WLAN-toegang beperken op basis van SSID met WLC en Cisco Secure ACS-configuratievoorbeeld

Inhoud

Inleiding

Dit document biedt een configuratievoorbeeld om de toegang voor elke gebruiker tot een WLAN te beperken op basis van de serviceset ID (SSID).

Voorwaarden

Vereisten

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

- Kennis van het configureren van de draadloze LAN-controller (WLC) en lichtgewicht access point (LAP) voor gebruik op basis
- Basiskennis over de manier waarop u Cisco Secure Access Control Server (ACS) kunt configureren
- Kennis van Lichtgewicht Access Point Protocol (LWAPP) en draadloze beveiligingsmethoden

Gebruikte componenten

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

- Cisco 2000 Series WLC-software met firmware 4.0
- Cisco 1000 Series LAP
- Cisco Secure ACS Server versie 3.2
- Cisco 802.11a/b/g draadloze clientadapter voor firmware 2.6
- Cisco Aironet Desktop Utility (ADU) versie 2.6

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.

Achtergrondinformatie

Door het gebruik van de op SSID gebaseerde WLAN-toegang kunnen de gebruikers op basis van de SSID worden geauthentiseerd die zij gebruiken om met de WLAN te verbinden. De Cisco Secure ACS-server wordt gebruikt om de gebruikers te authentiseren. Verificatie vindt plaats in twee fasen op Cisco Secure ACS:

1. Goedkope echtheidscontrole
2. SSID-verificatie op basis van Network Access Bepertions (NAR's) op Cisco Secure ACS

Als op EAP en SSID gebaseerde verificatie succesvol is, mag de gebruiker toegang krijgen tot WLAN of de gebruiker anders wordt de gebruiker uitgeschakeld.

Cisco Secure ACS gebruikt de NARs optie om gebruikerstoegang op basis van SSID te beperken. Een NAR is een definitie, die u in Cisco Secure ACS maakt, van extra voorwaarden die moeten worden vervuld voordat een gebruiker tot het netwerk kan toegang hebben. Cisco Secure ACS past deze voorwaarden toe met informatie van eigenschappen die door uw AAA-clients worden verzonden. Hoewel er verschillende manieren zijn waarop u NAR's kunt instellen, zijn deze gebaseerd op matchingstoewijzingsinformatie die door de AAA-client wordt verstuurd. Om deze reden moet u het formaat en de inhoud van de eigenschappen die uw AAA-klanten verzenden begrijpen als u effectieve NAR's wilt gebruiken.

Wanneer u een NAR instelt, kunt u kiezen of het filter positief of negatief werkt. In de NAR specificeert u of u netwerktoegang moet toestaan of weigeren, gebaseerd op een vergelijking van informatie die van AAA-klanten naar de informatie die in de NAR is opgeslagen. Echter, als een NAR niet genoeg informatie om te opereren tegenkomt, blijft het standaard toegang ontzegd.

U kunt een NAR definiëren voor een specifieke gebruiker of gebruikersgroep en deze toepassen op een bepaalde gebruiker of gebruikersgroep. Raadpleeg het Witboek over netwerktoegangsbeperkingen voor meer informatie.

Cisco Secure ACS ondersteunt twee soorten NAR-filters:

1. **IP-gebaseerde filters**-IP-gebaseerde NAR filters beperken de toegang op basis van de IP-

adressen van de eindgebruiker client en de AAA-client. Raadpleeg Over IP-gebaseerde NAR-filters voor meer informatie over dit type NAR-filter.

2. **Niet-IP-gebaseerde filters** - Niet-IP-gebaseerde NAR filters beperken toegang gebaseerd op eenvoudige string vergelijking van een waarde verzonden van de AAA client. De waarde kan het CLI-nummer (Call line ID) zijn, het DNIS-nummer (Dited Number Identification Service), het MAC-adres of een andere waarde die van de client afkomstig is. Om dit type van NAR in werking te kunnen stellen moet de waarde in de NAR beschrijving precies overeenkomen wat van de cliënt wordt verzonden, inclusief welk formaat dan ook wordt gebruikt. Bijvoorbeeld (217) 555-4534 komt niet overeen met 217-555-4534. Raadpleeg Over NAR-filters die niet op IP zijn gebaseerd voor meer informatie over dit type NAR-filter.

Dit document gebruikt de niet-IP-gebaseerde filters om op SSID gebaseerde verificatie te doen. Een niet op IP gebaseerd NAR-filter (dwz, een op DNIS/CLI gebaseerd NAR-filter) is een lijst van toegestane of ontkende aanroep/punt van toegangslocaties die u kunt gebruiken in de beperking van een AAA-client als u geen gevestigde IP-gebaseerde verbinding hebt. De niet-IP-gebaseerde NAR optie gebruikt over het algemeen het CLI-nummer en het DNIS-nummer. Er zijn uitzonderingen in het gebruik van de DNIS/CLI - velden. U kunt de naam van SSID in het DNIS-veld invoeren en op SSID gebaseerde verificatie uitvoeren. Dit komt doordat de WLC de DNIS-eigenschap, de naam van SSID, naar de RADIUS-server stuurt. Dus als u DNIS NAR in of de gebruiker of groep bouwt, kunt u SSID-beperkingen per gebruiker maken.

Als u RADIUS gebruikt, gebruiken de NAR-velden die hier worden genoemd deze waarden:

- **AAA client**-Het NAS-IP-adres (eigenschap 4) of, als NAS-IP-adres niet bestaat, NAS-identifier (RADIUS-kenmerk 32) wordt gebruikt.
- **Port**—De NAS-poort (eigenschap 5) of, als NAS-poort niet bestaat, NAS-Port-ID (eigenschap 87) wordt gebruikt.
- **CLI**—De call-station-ID (eigenschap 31) wordt gebruikt.
- **DNIS**—De opgeroepen station-ID (eigenschap 30) wordt gebruikt.

Raadpleeg Netwerktoegangsbeperkingen voor meer informatie over het gebruik van NAR.

Aangezien WLC in de DNIS eigenschap en de naam van SSID verstuurt, kunt u per-gebruiker SSID beperkingen creëren. In het geval van de WLC, hebben de NAR velden deze waarden:

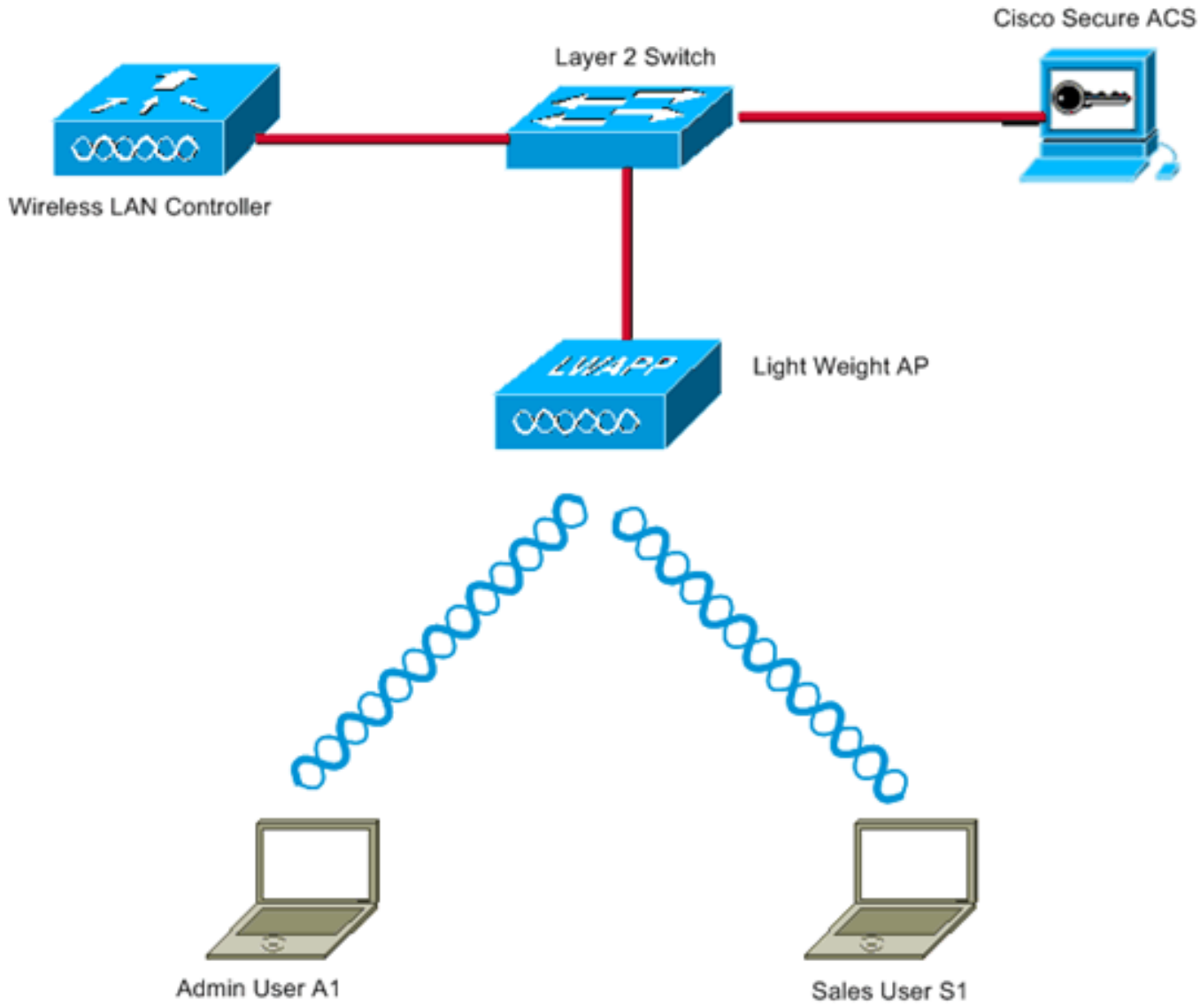
- **AAA client**-WLC IP-adres
- **haven**—*
- **CLI** —*
- **DNIS**—*naam

De rest van dit document biedt een configuratievoorbeeld van hoe u dit kunt realiseren.

Netwerkinstelling

Bij deze voorbeeldinstallatie is WLC op de LAP geregistreerd. Twee WLAN's worden gebruikt. Eén WLAN is voor de beheerder van de afdeling gebruikers en de andere WLAN is voor de gebruikers van de verkoopafdeling. Draadloze client-A1 (Admin-gebruiker) en S1 (verkoopgebruiker) maken verbinding met het draadloze netwerk. U moet de WLC- en de RADIUS-server zodanig configureren dat de Admin-gebruiker A1 alleen de WLAN-**beheerder** kan benaderen en de WLAN-**verkoop** beperkte toegang heeft tot de WLAN-**verkoop** en de verkoopgebruiker S1 de WLAN-**verkoop** kan benaderen en de **WLAN-beheerder** beperkte toegang hebben. Alle gebruikers gebruiken LEAP-verificatie als Layer 2-verificatiemethode.

N.B.: Bij dit document wordt ervan uitgegaan dat de WLC is geregistreerd op de controller. Als u nieuw bent aan WLC en niet weet hoe u de WLC voor basisbediening moet configureren, raadpleegt u Lichtgewicht AP (LAP) Registratie aan een draadloze LAN-controller (WLC).



WLC Management Interface IP address : 172.16.1.30/16
WLC AP-Manager Interface IP address: 172.16.1.31/16
Cisco Secure ACS server IP address: 172.16.1.60/16

SSID for the Admin department users : Admin
SSID for Sales department users: Sales

Configureren

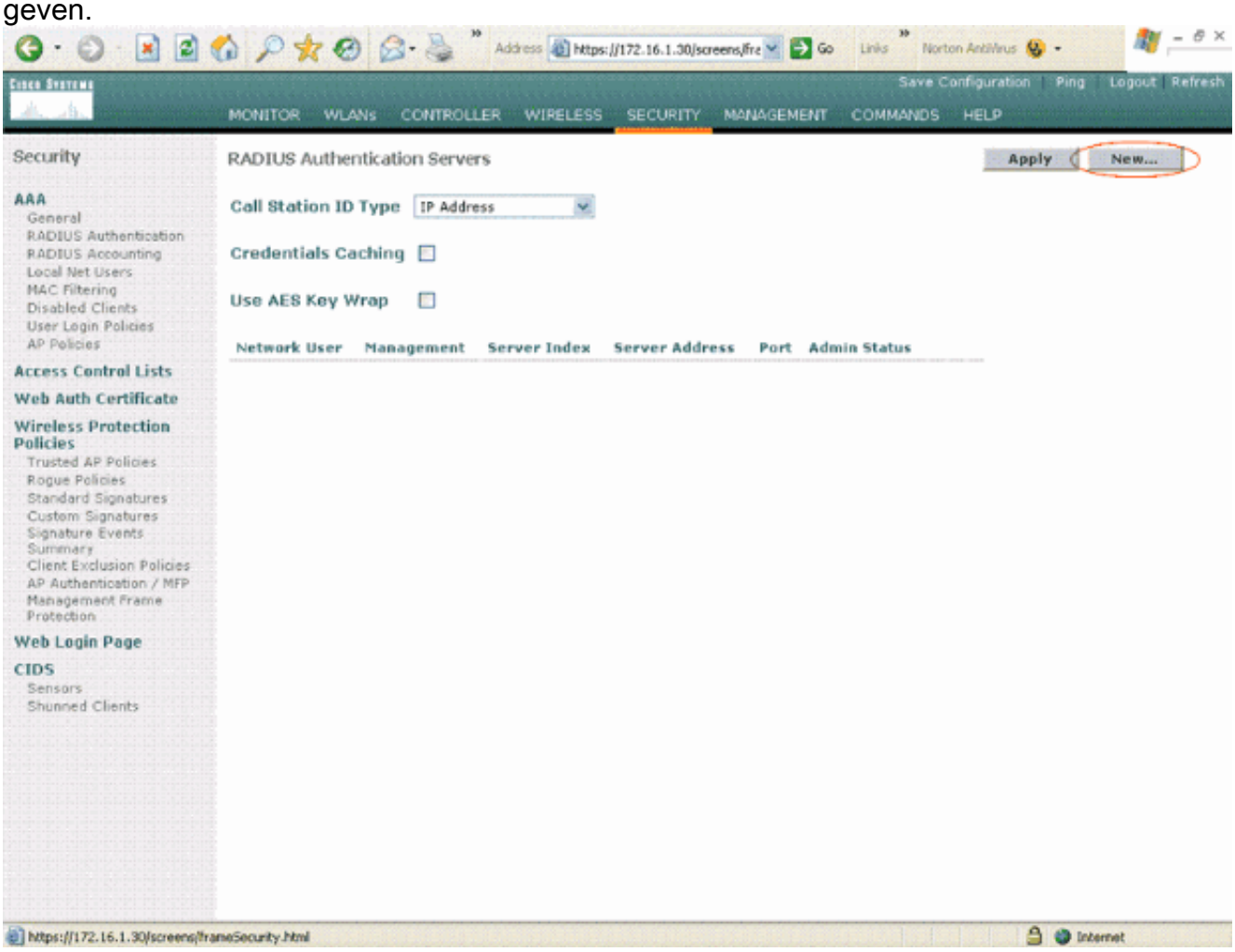
Om de apparaten voor deze instelling te configureren hebt u het volgende nodig:

1. Configureer de WLC voor de twee WLAN's en RADIUS-server.
2. Configureer de Cisco beveiligde ACS.
3. Configureer de draadloze clients en controleer deze.

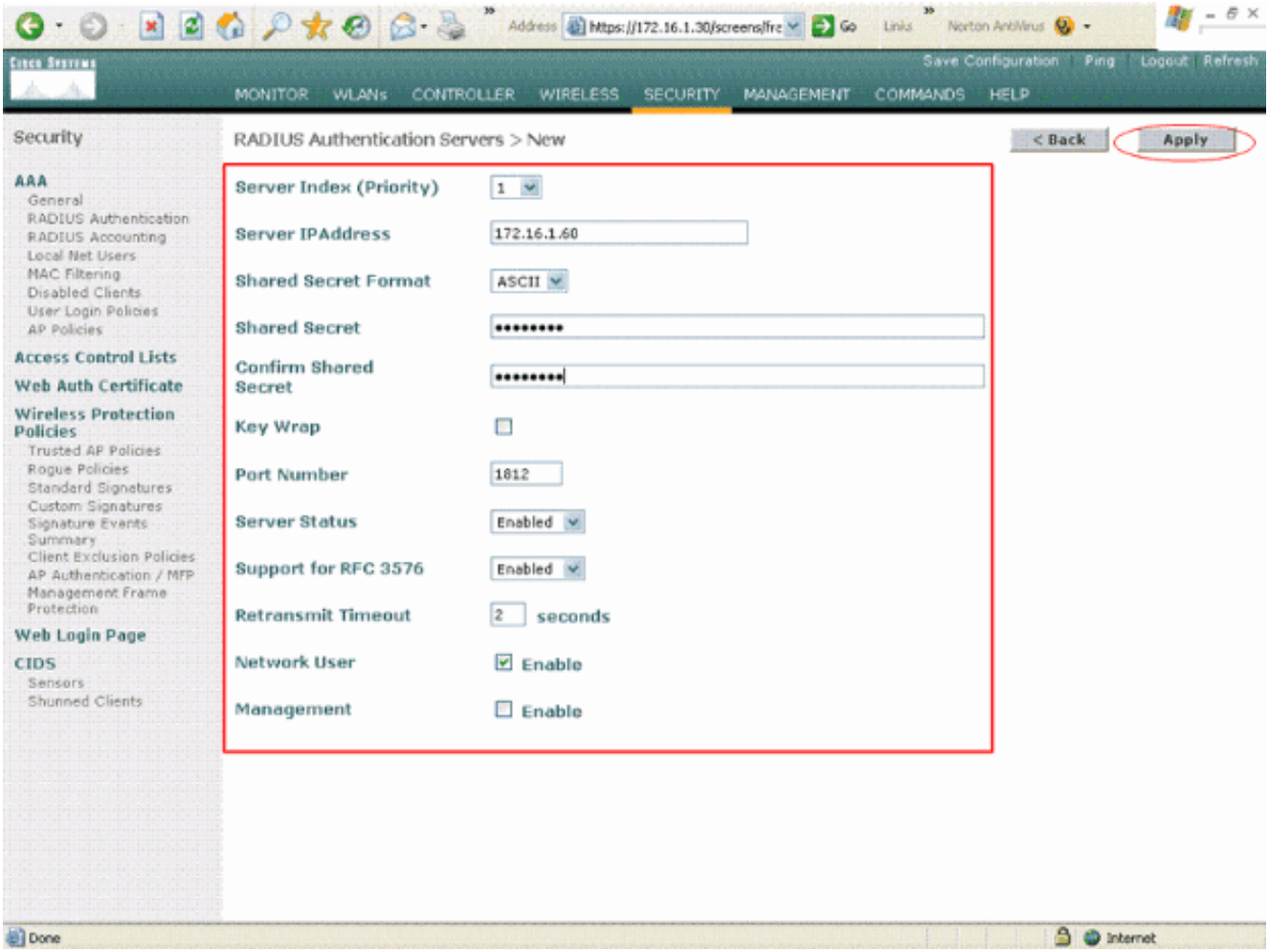
De WLC configureren

Volg deze stappen om de WLC te configureren voor deze instelling:

1. De WLC moet worden geconfigureerd om de gebruikersreferenties naar een externe RADIUS-server door te sturen. De externe RADIUS-server (Cisco Secure ACS in dit geval) bevestigt vervolgens de gebruikersreferenties en geeft toegang tot de draadloze clients. Voer de volgende stappen uit:Kies **Security > RADIUS-verificatie** van de controller GUI om de pagina RADIUS-verificatieservers weer te geven.

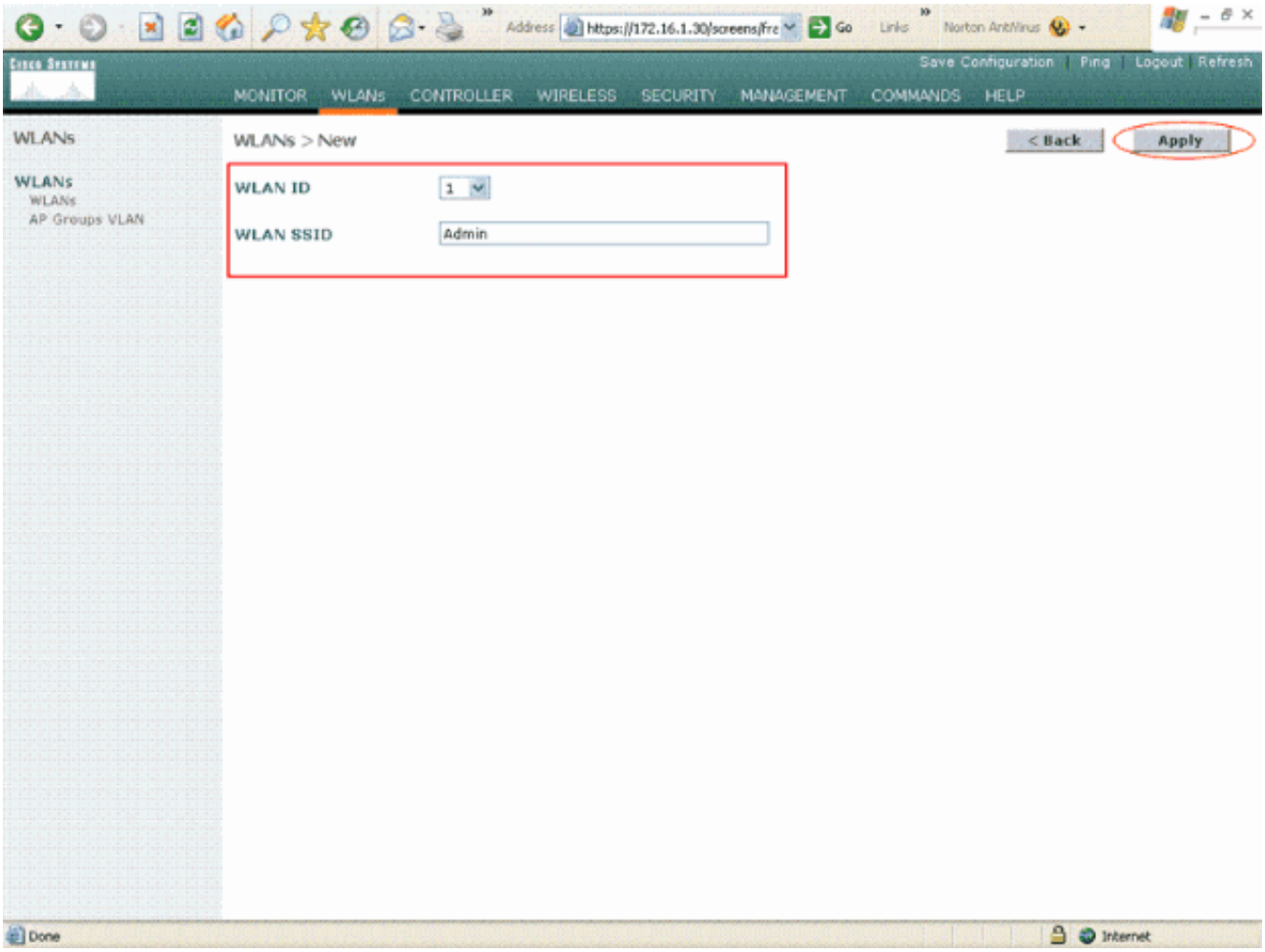


Klik op **New** om de RADIUS-serverparameters te definiëren.Deze parameters omvatten het IP-adres van de RADIUS-server, gedeeld geheim, poortnummer en serverstatus. De de controles van de Netwerkgebruiker en van het Beheer bepalen of de op RADIUS gebaseerde authenticatie van toepassing is voor beheer en netwerkgebruikers. Dit voorbeeld gebruikt Cisco Secure ACS als de RADIUS-server met IP-adres 172.16.1.60.

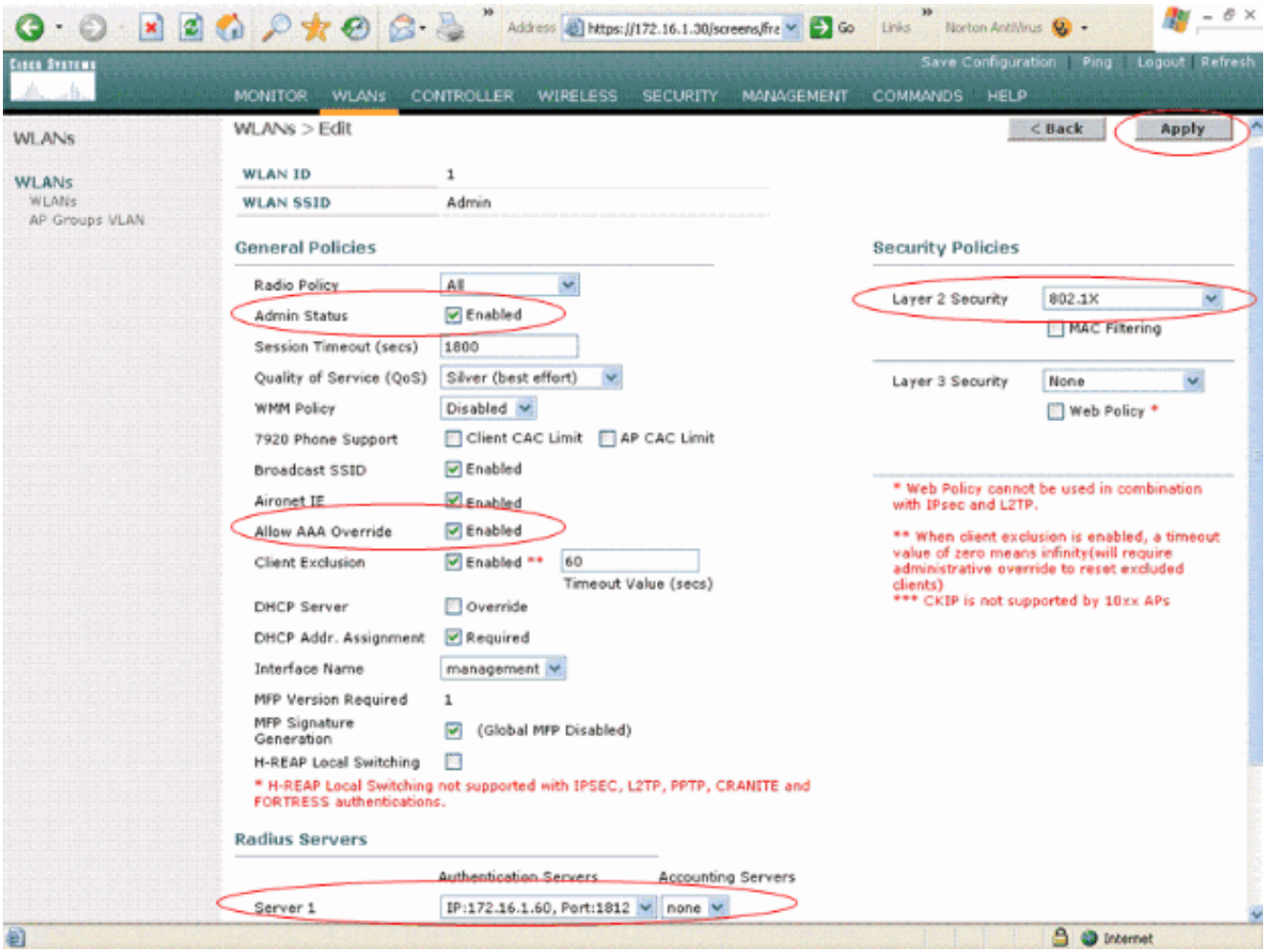


Klik op **Apply** (Toepassen).

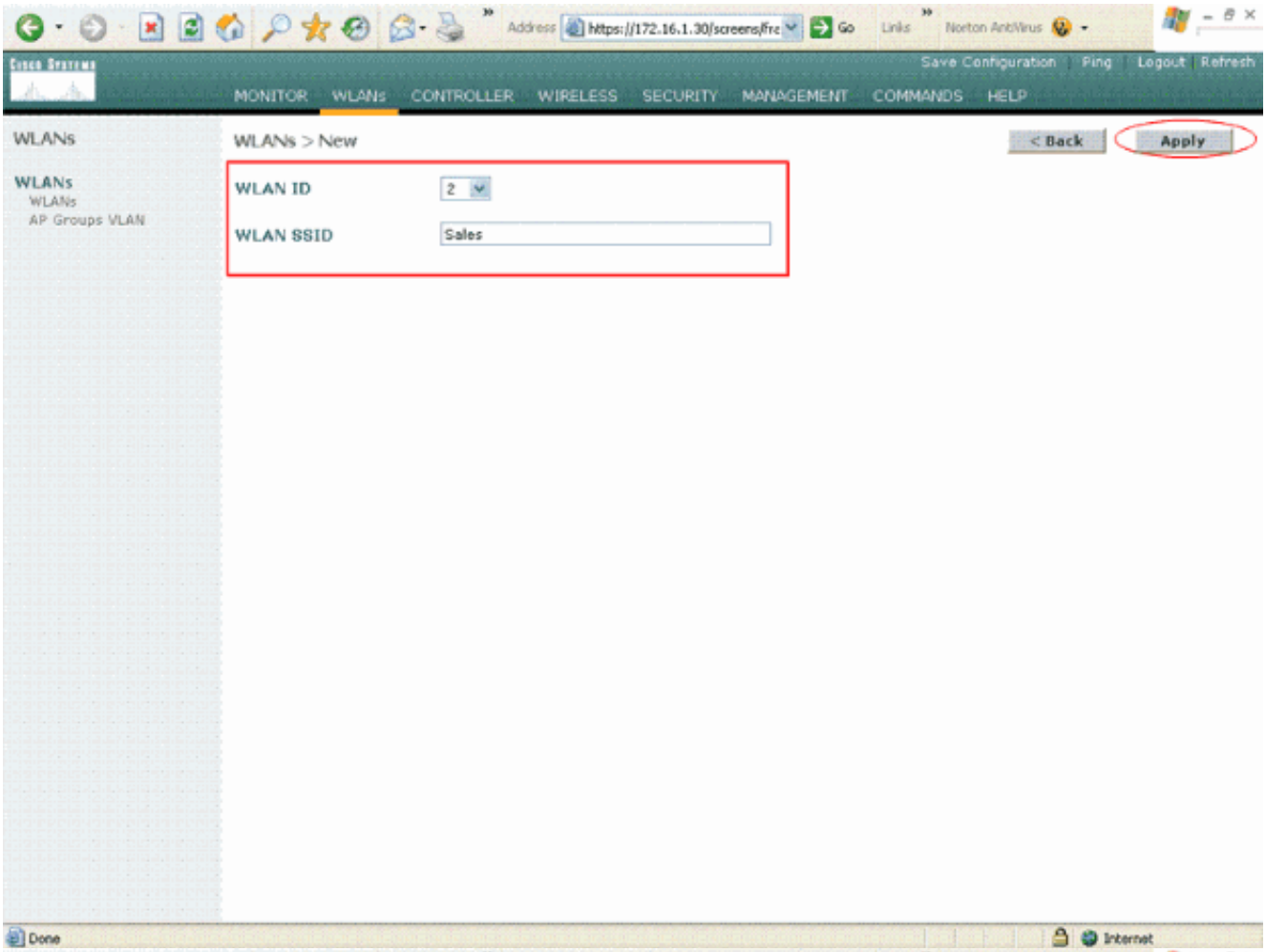
2. Configureer één WLAN voor de beheerder met SSID **Admin** en de andere WLAN's voor de verkoopafdeling met SSID **Sales**. Volg deze stappen om dit te doen:Klik op **WLAN's** van de controller GUI om een WLAN-functie te maken. Het WLAN-venster verschijnt. Dit venster toont de WLAN's die op de controller zijn geconfigureerd.Klik op **New** om een nieuwe WLAN te configureren.Dit voorbeeld maakt een WLAN met de naam **Admin** voor de beheerder en de WLAN-id is **1**. Klik op
Toepassen.

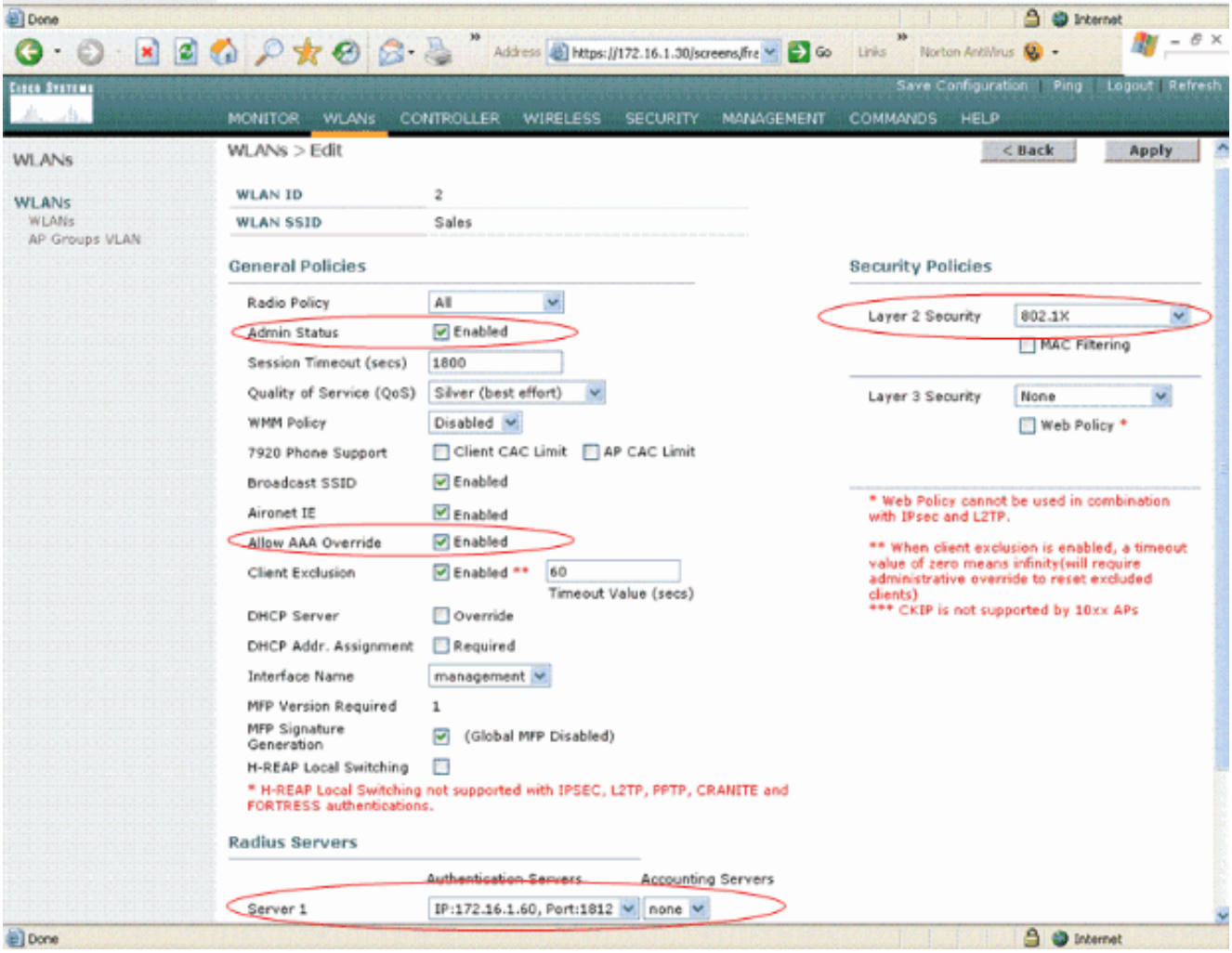


In het **WLAN >** venster **bewerken** definieert u de parameters die specifiek zijn voor WLAN:Selecteer in het keuzemenu Layer 2 Security **de** optie **802.1x**. Layer 2 Security optie is standaard 802.1x. Dit maakt 802.1x/EAP-verificatie mogelijk voor de WLAN.Controleer onder algemeen beleid het vakje **AAA-Override**. Wanneer AAA Override is ingeschakeld en een client conflicterende AAA- en controller WLAN-verificatieparameters heeft, wordt de client-verificatie uitgevoerd door de AAA-server.Selecteer de juiste RADIUS-server in het keuzemenu onder RADIUS-servers. De andere parameters kunnen worden gewijzigd op basis van de vereisten van het WLAN-netwerk. Klik op **Apply** (Toepassen).



Op dezelfde manier, om een WLAN voor de verkoopafdeling te maken, herhaalt u stappen b en c. Hier zijn de
screenshots.


Address https://172.16.1.30/screens/fra
Go
Links
Norton AntiVirus
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
AP Groups VLAN
WLANs > New
< Back
Apply
WLAN ID
2
WLAN SSID
Sales


Done
Internet
Address https://172.16.1.30/screens/fra
Go
Links
Norton AntiVirus
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
AP Groups VLAN
WLANs > Edit
< Back
Apply
WLAN ID 2
WLAN SSID Sales
General Policies
Radio Policy All
Admin Status Enabled
Session Timeout (secs) 1800
Quality of Service (QoS) Silver (best effort)
WMM Policy Disabled
7920 Phone Support Client CAC Limit AP CAC Limit
Broadcast SSID Enabled
Aironet IE Enabled
Allow AAA Override Enabled
Client Exclusion Enabled ** 60
Timeout Value (secs)
DHCP Server Override
DHCP Addr. Assignment Required
Interface Name management
MFP Version Required 1
MFP Signature Generation (Global MFP Disabled)
H-REAP Local Switching
* H-REAP Local Switching not supported with IPSEC, L2TP, PPTP, CRANITE and FORTRESS authentications.
Security Policies
Layer 2 Security 802.1X
MAC Filtering
Layer 3 Security None
Web Policy *
* Web Policy cannot be used in combination with IPsec and L2TP.
** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)
*** CKIP is not supported by 10xx APs
Radius Servers
Authentication Servers
Accounting Servers
Server 1 IP:172.16.1.60, Port:1812 none
Done
Internet

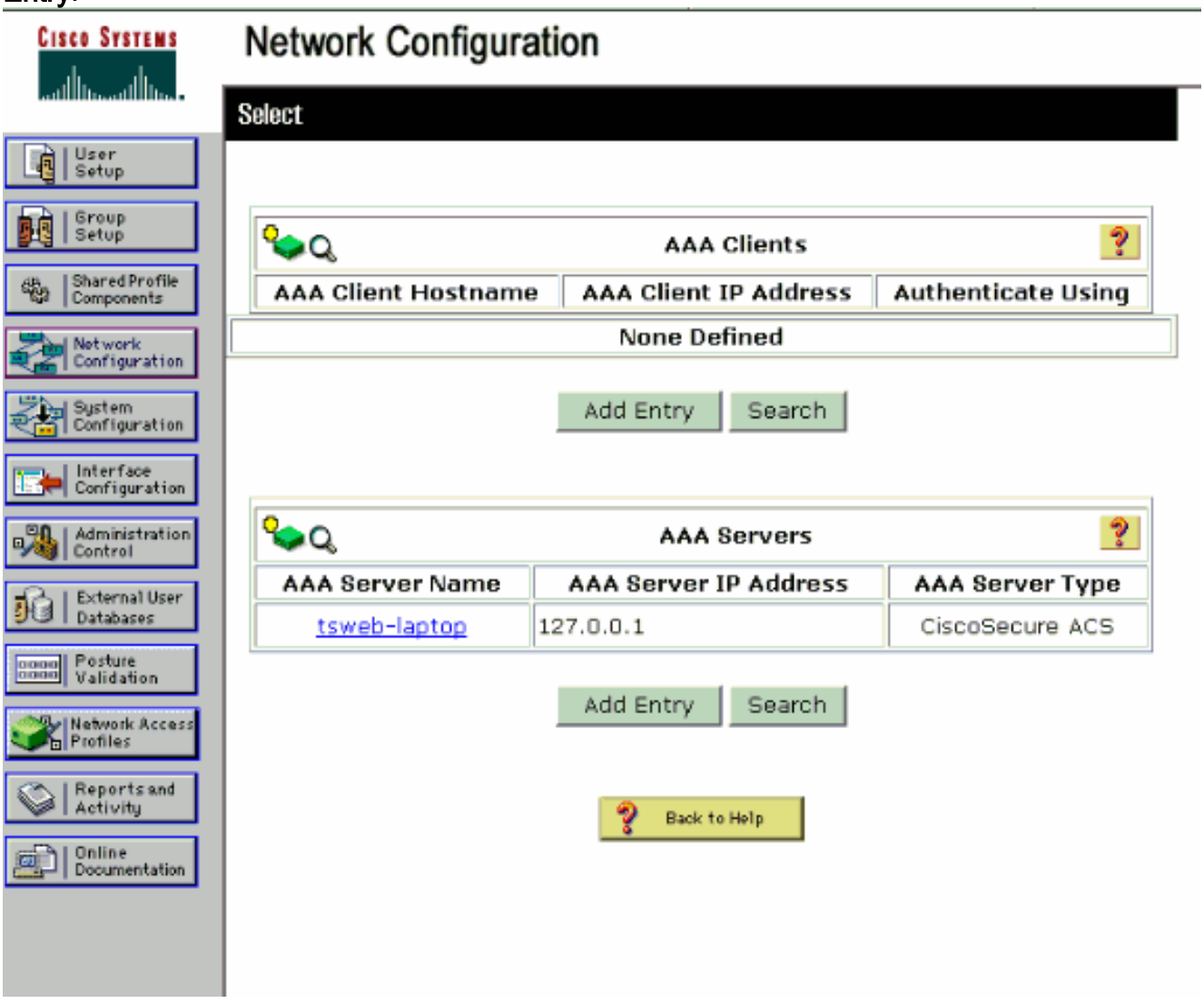
Cisco beveiligde ACS configureren

Op de Cisco Secure ACS-server moet u:

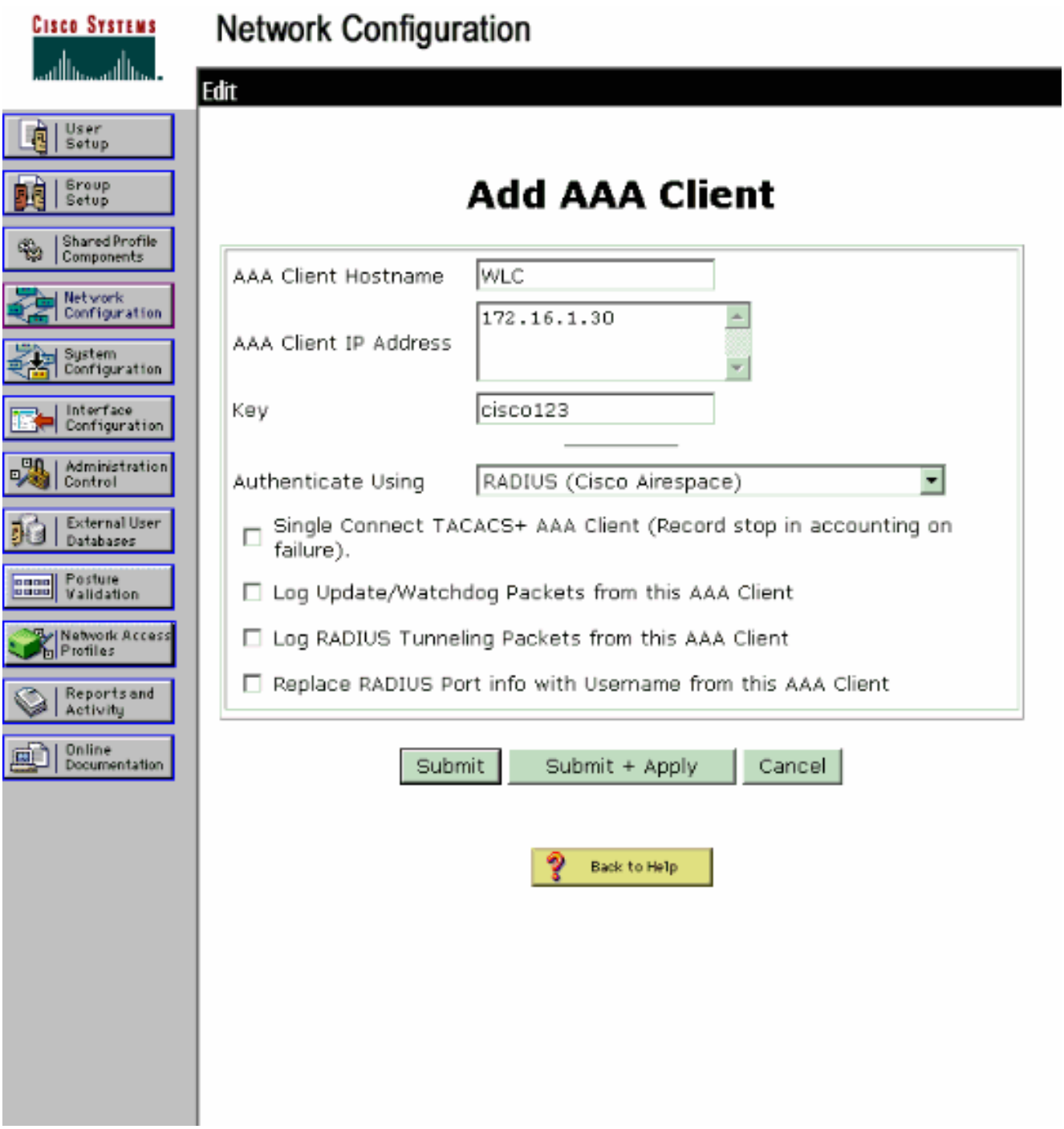
1. Configureer de WLC als een AAA-client.
2. Maak de gebruikersdatabase en definieer NAR voor op SSID gebaseerde verificatie.
3. MAP-verificatie inschakelen.

Voltooi deze stappen op Cisco Secure ACS:

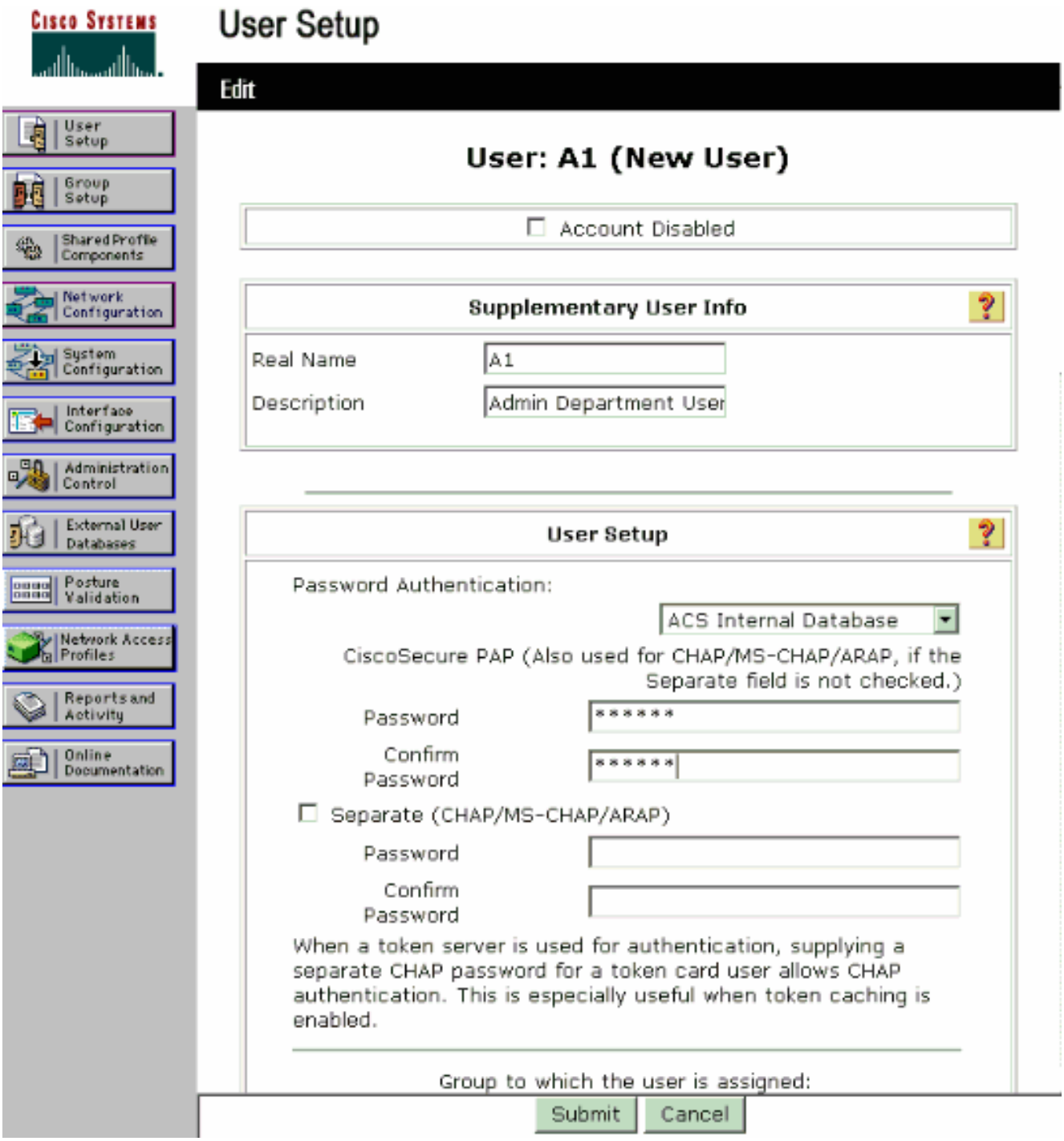
1. Om de controller als een AAA-client op de ACS-server te definiëren, klikt u op **Netwerkconfiguratie** vanuit de ACS-GUI. Klik onder AAA-clients op **Add Entry**.



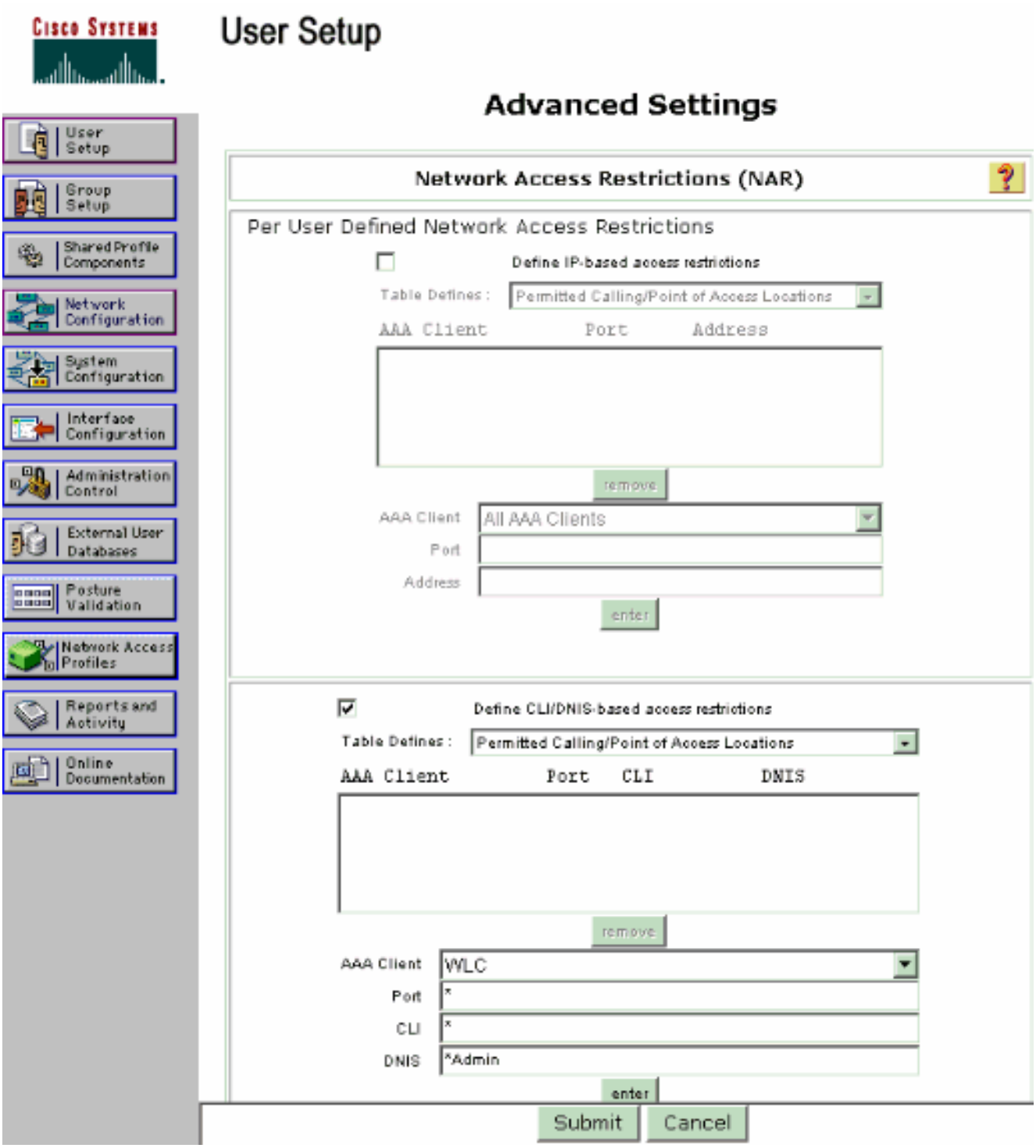
2. Wanneer de pagina Network Configuration verschijnt, specificeert u de naam van de WLC, IP-adres, gedeelde geheime en verificatiemethode (RADIUS Cisco Airespace).



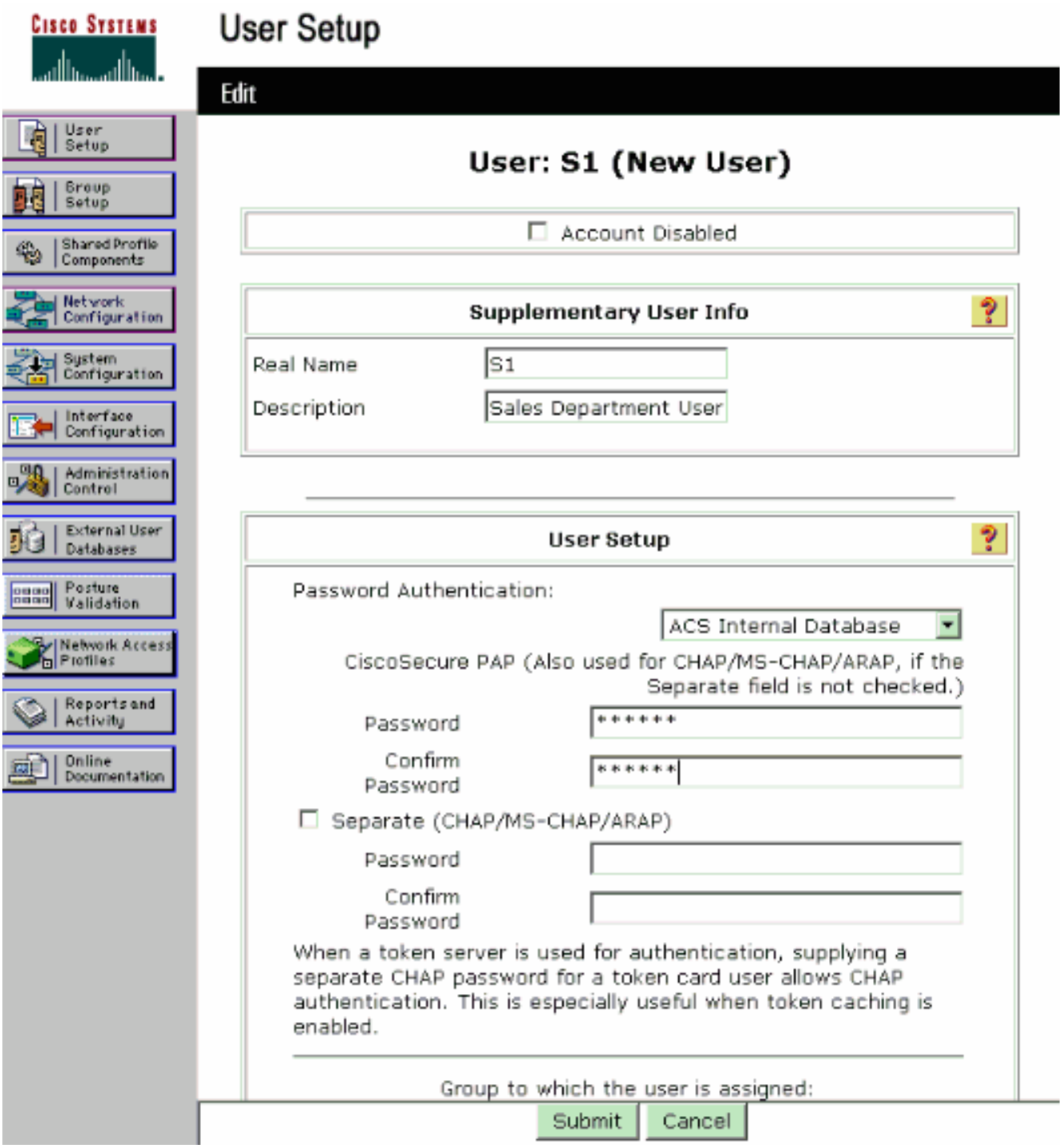
3. Klik op **Gebruikersinstelling** vanuit de ACS-GUI, voer de gebruikersnaam in en klik op **Toevoegen/Bewerken**. In dit voorbeeld is de gebruiker A1.
4. Wanneer de pagina Gebruikersinstellingen verschijnt, definieert u alle parameters die specifiek zijn voor de gebruiker. In dit voorbeeld worden de gebruikersnaam, het wachtwoord en de aanvullende gebruikersinformatie ingesteld omdat u deze parameters nodig hebt voor LEAP-
verificatie.

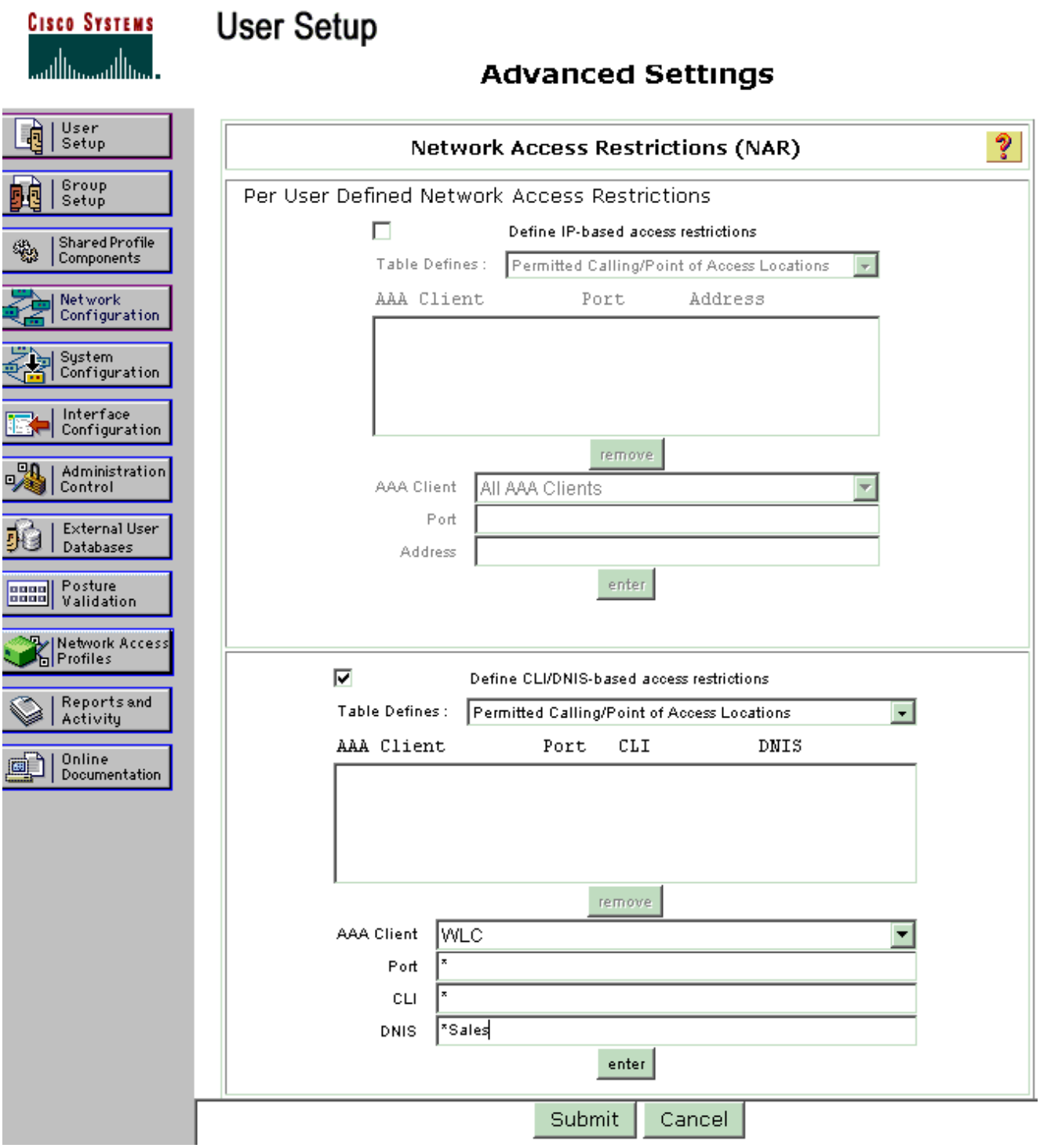


5. Scrolt door de pagina van de Gebruiker, tot u het gedeelte Netwerktoegangsbeperkingen ziet. Selecteer onder het kopje Gebruikersinterface van DNIS/CLI-toegangsbeperking de optie **Toegestaan bellen/point of Access Locations** en definieer deze parameters:**AAA client**-WLC IP-adres (172.16.1.30 in ons voorbeeld)**Poorten**—***CLI**—***DNIS**—*naam
6. De DNIS - eigenschap definieert SSID dat de gebruiker toegang mag krijgen. De WLC stuurt de SSID in de DNIS-eigenschap naar de RADIUS-server.Als de gebruiker alleen de WLAN-naam Admin moet benaderen, voert u ***Admin** in voor het DNIS-veld. Dit garandeert dat de gebruiker alleen toegang heeft tot de WLAN-beheerder met naam. Klik op **ENTER**.**Opmerking:** SSID moet altijd worden voorafgegaan door ***. Het is verplicht.

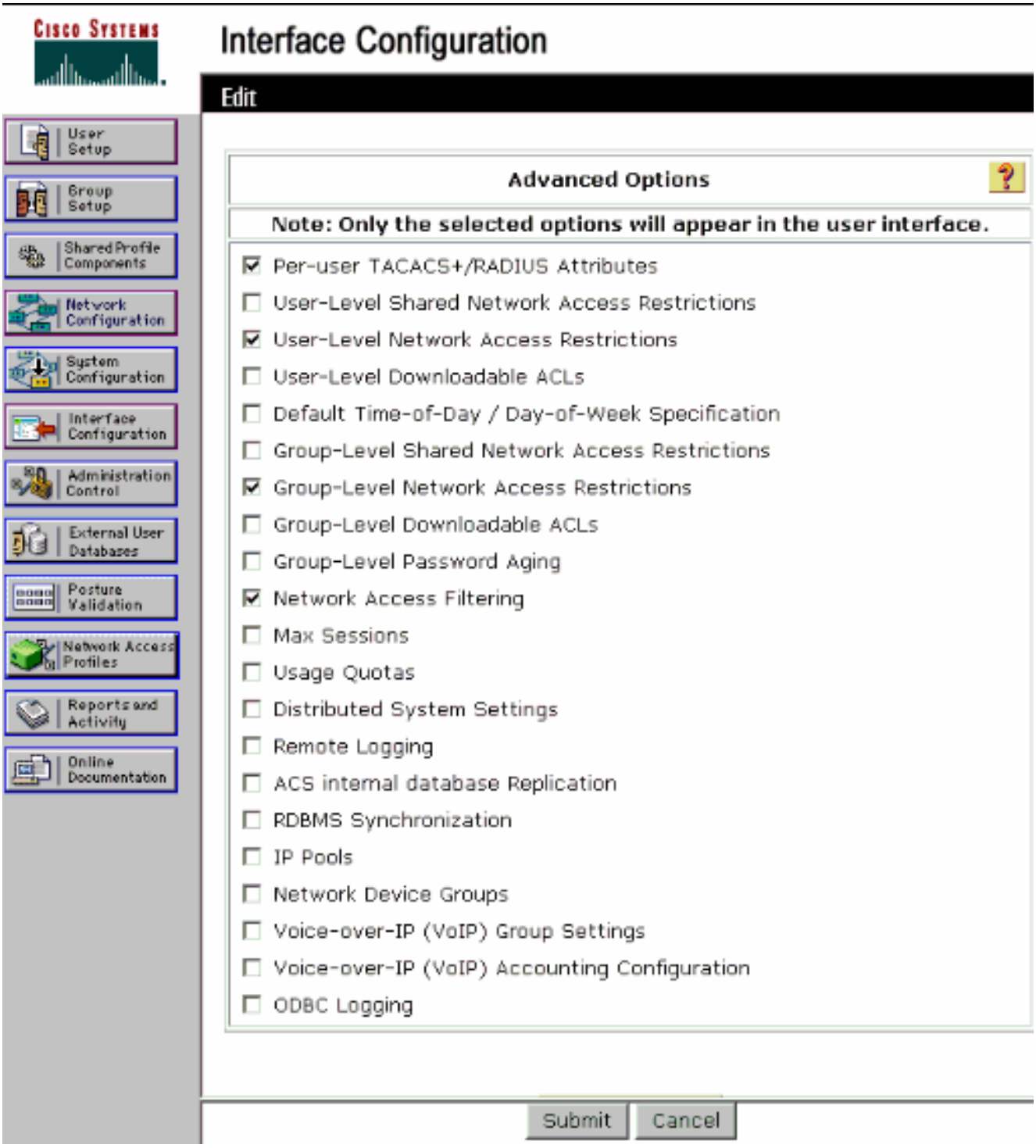


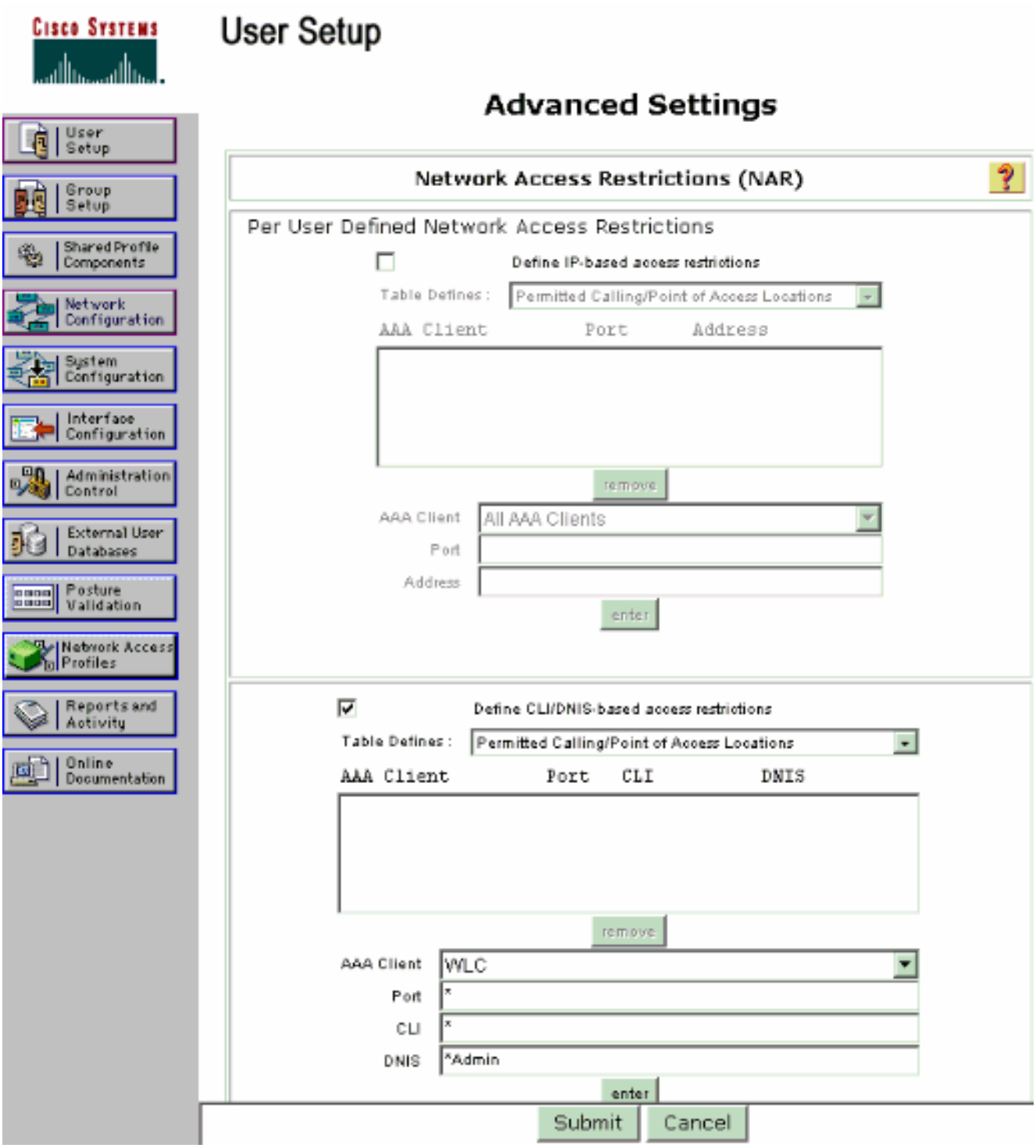
7. Klik op **Inzenden**.
8. Creëer op dezelfde manier een gebruiker voor de gebruiker van de Verkopingsdienst. Hier zijn de screenshots.


Cisco Systems
User Setup
Edit
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
User: S1 (New User)
Account Disabled
Supplementary User Info
Real Name
S1
Description
Sales Department User
User Setup
Password Authentication:
ACS Internal Database
CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)
Password
******
Confirm Password
******
Separate (CHAP/MS-CHAP/ARAP)
Password
Confirm Password
When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.
Group to which the user is assigned:
Submit
Cancel

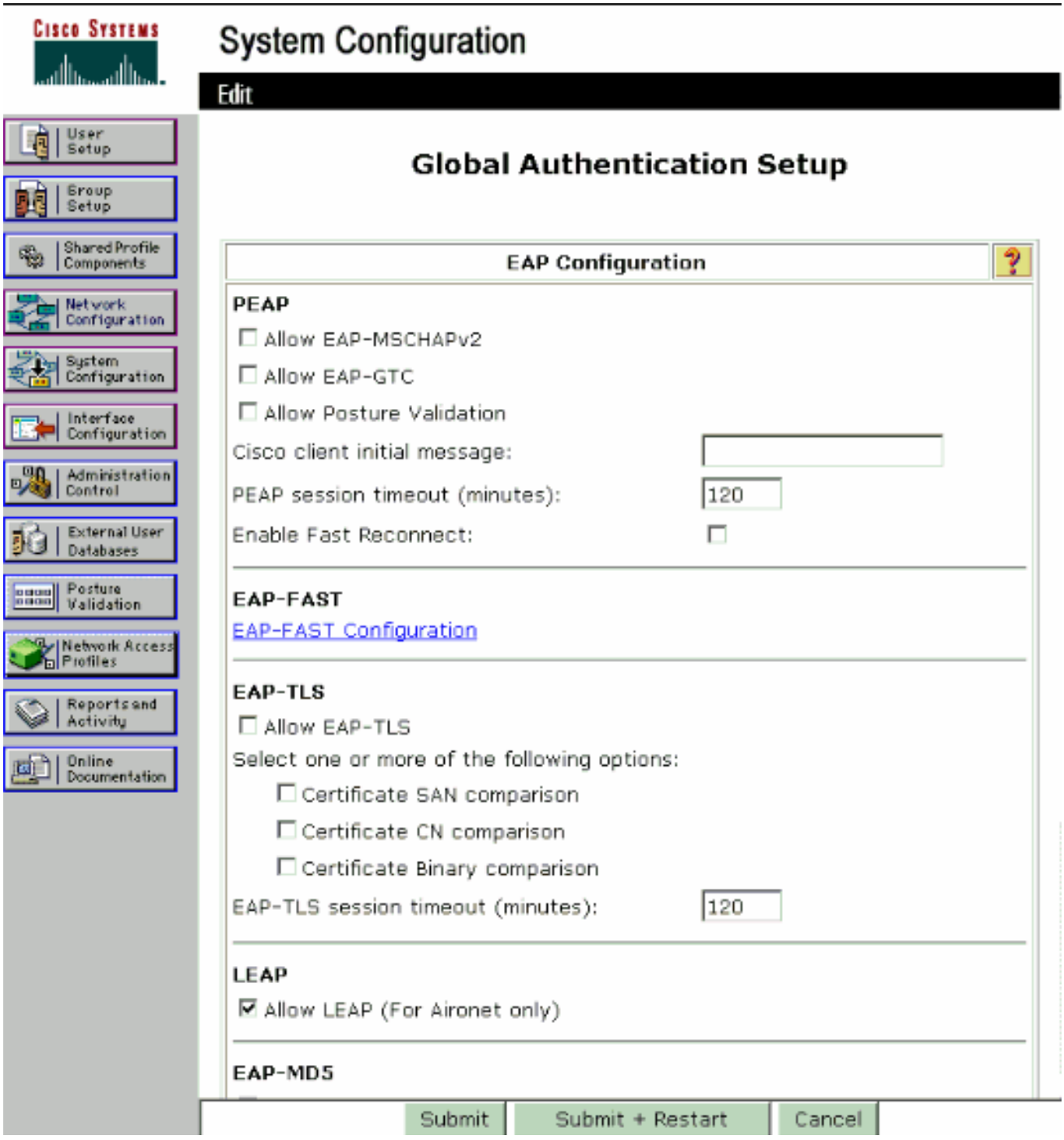


9. Herhaal hetzelfde proces om meer gebruikers aan de database toe te voegen.**N.B.:** Standaard worden alle gebruikers gegroepeerd onder de standaardgroep. Als u specifieke gebruikers aan verschillende groepen wilt toewijzen, raadpleegt u het gedeelte Gebruikersgroep Management van de gebruikersgids voor Cisco Secure ACS voor Windows Server 3.2.**Opmerking:** Als u de sectie voor netwerktoegangsbeperkingen in het venster van de gebruikersinstelling niet ziet, kan dit zijn omdat deze niet is ingeschakeld. Om de beperkingen voor netwerktoegang voor gebruikers in te schakelen, kiest u **Interfaces > geavanceerde opties** vanuit de ACS GUI, selecteert u **gebruikersniveau** netwerktoegangsbeperkingen en klikt u op **Indienen**. Dit stelt NAR in en verschijnt in het venster User
Setup.


Cisco Systems
Interface Configuration
Edit
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Advanced Options
Note: Only the selected options will appear in the user interface.
Per-user TACACS+/RADIUS Attributes
User-Level Shared Network Access Restrictions
User-Level Network Access Restrictions
User-Level Downloadable ACLs
Default Time-of-Day / Day-of-Week Specification
Group-Level Shared Network Access Restrictions
Group-Level Network Access Restrictions
Group-Level Downloadable ACLs
Group-Level Password Aging
Network Access Filtering
Max Sessions
Usage Quotas
Distributed System Settings
Remote Logging
ACS internal database Replication
RDBMS Synchronization
IP Pools
Network Device Groups
Voice-over-IP (VoIP) Group Settings
Voice-over-IP (VoIP) Accounting Configuration
ODBC Logging
Submit
Cancel



10. Om MAP-verificatie mogelijk te maken, klikt u op **Systeemconfiguratie** en **Global Verification Setup** om te verzekeren dat de verificatieserver is ingesteld om de gewenste MAP-verificatiemethode uit te voeren.Selecteer onder de MAP-configuratie-instellingen de juiste MAP-methode. In dit voorbeeld wordt gebruik gemaakt van MAP-authenticatie. Klik op **Inzenden** als u klaar
bent.

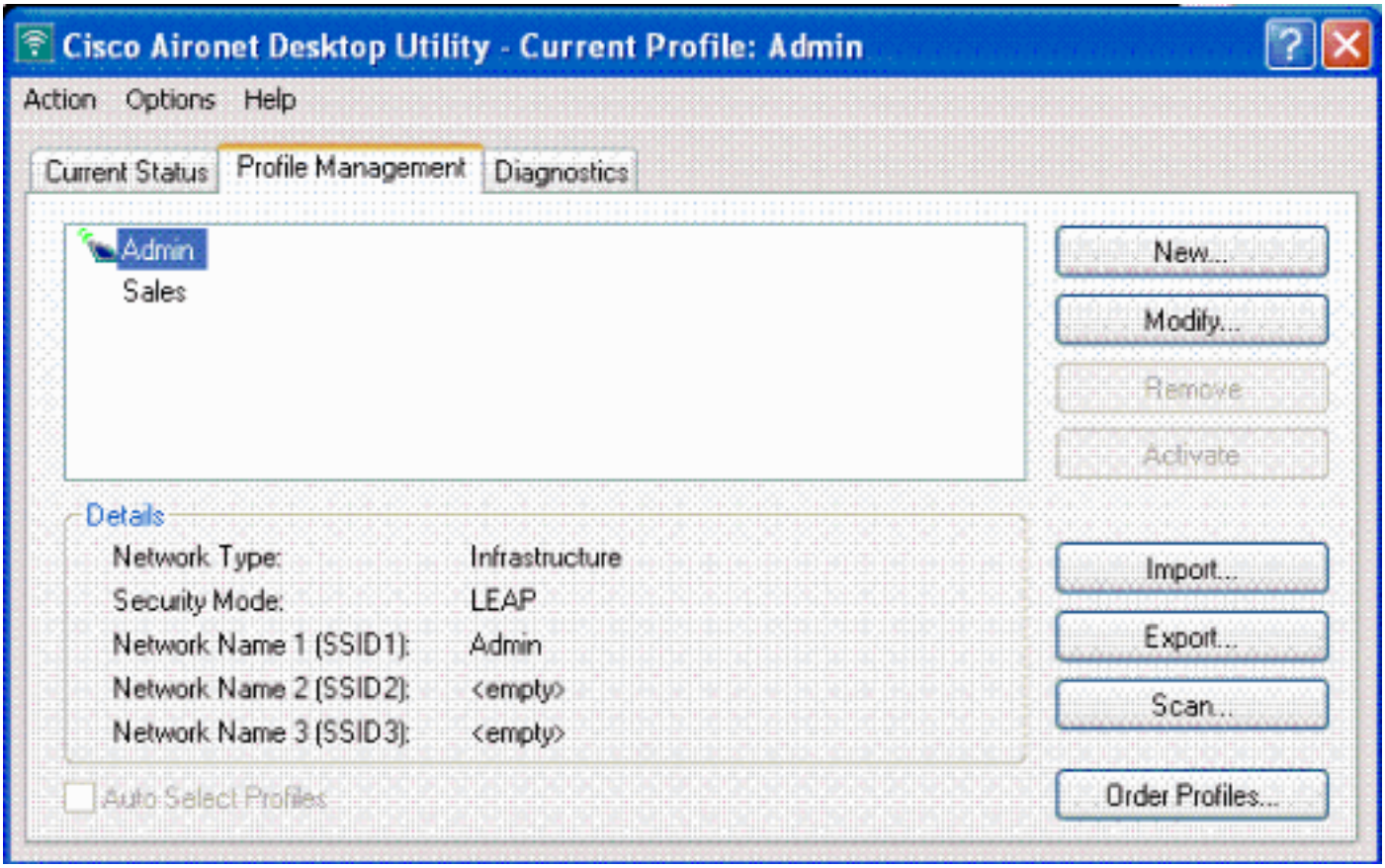


De draadloze client configureren en controleren

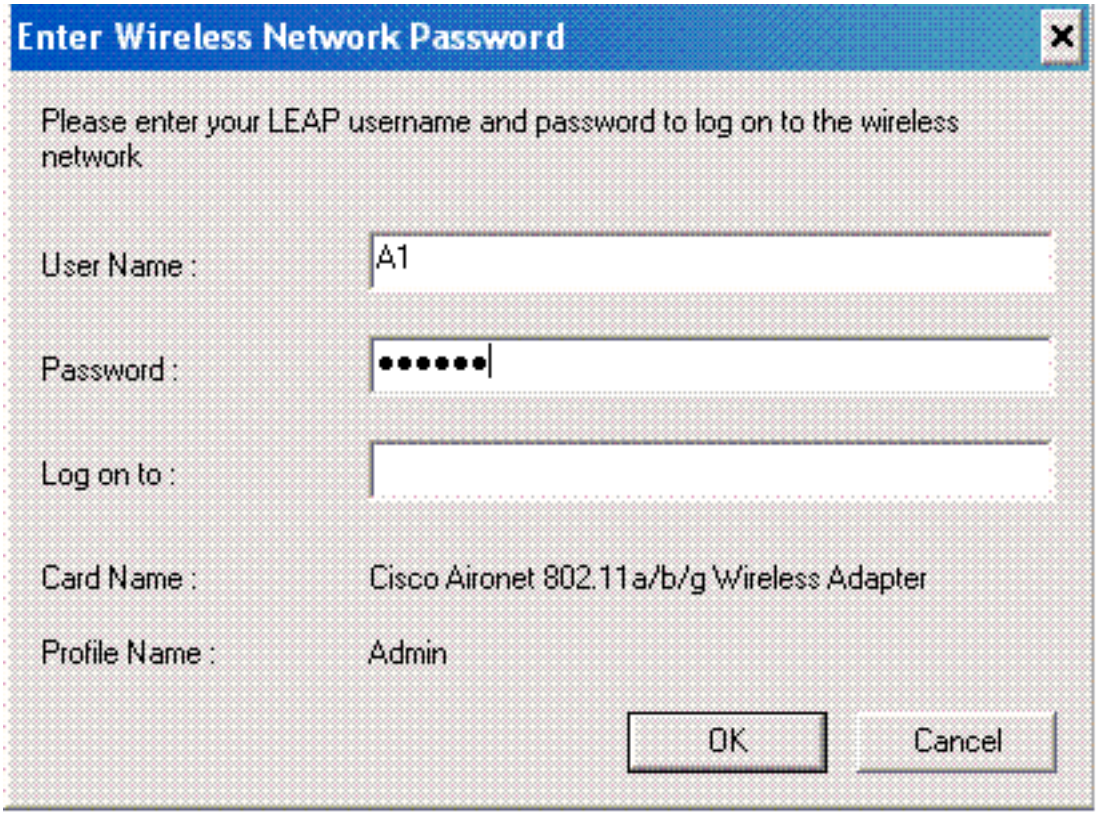
Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt. Probeer een draadloze client met de LAP te associëren door middel van LEAP-verificatie om te controleren of de configuratie werkt zoals verwacht.

Opmerking: In dit document wordt ervan uitgegaan dat het clientprofiel is ingesteld voor LEAP-verificatie. Raadpleeg het gebruik van EAP-verificatie voor informatie over het configureren van de 802.11a/b/g draadloze clientadapter voor LEAP-verificatie.

Opmerking: vanaf de ADU ziet u dat u twee clientprofielen hebt ingesteld. Eén voor de gebruikers van de Admin-afdeling met SSID **Admin** en het andere profiel voor de gebruikers van de verkoopafdeling met SSID **Sales**. Beide profielen zijn ingesteld voor LEAP-verificatie.



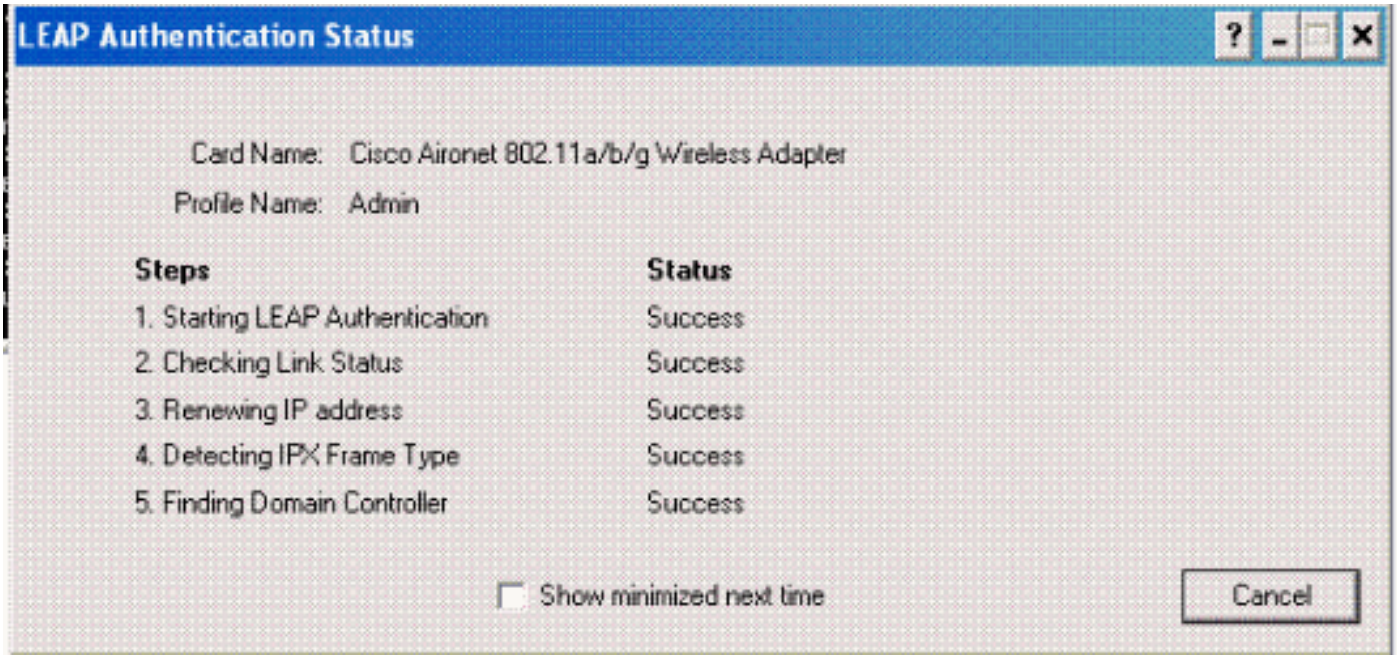
Wanneer het profiel voor de draadloze gebruiker vanuit de Admin-afdeling is geactiveerd, wordt de gebruiker gevraagd de gebruikersnaam/het wachtwoord voor de LEAP-verificatie in te voeren. Hierna volgt een voorbeeld:



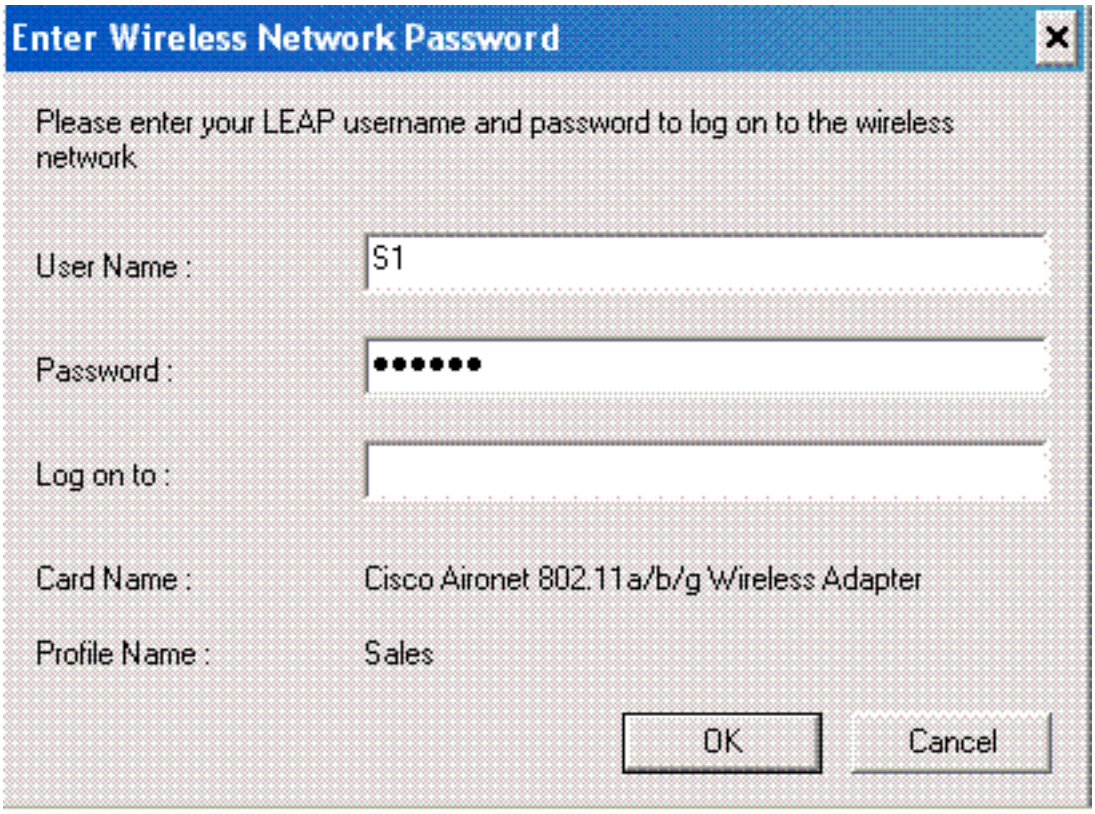
De LAP en vervolgens geeft WLC de gebruikersreferenties aan de externe RADIUS-server (Cisco Secure ACS) door om de aanmeldingsgegevens te valideren. De WLC geeft de referenties met inbegrip van de DNIS-eigenschap (SSID-naam) door aan de RADIUS-server voor validatie.

De RADIUS-server verifieert de gebruikersreferenties door de gegevens te vergelijken met de gebruikersdatabase (en de NAR's) en geeft toegang tot de draadloze client wanneer de gebruikersreferenties geldig zijn.

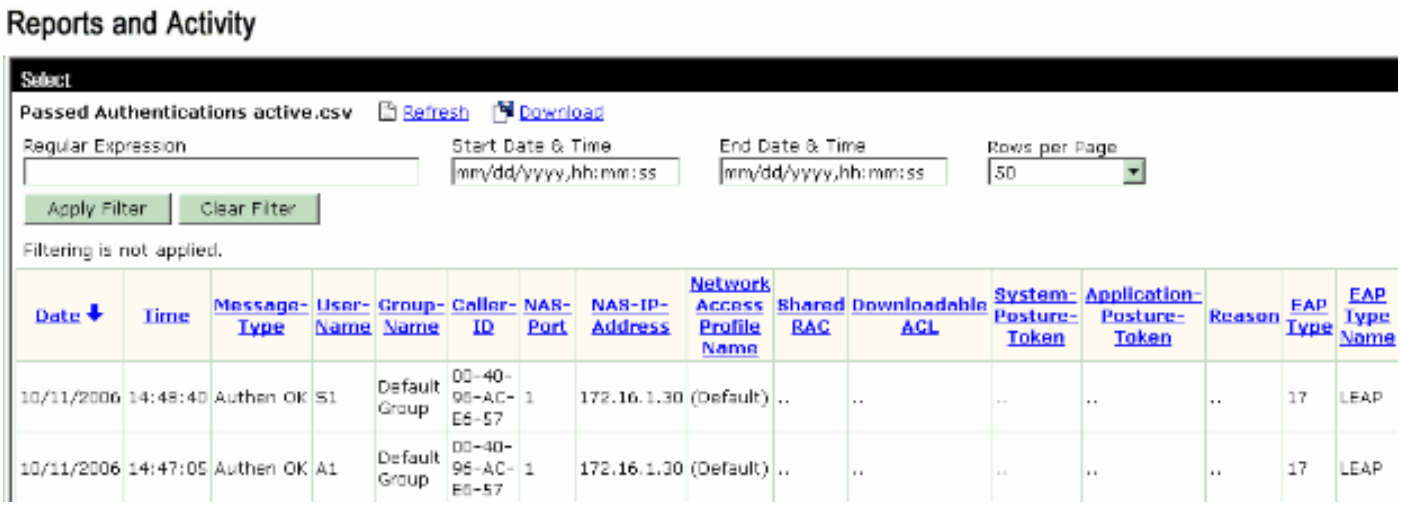
Bij succesvolle RADIUS-verificatie associeert de draadloze client met de LAP.



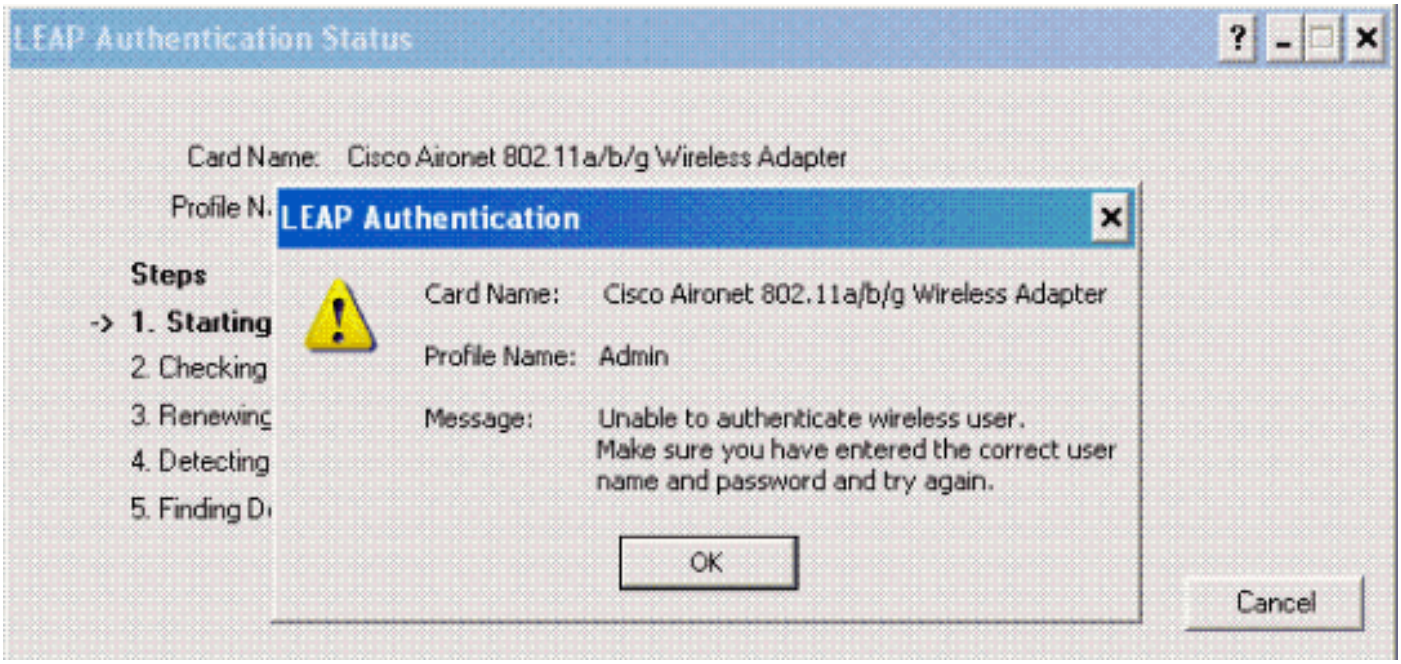
Op dezelfde manier wordt de gebruiker, wanneer een gebruiker uit de verkoopafdeling het verkoopprofiel activeert, geauthentiseerd door de RADIUS-server op basis van de LEAP-gebruikersnaam/het wachtwoord en de SSID.



Het Passed Authentication-rapport op de ACS-server toont aan dat de client de RADIUS-verificatie (EAP-verificatie en SSID-verificatie) heeft doorlopen. Hierna volgt een voorbeeld:



Als de verkoopgebruiker nu probeert de **Admin** SSID te benaderen, ontkent de RADIUS-server de gebruikerstoegang tot WLAN. Hierna volgt een voorbeeld:



Op deze manier kunnen de gebruikers beperkte toegang krijgen op basis van de SSID. In een ondernemingsklimaat kunnen alle gebruikers die in een specifieke afdeling vallen, in één groep worden gegroepeerd en de toegang tot de WLAN kan worden verleend op basis van de SSID die zij gebruiken zoals in dit document wordt uitgelegd.

Problemen oplossen

Opdrachten voor troubleshooting

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

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

- **debug dot1x aaa** schakelt het debug van 802.1x AAA-interacties in.
- **bug dot1x-pakket activeren**-schakelt het debug van alle punt1x-pakketten in.

- **debug in alle** schakelt u het debug van alle AAA-berichten in.

U kunt ook het Geautomatiseerde verificatierapport en het mislukte verificatierapport gebruiken op de Cisco Secure ACS-server om een oplossing voor de configuratie te vinden. Deze verslagen staan onder het venster **Rapporten en Activiteiten** op de ACS-GUI.

Gerelateerde informatie

- PPP-verificatie met WLAN-controllers (WLC) - configuratievoorbeeld
- Configuratievoorbeeld van draadloze LAN-controllers
- Configuratievoorbeeld van AP-groep VLAN's met draadloze LAN-controllers
- Draadloze ondersteuningspagina
- Technische ondersteuning en documentatie – Cisco Systems