Configuratie van draadloze domeinservices

Inhoud

Inleiding

Dit document introduceert het concept Wireless Domain Services (WDS). Het document beschrijft ook hoe u één access point (AP) of de draadloze LAN-servicesmodule (WLSM) kunt configureren als de WDS en op zijn minst één interface als AP. De procedure in dit document leidt u naar een WDS die functioneel is en klanten toestaat om aan of WDS AP of aan een infrastructuur AP te verbinden. Dit document is bedoeld om een basis te leggen waarvandaan u Fast Secure Roaming kunt configureren of een Wireless LAN Solutions Engine (WLSE) in het netwerk introduceren, zodat u de functies kunt gebruiken.

Voorwaarden

Vereisten

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

- Zorg voor een grondige kennis van draadloze LAN-netwerken en draadloze beveiligingsproblemen.
- Beschikken over de huidige MAP-beveiligingsmethoden (Extensible Authentication Protocol).

Gebruikte componenten

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

- APs met Cisco IOS® software
- Cisco IOS-softwarerelease 12.3(2)JA2 of hoger
- Catalyst 6500 Series draadloze LAN-servicesmodule

De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden gebruikt, zijn gestart met een geklaarde (standaard) configuratie en een IP-adres op interface BVI1. De unit is dus toegankelijk via de Cisco IOS-softwarerelease of de opdrachtregel-interface (CLI). Als u in een levend netwerk werkt, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Draadloze domeinservices

WDS is een nieuwe functie voor APs in Cisco IOS Software en de basis van Catalyst 6500 Series WLSM. WDS is een kernfunctie die andere eigenschappen zoals deze toelaat:

- Snelle beveiligde roaming
- WLSE-interactie
- Radiobeheer

U moet relaties aangaan tussen de AP's die deelnemen aan WDS en WLSM, voordat andere op WDS gebaseerde functies werken. Een van de doelstellingen van WDS is de noodzaak voor de authenticatieserver te elimineren om gebruikersreferenties te valideren en de tijd te verkorten die nodig is voor authenticaties van cliënten.

Om WDS te gebruiken, moet u één AP of WLSM als WDS aanwijzen. Een WDS AP moet een WDS gebruikersnaam en wachtwoord gebruiken om een relatie met een authenticatieserver in te stellen. De authenticatieserver kan een externe RADIUS-server of de lokale RADIUS-serverfunctie in de WDS-AP zijn. WLSM moet een relatie hebben met de authenticatieserver, ook al hoeft WLSM niet te authenticeren aan de server.

Andere APs, genaamd infrastructuur APs, communiceren met de WDS. Voordat de registratie plaatsvindt, moeten de infrastructurele APs zichzelf aan de WDS authentiek verklaren. Een infrastructuurservergroep op de WDS definieert deze infrastructurele authenticatie.

Een of meer groepen van clientservers op de WDS definiëren clientverificatie.

Wanneer een client probeert te associëren met een infrastructuur AP, geeft de infrastructuur AP de referenties van de gebruiker aan WDS voor validatie door. Als WDS de geloofsbrieven voor het eerst ziet, keert WDS zich aan de authenticatieserver om de geloofsbrieven te valideren. De WDS cakt dan de geloofsbrieven, om de noodzaak te elimineren om terug te keren naar de authenticatieserver wanneer de zelfde gebruiker opnieuw authenticatie probeert. Voorbeelden van herauthenticatie zijn:

- herblokkeren

- Roaming
- Wanneer de gebruiker het clientapparaat start

Elk op RADIUS gebaseerd EAP-verificatieprotocol kan via WDS worden getunneerd, zoals:

- Lichtgewicht MAP (LEAP)
- Beschermd MAP (PEAP)
- EAP-TLS-beveiliging (Transport Layer Security)
- EAP-flexibele verificatie door beveiligde tunneling (EAP-FAST)

MAC-adresverificatie kan ook worden tunnelgemaakt naar een externe verificatieserver of naar een lokale lijst met een WDS-AP. WLSM steunt geen MAC-adresverificatie.

De WDS en de infrastructuur APs communiceren via een multicast protocol dat WLAN Context Control Protocol (WLCCP) wordt genoemd. Deze multicast berichten kunnen niet worden routeerd, zodat een WDS en de bijbehorende infrastructuur APs in het zelfde IP en op het zelfde LAN segment moeten zijn. Tussen WDS en WLSE gebruikt WLCCP TCP- en User Datagram Protocol (UDP) op poort 2887. Wanneer WDS en WLSE op verschillende subnetwerken zijn, kan een protocol als Network Address Translation (NAT) de pakketten niet vertalen.

Een AP ingesteld als het WDS apparaat steunt tot 60 deelnemende APs. Een geïntegreerde services router (ISR) ingesteld als WDS-apparaten ondersteuning voor maximaal 100 deelnemende AP's. En een WLSM-uitgeruste switch ondersteunt tot 600 deelnemende AP's en tot 240 mobiliteitsgroepen. Eén AP ondersteunt maximaal 16 mobiliteitsgroepen.

Opmerking: Cisco raadt aan dat de infrastructuur APs dezelfde versie van IOS als het WDS-apparaat uitvoeren. Als u een oudere versie van IOS gebruikt, kunnen APs niet echt maken aan het WDS apparaat. Daarnaast raadt Cisco u aan de nieuwste versie van de IOS te gebruiken. U kunt de nieuwste versie van IOS vinden in de pagina Draadloze downloads.

Rol van het WDS-apparaat

Het WDS-apparaat voert verschillende taken uit op uw draadloos LAN:

- Hiermee wordt de WDS-functie aangepast en wordt deelgenomen aan het selecteren van het beste WDS-apparaat voor uw draadloze LAN-netwerk. Wanneer u uw draadloze LAN voor WDS configureren stelt u één apparaat in als de hoofdWDS-kandidaat en een of meer extra apparaten als back-upkandidaten voor WDS. Als het hoofdapparaat van WDS van lijn gaat, neemt één van de reservekopieapparaten zijn plaats.
- Verifieert alle APs in Subnet en stelt een veilig communicatiekanaal met elk van hen vast.
- Verzamelt radioverslaggegevens van APs in Subnet, aggregeert de gegevens, en zendt het naar het WLSE apparaat op uw netwerk door.
- Handelt in als doorvoersnelheid voor alle 802.1x-geauthenticeerde clientapparaten die gekoppeld zijn aan deelnemende AP's.
- Registreert alle client apparaten in het netwerk die dynamisch het controleren gebruiken, vastlegt sessiesleutels voor hen, en caches hun veiligheidsgeloofsbrieven. Wanneer een client naar een andere AP stroomt, stuurt het WDS-apparaat de beveiligingsreferenties van de client naar de nieuwe AP door.

Rol van access points die het WDS-apparaat gebruiken

De APs op uw draadloos LAN interactie met het WDS apparaat in deze activiteiten:

- Ontdek het huidige WDS-apparaat en verklaar WDS-advertenties aan het draadloze LAN.
- Verifieer met het WDS-apparaat en stel een beveiligd communicatiekanaal in naar het WDS-apparaat.
- Registreer gekoppelde clientapparaten met het WDS-apparaat.
- Rapporteer radiogegevens aan het WDS-apparaat.

Configuratie

WDS presenteert de configuratie op een ordelijke, modulaire manier. Elk concept bouwt voort op het concept dat voorafgaat. De WDS laat andere configuratie-items, zoals wachtwoorden, toegang op afstand en radio-instellingen, voor helderheid en focus op de kernonderwerp achter.

In deze sectie worden de benodigde informatie getoond om de functies te configureren die in dit document worden beschreven.

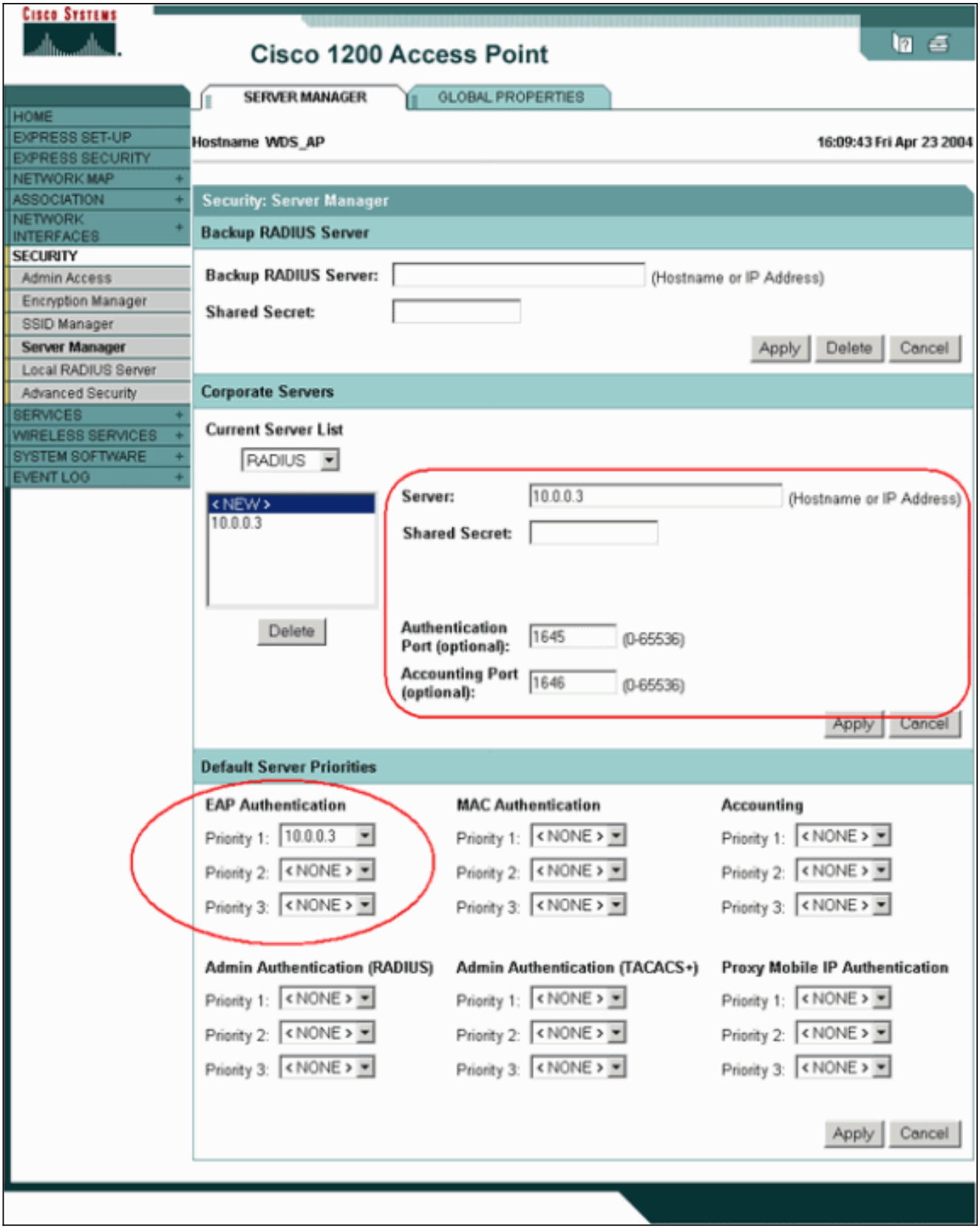
Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

AP als WDS toewijzen

De eerste stap is het aanwijzen van een AP als de WDS. WDS AP is de enige die met de authenticatieserver communiceert.

Voltooi deze stappen om een AP als WDS aan te wijzen:

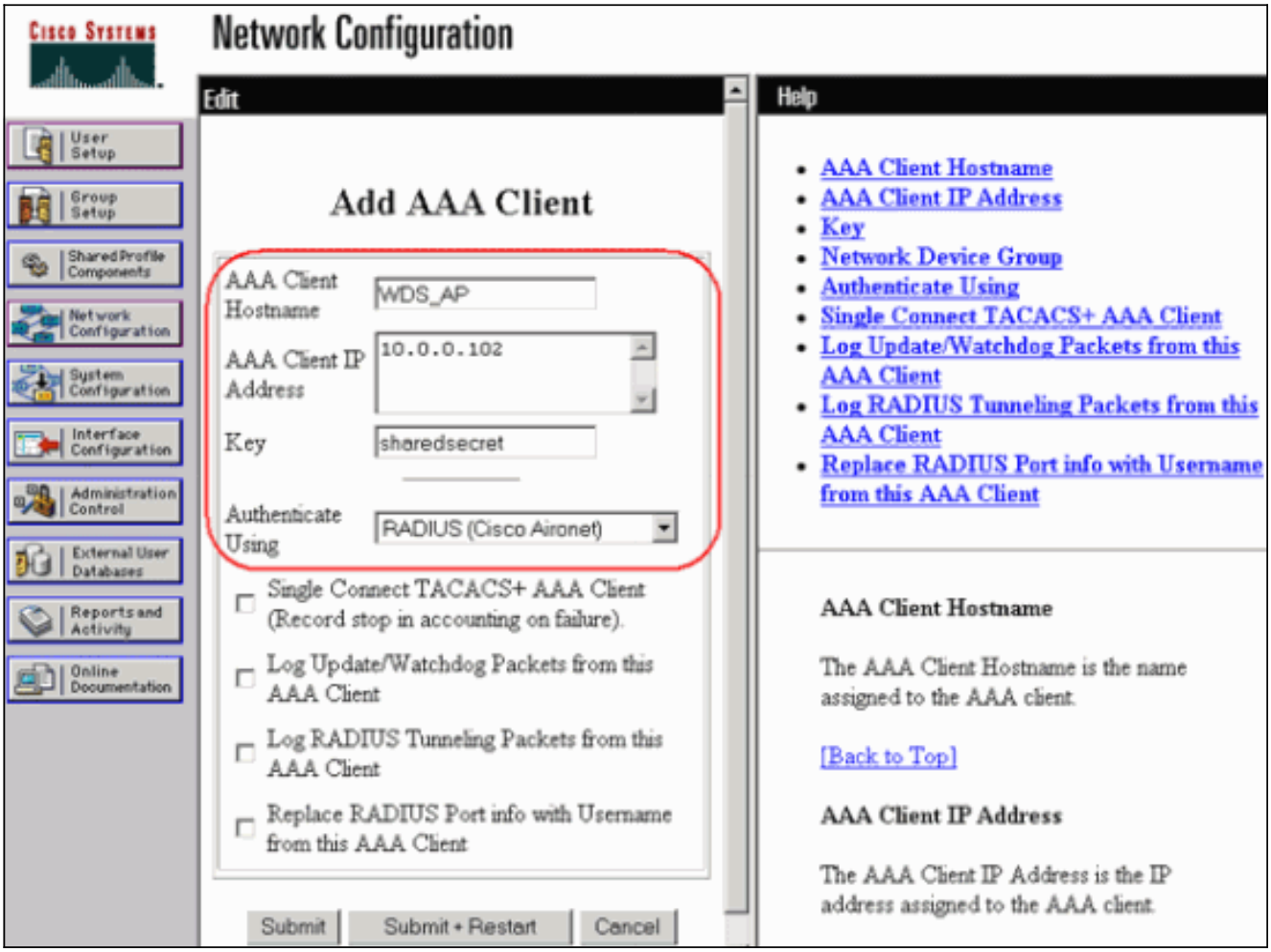
1. Om de verificatieserver op de WDS-pagina te configureren kiest u **Security > Server Manager** om naar het tabblad Server Manager te gaan:Typ onder Corporate Server het IP-adres van de verificatieserver in het veld Server.Specificeer het Gedeeld Gebied en de poorten.Stel onder Default Server Priorities het veld Prioriteit 1 in op dat server-IP-adres onder het juiste
verificatietype.



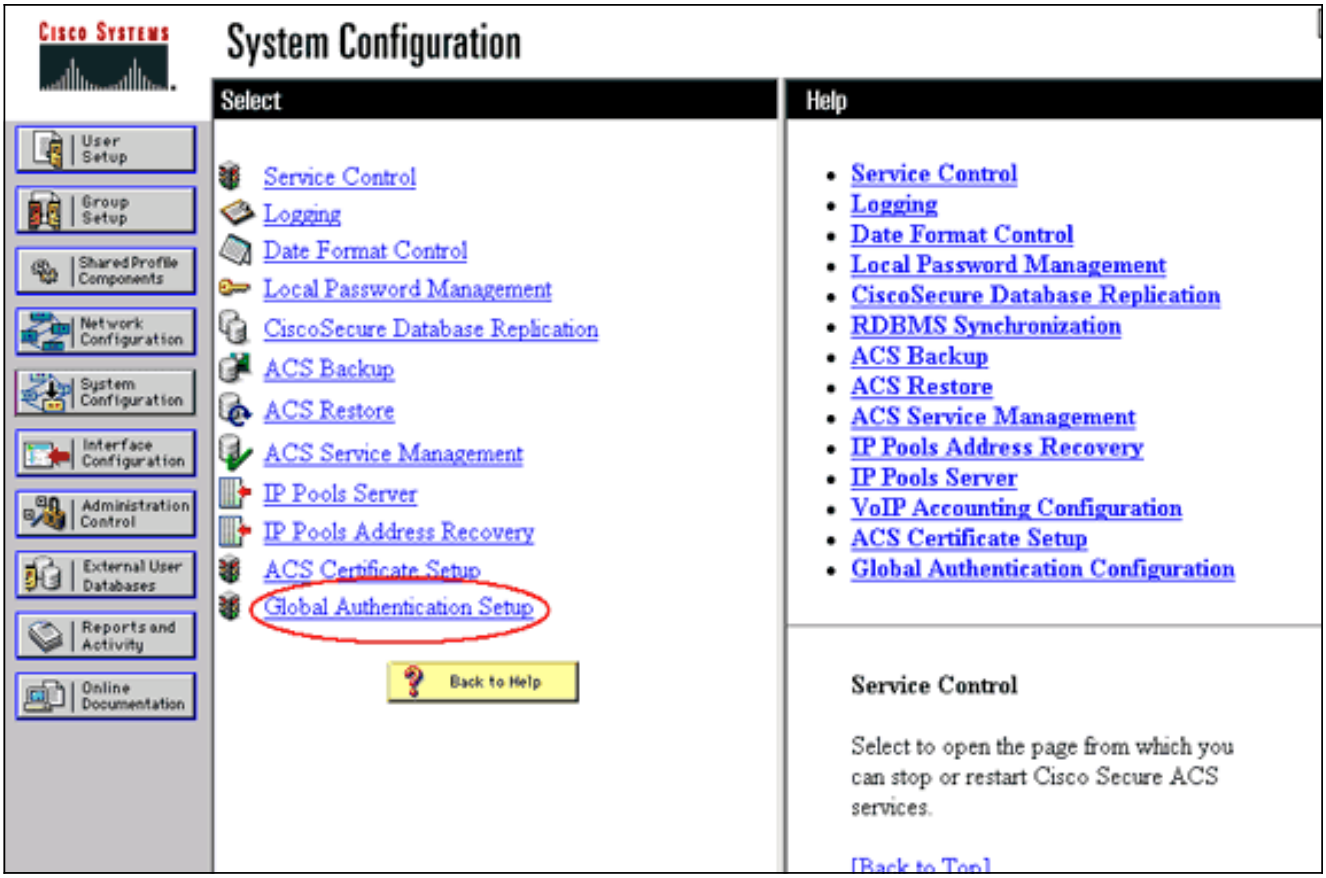
U kunt deze opdrachten ook vanuit de CLI uitgeven:

2. De volgende stap is het configureren van de WDS AP in de authenticatieserver als een verificatie-, autorisatie- en accounting (AAA) client. Hiervoor moet u de WDS AP als een AAA-client toevoegen. Voer de volgende stappen uit:**Opmerking:** Dit document gebruikt de Cisco Secure ACS-server als de verificatieserver.In Cisco Secure Access Control Server (ACS) gebeurt dit op de pagina Network Configuration waar u deze eigenschappen voor de WDS-AP definieert:NameIP-adresGedeeld geheimVerificatiemethodeRADIUS Cisco AironetRADIUS-taskforce Internet Engineering [IETF]Klik op **Inzenden**.Raadpleeg voor andere niet-ACS-verificatieservers de documentatie van de

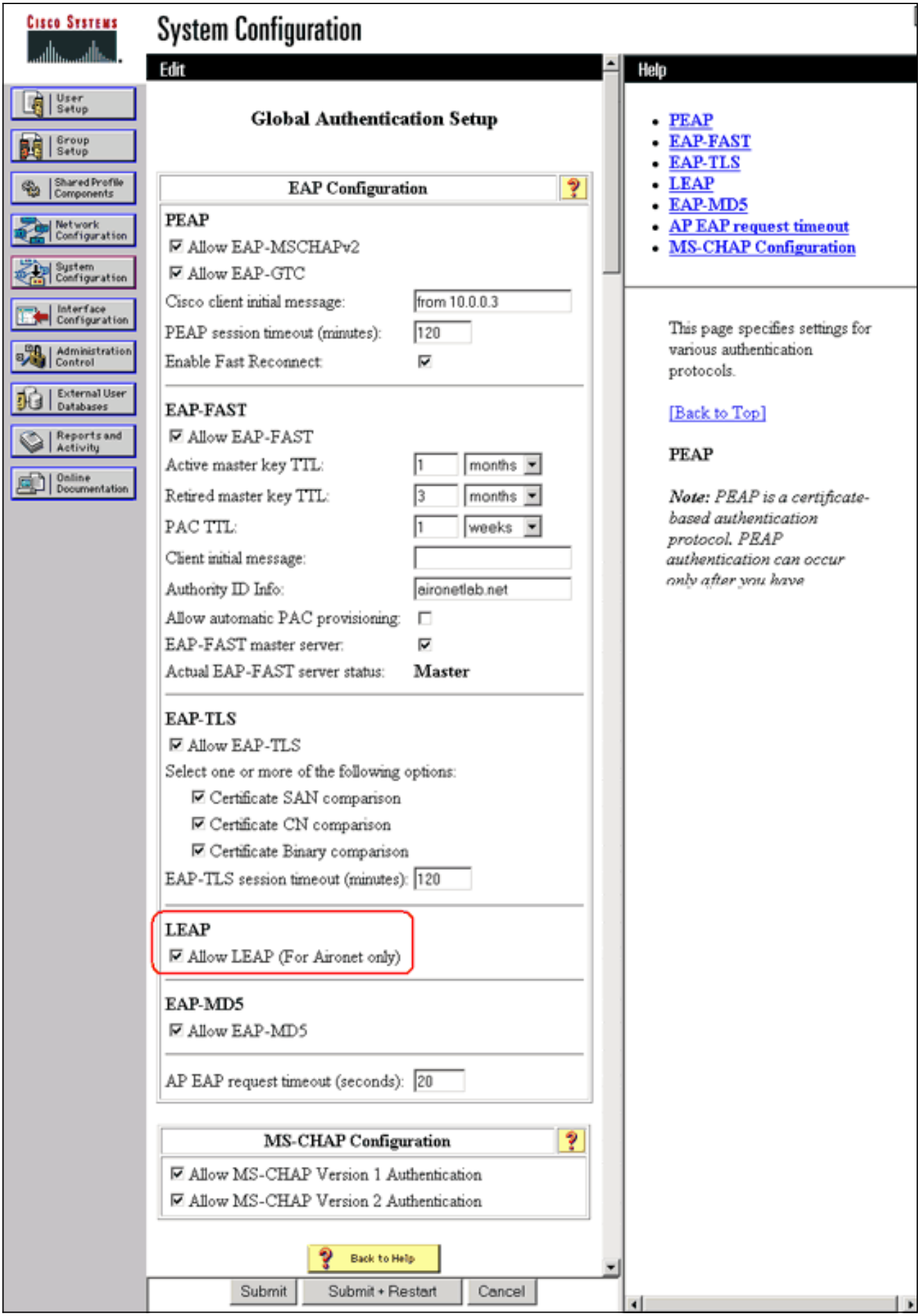
fabrikant.



Zorg er ook voor dat u in Cisco Secure ACS, dat u ACS configureren om LEAP-verificatie uit te voeren op de systeemconfiguratie - pagina Global Authentication Setup. Klik eerst op **System Configuration** en vervolgens op **Global Authentication Setup**.

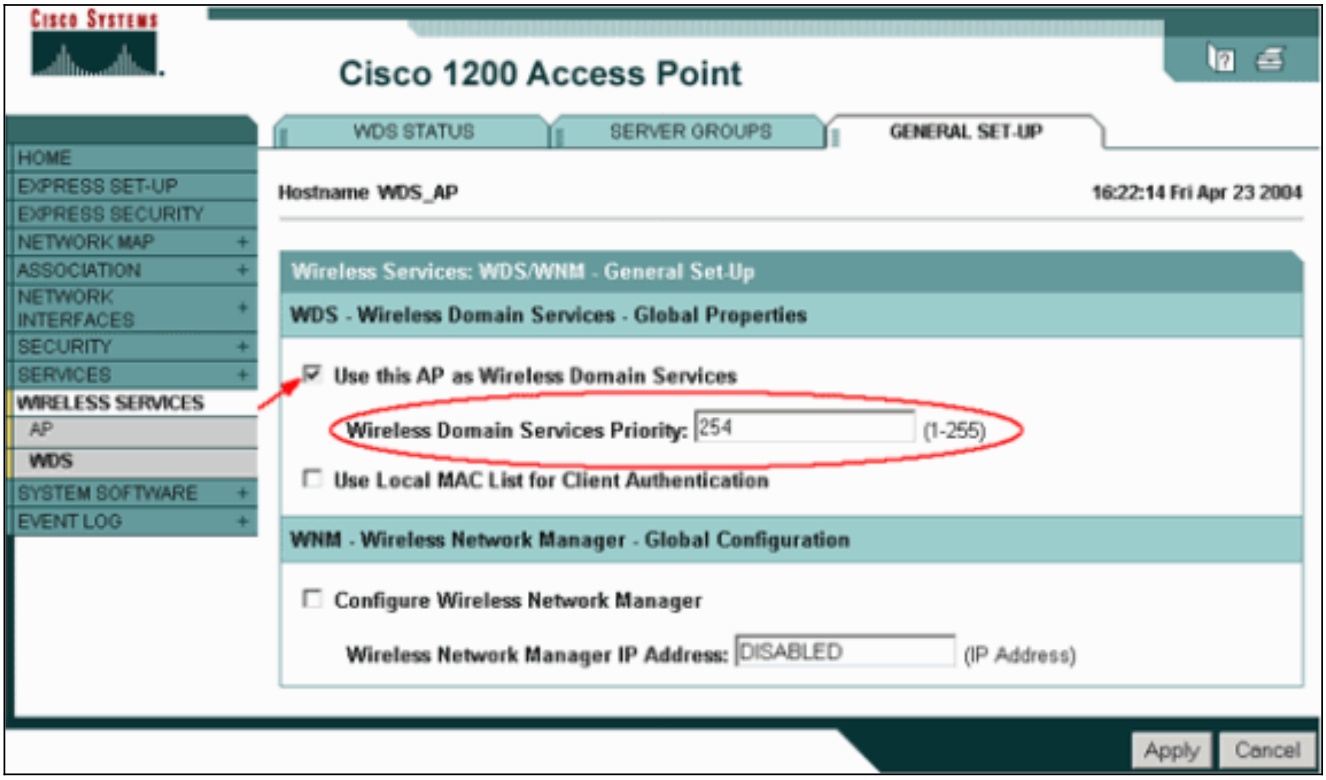


Scrolt de pagina naar de LEAP-instelling. Wanneer u het vakje aankruist, verifieert ACS LEAP.



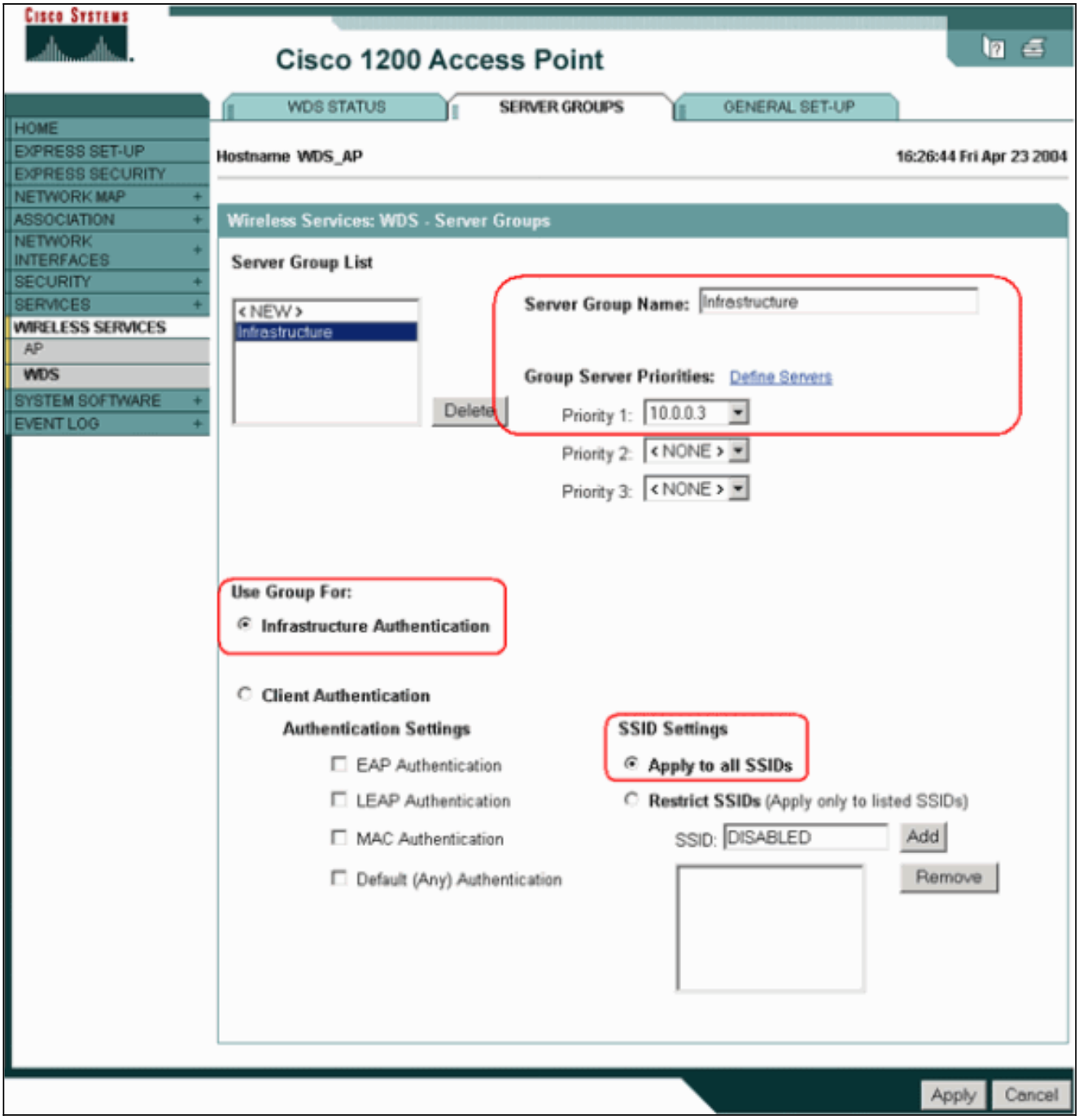
3. Om de instellingen van WDS op het AP van WDS te configureren, kiest u **Draadloze services > WDS** op het WDS AP en klikt u op het **tabblad General Setup**. Volg deze stappen:Controleer onder WDS-Wireless Domain Services - Global Properties **of deze AP**

als draadloze Domain Services gebruiken.Stel de waarde voor het prioriteitsveld voor draadloze domeinservices in op een waarde van ongeveer **254**, omdat dit de eerste is. U kunt een of meer APs of switches als kandidaten configureren om WDS te verstrekken. Het apparaat met de hoogste prioriteit verstrekt
WDS.



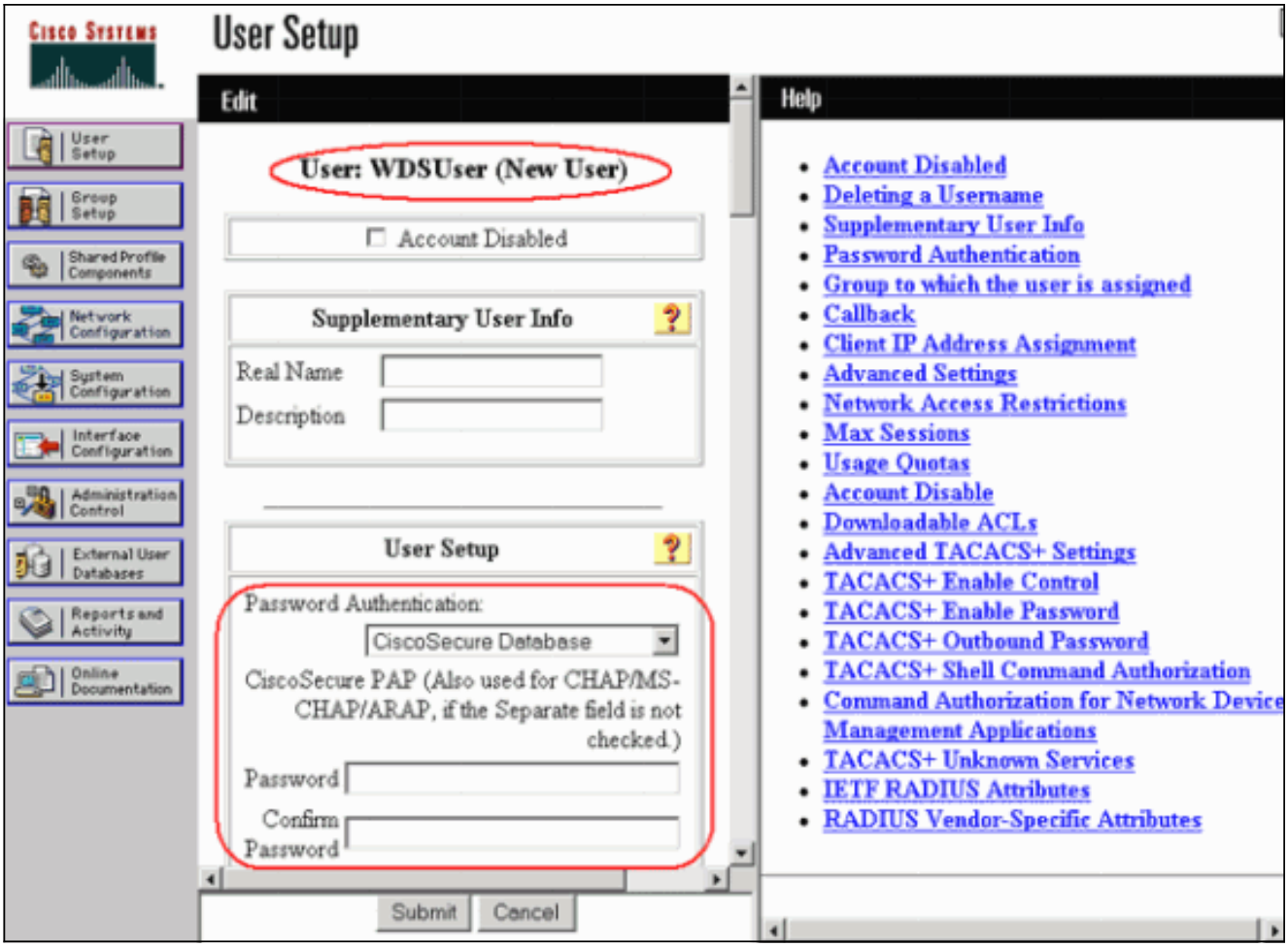
U kunt deze opdrachten ook vanuit de CLI uitgeven:

4. Kies **draadloze services > WDS** en ga naar het tabblad **servergroepen**:Defineer een naam van de Server die andere APs, een groep van de Infrastructuur voor authentiek verklaart.Stel Prioriteit 1 in op de eerder ingestelde authenticatieserver.Klik op de **gebruikersgroep voor:** radioknop **Infrastructuurverificatie**.Pas de instellingen toe op de relevante Service Set Identifier
(SSID's).



U kunt deze opdrachten ook vanuit de CLI uitgeven:

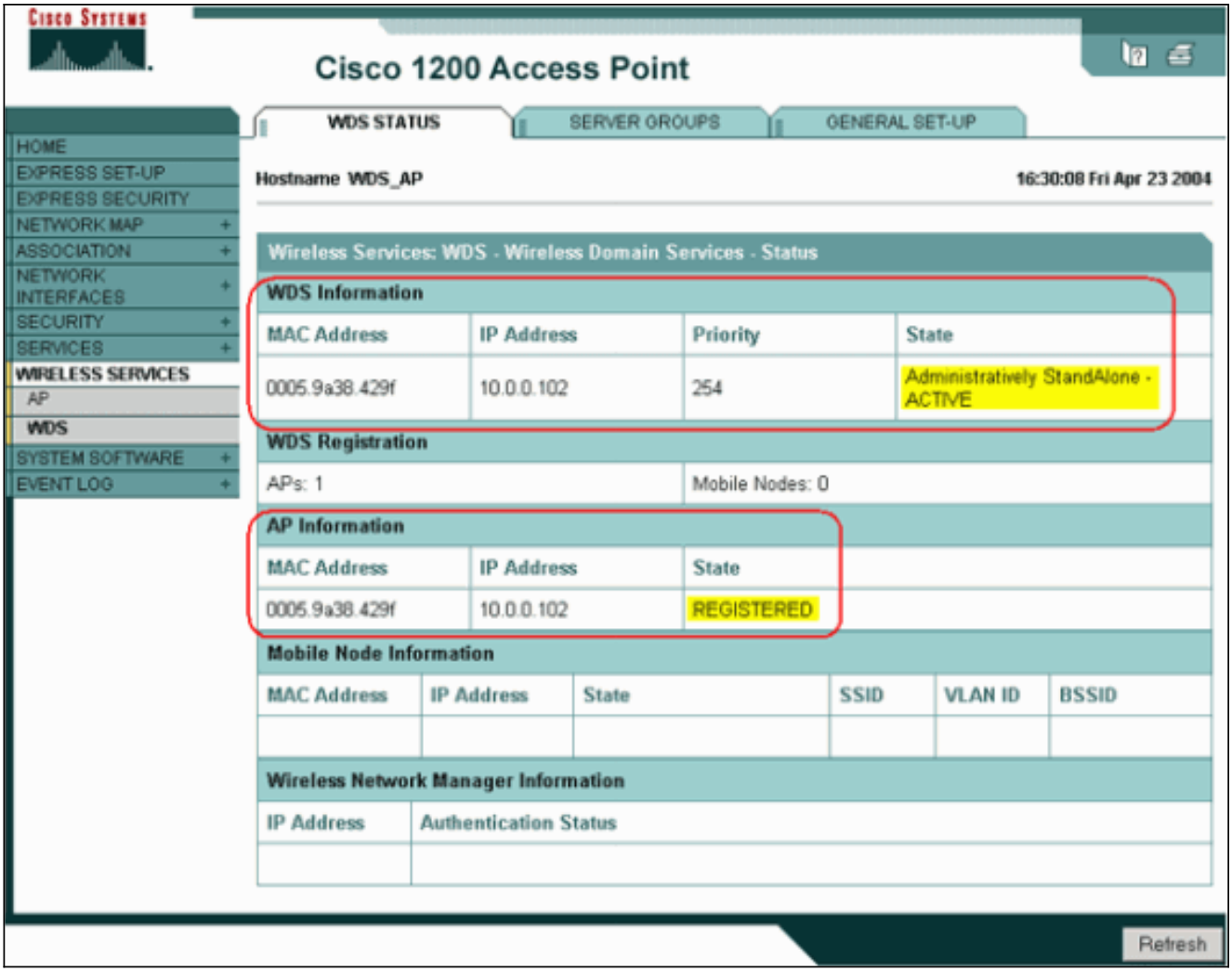
5. Configureer de naam en het wachtwoord van de WDS-gebruiker als een gebruiker in de verificatieserver.In Cisco Secure ACS, gebeurt dit op de pagina User Setup, waar u de WDS-gebruikersnaam en het wachtwoord definieert. Raadpleeg voor andere niet-ACS-verificatieservers de documentatie van de fabrikant.**Opmerking:** Plaats de WDS-gebruiker niet in een groep waaraan veel rechten en privileges zijn toegewezen — WDS vereist alleen beperkte
authenticatie.



6. Kies **Draadloze services > AP** en klik op **Toegang** voor de optie Deelnemen aan SWAN infrastructuur. Typ het wachtwoord voor het WDS-gebruik en het wachtwoord.U moet een WDS - gebruikersnaam en een wachtwoord op de authenticatieserver definiëren voor alle apparaten die u leden van de WDS
aanwijst.

U kunt deze opdrachten ook vanuit de CLI uitgeven:

7. Kies **draadloze services > WDS**. Controleer in het tabblad WDS AP Status of de WDS AP in het informatiegebied WDS, in de actieve staat, verschijnt. Het AP moet ook in het AP Informatiegebied verschijnen, met Staat zoals GEREGISTREERD.Als AP niet GEREGISTREERD of ACTIEF lijkt, controleer de authenticatieserver op fouten of mislukte authenticatiepogingen.Wanneer het AP correct registreert, voeg een infrastructuur AP toe om de diensten van de WDS te
gebruiken.



U kunt deze opdrachten ook vanuit de CLI uitgeven:**Opmerking:** je kunt cliëntenassociaties niet testen omdat de cliëntauthecertificering nog geen bepalingen heeft.

WLSM als WDS toewijzen

In deze sectie wordt uitgelegd hoe u een WLSM als een WDS kunt configureren. WDS is het enige apparaat dat met de authenticatieserver communiceert.

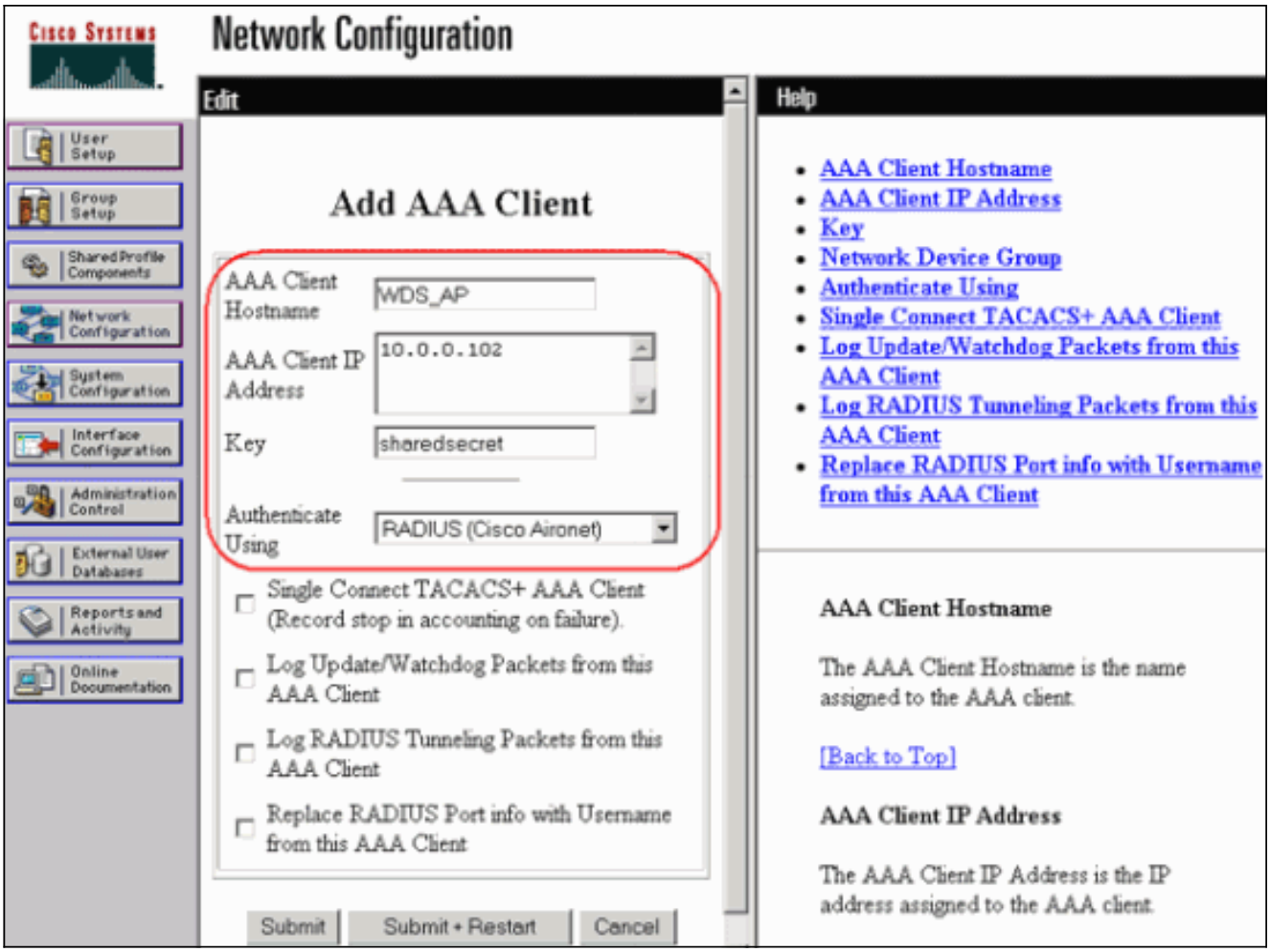
Opmerking: Geef deze opdrachten uit aan de opdrachtprompt van de WLSM en niet aan de Supervisor Engine 720. Om de opdrachtmelding van de WLSM te bereiken, geeft u deze opdrachten uit `zodat` u de opdrachtmelding in Supervisor Engine 720 `kunt` wijzigen:

```
c6506#session slot x proc 1
!--- In this command, x is the slot number where the
WLSM resides. The default escape character is Ctrl-^,
then x. You can also type 'exit' at the remote prompt to
end the session Trying 127.0.0.51 ... Open User Access
Verification Username: <username> Password: <password>
wlan>enable
Password: <enable password>
wlan#
```

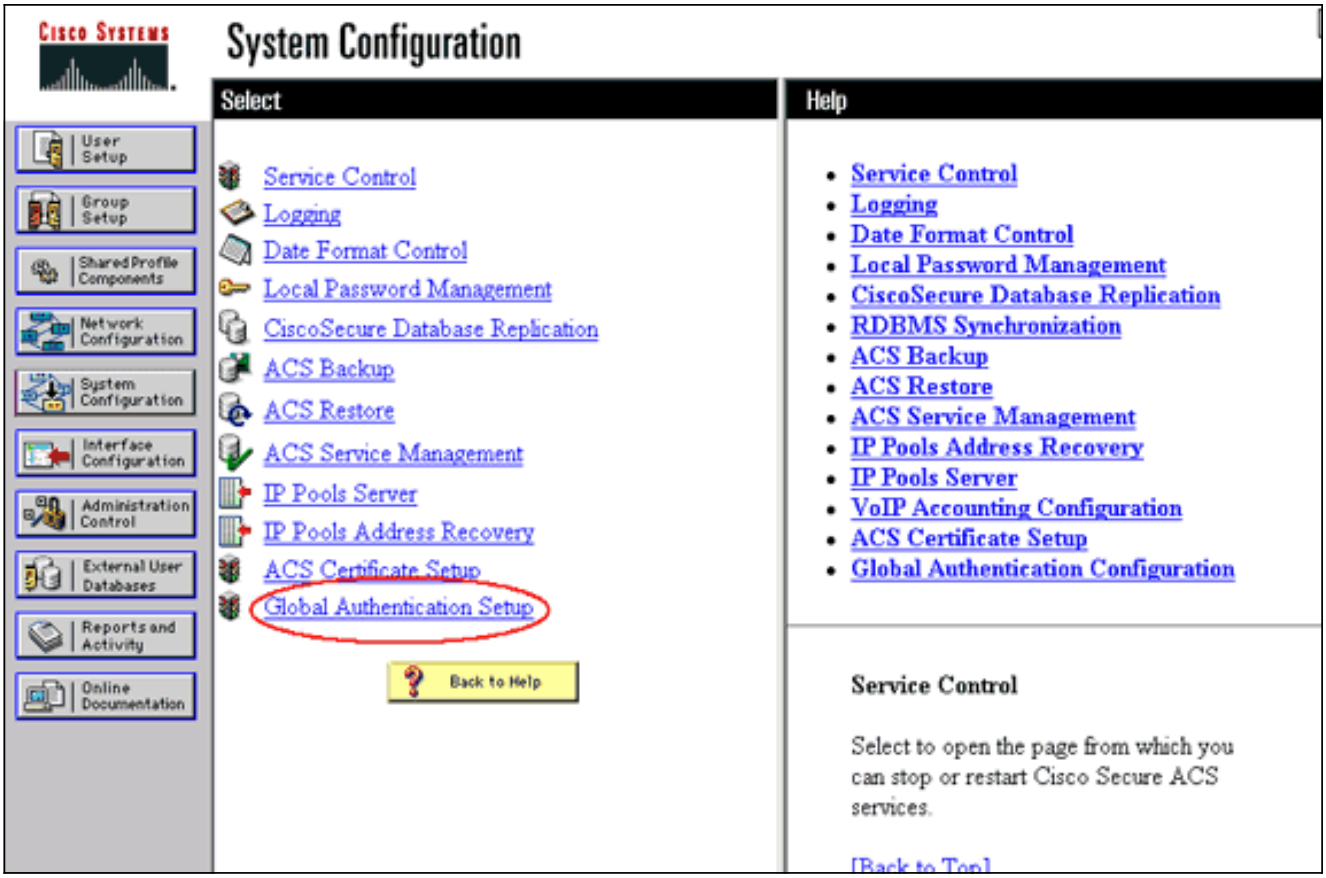
N.B.: Om probleemoplossing te ondersteunen en uw WLSM gemakkelijker te onderhouden, dient u de externe toegang van telers tot de WLSM te configureren. Raadpleeg Telnet-toegang configureren.

Zo wijst u een WLSM als WDS aan:

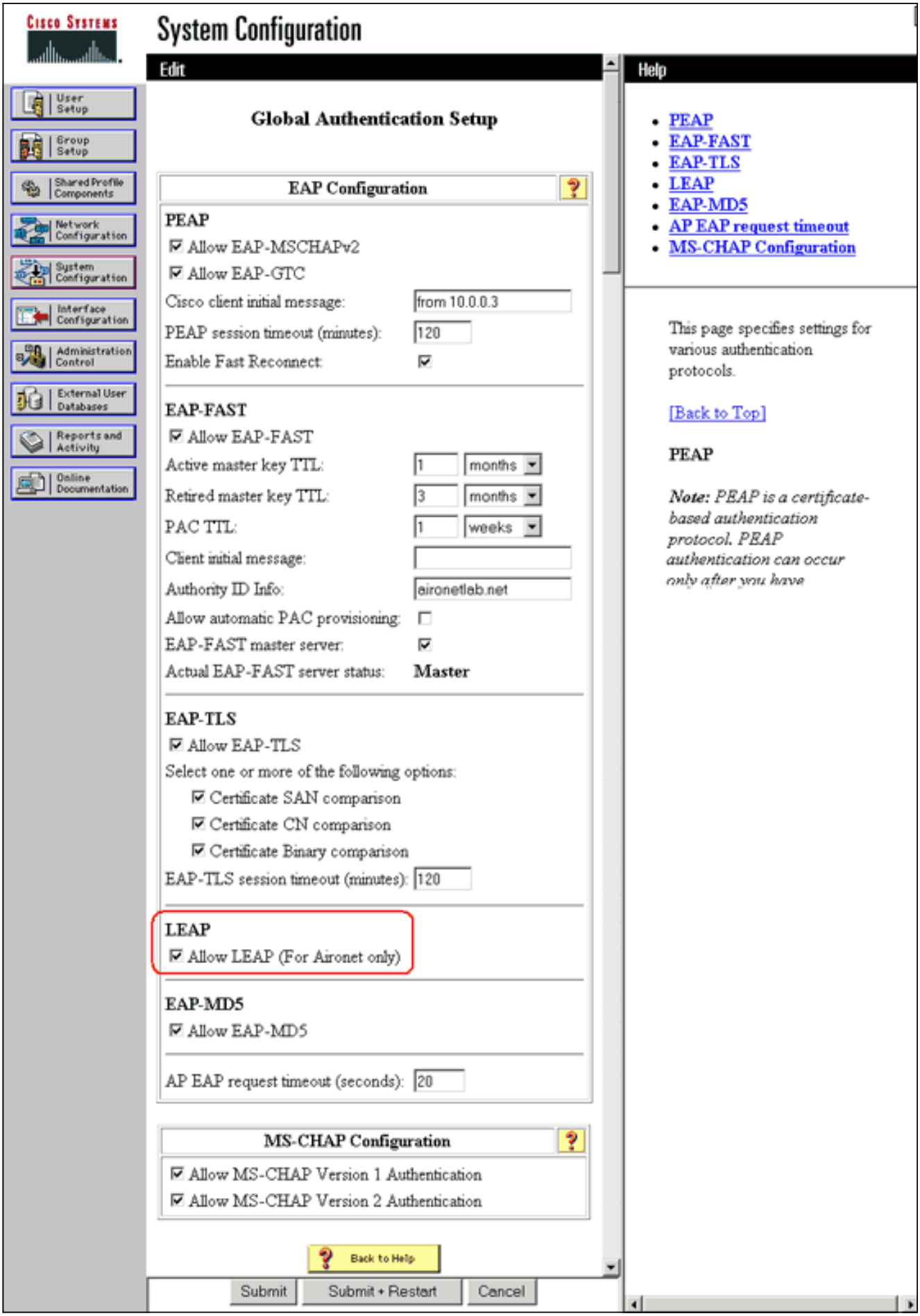
1. Vanuit CLI van WLSM, geef deze opdrachten uit en voer een relatie op met de authenticatieserver:**Opmerking:** Er is geen prioriteitscontrole in de WLSM. Als het netwerk meerdere WLSM modules bevat, gebruikt WLSM overtollige configuratie om de primaire module te bepalen.
2. Configureer de WLSM in de verificatieserver als een AAA-client.In Cisco Secure ACS komt dit voor op de pagina Network Configuration waar u deze eigenschappen voor de WLSM definieert:NameIP-adresGedeeld geheimVerificatiemethodeRADIUS Cisco AironetRADIUS-IETFRaadpleeg voor andere niet-ACS-verificatieservers de documentatie van de fabrikant.



Ook, in Cisco Secure ACS, moet u ACS configureren om LEAP-verificatie uit te voeren op de systeemconfiguratie - pagina Global Authentication Setup. Klik eerst op **System Configuration** en vervolgens op **Global Authentication Setup**.



Scrolt de pagina naar de LEAP-instelling. Wanneer u het vakje aankruist, verifieert ACS LEAP.



3. Op WLSM, definieer een methode die andere APs (een groep van de infrastructuurserver) authentiek verklaart.
4. Bepaal op WLSM een methode die de clientapparaten (een gebruikersservergroep) echt

maakt en welke EAP-typen deze klanten gebruiken.**N.B.:** Deze stap heft de noodzaak van het definiëren van de clientverificatieprocedure op.

5. Defineer een uniek VLAN tussen Supervisor Engine 720 en WLSM om WLSM in staat te stellen met externe entiteiten zoals APs en authenticatieservers te communiceren. Dit VLAN is overal anders of voor een ander doel op het netwerk niet gebruikt. Maak eerst het VLAN op Supervisor Engine 720 en geef deze opdrachten dan uit:Op Supervisor Engine 720:Op het WLSM:
6. Controleer de functie van WLSM met deze opdrachten:Op het WLSM:Op Supervisor Engine 720:

AP als infrastructuurapparaat aanwijzen

Daarna moet u ten minste één infrastructuurelap aanwijzen en de AP met de WDS verbinden. De klanten associëren met infrastructuur APs. De infrastructuur APs vragen WDS AP of WLSM om voor hen authenticatie uit te voeren.

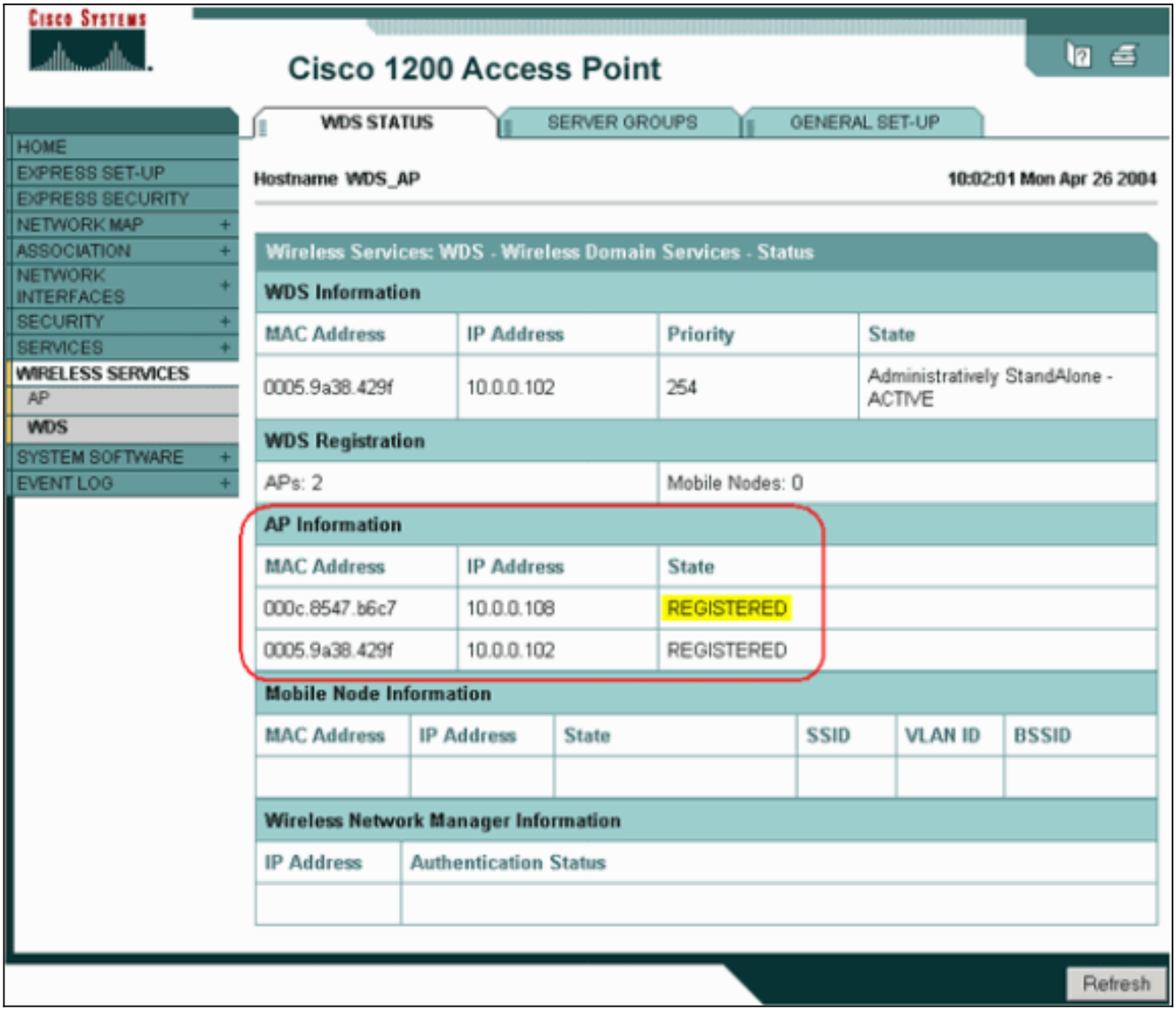
Voltooi deze stappen om een infrastructuur-AP toe te voegen dat de diensten van de WDS gebruikt:

Opmerking: deze configuratie is alleen van toepassing op de infrastructuur AP's en niet op de WDS AP.

1. Kies **draadloze services > AP**. Selecteer in het AP van de infrastructuur de optie Draadloze services **inschakelen**. Typ het wachtwoord voor het WDS-gebruik en het wachtwoord.U moet een WDS-gebruikersnaam en een wachtwoord op de authenticatieserver definiëren voor alle apparaten die lid moeten zijn van de
WDS.

U kunt deze opdrachten ook vanuit de CLI uitgeven:

2. Kies **draadloze services > WDS**. Op het tabblad WDS APStatus verschijnt de nieuwe infrastructuur AP in het informatiegebied WDS, met Staat als ACTIEF en in het AP Informatiegebied, met Staat zoals GEREGISTREERD.Als AP niet ACTIEF en/of GEREGISTREERD lijkt, controleer de authenticatieserver op om het even welke fouten of mislukte pogingen van authenticatie.Nadat AP ACTIEF en/of GEREGISTREERD lijkt, voeg een client authenticatiemethode toe aan
WDS.



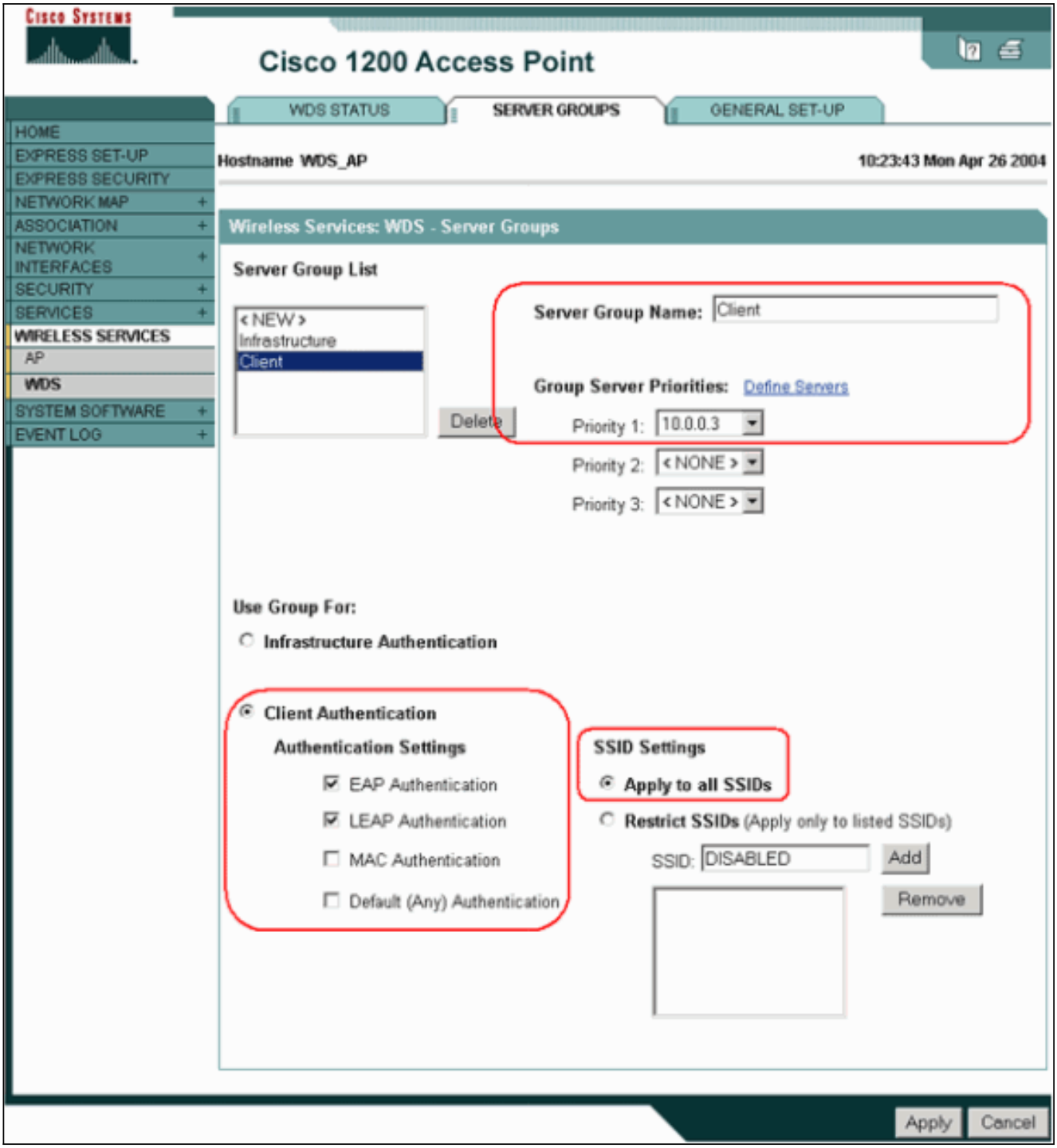
U kunt deze opdracht ook vanaf de CLI uitgeven:U kunt deze opdracht ook vanuit WLSM uitgeven:Geef deze opdracht vervolgens uit op de infrastructuur AP:**Opmerking:** je kunt cliëntenassociaties niet testen omdat de cliëntauthecertificering nog geen bepalingen heeft.

Clientverificatiemethode definiëren

Ten slotte een methode van cliënthectificatie definiëren.

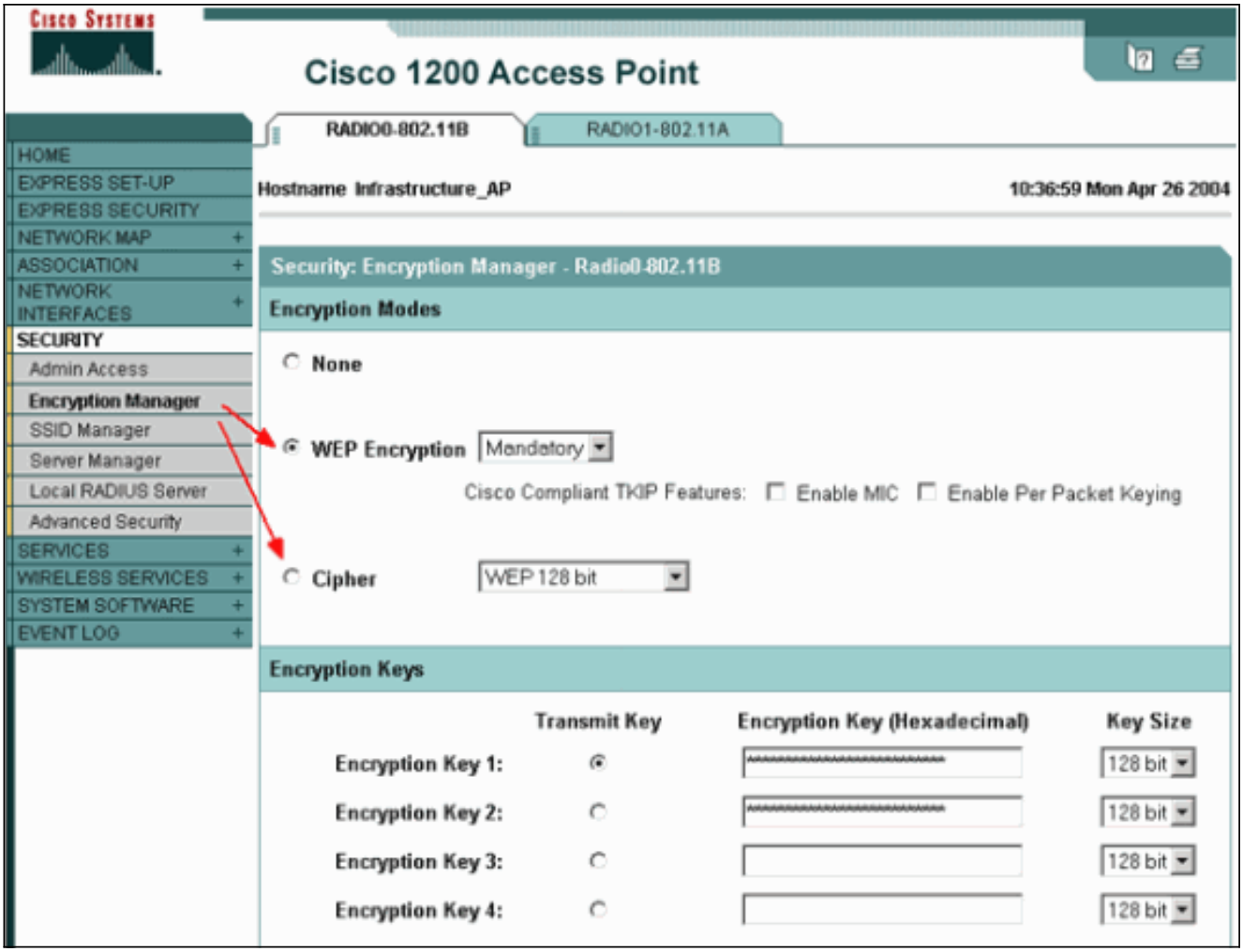
Voltooi deze stappen om een methode voor de verificatie van de cliënt toe te voegen:

1. Kies **draadloze services > WDS**. Voer deze stappen uit in het tabblad WDS AP Server Group:Defineer een servergroep die clients (een Clientgroep) voor de authenticatie van de client heeft.Stel Prioriteit 1 in op de eerder ingestelde authenticatieserver.Stel het toepasbare type van authenticatie in (LEAP, EAP, MAC, enzovoort).Pas de instellingen toe op de relevante
SSID's.

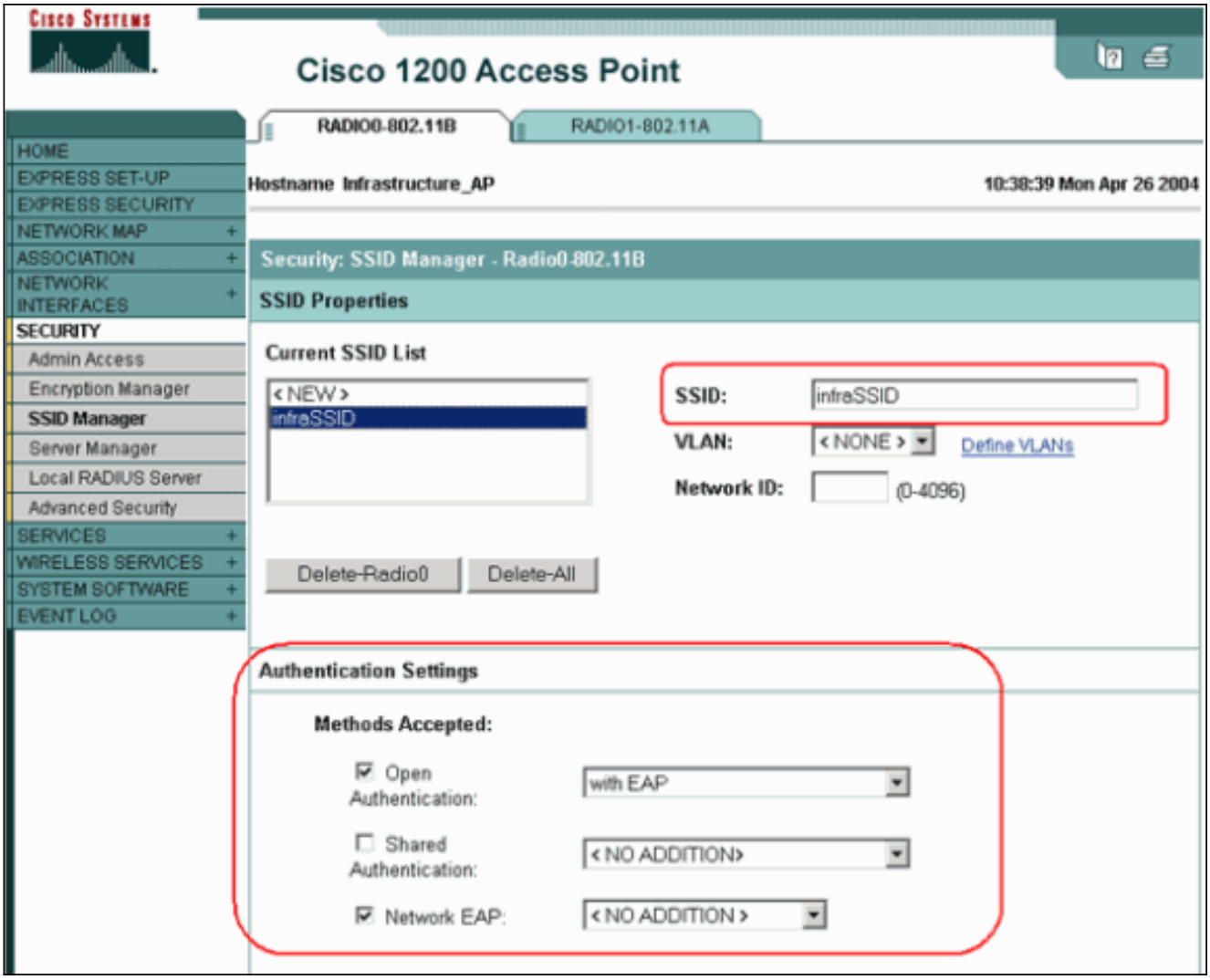


U kunt deze opdrachten ook vanuit de CLI uitgeven:**Opmerking:** Het voorbeeld WDS AP is gewijd en accepteert geen clientassociaties.**Opmerking:** configureer niet op de infrastructuur APs voor servergroepen omdat infrastructuren APs verzoeken naar de WDS doorsturen om te worden verwerkt.

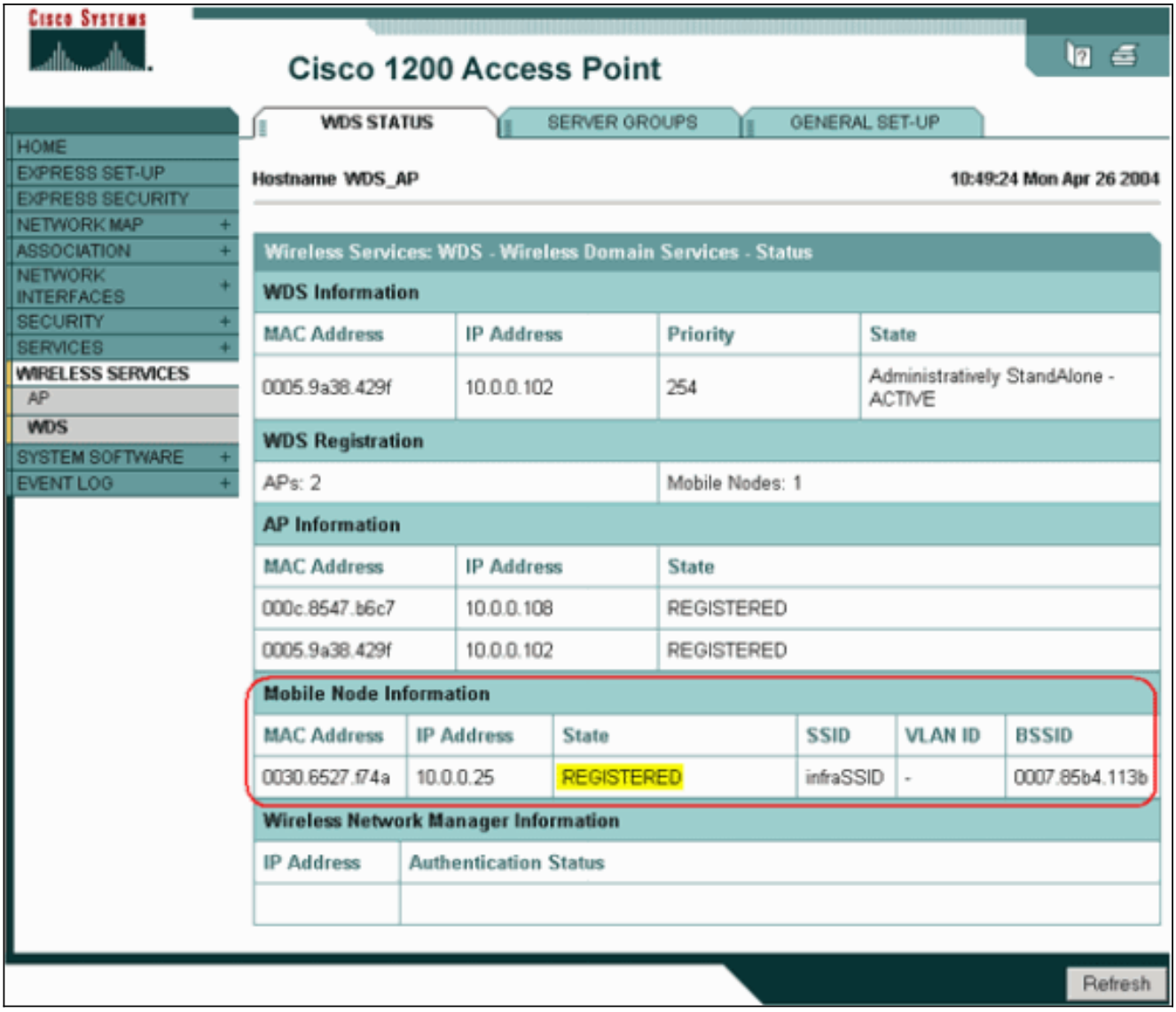
2. Op de infrastructuur AP of APs:Klik onder de menuoptie **Security > Encryption Manager** op **EFG Encryption** of **Cipher**, zoals vereist door het verificatieprotocol dat u gebruikt.



Selecteer onder de menuoptie **Security > SSID Manager** de verificatiemethoden zoals vereist door het verificatieprotocol dat u
gebruikt.



3. U kunt nu met succes testen of klanten authentiek aan infrastructuur APs. AP van de WDS in het tabblad Status WDS (onder de menuoptie **Draadloze services > WDS**) wijst erop dat de client verschijnt in het gebied met informatie over mobiel knooppunt en een GEREGISTREERDE status heeft.Als de client niet verschijnt, controleert u de verificatieserver op fouten of mislukte pogingen tot verificatie door de klanten.



U kunt deze opdrachten ook vanuit de CLI uitgeven:**Opmerking:** Als u verificatie moet debug, zorg er dan voor dat u op de WDS AP debug, omdat WDS AP het apparaat is dat met de authenticatieserver communiceert.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen op te lossen in uw configuratie. In deze lijst worden een aantal gemeenschappelijke vragen met betrekking tot de WDS-opdracht weergegeven om het nut van deze opdrachten verder te verduidelijken:

- **Vraag: Wat zijn de aanbevolen instellingen voor deze items op WDS AP?Straalserver-tijdmeevallerTime Key Integrity Protocol (TKIP) berichtintegriteitscontrole (MIC) mislukkingstijdClientwachttijdEAP of MAC-verificatieEAP-uitzending voor client (optioneel)Antwoord:** Aanbevolen wordt om de configuratie met standaardinstellingen voor deze speciale instellingen te bewaren, en deze alleen te gebruiken wanneer er een probleem is met de timing.Dit zijn de aanbevolen instellingen voor de WDS-applicatie:Uitschakelen

straal-server-out. Dit is het aantal seconden dat een AP wacht op een antwoord op een RADIUS-verzoek voordat het de aanvraag doorstuurt. De standaardinstelling is 5 seconden.Uitschakelen **straal-server-tijdstip**. De RADIUS wordt door extra verzoeken voor de duur van minuten overgeslagen, tenzij alle servers zijn gemarkeerd.De TKIP MIC van de Holdoff Tijd wordt standaard tot 60 seconden ingeschakeld. Als u de wachttijd instelt, kunt u het interval in seconden invoeren. Als AP twee MIC mislukkingen binnen 60 seconden ontdekt, blokkeert het alle TKIP cliënten op die interface voor de hier gespecificeerde lange periode van de heiligheid.De clientadaptertijd moet standaard worden uitgeschakeld. Als u Holdoff toelaat, voer het aantal seconden in dat AP na een authenticatiefout zou moeten wachten voordat een volgende authenticatieaanvraag verwerkt wordt.EAP of MAC-verificatie Interval is standaard uitgeschakeld. Als u herauthenticatie toelaat, kunt u het interval specificeren of het interval aanvaarden dat door de authenticatieserver gegeven wordt. Als u kiest om het interval te specificeren, voer het interval in seconden in dat AP wacht voordat het een geauthentiseerde client afdwingt om te reauthentiseren.EAP-uitzending voor client (optioneel) is standaard 120 seconden. Geef op hoeveel tijd de AP moet wachten tot draadloze klanten reageren op MAP-verificatieverzoeken.

- **Vraag: Wat de TKIP-wachttijd betreft, las ik dat deze op 100 ms en niet op 60 seconden moet worden ingesteld. Ik neem aan dat het is ingesteld op één seconde van de browser omdat dat het laagste aantal is dat je kunt selecteren?Antwoord:** Er is geen specifieke aanbeveling om de termijn op 100 ms te stellen, tenzij er sprake is van een mislukking, waarbij de enige oplossing is deze tijd te verhogen. Eén seconde is de laagste instelling.
- **Vraag: Helpen deze twee opdrachten op enige manier om klanten te controleren en zijn ze nodig op de WDS of de infrastructuur AP?attribuut 6 on-for-login-authattribuut 6-steunbalkAntwoord:** Deze opdrachten helpen het verificatieproces niet en zijn niet nodig op de WDS of de AP.
- **Vraag: Op de infrastructuur AP, veronderstel ik dat geen van de van de Server Manager en de Algemene instellingen van de Eigenschappen nodig zijn omdat AP informatie van WDS ontvangt. Zijn één van deze specifieke opdrachten nodig voor de infrastructuur AP?attribuut 6 on-for-login-authattribuut 6-steunbalkStraalserver-tijdmeevallerAntwoord:** Er hoeft geen Server Manager en Global Properties te hebben voor de infrastructuur APs. De WDS zorgt voor die taak en de volgende instellingen zijn niet nodig:**attribuut 6 on-for-login-authattribuut 6-steunbalkStraalserver-tijdmeevaller**De **eigenschap Straal-Server 32 omvat-in-toegang-req formaat %h** instelling blijft standaard en is vereist.

AP is een Layer 2 apparaat. Daarom ondersteunt AP Layer 3 mobiliteit niet wanneer AP wordt gevormd om als WDS apparaat te handelen. U kunt Layer 3 mobiliteit alleen bereiken wanneer u WLSM als het WDS-apparaat configureren. Raadpleeg het gedeelte *Layer 3 Mobility Architecture* van Cisco Catalyst 6500 Series draadloze LAN-servicesmodule: Witboek voor meer informatie.

Daarom, wanneer u AP als apparaat WDS vormt, gebruik niet de **mobiliteit netwerk-id** opdracht. Deze opdracht is van toepassing op Layer 3 mobiliteit en u moet een WLSM hebben als uw WDS-apparaat om Layer 3 mobiliteit correct te kunnen configureren. Als u de opdracht **mobiliteitsnetwerk-id** niet correct gebruikt, kunt u een aantal van deze symptomen zien:

- Draadloze klanten kunnen niet met AP associëren.
- Draadloze klanten kunnen aan AP associëren, maar ontvangen geen IP adres van de server van DHCP.
- Een draadloze telefoon is niet echt bevonden wanneer u een stem via WLAN-implementatie hebt.

- Econforme authenticatie gebeurt niet. Met de **netwerk-id van het mobiliteitsnetwerk**, probeert AP een Generic Routing Encapsulation (GRE)-tunnel te bouwen om EAP-pakketten door te sturen. Als er geen tunnel is ingericht gaan de pakketten nergens heen.
- AP gevormd als een WDS apparaat functioneert niet zoals verwacht, en de configuratie van WDS werkt niet.**Opmerking:** u kunt Cisco Aironet 1300 AP/Bridge niet als een WDS-master configureren. De 1300 AP/Bridge ondersteunt deze functie niet. AP/Bridge 1300 kan aan een WDS-netwerk deelnemen als een infrastructuurapparaat waarin een andere AP of WLSM als WDS-master wordt geconfigureerd.

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 dot11 a authenticator all** — toont de verschillende onderhandelingen die een cliënt doorvoert als de cliënt associeert en authenticeert door het 802.1x of EAP proces. Dit debug werd geïntroduceerd in Cisco IOS-softwarerelease 12.2(15)JA. Deze opdracht vervalt **debug dot11 a dot1x allemaal** in dat en laat releases.
- **debug a authenticatie**-toont het authenticatieproces vanuit een generisch AAA-perspectief.
- **debug WCCP-ap** — Geeft de betrokken WLCCP-onderhandelingen weer omdat een AP zich bij een WDS voegt.
- **debug** van **het TCP-pakket**: geeft de gedetailleerde informatie over WLCCP-onderhandelingen weer.
- **debug van WinCp leap-client**: hier worden de gegevens weergegeven naarmate een infrastructuurapparaat zich bij een WDS aansluit.

Gerelateerde informatie

- WDS configureren, snel beveiligde roaming en radiobeheer
- Catalyst 6500 Series configuratie van draadloze LAN-servicesmodule
- Cipuites en EFN configureren
- Verificatietypen configureren
- Draadloze LAN-ondersteuningspagina's
- Technische ondersteuning en documentatie – Cisco Systems