Cisco Secure Services-client met EAP-FAST-verificatie

Inhoud

Inleiding

Dit document beschrijft hoe u de Cisco Secure Services Client (CSSC) kunt configureren met de draadloze LAN-controllers, Microsoft Windows 2000®-software en Cisco Secure Access Control Server (ACS) 4.0 via EAP-FAST. Dit document introduceert de EAP-FAST-architectuur en biedt voorbeelden van implementatie en configuratie. CSSC is de client software component die de communicatie van gebruikersreferenties aan de infrastructuur biedt om een gebruiker aan het netwerk te authentiseren en een juiste toegang toe te wijzen.

Dit zijn een aantal van de voordelen van de CSSC-oplossing die in dit document worden geschetst:

- Verificatie van elke gebruiker (of apparaat) voordat u toegang krijgt tot de WLAN/LAN met verlengbare verificatieprotocol (EAP)
- End-to-end WLAN security oplossing met server, authenticator en clientcomponenten
- Gemeenschappelijke oplossing voor bekabelde en draadloze authenticatie
- Dynamisch, per gebruiker coderingstoetsen afgeleid in het authenticatieproces
- Niet vereist voor openbare sleutelinfrastructuur (PKI) of certificaten (certificatie facultatief)
- Toewijzing van toegangsbeleid en/of MAP met NAC-ondersteuning

Opmerking: Raadpleeg de Cisco SAFE Wireless Blueprint voor informatie over de implementatie van veilige draadloze verbindingen.

Het 802.1x-verificatiekader is geïntegreerd in de 802.11i-standaard (draadloze LAN-beveiliging) om op laag 2 gebaseerde verificatie-, autorisatie- en accounting functies in een 802.11 draadloos LAN-netwerk mogelijk te maken. Vandaag de dag zijn er verschillende EAP protocollen beschikbaar voor plaatsing in zowel bekabelde als draadloze netwerken. Vaak gebruikte EAP-protocollen omvatten LEAP, PEAP en EAP-TLS. Naast deze protocollen heeft Cisco EAP Flexibele Verificatie door middel van Beveiligd Tunnel (EAP-FAST) gedefinieerd en geïmplementeerd als een op standaarden gebaseerd EAP-protocol dat beschikbaar is voor implementatie in zowel bekabelde als draadloze LAN-netwerken. De specificatie van het EAP-FAST-protocol is voor het publiek beschikbaar op de IETF-website .

Net als bij sommige andere EAP-protocollen is EAP-FAST een client-server security architectuur die EAP-transacties binnen een TLS-tunnel versleutelt. Hoewel het op dit punt vergelijkbaar is met PEAP- of EAP-TTLS, verschilt het in die zin dat de instelling van de MAP-FAST-tunnel gebaseerd is op sterke gedeelde geheime sleutels die uniek zijn voor elke gebruiker in vergelijking met PEAP/EAP-TTLS (die een server X.509-certificaat gebruiken om de authenticatiesessie te beschermen). Deze gedeelde geheime toetsen worden Protected Access Credentials (PAC's) genoemd en kunnen automatisch (Automatic of Inband Provisioning) of handmatig (Handmatig of Out-of-band Provisioning) worden verdeeld naar clientapparaten. Omdat handschokken gebaseerd op gedeelde geheimen efficiënter zijn dan handschokken gebaseerd op een PKI-infrastructuur, is EAP-FAST het snelste en minder processor-intensief MAP-type van degenen die beschermde authenticatie-uitwisselingen aanbieden. EAP-FAST is ook ontworpen om eenvoudig te kunnen worden ingezet, aangezien het geen certificaat vereist op de draadloze LAN-client of op de RADIUS-infrastructuur, maar wel een ingebouwd voorzieningsmechanisme bevat.

Dit zijn enkele van de belangrijkste mogelijkheden van het EAP-FAST-protocol:

- Enkelvoudig aanmelding (SSO) met Windows gebruikersnaam/wachtwoord
- Ondersteuning van de uitvoering van inlogscripts
- Ondersteuning van Wi-Fi Protected Access (WAP) zonder derden (alleen Windows 2000 en XP)
- Eenvoudige implementatie zonder noodzaak voor PKI-infrastructuur
- Windows Wachtwoordverloop (d.w.z. ondersteuning voor wachtwoordverloopdatums op de server)
- Integratie met Cisco Trust Agent voor netwerktoegangscontrole met juiste clientsoftware

Voorwaarden

Vereisten

Er wordt aangenomen dat de installateur kennis heeft van de basisinstallatie van Windows 2003

en de installatie van Cisco WLC, aangezien dit document alleen de specifieke configuraties bevat om de tests te vergemakkelijken.

Raadpleeg de Snelle startgids voor informatie over de installatie en de configuratie van de Cisco 4400 Series controllers: Cisco 4400 Series draadloze LAN-controllers. Raadpleeg de Snelle startgids voor informatie over de installatie en de configuratie van de Cisco 2000 Series controllers: Cisco 2000 Series draadloze LAN-controllers.

Voordat u begint, installeert u de Microsoft Windows Server 2000 met de nieuwste servicepakket-software. Installeer de controllers en lichtgewicht access points (LAP's) en zorg ervoor dat de laatste softwareupdates worden geconfigureerd.

Gebruikte componenten

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

- Cisco 2006 of 4400 Series controller die 4.0.15.5 draait
- Cisco 1242 WAPP AP
- Windows 2000 met actieve map
- Cisco Catalyst 3750G Switch
- Windows XP met CB21AG adapterkaart en Cisco Secure Services client versie 4.0

Conventies

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

Ontwerpparameters

Databaseverslag

Wanneer u een WLAN-netwerk implementeert en naar een verificatieprotocol zoekt, is het meestal wenselijk een huidige database voor gebruikers/machines-verificatie te gebruiken. Typische databases die kunnen worden gebruikt zijn Windows Active Directory, LDAP of een ONE Time Password (OTP) database (d.w.z. RSA of SecureID). Al deze databases zijn compatibel met het EAP-FAST-protocol, maar als je de implementatie wil realiseren, zijn er een aantal compatibiliteitseisen die in overweging moeten worden genomen. De eerste implementatie van een PAC-bestand voor klanten wordt gerealiseerd door middel van anonieme automatische provisioning, geauthentiseerde provisioning (via het huidige client-X.509-certificaat) of handmatige provisioning. In dit document worden anonieme automatische provisioning en handmatige provisioning overwogen.

Automatische PAC-voorziening gebruikt Veriated Diffie-Hellman Key Agreement Protocol (ADHP) om een beveiligde tunnel op te zetten. De beveiligde tunnel kan anoniem of via een server - authenticatiemechanisme worden opgezet. Binnen de ingestelde tunnelverbinding wordt MS-CHAPv2 gebruikt om de client voor de authenticatie te verklaren en, bij succesvolle authenticatie, om het PAC-bestand aan de client te distribueren. Nadat de PAC met succes is bevoorraad, kan het PAC-bestand worden gebruikt om een nieuwe EAP-FAST-authenticatiesessie te initiëren om een veilige netwerktoegang te verkrijgen.

Automatische PAC-voorziening is relevant voor de in gebruik zijnde database omdat, aangezien het automatische provisioningmechanisme op MSCHAPv2 berust, de database die wordt gebruikt om gebruikers voor authenticatie te controleren compatibel moet zijn met deze wachtwoordindeling. Als u EAP-FAST gebruikt met een gegevensbank die MSCHAPv2-indeling niet ondersteunt (zoals OTP, Novell of LDAP), moet u een ander mechanisme (dat wil zeggen handmatige provisioning of geauthentiseerde provisioning) gebruiken om PAC-bestanden van gebruikers in te zetten. Dit document geeft een voorbeeld van automatische provisioning met een Windows-gebruikersdatabase.

Versleuteling

Voor EAP-FAST-verificatie is het gebruik van een specifiek WLAN-coderingstype niet vereist. Het WLAN-encryptie type dat moet worden gebruikt, wordt bepaald door de mogelijkheden van de client-NIC-kaart. Aanbevolen wordt om WAP2 (AES-CCM) of de encryptie van de SLP (TKIP) te gebruiken, afhankelijk van de NIC kaartmogelijkheden in de specifieke plaatsing. Merk op dat de oplossing van Cisco WLAN het coëxisteren van zowel WAP2 als de clientapparaten van WAP op een gemeenschappelijke SSID toestaat.

Als de clientapparaten geen WAP2 of WAP ondersteunen, is het mogelijk om 802.1X-verificatie in te voeren met de dynamische EFN-toetsen, maar vanwege de bekende explosies tegen de sleutels van EFG wordt dit WLAN-encryptie mechanisme niet aanbevolen. Als het vereist is om de cliënten van alleen EFL te steunen, wordt het aanbevolen om een sessie-timeout interval te gebruiken, wat vereist dat de cliënten een nieuwe sleutel van EFG afleiden op een frequente tussenpoos. Dertig minuten is het aanbevolen sessieinterval voor normale WLAN-gegevenssnelheden.

Eenmalige aanmelding en crediteuren machine

Eenvoudig aanmelding verwijst naar de mogelijkheid van één enkel teken van de gebruiker of intrede van de authenticiteitsreferenties om toegang te krijgen tot meerdere toepassingen of meerdere apparaten. Voor de toepassing van dit document verwijst Single Sign-On naar het gebruik van de geloofsbrieven die worden gebruikt om aan te loggen op een PC voor authenticatie aan de WLAN.

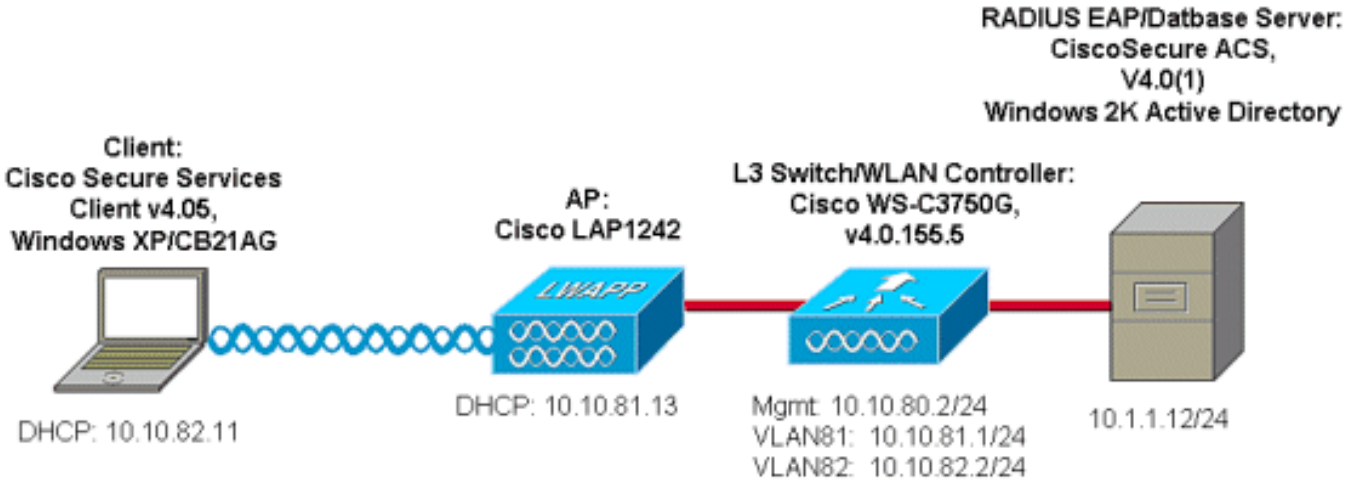
Met de Cisco Secure Services Client is het mogelijk de aanmeldingsgegevens van een gebruiker te gebruiken om ook te authentiseren voor het WLAN-netwerk. Als het nodig is om een pc voor het netwerk te authenticeren voordat de gebruiker zich bij de PC aanmeldt, moet de gebruiker de opgeslagen gebruikersreferenties of de aanmeldingsgegevens gebruiken die gekoppeld zijn aan een machineprofiel. Een van deze methoden is handig in gevallen waar het is gewenst om een aanmelding script of een map te starten wanneer de PC opstart, in tegenstelling tot wanneer een gebruiker zich inlogt.

Netwerkdiagram

Dit is het netwerkdiagram dat in dit document wordt gebruikt. In dit netwerk worden vier subnetten gebruikt. Merk op dat het niet nodig is om deze apparaten in verschillende netwerken te segmenteren, maar dit biedt de meeste flexibiliteit voor integratie met bestaande netwerken. De Catalyst 3750G geïntegreerde draadloze LAN-controller biedt Power over Ethernet (PoE)-switches, L3-switching en WLAN-controller op een gemeenschappelijk chassis.

1. Netwerk 10.1.1.0 is het servernetwerk waar ACS zich bevindt.

2. Network 10.10.80.0 is het beheernetwerk dat door de WLAN-controller wordt gebruikt.
3. Netwerk 10.10.81.0 is het netwerk waar APs wonen.
4. Network 10.10.82.0 wordt gebruikt voor de WLAN-clients.



Het configureren van de toegangscontroleserver (ACS)

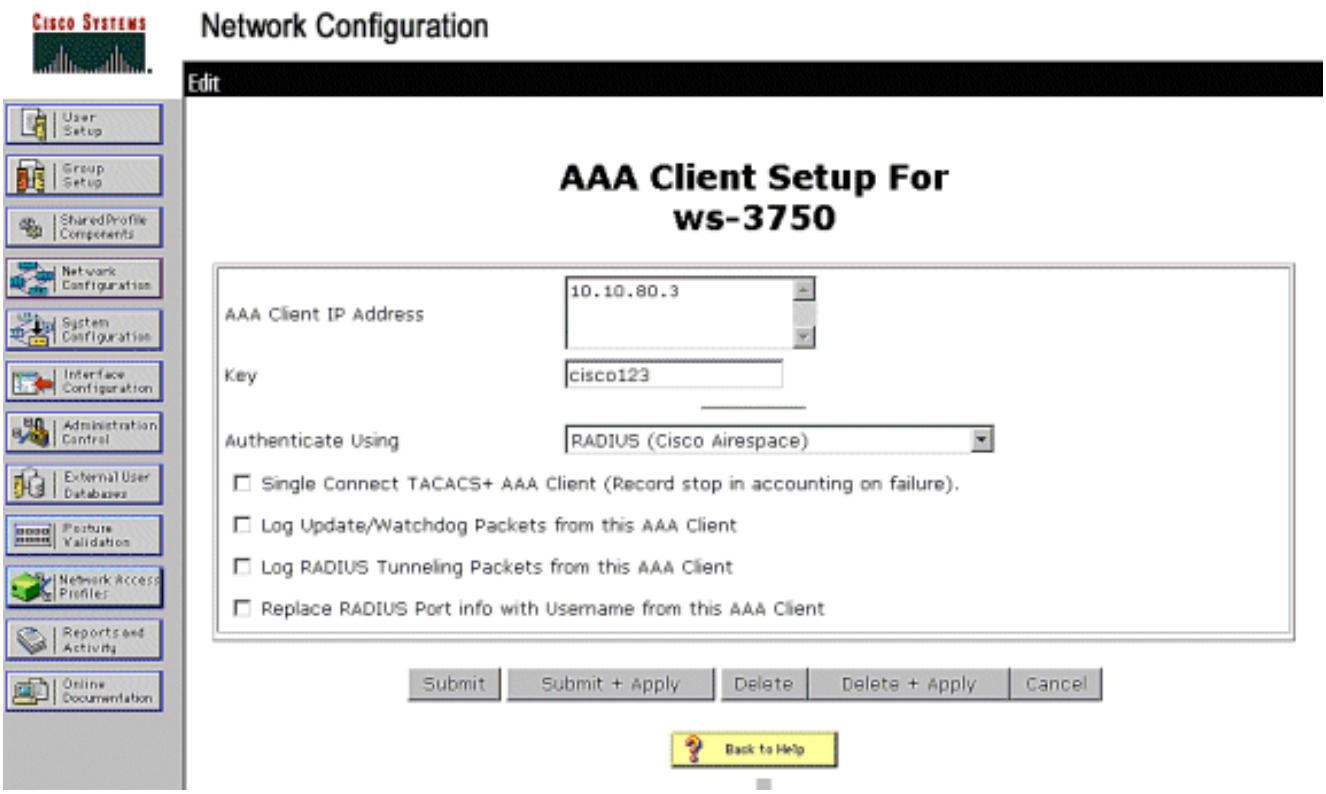
Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

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

Access point als AAA-client (NAS) toevoegen in ACS

In dit deel wordt beschreven hoe u ACS voor EAP-FAST kunt configureren met in-band PAC-voorziening met Windows Active Directory als de externe database.

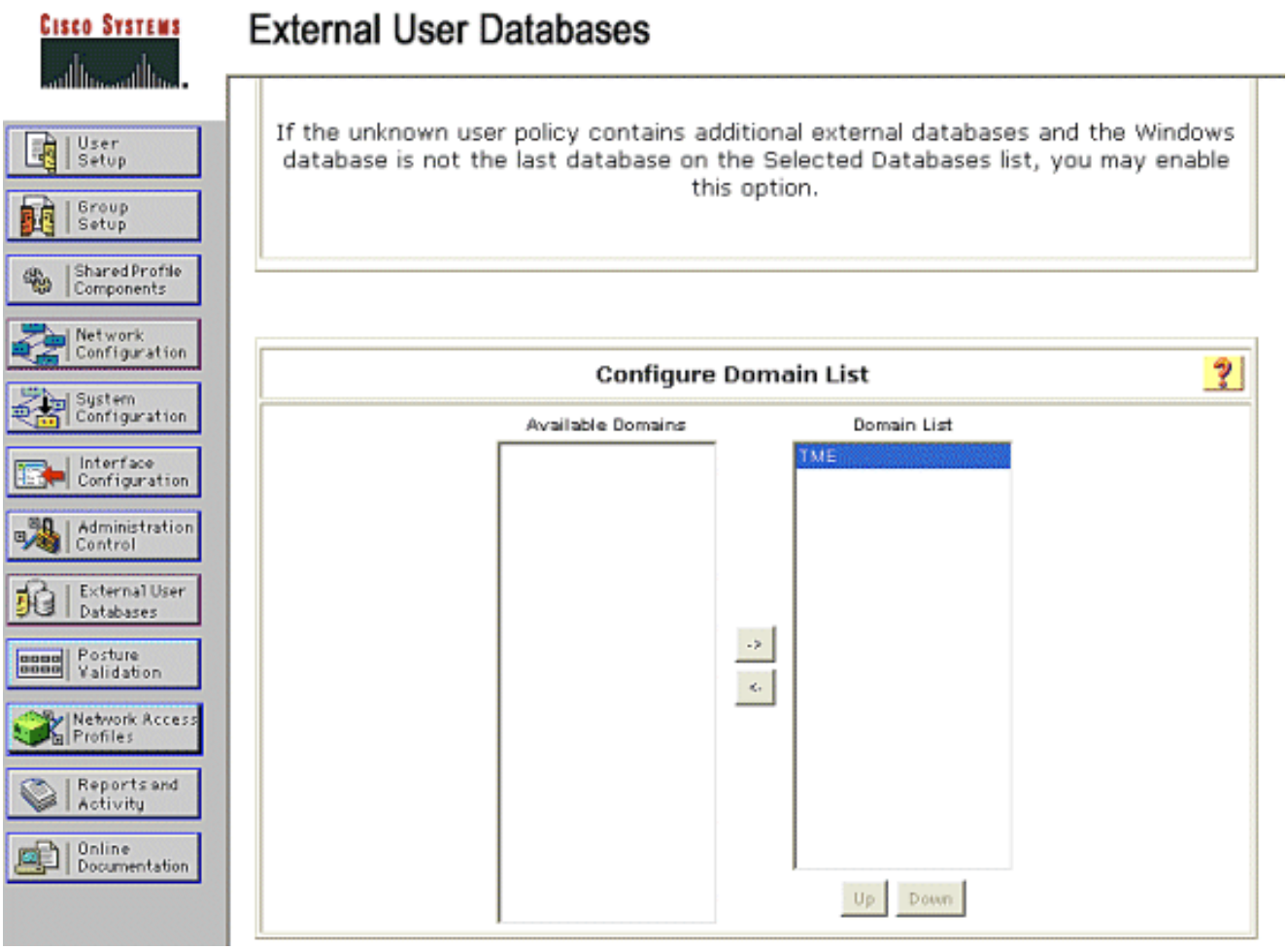
1. Log in op **ACS > Netwerkconfiguratie** en klik op **Ingang toevoegen**.
2. Vul de WLAN-controlenaam, IP-adres, gedeelde geheime sleutel en onder Verificeren met behulp van RADIUS in (Cisco Airespace), die ook RADIUS IETF-eigenschappen bevat.**Opmerking:** Als de Network Devices Group (NDG) is ingeschakeld, kiest u eerst de juiste NDG en voegt u de WLAN-controller toe. Raadpleeg de ACS-configuratiegids voor meer informatie over de NDG.
3. Klik op **Inzenden+ opnieuw starten**.



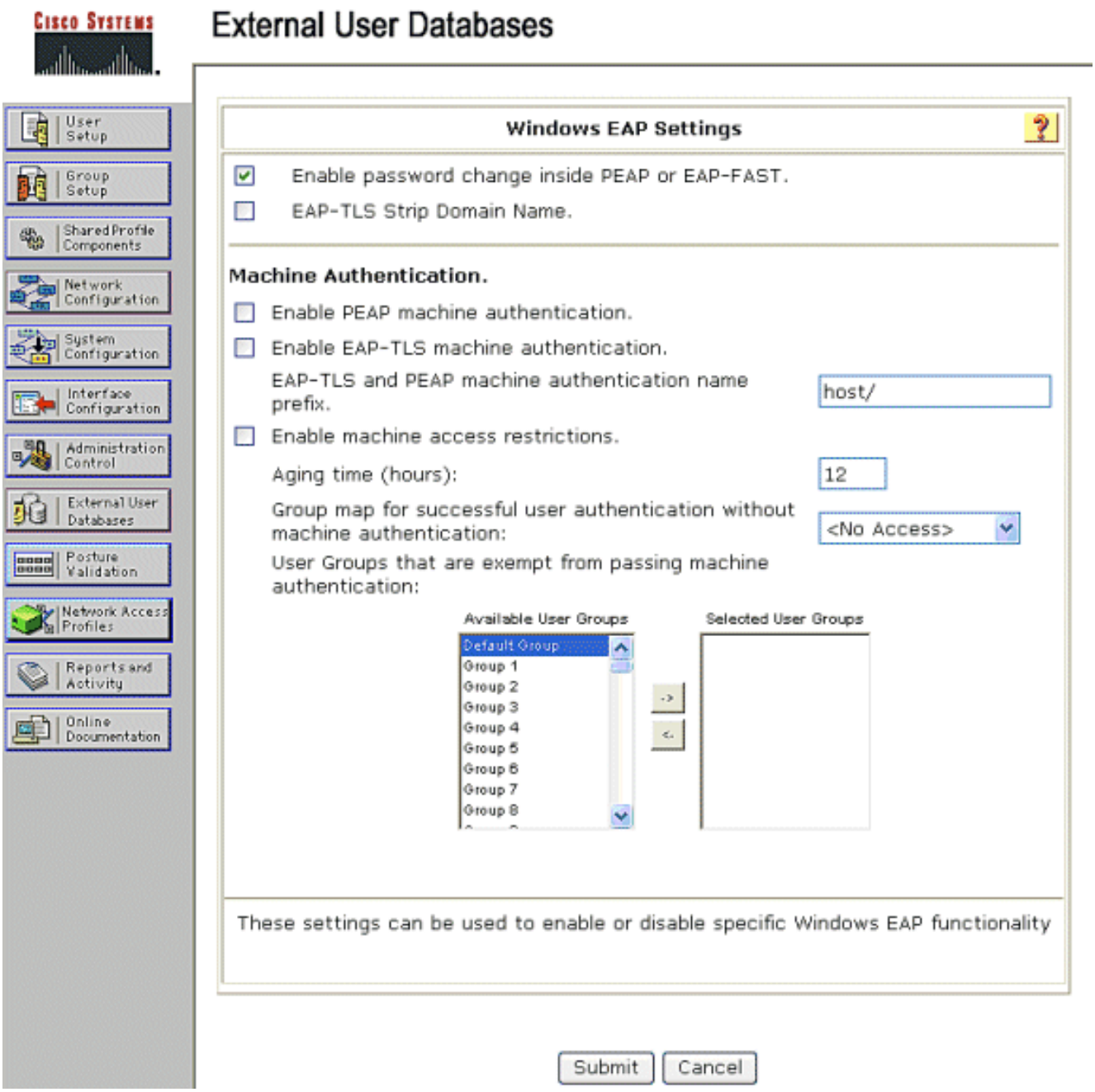
ACS configureren om de externe database op te vragen

In deze sectie wordt beschreven hoe de ACS moet worden ingesteld om de externe database af te vragen.

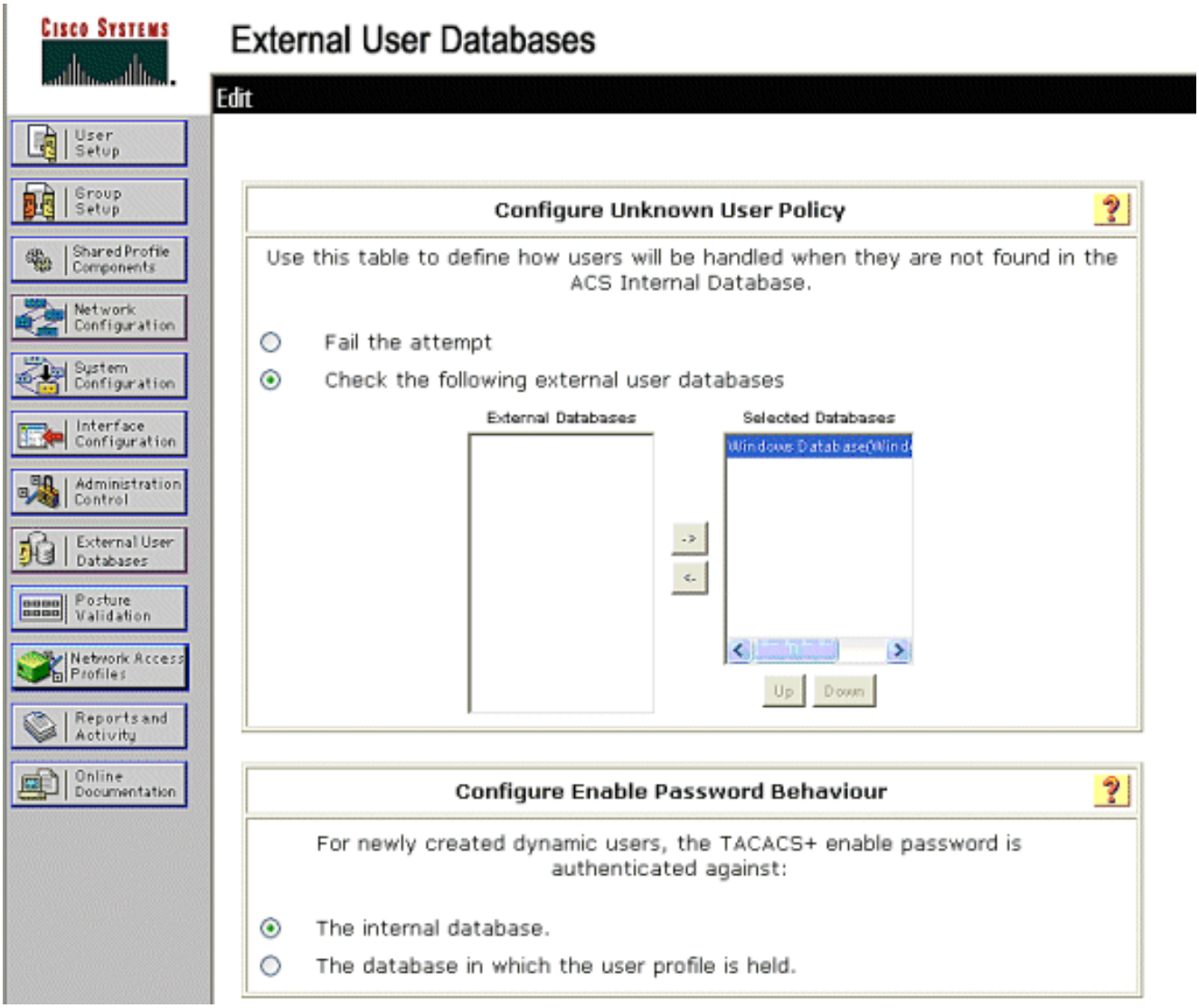
1. Klik op **Externe gebruikersdatabase > Databaseverdeling > Windows database > Configureren**.
2. Onder Domain List configureren **verplaatst u** de **domeinen** van Beschikbare velden naar Domain List.**Opmerking:** De server die de ACS beheert moet kennis van deze domeinen hebben zodat de ACS-toepassing deze domeinen kan detecteren en gebruiken voor verificatiedoeleinden.



3. Stel onder de Windows EAP-instellingen de optie in om de wachtwoordwijziging binnen de PEAP- of EAP-FAST-sessie toe te staan. Raadpleeg de Configuration Guide voor Cisco Secure ACS 4.1 voor meer informatie over de vergrijzing van EAP-FAST en Windows-wachtwoord.
4. Klik op **Inzenden**.**Opmerking:** U kunt de optie Dialin Permission ook inschakelen voor EAP-FAST onder de configuratie van Windows User Database om de externe Windows-database in staat te stellen toegangstoestemming te controleren. De MS-CHAP-instellingen voor wachtwoordwijziging op de Windows-pagina voor de configuratie van de database zijn alleen van toepassing op niet-EAP MS-CHAP-verificatie. Om een wachtwoordwijziging in combinatie met EAP-FAST mogelijk te maken, is het nodig om een wachtwoordwijziging onder de Windows EAP-instellingen mogelijk te
maken.



5. Klik op **Externe gebruikersdatabase > Onbekend gebruikersbeleid** en kies de radioknop **Controleer de volgende externe gebruikersdatabases**.
6. Verplaats de Windows-database van **externe databases** naar **geselecteerde databases**.
7. Klik op **Inzenden**.**Opmerking:** Vanaf dit punt controleert de ACS de Windows DB. Als de gebruiker niet in de lokale ACS-database gevonden wordt, plaatst hij de gebruiker in de standaardgroep ACS. Raadpleeg de ACS-documentatie voor meer informatie over de methoden van de Databasegroep.**Opmerking:** Aangezien ACS de Microsoft Active Directory-database vraagt om gebruikersreferenties te controleren, moeten extra instellingen voor toegangsrechten op Windows worden ingesteld. Raadpleeg de installatiehandleiding voor Cisco Secure ACS voor Windows Server voor meer informatie.

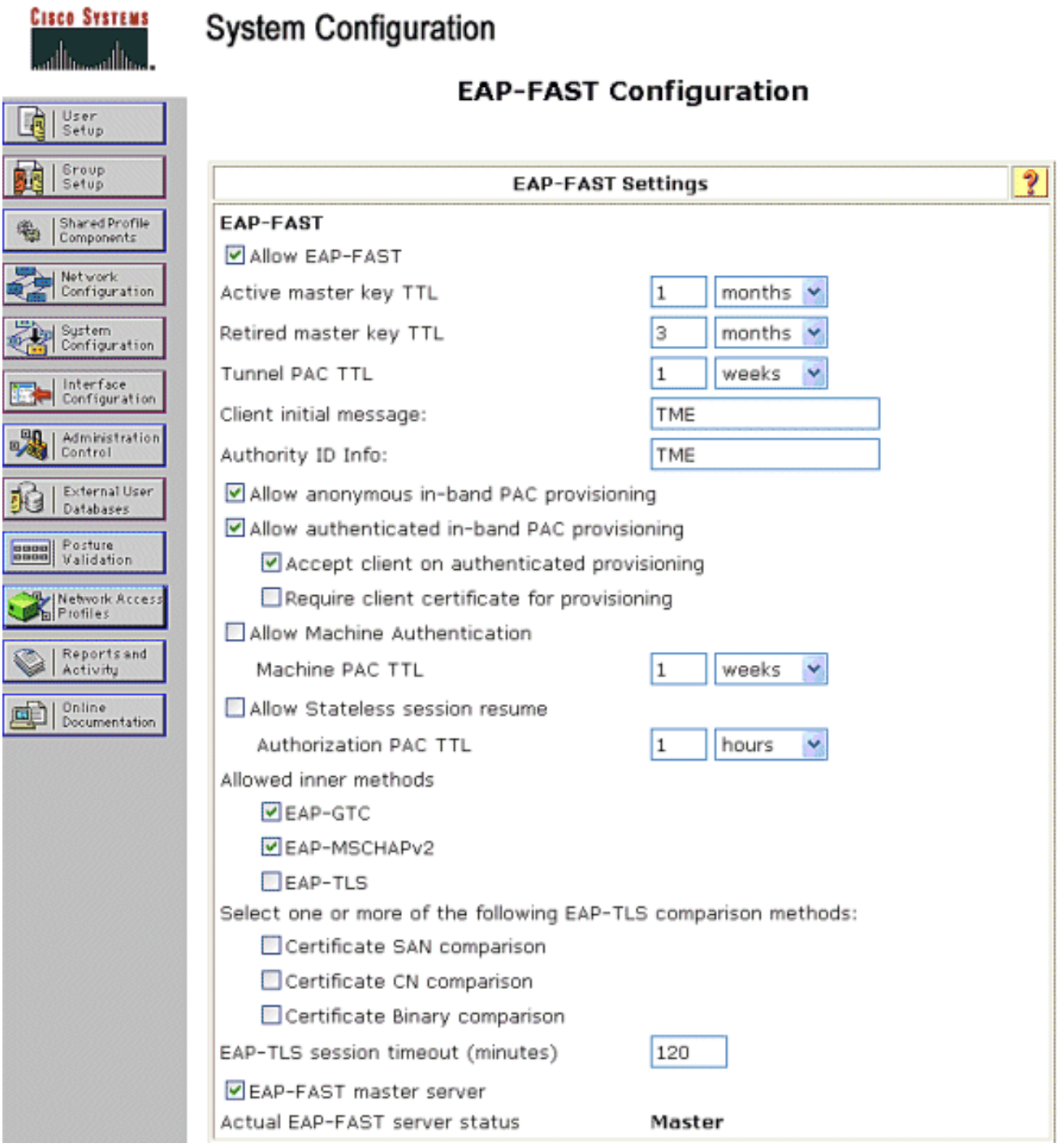


Accessoire-FAST ondersteuning op ACS inschakelen

In dit deel wordt beschreven hoe de MAP-FAST-ondersteuning op de ACS mogelijk moet worden gemaakt.

1. Ga naar **systeemconfiguratie > Global verificatieinstelling > EAP-FAST-configuratie**.
2. Kies **MAP-FAST toestaan**.
3. Configuratie van deze aanbevelingen: Master key TTL/ Revermoeid master key TTL/ PAC TTL. Deze instellingen worden standaard ingesteld in Cisco Secure ACS:Hoofdsleutel TTL:1 maandGepensioneerde sleutel: 3 maandenPAC TTL: 1 week
4. Vul het veld **Informatie over autoriteit in**. Deze tekst is opgenomen in een aantal EAP-FAST-clientsoftware waarin de PAC-autoriteit als verantwoordelijke is geselecteerd.**Opmerking:** De Cisco Secure Services Client gebruikt deze beschrijvende tekst niet voor de PAC-autoriteit.
5. Kies het veld **Toegestaan in-band PAC-**provisioning. Dit veld maakt automatische PAC-provisioning mogelijk voor goed-enabled EAP-FAST-clients. Bijvoorbeeld, auto-provisioning wordt gebruikt.
6. Kies **Toegestaan binnenmethoden**: EAP-GTC en EAP-MSCHAP2. Dit maakt het mogelijk dat zowel de EAP-FAST v1- als de EAP-FAST v1a-klanten actief zijn. (Cisco-client voor beveiligde services ondersteunt EAP-FAST v1a.) Als het niet nodig is om de cliënten van EAP-FAST v1 te ondersteunen, is het alleen nodig om EAP-MSCHAPv2 als innerlijke methode mogelijk te maken.

7. Kies het selectieteken **EAP-FAST Master Server** om deze EAP-FAST server als meester in te schakelen. Dit maakt het mogelijk dat andere ACS-servers deze server als de enige PAC-autoriteit gebruiken om te voorkomen dat er unieke sleutels voor elk ACS in een netwerk beschikbaar zijn. Raadpleeg de ACS-configuratiegids voor meer informatie.
8. Klik op **Inzenden+Opnieuw beginnen**.



Cisco WLAN-controller

Voor de doeleinden van deze implementatiegids wordt een Cisco WS 3750G geïntegreerde draadloze LAN-controller (WLC) gebruikt met Cisco AP1240 lichtgewicht AP's (LAP) om de WLAN-infrastructuur voor CSSC-tests te leveren. De configuratie is van toepassing op elke Cisco WLAN-controller. De gebruikte softwareversie is 4.0.15.5.

De draadloze LAN-controller configureren

Basisbediening en registratie van LAP aan de controller

Gebruik de wizard opstartconfiguratie in de opdrachtregel-interface (CLI) om de WLC te configureren voor een eenvoudige bediening. U kunt ook de GUI gebruiken om de WLC te configureren. Dit document legt de configuratie op de WLC uit met de wizard opstarten in de CLI.

Nadat de WLC voor het eerst start, gaat het in de opstartconfiguratie wizard. Gebruik de configuratiewizard om basisinstellingen te configureren. U hebt toegang tot de wizard via de CLI of de GUI. Deze uitvoer toont een voorbeeld van de opstartconfiguratiewizard in de CLI:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: ws-3750
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 10.10.80.3
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.80.2
Management Interface VLAN Identifier (0 = untagged):
Management Interface DHCP Server IP Address: 10.10.80.2
AP Manager Interface IP Address: 10.10.80.4
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (172.16.1.1):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Security
Network Name (SSID): Enterprise
Allow Static IP Addresses [YES][no]: yes
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configuration saved!
Resetting system with new configuration.
```

Met deze parameters wordt de WLC ingesteld voor een eenvoudige bediening. In deze voorbeeldconfiguratie gebruikt de WLC **10.10.80.3** als het IP-adres van de beheerinterface en **10.10.80.4** als het IP-adres van de AP-Manager-interface.

Voordat er andere functies op de WLC's kunnen worden ingesteld, moeten de LAP's zich registreren bij de WLC. In dit document wordt ervan uitgegaan dat de LAP bij de WLC is geregistreerd. Raadpleeg het gedeelte Lichtgewicht AP registreren bij de WLCs-sectie van WLAN Controller failover voor lichtgewicht access points Configuration Voorbeeld voor informatie over hoe de lichtgewicht APs bij de WLC registreren. Ter verwijzing naar dit configuratievoorbeeld, wordt AP1240s op een afzonderlijk netwerk (10.10.81.0/24) van de WLAN controller (10.10.80.0/24) ingezet en wordt DHCP-optie 43 gebruikt om de ontdekking van controllers te bieden.

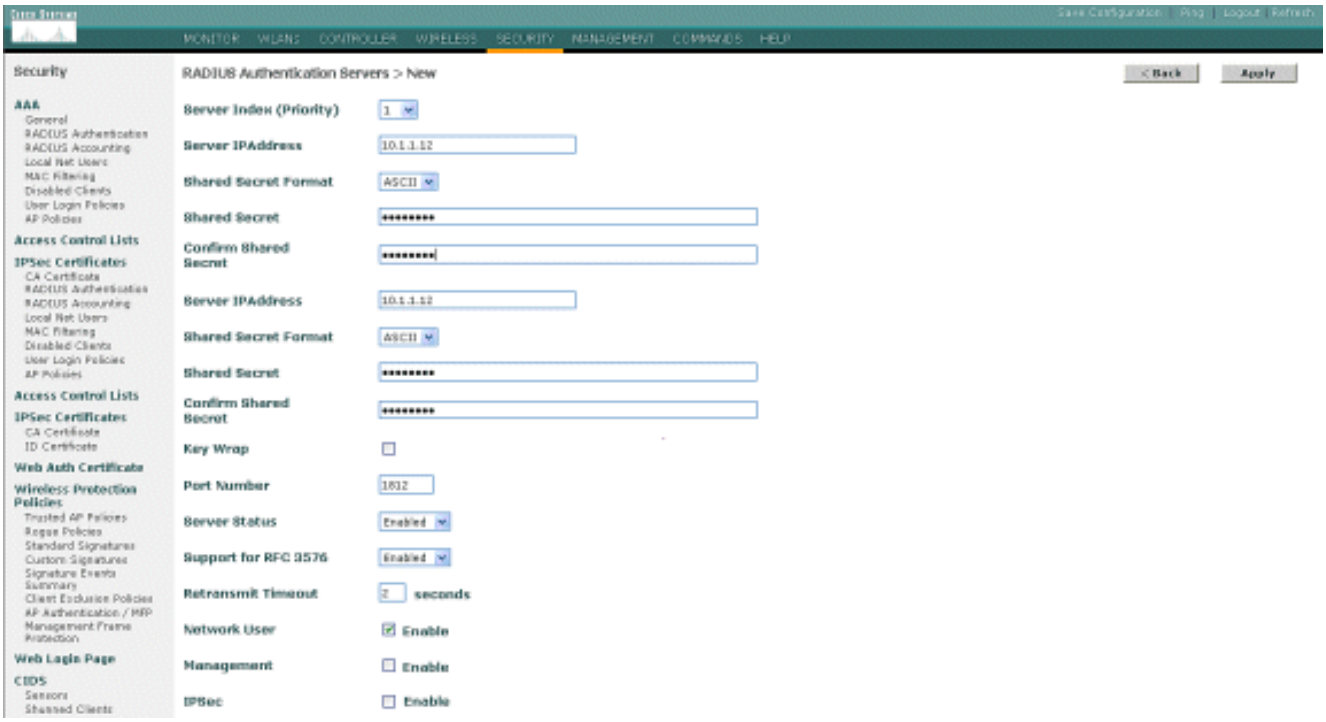
RADIUS-verificatie via Cisco Secure ACS

De WLC moet worden geconfigureerd om de gebruikersreferenties naar de Cisco Secure ACS-server te sturen. De ACS server bevestigt dan de gebruikersgeloofsbrieven (door de gevormd gegevensbestand van Windows) en verleent toegang tot de draadloze cliënten.

Voltooi deze stappen om de WLC voor communicatie naar de ACS-server te configureren:

1. Klik op **Security** en **RADIUS-verificatie** van de controller GUI om de pagina RADIUS-verificatieservers weer te geven. Klik vervolgens op **New** om de ACS-server te definiëren.

2. Defineert de ACS serverparameters in de RADIUS-verificatieservers > Nieuwe pagina. Deze parameters omvatten het ACS IP-adres, gedeeld geheim, poortnummer en serverstatus.**Opmerking:** De poortnummers 1645 of 1812 zijn compatibel met ACS voor RADIUS-verificatie.De de controlevensters Netwerkgebruiker en -beheer bepalen of de op RADIUS gebaseerde verificatie van toepassing is op netwerkgebruikers (bijvoorbeeld WLAN-clients) en -beheer (dat wil zeggen administratieve gebruikers). De voorbeeldconfiguratie gebruikt de Cisco Secure ACS als RADIUS-server met IP-adres 10.1.1.12:



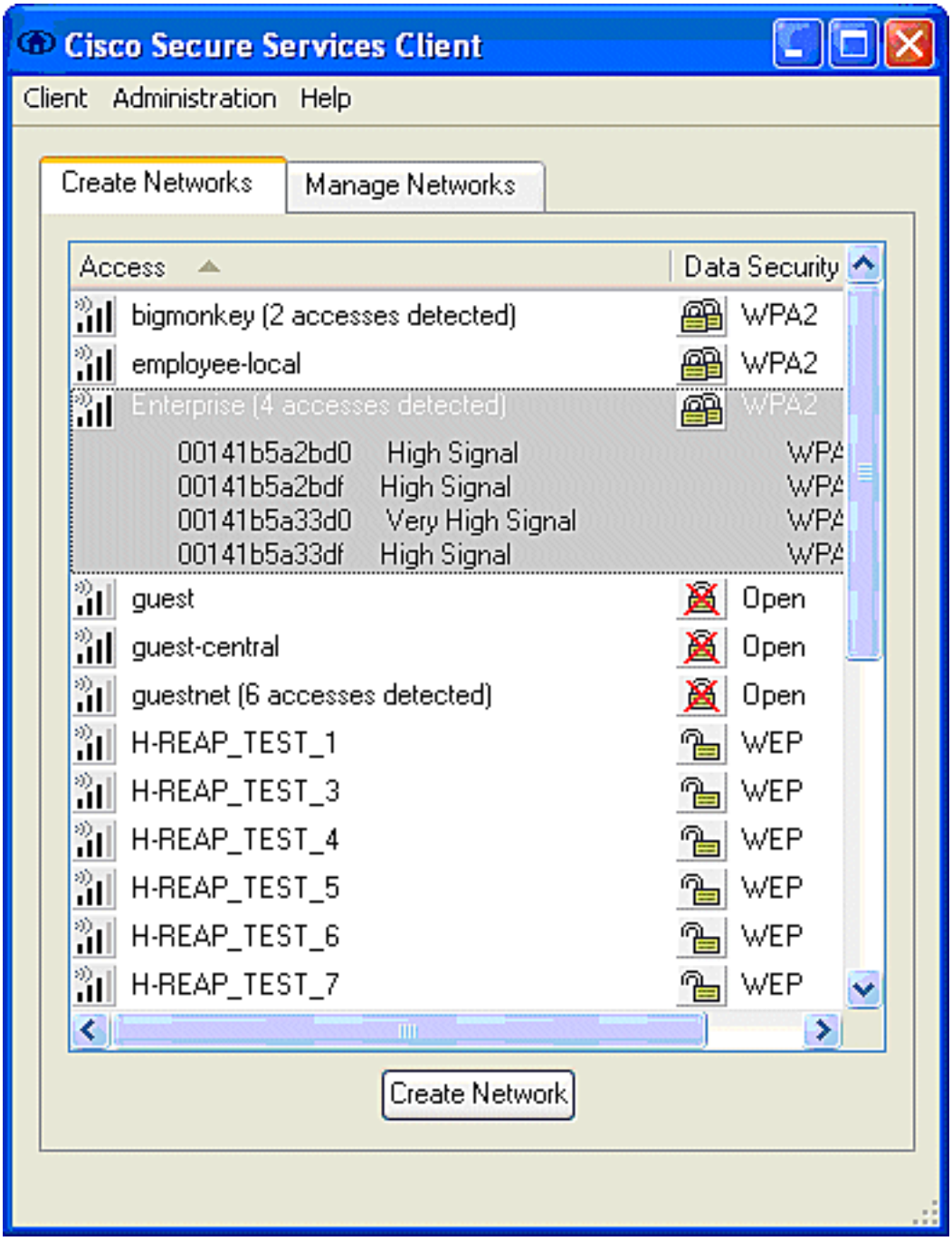
Configuratie van de WLAN-parameters

In dit gedeelte wordt de configuratie van de Cisco Secure Services Client beschreven. In dit voorbeeld wordt CSSC v4.0.5.4783 gebruikt met een Cisco CB21AG clientadapter. Controleer vóór de installatie van de CSSC-software of alleen de stuurprogramma's voor de CB21AG zijn geïnstalleerd, niet het Aironet Desktop Utility (ADU).

Nadat de software is geïnstalleerd en deze als service wordt uitgevoerd, scant hij naar beschikbare netwerken en geeft hij de beschikbare netwerken weer.

Opmerking: CSSC schakelt Windows Nul Config uit.

Opmerking: Alleen SSID's die zijn ingeschakeld voor uitzending zijn zichtbaar.



Opmerking: De WLAN-controller zendt standaard SSID's uit, zodat deze wordt weergegeven in de lijst Create Networks of gescande SSID's. Als u een netwerkprofiel wilt maken, kunt u eenvoudig op **SSID** klikken in de lijst (Enterprise) en in de radioknop **Netwerk maken**.

Als de WLAN-infrastructuur is geconfigureerd met SSID's die zijn uitgeschakeld, moet u handmatig de SSID's toevoegen; Klik op de radioknop **Add** onder Access Devices en voer handmatig de juiste **SSID's** in (bijvoorbeeld Enterprise). Configureer actief probe gedrag voor de client, d.w.z. waar de client actief probeert om de geconfigureerde SSID te bepalen; Specificeer **actief op dit toegangsapparaat** nadat u SSID in het venster Toevoegen toegangsapparaat hebt ingevoerd.

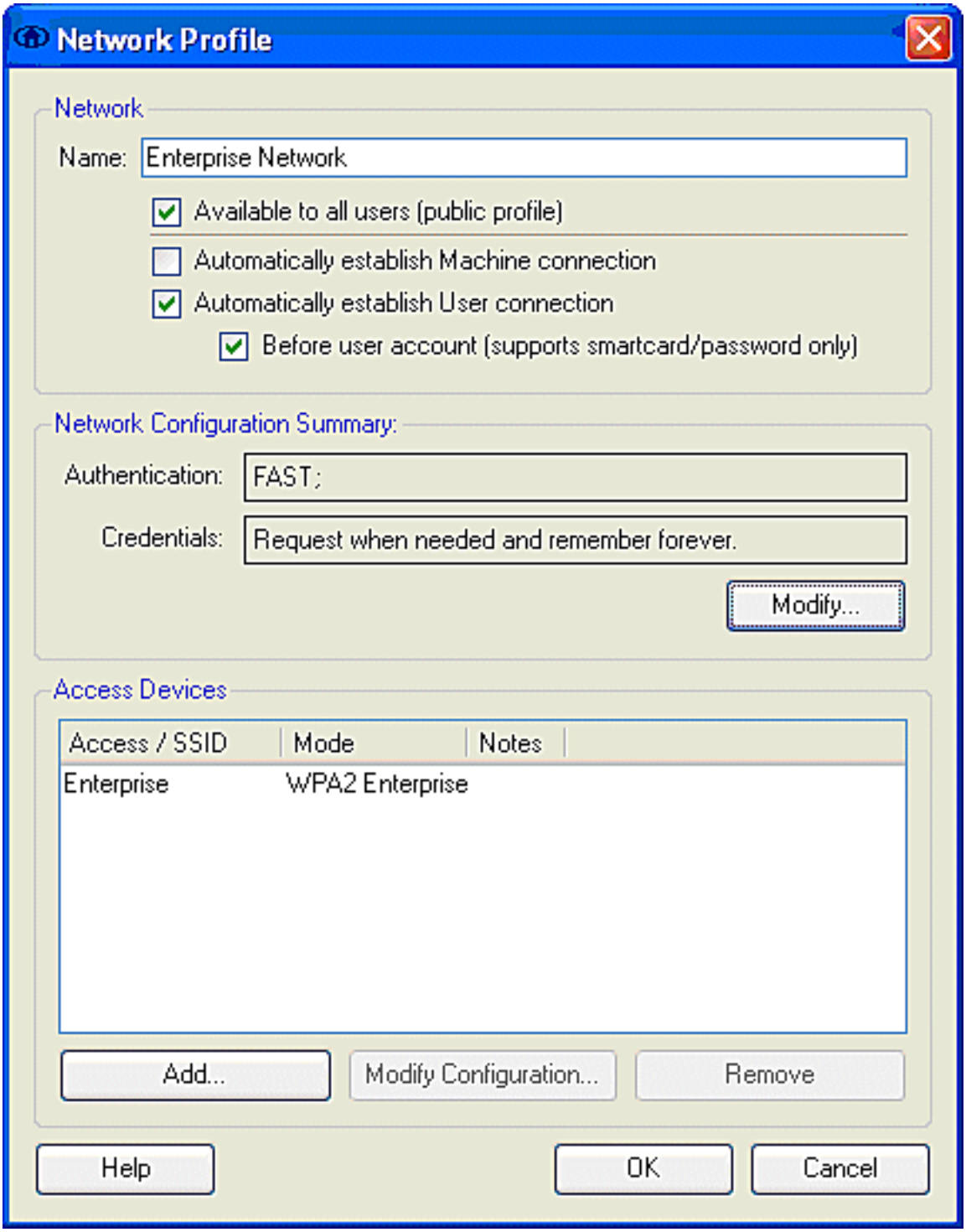
Opmerking: de poortinstellingen staan geen bedrijfsmodi toe (802.1X) indien de MAP-echtheidsinstellingen niet voor het profiel zijn ingesteld.

De radioknop **Create Network** start het venster Network Profile, dat u de geselecteerde (of geconfigureerde) SSID kunt koppelen aan een verificatiemechanisme. Geef een beschrijvende naam voor het profiel toe.

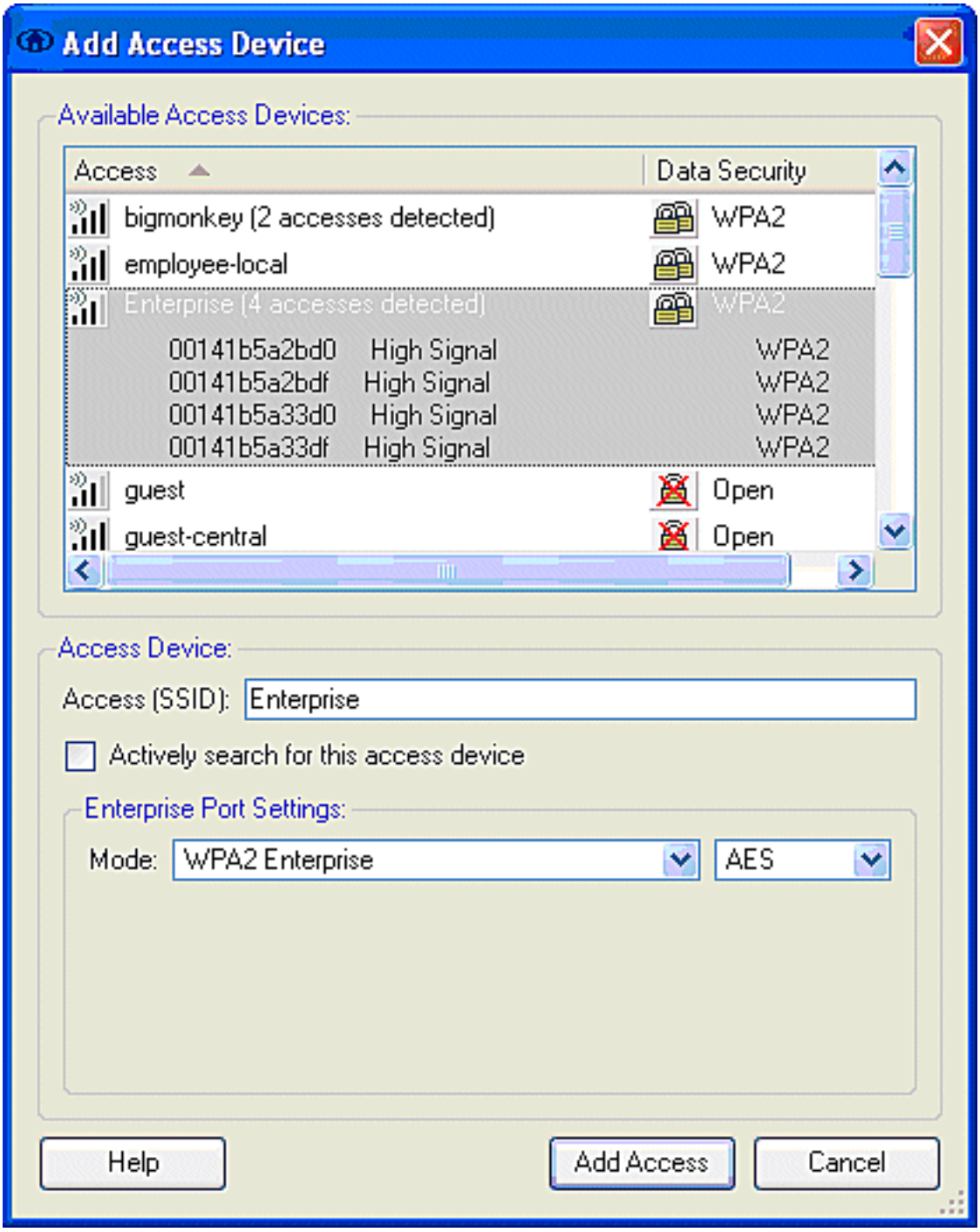
Opmerking: Meerdere WLAN-beveiligingstypen en/of SSID's kunnen bij dit verificatieprofiel worden gekoppeld.

Als u wilt dat de client automatisch verbinding maakt met het netwerk binnen het bereik van RF, kiest u **Automatisch een gebruikersverbinding**. Schakel **de** optie **uit voor alle gebruikers** als het niet wenselijk is dit profiel te gebruiken met andere gebruikersaccounts in de machine. Als **Automatisch** niet geselecteerd is, is het nodig dat de gebruiker het CSSC-venster opent en handmatig de WLAN-verbinding met de **Connect**-radioknop opent.

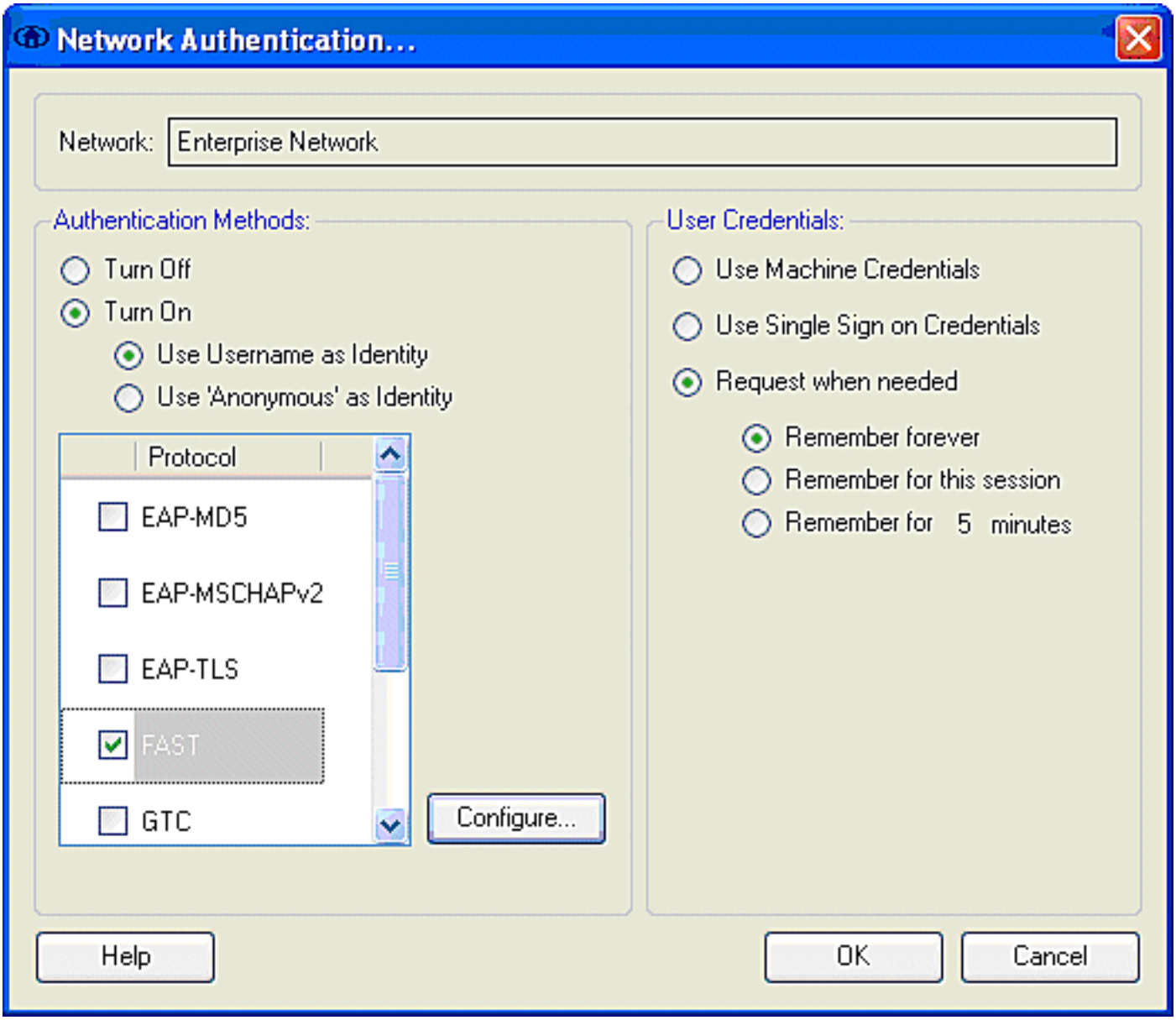
Als het gewenste is om de WLAN-verbinding te openen voordat er een gebruikerslog wordt ingeschakeld, kiest u **Voor een gebruikersaccount**. Dit maakt een eenmalige aanmelding mogelijk met opgeslagen gebruikersreferenties (wachtwoord of certificaat/kaart wanneer u TLS gebruikt binnen EAP-FAST).



Opmerking: Voor WAP/TKIP-handeling met Cisco Aironet 350 Series clientadapter is het nodig om de WAP-handdruk-validatie uit te schakelen omdat er momenteel een oncompatibiliteit is tussen de CSSC-client en 350 stuurprogramma's met betrekking tot de WAP-handshake-validatie. Dit is uitgeschakeld onder **Clientbeveiliging > Geavanceerde instellingen > WAP/WAP2 Handshake Authentication**. De gehandicapte handdruk validatie maakt nog steeds de veiligheidseigenschappen die inherent zijn aan WAP (TKIP per pakket controle en de Controle van de Integriteit van het Bericht) mogelijk, maar schakelt de eerste van de sleutel van WAPverificatie uit.



Klik onder Network Configuration Summary op **Wijzigen** om de instellingen EAP/Credentials te configureren. Specificeer **Inschakelen**, kies **FAST** onder Protocol en kies **'Anonymous' als Identity** (om geen gebruikersnaam te gebruiken in het eerste MAP-verzoek). Het is mogelijk om de **gebruikersnaam als** Identificatiecode te gebruiken als de externe MAP-identiteit, maar veel klanten willen de gebruiker-ID's in het oorspronkelijke, niet-gecodeerde verzoek niet aan de kaak stellen. Specificeer **Gebruik Single Sign on Credentials** om logaanmeldingsgegevens voor netwerkverificatie te gebruiken. Klik op **Configureren** om de MAP-FAST parameters in te stellen.



Onder FAST-instellingen is het mogelijk om **Valideren van servercertificaat** te specificeren, waarmee de klant het EAP-FAST server (ACS) certificaat kan valideren voordat een EAP-FAST-sessie wordt ingesteld. Dit biedt de clientapparaten bescherming tegen verbinding met een onbekende of schurkene EAP-FAST server en onbedoelde indiening van hun verificatiegegevens aan een onbetrouwbare bron. Dit vereist wel dat de ACS-server een certificaat heeft geïnstalleerd en dat de klant ook het certificaat van de correspondent Root Certificate Authority heeft geïnstalleerd. In dit voorbeeld is de validatie van servercertificaten niet ingeschakeld.

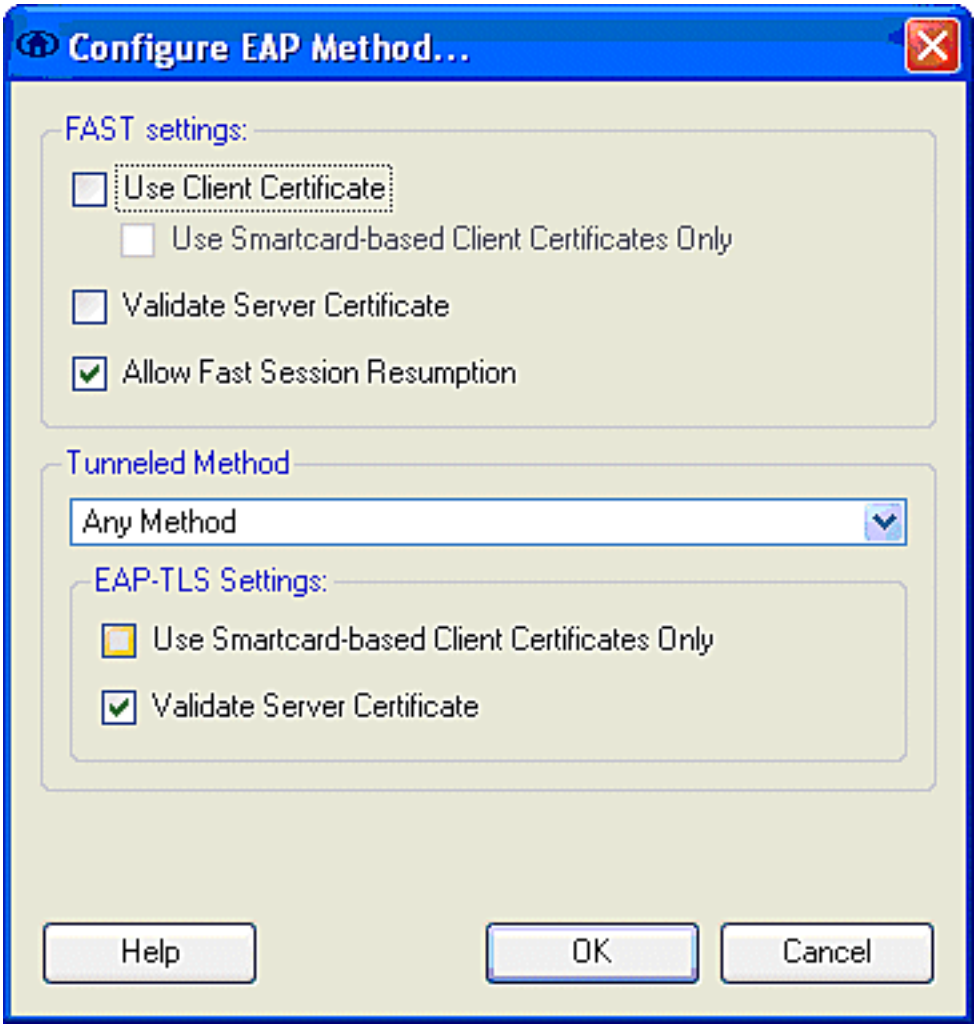
Onder FAST-instellingen is het mogelijk om **een snelle sessiehervatting toe te staan**, hetgeen de hervatting mogelijk maakt van een MAP-FAST-sessie gebaseerd op de informatie van de tunnel (TLS-sessie) in plaats van de vereiste van een volledige MAP-FAST-herauthenticatie. Als de EAP-FAST-server en de client gemeenschappelijke kennis hebben van de TLS-sessieinformatie waarover in de eerste EAP-FAST-verificatieuitwisseling is onderhandeld, kan de sessie worden hervat.

Opmerking: zowel EAP-FAST-server als client moeten worden geconfigureerd voor EAP-FAST-sessie.

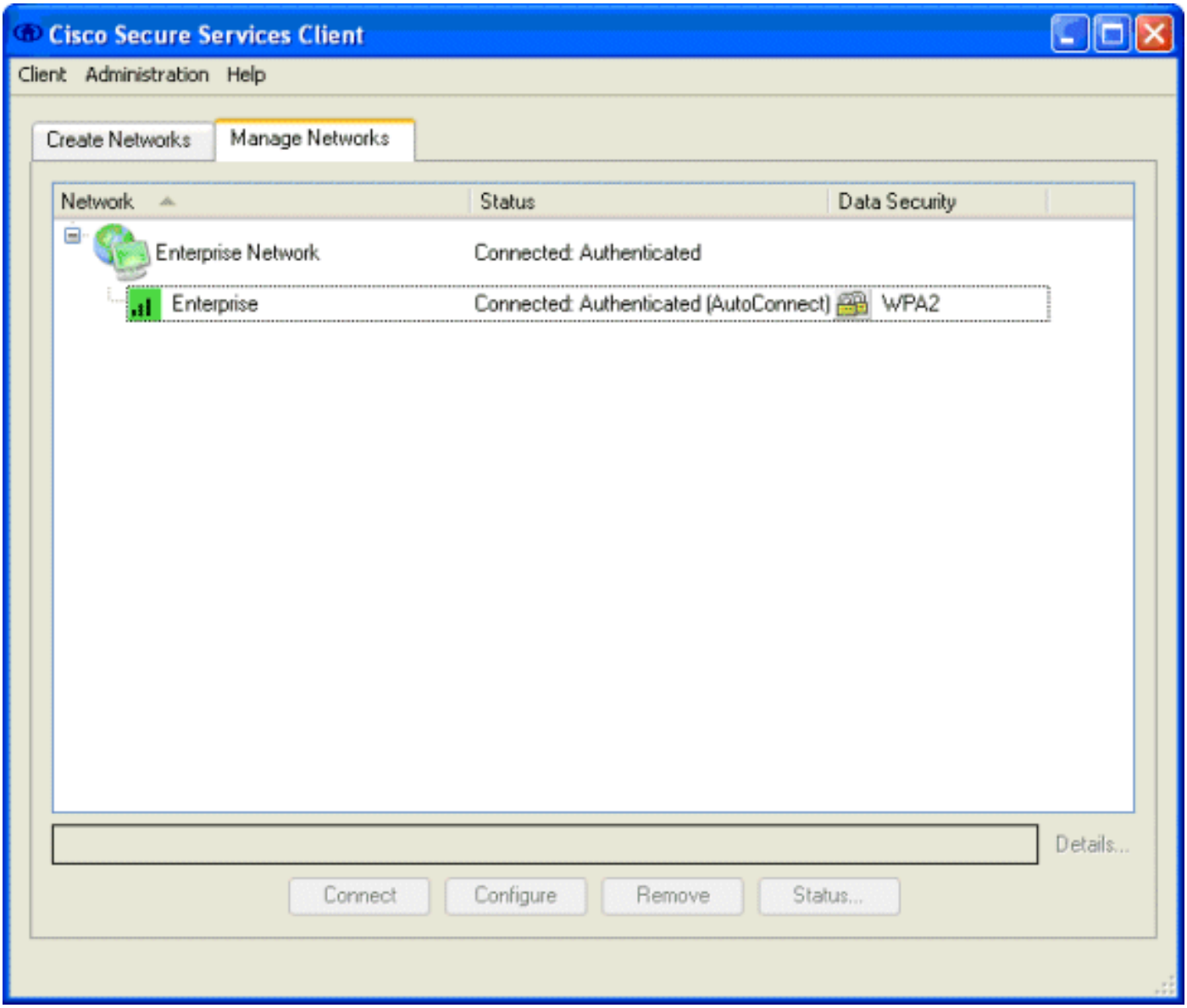
Specificeer onder Tunneled Methode > EAP-TLS Instellingen **elke methode** om de EAP-MSCHAPv2 voor PAC-automatische voorziening en EAP-GTC voor authenticatie toe te staan. Als u een Microsoft-formaat database gebruikt, zoals Active Directory, en als u geen EAP-FAST v1

clients op het netwerk ondersteunt, kunt u ook het gebruik van alleen **MSCHAPv2** specificeren als de Tunneled Methode.

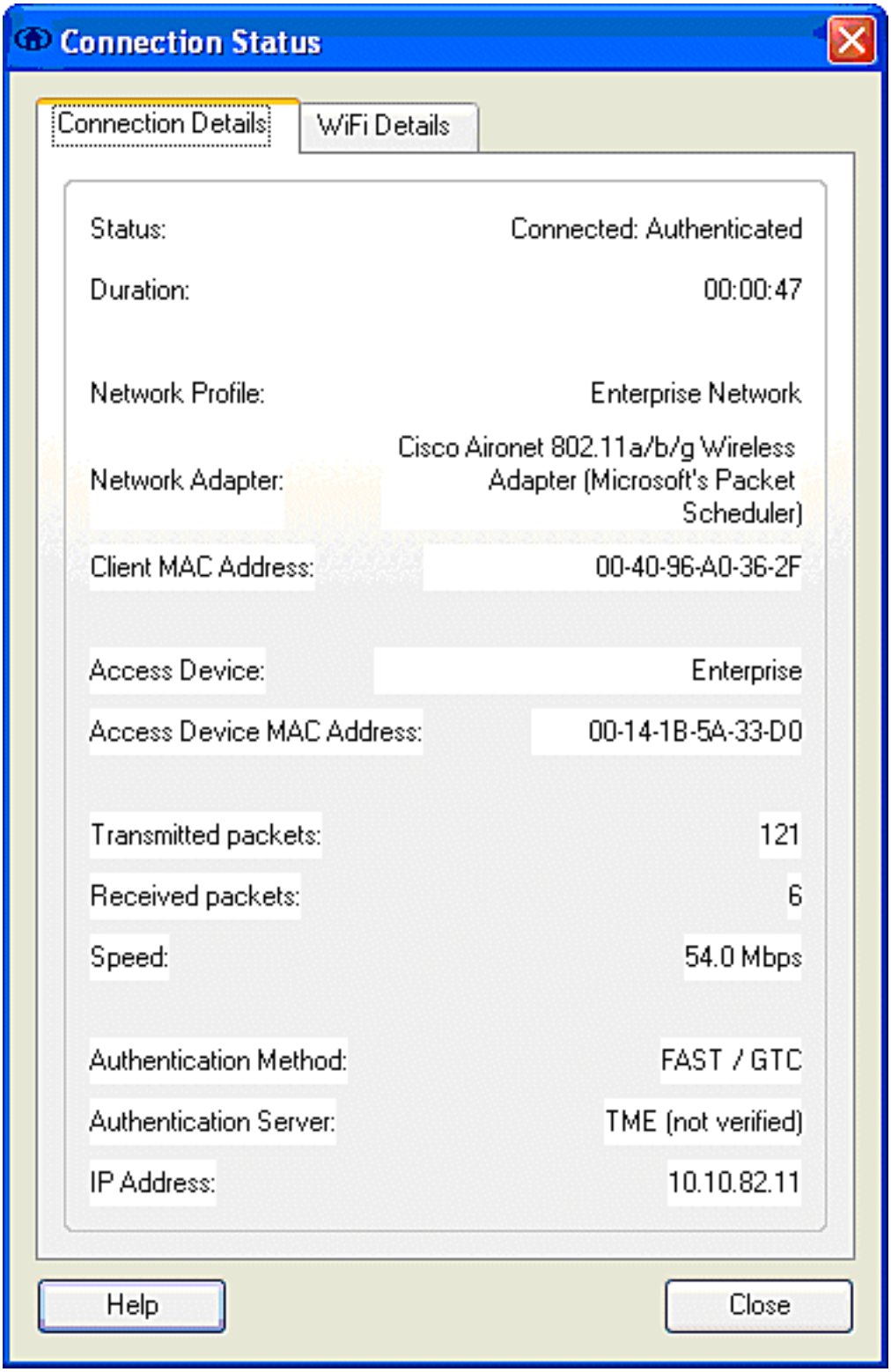
N.B.: Geldig servercertificaat is standaard ingeschakeld onder de MAP-TLS instellingen in dit venster. Aangezien het voorbeeld geen EAP-TLS als interne authenticatiemethode gebruikt, is dit veld niet van toepassing. Als dit veld is ingeschakeld, stelt het de cliënt in staat het servercertificaat naast de servervalidatie van het client certificaat binnen EAP-TLS te valideren.

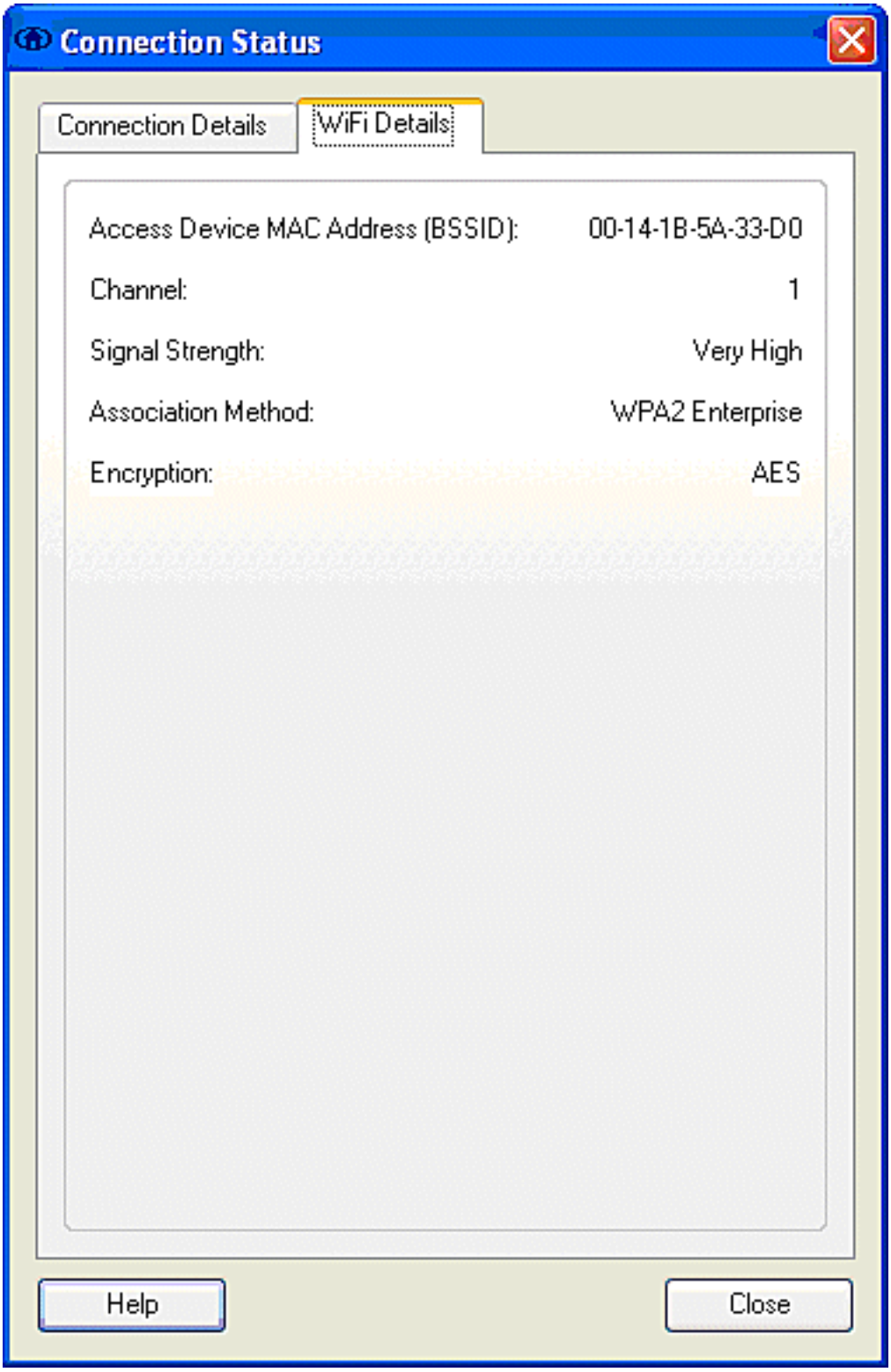


Klik op **OK** om de MAP-FAST instellingen op te slaan. Omdat de client is ingesteld voor "automatisch opzetten" onder profiel, wordt er automatisch associatie/verificatie met het netwerk gestart. In het tabblad Netwerk beheren, geven het veld Netwerk, Status en gegevensbeveiliging de verbindingsstatus van de client aan. Van het voorbeeld, wordt gezien dat het Netwerk van de Enterprise van het Profiel in gebruik is, en het apparaat van de Toegang van het Netwerk is de SSID Enterprise, die Connected:Authenticated en gebruikt Automatisch verbinden. Het veld Beveiliging van gegevens geeft het 802.11-coderingstype aan dat wordt gebruikt, dat in dit voorbeeld WAP2 is.



Nadat de client voor authenticatie is geselecteerd, kiest u **SSID** onder het profiel in het tabblad Oplossingen beheren en klikt u op **Status** om verbindingsdetails te vragen. Het venster Connection Details geeft informatie over het clientapparaat, de verbindingsstatus en de statistieken en de verificatiemethode. Het tabblad WiFi biedt details over de 802.11-verbindingsstatus, waaronder RSSI, 802.11-kanaal en verificatie/encryptie.


Connection Status
Connection Details
WiFi Details
Status:
Connected: Authenticated
Duration:
00:00:47
Network Profile:
Enterprise Network
Network Adapter:
Cisco Aironet 802.11a/b/g Wireless Adapter (Microsoft's Packet Scheduler)
Client MAC Address:
00-40-96-A0-36-2F
Access Device:
Enterprise
Access Device MAC Address:
00-14-1B-5A-33-D0
Transmitted packets:
121
Received packets:
6
Speed:
54.0 Mbps
Authentication Method:
FAST / GTC
Authentication Server:
TME (not verified)
IP Address:
10.10.82.11
Help
Close



Als systeembeheerder hebt u recht op het diagnostische hulpprogramma, Cisco Secure Services Client System Report, dat beschikbaar is bij de standaard CSSC-distributie. Dit hulpprogramma is beschikbaar in het beginmenu of in de CSSC-directory. Klik om gegevens te verkrijgen op **Verzamelen van gegevens > Kopieer naar het klembord > Rapportbestand lokaliseren**. Dit leidt een venster van Microsoft File Explorer naar de map met het zipped rapport. Binnen het zipped bestand bevinden de meest bruikbare gegevens zich onder log (log_huidige).

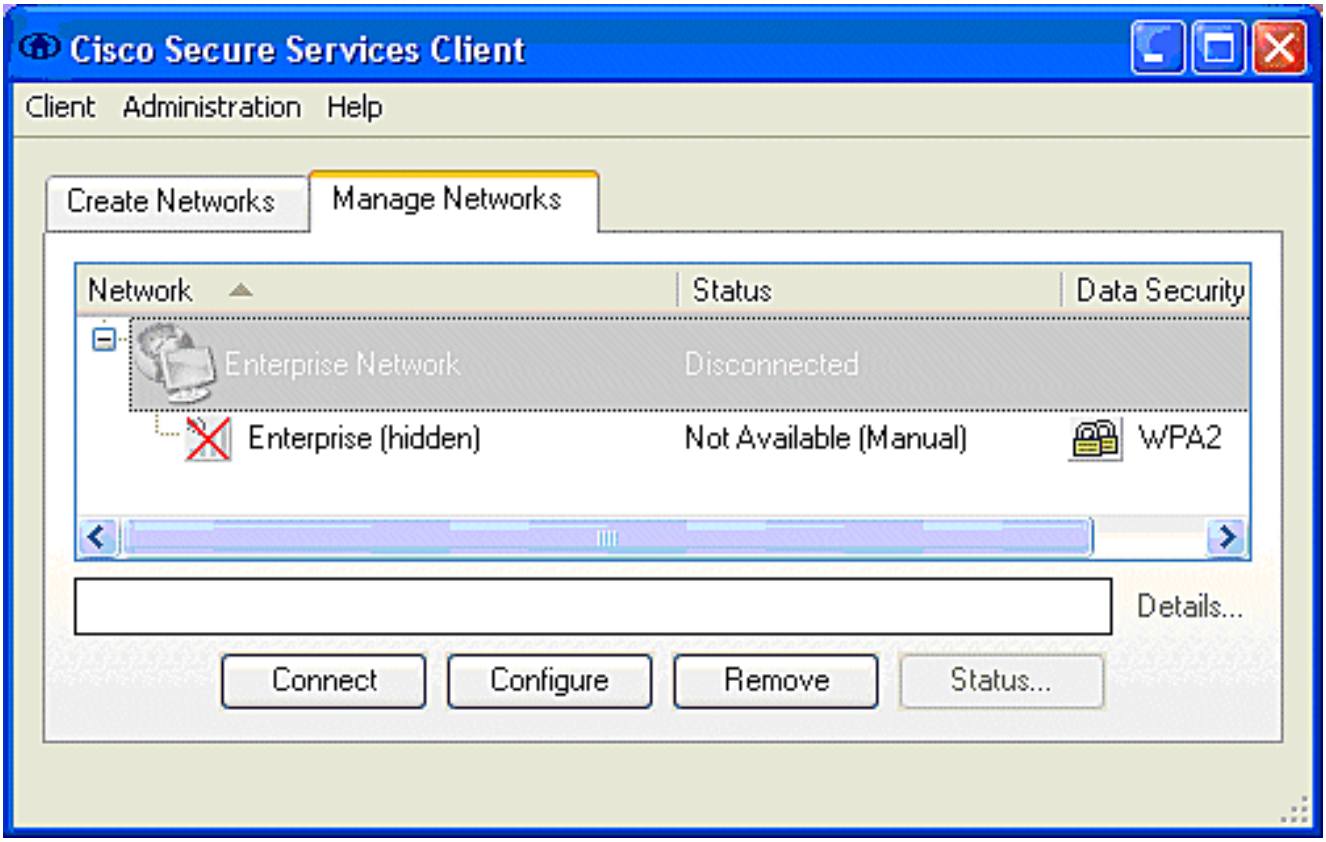
Het hulpprogramma geeft de huidige status van CSSC, interface en driver-details, evenals de WLAN-informatie (SSID gedetecteerd, associatie-status, enzovoort). Dit kan nuttig zijn, vooral om problemen met connectiviteit tussen CSSC en de WLAN-adapter te diagnosticeren.

Controleer de bediening

Na de configuratie van de Cisco Secure ACS-server, WLAN-controller, CSSC-client en vermoedelijk correcte configuratie- en databases, wordt het WLAN-netwerk geconfigureerd voor EAP-FAST-verificatie en beveiligde client-communicatie. Er zijn talrijke punten die kunnen worden gecontroleerd om de vooruitgang / fouten voor een beveiligde sessie te controleren.

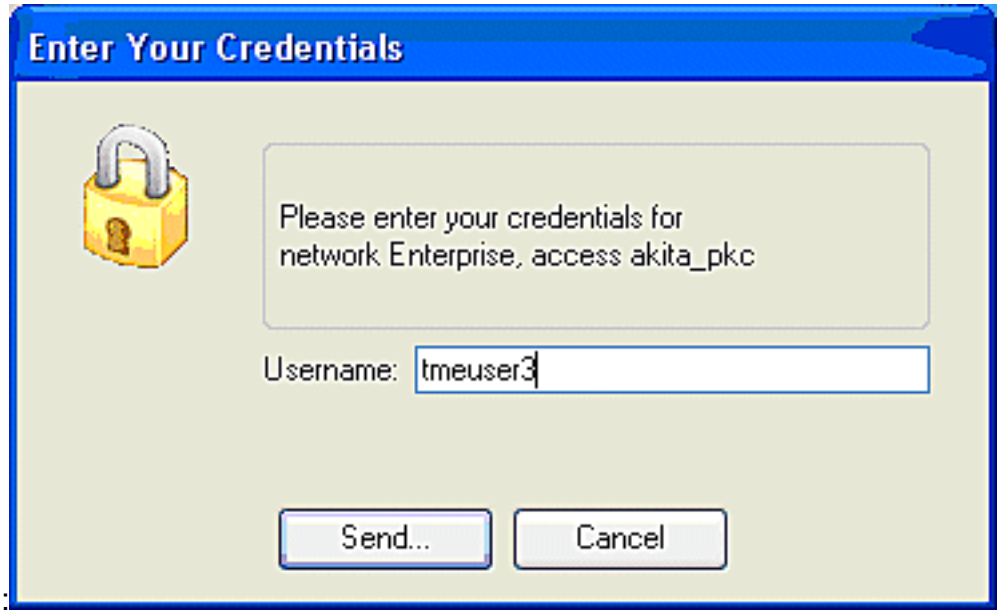
Om de configuratie te testen, probeert u een draadloze client te associëren met de WLAN-controller met EAP-FAST-verificatie.

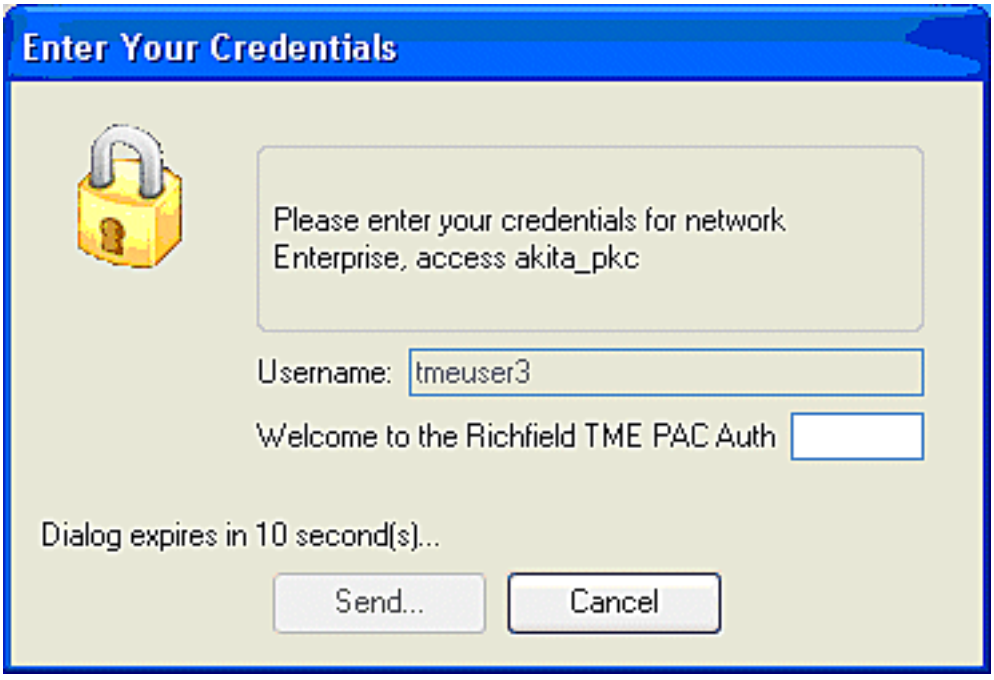
1. Als CSSC is ingesteld voor automatische verbinding, probeert de client deze verbinding automatisch. Als deze niet is ingesteld voor Auto-Connection en Single Sign-on bewerking, moet de gebruiker de WLAN-verbinding initiëren via de **Connect**-radioknop. Hiermee wordt het associatieproces van 802.11 op gang gebracht waarover de MAP - authenticatie plaatsvindt.Dit is een voorbeeld:



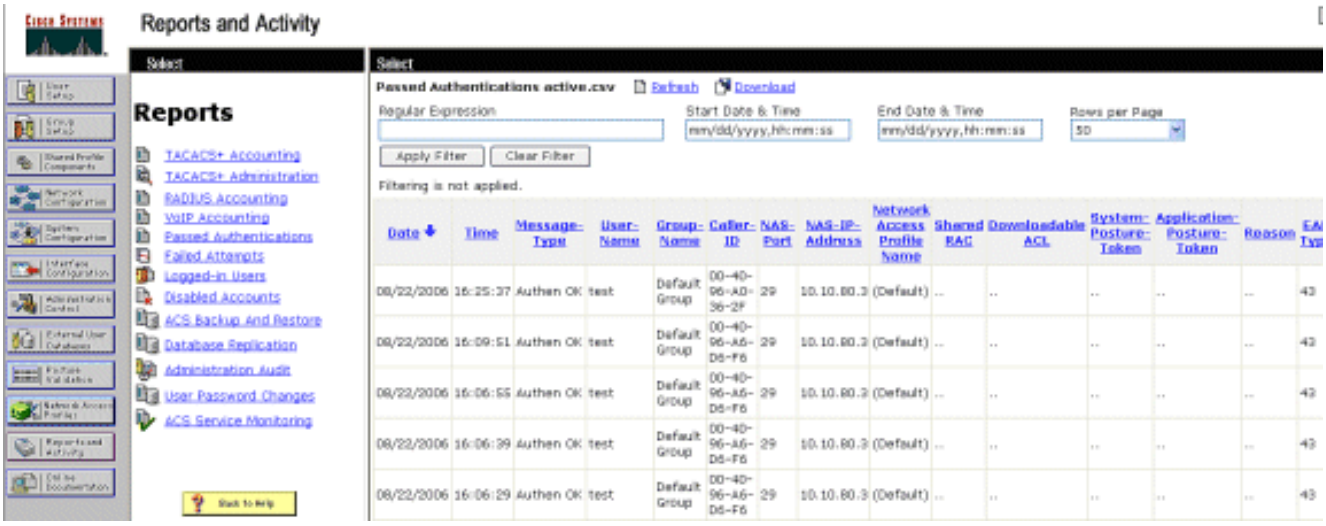
2. De gebruiker wordt vervolgens verzocht de gebruikersnaam en het wachtwoord voor de MAP-FAST-verificatie te verstrekken (van de EAP-FAST PAC-autoriteit of ACS).Dit is een

voorbeeld:

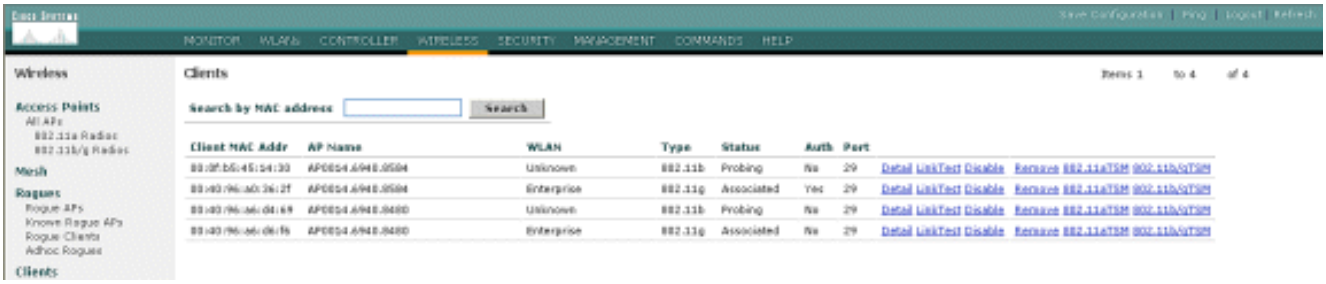




3. De CSSC client geeft via het WLC de gebruikersreferenties toe aan de RADIUS-server (Cisco Secure ACS) om de aanmeldingsgegevens te valideren. ACS verifieert de gebruikersgeloofsbrieven met een vergelijking van de gegevens en het gevormde gegevensbestand (in de voorbeeldconfiguratie, is de externe databank Windows Active Directory) en verleent toegang tot de draadloze client wanneer de gebruikersgeloofsbrieven geldig zijn. Het Passed Authentications rapport op de ACS-server toont aan dat de client de RADIUS/EAP-verificatie heeft doorlopen.Dit is een voorbeeld:



4. Bij een succesvolle RADIUS/EAP-verificatie wordt de draadloze client (00:40:96:ab:36:2f in dit voorbeeld) geauthenticeerd met de AP/WLAN-controller.



Bijlage

Naast de diagnostische en statusinformatie, die beschikbaar is in de Cisco Secure ACS en Cisco WLAN-controller, zijn er extra punten die kunnen worden gebruikt om EAP-FAST-verificatie te diagnosticeren. Hoewel de meerderheid van de authenticiteitsproblemen kan worden gediagnosticeerd zonder het gebruik van een WLAN-snuffelaar of het zuiveren van een EAP-uitwisselingsprogramma bij de WLAN-controller, wordt dit referentiemateriaal opgenomen om probleemoplossing te helpen.

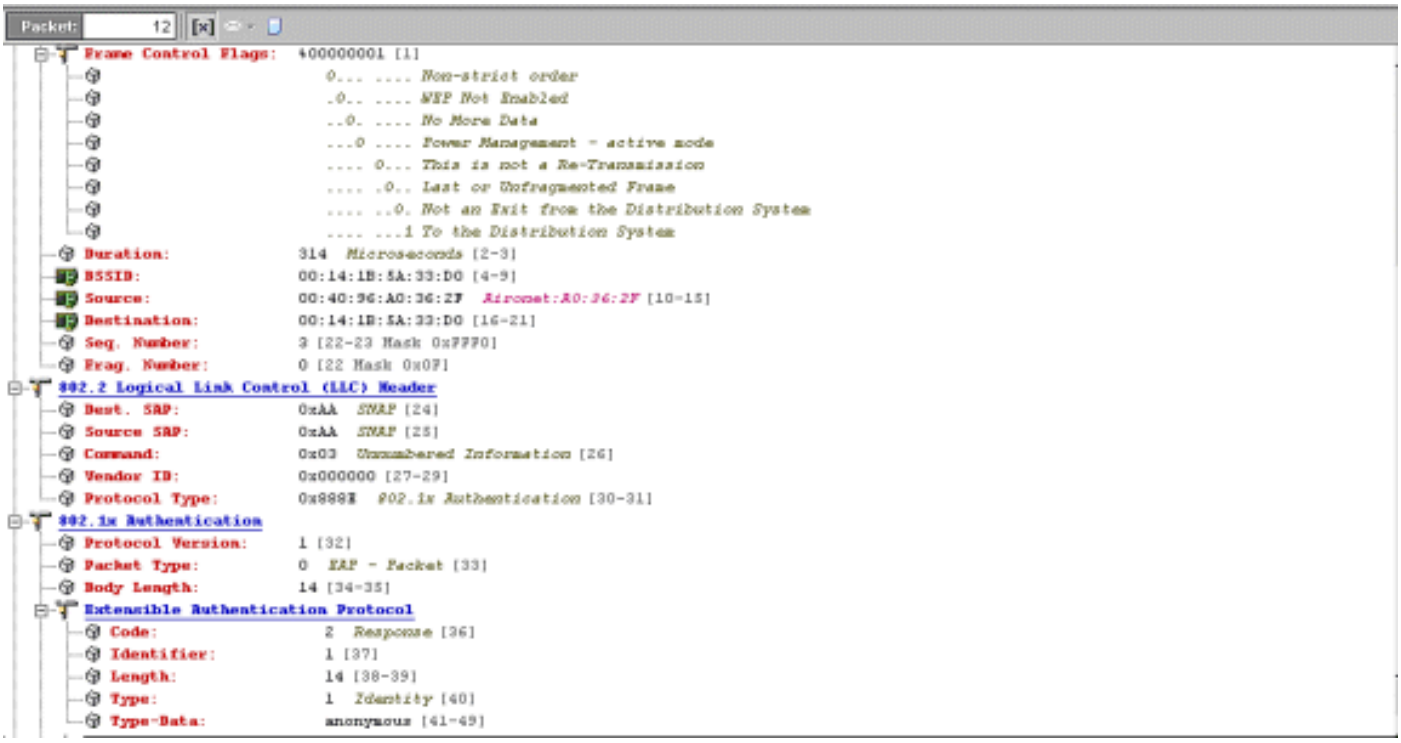
Snellere vastlegging voor EAP-FAST-uitwisseling

Deze 802.11 snuffelzoekopdracht toont de authenticatie-uitwisseling.

Source	Flags	Channel	Signal	Data Rate	Size	Relative Time	Protocol	Summary
00:14:1B:5A:33:D0	*	11	68%	36.0	101	00.033877	802.11 Assoc Rsp	FC=...R....,SN=2867,FN= 0,Status...
00:14:1B:5A:33:D0	*	11	70%	24.0	101	00.036453	802.11 Assoc Rsp	FC=...R....,SN=2867,FN= 0,Status...
00:14:1B:5A:33:D0		11	71%	54.0	90	00.036494	802.1x	FC=.F......,SN=2868,FN= 0
Aironet:A0:36:2F		11	54%	1.0	82	00.123205	EAP Response	FC=T.......,SN= 3,FN= 0
00:14:1B:5A:33:D0	#	11	71%	1.0	14	00.123517	802.11 Ack	FC=.........
00:14:1B:5A:33:D0		11	67%	54.0	65	00.165611	802.1x	FC=.F......,SN=2870,FN= 0
Aironet:A0:36:2F		11	55%	1.0	82	00.173920	EAP Response	FC=T.......,SN= 4,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.174228	802.11 Ack	FC=.........
00:14:1B:5A:33:D0		11	68%	54.0	66	00.178863	802.1x	FC=.F......,SN=2871,FN= 0
Aironet:A0:36:2F		11	58%	1.0	282	00.200632	EAP Response	FC=T.......,SN= 5,FN= 0
Aironet:A0:36:2F		11	58%	1.0	282	00.203340	EAP Response	FC=T..R....,SN= 5,FN= 0
00:14:1B:5A:33:D0	#	11	71%	1.0	14	00.203639	802.11 Ack	FC=.........
00:14:1B:5A:33:D0		11	70%	54.0	188	00.207634	802.1x	FC=.F......,SN=2872,FN= 0
Aironet:A0:36:2F		11	55%	1.0	105	00.216295	EAP Response	FC=T.......,SN= 6,FN= 0
Aironet:A0:36:2F		11	57%	1.0	105	00.217444	EAP Response	FC=T..R....,SN= 6,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.217754	802.11 Ack	FC=.........
00:14:1B:5A:33:D0		11	67%	54.0	99	00.222799	802.1x	FC=.F......,SN=2874,FN= 0
Aironet:A0:36:2F		11	55%	1.0	152	00.254189	EAP Response	FC=T.......,SN= 7,FN= 0
00:14:1B:5A:33:D0	#	11	68%	1.0	14	00.254499	802.11 Ack	FC=.........
00:14:1B:5A:33:D0		11	64%	54.0	147	00.288950	802.1x	FC=.F.R....,SN=2875,FN= 0
Aironet:A0:36:2F		11	55%	1.0	232	00.318087	EAP Response	FC=T.......,SN= 8,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.318383	802.11 Ack	FC=.........
00:14:1B:5A:33:D0		11	68%	54.0	44	00.326833	802.1x	FC=.F......,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	65%	54.0	44	00.326882	802.1x	FC=.F.R....,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	67%	48.0	44	00.326922	802.1x	FC=.F.R....,SN=2877,FN= 0
00:14:1B:5A:33:D0		11	67%	54.0	157	00.326964	802.1x	FC=.F......,SN=2878,FN= 0
Aironet:A0:36:2F		11	57%	1.0	157	00.333742	EAP01-Key	FC=T.......,SN= 9,FN= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.334019	802.11 Ack	FC=.........
00:14:1B:5A:33:D0		11	65%	54.0	207	00.340467	802.1x	FC=.F......,SN=2879,FN= 0
00:14:1B:5A:33:D0		11	67%	54.0	207	00.341130	802.1x	FC=.F.R....,SN=2879,FN= 0
Aironet:A0:36:2F		11	57%	1.0	135	00.342542	EAP01-Key	FC=T.......,SN= 10,FN= 0

Dit pakket toont de eerste EAP-FAST-respons.

Toelichting: Zoals bij de CSSC-client is ingesteld, wordt in de eerste MAP-respons anoniem gebruikt als de externe MAP-identiteit.



Debug in de WLAN-controller

Deze debug-opdrachten kunnen worden gebruikt bij de WLAN-controller om de voortgang van de verificatieuitwisseling te bewaken:

- **debug aaaaaathedingen activeren**
- **u kunt gegevens debug a**

- debug dot1x gebeurtenissen in staat stellen
- debug dot1x-staten

Dit is een voorbeeld van het begin van een verificatietransactie tussen de CSSC-client en ACS zoals gecontroleerd bij de WLAN-controller met de debugs:

```
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing RSN IE type 48,
   length 20 for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received RSN IE with
   0 PMKIDs from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x -
   moving mobile 00:40:96:a0:36:2f into Connecting state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP-
   Request/Identity to mobile 00:40:96:a0:36:2f (EAP Id 1)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received Identity Response
   (count=1) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f EAP State update from
   Connecting to Authenticating for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x - moving mobile
   00:40:96:a0:36:2f into Authenticating state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth
   Response state for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: AuthenticationRequest: 0x138dd764
Thu Aug 24 18:20:54 2006:       Callback.......0x10372764
Thu Aug 24 18:20:54 2006:       protocolType...0x00040001
Thu Aug 24 18:20:54 2006:       proxyState.....00:40:96:A0:36:2F-11:00
Thu Aug 24 18:20:54 2006:       Packet contains 15 AVPs (not shown)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Successful transmission of
   Authentication Packet (id 84) to 10.1.1.12:1812, proxy state0
Thu Aug 24 18:20:54 2006: ****Enter processIncomingMessages: response code=11
Thu Aug 24 18:20:54 2006: ****Enter processRadiusResponse: response code=11
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Access-Challenge received from
   RADIUS server 10.1.1.12 for mobile 00:40:96:a0:36:2f rec7
Thu Aug 24 18:20:54 2006: AuthorizationResponse: 0x11c8a394
Thu Aug 24 18:20:54 2006:       structureSize..147
Thu Aug 24 18:20:54 2006:       resultCode.....255
Thu Aug 24 18:20:54 2006:       protocolUsed...0x00000001
Thu Aug 24 18:20:54 2006:       proxyState.....00:40:96:A0:36:2F-11:00
Thu Aug 24 18:20:54 2006:       Packet contains 4 AVPs (not shown)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing Access-Challenge
   for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth Req state
   (id=249) for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f WARNING:
   updated EAP-Identifer 1 ===> 249 for STA 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP Request from
   AAA to mobile 00:40:96:a0:36:2f (EAP Id 249)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAP Response from
   mobile 00:40:96:a0:36:2f (EAP Id 249, EAP Type 3)
```

Dit is de succesvolle voltooiing van de MAP-uitwisseling van de controller debug (met WAP2-verificatie):

```
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing Access-
   Accept for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Applying new AAA
   override for station 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Override values for station
```

```
   00:40:96:a0:36:2f source: 4, valid bits: 0x0
qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout:
   -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, r1'
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Unable to apply override
   policy for station 00:40:96:a0:36:2f - VapAllowRadiusOverride E
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Creating a new PMK Cache Entry
   for station 00:40:96:a0:36:2f (RSN 2)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Adding BSSID
   00:14:1b:5a:33:d0 to PMKID cache for station 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: New PMKID: (16)
Thu Aug 24 18:20:54 2006:      [0000] a6 c0 02 95 66 e8 ed 9b 1c 65 9b
   72 1f 3f 5f 5b
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP-Success
   to mobile 00:40:96:a0:36:2f (EAP Id 0)
Thu Aug 24 18:20:54 2006: Including PMKID in M1  (16)
Thu Aug 24 18:20:54 2006:
   [0000] a6 c0 02 95 66 e8 ed 9b 1c 65 9b 72 1f 3f 5f 5b
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAPOL-Key Message to
   mobile 00:40:96:a0:36:2f state INITPMK (message 1), repl0
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend
   Auth Success state (id=0) for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received Auth Success
   while in Authenticating state for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x -
   moving mobile 00:40:96:a0:36:2f into Authenticated state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-
   Key from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Invalid EAPOL version
   (1) in EAPOL-key message from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-key
   in PKT_START state (message 2) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Stopping retransmission
   timer for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAPOL-Key Message
   to mobile 00:40:96:a0:36:2f state PTKINITNEGOTIATING (messa1
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received
   EAPOL-Key from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Invalid EAPOL version (1)
   in EAPOL-key message from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-key in
   PTKINITNEGOTIATING state (message 4) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: AccountingMessage
   Accounting Interim: 0x138dd764
Thu Aug 24 18:20:54 2006: Packet contains 20 AVPs:
Thu Aug 24 18:20:54 2006:
   AVP[01] User-Name.................enterprise (10 bytes)
Thu Aug 24 18:20:54 2006: AVP[02]
   Nas-Port..........................0x0000001d (29) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[03]
   Nas-Ip-Address....................0x0a0a5003 (168448003) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[04]
   Class.............................CACS:0/28b5/a0a5003/29 (22 bytes)
Thu Aug 24 18:20:54 2006: AVP[05]
   NAS-Identifier....................ws-3750 (7 bytes)
Thu Aug 24 18:20:54 2006: AVP[06]
   Airespace / WLAN-Identifier........0x00000001 (1) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[07]
   Acct-Session-Id...................44ede3b0/00:40:
   96:a0:36:2f/14 (29 bytes)
Thu Aug 24 18:20:54 2006: AVP[08]
   Acct-Authentic....................0x00000001 (1) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[09]
   Tunnel-Type.......................0x0000000d (13) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[10]
```

```
   Tunnel-Medium-Type.................0x00000006 (6) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[11]
   Tunnel-Group-Id....................0x3832 (14386) (2 bytes)
Thu Aug 24 18:20:54 2006: AVP[12]
   Acct-Status-Type...................0x00000003 (3) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[13]
   Acct-Input-Octets..................0x000b99a6 (760230) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[14]
   Acct-Output-Octets.................0x00043a27 (277031) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[15]
   Acct-Input-Packets.................0x0000444b (17483) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[16]
   Acct-Output-Packets................0x0000099b (2459) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[17]
   Acct-Session-Time..................0x00000a57 (2647) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[18]
   Acct-Delay-Time....................0x00000000 (0) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[19]
   Calling-Station-Id.................10.10.82.11 (11 bytes)
Thu Aug 24 18:20:54 2006: AVP[20]
   Called-Station-Id..................10.10.80.3 (10 bytes)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f
   Stopping retransmission timer for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:57 2006: User admin authenticated
```

Gerelateerde informatie

- Installatiegids voor Cisco Secure ACS voor Windows Server
- Configuratiehandleiding voor Cisco Secure ACS 4.1
- WLAN-toegang beperken op basis van SSID met WLC en Cisco Secure ACS-configuratievoorbeeld
- EAP-TLS onder Unified Wireless Network met ACS 4.0 en Windows 2003
- Configuratievoorbeeld van dynamische VLAN-toewijzing met RADIUS-server en draadloze LAN-controllers
- Technische ondersteuning en documentatie – Cisco Systems