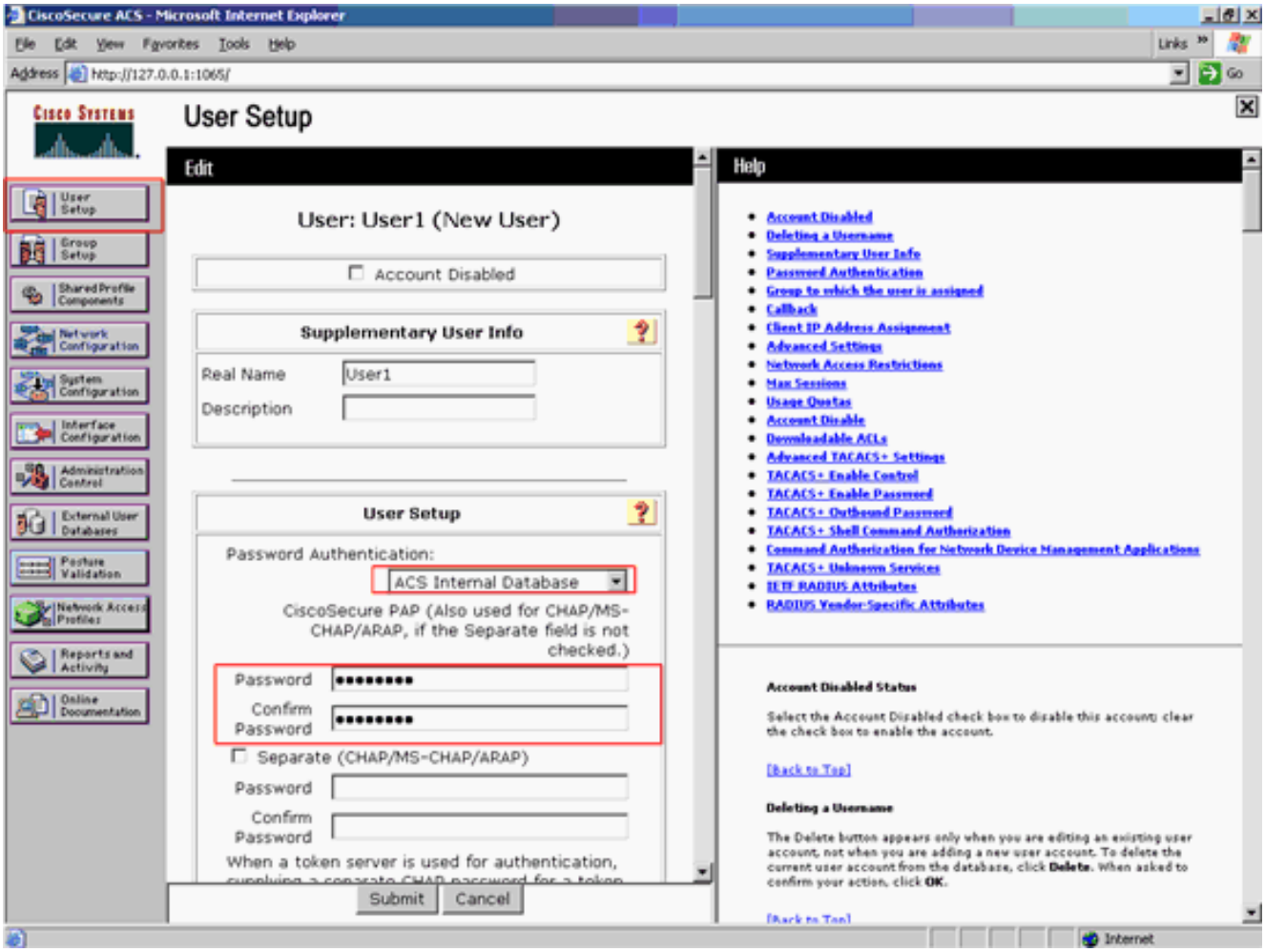


3. Voltooi deze stappen om de gebruikers aan de TACACS+-database toe te voegen:Klik op het tabblad **Gebruikersinstelling**.Als u een nieuwe gebruiker wilt maken, voert u de gebruikersnaam in het veld Gebruiker in en klikt u op **Toevoegen/Bewerken**.Hier is een voorbeeld dat **Gebruiker1**
maakt:

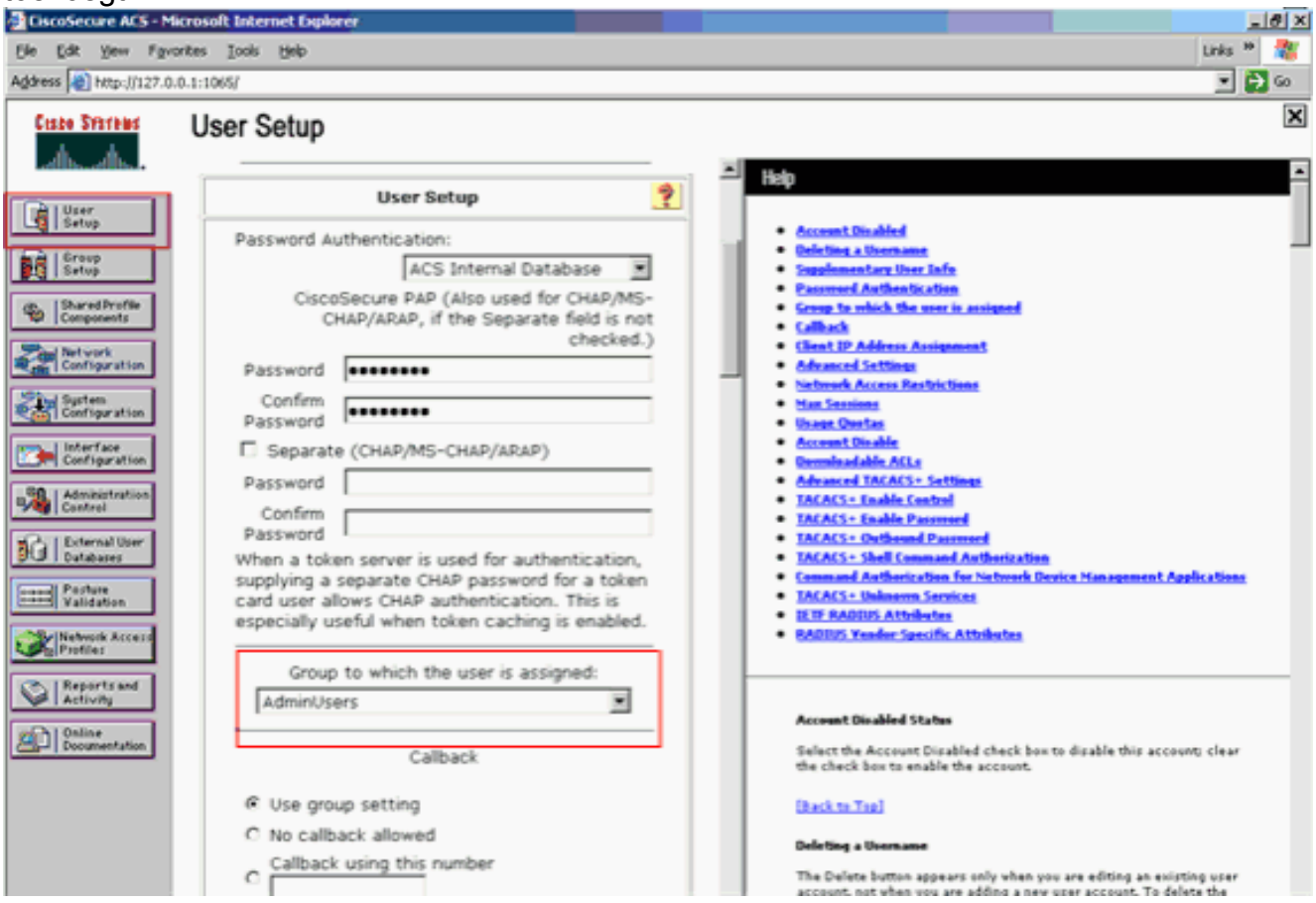


Nadat u op Toevoegen/Bewerken klikt, verschijnt het venster Toevoegen/Bewerken voor deze gebruiker.

4. Voer aanmeldingsgegevens in die specifiek zijn voor deze gebruiker en klik op **Indienen** om de configuratie op te slaan.De geloofsbrieven die u kunt binnengaan omvatten:Aanvullende gebruikersinformatieInstellingen gebruikerDe groep waaraan de gebruiker is toegewezenHierna volgt een
voorbeeld:



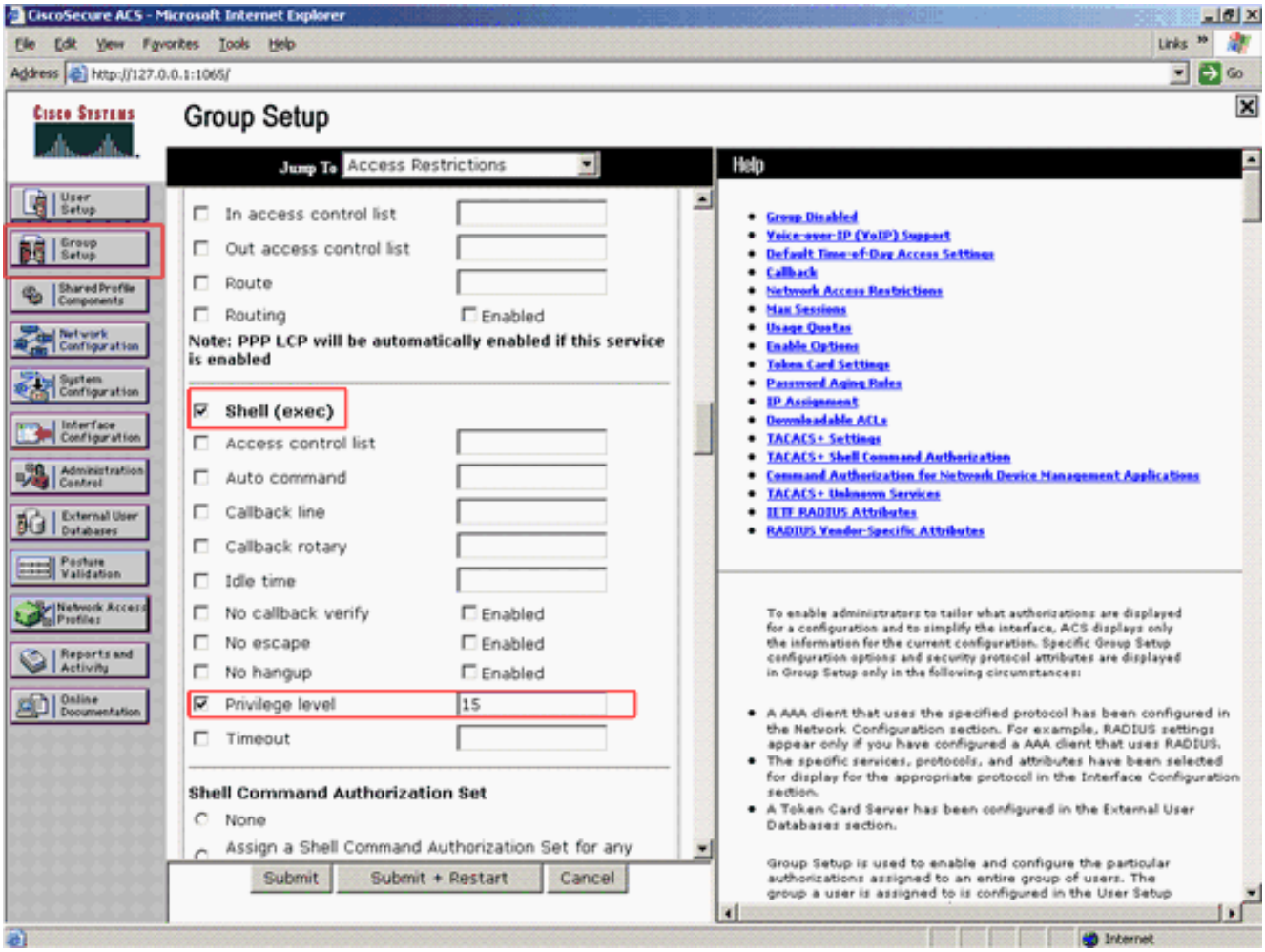
U kunt zien dat dit voorbeeld de gebruiker User1 aan de groep AdminGebruikers toevoegt.



N.B.: Als u geen specifieke groep maakt, worden de gebruikers toegewezen aan de

standaardgroep.

5. Voltooi deze stappen om het voorkeursniveau te bepalen:Klik op het tabblad **Groepsinstallatie**.Selecteer de groep die u eerder aan deze gebruiker hebt toegewezen en klik op **Instellingen bewerken**.Dit voorbeeld gebruikt de groep AdminGebruikers.Controleer onder TACACS+ instellingen het aanvinkvakje **Shell (exec)** en controleer het aanvinkvakje **Privileniveau** dat een waarde van 15 heeft.Klik op **Inzenden + opnieuw starten**.



Opmerking: Privacyniveau 15 moet voor de GUI en telnet worden gedefinieerd om toegankelijk te zijn als niveau 15. Anders kan de gebruiker standaard alleen toegang hebben tot niveau 1. Als het voorkeursniveau niet is gedefinieerd en de gebruiker probeert om mode op de CLI (met gebruik van telnet) in te schakelen, wordt deze foutmelding weergegeven door AP:

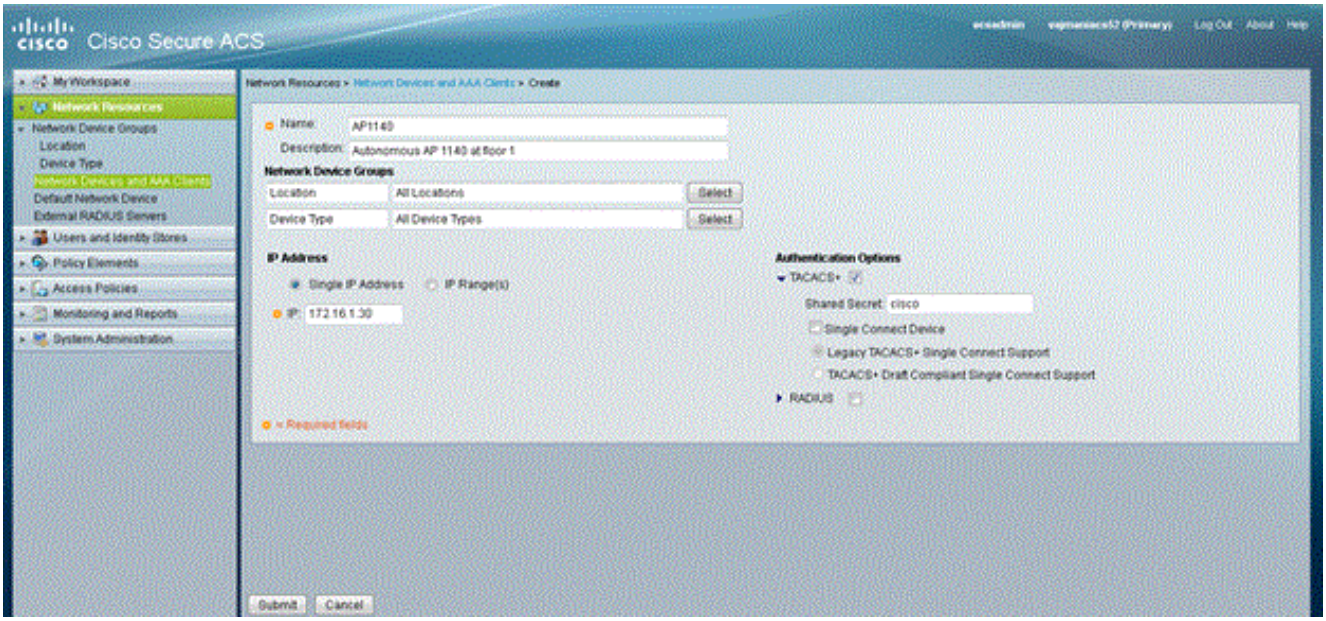
```
AccessPoint>enable
% Error in authentication
```

Herhaal stap 2 tot en met 4 van deze procedure als u meer gebruikers aan de TACACS+ database wilt toevoegen. Nadat u deze stappen hebt voltooid, is de TACACS+ server klaar om gebruikers te valideren die proberen in te loggen op AP. U moet nu de AP configureren voor TACACS+ verificatie.

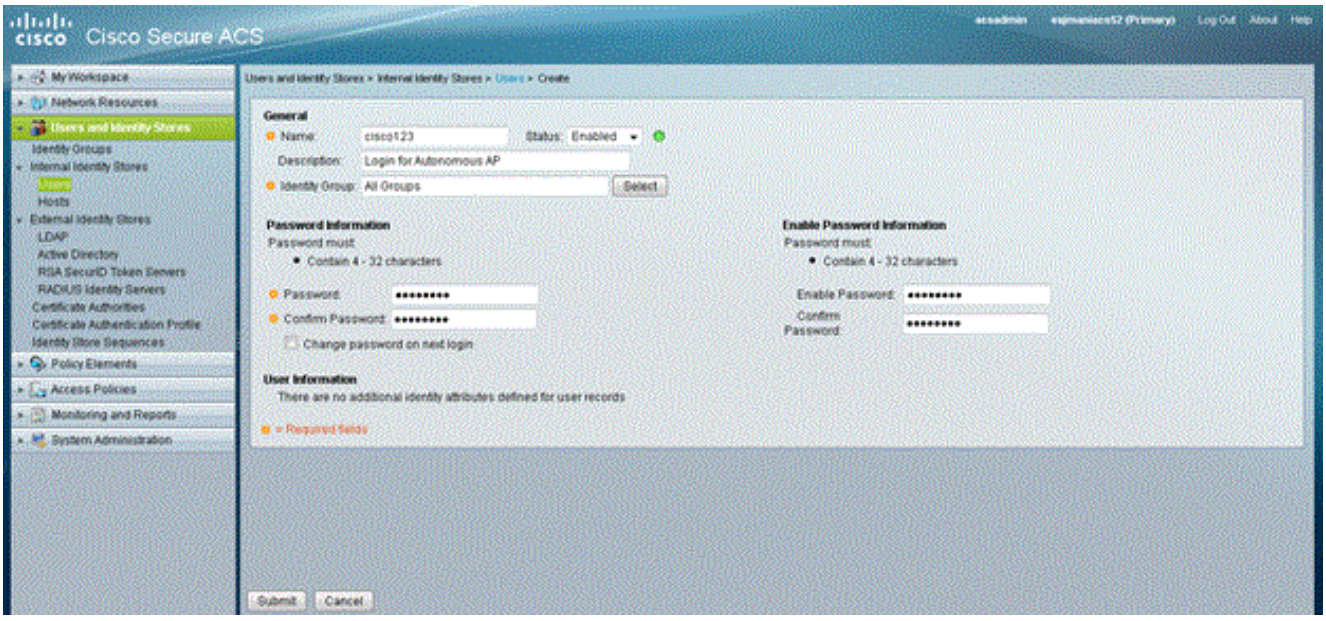
Configureer de TACACS+ server voor inlogverificatie - met behulp van ACS 5.2

De eerste stap is om AP als een AAA-client in de ACS toe te voegen en een TACACS-beleid te maken voor de inlognaam.

1. Voltooi deze stappen om AP als een AAA-client toe te voegen:Klik vanuit de ACS GUI, op **Netwerkbronnen** en vervolgens op **Netwerkapparaten en AAA-clients**.Klik onder Netwerkapparaten op **Maken**.Voer de hostnaam van de AP in in **Name**, en geef een beschrijving van de AP.Selecteer de **locatie** en het **type apparaat** als deze categorieën zijn gedefinieerd.Omdat slechts één AP wordt gevormd, klik op **ÉÉN IP Adres**. U kunt het bereik van IP-adressen toevoegen voor meerdere AP's door op **IP-bereik(s)** te klikken. Voer vervolgens het IP-adres van het AP in.Onder **Verificatieopties**, controleer het **TACACS+** vakje en voer het **gedeelde geheim** in.Hierna volgt een voorbeeld:

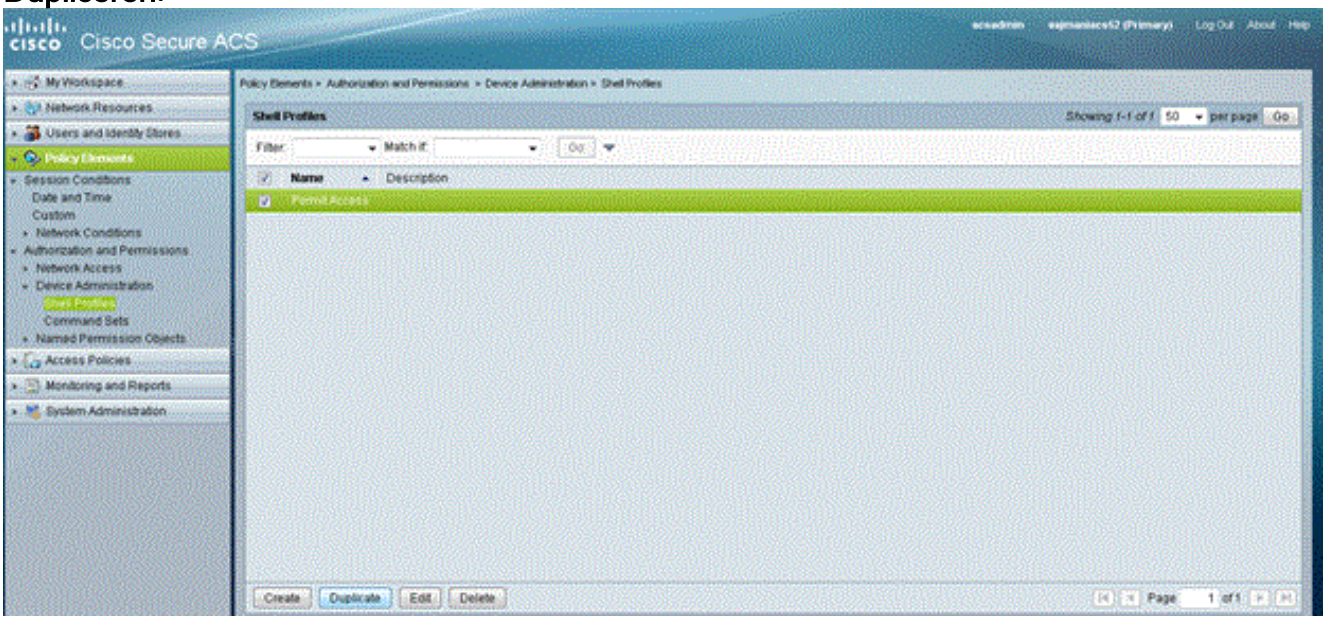


2. De volgende stap is het maken van een inloggebruikersnaam en een wachtwoord:Klik op **Gebruikers en identiteitsopslag** en vervolgens op **gebruikers**.Klik op **Maken**.Geef de gebruikersnaam op onder **Naam** en geef een beschrijving.Selecteer de eventuele **identiteitsgroep**.Voer het wachtwoord in onder het tekstvak **Wachtwoord** en voer het opnieuw in onder **Wachtwoord voor bevestigen**.U kunt het wachtwoord voor het inschakelen wijzigen door een wachtwoord in te voeren onder **Wachtwoord voor inschakelen**. Voer dit nogmaals in om het te bevestigen.Hierna volgt een voorbeeld:

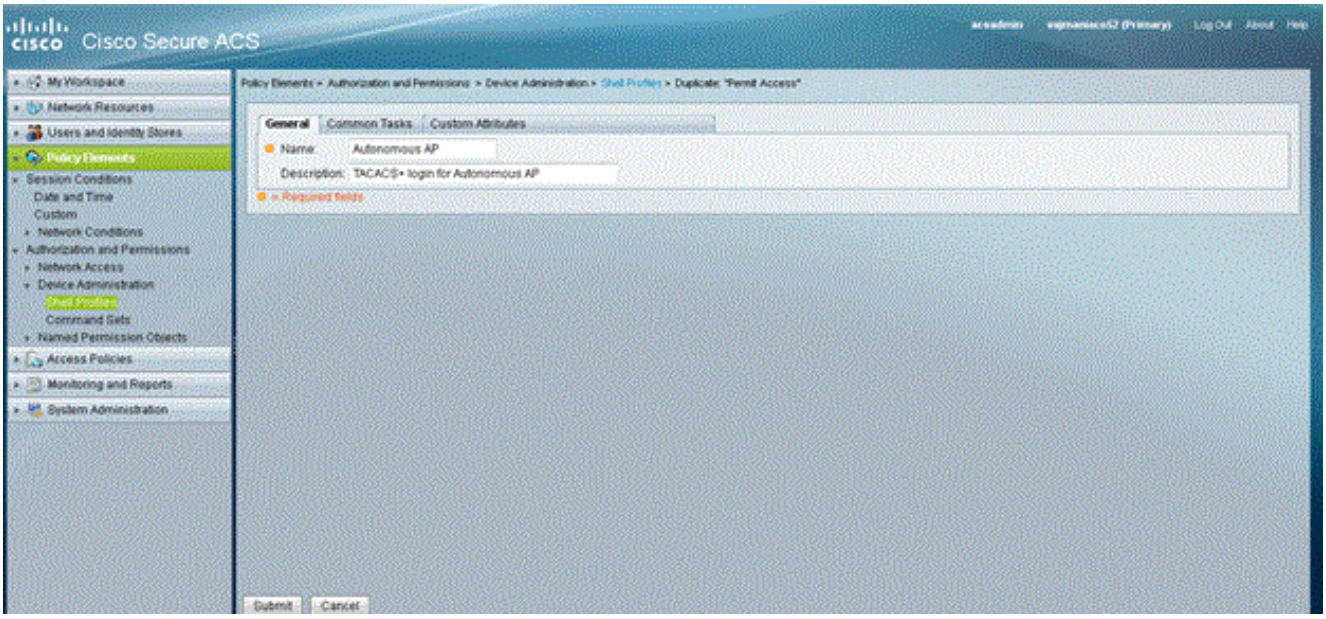


3. Voltooi deze stappen om het voorkeursniveau te bepalen:Klik op **Beleidselementen** > **Vergunningen en toegangsrechten** > **Apparaatbeheer** > **Shell-profielen**.Controleer het

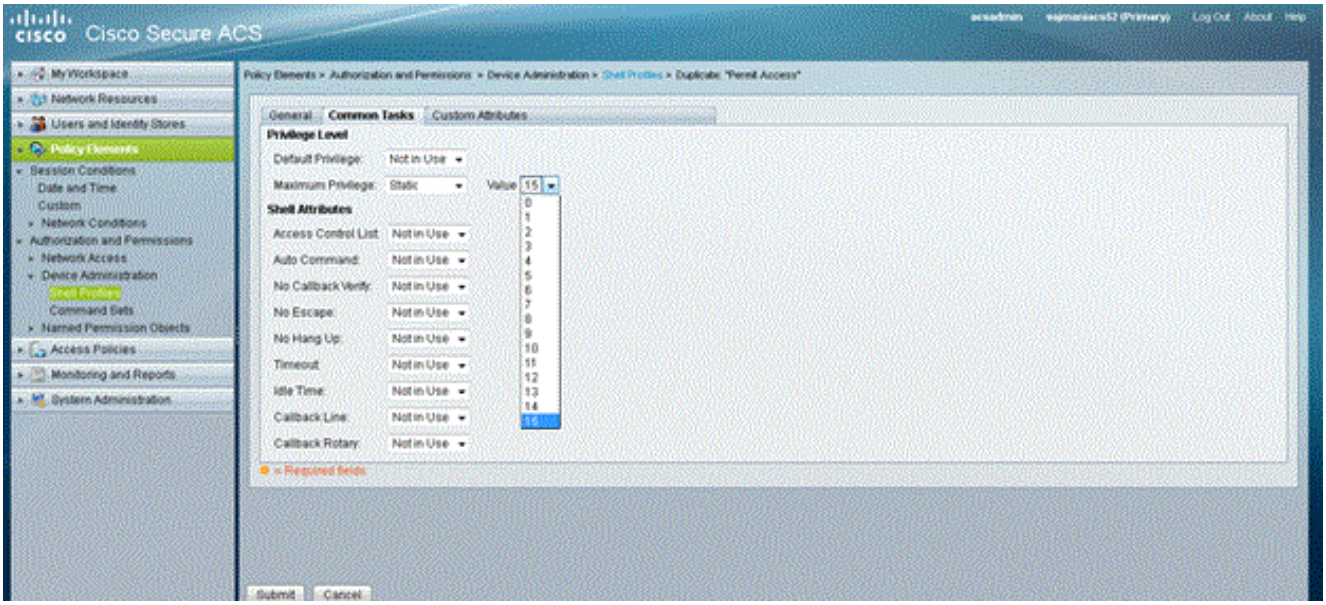
dialoogvenster **Toegang toestaan** en klik op **Dupliceren**.



Voer de **naam** en de **beschrijving in**.

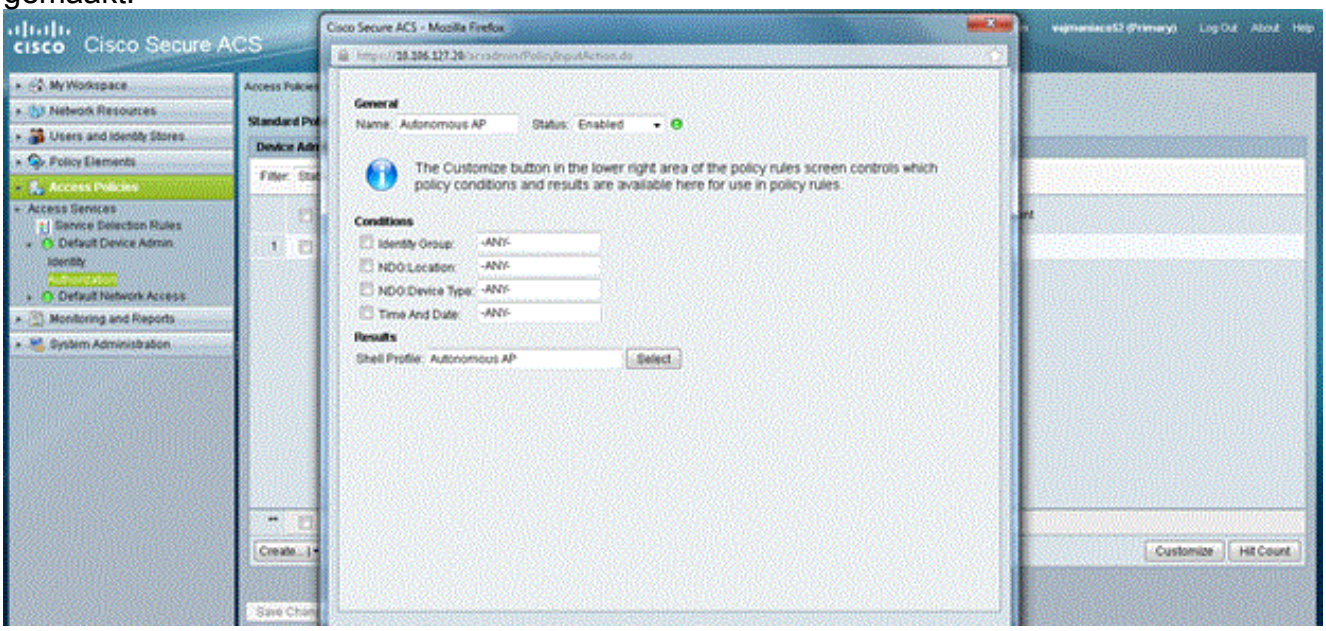


Selecteer het tabblad Common Tasks en kies **15** voor de maximale prioriteit.

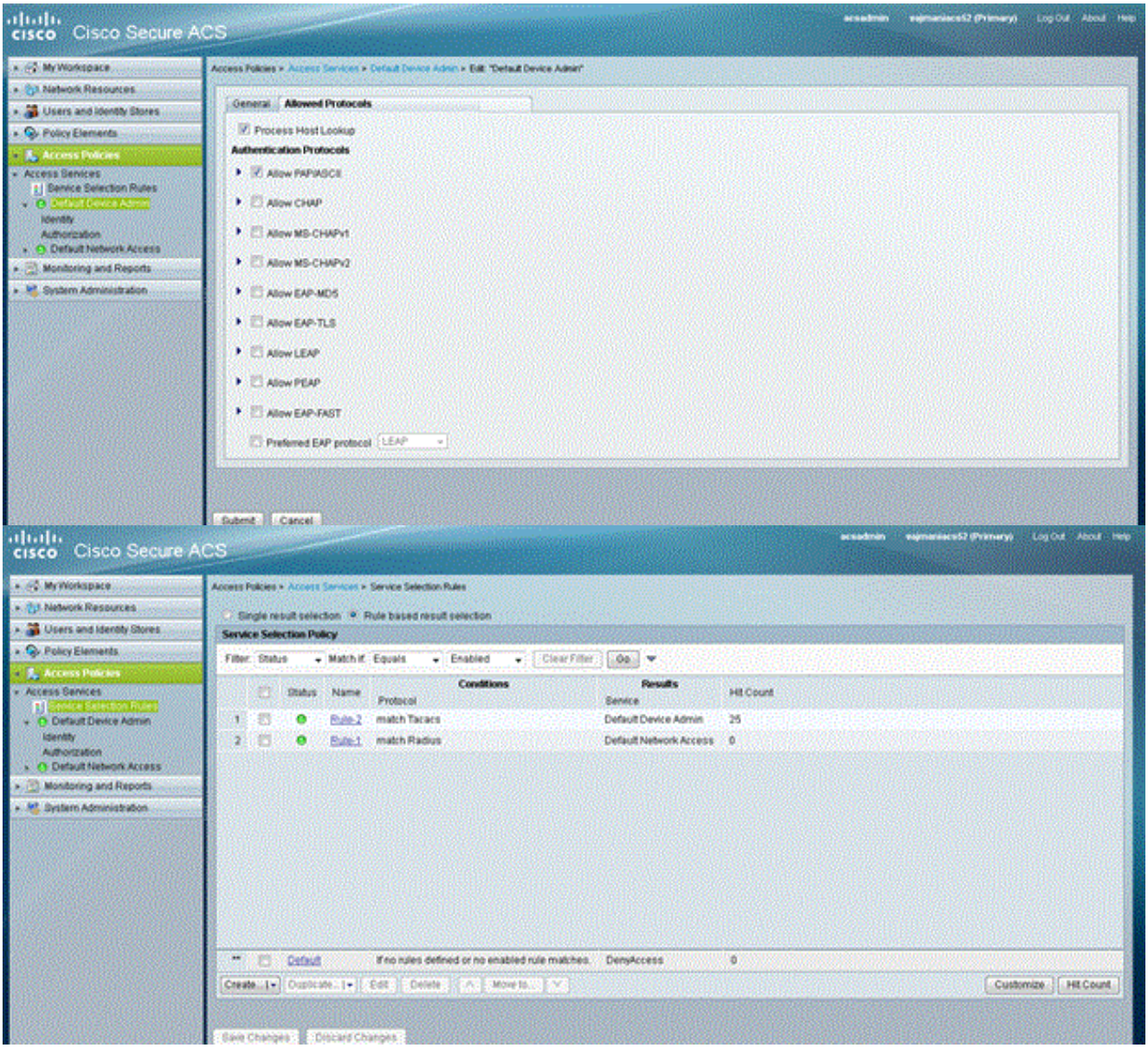


Klik op **Inzenden**.

4. Voltooi deze stappen om een autorisatiebeleid te creëren:Klik op **Toegangsbeleid > Toegangsservices > standaard apparaatbeheer > autorisatie**.Klik op **Maken** om een nieuw Vergunningsbeleid te creëren.Een nieuwe pop-up lijkt de regels voor het machtigingsbeleid te creëren.Selecteer de optie **Identity Group**, **Location** enz. voor de specifieke gebruikersnaam en AAA-client (AP), indien aanwezig.Klik op **Selecteren** voor het Shell-profiel om het profiel te kiezen dat met Autonome AP is gemaakt.



Klik op **Wijzigingen opslaan** nadat dit is gedaan.Klik op **Standaard apparaatbeheer** en klik vervolgens op **Toegestane protocollen**.Controleer **PAP/ASCII toestaan** en klik op **Inzenden**.Klik op **Service Selection Regels** om er zeker van te zijn dat er een TACACS-regeling wordt aangepast en dat u naar Default Devices Admin wijst.

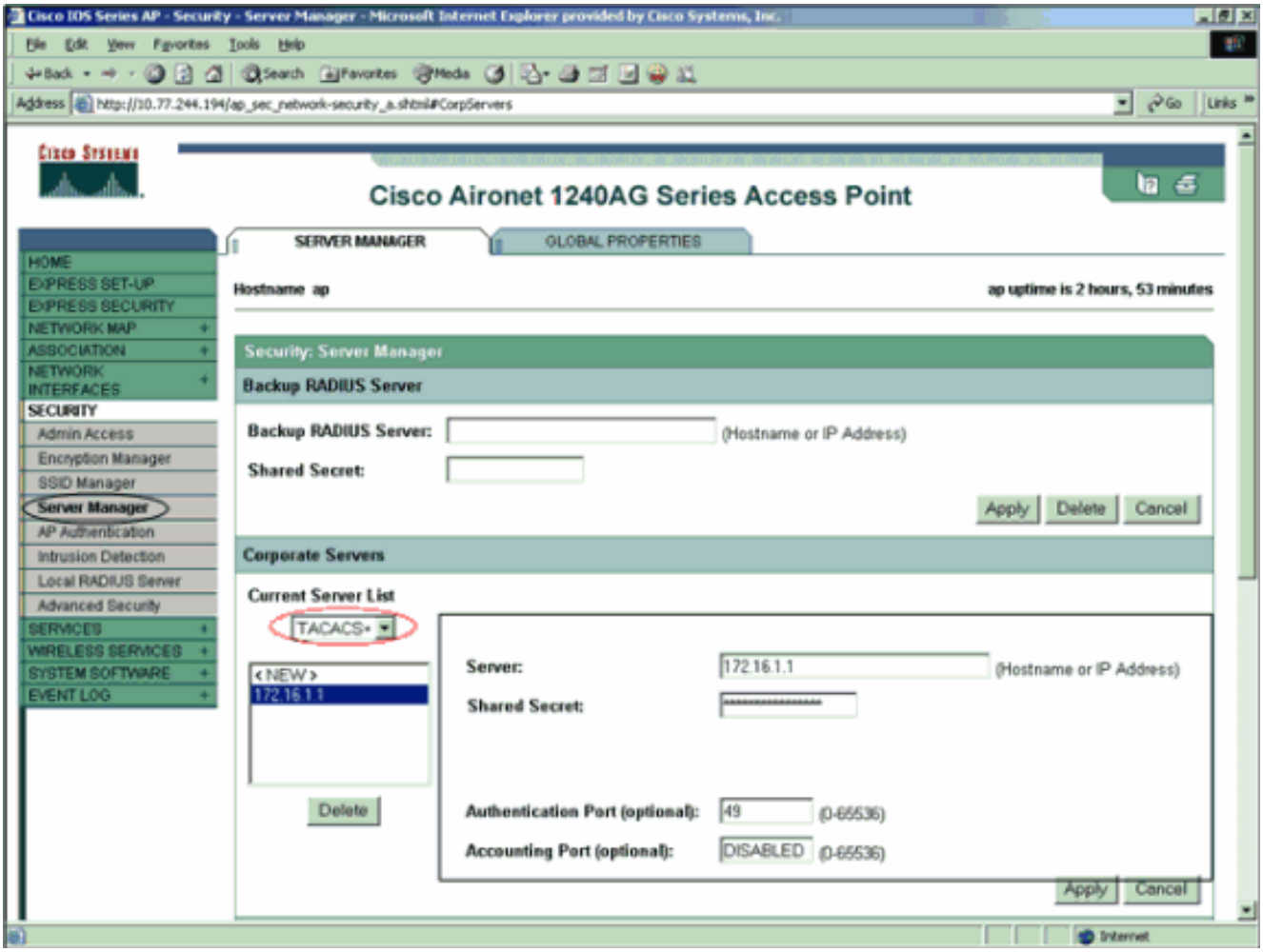


Configureer de Aironet AP voor TACACS+ verificatie

U kunt CLI of GUI gebruiken om de TACACS+ functies op Aironet AP in te schakelen. In deze sectie wordt uitgelegd hoe u de AP voor TACACS+ aanmelding-verificatie kunt configureren met gebruik van de GUI.

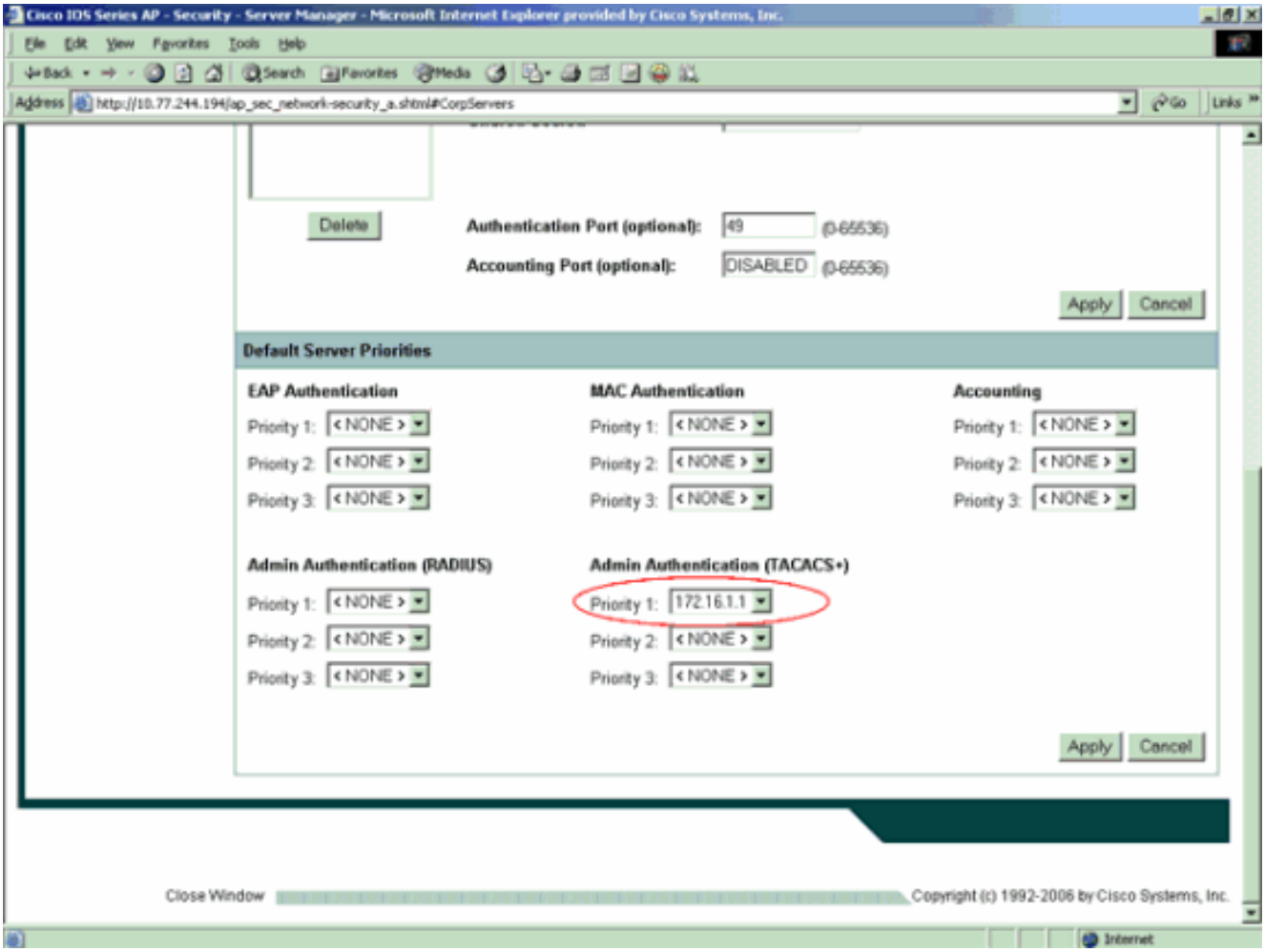
Voltooi deze stappen om TACACS+ op het AP te configureren met behulp van de GUI:

1. Voltooi deze stappen om de parameters van de TACACS+ server te definiëren:Kies in de AP GUI, **Security > Server Manager**.Beveiliging: Het venster Server Manager verschijnt.Selecteer in het gebied Corporate Server de optie **TACACS+** in het vervolgkeuzemenu Huidige serverlijst.Op dit zelfde gebied, ga het IP adres, het gedeelde geheim, en het authentificatiehavenaantal van de TACACS+ server in.Klik op **Apply** (Toepassen).Hierna volgt een
voorbeeld:

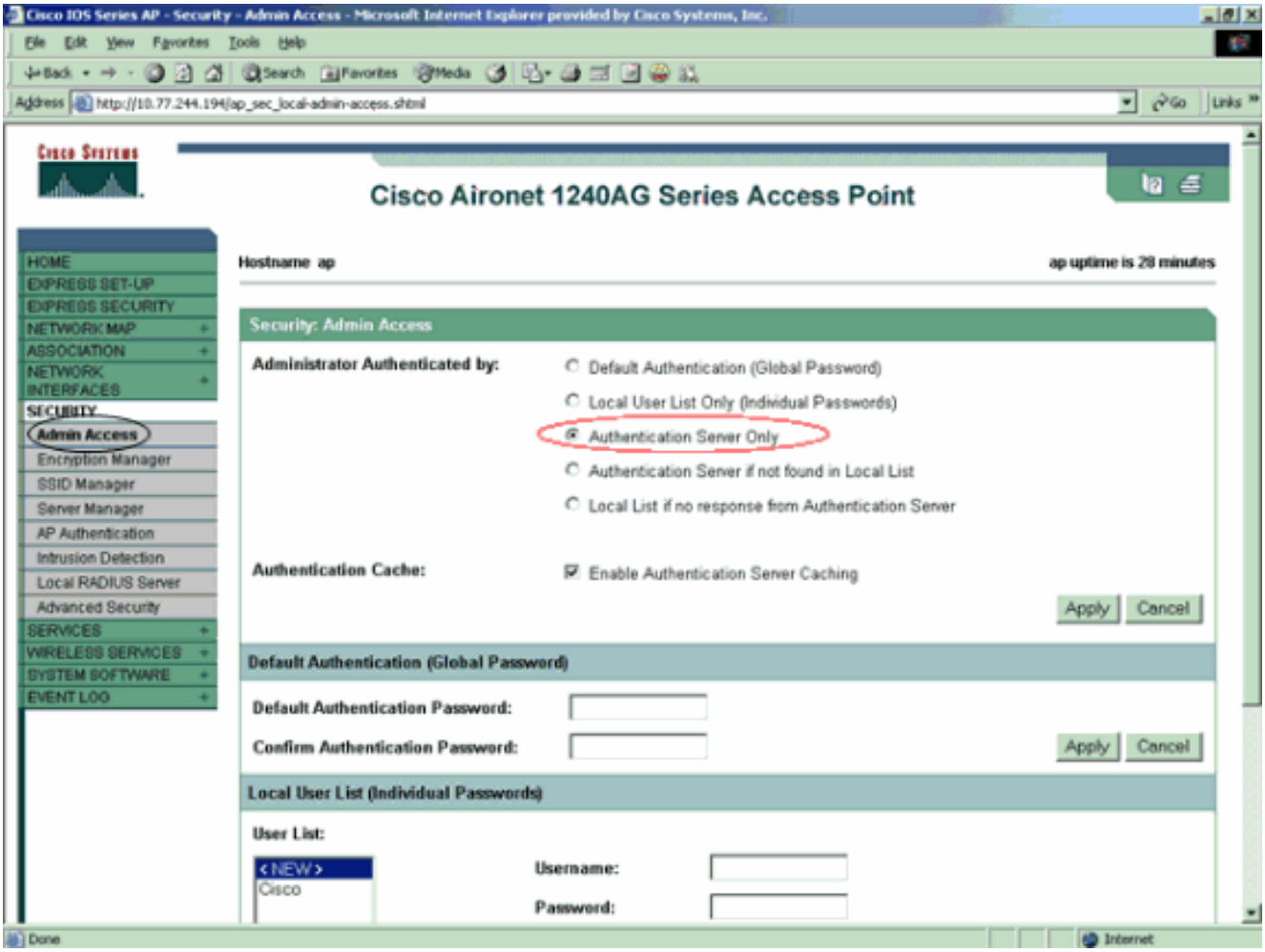


Opmerking: standaard gebruikt TACACS+ TCP poort 49.**Opmerking:** De gedeelde geheime sleutel die u op ACS vormt en AP moet overeenkomen.

2. Kies **Standaardserverprioriteiten > Admin-verificatie (TACACS+)**, selecteer in het vervolgkeuzemenu Prioriteit 1 het IP-adres van de TACACS+ server dat u hebt ingesteld en klik op **Toepassen**.Hierna volgt een
voorbeeld:



3. Kies **Security > Admin Access** en, voor beheerder die is gecertificeerd met:, kies **alleen** de **verificatieserver** en klik op **Toepassen**.Deze selectie waarborgt dat gebruikers die proberen in te loggen op AP geauthentiseerd worden door een authenticatieserver.Hierna volgt een voorbeeld:



Dit is de CLI-configuratie voor het configuratievoorbeeld:

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
```

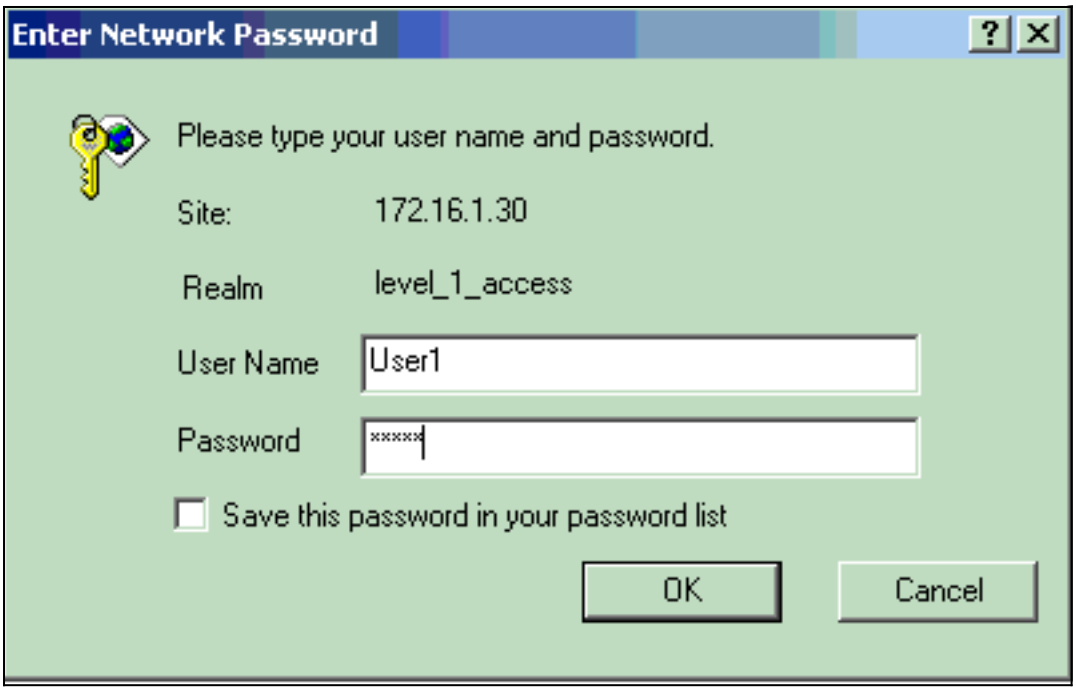
Opmerking: U moet beschikken over Cisco IOS-softwarerelease 12.3(7)JA of hoger om alle opdrachten in deze configuratie correct te laten werken. Een eerdere Cisco IOS-softwarerelease heeft mogelijk niet al deze opdrachten beschikbaar.

Verifiëren

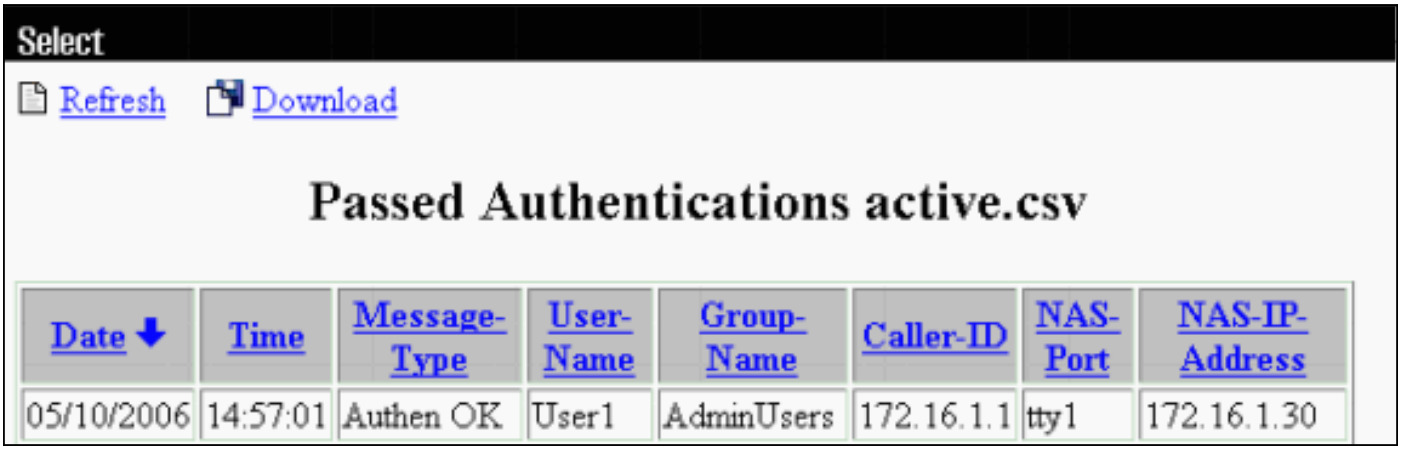
Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Probeer om de configuratie te verifiëren aan AP met gebruik van de GUI of de CLI in te loggen. Wanneer u toegang tot AP probeert te krijgen, leidt AP u tot een gebruikersnaam en een wachtwoord.



Wanneer u de gebruikersreferenties verstrekt, stuurt AP de geloofsbrieven naar de server TACACS+ door. De TACACS+ server bevestigt de geloofsbrieven op basis van de informatie die in zijn databank beschikbaar is en verleent toegang tot AP na succesvolle authenticatie. U kunt **Rapporten en Activiteit > Gepasseerde Verificatie** kiezen op de ACS en het Geautomatiseerde Verificatierapport gebruiken om voor deze gebruiker te controleren op succesvolle verificatie. Hierna volgt een voorbeeld:



U kunt de opdracht **Tacacs** ook gebruiken om de juiste configuratie van de TACACS+ server te controleren. Hierna volgt een voorbeeld:

```
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
```

Verificatie voor ACS 5.2

U kunt de mislukte/gepasseerde pogingen voor inlogaanmeldingsgegevens van ACS 5.2 verifiëren:

1. Klik op **Monitoring and Reports > Start Monitoring and Report Viewer**.Er wordt een nieuwe pop geopend met het Dashboard.
2. Klik op **Authenticaties-TACACS-Vandaag**. Dit toont de details van mislukte/doorgegeven pogingen.

Problemen oplossen

U kunt deze debug-opdrachten op het AP gebruiken om problemen met uw configuratie op te lossen:

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

- **debug tacacs gebeurtenissen**—Deze opdracht toont de opeenvolging van gebeurtenissen die tijdens TACACS authenticatie plaatsvinden. Hier is een voorbeeld van de uitvoer van deze opdracht:

```
*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 authenticatie**-gebruik deze opdracht om HTTP authenticatieproblemen op te lossen. De opdracht toont de authenticatiemethode die de router heeft geprobeerd en de

authenticatie-specifieke statusberichten.

- **debug van verificatie**—Deze opdracht geeft informatie weer over AAA TACACS+ verificatie.

Als de gebruiker een gebruikersnaam invoert die niet op de TACACS+ server bestaat, mislukt de verificatie. Hier is **debug tacacs authenticatie** opdrachtoutput voor een mislukte authenticatie:

```
*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)
```

U kunt kiezen **Rapporten en Activiteit > Verstoring van verificatie** om de mislukte verificatiepoging op de ACS te zien. Hierna volgt een voorbeeld:

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	..	..	..

Als u een Cisco IOS-softwarerelease op de AP gebruikt die eerder is dan Cisco IOS-softwarerelease 12.3(7)JA, kunt u elke keer dat u probeert in te loggen op de AP met gebruik van HTTP een bug raken. Cisco bug-ID is CSCeb52431 (alleen geregistreerde klanten).

De implementatie van Cisco IOS HTTP/AAA-software vereist de onafhankelijke authenticatie van elke afzonderlijke HTTP-verbinding. De draadloze Cisco IOS-software GUI heeft betrekking op de referentie van vele tientallen afzonderlijke bestanden binnen één webpagina (bijvoorbeeld Javascript en GIF). Dus als u één pagina in de draadloze Cisco IOS-softwarerelease laadt, kunnen tientallen afzonderlijke verificatie-/autorisatieverzoeken op de AAA-server verschijnen.

Gebruik voor HTTP-verificatie RADIUS of lokale verificatie. De RADIUS-server is nog steeds onderworpen aan de meerdere verificatieverzoeken. Maar RADIUS is schaalbaarder dan TACACS+ en zal dus waarschijnlijk een minder negatieve impact hebben op de prestaties.

Als u TACACS+ moet gebruiken en u een Cisco ACS hebt, gebruik het sleutelwoord **van één verbinding** met de **tacacs-server** opdracht. Gebruik van dit sleutelwoord met het commando spaart de ACS het grootste deel van de TCP verbinding instelling/uitloopoverhead en zal waarschijnlijk de lading op de server tot op zekere hoogte verminderen.

Voor Cisco IOS-softwarereleases 12.3(7) JA en hoger op de AP bevat de software een tijdelijke oplossing. De rest van dit deel beschrijft de oplossing.

Gebruik de AAA authenticatiescachefunctie om de informatie in te delen die de TACACS+ server teruggeeft. Met de authenticatiecache en de profielfunctie kan AP de authenticatie/autorisatie-responsen voor een gebruiker in het geheugen zetten zodat latere echtheids-/autorisatieverzoeken niet naar de AAA-server hoeven te worden verstuurd. Gebruik deze opdrachten om deze optie met de CLI te activeren:

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

Raadpleeg voor meer informatie over deze functie en de opdrachten het gedeelte *Verificatie-cache en profiel* van het access point *configureren*.

Kies **Security > Admin Access** en controleer het vakje **Caching** van **verificatieserver** inschakelen om deze optie in de GUI te schakelen. Omdat dit document Cisco IOS-softwarerelease 12.3(7)JA gebruikt, gebruikt het document de tijdelijke oplossing zoals de configuraties illustreren.

Gerelateerde informatie

- RADIUS- en TACACS+ servers configureren
- Opmerking over het veld: IOS access point bommen voor TACACS+ server met aanvragen
- EAP-verificatie met RADIUS-server
- Ondersteuning voor wireless producten
- Technische ondersteuning en documentatie – Cisco Systems